VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY
Ho Chi Minh City University of Technology
Faculty of Computer Science and Engineering

Computer Networks (CO3093 – CO3094)

Assignment 2

Network Design and Simulation for a Critical Large Hospital

Advisor(s):	Nguyen Thanh Nhan	
Student(s):	Tieu Tri Bang	2252079
	Le Pham Tien Long	2352688
	Le Hoang Chi Vi	2353336
	Nguyen Le Nam Khanh	2352522

HO CHI MINH CITY, NOVEMBER 2025

Contents

List of Figures

List of Tables

1 Introduction

The design and implementation of a robust network infrastructure for a Specialized Hospital represents a critical investment in modern healthcare delivery. This project focuses on creating a comprehensive network solution for a hospital system comprising one Main Hospital Site in Ho Chi Minh City and two Auxiliary Sites (DBP and BHTQ). The network must support approximately 600 workstations, 10 enterprise-grade servers, and numerous medical IoT devices while ensuring seamless connectivity, data security, and 24/7 operational availability across all locations.

The motivation behind this network design stems from the imperative need to ensure scalability, security, reliability, and high availability in a healthcare-critical environment. The hospital network must accommodate at least 20% growth in staff, devices, and medical systems over the next five years, maintaining stability as new departments and medical technologies are integrated. Critical hospital applications—including the Hospital Information System (HIS), Radiology Information System (RIS-PACS), and Laboratory Information System (LIS)—require continuous uptime, necessitating redundant network paths and failover systems to ensure uninterrupted access to patient data and clinical services. Furthermore, the network must protect sensitive patient information and medical records through advanced firewalls, encryption, and secure VPN tunnels, ensuring compliance with healthcare data protection standards and patient privacy regulations.

The domain context emphasizes a healthcare environment where the network infrastructure must support medical, administrative, and operational functions critical to hospital performance and patient care. The hospital handles a large volume of confidential information, including Electronic Medical Records (EMR), laboratory test results, radiology images, and patient billing data, requiring strict data protection, integrity, and privacy measures. Operating continuously around the clock, any network downtime could disrupt critical systems and potentially affect patient treatment and clinical workflows. The design must therefore incorporate redundancy, failover mechanisms, and robust hardware to maintain consistent service availability.

To address these challenges, the network architecture implements a three-tier hierarchical model combining core, distribution, and access layers. The design features VLAN segmentation by department to isolate traffic and improve security, GPON fiber backbone for high-speed inter-building connectivity, and enterprise-grade Wi-Fi 6 coverage throughout all hospital areas. SD-WAN technology connects the Main Hospital to auxiliary branches (DBP and BHTQ) with 25 Mb/s dedicated bandwidth per site, utilizing OSPF dynamic routing and secure IPsec VPN tunnels for encrypted data transmission.

Dual 200 Mb/s xDSL Internet connections with load balancing and failover ensure reliable external connectivity. The integration of medical IoT devices, CCTV surveillance systems, and patient monitoring sensors through isolated VLANs enhances both patient safety and facility management capabilities.

2 Requirements

2.1 Network System Requirements

2.1.1 Main Hospital

Building Layout

- The Main Hospital includes two main buildings (A and B), each with five floors and approximately ten rooms per floor, serving medical departments such as Administration, Radiology, Laboratory, Surgery, Pharmacy, and IT.
- A separate Data Center and Cabling Central Local is located about 50 meters from the main buildings, containing all core networking and server equipment.
- Structured cabling through patch panels and fiber backbone (GPON) is used to interconnect buildings and floors.

Devices and Infrastructure

- Approximately 600 workstations distributed across departments and service units.
- 10 enterprise-grade servers, including HIS (Hospital Information System), LIS (Laboratory Information System), PACS (Picture Archiving and Communication System), CRM, Web, and Backup servers.
- Around 12 networking devices (core/distribution/access switches, routers, firewalls, load balancers).
- IoT and security devices such as IP cameras, patient monitoring sensors, and access control systems are also integrated.

Network Technologies

- Hybrid network combining wired (1GbE/10GbE) and wireless (Wi-Fi 6) infrastructure.

- VLAN segmentation by department (e.g., Medical, Administration, Pharmacy, Laboratory, IoT).
- GPON fiber backbone between buildings to support high data rates.
- Wireless coverage across all areas, including patient wards and lobbies.

WAN and Internet Connectivity

- Two leased lines connecting to the auxiliary sites (DBP and BHTQ) with SD-WAN overlay for enhanced traffic management.
- Two xDSL lines (200 Mb/s each) for Internet access, configured with load balancing and failover to ensure reliability.
- SD-WAN technology selected for cost-effectiveness, security, and dynamic traffic optimization (detailed analysis in WAN and Throughput Design section).
- All Internet-bound traffic passes through the Main Site, enabling centralized control and monitoring.

Security and High Availability

- The Main Hospital network integrates firewalls (ASA), Intrusion Prevention/Detection Systems (IPS/IDS), and phishing protection to safeguard medical data and prevent unauthorized access.
- Redundant core switches and routers provide failover capabilities to minimize downtime.
- All critical systems are hosted in a high-availability configuration with periodic backup synchronization to off-site storage.

VPN Configuration

- Site-to-Site VPNs connect the Main Hospital to the DBP and BHTQ branches securely over WAN links.
- Teleworker VPNs enable doctors and IT administrators to access internal resources remotely during emergency or off-site operations.

Medical IoT and Surveillance

- A CCTV surveillance network covers key hospital areas for safety and monitoring.
- IoT medical devices (e.g., patient monitors, smart infusion pumps) operate on isolated VLANs for security and performance.
- Network monitoring systems are deployed for real-time performance tracking, fault detection, and preventive maintenance.

2.1.2 Auxiliary Sites

Building Layout

- Each auxiliary site includes a two-floor hospital building with one IT Room and a Cabling Central Local on the first floor.
- The IT Room contains local networking equipment, servers, and UPS systems to maintain essential services even if the WAN connection is interrupted.

Devices and Infrastructure

- Each site operates approximately 60 workstations, 2 servers, and at least 5 networking devices (router, ASA firewall, multilayer switch, and access switches).
- Local servers support limited file sharing, caching, and internal data collection before synchronization with the Main Hospital.
- Wireless access points ensure full Wi-Fi coverage across departments and public areas.
- Surveillance cameras (CCTV) are installed for physical security and connected via the IoT VLAN.

WAN Connectivity

- Each branch connects to the Main Hospital through dedicated serial WAN links:
  - DBP: 200.100.20.0/30
  - BHTQ: 200.100.30.0/30
- Routing between sites uses OSPF dynamic routing to exchange internal subnets efficiently.

- SD-WAN overlay enhances traffic control, provides failover resilience, and enables dynamic bandwidth aggregation across dual links.

Security and High Availability

- Each site deploys a Cisco ASA firewall to protect local resources and enforce VPN tunnels with the Main Hospital.
- Local VLAN segmentation separates departments, guest Wi-Fi, and IoT devices.
- Essential services (e.g., local HIS access, backup) continue operating in standalone mode if WAN connectivity is lost.

Surveillance and Monitoring

- Each site is equipped with IP cameras and IoT monitoring sensors connected to the hospital's centralized surveillance system.
- Network monitoring tools track bandwidth, device health, and uptime for all branch sites through the Main Hospital's NOC (Network Operations Center).

2.2 Site Survey Requirements

Before implementing the hospital network, a comprehensive site survey must be conducted to evaluate the physical layout, cabling infrastructure, power systems, and placement of networking and IoT devices. This ensures optimal coverage, performance, and scalability for both the Main Hospital and the Auxiliary Sites (DBP and BHTQ).

2.2.1 Main Hospital

Building Layout

- Two main buildings (A and B), each with five floors and ten rooms per floor, dedicated to different departments:
  - Building A: Administration, Pharmacy, Surgery, Radiology
  - Building B: Laboratory, IT Department, Patient Services, Research Units
- Data Center and Cabling Central Local located 50 meters away, connected via underground GPON fiber links.

Table 2.1: Main Hospital Survey Checklist

Category	**Key Survey Items**	**Description**
Building Layout	Number of floors and rooms; Locations for IT rooms and distribution cabinets	Verify space and access for structured cabling, switches, and UPS systems
Workstations and Devices	Approx. 600 PCs, laptops, and terminals; Placement of medical devices	Identify LAN drops per room and power availability for devices
Cabling and Connectivity	Existing cabling type (Cat6, fiber); Required new GPON/10GbE lines	Plan structured cabling routes and patch panel terminations per floor
Wireless Access Points	Required Wi-Fi coverage zones; Ceiling height and material	Measure signal propagation and mark optimal AP positions for full coverage
Network Requirements	VLAN planning per department; Load balancing for xDSL and WAN lines	Ensure adequate uplink capacity and logical segmentation
Security and High Availability	Firewall, IDS/IPS, and load balancer positions; Rack capacity in Data Center	Plan redundant paths and physical separation of power sources
IoT and Surveillance System	IP camera locations; IoT gateways for patient monitoring	Ensure VLAN isolation and network reachability for all devices
Environmental and Power	Air-conditioning, backup power, grounding	Verify proper cooling and UPS for core racks and servers

Schematic Physical Setup

- Core network devices (routers, firewalls, load balancers, core switches) are housed

in the Data Center.

- Each building floor connects to its access switch through structured cabling routed to patch panels.
- Wireless APs are mounted on ceilings in wards, lobbies, and administrative offices.
- IoT sensors (temperature, patient monitors) and CCTV cameras are distributed throughout the buildings and linked to the IoT VLAN.

2.2.2 Auxiliary Sites

Building Layout

- Each auxiliary site includes a two-floor hospital building with:
  - 1 IT Room (first floor)
  - 1 Cabling Central Local
  - Departmental areas: Registration, Pharmacy, Examination Rooms, and Nursing Area

Table 2.2: Auxiliary Sites Survey Checklist

Category	**Key Survey Items**	**Description**
Building Layout	Number of floors (2); Room purposes per floor	Define cable routes and AP placement according to patient/staff zones
Workstations and Devices	∼60 workstations per site; Printers, terminals, and medical PCs	Assess required LAN ports and power sockets
Cabling and Connectivity	Cat6 / GPON backbone; Patch panels and local racks	Identify trunk lines to IT Room and inter-floor cabling routes
Wireless Coverage	AP locations and overlap zones	Ensure no dead zones in waiting areas and wards
Server and Network Equipment	Placement of router, ASA firewall, multilayer switch	Confirm rack space, cooling, and electrical load capacity
WAN Connectivity	Serial link to Main Hospital; Routing via OSPF	Verify cable routing and secure conduit to external WAN provider
IoT and Surveillance System	IP cameras per floor; IoT sensors for environment monitoring	Plan VLAN allocation and confirm PoE switch requirements
Power and Backup	UPS and grounding; Separate circuits for IT Room	Guarantee continuous operation during power fluctuations

Schematic Physical Setup

- **IT Room (Ground Floor):** Contains router (Cisco 1941), ASA firewall, multilayer switch (Cisco 3560), access switch (Cisco 2960), and two local servers. Connected directly to the WAN line to the Main Hospital.
- **Floor 1 and Floor 2:** Each floor has an access switch connected to the core via trunk links. PCs, printers, and APs connect to these access switches through Cat6 cables.

