VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

COMPUTER NETWORK ASSIGNMENT 2

Network design and simulation for a critical large hospital

Instructor(s): Nguyễn Thành Nhân, *CSE - HCMUT*

Students: Trần Anh Đức - 2352271 *(Class CC06, **Leader**)*
Hồ Lâm Khánh Vy - 2353353 *(Class CC06)*
Trần Hoàng Khánh - 2352533 *(Class CC06)*
Huỳnh Quốc Đạt - 2352228 *(Class CC06)*

HO CHI MINH CITY, October 2025

Contents

1 Member List & Workload

No.	Fullname	Student ID	Work	% done
1	Trần Anh Đức	2352271	- Design Packet Tracer File - Report Writing	100%
2	Hồ Lâm Khánh Vy	2353353	- Design Packet Tracer File - Report Writing	100%
3	Trần Hoàng Khánh	2352533	- Design Packet Tracer File - Report Writing	100%
4	Huỳnh Quốc Đạt	2352228	- Design Packet Tracer File - Report Writing	100%

Table 1: Member list & workload distribution

2 Project Summary

2.1 Case Study

CCC (Computer & Construction Consultant) Agency was asked to design a computer network to be deployed in the Main Site (at Ho Chi Minh City) and two Auxiliary Sites (at DBP Street and BHTQ Street) of a Specialized Hospital under construction. The key characteristics of IT usage in this Hospital are as follows.

Main Site Specifications

- 2 buildings A and B (5 floors with 10 rooms/floor) equipped with computers and medical devices.
- The data center, IT, and Cabling Central Local (using patch panels gathering wires) are located in a separate room, 50 meters from buildings A and B.
- Medium-scale: 600 workstations, 10 servers, 12 networking devices (or maybe more with security-specific devices).
- The wireless connection has to be covered for the whole Site.
- Using new technologies for network infrastructure including wired and wireless connections, fiber cabling (GPON), and GigaEthernet 1GbE/10GbE/40GbE. The network is organized according to the VLAN structure for different departments.
- The main Site subnetwork connects two other Sites (Site DBP and Site BHTQ) subnetworks by 2 leased lines for WAN connection (possibly applying SD-WAN, MPLS).
- 2 xDSL for Internet access with a load-balancing mechanism. All traffic to the Internet passes through the main site subnet.
- For software acquisition, the Hospital uses a mix of licensed and open-source software, hospital software (HIS, RIS - PACS, LIS, CRM, etc.), office applications, client-server applications, multimedia, and databases.
- Requirements for capability of extension, high security (e.g., firewall, IPS/IDS, phishing detection), high availability (HA), robustness when problems occur, ease of upgrading the system.
- Propose a VPN configuration for site-to-site and for a teleworker to connect to Company LAN.
- Propose a surveillance camera system for the Company.

Other Sites Specifications

- The building has 2 floors, the first floor is equipped with 1 IT room and 1 Cabling Central Local.
- Small-scale: 60 workstations, 2 servers, 5 or more networking devices.
- Suggest options with cost.
- Analyze the advantages and disadvantages of the selected solution.

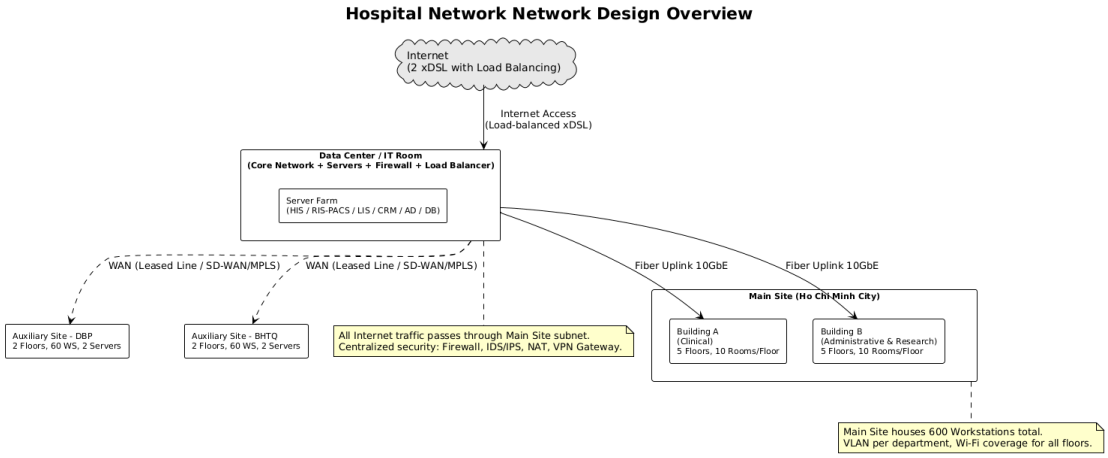

Figure 1: Hospital Network Design Overview

2.2 Project Approach

The hospital network infrastructure is designed to ensure robust, high-availability connectivity across its main and auxiliary sites. The **Main Site** consists of two primary buildings (Building A – Clinical, and Building B – Administrative & Research), each with five floors and ten rooms per floor. In addition, a dedicated **Data Center, IT, and Cabling Central Local** is located in a separate room, approximately 50 meters from the two buildings. This room serves as the aggregation and control point for all network communications.

To provide reliable Internet connectivity, the hospital employs **two xDSL connections** configured with a **load-balancing mechanism**. This configuration ensures that bandwidth usage is distributed across both Internet Service Providers (ISPs), improving throughput and providing fault tolerance in case one link fails. The dual xDSL setup enhances both performance and network resilience by allowing automatic failover and dynamic traffic distribution between the two connections.

Importantly, **all traffic to the Internet passes through the Main Site subnet**. This means that any data from workstations, servers, or auxiliary sites (DBP and BHTQ) must first be routed through the core network at the Main Site before being forwarded to the Internet. The Data Center functions as the central routing and security point, hosting critical components such as firewalls, NAT gateways, load balancers, and intrusion prevention systems (IPS/IDS). This centralized Internet breakout architecture allows the hospital to maintain strict security control, apply unified policies, and perform traffic monitoring and logging for all Internet-bound communications.

Overall, the system design integrates both wired (Ethernet/Fiber GPON) and wireless (Wi-Fi) infrastructure, organized by VLAN segmentation for each department. The centralized data flow through the Main Site subnet ensures high security, scalability, and centralized management—meeting the requirements for **high availability, robustness, and extensibility** as specified in the project.

2.3 Data Flow and Network Load

The dataflows and workload of the system (about 80% at peak hours 9g–11g and 15g–16g) can be shared for the Main Site and the two Auxiliary Sites as follows:

- **Servers:** for software updates, web access, and database access, etc. The total download estimate is about 1000 MB/day and the upload estimate is 2000 MB/day.
- **Each workstation:** is used for web browsing, document downloads, and customer transactions, etc. The total download estimate is about 500 MB/day and the upload estimate is 100 MB/day.
- **WiFi-connected devices:** from customers' access for downloading are about 500 MB/day.

Hospital Network is estimated to have a growth rate of 20% in 5 years (in terms of the number of users, network load, site extensions, etc.).

3 Proposed suitable network infrastructure

3.1 Networking system requirements analysis

The hospital network system must s upport a multi-site structure including a **Main Site** (two 5-floor buildings and one IT & Data Center block) and **two branch offices** located on different streets. Each site requires a secure, stable, and scalable infrastructure that supports both wired and wireless connectivity.

- Approximately **600 workstations**, **10 servers**, and **12 networking devices** are deployed at the Main Site.
- Each branch site has around **260 workstations**, **2 servers**, and **5 networking devices**.
- Internet connectivity is provided through two xDSL lines for **load balancing** and **redundancy**.
- WAN links between Main Site and Branch Sites use **two leased lines per branch** to ensure high availability and failover support.
- **Firewall protection**, **VLAN segmentation**, and **VPN connectivity** are required for network security and remote access.
- Wireless network must cover all floors, secured by WPA2 encryption and separated VLANs for staff and guests.

The network must support both current needs and a projected growth of approximately **20% in users and traffic over five years**.

3.2 Networking system Specifications

To satisfy these requirements, the system is designed following the **Hierarchical Network Model** with three layers: Core, Distribution, and Access. This model provides a structured, scalable, and easily manageable framework.

Layer	Main Function	Devices Used
Core Layer	Handles inter-site routing, Internet access, and WAN connections. Provides redundancy and load balancing through OSPF and ECMP.	Duo Cisco 3650 routers
Distribution Layer	Performs inter-VLAN routing, ACL filtering, and load balancing using HSRP/VRRP. Connects all Access switches within each building.	Cisco 3650 Layer-3 switches
Access Layer	Connects end devices (PCs, IoT, printers) and provides VLAN separation for departments.	Cisco 2960 Layer-2 switches and Access Points

Table 2: Hierarchical network model structure

Additional technical details:

- **Routing protocol:** OSPF for dynamic routing with equal-cost multi-path (ECMP) load balancing.

- **Firewall:** Cisco ASA 5506-X dividing the system into Inside, Outside, and DMZ zones.
- **VPN:** Site-to-Site IPsec VPN for branch connectivity and Remote Access VPN for teleworkers.
- **DHCP & DNS:** Centralized at the IT block; static IP addresses reserved for servers.
- **NAT & ACL:** Applied on firewall and L3 switches to prevent guest VLAN from accessing internal LAN.

3.3 High network load area analysis

The network load distribution was analyzed based on expected data flow and user activity during peak hours (9:00–11:00 AM and 3:00–4:00 PM).

- **Core–WAN links:** Highest load due to large inter-site traffic. Dual leased lines with ECMP ensure redundancy and prevent congestion.
- **Core–Internet gateway:** Peak load occurs from concurrent user web access and database synchronization.
- **DMZ zone:** Web, Mail, and DNS servers experience heavy public access and external traffic.
- **Wireless areas:** Public zones such as reception and cafeteria accommodate the most simultaneous guest connections.

To mitigate overload, mechanisms such as **OSPF ECMP**, **EtherChannel** for link aggregation, and dual WAN interfaces are implemented for balancing and failover.

3.4 Networking structure selection

After evaluating multiple designs, a **hybrid model** combining the **Hierarchical Network Architecture** and **Star topology** per building is selected.

Reasons for selection:

1. **Scalability:** New departments or branches can be easily added by expanding VLANs or adding switches.
2. **Performance:** Traffic isolation per layer reduces broadcast storms and increases efficiency.
3. **Reliability:** Redundant Layer-3 switches (HSRP) ensure uninterrupted operation in case of device failure.
4. **Security:** VLANs, ACLs, and firewall zones separate internal, DMZ, and external traffic.
5. **Maintainability:** Star topology per building simplifies cabling, monitoring, and troubleshooting.

Network hierarchy overview:

- **Core Layer:** Two routers configured with OSPF and ECMP, connecting WAN and Internet.
- **Distribution Layer:** Layer-3 switches manage inter-VLAN routing and implement ACL-based access control.
- **Access Layer:** Each floor or department forms a separate VLAN (e.g., VLAN10–VLAN100).

3.5 Wireless network

A wireless network is deployed to ensure complete coverage for staff and visitors. Cisco **Lightweight Access Points (LWAP)** are controlled by a central **Wireless LAN Controller (WLC)** located at the IT block.

- **SSID "StaffNet":** WPA2-Enterprise authentication, mapped to internal VLAN for employees.
- **SSID "GuestNet":** WPA2-PSK security, isolated from internal network using ACL (Internet access only).
- **Controller:** Centralized monitoring, load management, and AP roaming support.
- **Deployment:** One AP per floor (serving up to 60 devices), dual-band (2.4/5GHz) with smooth roaming.

This wireless design ensures network security, seamless coverage, and high performance for both staff and guest users across all sites.

4 List of minimum equipment, IP plan, and wiring diagram (cabling)

4.1 List of recommended equipment and typical specifications

To ensure **stability, scalability, and high performance**, the proposed network employs **Cisco enterprise-grade equipment**, commonly used in medium and large-scale organizations. The following list summarizes the recommended devices, their core functions, and key specifications.

Routers (Core Layer)

Figure 2: Cisco ISR 4331 Routers

- Two **Cisco ISR 4331 Routers** are deployed at the core layer.
- Support **dynamic routing (OSPF)** and modern WAN technologies such as **SD-WAN** and **MPLS**.
- Each router includes **three Gigabit Ethernet ports** and one modular slot for serial interfaces.
- Provides throughput up to **300 Mbps**.
- Operate in **redundant mode** for load balancing and fault tolerance, maintaining Internet and WAN connectivity during failures.

Switches (Distribution Layer & Access Layer)

- **Cisco Catalyst 3650 Layer-3 Switches** (Distribution Layer):

Figure 3: Cisco Catalyst 3650 Layer-3 Switches

  - Perform **Inter-VLAN routing**, implement **Access Control Lists (ACLs)**, and support redundancy via **HSRP/VRRP**.
  - Provide **24 Gigabit Ethernet ports** and **4 SFP uplinks**.
  - Support **Power over Ethernet (PoE)** for powering Access Points or IP Phones.

- **Cisco Catalyst 2960 Switches** (Access Layer):

Figure 4: Cisco Catalyst 2960 Switches

  - Connect end devices such as PCs, printers, and IoT nodes.
  - Include **24 Fast Ethernet ports** and **2 Gigabit uplinks**.
  - Fully support **VLAN segmentation** and **802.1Q trunking** for traffic isolation and reduced broadcast domains.

Firewall

Figure 5: Cisco ASA 5506-X Firewall

- The system uses a **Cisco ASA 5506-X Firewall** at the main site.
- Divides the network into **Inside**, **DMZ**, and **Outside** zones.
- Supports **IPsec VPN**, **NAT**, and **Deep Packet Inspection**.
- Provides throughput up to **250 Mbps** and handles more than **50,000 concurrent connections**.
- Serves as the **central gateway** for Internet access and inter-site VPN tunnels.

Wireless LAN Controller & Access Points

- **Cisco 3504 Wireless LAN Controller (WLC)**:

Figure 6: Cisco 3504 Wireless LAN Controller (WLC)

  - Manages up to **150 lightweight Access Points**.
  - Provides centralized configuration and **WPA2-Enterprise authentication**.

- **Cisco Aironet 3702i Lightweight Access Points**:

Figure 7: Cisco Aironet 3702i Lightweight Access Points

  - Support dual-band **2.4/5 GHz**, **IEEE 802.11ac Wave 2**, and **4x4 MIMO** technology.
  - Deliver high data rates and stable roaming for staff and guest users.

Server Infrastructure

- The main site hosts **10 servers** for Web, Mail, Database, DHCP/DNS, and Monitoring services.
- Each branch site includes **2 local servers** for storage and backup.
- All servers are directly connected to the Distribution Layer to ensure low latency and high security.

End Devices & IoT Systems

- The network supports approximately 1,100 end devices including workstations, servers, IoT sensors, PCs, laptops, IP cameras.
- User workstations connect to the Access Layer switches.
- IoT and surveillance systems are placed in dedicated VLANs for easier management and traffic control.

4.2 IP Addressing Plan

The addressing scheme follows a hierarchical pattern to ease management and future expansion. All Internet-bound traffic is routed through the Main Site as required by the assignment. Each VLAN uses a /24 subnet for simplicity; point-to-point WAN links use /30.

In this network design, each subnet follows a structured addressing convention rather than using the entire host range from `.1` to `.254` for dynamic allocation. This approach ensures manageability, avoids address conflicts, and allows future scalability. The address space within each /24 subnet is logically divided into segments according to function and administrative policy, as described below.

- **.1:** Reserved for the default gateway configured on the Layer-3 switch or router interface.
- **.2–.19:** Assigned to core infrastructure devices such as routers, firewalls, distribution switches, wireless controllers, and network monitoring servers. These static addresses are reserved permanently to prevent IP conflicts and to simplify troubleshooting.
- **.20–.200:** Allocated for dynamic IP assignment via DHCP. This range is used for regular user devices such as staff computers, laptops, and mobile clients.
- **.201–.239:** Reserved for semi-static devices that require predictable addressing but are not part of the core infrastructure, such as printers, IP cameras, and IP phones.
- **.240–.254:** Kept for testing, administrative access, and future expansion. This reserved range allows the network to integrate new devices or subnets without reconfiguring the existing DHCP scope.

4.2.1 Main Site – Building A

VLAN	Floor	Subnet (/24)	Gateway	Addressing Policy
VLAN10	Floor 1	10.10.10.0/24	10.10.10.1	10.10.10.20 → 10.10.10.200
VLAN20	Floor 2	10.10.20.0/24	10.10.20.1	10.10.20.20 → 10.10.20.200
VLAN30	Floor 3	10.10.30.0/24	10.10.30.1	10.10.30.20 → 10.10.30.200
VLAN40	Floor 4	10.10.40.0/24	10.10.40.1	10.10.40.20 →10.10.40.200
VLAN50	Floor 5	10.10.50.0/24	10.10.50.1	10.10.50.20 → 10.10.50.200
VLAN110	Guest Wi-Fi (A)	10.10.110.0/24	10.10.110.1	10.10.110.50 → 10.10.110.250; ACL blocks Guest→LAN
VLAN120	Cameras/IoT (A)	10.10.120.0/24	10.10.120.1	Static for cameras/sensors; DHCP for spares 10.10.120.100–150

Table 3: Addressing for Main Site – Building A

4.2.2 Main Site – Building B

VLAN	Floor	Subnet (/24)	Gateway	Addressing Policy
VLAN60	Floor 1	10.10.60.0/24	10.10.60.1	10.10.60.20 → 10.10.60.200
VLAN70	Floor 2	10.10.70.0/24	10.10.70.1	10.10.70.20 → 10.10.70.200
VLAN80	Floor 3	10.10.80.0/24	10.10.80.1	10.10.80.20 → 10.10.80.200
VLAN90	Floor 4	10.10.90.0/24	10.10.90.1	10.10.90.20 → 10.10.90.200
VLAN100	Floor 5	10.10.100.0/24	10.10.100.1	10.10.100.20 → 10.10.100.200
VLAN140	Guest Wi-Fi (B)	10.10.140.0/24	10.10.140.1	10.10.140.50 → 10.10.140.250; Guest→Internet only
VLAN150	Cameras/IoT (B)	10.10.150.0/24	10.10.150.1	Static for cameras/sensors; DHCP for spares 10.10.150.100–150

Table 4: Addressing for Main Site – Building B

4.2.3 Main Site – IT & Data Center Block (50m away)

VLAN	Service Zone	Subnet (/24)	Gateway	Addressing Policy
VLAN200	Server Farm (Internal Apps, DB, HIS/RIS/LIS)	10.10.200.0/24	10.10.200.1	Static for servers; DHCP reserved for admins
VLAN210	DMZ (Web, Mail, DNS)	10.10.210.0/24	10.10.210.1	Static; published via ASA policies/NAT
VLAN220	IT Ops/Monitoring	10.10.220.0/24	10.10.220.1	Static: NMS, Syslog, NetFlow, AAA, Backup
VLAN230	Voice (optional)	10.10.230.0/24	10.10.230.1	DHCP with option 150 (if IP phones used)
VLAN130	IT/Management (NMS, WLC, FW)	10.10.130.0/24	10.10.130.1	Static for infra (WLC, ASA, core/dist SVI, syslog/NTP)

Table 5: Addressing for Main Site – IT & Data Center

4.2.4 Branch 1 – Dien Bien Phu

VLAN	Zone / Floor	Subnet (/24)	Gateway	Addressing Policy
VLAN310	Floor 1 – IT/Local Services	10.20.10.0/24	10.20.10.1	Static for 2 local servers; DHCP for PCs: .50 → .200
VLAN320	Floor 2 – Staff Work Area	10.20.20.0/24	10.20.20.1	10.20.20.20 → 10.20.20.200
VLAN330	Guest Wi-Fi (Branch 1)	10.20.30.0/24	10.20.30.1	10.20.30.50 → 10.20.30.250; ACL Guest→Internet only
VLAN340	Cameras/IoT (Branch 1)	10.20.40.0/24	10.20.40.1	Static for cameras; DHCP for spares .150 → .200

Table 6: Addressing for Branch 1 – Dien Bien Phu

4.2.5 Branch 2 – Ba Huyen Thanh Quan

VLAN	Zone / Floor	Subnet (/24)	Gateway	Addressing Policy
VLAN410	Floor 1 – IT/Local Services	10.30.10.0/24	10.30.10.1	Static for 2 local servers; DHCP for PCs: .50–.200
VLAN420	Floor 2 – Staff Work Area	10.30.20.0/24	10.30.20.1	DHCP: 10.30.20.20–10.30.20.200
VLAN430	Guest Wi-Fi (Branch 2)	10.30.30.0/24	10.30.30.1	DHCP: 10.30.30.50–10.30.30.250; ACL Guest→Internet only
VLAN440	Cameras/IoT (Branch 2)	10.30.40.0/24	10.30.40.1	Static for cameras; DHCP for spares .150–.200

Table 7: Addressing for Branch 2 – Ba Huyen Thanh Quan

4.2.6 WAN, Internet, and Management Blocks

Purpose	Subnets	Notes
Main–Branch1 Leased Line	172.16.1.0/30 (CoreMS–CoreB1)	OSPF area 0
Main–Branch2 Leased Line	172.16.2.0/30 (CoreMS–CoreB2)	OSPF area 0
Internet xDSL (Main Site)	Public /30 (ISP 1) Public /30 (ISP 2)	Default route → ASA; PBR/track for failover/load-share
Loopbacks (routing/ID)	Main Core: 10.255.0.1/32 B1 Core: 10.255.0.11/32 B2 Core: 10.255.0.21/32	Used as OSPF router-IDs, NMS targets
Out-of-Band Management	10.254.0.0/24	Console servers, iDRAC/ILO, OOB switch

Table 8: WAN, Internet, and management addressing

Gateway/HSRP policy: All VLAN default gateways are configured on the Distribution layer (pair of L3 switches) using HSRP virtual IPs (e.g., `.1`) for high availability. DHCP scopes exclude the first 20 addresses for infrastructure and static reservations (printers, APs, UPS cards).

4.3 Schematic Physical Setup of the Network

The network follows the hierarchical structure with a clear separation of Core, Distribution, and Access layers.

- Each building has one Distribution Layer (2× L3 switches) connected redundantly to the Core routers using Gigabit Ethernet links.
- Each floor uses one Access Switch (Cisco 2960) connected via uplink (EtherChannel) to both Distribution switches.
- Lightweight Access Points are PoE-powered from Access switches and managed by the central WLC.

- All servers (Web, Mail, DB, DHCP/DNS) are hosted in the IT block and connected directly to the internal Distribution switches.
- The ASA Firewall separates Inside, DMZ, and Outside zones and connects to the dual xDSL modems for Internet access.

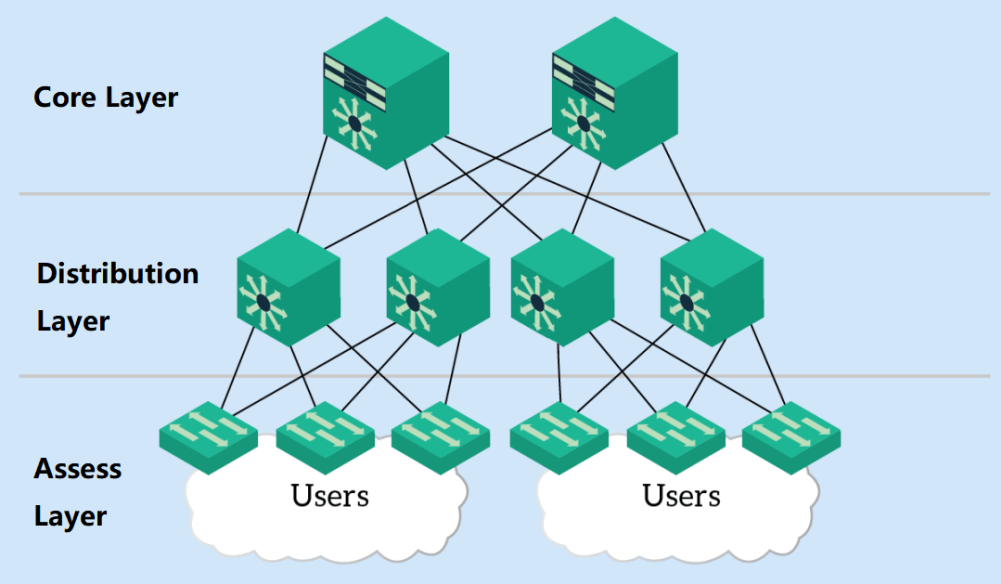

Figure 8: Schematic physical setup of the Main Site

4.4 WAN Connection Diagram Between Main Site and Auxiliary Sites

The Main Site connects to two branch offices (Dien Bien Phu and Ba Huyen Thanh Quan) using two leased lines implementing SD-WAN over OSPF routing. This ensures dynamic path selection, automatic failover, and optimized bandwidth utilization.

