

**Project Report**

**Hospital Network Design**

**Course Title - Computer Network Lab**

**Course Code - CSE 416**

**Submitted to**

Momtaj Hossain Mow

Lecturer

Eastern University

**Submitted by**

Name: Jannatul Firdous Samiya

ID: 222400024

Department of CSE

| **Sl. No.** | **Content Title** | **Page No.** |
| --- | --- | --- |
| 1 | Introduction | 3 |
| 2 | Project Objective | 3 |
| 3 | Network Zones | 3 |
| 4 | Devices Used | 4 |
| 5 | Network Topology Overview | 4 |
| 6 | IP Addressing | 4 |
| 7 | Routing Configuration | 4 |
| 8 | Services Configured | 4 |
| 9 | Connectivity & Testing | 5 |
| 10 | Limitations & Recommendations | 6 |
| 11 | Network Diagram | 7 |
| 12 | Conclusion | 8 |

**Introduction**

This project focuses on designing a structured and scalable **Hospital Network System** using **Cisco Packet Tracer**. The goal is to ensure **reliable communication**, **secure data sharing**, and **efficient resource access** across different hospital departments including IT, Clinical, General and Private Wards, and Reception.

**Objective:**

The objective of this project is to design and simulate a functional hospital network using Cisco Packet Tracer.  
It aims to:

* Ensure smooth communication between hospital departments
* Provide access to essential services (DNS, HTTP, FTP, SMTP)
* Organize the network through subnet-based segmentation
* Create a secure guest Wi-Fi zone with limited access
* Demonstrate basic routing and service setup in a real-world scenario

**Network Zones**

The hospital network is logically divided into several subnet-based departments:

| **Department** | **Subnet** |
| --- | --- |
| IT Department | 192.168.1.0/24 |
| Clinical Area | 192.168.2.0/24 |
| Entrance Reception | 192.168.3.0/24 |
| General Ward | 192.168.4.0/24 |
| Private Ward | 192.168.5.0/24 |
| Guest Wi-Fi Zone | DHCP-based (Wi-Fi) |
|  |  |

**Devices Used**

* **Routers:** 5 (Router0 to Router4)
* **Switches:** 6 (2960-24TT switches)
* **End Devices:** PCs, Laptops, Smartphones, Tablets
* **Servers:** DNS, HTTP, SMTP, FTP
* **Wireless Router:** WRT300N (for Guests)

**Network Topology Overview**

* **Router0 (IT Department)** connects the IT PCs, servers, and links with Clinical & Reception routers via serial links.
* **Router1 (Clinical)** connects Ultrasound, OT, Rooms, etc.
* **Router2 (General Ward)** connects ward PCs and doctors.
* **Router3 (Private Ward)** connects private ward PCs.
* **Router4 (Entrance)** connects Reception, Info Counter, Billing.
* **WRT300N Router** serves Guest Wi-Fi, isolated from the core hospital LAN.

**IP Addressing**

Each subnet is assigned a unique Class C private network with subnet mask **255.255.255.0**. IPs are statically assigned to routers and PCs.

**Routing Configuration:**

Routing between subnets is achieved using either:

* **Static routing**: Simple for small networks
* or **OSPF dynamic routing**: Recommended for scalability (if implemented)

Each router includes proper routes to reach all subnets.

**Services Configured**

### ****DNS Server: Resolves Domain Names****

Converts domain names (e.g., hospital.local) into IP addresses. Helps users access internal services easily without typing IPs.

### ****HTTP Server: Web-Based Access****

Hosts the hospital’s internal website or portal. Allows staff to access information through a web browser.

### ****SMTP (Simple Mail Transfer Protocol):****

Used for sending emails between hospital departments. Helps in delivering messages like test results or appointment info.

### ****FTP (File Transfer Protocol):****

Used for transferring large files such as medical reports and scans. Allows secure file sharing between different hospital units.

### ****DHCP: Used for Wi-Fi Guest Zone****

Automatically provides IP addresses to guest devices. Used in the Wi-Fi zone to connect smartphones and laptops easily.

**Connectivity & Testing**

**Successful Communication:**

* IT Dept ↔ Clinical Area
* Clinical ↔ General ↔ Private
* Entrance ↔ IT ↔ Clinical
* Servers accessible within hospital LAN

**Restricted Communication**

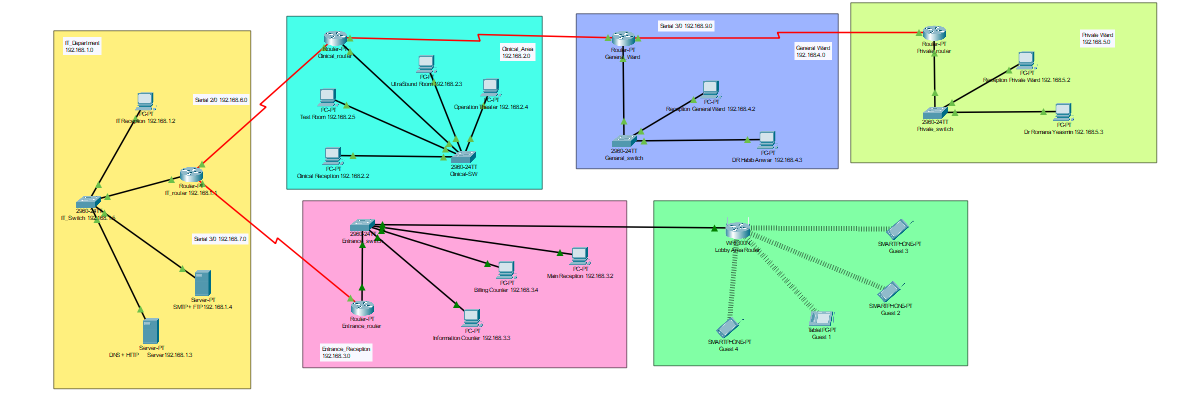
Guest Wi-Fi devices **cannot access** hospital PCs or servers, maintaining **security**.

All connections were tested via **ping**, and each zone communicates successfully if routing is configured properly.

**Limitations & Recommendations**

* **Wi-Fi zone** should be NAT-enabled if internet access is required.
* Add **Access Control Lists (ACLs)** to secure sensitive subnets.
* Consider **VLANs** in future to segment traffic further.

**Network Diagram**



**Conclusion**

This hospital network design demonstrates how a medium-sized organization like a hospital can implement a robust and secure LAN infrastructure using routers, switches, and basic services. Proper segmentation and routing ensure data isolation, internal communication, and service availability.