- **IoT and CCTV:** IP cameras and IoT sensors connect to their isolated VLANs through PoE ports. The feeds are sent to the Main Hospital's monitoring center via the WAN connection.

3 Analysis and Design

3.1 High Load Areas and Device Configuration

The Specialized Hospital operates a complex, high-traffic network that integrates patient data systems, diagnostic imaging, medical IoT devices, and real-time communication across multiple sites. To maintain stability and performance, the network design identifies high load areas—zones of intensive data transmission—and defines appropriate device configurations to handle traffic effectively and ensure reliability.

3.1.1 Main Hospital

Based on the topology shown in Figure 4.1 (Main Site Network) and Figure 4.4 (Internet Connectivity Layer), the following zones have the highest concentration of data and processing load:

Data Center

- **Subnets:** 10.0.3.0/24, 172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24
- **Devices:**
  - Multilayer Switches (Cisco 3560-24PS, 3560-24FS)
  - Core Router (Cisco 2911)
  - ASA Firewall (Cisco 5516-X)
  - Servers: DNS, HTTP, Email, FTP, IoT, Backup
- **Functions:**
  - Centralized routing and VLAN management.
  - Hosting critical systems: HIS, LIS, PACS, CRM, and internal applications.
  - Handling inter-site traffic between DBP, BHTQ, and Internet gateways.
- **Reason for High Load:**
  - Peak-time access from 600 local workstations and remote users.

  - Simultaneous data uploads from branch sites (imaging, medical reports).
  - High volume of internal queries to HIS/Database servers.

Configuration Optimization:

- Redundant multilayer switches connected in trunk mode for load balancing.
- Core router (2911) configured with OSPF for dynamic route exchange with branches.
- Dual WAN lines connected through the ASA firewall with load-balancing and failover.
- VLAN-based QoS applied to prioritize HIS, RIS-PACS, and database traffic.

Departmental Floors (Buildings A and B)

- **Subnets (example Building A):**
  - 192.168.10.0/24 → 1st floor
  - 192.168.20.0/24 → 2nd floor
  - 192.168.30.0/24 → 3rd floor
  - 192.168.40.0/24 → 4th floor
  - 192.168.50.0/24 → 5th floor
- **Subnets (Building B):** 192.168.60.0/24 to 192.168.100.0/24 (5 floors)
- **Devices:** Access switches (Cisco 2960 series), Access Points, IoT Cameras.
- **High Load Areas:**
  - Radiology (X-ray image transfer).
  - Laboratory (test data synchronization).
  - Surgery and Pharmacy (real-time HIS data entry).
- **Reason for High Load:**
  - Large data packets from diagnostic imaging equipment.
  - Constant access to EMR servers and patient databases.
  - Increased wireless usage by tablets, mobile devices, and staff laptops.

Configuration Optimization:

- Each floor has a dedicated VLAN and access switch linked to the building's distribution switch (3560).
- Uplink trunks use Gigabit Ethernet connections to reduce congestion.
- VLAN tagging isolates traffic by department, improving performance and security.
- DHCP is centrally managed, but each building includes relay agents for faster IP assignment.

Internet Gateway and External Communication

- **Subnets:** 200.100.100.0/24, 200.200.200.0/24
- **Devices:** Dual Routers (Cisco 1941), ASA 5516-X, and DSL modems connected to Cloud.
- **High Load Reason:**
  - Simultaneous outbound web traffic from hospital clients.
  - VPN tunnels from DBP and BHTQ.
  - Remote telemedicine connections and software updates.

Configuration Optimization:

- Dual xDSL configured for load balancing via ASA firewall.
- NAT and ACLs configured to restrict external access to internal servers.
- VPN IPsec tunnels for remote staff and inter-site communications.
- Firewall policies prioritize medical system traffic while rate-limiting guest Internet.

3.1.2 Auxiliary Sites

Site DBP

- **Subnets:**
  - LAN floors: 192.168.110.0/24, 192.168.120.0/24
  - Wi-Fi: 192.168.115.0/24
  - IoT: 192.168.125.0/24

  - Server subnet: 10.0.1.0/24

- **Devices:** Router 1941, ASA Firewall, 3560 Multilayer Switch, two 2960 Access Switches.
- **High Load Reason:**
  - Database synchronization with Main Hospital.
  - HIS transactions and video conferencing.
  - IoT camera streams during operational hours.

Configuration Optimization:

- OSPF adjacency to Main Site router over WAN (200.100.20.0/30).
- VLAN prioritization for HIS and database traffic.
- ACLs restricting Wi-Fi and IoT VLANs from accessing LAN.

Site BHTQ

- **Subnets:**
  - LAN floors: 192.168.130.0/24, 192.168.140.0/24
  - Wi-Fi: 192.168.135.0/24
  - IoT: 192.168.145.0/24
  - Server subnet: 10.0.2.0/24
- **Devices:** Router 1941, ASA Firewall, 3560 Multilayer Switch, 2960 Access Switches.
- **High Load Reason:**
  - Laboratory imaging and HIS data synchronization.
  - Remote consultations via VPN with specialists at Main Hospital.

Configuration Optimization:

- Bandwidth throttling for non-essential services.
- Use of DHCP relay and VLAN separation to reduce broadcast load.
- Firewall-based QoS policies prioritizing medical database traffic.

Table 3.1 summarizes the main devices used in the network along with their roles and configuration handle the high load areas.

Table 3.1: Device Configuration Summary

Device	**Model / Role**	**Configuration Highlights**
Cisco 2911 Router	Core WAN Router	OSPF Area 0, dual WAN, static backup routes
Cisco 5516-X ASA	Firewall	Dual ISP load balancing, NAT, ACLs, VPN
Cisco 3560-24PS	Core Switch	VLAN trunking, inter-VLAN routing, DHCP relay
Cisco 2960-24TT	Access Switch	Per-floor VLAN, QoS for medical devices
Cisco 1941 Router	Branch Router	OSPF, static default route, VPN tunnel
Server (HIS/PACS)	Application Server	Central database and imaging
IoT Server	Management	Monitors camera streams and sensors
Access Points	Wi-Fi 6	SSID segmentation (Staff / Guest)

3.2 Network Structure

The network structure of the Specialized Hospital is designed according to a three-tier hierarchical model—Core, Distribution, and Access layers—to ensure scalability, high performance, and clear separation of functions. This structure provides a balance between central management in the Main Hospital, autonomous operation at the Auxiliary Sites (DBP and BHTQ), and optimized data flow between departments and floors within each building.

3.2.1 Hierarchical Network Design

Core Layer (Data Center and Main Routing Backbone)

- **Purpose:** The core layer provides centralized connectivity and routing between the hospital's departments, the auxiliary sites, and external networks (Internet and VPNs).
- **Physical Location:** The Data Center, situated in a separate facility near Buildings A and B at the Main Hospital.

- **Devices:**
  - Cisco 2911 Router (WAN gateway)
  - Cisco ASA 5516-X Firewall (Internet/VPN termination)
  - Cisco 3560 Multilayer Switches (L3 core switching)
  - High-performance servers (HIS, PACS, LIS, FTP, DNS, Email)
- **Functions:**
  - High-speed inter-VLAN routing between hospital departments.
  - OSPF backbone routing for all internal and branch networks.
  - Redundant WAN links to DBP and BHTQ auxiliary sites.
  - Internet access control, NAT, and VPN termination through the ASA firewall.
- **Design Justification:** This centralized core design ensures that all data traffic—including medical images, EMR access, and inter-site synchronization—is efficiently routed through secure, high-capacity links, supporting both scalability and manageability.

Distribution Layer (Buildings A and B, and Auxiliary IT Rooms)

- **Purpose:** The distribution layer aggregates connections from each floor and acts as the intermediary between access switches and the core network.
- **Physical Location:**
  - One distribution switch per building (Cisco 3560-24PS).
  - Each auxiliary site (DBP, BHTQ) includes one Multilayer Switch (Cisco 3560) in its IT Room.
- **Devices:**
  - Cisco 3560-24PS Multilayer Switch (L3 capable).
  - Cisco 2960-24TT Access Switches on each floor (connected via trunk links).
- **Functions:**
  - Perform inter-VLAN routing between departmental subnets.

  - Implement Access Control Lists (ACLs) to restrict communication between VLANs (e.g., Guest Wi-Fi cannot access internal networks).
  - Enforce Quality of Service (QoS) to prioritize medical data (HIS, PACS) over less critical traffic (web browsing, printing).

- **Design Justification:** This structure provides a clear boundary between departmental traffic and the hospital's core, improving both security and performance. VLAN traffic is contained within buildings, reducing unnecessary load on the core.

Access Layer (Department and Floor Networks)

- **Purpose:** The access layer connects all end devices, including PCs, laptops, tablets, and IoT medical devices.
- **Physical Location:** Each floor of Buildings A and B at the Main Hospital and both floors of each auxiliary site.
- **Devices:**
  - Cisco 2960-24TT Access Switches (wired connectivity).
  - Wireless Access Points (Wi-Fi 6).
  - IoT Cameras and Sensors (connected via PoE ports).
- **Functions:**
  - Provide wired and wireless access to hospital staff and medical systems.
  - Assign VLANs based on department or device type (Medical Staff, Admin, Guest, IoT).
  - Distribute DHCP addresses to end devices (managed by relay or central DHCP server).
  - Ensure redundancy by connecting access switches to the distribution layer with dual uplinks.
- **Design Justification:** The access layer enables smooth daily operations across all floors and departments. By implementing VLANs and PoE-enabled switches, it supports modern hospital technologies like mobile EMR devices, patient monitoring sensors, and IP cameras.

3.2.2 VLAN-Based Logical Segmentation

To achieve security, traffic isolation, and efficient management, VLANs are implemented across all sites. VLAN segmentation is done by department and function, as follows:

Table 3.2: VLAN Segmentation

VLAN Function	**Subnet Example**	**Purpose / Connected Devices**
Administration	192.168.10.0/24	Staff PCs, printers, HR systems
Medical & Clinical	192.168.20.0/24	HIS, PACS terminals, patient PCs
Laboratory	192.168.30.0/24	Laboratory analysis devices
Pharmacy	192.168.40.0/24	Dispensing systems, POS devices
Wi-Fi (Staff/Guest)	192.168.15.0/24	Wireless access for mobile devices
IoT & CCTV	192.168.55.0/24	Cameras, sensors, IoT devices
IT Management	172.16.10.0/24	Network device management
Servers & Data Center	10.0.3.0/24	Core servers (DNS, FTP, Email, Web)

Each VLAN is assigned an IP subnet and controlled by ACLs on the multilayer switches and ASA firewall. This ensures that, for example, IoT devices cannot access HIS databases, and guest Wi-Fi cannot reach administrative PCs.

3.2.3 WAN Connectivity Structure

The Main Hospital Core connects to both auxiliary sites through dedicated WAN links using OSPF dynamic routing and SD-WAN overlay technology. Each auxiliary site requires 25 Mb/s of dedicated bandwidth, while the Main Site requires dual 200 Mb/s Internet connections for external connectivity (see WAN and Throughput Design section for detailed calculations).

Table 3.3: WAN Connectivity

Connection	**Link Type**	**IP Range**	**Routing Protocol**
Main Site ↔ DBP Site	SD-WAN over Leased Line (25 Mb/s)	200.100.20.0/30	OSPF
Main Site ↔ BHTQ Site	SD-WAN over Leased Line (25 Mb/s)	200.100.30.0/30	OSPF
Main Site ↔ Internet	Dual xDSL (2 × 200 Mb/s)	200.100.100.0/24, 200.200.200.0/24	Static + NAT

3.2.4 Internet and DMZ Integration

- All Internet access passes through the ASA Firewall at the Main Hospital.
- The firewall also maintains a DMZ (10.0.3.0/24) containing web, email, FTP, and IoT servers accessible to external users through controlled NAT policies.
- This DMZ isolates public-facing services from internal networks, protecting patient data from potential breaches.

3.3 WAN and Throughput Design

The WAN constitutes the central nervous system of the hospital's information infrastructure, linking the Main Site in Ho Chi Minh City to the auxiliary branches at DBP Street and BHTQ Street. The design must guarantee high throughput, low latency, and uncompromised security for medical, administrative, and public services. This subsection presents a quantitative estimation of throughput and bandwidth based on the hospital's operational data, followed by a justification for the chosen WAN technology.

3.3.1 Throughput and Bandwidth Estimation

The data communication model adopted by the hospital relies on the main site as the central hub through which all Internet and inter-site traffic is routed. Based on the system specifications, the main site comprises approximately 600 workstations and 10 servers, while each auxiliary site accommodates around 60 workstations and 2 servers.

To determine the appropriate throughput, the expected data volumes generated by workstations, servers, and Wi-Fi users were first quantified. According to the assignment, each workstation downloads approximately 0.5 GB/day and uploads 0.1 GB/day, while each server downloads 1 GB/day and uploads 2 GB/day. Guest Wi-Fi users each download about 0.5 GB/day. Peak utilization reaches 80% of total capacity between 09:00–11:00 and 15:00–16:00, and overall traffic is expected to grow by 20% over five years.

Main Site Daily Data Load

The Main Site's daily data load is calculated as follows:

$$\begin{aligned} D_{\text{workstations}} &= 600 \times (0.5 + 0.1) = 360 \text{ GB/day} \\ D_{\text{servers}} &= 10 \times (1 + 2) = 30 \text{ GB/day} \\ D_{\text{Wi-Fi}} &= 300 \times 0.5 = 150 \text{ GB/day} \\ D_{\text{total, main}} &= 360 + 30 + 150 = 540 \text{ GB/day} \end{aligned}$$

Thus, the Main Site generates approximately 540 GB of internal network traffic daily. To estimate hourly throughput, this total is distributed over 24 hours with 80% utilization during peak hours:

$$T_{\text{peak, main}} = D_{\text{total, main}} \times 0.8 \times 2/24 = 36 \text{ GB/h}$$

The equivalent bit rate (throughput) is:

$$B_{\text{peak, main}} = \frac{36 \times 8 \times 10^9}{3600} \approx 80 \text{ Mb/s}$$

Hence, the main site's internal LAN backbone must sustain a minimum throughput of 80 Mb/s during peak usage, excluding WAN and Internet loads.

Auxiliary Site Daily Data Load

Each auxiliary site hosts 60 workstations and 2 servers:

$$D_{\text{workstations, aux}} = 60 \times (0.5 + 0.1) = 36 \text{ GB/day}$$
$$D_{\text{servers, aux}} = 2 \times (1 + 2) = 6 \text{ GB/day}$$
$$D_{\text{total, aux}} = 36 + 6 = 42 \text{ GB/day}$$

At 80% peak utilization over two hours:

$$T_{\text{peak, aux}} = 42 \times 0.8 \times 2/24 = 2.8 \text{ GB/h}$$
$$B_{\text{peak, aux}} = \frac{2.8 \times 8 \times 10^9}{3600} \approx 6.2 \text{ Mb/s}$$

Considering protocol overhead (+30%), reliability margin (+50%), and projected growth (+20%), the design throughput is:

$$B_{\text{design, aux}} = 6.2 \times (1.3 + 0.5 + 0.2) \approx 24.8 \text{ Mb/s}$$

Rounded up, each auxiliary site requires 25 Mb/s dedicated bandwidth for stable operation.

Internet Bandwidth at Main Site

All Internet traffic from the hospital passes through the Main Site. Assuming external communications account for approximately 50% of total internal load ($D_{\text{ext}} = 270$ GB/day):

$$T_{\text{peak, internet}} = 270 \times 0.8 \times 2/24 = 18 \text{ GB/h}$$
$$B_{\text{internet}} = \frac{18 \times 8 \times 10^9}{3600} \approx 40 \text{ Mb/s}$$

Allowing for burst traffic, a 5× headroom factor ensures adequate performance during simultaneous cloud or telemedicine sessions:

$$B_{\text{required, internet}} = 40 \times 5 = 200 \text{ Mb/s}$$

Therefore, the Main Site should be equipped with dual 200 Mb/s xDSL connections operating under a load-balancing and failover configuration.

Table 3.4 summarizes the recommended bandwidth and design decisions for each segment of the hospital's network infrastructure.

Table 3.4: Recommended Throughput and Link Design

Link Type	**Required Bandwidth**	**Design Decision**
Main Site Internal Backbone	$\geq$ 10 Gb/s (expandable to 40 Gb/s)	Fiber-optic core interconnecting Data Center, Buildings A & B
Main $\leftrightarrow$ DBP Site	2×25 Mb/s	Dual SD-WAN tunnels (active/standby)
Main $\leftrightarrow$ BHTQ Site	2×25 Mb/s	Dual SD-WAN tunnels (active/standby)
Internet Access	2×200 Mb/s	Dual xDSL, load balancing & failover
Wi-Fi Backhaul	$\approx$ 2 Gb/s aggregate	Supports 20 Access Points

3.3.2 Technology Selection

The assignment explicitly requires consideration of new WAN technologies such as SD-WAN or MPLS, together with cost analysis and performance evaluation. After comparing these alternatives, the SD-WAN approach is identified as the optimal solution for the hospital environment.

MPLS provides dedicated circuits and carrier-level Quality of Service, ensuring predictable latency. However, it involves high operational expenses (typically exceeding 100 USD per Mb per month) and limited flexibility. Its reliance on service-provider management delays scalability and network updates. Moreover, MPLS by default does not encrypt traffic, necessitating additional IPsec configuration to meet the hospital's strict data protection requirements. These constraints conflict with the assignment's criteria emphasizing ease of upgrade, high security, robustness under failure, and the capability of future extension.

Conversely, SD-WAN (Software-Defined Wide Area Network) fully aligns with these requirements. It integrates encrypted IPsec tunnels, centralized management, and real-time traffic optimization using software controllers. SD-WAN dynamically distributes data

flows across multiple links based on performance metrics such as latency and jitter, allowing the system to prioritize mission-critical medical traffic automatically. Its cost is considerably lower, operating efficiently on commercial leased lines or broadband connections (approximately 30–50 USD per Mb per month). Furthermore, SD-WAN simplifies deployment through virtual overlays that can be monitored and reconfigured without external provider intervention, thus satisfying the project's emphasis on manageability and maintainability.

Performance differentiation is another decisive advantage. Through integrated Quality of Service mechanisms, SD-WAN can classify and prioritize traffic into hierarchical classes such as: (1) diagnostic imaging and PACS data, (2) clinical and database transactions (HIS/LIS), (3) administrative communications, and (4) public or guest Wi-Fi. This ensures that latency-sensitive and high-bandwidth medical data receive transmission priority even during congestion periods, an essential requirement in healthcare systems. The dynamic nature of SD-WAN also permits bandwidth aggregation across dual leased lines, effectively doubling available throughput and ensuring failover resilience.

Mathematically, the effective throughput under SD-WAN link aggregation can be represented as:

$$B_{\text{effective}} = \sum_{i=1}^{n} (B_i \times \eta_i) \tag{3.1}$$

where B_i represents the capacity of each link and η_i denotes the utilization efficiency (typically $0.9 \leq \eta_i \leq 1.0$). For two 25 Mb/s links operating at 95% efficiency, the total effective throughput is:

$$B_{\text{effective}} = (25 + 25) \times 0.95 = 47.5 \text{ Mb/s}$$

This configuration not only achieves redundancy but also ensures nearly full utilization of available resources. In the event of one link's failure, the remaining connection still sustains the minimum required bandwidth of 25 Mb/s, thus maintaining service continuity for both auxiliary sites.

The SD-WAN configuration can be implemented using Cisco ISR 4331 routers equipped with SD-WAN feature sets, which comply with the assignment's guideline to utilize Cisco Packet Tracer or GNS3 for simulation. OSPF is employed for dynamic routing within the LAN, and site-to-site VPN tunnels ensure secure data transmission between the Main Site and the auxiliary branches. Internet load balancing and failover are achieved through

Policy-Based Routing and Equal-Cost Multi-Path configurations across the dual xDSL gateways.

3.4 Wireless Network Design and Security Standards

The wireless network within the Specialized Hospital is designed to provide complete coverage, secure access, and seamless mobility for medical staff, administrative users, and patients. It follows strict healthcare data protection standards and integrates with the hospital's VLAN-based wired infrastructure to maintain security, performance, and service continuity. The Wi-Fi network uses enterprise-grade architecture—combining centralized management, multiple SSIDs, VLAN tagging, and WPA3 encryption—to ensure both accessibility and patient data safety.

3.4.1 Wireless Network Architecture

Design Objectives

- Ensure full Wi-Fi coverage across hospital buildings, wards, laboratories, and public areas.
- Support mobile healthcare applications such as EMR access, patient monitoring, and teleconsultation.
- Separate traffic between staff, administrative users, guests, and IoT devices.
- Maintain compliance with hospital data protection regulations and prevent unauthorized access.
- Provide redundant uplinks for high availability and load balancing across access points.

Access Point Deployment

- **Technology:** Wi-Fi 6 (802.11ax) dual-band access points (2.4GHz & 5GHz)
- **AP Quantity:**
  - 15 units in Main Hospital (covering 2 buildings × 5 floors)
  - 3 units per auxiliary site (DBP and BHTQ)
- **Backhaul Connectivity:** Gigabit Ethernet connections to 2960 Access Switches, powered via PoE.

- **Coverage Strategy:**
  - Access points are ceiling-mounted in corridors and wards to provide uniform coverage.
  - Signal overlap between APs is limited to 15–20% to minimize interference.
  - Guest access zones (waiting areas, cafeteria) use separate SSIDs and VLANs.

Table 3.5: Wireless Access Point Layout

Location	**AP Count**	**SSID**	**Assigned VLAN / Subnet**
Building A (Staff & Medical)	8	Hospital-Staff	VLAN 30 - 192.168.15.0/24
Building B (Admin & Patients)	7	Hospital-Guest	VLAN 50 - 192.168.25.0/24
DBP Site	3	DBP-WiFi	VLAN 115 - 192.168.115.0/24
BHTQ Site	3	BHTQ-WiFi	VLAN 135 - 192.168.135.0/24

3.4.2 Security Standards

Authentication and Encryption

- WPA3-Enterprise is adopted for internal networks, using 802.1X authentication through RADIUS servers located in the Main Hospital's Data Center.
- WPA2-Personal (with captive portal) is applied for guest access, isolating guest traffic from hospital VLANs.
- AES encryption ensures confidentiality of all wireless transmissions, preventing eavesdropping or man-in-the-middle attacks.

VLAN Segmentation Wireless traffic is separated by SSID and VLAN assignment:

Table 3.6: Wireless VLAN Segmentation

SSID	VLAN ID	Subnet	Access Policy
Hospital-Staff	30	192.168.15.0/24	Full access to HIS, LIS, PACS systems
Hospital-Admin	40	192.168.20.0/24	Limited access to management systems
Hospital-Guest	50	192.168.25.0/24	Internet access only, blocked to LAN
Hospital-IoT	60	192.168.55.0/24	IoT sensors, CCTV, VLAN-isolated

Key Enforcement Policies:

- Staff VLANs can reach internal servers (10.0.3.0/24).
- Guest VLANs are blocked by ASA ACLs from accessing any 192.168.x.x subnets.
- IoT VLANs communicate only with IoT servers (10.0.3.10) via TCP port filtering.

Firewall and Intrusion Protection

- The Cisco ASA 5516-X Firewall filters all inbound/outbound traffic.
- IDS/IPS (Intrusion Detection/Prevention System) modules are deployed to monitor suspicious activity, such as rogue APs or abnormal traffic patterns.
- Access Control Lists (ACLs) enforce segmentation between VLANs and block inter-VLAN routing for guest networks.

Network Access Control (NAC)

To prevent unauthorized devices from joining the hospital network:

- MAC address filtering is enabled for IoT and staff VLANs.
- Port Security limits the number of devices per access port on switches.
- Dynamic ARP Inspection (DAI) and DHCP Snooping are enabled to mitigate spoofing attacks.
- Guest devices are automatically redirected to a Captive Portal for login and bandwidth control.

3.4.3 Wireless Controller and Management

The hospital uses a centralized controller-based WLAN architecture for scalability and unified management.

Table 3.7: Wireless Management Components

Component	**Function**
Wireless LAN Controller (WLC)	Central AP management, firmware updates, SSID configuration
RADIUS Server	Authentication for WPA3-Enterprise users
Syslog & SNMP	Monitor AP uptime, interference, and client count
Network Monitoring	Detects rogue devices and AP channel overlap

Advantages:

- Simplifies configuration of APs across multiple buildings.
- Enables centralized firmware updates and security policy enforcement.
- Provides real-time analytics on Wi-Fi usage and client load.

3.4.4 Quality of Service (QoS) and Bandwidth Control

To ensure medical systems always receive priority bandwidth:

- Voice and Video traffic (telemedicine) are assigned high-priority queues.
- HIS and PACS applications use assured forwarding (AF31–AF33).
- Guest VLANs have capped bandwidth per user (2 Mbps).
- IoT VLANs are rate-limited to prevent background sensor floods.

QoS configurations are implemented both on the WLC and Core/Distribution switches using DSCP marking.

3.4.5 Wireless Security and Monitoring Enhancements

- **Wireless Intrusion Prevention System (WIPS):** Detects rogue APs and wireless spoofing attempts.

- **Rogue AP containment:** Automatically blocks unauthorized SSIDs.
- **Network Segmentation with ASA:** Guest and IoT VLANs terminate at ASA interfaces with strict ACL filtering.
- **Syslog Integration:** All wireless logs are forwarded to the hospital's central monitoring server.
- **Scheduled Re-authentication:** Forces users to re-authenticate periodically to maintain session integrity.

3.5 Network Server Partitioning and DMZ Configuration

In a healthcare network, protecting patient data and ensuring uninterrupted service delivery are paramount. The Specialized Hospital's network adopts a multi-tiered server partitioning model that separates internal, DMZ, and Internet zones through firewalls and access control lists (ACLs). This design guarantees data confidentiality, prevents unauthorized access, and maintains compliance with hospital cybersecurity standards.

3.5.1 Server Architecture Overview

The hospital's servers are organized into three logical zones to optimize security and performance:

Table 3.8: Server Zone Architecture

Zone	**Subnet / Example**	**Primary Function**
Internal Network Zone	10.0.3.0/24, 172.16.x.x	Internal hospital applications (HIS, LIS, PACS, Database, Backup)
DMZ (Demilitarized Zone)	10.0.3.1/24	Public-facing services (Web, Email, FTP, IoT gateway)
External / Internet Zone	200.x.x.x	Internet access and external connections (VPN, cloud services)

Each zone is physically and logically separated by the Cisco ASA 5516-X firewall. Traffic between these zones is regulated through firewall rules, static routes, and NAT policies to maintain both accessibility and isolation.

3.5.2 Internal Network Zone

The Internal Zone hosts all critical medical and operational systems required for hospital management. Access to this zone is strictly limited to trusted internal VLANs (Administration, Medical, Laboratory, Pharmacy).

Contained Servers and Services

Table 3.9: Internal Zone Servers

Server Type	**Function**	**Subnet**
HIS (Hospital Information System)	Centralized patient records and scheduling	10.0.3.10
LIS (Laboratory Information System)	Test result management	10.0.3.20
PACS (Radiology Imaging Server)	Imaging storage and retrieval	10.0.3.30
Database Server	Medical data and patient archives	10.0.3.40
Backup Server	Daily snapshots and off-site replication	10.0.3.50

Security and Access Rules

- Access only from VLANs assigned to medical departments.
- No direct Internet access; all outbound traffic passes through the ASA firewall.
- Internal communication between HIS/LIS/PACS servers occurs via a private subnet using internal routing on multilayer switches.
- Periodic synchronization with DBP and BHTQ sites via secure OSPF and VPN tunnels.

3.5.3 DMZ Zone Configuration

The DMZ (Demilitarized Zone) serves as a buffer between the hospital's internal network and the Internet. It hosts systems that require external accessibility while isolating them from sensitive internal data.

Contained Servers and Services

Table 3.10: DMZ Zone Servers

Server	**Function**	**Subnet (DMZ)**	**Access**
Web Server	Public hospital portal and patient information site	10.0.3.11	Accessible from Internet (HTTP/HTTPS)
Email Server	Staff and departmental email communication	10.0.3.12	Accessible via secure SMTP/IMAP (VPN required externally)
FTP Server	File uploads (medical forms, reports)	10.0.3.13	Restricted access from authenticated staff only
IoT Gateway Server	Collects camera and sensor data from IoT VLANs	10.0.3.14	Accessible only from IoT VLAN and Admin VLAN
DNS Server	Resolves internal hospital domains	10.0.3.15	Accessible from all VLANs, limited from Internet

Firewall Policies (ASA Configuration)

Traffic between the DMZ and other zones is strictly controlled by the ASA firewall.

Table 3.11: ASA Firewall Rules

Rule No.	Source Zone	Destination Zone	Action	Purpose
1	Internet	DMZ (Web Server)	Allow TCP 80/443	Public website access
2	Internet	DMZ (Mail Server)	Allow TCP 25/465/993	Secure email access
3	Internal VLANs	DMZ	Allow necessary ports	Internal access to web and mail
4	DMZ	Internal	Deny by default	Prevent external compromise
5	IoT VLAN	IoT Server (DMZ)	Allow TCP 8080/1883	IoT data ingestion
6	Guest VLAN	Any Internal	Deny all	Guest isolation
7	Any	Internet	NAT + Allow	Outbound Internet access via firewall

3.5.4 External and Internet Zone

The External Zone connects the hospital's network to the Internet and to the WAN links leading to the DBP and BHTQ sites. It enables secure connectivity for external users, telemedicine specialists, and remote administrators through VPNs.

Security Measures

- **Dual-WAN redundancy** ensures continuous Internet access.
- **IPsec VPN tunnels** connect to DBP and BHTQ auxiliary sites.
- **VPN for Teleworkers** allows doctors to securely access HIS and EMR systems remotely.
- **Firewall inspection** monitors inbound and outbound packets to detect anomalies.
- **Anti-spoofing ACLs** block traffic using invalid source IPs.

