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

ASSIGNMENT

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

CLASS: CC10-Group: 03

Instructor(s):	Nguyen Phuong Duy
Students:	Luu Thien Phuc - 2352936
	Nguyen Quang Linh - 2352679
	Hoang Khang Huy - 2352376
	Pham Minh Tuan - 2353265
	Nguyen Thanh Tai - 2353062
	Hoang Duc Hieu Anh - 2352030

HO CHI MINH CITY, DECEMBER 2025

List of Figures

List of Tables

Contents

1 Member List & Workload

No.	Fullname	Student ID	Workload
1	Luu Thien Phuc	2352936	100%
2	Nguyen Quang Linh	2352679	100%
3	Hoang Khang Huy	2352376	100%
4	Pham Minh Tuan	2353265	100%
5	Nguyen Thanh Tai	2353062	100%
6	Hoang Duc Hieu Anh	2352030	100%

Table 1: Team Member Workload Distribution

2 Suitable Network Structures and Requirement Analysis

2.1 Network System Requirements Analysis

2.1.1 Main Site

The Main Site includes:

- 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).
- 2xDSL 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 hospital LAN.
- Propose a surveillance camera system for the Company.

2.1.2 Auxiliary Sites

- The building has 2 floors, the first floor is equipped with 1 IT room and 1 Cabling Central Local.
- Small-scale: 260 workstations, 2 servers, 5 or more networking devices

2.1.3 Traffic and Workload

The dataflow and workload reach the peak about 80% in the periods of time from 9AM to 11AM and from 3PM to 4 PM can be shared for 3 Sites as below:

- Servers for software updates, web access, and database access,... The total download is about 1000 MB/day and the upload is estimated to be about 2000 MB/day.
- Each workstation is used for Web Browsing, document downloads, and customer transactions, ...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.

2.2 Installation Site Survey Checklist

Category	**Survey Item**	**Requirement/Standard**
Physical Layout	Distance to Data Center	Confirm distinct IT room is within 50m of Buildings A & B.
Cabling	Inter-building Connectivity	Verify pathway for Fiber (GPON) backbone between buildings.
Power & Cooling	Server Farm (Main Site)	Ensure redundant power and AC for 10 servers + 12 network devices.
Wireless	Signal Propagation	Check for walls/interference to ensure 100% coverage on all 5 floors.
Auxiliary Sites	IT Room Location	Verify space on the 1st Floor for the IT/Cabling room.
Security	Camera Placement	Identify blind spots for the surveillance system.

2.3 Identification of High Load Areas

In Computer Network, load balancing is a very important mechanism, which helps minimize the probability of overloaded or down network system. Connections between 2 auxiliary sites to the main site are the area with high load and this means we must consider load-balancing here. Also, DMZ with Web server and mail server will observe a high amount of connection. The reason is that the website of hospital is published to everyone, not only staff can access to this website but normal user inside LAN or in the Internet can access to it.

2.4 Network Structure Selection

The hospital's network is designed according to the 3-tier LAN Architecture, consisting of three layers: Access Layer, Distribution Layer, and Core Layer. This is a common model in large network systems, offering many benefits regarding management, performance, and scalability.

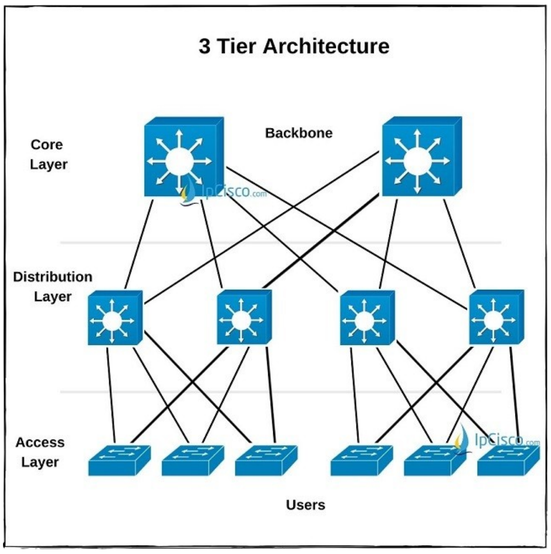


Figure 1: 3-tier Network Architecture

Reasons for Selection:

- **Hierarchical Management:** The division into 3 layers allows for centralized traffic management at the Core layer, aggregated processing at the Distribution layer, and user device deployment at the Access layer. This simplifies administration and troubleshooting.
- **Scalability:** The 3-tier LAN Architecture supports easy network expansion, from adding workstations at the Access Layer to upgrading devices at the Distribution or Core Layers.
- **High Performance:** Each layer in the architecture is designed to handle a specific type of traffic, helping to optimize resources and ensure high performance for the entire system.
- **Security and Flexibility:** It is easy to deploy security technologies (Firewall, IDS/IPS) and route traffic through layers to ensure safety and efficiency.