- Each branch is connected to the Main Site using one Serial links (Leased Lines) configured in **OSPF area 0**; traffic is naturally balanced because each branch uses its own dedicated leased line.
- **SD-WAN overlay** dynamically monitors link quality (latency, loss) and switches traffic when degradation is detected.
- **MPLS backbone** can be integrated in future for large-scale expansion.

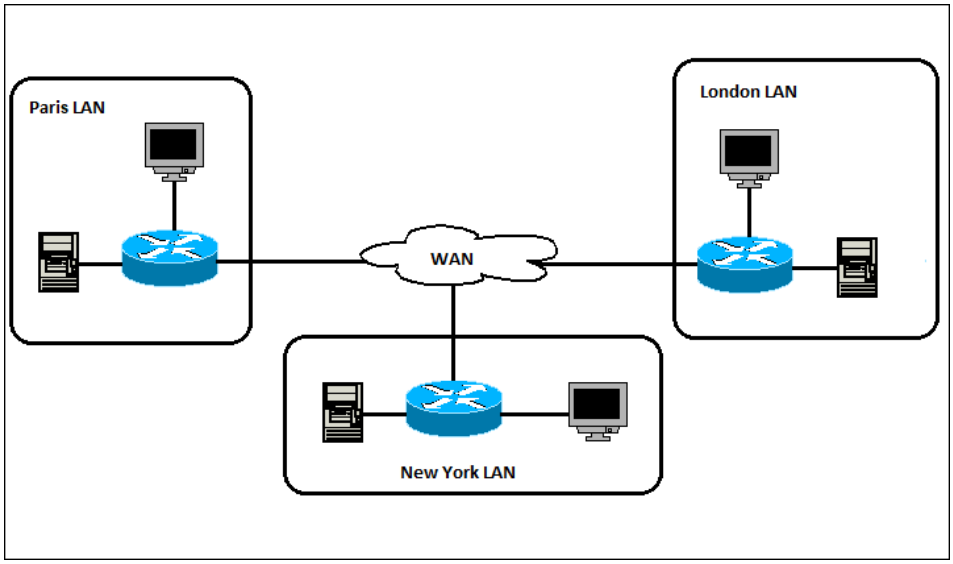

Figure 9: WAN connection between Main Site and two Branch Sites

Routing summary:

- OSPF is used as the internal routing protocol (Area 0 backbone).
- Each site advertises its local subnets to OSPF.
- Default route from Core router points to the Firewall ASA for Internet access.
- NAT is performed at the Firewall to hide internal addresses.

This topology provides high availability, simplified configuration, and scalable WAN integration suitable for future technologies such as MPLS and SD-WAN.

5 Throughput, Bandwidth calculation from ISP and configuration suggestion

5.1 Definition

Throughput is the actual amount of data successfully transmitted over the network per unit time (in Mbps).

Bandwidth is the maximum data transfer rate that a network link can handle per second—it represents the total capacity of the channel.

According to the assignment specification, 80% of network load occurs during two peak periods: **9:00–11:00 AM** and **3:00–4:00 PM** (a total of 3 hours). The hospital network includes 600 workstations, 10 servers, and approximately 100 WiFi users at the main site. Each auxiliary site hosts 60 workstations, 2 servers, and 50 WiFi users. The system is expected to grow by 20% within the next 5 years.

5.2 Throughput and Bandwidth Calculation

5.2.1 Main Site

Given:

- Servers: $10 \times (1000 + 2000) = 30{,}000$ MB/day
- Workstations: $600 \times (500 + 100) = 360{,}000$ MB/day
- WiFi users: $100 \times 500 = 50{,}000$ MB/day

Total daily traffic:

$$T = 30{,}000 + 360{,}000 + 50{,}000 = 440{,}000 \text{ MB/day}$$

Average throughput over 8 working hours:

$$\text{Throughput} = \frac{440{,}000}{8 \times 3600} = 15.27 \text{ MB/s} = 122.22 \text{ Mbps}$$

Peak bandwidth (80% of traffic in 3 hours):

$$\text{Bandwidth}_{\text{peak}} = \frac{440{,}000 \times 0.8}{3 \times 3600} = 32.59 \text{ MB/s} = 260.74 \text{ Mbps}$$

Accounting for 20% growth in 5 years:

$$\text{Bandwidth}_{\text{future}} = 260.74 \times 1.2 = 312.89 \text{ Mbps}$$

→ Required bandwidth at Main Site: approximately 313 Mbps.

5.2.2 Auxiliary Sites (DBP and BHTQ)

Given:

- Servers: $2 \times (1000 + 2000) = 6{,}000$ MB/day
- Workstations: $60 \times (500 + 100) = 36{,}000$ MB/day

- WiFi users: $50 \times 500 = 25{,}000$ MB/day

Total daily traffic:

$$T = 6{,}000 + 36{,}000 + 25{,}000 = 67{,}000 \text{ MB/day}$$

Average throughput:

$$\text{Throughput} = \frac{67{,}000}{8 \times 3600} = 2.33 \text{ MB/s} = 18.64 \text{ Mbps}$$

Peak bandwidth:

$$\text{Bandwidth}_{\text{peak}} = \frac{67{,}000 \times 0.8}{3 \times 3600} = 4.96 \text{ MB/s} = 39.73 \text{ Mbps}$$

Future projection (20% increase):

$$\text{Bandwidth}_{\text{future}} = 39.73 \times 1.2 = 47.68 \text{ Mbps}$$

→ Required bandwidth per Auxiliary Site: approximately 48 Mbps.

5.3 ISP Bandwidth Recommendation

Since all Internet traffic passes through the Main Site, the total required Internet capacity is:

$$\text{Total} = 312 + (2 \times 48) = 408 \text{ Mbps}$$

To ensure redundancy, high availability, and allow for burst traffic, the hospital should deploy two symmetric 300 Mbps GPON or Fiber Internet connections from separate ISPs (total 600 Mbps), configured with load balancing and automatic failover.

5.4 Summary

Table 9: Throughput and Bandwidth Summary

Location	**Avg. (Mbps)**	**Peak +20%**	**Provisioning**
Main Site	122	**313**	2×300 Mbps (Dual ISP)
Each Auxiliary Site	19	**48**	≥100 Mbps (MPLS / SD-WAN)
Total ISP Capacity	–	**≈410**	**600 Mbps (HA setup)**

Explanation:

- The total peak demand after growth is about **410 Mbps**.
- The main site needs around **313 Mbps**, so we use **two 300 Mbps Internet links**.
- This setup allows the network to keep running even if one link fails (called *failover*). In that case, one 300 Mbps line is still enough to keep core hospital systems working while traffic is balanced by QoS.
- Each auxiliary site connects at **100 Mbps or higher** through SD-WAN/MPLS for smooth communication with the main site.
- Choosing 600 Mbps total gives space for protocol overhead, VPNs, monitoring traffic, and future devices.

6 Design the network map using Packet Tracer

6.1 Core Infrastructure Implementation at the Main Site

This phase involved constructing the network's backbone, comprising the central routing, switching, and security devices.

6.1.1 Workspace Organization

The Packet Tracer workspace was logically divided into distinct areas representing the 'Data Center', 'Building A', and 'Building B' to ensure clarity and organization, as per the hospital's physical layout.

6.1.2 Core Device Deployment

Based on the equipment list, the following core devices were deployed into their respective zones:

- **Data Center:** Two **Cisco ISR 4331** routers were placed to serve as the Core/WAN routers. A **Cisco ASA 5506-X** firewall was implemented as the central security appliance. Two Layer-3 switches (e.g., **Catalyst 3650**) were deployed as the Core Switches.
- **Buildings A & B:** Two Layer-3 switches (e.g., **Catalyst 3650**) were deployed in each building to function as the Distribution Layer switches.

6.1.3 Physical Connectivity

High-speed and redundant links were established using **Copper Straight-Through** cables to adhere to the hierarchical design principles.

- Each Distribution Switch was cross-connected to both Core Switches to provide high availability.
- Core Switches were connected to the 'inside' interface of the ASA firewall.
- The firewall's 'outside' interface was connected to the Core Routers, which in turn connect to the WAN and Internet.
- **EtherChannel** was configured on inter-switch links to aggregate bandwidth and provide link redundancy, mitigating potential bottlenecks.

6.2 Basic Configuration and Network Segmentation (VLAN)

This phase established device identities and created logical network segments to enhance security and manage broadcast traffic.

6.2.1 Basic Device Configuration

All routers, switches, and firewalls were configured with unique hostnames and secured with console and enable passwords for administrative access control.

6.2.2 VLAN Creation

In accordance with the IP Addressing Plan, a comprehensive VLAN structure was created across all Core, Distribution, and Access switches. This segmentation separates traffic based on function and department. Key VLANs include:

- **User VLANs:** VLANs 10-50 for Building A floors, VLANs 60-100 for Building B floors.
- **Functional VLANs:** VLAN 200 for the internal 'Server Farm', VLAN 210 for the 'DMZ', and VLAN 110 for the 'Guest Wi-Fi' network.

6.2.3 Trunking Configuration

All inter-switch links were configured as 802.1Q trunks (`switchport mode trunk`). This is mandatory to allow traffic from multiple VLANs to traverse a single physical link, ensuring end-to-end VLAN connectivity.

6.3 Server and End-Device Deployment

This phase involved placing the servers and user workstations into their designated network segments.

6.3.1 Server Placement

- **DMZ Zone:** Public-facing servers (Web, Mail, external DNS) were connected to a dedicated switch which, in turn, was connected to a dedicated 'dmz' interface on the ASA firewall. This isolates them from the internal network, a critical security requirement.
- **Server Farm Zone (VLAN 200):** Mission-critical internal servers (Database, HIS/LIS, DHCP, ...) were connected to the Core Switches and assigned to the secure 'Server-Farm' VLAN.
- All servers were configured with static IP addresses as defined in the IP plan.

6.3.2 End-Device Placement

- Access Switches (e.g., **Catalyst 2960**) were deployed on each floor of Buildings A and B.
- PCs and laptops were placed in their respective departments and connected to these Access Switches.
- Each switchport connected to an end device was configured as an 'access' port and assigned to the correct VLAN (e.g., ports for the Cardiology department were assigned to VLAN 20).

6.4 Routing and Network Services Configuration

This phase enabled communication between different network segments and automated essential services.

6.4.1 Inter-VLAN Routing

Configured on the **Distribution Layer switches**. Switched Virtual Interfaces (SVIs) were created for each VLAN, assigned an IP address, and set as the default gateway for all devices within that VLAN. The `ip routing` command was enabled to activate Layer-3 functionality on these switches.

6.4.2 OSPF Dynamic Routing

The **OSPF** routing protocol was configured on all routers and Layer-3 switches within 'Area 0'. This allows for the automatic discovery and sharing of routes throughout the entire enterprise network, including across the WAN links to the branches, ensuring full network reachability.

6.4.3 DHCP Service

A dedicated server in the 'Server-Farm' was configured as the DHCP server. Separate IP pools were created for each user and guest VLAN. The `ip helper-address` command was configured on each SVI on the Distribution switches to forward broadcast DHCP requests from clients to the centralized DHCP server.

6.5 Branch Office and WAN Implementation

This phase extended the network to the two auxiliary sites, simulating a real-world enterprise WAN.

6.5.1 Branch Network Build

A smaller-scale network was built for each branch, consisting of a router, access switches, two servers, and end devices, following the VLAN and IP plan for that specific site. "Router-on-a-Stick" was used for inter-VLAN routing at the branches.

6.5.2 WAN Connectivity

- **Serial Modules (HWIC-2T)** were added to the Core routers and branch routers.
- **Serial DCE/DTE cables** were used to simulate the two private leased lines connecting each branch back to the main site, as required for high availability and load balancing.
- IP addresses from the '/30' WAN subnets were assigned to these serial interfaces. OSPF was enabled on these links to ensure seamless routing between the main site and the branches.

6.6 Wireless Network Configuration

The final implementation step was to deploy a centralized wireless network.

6.6.1 Device Deployment

A Wireless LAN Controller (WLC) was placed in the Data Center, and Lightweight Access Points (LWAP) were distributed across the floors of the main site.

6.6.2 WLC Configuration

The WLC was configured to manage all APs centrally.

- Logical interfaces were created and mapped to their respective VLANs.
- Two distinct SSIDs were created:
  - `StaffNet`: For internal employees, mapped to a trusted user VLAN and secured with **WPA2-Enterprise** for robust authentication.
  - `GuestNet`: For visitors, mapped to the isolated guest VLAN and secured with **WPA2-PSK**. An ACL was applied on the Distribution switch to ensure this network is completely isolated from the internal LAN and can only access the Internet.

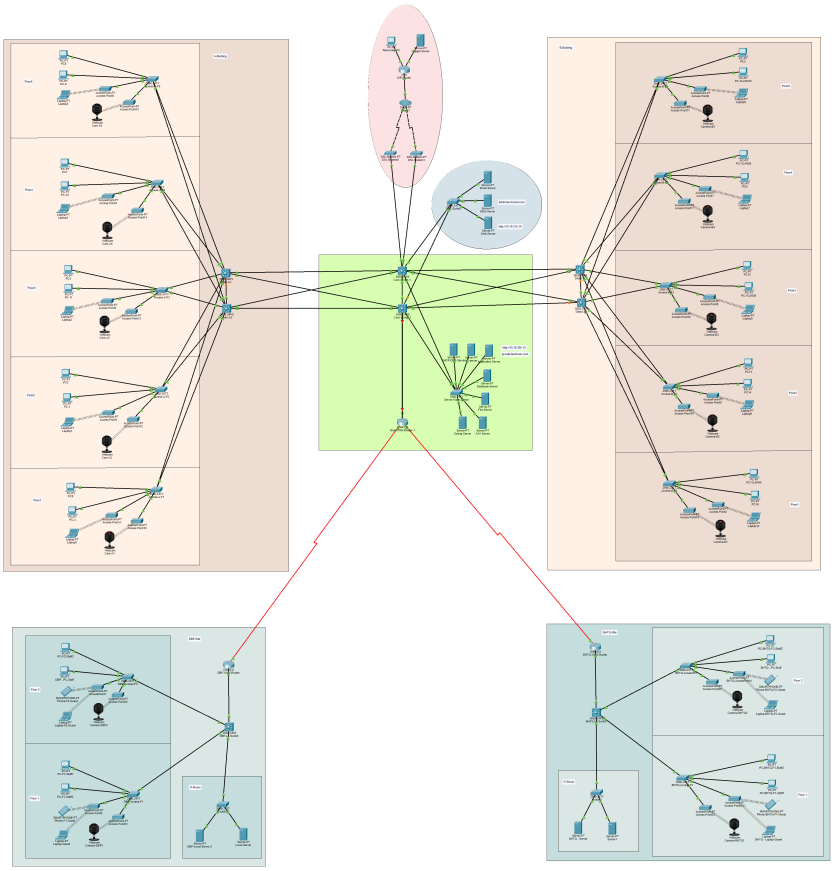

Figure 10: Overall hospital network topology

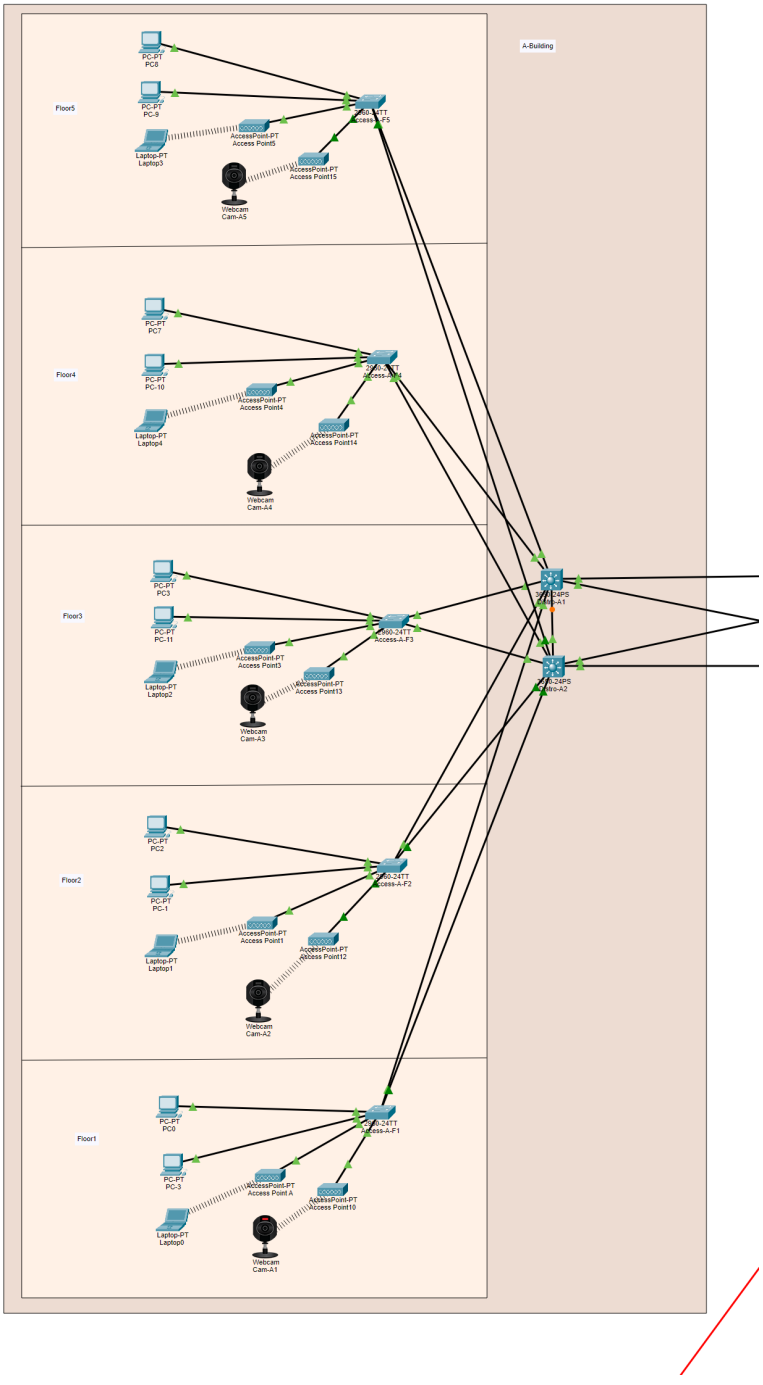

Figure 11: Network topology of Building A

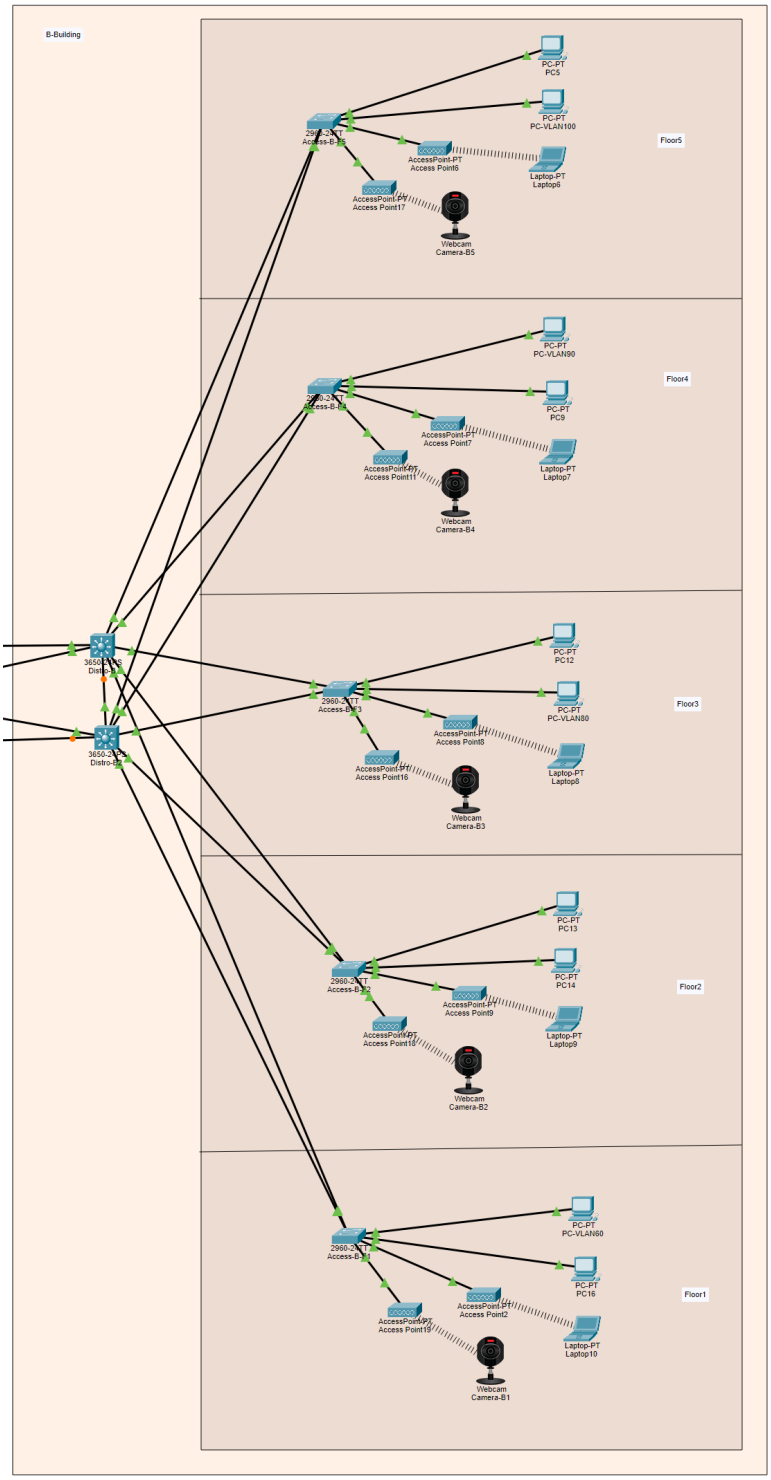

Figure 12: Network topology of Building B

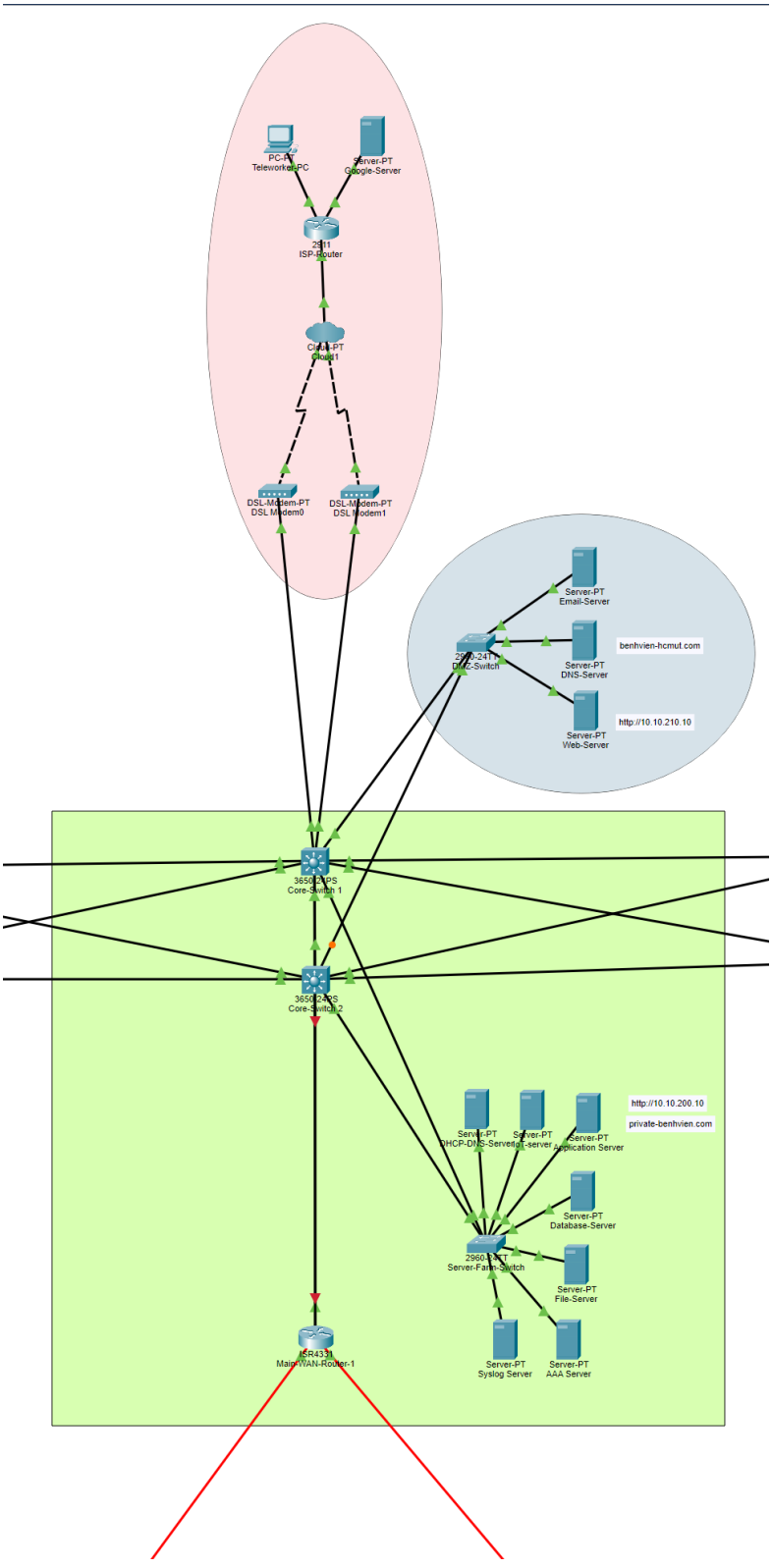

Figure 13: Network topology of Data Center, DMZ, and Internet

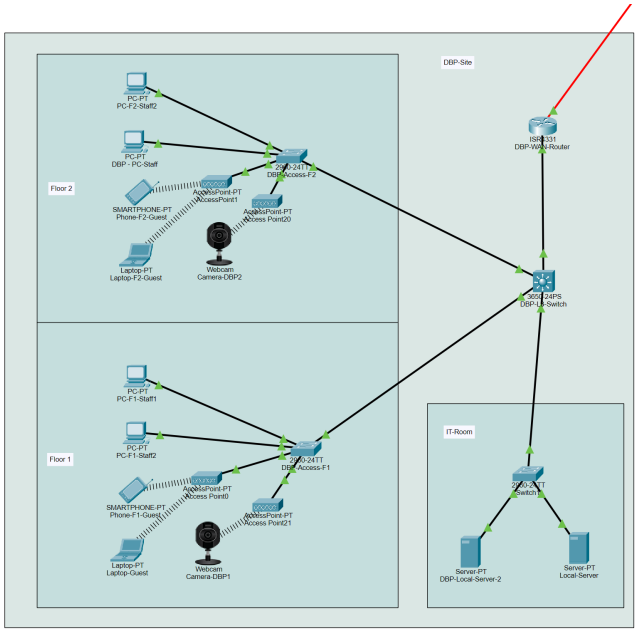

Figure 14: Network topology of DBP Branch Site

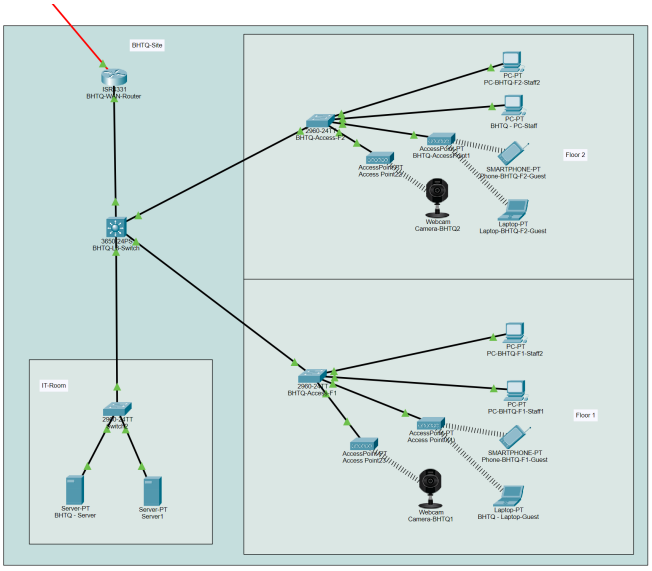

Figure 15: Network topology of BHTQ Branch Site

7 System Testing with popular tools on proposed system

This section documents the testing procedures performed on the simulated network in Cisco Packet Tracer. The goal is to verify that the implemented design meets all functional, connectivity, and security requirements as specified in the assignment brief. Each test case is designed to validate a specific aspect of the network, from basic local connectivity to complex, multi-site and security-enforced communications.

7.1 Intra-VLAN Connectivity Test

- **Objective:** To verify that devices within the same VLAN can communicate with each other, confirming that basic Layer 2 switching and VLAN port assignments are correct.
- **Methodology:**
  1. Two PCs were placed in Building A, Floor 1, and connected to the same Access Switch.
  2. Both PCs were configured to be in **VLAN 10**.
  3. A `ping` command was initiated from the first PC (e.g., IP `10.10.10.20`) to the second PC (e.g., IP `10.10.10.21`).
- **Expected Result:** A successful ping, with 0% packet loss.
- **Actual Result:** The ping was successful. The output displayed four replies from the destination PC, confirming reachability.

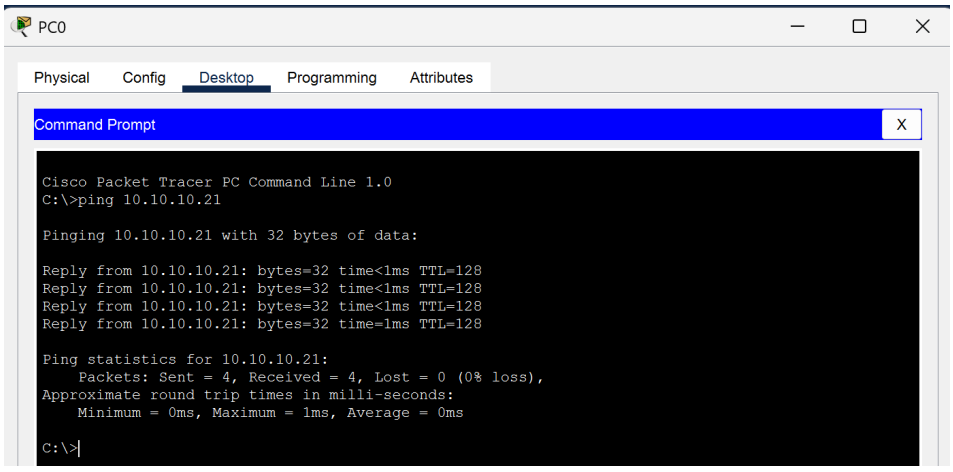

Figure 16: Ping result from 10.10.10.20 to 10.10.10.21

- **Analysis:** This successful test validates that the Access Layer switches are correctly configured and that port-to-VLAN assignments are functioning as designed.

7.2 Inter-VLAN Connectivity Test

- **Objective:** To verify that the Inter-VLAN routing configured on the Distribution Layer switches is functioning correctly, allowing communication between different departments/VLANs.

- **Methodology:**
  1. A `ping` command was initiated from a PC in **VLAN 10** (Building A, Floor 1, e.g., IP `10.10.10.21`).
  2. The destination was a PC in **VLAN 20** (Building A, Floor 2, e.g., IP `10.10.20.20`).
- **Expected Result:** A successful ping. The first packet might time out due to ARP resolution, but subsequent packets should succeed.
- **Actual Result:** The ping was successful, demonstrating that traffic was correctly routed from VLAN 10 to VLAN 20 via the Switched Virtual Interfaces (SVIs) on the Distribution Switch.

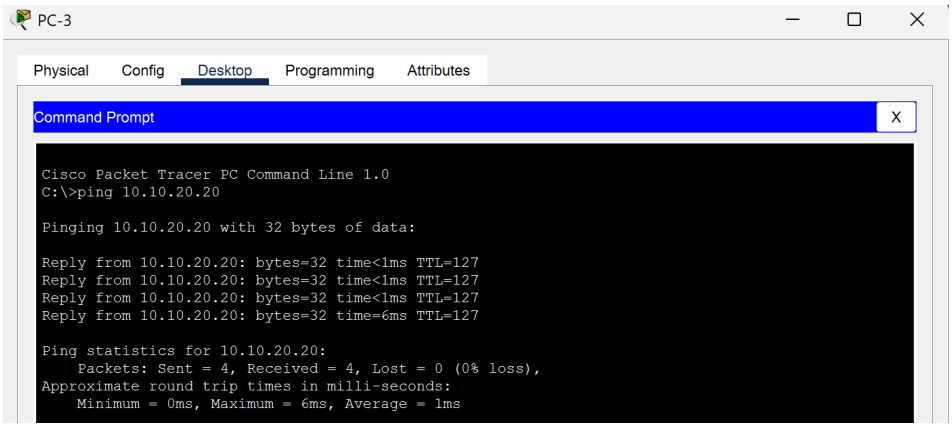

Figure 17: Ping result from 10.10.10.21 to 10.10.20.20

- **Analysis:** This confirms that the Layer 3 functionality of the Distribution switches is correctly configured and that OSPF is properly advertising these connected routes to the rest of the network.

7.3 WAN Connectivity Test

- **Objective:** To verify end-to-end connectivity between the Main Site and an Auxiliary Site, confirming that the WAN links and OSPF routing across the WAN are operational.
- **Methodology:**
  1. A `ping` command was initiated from a PC at the Main Site (e.g., VLAN 30, IP `10.10.30.20`).
  2. The destination was a PC at the DBP Branch (e.g., VLAN 320, IP `10.20.20.51`).
- **Expected Result:** A successful ping.
- **Actual Result:** The ping was successful. A `tracert` command confirmed that the packets were routed through the Core Router at the Main Site, across one of the serial WAN links, and to the Branch Router before reaching the destination PC.

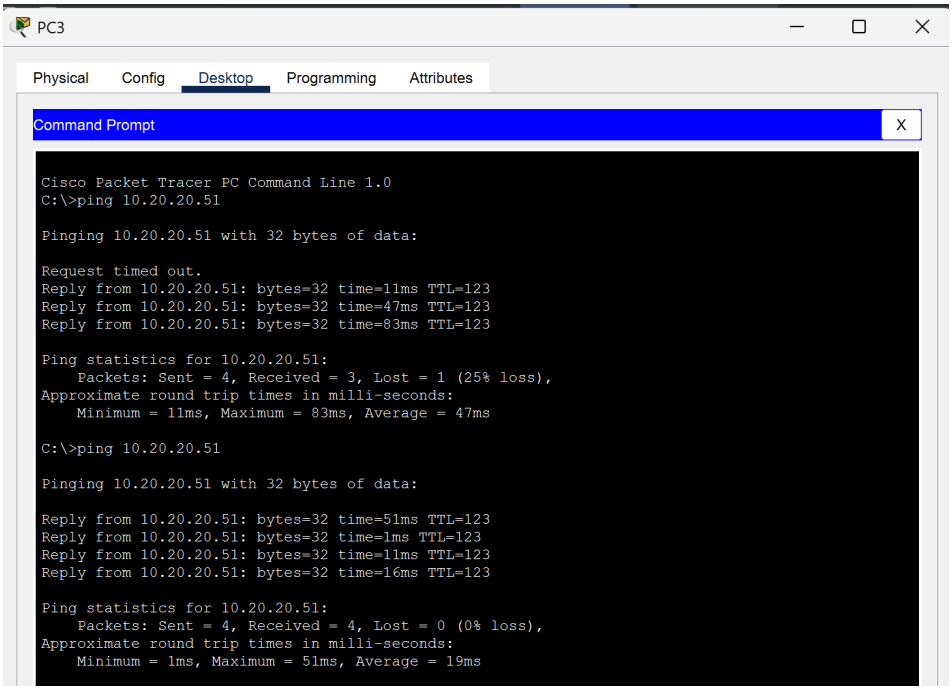

Figure 18: Ping result from 10.10.30.20 to 10.20.20.51

- **Analysis:** This test validates the entire routing infrastructure, including OSPF route advertisement across all sites and the proper configuration of the serial WAN interfaces.

7.4 DMZ Access Test

- **Objective:** To confirm that internal users can access public services hosted in the DMZ, while adhering to the firewall's security policies.
- **Methodology:**
  1. A `ping` command was initiated from a PC in the internal LAN ('inside' zone).
  2. The destination was the Web Server located in the **DMZ** ('dmz' zone, e.g., IP `10.10.210.10`).
- **Expected Result:** A successful ping.
- **Actual Result:** The ping was successful.

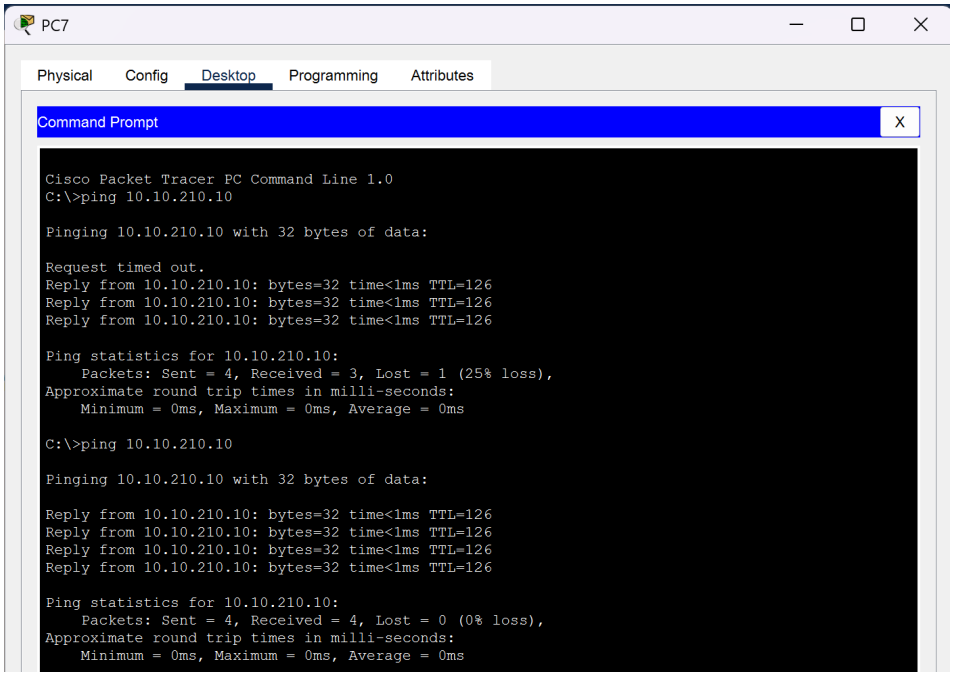

Figure 19: Ping result from 10.10.40.21 to Web Server 10.10.210.10

- **Analysis:** By default, the ASA firewall allows traffic to flow from a higher security level (‘inside‘, level 100) to a lower one (‘dmz‘, level 50). This result confirms the default security policy is in effect and that routing between the ‘inside‘ zone and the ‘dmz‘ zone is correct.

7.5 Intra-DMZ Connectivity

- **Objective:** To verify that servers located within the same security zone (DMZ) can communicate with each other, which is necessary for multi-tier applications.
- **Methodology:** A ‘ping‘ command was initiated from the Email Server (VLAN 210) to the Web Server (VLAN 210).
- **Expected Result:** Success (0% packet loss).
- **Actual Result:** The ping was successful.

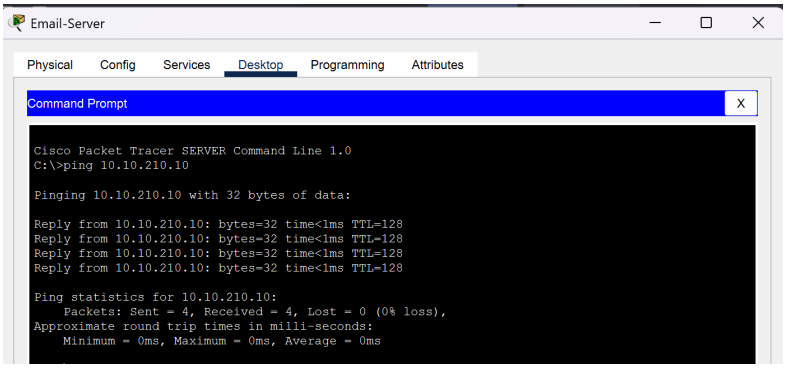

Figure 20: Ping result from Email Server 10.10.210.12 to Web Server 10.10.210.10

- **Analysis:** The result confirms that devices within the same VLAN and subnet have direct Layer 2 connectivity through the DMZ switch, and no firewall policies are blocking this internal communication.

7.6 Server-Farm Access Test

- **Objective:** To verify that authorized internal staff can access resources in the secure Server Farm.
- **Methodology:** A ‘ping‘ command was initiated from a staff PC in VLAN 20 to the Database Server in VLAN 200.
- **Expected Result:** Success (0% packet loss).
- **Actual Result:** The ping was successful.

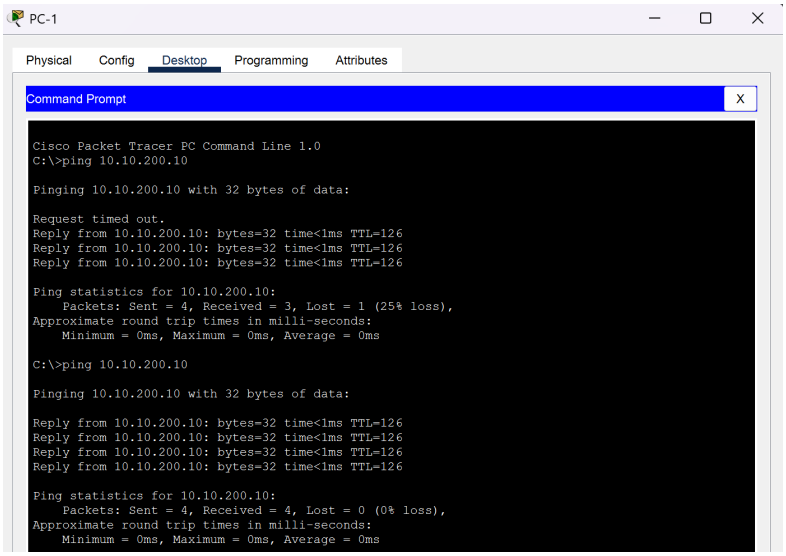

Figure 21: Ping result from PC 10.10.20.21 to Application Server 10.10.200.10

- **Analysis:** This result validates that Inter-VLAN routing is correctly forwarding traffic between user VLANs and the Server Farm VLAN, and that no internal ACLs are incorrectly blocking legitimate business traffic.

7.7 Intra-Server Farm Connectivity

- **Objective:** To verify that critical internal servers within the secure Server Farm (VLAN 200) can communicate with each other.
- **Methodology:** A 'ping' command was initiated from the Database Server (VLAN 200) to an Syslog Server (VLAN 200).
- **Expected Result:** Success (0% packet loss).
- **Actual Result:** The ping was successful.

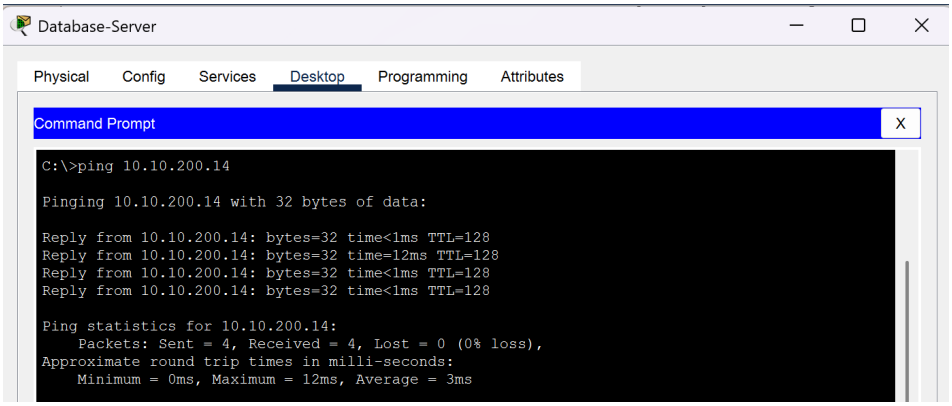

Figure 22: Ping result from Database Server 10.10.200.11 to Syslog Server 10.10.210.14

- **Analysis:** This confirms basic connectivity within the most secure internal zone, essential for application-to-database communication.

7.8 DMZ to Server Farm Security Test

- **Objective:** To verify basic Layer 3 reachability between the DMZ and the internal Server Farm, confirming that the underlying routing infrastructure is operational before applying security policies.
- **Methodology:** A 'ping' command was then initiated from the Web Server in the DMZ (VLAN 210) to the Database Server in the internal Server Farm (VLAN 200).
- **Expected Result:** The 'ping' **must succeed** with 0
- **Actual Result:** The 'ping' was successful.

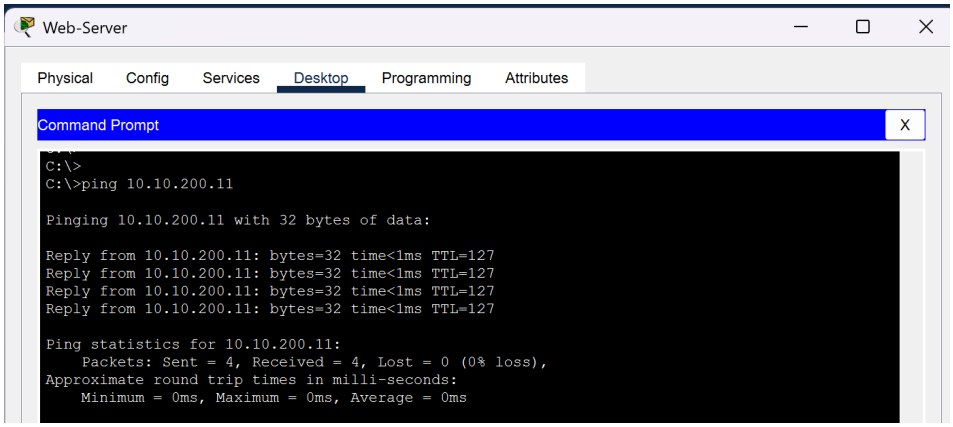

Figure 23: Ping result from Web Server 10.10.210.10 to Database Server 10.10.200.11

- **Analysis:** The successful result confirms that OSPF routing and Inter-VLAN configurations are functioning correctly, providing a valid path between the DMZ and Server Farm. This test isolates network connectivity from security policy enforcement, proving that the network's foundational routing is sound. Any subsequent blocking of this traffic path would be the intended result of the re-enabled security policies on the ASA firewall

7.9 Guest Network Isolation Test (Security Test)

- **Objective:** This is a critical security test to ensure that users on the guest Wi-Fi network are completely isolated from the internal hospital LAN, as required by the design.
- **Methodology:**
  1. A laptop was connected to the `GuestNet` **SSID**, receiving an IP address from the guest VLAN.
  2. A `ping` command was initiated from this laptop to a PC on the internal staff network.
- **Expected Result:** The ping must **fail**, with a 'Destination host unreachable' message.
- **Actual Result:** The ping failed as expected. All four packets were lost.

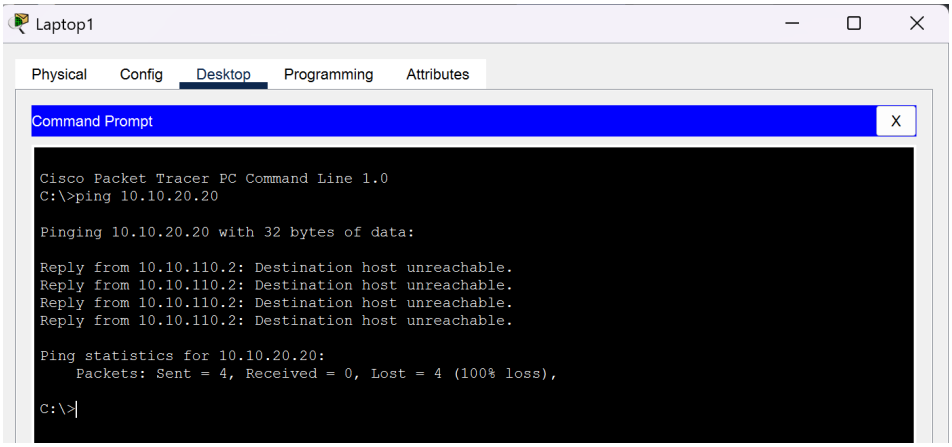

Figure 24: Ping result from 10.10.110.21 to 10.10.20.20

- **Analysis:** This successful failure confirms that the Access Control List (ACL) applied on the Distribution Switch (or Firewall) is correctly blocking traffic originating from the guest network destined for any internal network addresses, while still allowing it to reach the Internet.

7.10 Teleworker Remote Access via Internet Cloud

- **Objective:** To validate that a remote Teleworker PC located outside the hospital LAN can access internal resources through the simulated Internet cloud and ISP router, confirming the system's capability for remote work operations.
- **Methodology:**
  1. The Teleworker PC was assigned an IP address in the external network range (`192.168.10.x`) and connected to the hospital network via the **Internet Cloud** and **ISP Router**.
  2. The ISP Router was configured with proper static routes and NAT rules to forward packets toward the hospital's core switch.
  3. The Teleworker attempted to `ping` internal hosts and accessed the hospital's web interface using its private IP address.
- **Expected Result:** The Teleworker should be able to reach all tested internal IP addresses and successfully load the internal hospital webpage through the simulated public network.
- **Actual Result:** The Teleworker established stable connectivity to all internal devices. ICMP replies were received without loss, and the web application loaded successfully in the browser.

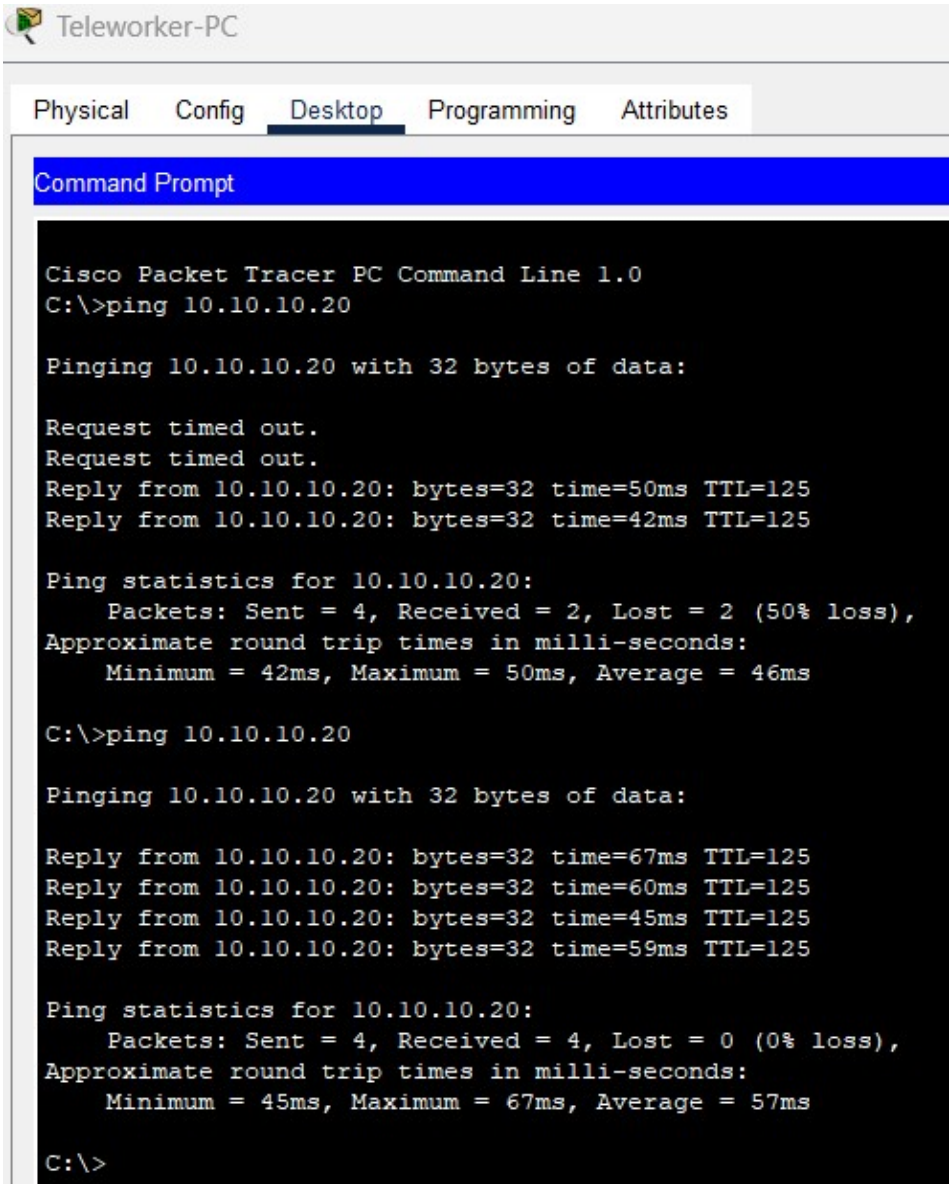

Figure 25: Successful ping and web access from the Teleworker PC to internal hospital devices through the Internet Cloud.

- **Analysis:** This test confirms that remote access to the hospital's internal network is fully functional through the configured Internet-ISP-Core route. Although no VPN encryption or firewall appliance is present, the topology effectively simulates a secure remote connection for teleworking scenarios. In a real deployment, a VPN or firewall-based security layer could be added to enhance encryption and authentication.

7.11 DMZ

7.11.1 Email system

Proceed to send and receive emails to test the email functionality.

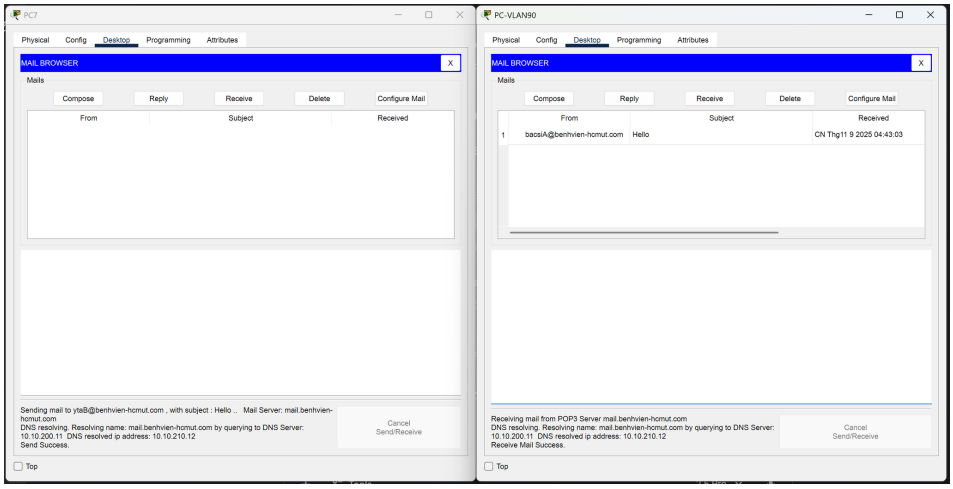

Figure 26: Access result from Email system

7.11.2 DNS server

The DNS server is configured with two **A Records** to resolve domain names within the hospital network:

- `benhvien-hcmut.com` → `10.10.210.10`
- `mail.benhvien-hcmut.com` → `10.10.210.12`

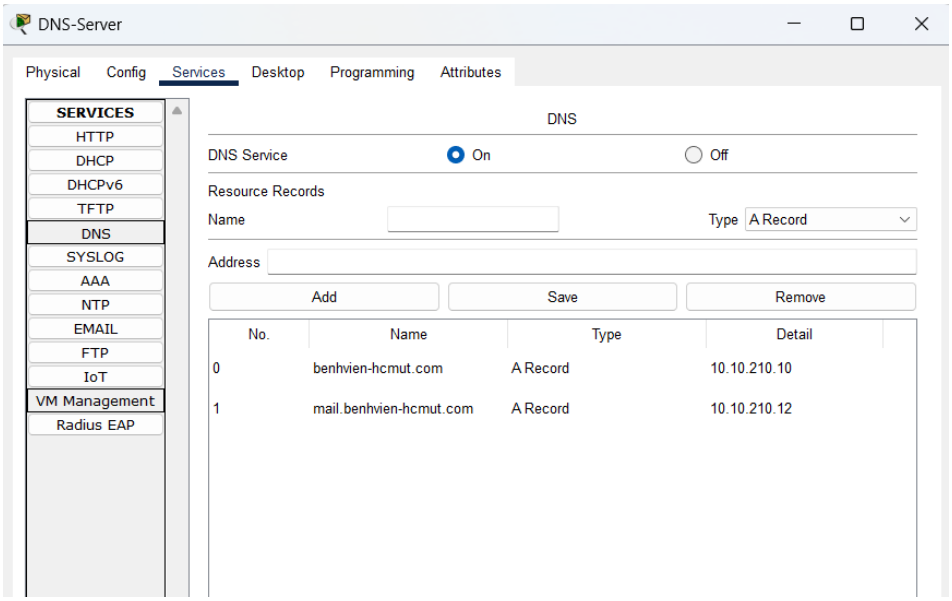

Figure 27: DNS system

7.11.3 Hospital Web system

The simulation demonstrates successful access to two hospital web systems:

- **Public Website:** `http://benhvien-hcmut.com` displays "Chao mung den voi Website Benh Vien H", representing the hospital's public site hosted in the DMZ zone.
- **Internal HIS System:** `http://10.10.200.10` displays "He Thong Quan Ly Benh An (HIS) – Noi Bo", accessible only within the internal network.

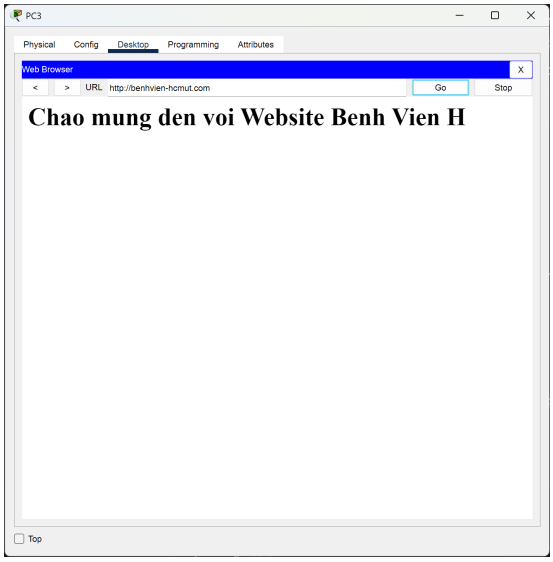

Figure 28: http://benhvien-hcmut.com

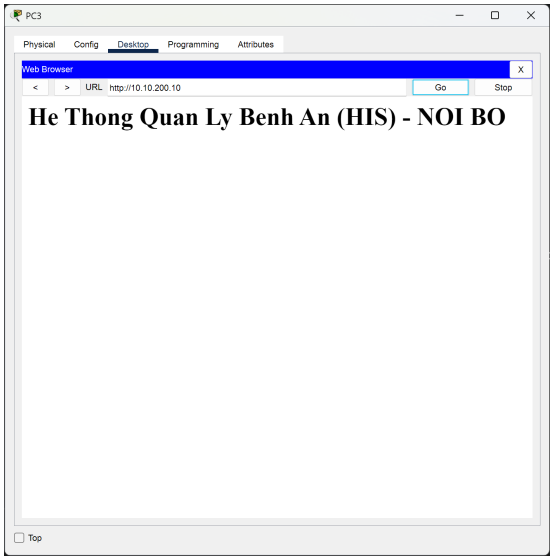

Figure 29: http://10.10.200.10

These results confirm the correct configuration of VLANs, routing, and server connectivity between the public and internal hospital networks, ensuring both external access and internal security.

7.12 Server farm

7.12.1 Camera System

Access to the camera management monitoring system (account and password: hcmut)

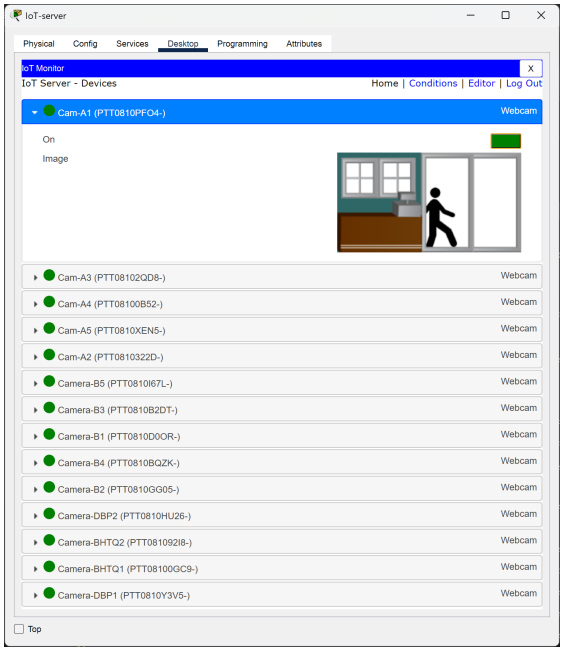

Figure 30: Access result from Camera system

7.12.2 Log system

The Syslog Server (`DBP-Syslog`) successfully receives log messages from the network device at `10.20.10.1`. The logs include system events such as interface state changes, indicating that network monitoring and event reporting functions are working correctly. This verifies that centralized logging is properly configured, allowing administrators to track network device activities in real time.

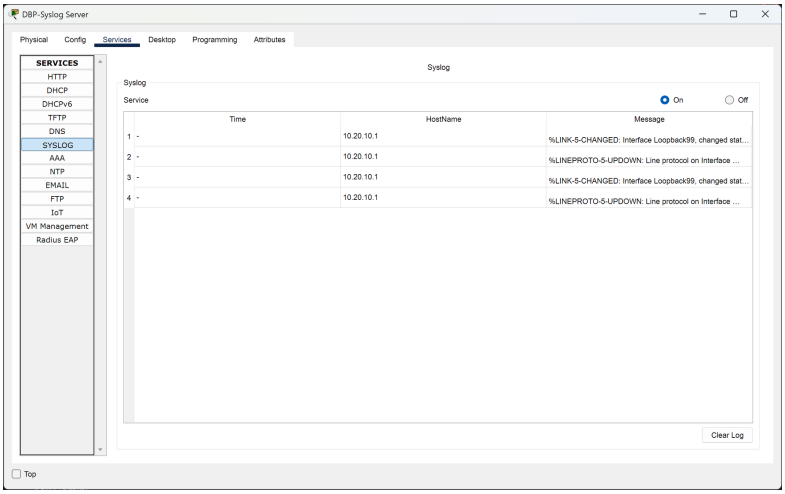

Figure 31: Access result from log system

7.12.3 File System

The figure shows that the client `PC-F1-Staff1` successfully connects to the FTP server at `10.20.10.50`. After entering the username `user_dbp` and password, the login is authenticated with the message "230 - Logged in" and the connection enters passive mode. This confirms that the FTP service is properly configured and accessible, enabling secure file exchange between internal users and the central server.

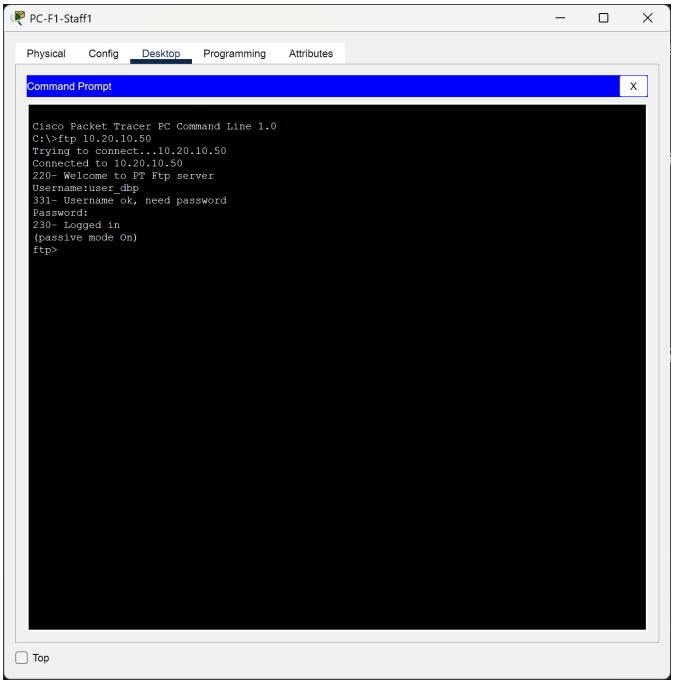

Figure 32: Access result from file system

8 System Evaluation

8.1 Complete structure of the system

The final implemented system is a robust, hierarchical, and multi-site network, adhering to modern design principles. The complete structure can be summarized as follows:

- **Hierarchical Architecture:** The network is built on a three-layer model (Core, Distribution, and Access). The Access Layer connects end-users via Cisco Catalyst 2960 switches. The Distribution Layer, using redundant Cisco Catalyst 3650 switches, aggregates traffic from the access layer and performs inter-VLAN routing. The Core Layer, powered by redundant Cisco ISR 4331 routers, provides high-speed backbone connectivity and serves as the gateway to the WAN and Internet.
- **Security Segmentation:** Security is enforced through a zone-based architecture managed by a central **Cisco ASA 5506-X Firewall**. The network is segmented into distinct zones:
  - An `inside` zone for the trusted internal LAN.
  - An `outside` zone for untrusted Internet traffic.
  - A `dmz` (Demilitarized Zone) for public-facing servers (Web, Mail), isolating them from the internal network.
  - A secure **Server Farm (VLAN 200)** for critical internal applications like HIS, LIS, and databases, protected behind the firewall.
- **Connectivity:**
  - **WAN:** The Main Site is connected to two auxiliary sites (DBP and BHTQ) via dual private **leased lines**, with **OSPF** configured to provide dynamic routing and load balancing (ECMP).
  - **Internet:** The Main Site has dual **xDSL Internet connections** configured for load balancing and high availability, ensuring continuous internet access.
- **Wireless Network:** A centralized wireless infrastructure is deployed using a **Cisco 3504 WLC** to manage all Lightweight Access Points (LWAPs). Two SSIDs are broadcast: `StaffNet` for employees with WPA2-Enterprise security, and `GuestNet` for visitors with WPA2-PSK, which is completely isolated from the internal network via ACLs.

8.2 Evaluation metrics

The designed system was evaluated against the key non-functional requirements specified in the project brief.

1. **High Availability (HA) / Reliability:**
   The system achieves a high degree of availability. This is demonstrated through device and link redundancy at every critical layer. The use of dual Core routers, dual Distribution switches per building with **HSRP** for gateway redundancy, **dual WAN links** to each branch, and **dual Internet connections** ensures that no single point of failure can disrupt the entire network's operation. **EtherChannel** further enhances link reliability between switches.

2. **Scalability:**
   The design is highly scalable. The hierarchical model allows for the easy addition of new floors or departments by simply adding an access switch and a new VLAN. The choice of a large private IP address space (`10.0.0.0/8`) provides ample room for future expansion. The modular nature of the core routers and the use of OSPF mean that new branches can be integrated with minimal reconfiguration. The design explicitly accounts for a **20% growth projection** over five years.

3. **Security:**
   A defense-in-depth security strategy has been successfully implemented. The **ASA Firewall** acts as the primary perimeter defense, while **VLANs** segment traffic internally, preventing unauthorized lateral movement. The **DMZ** effectively isolates public servers from the sensitive internal Server Farm. Furthermore, the `GuestNet` is isolated by **ACLs**, and the staff wireless network is secured with strong **WPA2-Enterprise** authentication, meeting the high-security demands of a hospital environment.

4. **Performance:**
   The network is designed for high performance. The use of **Gigabit Ethernet** and **Fiber** for all backbone links (Core-to-Distribution and Distribution-to-Access uplinks) prevents bottlenecks. **EtherChannel** link aggregation increases throughput on critical inter-switch connections. Load balancing on both Internet and WAN links ensures efficient use of available bandwidth and optimal traffic flow for data-intensive applications like PACS.

8.3 Remaining problems for the project

The implemented network system meets most of the assignment's requirements, However, several advanced features have not yet been realized due to simulation limitations:

- **Firewall Advanced Features:** The Cisco ASA Firewall has been deployed and integrated with the system, and Access Control Lists (ACLs) were successfully configured to control traffic between zones (Inside, DMZ, and Guest). However, **Intrusion Detection and Prevention Systems (IDS/IPS)** and advanced security monitoring have not been implemented. As a result, real-time threat detection and packet inspection could not be demonstrated.
- **VPN for Teleworkers:** The site-to-site VPN between the main site and the branch offices has been successfully implemented and verified. However, the **Remote Access VPN** feature for teleworkers remains unconfigured due to tool constraints, preventing off-site users from securely accessing internal hospital systems.
- **Security Logging and Monitoring:** While the Syslog system has been activated to collect basic event logs, a complete integration with centralized security analysis (e.g., attack alerts, firewall log correlation) has not yet been achieved.

8.4 Future development orientation

To enhance the network's security and operational capabilities, the following improvements are proposed:

1. **Deploy IDS/IPS for Deep Packet Inspection:** Integrate an Intrusion Detection/Prevention System into the ASA firewall or through a dedicated appliance to monitor, detect, and block malicious traffic in real time.

2. **Implement Remote Access VPN:** Extend the current VPN setup by enabling IPsec or SSL-based Remote Access VPN for teleworkers, allowing secure external connections to internal systems.
3. **Establish Centralized Security Management:** Deploy a Security Information and Event Management (SIEM) or Network Monitoring System (NMS) for unified log collection, correlation, and threat analysis.
4. **Apply Network Access Control (NAC):** Implement Cisco ISE or similar solutions to authenticate users and devices based on identity and compliance before network access.
5. **Upgrade to Next-Generation Wireless and WAN:** Transition to Wi-Fi 6/6E for higher throughput and better reliability. Implement SD-WAN to optimize WAN routing, bandwidth utilization, and branch site management.