3.5.5 Network Traffic Flow Examples

Table 3.12: Network Traffic Flow Scenarios

Scenario	Path	Security Mechanism
Doctor accesses HIS system	VLAN 20 → Core Switch → HIS Server	Internal route (no Internet exposure)
Patient visits hospital website	Internet → ASA Firewall → DMZ Web Server	NAT + HTTP ACL
IoT camera sends data	VLAN 55 → ASA → DMZ IoT Server	ACL port-based restriction
Staff email synchronization	VLAN 40 → ASA → DMZ Email Server → Internet	Authenticated SMTP/IMAP
Remote staff VPN login	Internet → ASA VPN → Internal VLAN	IPsec encryption + 2FA
DBP/BHTQ synchronization	WAN (OSPF) → Core Router → Data Center	VPN tunnel over leased line

4 Equipment List, IP Plan, and System Diagram

4.1 Equipment List

4.1.1 Router

- **Model:** Cisco 2911 Integrated Services Router or above
- **Features:** Supports OSPF, static routing, VPN, and QoS; dual WAN interfaces for redundancy
- **Memory:** 512 MB DRAM, 256 MB Flash
- **Data Rate:** Up to 1 Gbps throughput
- **Purpose:** Core routing between hospital buildings and WAN links to DBP and BHTQ branches

4.1.2 Switch

- **Model:** Cisco Catalyst 3560-X or Cisco Catalyst 9300 Series
- **Type:** Layer 3 Switch (used at Core and Distribution Layers)
- **Features:** VLAN support, inter-VLAN routing, QoS, redundancy (HSRP/VRRP), trunking support
- **Data Rate:** Up to 10 Gbps per port (fiber uplinks)
- **Purpose:** Core and distribution connectivity in Data Center and main buildings

4.1.3 Access Switch

- **Model:** Cisco Catalyst 2960 Series or above
- **Type:** Layer 2 Switch (used at floor level and in branch sites)
- **Features:** VLAN tagging, PoE support for APs and IP cameras, port security
- **Data Rate:** 1 Gbps per port
- **Purpose:** Connects end-user PCs, IoT devices, and wireless APs to the network

4.1.4 Server

- **Model:** Cisco UCS C240 M7 Rack Server or equivalent
- **Features:** High-performance, scalable for virtualization (HIS, LIS, PACS, CRM, Web, Mail)
- **Processor:** 4th Gen Intel Xeon Scalable Processors
- **RAM:** Up to 8 TB
- **Storage:** Up to 24 drive bays (SSD/HDD hybrid)
- **Network Interface:** Dual 10/100/1000 Mbps Ethernet ports, optional 10GbE SFP+
- **Purpose:** Hosting all hospital management systems, databases, and services

4.1.5 Wireless Access Point (AP)

- **Model:** Cisco Aironet 3800 or Catalyst 9120AX Series
- **Features:** Dual-band 2.4/5 GHz, Wi-Fi 6 (802.11ax), WPA3 security, centralized controller support
- **Data Rate:** Up to 5.2 Gbps
- **Antennas:** Internal (omni) for indoor coverage
- **Purpose:** Wireless connectivity for medical staff, administrative staff, and patients

4.1.6 Firewall (ASA)

- **Model:** Cisco ASA 5516-X or Firepower 1000 Series
- **Features:** Stateful firewall, NAT, IPsec/SSL VPN, IPS/IDS modules, dual ISP load balancing
- **Throughput:** Up to 1 Gbps
- **VPN Support:** IPsec Site-to-Site and SSL VPN for teleworkers
- **Interfaces:** 8 × Gigabit Ethernet ports
- **Purpose:** Protects the internal network, isolates DMZ, and handles VPN connectivity to DBP & BHTQ

4.1.7 Webcam / Surveillance Camera

- **Model:** Cisco Desk Camera 1080p or equivalent IP CCTV
- **Features:** 8MP image sensor, 4× digital zoom, 1080p@30fps, night vision, PoE-powered
- **Network Interface:** 10/100 Ethernet (PoE)
- **Purpose:** Real-time patient and facility monitoring via IoT VLAN

4.1.8 IoT Sensors

- **Model:** Cisco Industrial IoT Series
- **Features:** Temperature, humidity, patient vitals monitoring via MQTT/HTTP
- **Connectivity:** Wi-Fi / Ethernet (VLAN 55)
- **Purpose:** Environmental control and patient condition monitoring integrated into HIS

4.1.9 UPS and Power Backup

- **Model:** APC Smart-UPS 3000VA or equivalent
- **Feature:** Online double conversion, surge protection, network monitoring
- **Purpose:** Maintains continuous operation of Data Center, servers, and network racks

4.2 WAN Connection Diagram Between Main Hospital and Branches

4.2.1 WAN Connection to Main Hospital

The Main Hospital located in Ho Chi Minh City serves as the central hub of the entire network system. It includes two main buildings (Building A and Building B), each with five floors, and a dedicated Data Center that hosts all hospital servers and security devices. The Main Site also manages WAN connections to both auxiliary branches (DBP and BHTQ) through secure leased lines and VPN tunnels.

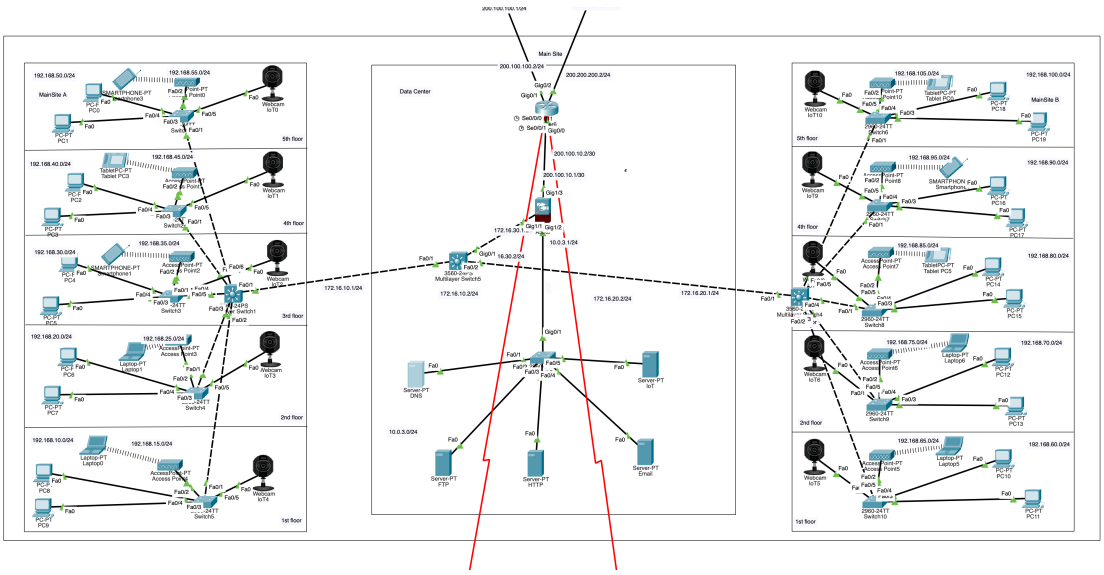

Figure 4.1: WAN Connection - Main Hospital

Network stucture is as follows:

- The Main Hospital connects two 5-floor buildings (A and B) to the Data Center using fiber cabling and Layer 3 switches (Cisco Catalyst 3560-24PS).
- Each building is divided into multiple VLANs by floor to isolate departmental traffic and IoT devices such as IP cameras and wireless access points.
- All VLANs converge to the core multilayer switch (3560-24PS) in the Data Center, which connects to the ASA firewall (5516-X) and Core Router (2911) for external communication.
- The Core Router (2911) manages internal routing and two WAN links that connect to:
  - DBP Branch: via subnet 200.100.20.0/30
  - BHTQ Branch: via subnet 200.100.30.0/30
- The ASA Firewall performs NAT, VPN, and Internet routing through dual xDSL links (200.100.100.0/24 and 200.200.200.0/24).

IP Addressing and Subnets

Table 4.1: Main Hospital Network Subnets

Network / VLAN	**Purpose**	**IP Range**
VLAN 10	IT Department - Building A	192.168.10.0/24
VLAN 20	Administration - Building A	192.168.20.0/24
VLAN 30	HR & Accounting - Building A	192.168.30.0/24
VLAN 40	Medical & Laboratory - Building A	192.168.40.0/24
VLAN 50	Wi-Fi / Smartphones - Building A	192.168.50.0/24
VLAN 55	IoT Devices (Cameras, Sensors) - Building A	192.168.55.0/24
VLAN 60	IT Department - Building B	192.168.60.0/24
VLAN 70	Administration - Building B	192.168.70.0/24
VLAN 80	HR & Pharmacy - Building B	192.168.80.0/24
VLAN 90	Medical & Imaging - Building B	192.168.90.0/24
VLAN 100	Wi-Fi / Staff Devices - Building B	192.168.100.0/24
VLAN 105	IoT Devices (Cameras, Sensors) - Building B	192.168.105.0/24
VLAN 200	Data Center Servers (DNS, HTTP, Email, IoT)	10.0.3.0/24
VLAN 300	DMZ Network	10.0.3.1/24
VLAN 400	Inter-building backbone (fiber trunk)	172.16.10.0/24
VLAN 500	Management VLAN (Switches, APs, Firewalls)	172.16.30.0/24

Devices and Connections

Table 4.2: Main Hospital Devices

Device	**Model**	**Function**
Core Router	Cisco 2911 ISR	Central routing between LAN, DMZ, and WAN connections
Firewall	Cisco ASA 5516-X	NAT, VPN (IPsec + SSL), security filtering, dual-ISP load balancing
Multilayer Switch (Core)	Cisco Catalyst 3560-24PS	Inter-VLAN routing, OSPF, VLAN trunking
Access Switches	Cisco Catalyst 2960-24TT	Connects PCs, APs, and IP cameras per floor
Access Points	Cisco Aironet 3800 Series	Wireless coverage (Wi-Fi 6) throughout both buildings
Servers (Data Center)	DNS, HTTP, Email, IoT Servers	Host HIS/LIS/PACS and hospital services
IoT Cameras	Cisco Desk Camera 1080p	Surveillance and patient monitoring
PCs and Laptops	HP / Dell OptiPlex	End-user terminals for hospital staff

Routing and WAN Interfaces

Table 4.3: Main Site WAN Interfaces

Interface	IP Address	Connected To	Description
Serial0/0/0	200.100.20.1/30	DBP Router	Leased line to DBP branch
Serial0/1/0	200.100.30.1/30	BHTQ Router	Leased line to BHTQ branch
Gig0/0	172.16.10.1/24	Multilayer Switch (Core)	Internal backbone connection
Gig0/1	200.100.100.2/24	ASA Firewall / Internet	Dual WAN to ISP 1
Gig0/2	200.200.200.2/24	ASA Firewall / Internet	Dual WAN to ISP 2

4.2.2 WAN Connection to DBP Branch

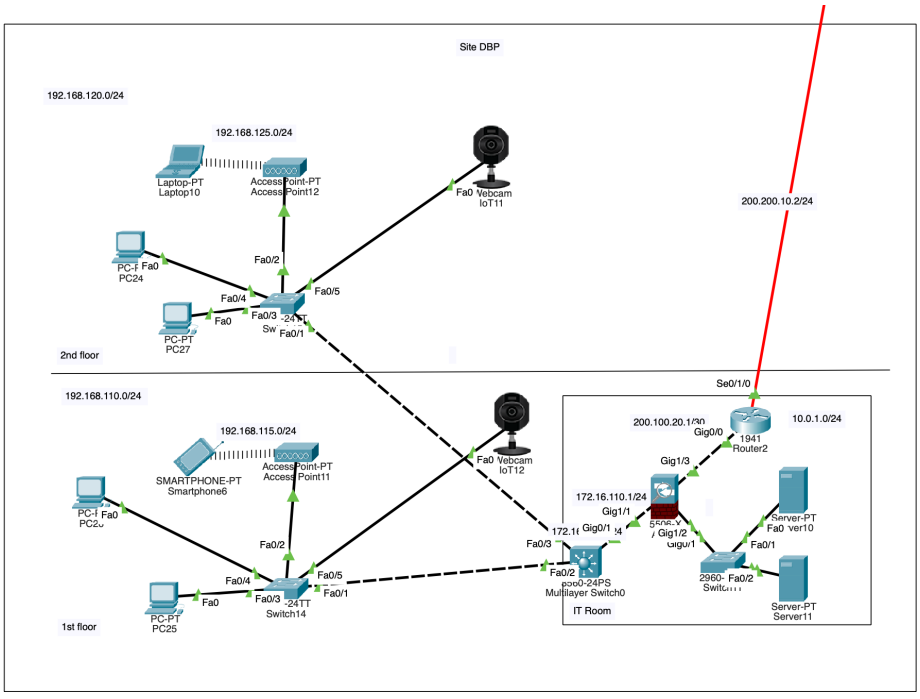

Figure 4.2: WAN Connection to DBP Branch

Labels & Addressing

- **Main Site (Data Center router / core)**
  - Router (Core/2911) interface to DBP: Serial0/0/0 — 200.100.20.1/30

  - Core interface toward internal switches: Gig0/1 — 172.16.10.1/24
  - ASA outside (Internet): 200.100.100.2/24

- **DBP Site (Branch router / 1941)**
  - Router (DBP 1941) Serial interface to Main: Serial0/0/0 — 200.100.20.2/30
  - DBP router Gig interface to local multilayer switch: Gig0/0 — 172.16.110.1/24
  - Local IT Room multilayer switch SVI: 172.16.110.2/24

- **Local DBP subnets**
  - Floor 1: 192.168.110.0/24
  - Floor 2: 192.168.120.0/24
  - Wi-Fi: 192.168.115.0/24
  - IoT (Cameras): 192.168.125.0/24
  - Local servers: 10.0.1.0/24

4.2.3 WAN Connection to BHTQ Branch

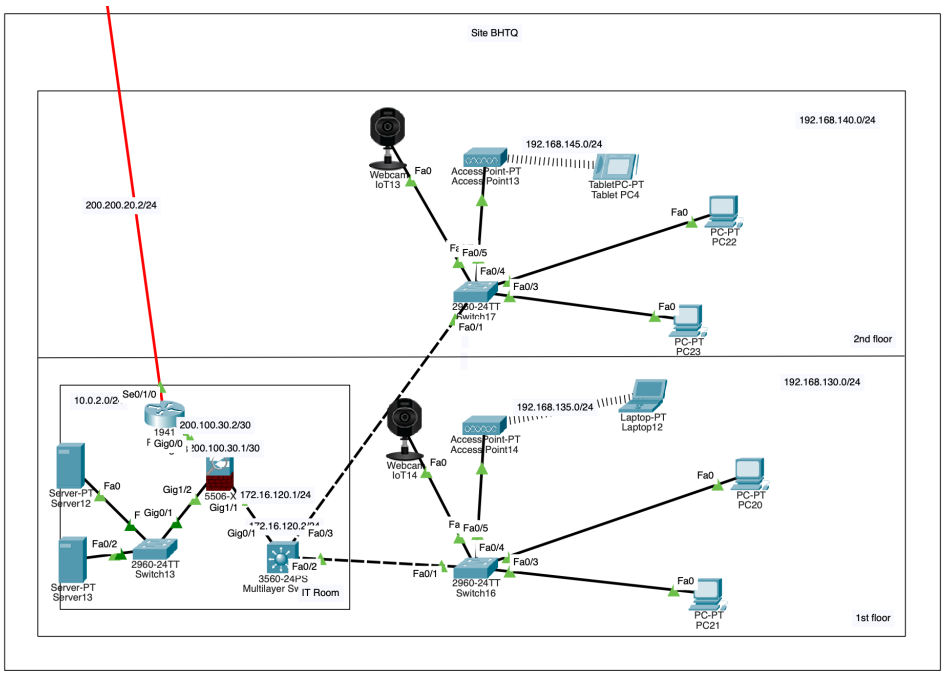

Figure 4.3: WAN Connection to BHTQ Branch

Labels & Addressing

- **Main Site (Data Center / core)**
  - Router interface to BHTQ: Serial0/1/0 — 200.100.30.1/30
  - Internal core: 172.16.10.1/24
- **BHTQ Site (Branch router / 1941)**
  - Router Serial interface to Main: Serial0/0/0 — 200.100.30.2/30
  - Router Gig to local LAN: Gig0/0 — 172.16.120.1/24
  - Local multilayer switch SVI: 172.16.120.2/24
- **Local BHTQ subnets**
  - Floor 1: 192.168.130.0/24
  - Floor 2: 192.168.140.0/24
  - Wi-Fi: 192.168.135.0/24
  - IoT: 192.168.145.0/24
  - Local servers: 10.0.2.0/24

4.2.4 Internet Connectivity and Centralized NAT

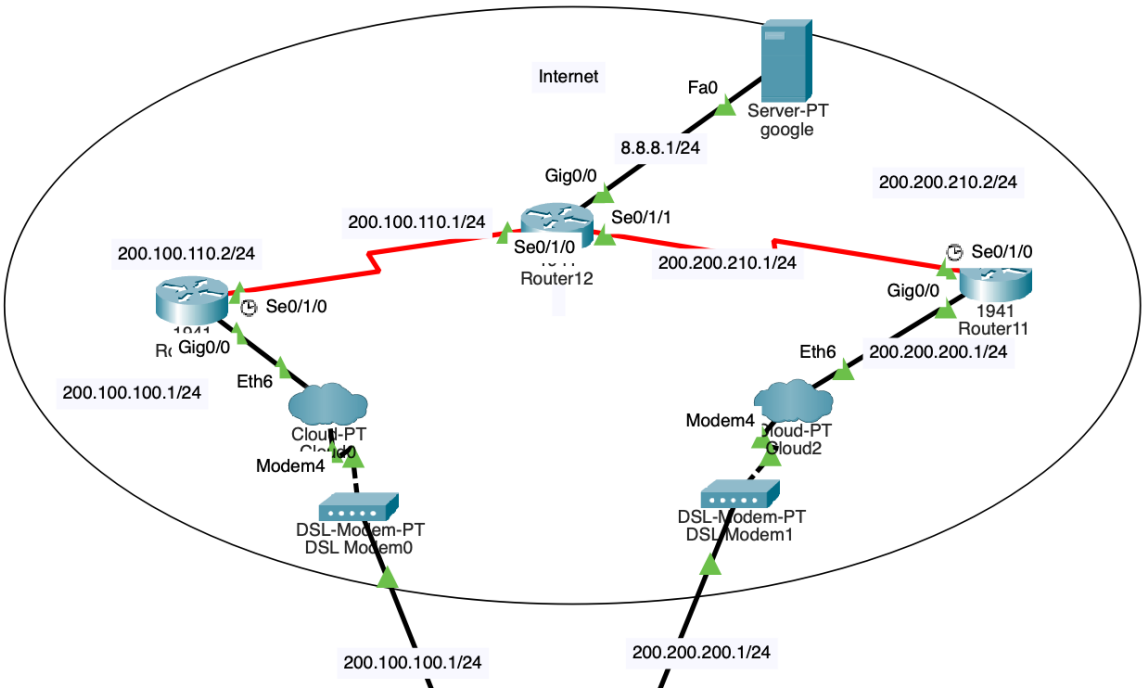

Figure 4.4: Internet Layer Topology

IP Addressing & Components

- ISP Link A (xDSL/fiber): 200.100.100.0/24 — Main ASA outside IP: 200.100.100.2
- ISP Link B (xDSL/fiber): 200.200.200.0/24 — secondary link for failover/load balancing
- Public-facing DMZ IPs NATed to internal servers (e.g., Web server 10.0.3.11 → public 200.100.100.10)

5 Test the System

After completing the network configuration and establishing the connections between the Main Hospital and its branches (DBP and BHTQ), we conducted several tests to verify end-to-end connectivity, VLAN segmentation, inter-site routing, and server accessibility.

5.1 Connection between PCs in the same VLAN

- **Purpose:** To verify internal communication among devices in the same department (same VLAN).
- **Test Setup:**
  - **Source:** PC0 (Building A - VLAN 50: Wi-Fi / Smartphones) - IP: 192.168.50.12
  - **Destination:** PC1 (Building A - VLAN 50: Wi-Fi / Smartphones) - IP: 192.168.50.11
- **Result:** Successful ping and communication between devices in the same VLAN.

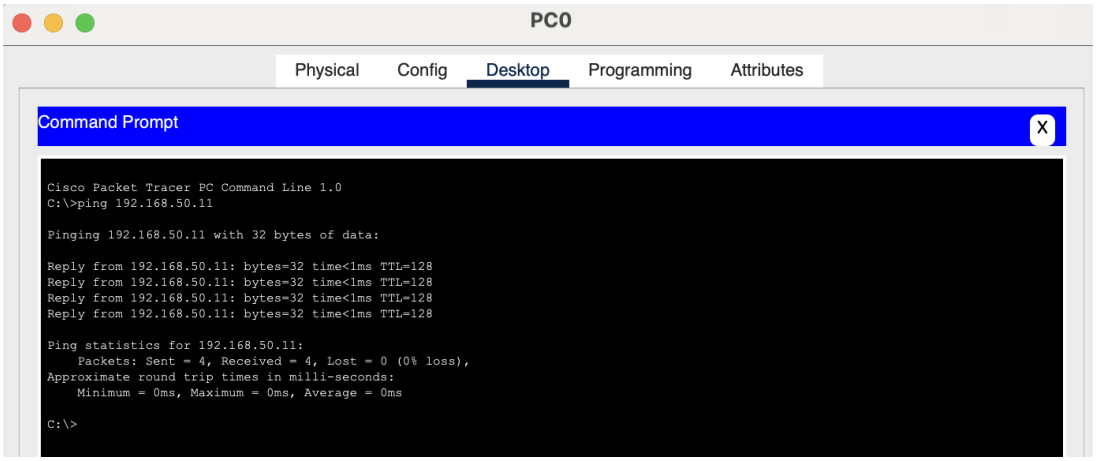

Figure 5.1: Ping Test between PC1 and PC0 in VLAN 50

5.2 Connection between two PCs in different VLANs

- **Purpose:** To confirm that inter-VLAN routing via the Core Multilayer Switch (3560-24PS) works properly.
- **Test Setup:**
  - **Source:** PC1 (Building A - VLAN 50: Administration) - IP: 192.168.50.11
  - **Destination:** PC18 (Building B - VLAN 100: Wi-Fi / Staff Devices) - IP: 192.168.100.11
- **Result:** Successful routing between different VLANs through the multilayer switch.

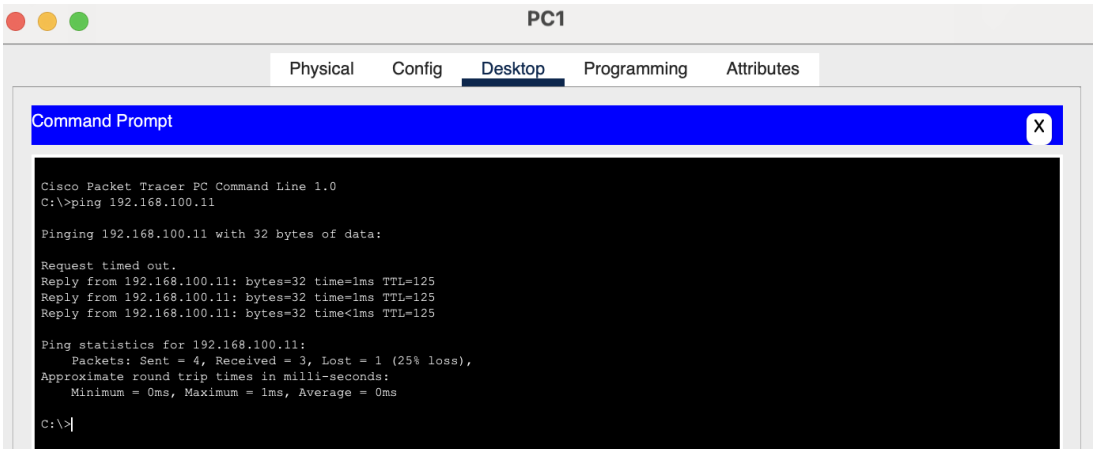

Figure 5.2: Ping Test between PC1 and PC19 in VLAN 50 - VLAN 100

5.3 Connection between Main Hospital and DBP Branch

- **Purpose:** To test WAN communication between sites through the leased line and OSPF routing.
- **Test Setup:**
  - **Source:** PC4 (Building A, 3rd Floor - Main Site: Admin) - IP: 192.168.30.11
  - **Destination:** PC25 (1st Floor - DBP Site) - IP: 192.168.110.12
- **Result:** Successful end-to-end connectivity across WAN link using OSPF routing.

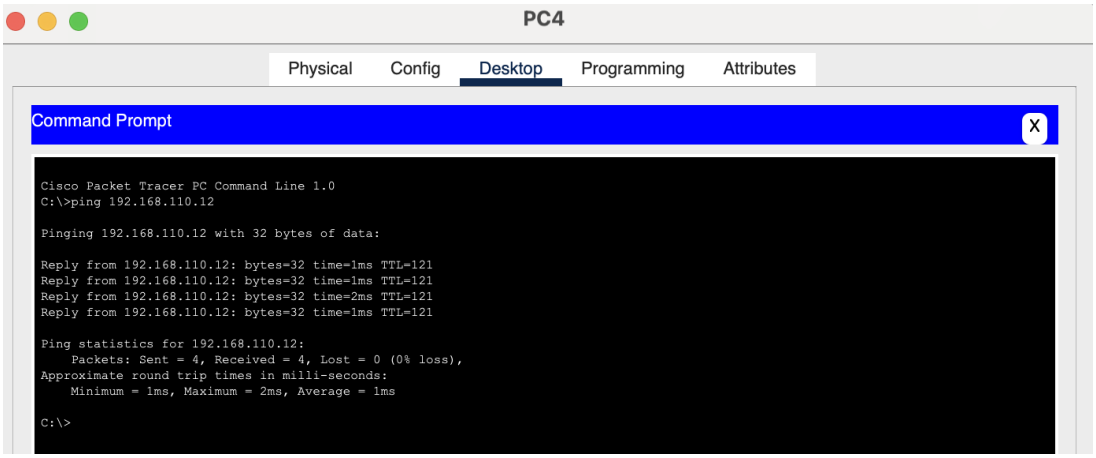

Figure 5.3: Ping Test between PC4 and PC25 across WAN

5.4 Connection between Main Hospital and BHTQ Branch

- **Purpose:** To test inter-site connectivity through the second WAN link.
- **Test Setup:**
  - **Source:** PC21 (2nd Floor - BHTQ Site: Admin) - IP: 192.168.130.12
  - **Destination:** PC17 (Building B, 4th Floor - BHTQ Site) - IP: 192.168.90.12
- **Result:** Successful WAN communication to BHTQ branch via OSPF.

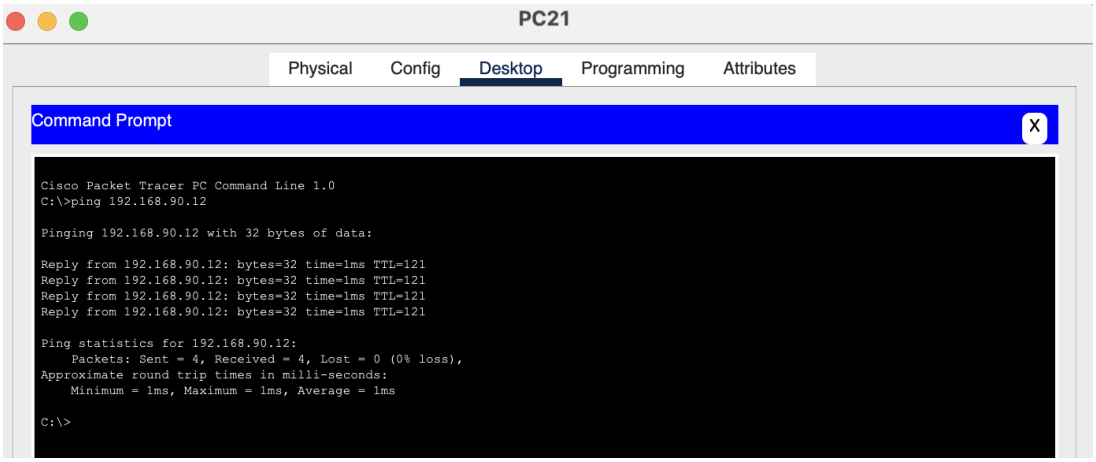

Figure 5.4: Ping Test between PC21 and PC17 across WAN

5.5 Test HTTP Web Access

- **Purpose:** To test web browsing from LAN client to hospital's internal website (hosted on Web Server in DMZ).
- **Test Setup:**
  - **Source:** PC6 (Building A, 2nd Floor - Main Site: Admin) - IP: 192.168.20.12
  - **Web address:** google.com at 10.0.3.3
- **Result:** Successful HTTP response from internal web server.

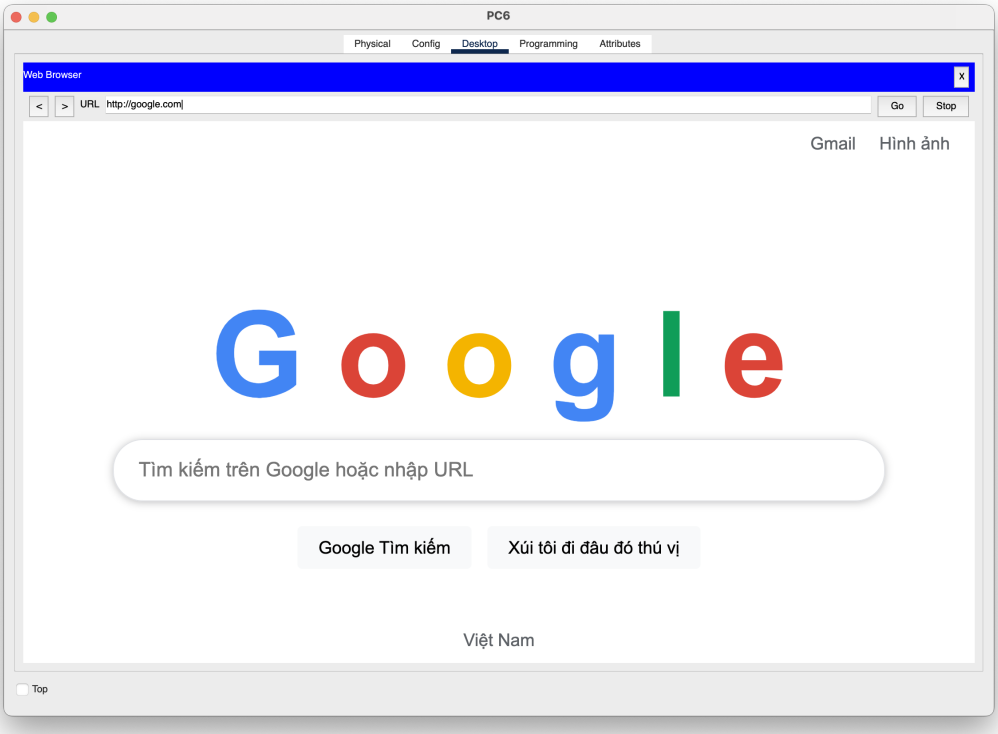

Figure 5.5: HTTP Test from PC6 to Web Server

5.6 Email Communication between Branches

- **Purpose:** To confirm that Email Server configuration (SMTP/POP3) and DNS resolution work across sites.
- **Test Setup:**
  - **Source:** PC9 (Building A, 1st Floor - Main Site) - IP: 192.168.20.2 via pc9@email.hospital.

  - **Destination:** PC19 (Building B, 5th Floor - Main Site) - IP: 192.168.110.12 via pc19@email.hospital.com
  - **Mail Server IP:** 10.0.3.5 via email.hospital.com

- **Result:** Email successfully sent from Main Hospital to DBP branch and received without errors.

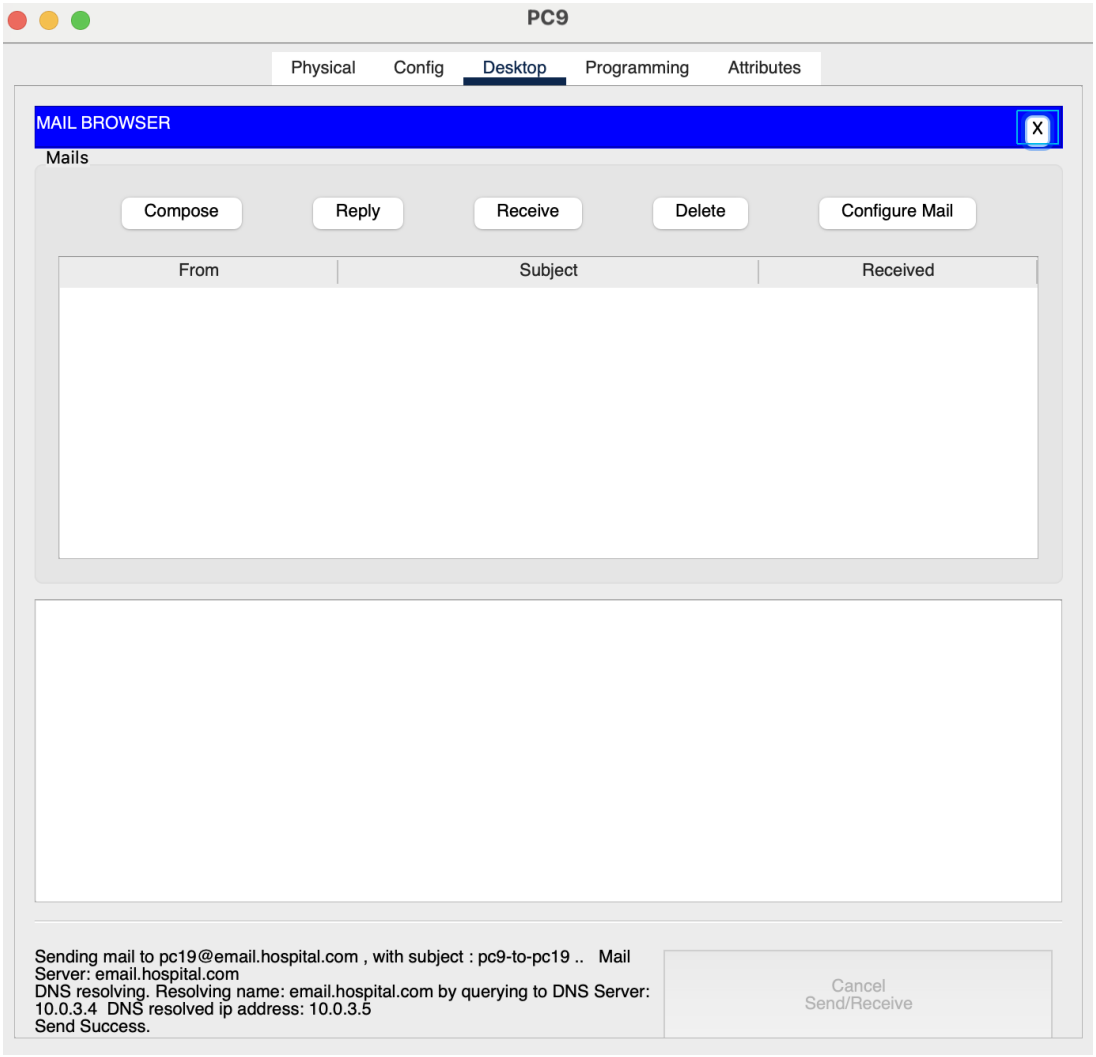

Figure 5.6: Email sent from PC9 to PC19

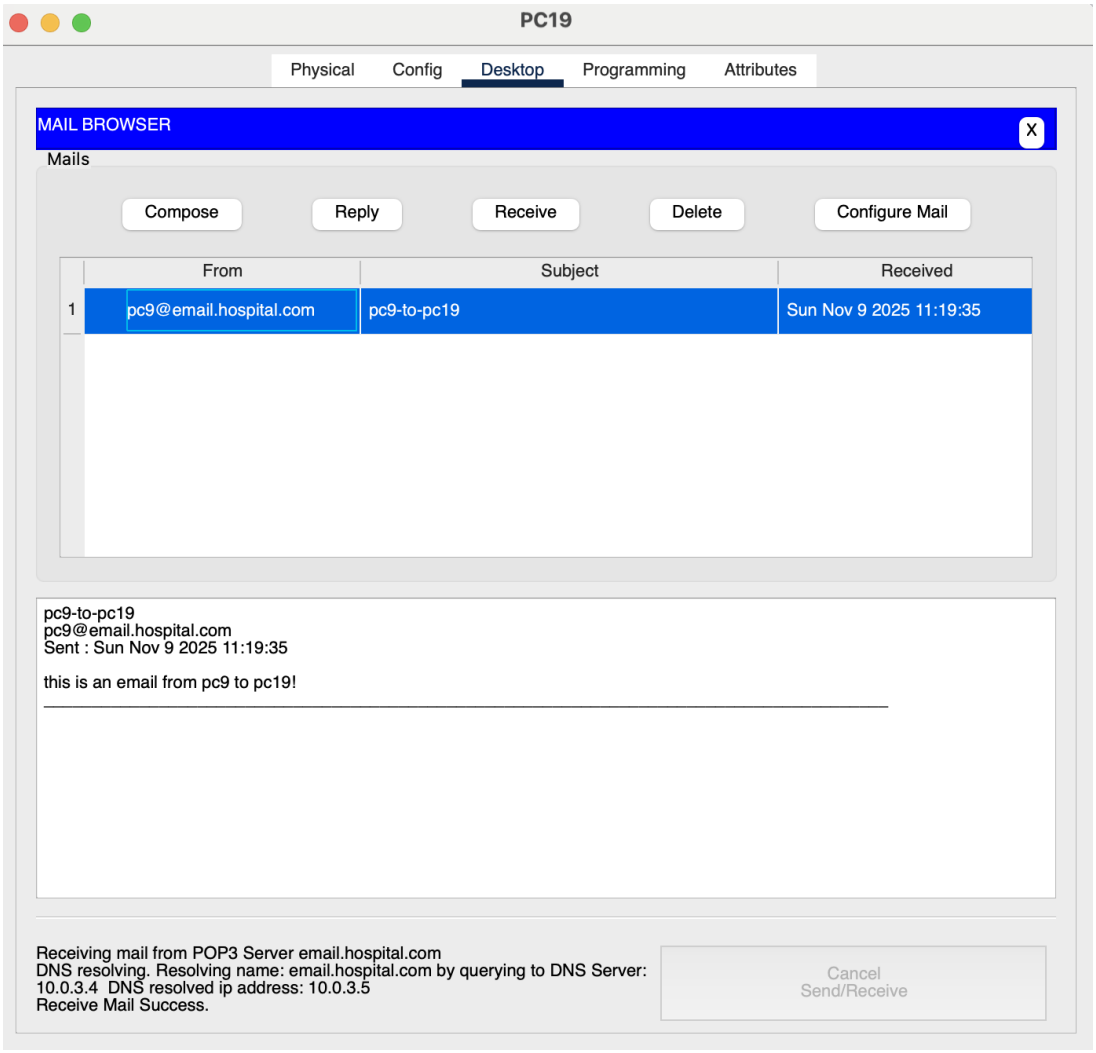

Figure 5.7: Email received at PC19 from PC9

6 Conclusion

This project presented a practical, scalable network design tailored for a large, specialized hospital with one Main Site and two Auxiliary Sites. The proposed three-tier architecture (core, distribution, and access) combined with VLAN segmentation, redundant core devices, and an SD-WAN overlay delivers the reliability, performance, and security required by critical healthcare applications such as HIS, PACS, and LIS. By sizing links conservatively and including dual xDSL Internet connections and redundant WAN tunnels, the design provides both daily capacity and headroom for growth.

Security and availability were prioritized: the ASA firewall and DMZ isolate public services, IDS/IPS and NAC protect internal resources, and VLANs isolate IoT and guest

traffic from sensitive medical systems. Quality of Service and Wi-Fi 6 deployment ensure that latency-sensitive services (telemedicine, imaging) receive priority during peak periods. The equipment selection and IP addressing plan support manageable expansion and straightforward operations for the hospital IT team.

The design acknowledges limitations and areas for future improvement. While SD-WAN offers a cost-effective, flexible WAN solution, a migration plan and vendor testing should precede production deployments; likewise, regular penetration testing and periodic capacity reviews will be essential as device counts and traffic grow. Finally, automating monitoring and backup procedures and adopting a staged rollout (pilot in one auxiliary site) will reduce operational risk and simplify troubleshooting.

Overall, the network design balances performance, security, and cost to meet the hospital's immediate needs while providing a clear path for scale and resilience. The recommendations and configurations in this report form a practical blueprint for implementation and ongoing maintenance to support secure, continuous healthcare services.