Advantages:

- **Clear Role Separation:** Each layer performs a specific task:
  - **Access Layer:** Connects end devices such as workstations, IP phones, and IoT devices.
  - **Distribution Layer:** Handles aggregated traffic from the Access Layer, performs inter-VLAN routing, and applies security policies.
  - **Core Layer:** Forwards traffic at high speed and ensures high availability.
- **High Availability:** Using redundancy protocols (such as HSRP, VRRP) and redundant links between layers helps reduce the risk of service interruption when errors occur.
- **Flexible Scalability:** This model is easily scalable both horizontally (adding devices at the Access Layer) and vertically (upgrading devices at the Core Layer).
- **High Performance Support:** The Core Layer is designed to process traffic at high speed, ensuring the network operates smoothly even during peak hours.
- **Easy Security Deployment:** The Distribution and Core layers provide centralized control points (Firewall, etc.) to implement security policies.

Disadvantages:

- **High Cost:** Requires investment in high-performance devices, especially at the Core and Distribution layers.
- **Complex Configuration:** VLAN configuration, inter-VLAN routing, and routing protocols require high professional knowledge from the network administration team.
- **Core Layer Bottleneck:** Traffic from the entire system passes through the Core layer. If an incident occurs here, the network can be seriously affected, but the risk has been mitigated by using redundant devices such as 2 Routers, 2 Firewalls, and 2 Layer 3 Switches.
- **Difficulty if Initial Core is Insufficient:** When traffic exceeds the processing capability of devices at the Core layer, upgrading can be complex and costly.

For the ”Critical Large Hospital” network, we have selected a Department-based VLAN strategy. In this model, VLANs correspond to organizational functions (e.g., Emergency, Pharmacy, Administration) regardless of where the user is physically sitting. This architectural choice is justified by the following key factors:

- **Data Isolation:** Hospital networks handle sensitive patient data (Electronic Health Records - EHR). A Department-based design ensures that a receptionist or a guest on Floor 1 cannot access the broadcast domain of the ”Finance” or ”Surgery” departments, even if they are sitting in the next room.

- **Access Control Policies:** It is much easier to write Firewall rules and Access Control Lists (ACLs) based on function. For example, you can write a single rule: ”Deny all traffic from VLAN 100 (Guest) to VLAN 50 (Pharmacy Database)”.

- **Roaming Capability:** In a hospital, doctors and nurses move between floors constantly (e.g., from the ER on Floor 1 to the Ward on Floor 3). With Department-based VLANs, a doctor's laptop can stay in the ”Medical Staff VLAN” wherever they plug in or connect via Wi-Fi, maintaining their access rights without reconfiguration.

- **Scalability:** If the ”Administration” department expands from Floor 4 to Floor 5, they simply use the same ”Administration VLAN” on the new switches. In a floor-based model, you would have to route traffic between ”Floor 4 Admin” and ”Floor 5 Admin,” creating unnecessary router overhead.

2.5 Security Partitions

Access Control List (ACL) is applied on Layer 3 switches to prevent customer's devices (devices using Wireless connection) from communicating to host devices of hospital. Therefore, customer's devices like Laptops or phones using WiFi can communicate to every other devices in case they also use WiFi. They can not connect to Hospital's PCs.

Firewall ASA is installed at the main site to ensure the security for the system and ACL is also configured here to decide whether to accept or drop packets from Internet. This Firewall separates the system into 3 partitions: DMZ Zone, Outside and Inside. Actually, there is one more partition, which is ServerFarm (place important server here) but we place this zone inside the IT block and we consider it as INSIDE ZONE.

3 Equipment List, IP Plan, and Diagrams

3.1 Recommended Equipment List

3.1.1 Cisco ISR 4331

Figure 2: Cisco ISR 4331 Router

Key Specifications:

- Ports: 3x Integrated Gigabit Ethernet (GE).
- Throughput: Scalable up to 2 Gbps (With Boost License).
- Expansions: 2 NIM slots and 1 SM slot.
- Memory:
  - Flash Memory: 4 GB (Default) / 16 GB (Max).
  - DRAM: 4 GB (Default) / 16 GB (Max)
- Advanced Features: Separated Control & