Secure-Hospital-Network-Architecture

Instructor: Dr. SYED HUSSEIN

Prepared by: -

Vignesh Reddy Sama

Table of Contents

ABSTRACT:

Designing a network for a hospital campus demands a robust, scalable, and future-proof infrastructure that ensures seamless communication, secure operations, and exceptional healthcare delivery. The network must provide uninterrupted, real-time access to critical data such as electronic health records (EHRs), imaging systems, and patient monitoring data to facilitate timely and precise medical decisions. Scalability is vital to accommodate future growth, including new departments, medical technologies, and the increasing integration of IoT devices like wearable health monitors and smart diagnostic tools. Flexibility is equally important to adapt to the evolving demands of healthcare, such as telemedicine services, remote consultations, and AI-driven diagnostics. The infrastructure must comply with stringent regulatory mandates like the Security and Data Privacy Act (SADBA) to ensure the confidentiality, integrity, and availability of sensitive patient information. This compliance, combined with operational efficiency, creates a secure environment that fosters collaboration among healthcare professionals, enhances patient outcomes, and supports innovation. A well-designed hospital network becomes the backbone of modern healthcare delivery, providing reliable communication, optimized workflows, and a strong foundation for long-term growth and excellence.

Overview

- **Comprehensive Infrastructure:**
  The Hospital Campus Network is designed to meet the diverse needs of a hospital environment, covering various areas such as emergency rooms, operating theaters, patient wards, and administrative offices.
- **Network Architecture:**
  The architecture consists of core, distribution, and access layers, ensuring high availability, reliability, and scalability to support the demanding healthcare operations.
- **Key Components:**
  The network includes essential components such as switches, routers, access points, servers, and security appliances, all integrated to enable seamless communication, data sharing, and resource management across the hospital.
- **Security and Compliance:**
  Robust security measures, including encryption and advanced protocols, are in place to safeguard patient data and ensure compliance with regulatory standards.

Benefits of well designed:

- **Improved Patient Care**: Real-time access to patient records and diagnostic data.
- **Operational Efficiency**: Streamlined communication and data sharing across departments.
- **Enhanced Security**: Protection against data breaches and compliance with legal standards.
- **Scalability**: Ability to expand and integrate new technologies as the hospital grows.
- This design ensures that the hospital operates efficiently, securely, and reliably, supporting both medical staff and administrative functions in delivering high-quality healthcare

OBJECTIVES:

- The hospital campus network aims to improve healthcare delivery within the hospital by focusing on the following key objectives:
- **Seamless Communication**: Ensuring efficient and uninterrupted communication across departments and healthcare professionals.
- Timely Access to Information: Enabling quick access to critical patient data, medical records, and hospital systems.
- **Scalability and Flexibility**: Designing the network to grow and adapt as healthcare needs evolve.
- **Data Security and Compliance**: Safeguarding patient information while meeting healthcare regulatory requirements.
- **Disaster Recovery and Continuity**: Implementing strategies to maintain operations and recover swiftly during unexpected disruptions.
- **Patient Experience and Satisfaction:** Enhancing overall patient experience through efficient, reliable network services.

SYSTEM DEVELOPMENT LIFE CYCLE(SDLC):

The network design for the Airport is done in the following phases.

1. Identifying Customer Needs or Goals
2. Logical Network Design
3. Physical Network Design
4. Testing/ Optimizing/ Documenting

BUSINESS GOALS:

1. The hospital campus network is designed to enhance healthcare delivery by focusing on these key goals:
2. **Efficient Communication**: Ensuring smooth, uninterrupted communication between departments and healthcare professionals for better coordination.
3. **Quick Access to Information**: Providing fast access to critical patient data, medical records, and hospital systems to support timely decision-making.
4. **Scalability and Flexibility**: Building a network that can expand and adapt to evolving healthcare needs and future technologies.
5. **Data Security and Compliance**: Protecting patient information while adhering to healthcare regulations to maintain privacy and security.
6. **Disaster Recovery and Continuity**: Establishing robust systems to ensure hospital operations can continue and recover quickly in case of unexpected events.
7. **Enhanced Patient Experience**: Improving patient satisfaction by delivering reliable, efficient network services that support smooth healthcare operations.
8. **Optimized Administration**: Focuses on identifying and resolving inefficiencies in administrative processes by introducing structured improvements to streamline workflows, minimize paperwork, and boost overall productivity in hospital management.
9. **Comprehensive Training and Documentation:** Ensures that staff stay proficient, compliant, and adaptable by providing ongoing education and clear guidelines on evolving technologies, regulations, and best practices.
10. These objectives work together to create a network that not only supports hospital staff but also ensures a positive experience for patients.

TECHNICAL GOALS:

1. **Network Optimization** (Performance): Enhances network efficiency by reducing latency and maximizing throughput.
2. **Network Scalability:** Allows the network to grow and handle increasing traffic without performance loss.
3. **Redundancy and Reliability**: Implements backup systems to ensure continuous operation in case of failures.
4. **Data Security:** Protects data from unauthorized access, breaches, and loss through encryption and secure protocols.
5. **Affordability:** Balances cost-effectiveness while meeting network performance and security needs.
6. **Availability**: Guarantees uninterrupted network access and service uptime for users and applications.
7. Security and Compliance: Ensures network integrity and adheres to legal regulations to protect sensitive data

STRUCTURE OF THE HOSPITAL:

- Floors – 3
- Doctors – 15
- Nurses – 30
- Administrative Staff – 10
- Non-Administrative Staff – 25

Network topology

- Star Topology: Inside each department or floor.
- Hierarchical Topology: For organizing the network into layers (access, distribution, core).
- Mesh Topology: For the backbone connections between routers.

Servers

- HTTP: Hyper Text Transfer Protocol
- SMTP: Simple Mail Transfer protocol
- AAA: Authentication Authorization Accounting

DEPARTMENTS IN HOSPITAL:

- General Ward
- ICU
- IT Department
- Administration
- Reception, Lobby, Parking, Cafeteria

Logical design:

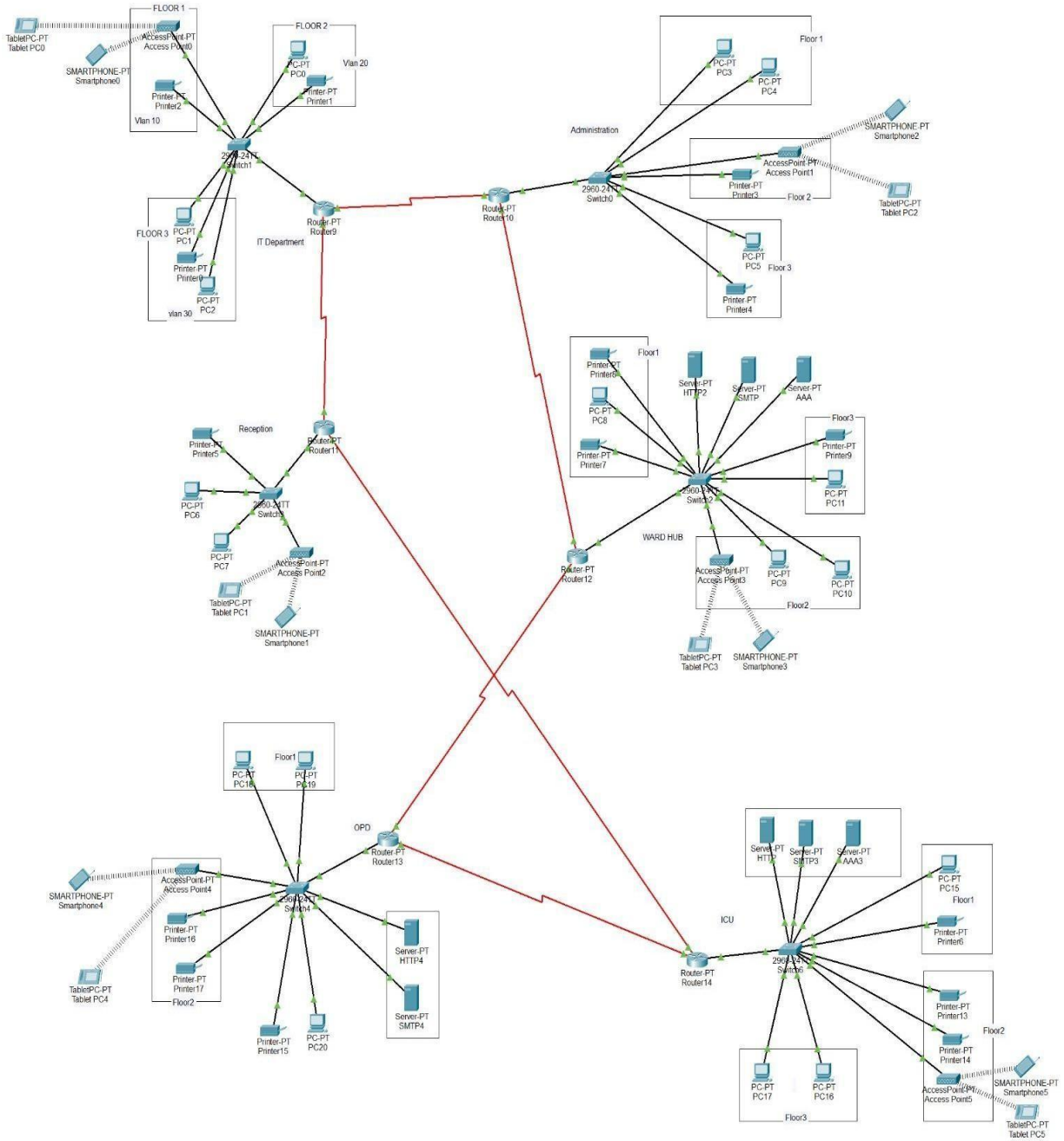

Fig 1: Complete hospital network design

Design & IP Addressing of IT Hub

The **IT Department** network serves as the backbone of the organization's technological operations, ensuring seamless connectivity and efficient management of resources across all departments. This design integrates essential components, including PCs for administrative tasks, printers for documentation needs, access points for wireless connectivity, and switches to facilitate robust communication between devices. Leveraging VLAN segmentation, the network enhances security by isolating traffic and reducing the risk of unauthorized access. A centralized router connects the IT Department to other departments, allowing data exchange and coordination. This infrastructure supports the organization's critical operations, maintaining reliability, scalability, and streamlined workflows for optimal performance.

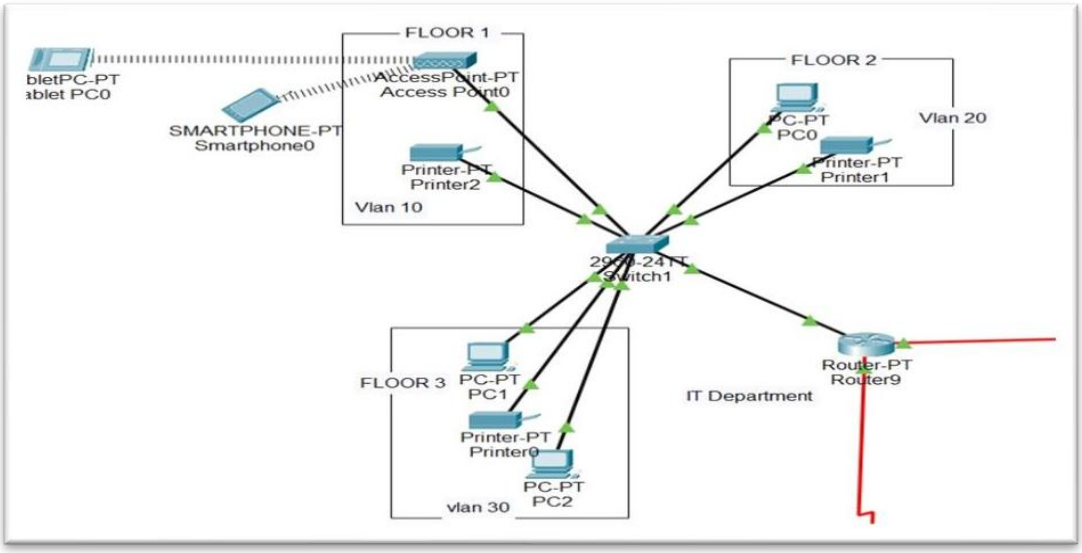

Fig 2 IT hub

Design & IP Addressing Assignment

This section will summarize the VLAN and IP addressing for LAN and WAN of the new proposed network infrastructure design.

VLAN	Device	IP Address	Subnet Mask	Default Gateway
VLAN 10	Router Gateway	192.168.10.1	255.255.255.0	-
	PC0 (Floor 1)	192.168.10.10	255.255.255.0	192.168.10.1
	Printer2 (Floor 1)	192.168.10.11	255.255.255.0	192.168.10.1
	Access Point	192.168.10.12	255.255.255.0	192.168.10.1

VLAN 20	Router Gateway	192.168.20.1	255.255.255.0	-
	PC1 (Floor 2)	192.168.20.10	255.255.255.0	192.168.20.1
	Printer1 (Floor 2)	192.168.20.11	255.255.255.0	192.168.20.1
VLAN 30	Router Gateway	192.168.30.1	255.255.255.0	-
	PC2 (Floor 3)	192.168.30.10	255.255.255.0	192.168.30.1
	Printer0 (Floor 3)	192.168.30.11	255.255.255.0	192.168.30.1

Design & Ip addressing for administration Department

The administration department supports essential tasks such as billing, human resource management, and logistics. The logical design integrates workstations with centralized databases and office management tools, ensuring smooth operations. Virtual LANs (VLANs) are implemented to separate administrative traffic from clinical data, improving both security and performance. Secure internet access is also provided for communication with external stakeholders, such as insurance companies and suppliers.

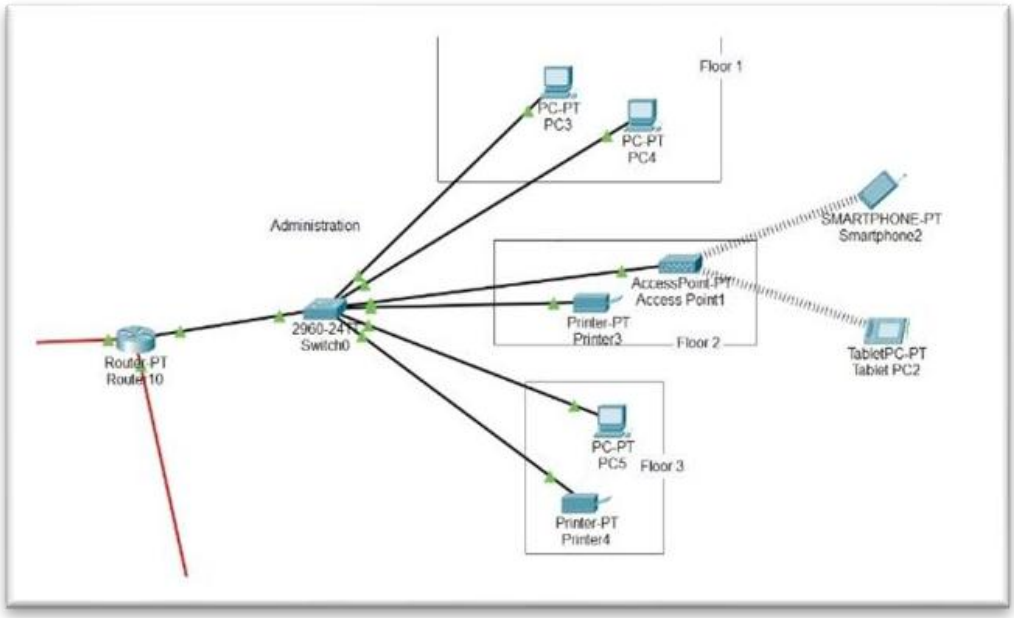

Fig 3 Administration Design

Device	IP Address	Subnet Mask	Default Gateway
Floor 1			
PC 1	192.168.10.2	255.255.255.0	192.168.10.1
PC 2	192.168.10.3	255.255.255.0	192.168.10.1
Floor 2			
Printer	192.168.20.2	255.255.255.0	192.168.20.1
Access Point	192.168.20.3	255.255.255.0	192.168.20.1
Floor 3			
PC 1	192.168.30.2	255.255.255.0	192.168.30.1
Printer	192.168.30.3	255.255.255.0	192.168.30.1

Design & IP Address of ICU

The ICU (Intensive Care Unit) is designed to support real-time data transmission for critical patient monitoring systems like ventilators and imaging devices. High-speed switches are deployed to minimize latency and ensure uninterrupted communication. The ICU network is also isolated using subnetting to enhance security and protect sensitive patient data. Additionally, failover mechanisms are implemented to guarantee continuous operation of life-critical systems.

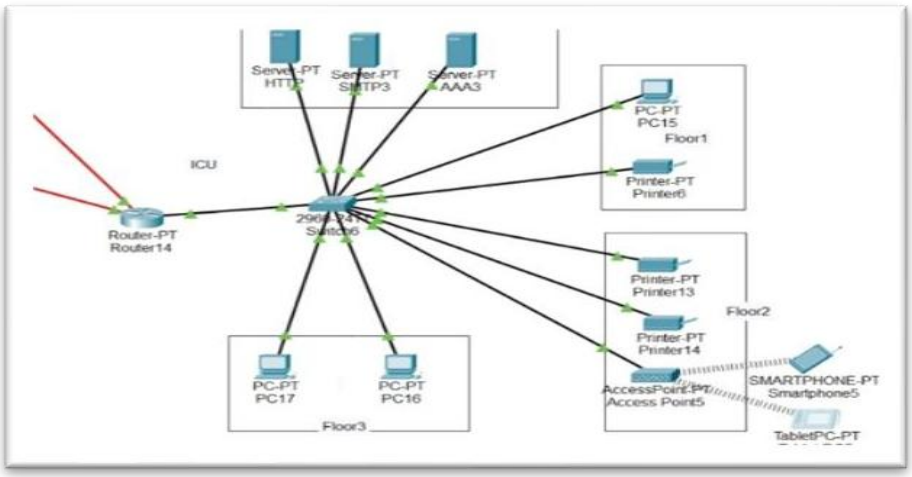

Fig 4 ICU Design

Device	VLA N	IP Address	Subnet	Port	Default Gateway
Router Sub interface	100	192.168.10.1	255.255.255.0	fa0/1	-
PC1 (Floor 1)	100	192.168.10.2	255.255.255.0	fa0/2	192.168.10.1
Printer (Floor 1)	100	192.168.10.3	255.255.255.0	fa0/3	192.168.10.1
Printer1 (Floor 2)	110	192.168.11.2	255.255.255.0	fa0/4	192.168.11.1
Printer2 (Floor 2)	110	192.168.11.3	255.255.255.0	fa0/5	192.168.11.1

Access Point	110	192.168.11.4	255.255.255.0	fa0/6	192.168.11.1
PC1 (Floor 3)	120	192.168.12.2	255.255.255.0	fa0/7	192.168.12.1
PC2 (Floor 3)	120	192.168.12.3	255.255.255.0	fa0/8	192.168.12.1
Server 1	200	192.168.20.2	255.255.255.0	fa0/9	192.168.20.1
Server 2	200	192.168.20.3	255.255.255.0	fa0/1 0	192.168.20.1
Server 3	200	192.168.20.4	255.255.255.0	fa0/1 1	192.168.20.1

The ICU department encompasses three floors, each with a distinct network environment. A central network switch acts as the hub, seamlessly connecting and coordinating the network operations across these floors. Within this framework, key servers play a pivotal role. The HTTP server ensures prompt access to web-based resources, while the SMTP server manages email communication, streamlining critical information sharing. Additionally, the AAA (Authentication, Authorization, and Accounting) server maintains robust security measures and user access control, ensuring the protection of sensitive patient data and hospital resources. This diagram provides a snapshot of the ICU department's network structure, emphasizing efficient connectivity, and vital server functions critical to patient care and operational integrity

Design & IP Address of OPD (Out-patent ward)

The Outpatient Department (OPD) manages consultations, diagnostic tests, and patient records. Workstations in the OPD are equipped with secure access to patient histories and imaging systems, while subnetting ensures segregation of outpatient and inpatient data. Wireless access is provided for doctors and staff using tablets or mobile devices, enhancing mobility and productivity.

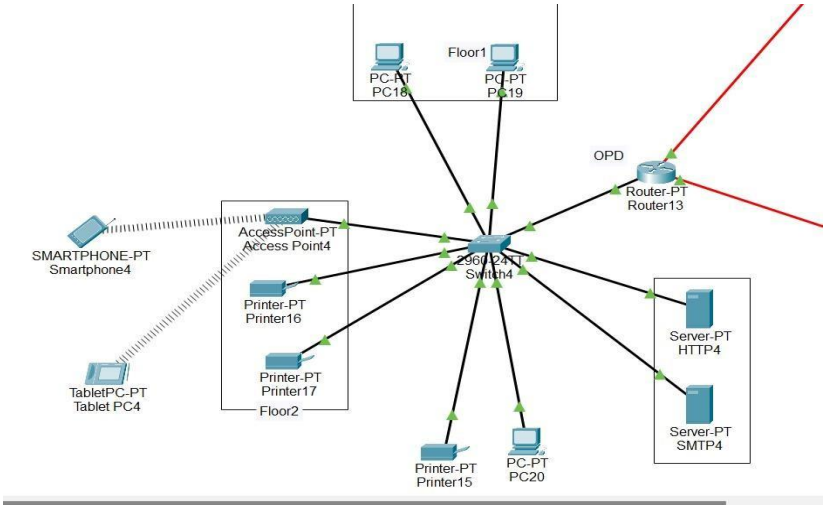

Fig 5: Patient ward

Device	IP Address	Subnet Mask	Default Gateway
Router (GigabitEthernet0/0.10)	192.168.10.1	255.255.255.0	-
Router (GigabitEthernet0/0.20)	192.168.20.1	255.255.255.0	-
Router (GigabitEthernet0/0.30)	192.168.30.1	255.255.255.0	-
Router (GigabitEthernet0/0.40)	192.168.40.1	255.255.255.0	-
Floor 1 PC 1	192.168.10.2	255.255.255.0	192.168.10.1 (Router)
Floor 1 PC 2	192.168.10.3	255.255.255.0	192.168.10.1 (Router)
Floor 2 Access Point	192.168.20.2	255.255.255.0	192.168.20.1 (Router)
Floor 2 Printer 1	192.168.20.3	255.255.255.0	192.168.20.1 (Router)
Floor 2 Printer 2	192.168.20.4	255.255.255.0	192.168.20.1 (Router)
Floor 3 Printer 1	192.168.30.2	255.255.255.0	192.168.30.1 (Router)
Floor 3 PC 1	192.168.30.3	255.255.255.0	192.168.30.1 (Router)
Server 1	192.168.40.2	255.255.255.0	192.168.40.1 (Router)
Server 2	192.168.40.3	255.255.255.0	192.168.40.1 (Router)

This network layout comprises various elements, including computers that facilitate patient check-ins, appointments, and digital medical records management. These devices are interconnected through a central network switch, ensuring smooth data flow and communication within the OPD. Moreover, the OPD network incorporates a wireless access point, enabling patients and visitors to connect their personal devices to the hospital's network. This feature enhances patient experience and engagement while providing convenient access to digital resources during their visits. The network infrastructure in the OPD is designed to optimize patient care, streamline administrative tasks, and support the medical staff in delivering high-quality healthcare services to outpatient visitors. This diagram provides an overview of the network setup within the OPD, emphasizing its role in fostering efficient communication and enhancing the overall patient experience.

Design & IP Address of ward -hub

Wards are designed to support general patient care, including bedside monitors and nurse call systems. A star topology is employed within each ward, providing a reliable connection for all devices. Ward hubs are connected to the central network via high-speed links, and Quality of Service (QoS) policies prioritize critical communication to ensure smooth operation of patient care systems.

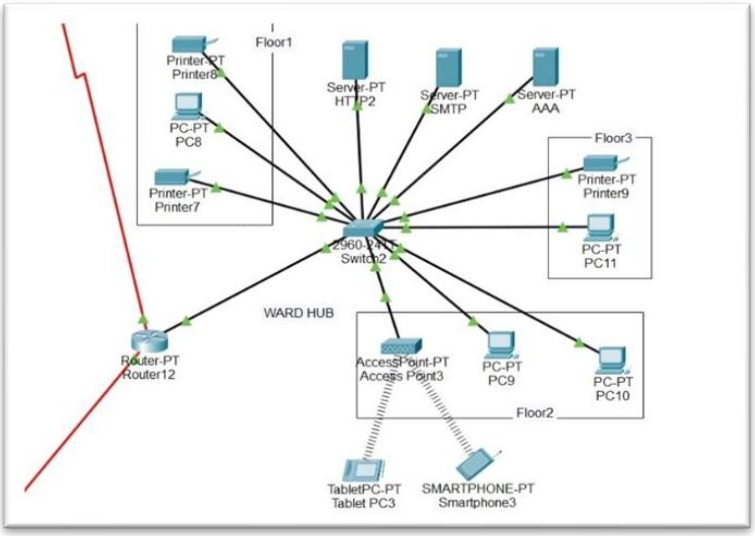

Fig 6: Ward Hub

Device	IP Address	Subnet Mask	Default Gateway
Printer (Floor1)	**192.168.10.2**	**255.255.255.0**	**192.168.10.1**
PC1 (Floor1)	**192.168.10.3**	**255.255.255.0**	**192.168.10.1**
Printer2 (Floor1)	**192.168.10.4**	**255.255.255.0**	**192.168.10.1**
Access Point (Floor2)	**192.168.11.2**	**255.255.255.0**	**192.168.11.1**
PC1 (Floor2)	**192.168.11.3**	**255.255.255.0**	**192.168.11.1**
PC2 (Floor2)	**192.168.11.4**	**255.255.255.0**	**192.168.11.1**
PC1 (Floor3)	**192.168.12.2**	**255.255.255.0**	**192.168.12.1**
Printer (Floor3)	**192.168.12.3**	**255.255.255.0**	**192.168.12.1**
Server1	**192.168.20.2**	**255.255.255.0**	**192.168.20.1**
Server2	**192.168.20.3**	**255.255.255.0**	**192.168.20.1**
Server3	**192.168.20.4**	**255.255.255.0**	**192.168.20.1**

The Ward network includes dedicated computers for healthcare professionals, aiding in patient data management, medical record access, and communication. These devices are interconnected through a central network switch, guaranteeing quick and reliable data exchange within the Ward. Additionally, the network supports patients' access to healthcare resources through the provision of a wireless access point. Patients and visitors can connect their personal devices to the network, facilitating communication and entertainment while admitted to the Ward. The Ward network design prioritizes the needs of both patients and medical staff, aiming to create an environment that promotes effective healthcare delivery, data management, and patient comfort. This diagram provides a snapshot of the network configuration within the Wards, underscoring its role in supporting patient care and medical services.

Design & IP Address of Reception

The reception area is the first point of contact for patients, handling registration, scheduling, and inquiries. Workstations in this area are connected to the main server to allow real-time access to patient information. Secure communication protocols are used to protect sensitive data exchanged at this level. Additionally, guest network access is available for patients and visitors via a segregated Wi-Fi system.

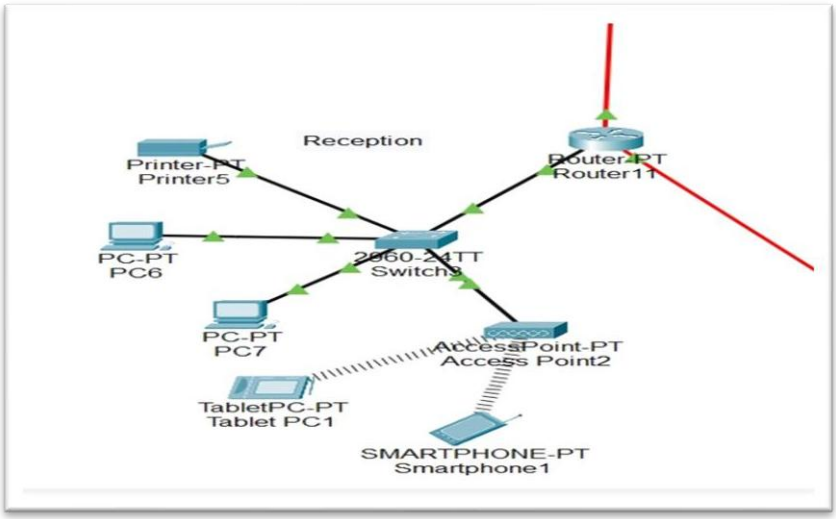

Fig:7 Reception Network

Device	Port	IP Address	Subnet Mask	Default Gateway
Router	Gig0/0/0	192.168.10.1	255.255.255.0	N/A
PC 1	fa0/3	192.168.10.2	255.255.255.0	192.168.10.1
PC 2	fa0/4	192.168.10.3	255.255.255.0	192.168.10.1
Printer	fa0/5	192.168.10.4	255.255.255.0	192.168.10.1
Access Point	fa0/2	192.168.10.5	255.255.255.0	192.168.10.1

To enhance visitor and patient experience, the network in the reception area also features a wireless access point. This enables patients and visitors to connect their devices, such as smartphones and tablets, to the hospital's network, facilitating information access and communication during their time at the hospital. The reception network is designed to streamline administrative tasks, enhance patient engagement, and provide quick access to essential healthcare services. This diagram captures the essence of the network configuration within the reception area, underlining its pivotal role in facilitating efficient hospital operations and ensuring a positive experience for all who enter the hospital.

Routing Protocols:

There are various routing protocols available for configuring and enabling device connection. The major class of routing protocols is

- Static Routing
- Dynamic Routing

Static routing would not be the best solution in the new planned network design because it required human configuration for each route. Furthermore, there is a greater possibility of human error during configuration. Static routing is best suited for small groups of devices. It is strongly advised to utilize a dynamic routing protocol such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), or Routing Information Protocol for the new network concept (RIP). Dynamic Routing is preferred for Hospital Network Design.

Physical Design:

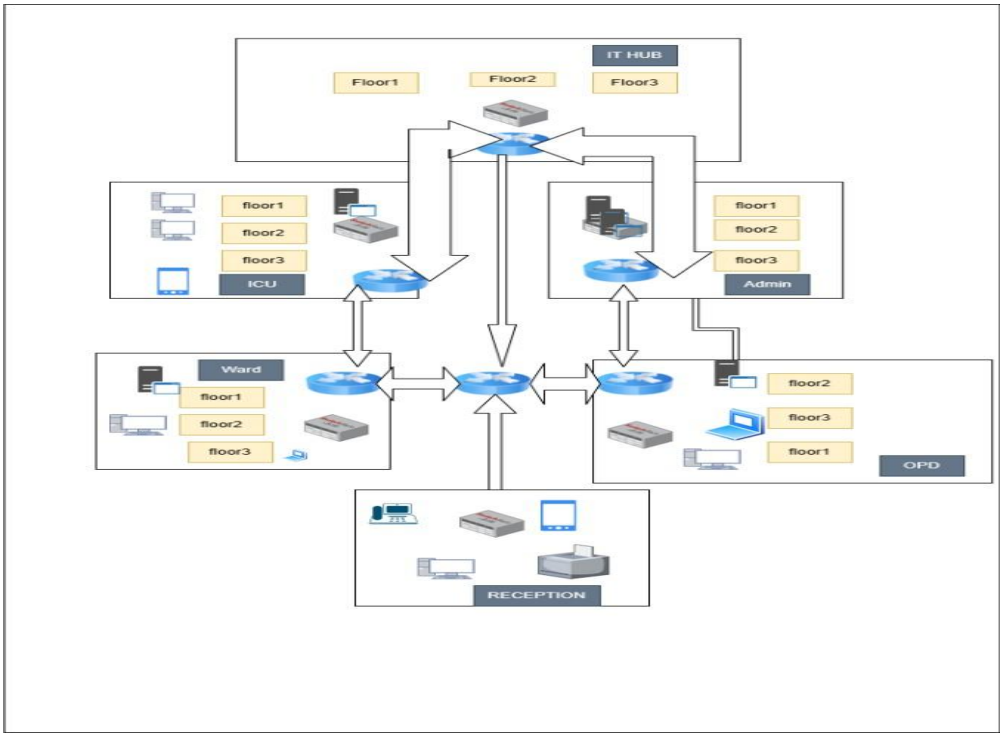

Fig 8 Physical Layer

Hardware Components used:

Devices	Type	Specifications	Numbers	Location
Generic PCs	Hosts	CPU: Intel Core I5 RAM: 8GB 2666mHz DDR4 RAM: 128GB NvME SSD	18	All wards
Router PT	Integrated services router	10 GE SPF+, PoE GE/SFP, GE/SFP 10 Gbps+ performance 7Gbps encrypted throughput	6	All wards Interconnection
CISCO Catalyst 2960-IOS15 L smart managed switches	Switches	16 PoE+ ports with line rate forwarding	6	All Wards
Cables,	Co-axial, Multimode fiber, cAT 6A	Support for 10Gb and 40Gb Ethernet communication	As per required	
Cisco C9120AXI-B catalyst Access Point PT	Access point	4×4 Flexible Dual Radio with 5GHz and 2.4GHz or two 5GHz configuration, up to 5.38 Gbps data rate, uplink/downlink OFDMA	6	One in each building
Cisco UCS X210c M6	Server	3rd Gen Intel Xeon Scalable Processors	8	

BUDGET ESTIMATION:

COMPONENT	DESCRIPTION	PRICE PER UNIT (USD)	QUANTITY	TOTAL COST (USD0
Switches	Cisco Catalyst 3650 Switches	1500	6	9000
Routers	Juniper MX Series Routers	1500	6	9000
Access Points	Aruba 500 Series APs	300	6	1800
Server Hardware	Dell PowerEdge R740 Servers	8000	8	64,000
Software Licenses	Microsoft Server 2019 licenses	1200	30	36,000
Network Cabling	CAT6 Ethernet Cables (per ft)	0.5	5000	2,500
Staff Training	Certification Training Programs	2000	5	10,000
Maintenance Support	Annual Support Contracts	Varies	-	25,000
Telecommunication	Internet Service Provider	2000/month	12 months	24,000
Compliance Measures	HIPAA Compliance Audit	5000	1	5,000
Total				**1,86,300(Initial Budget Approx)**

CONCLUSION:

In conclusion, the proposed network design for our hospital promises to significantly enhance efficiency, security, and scalability. By implementing a robust infrastructure with redundant systems, we aim to ensure uninterrupted access to critical patient data and medical resources. This design not only meets current needs but also anticipates future growth and technological advancements. We are confident that this network will empower our healthcare professionals to deliver exceptional patient care while maintaining the highest standards of data privacy and security.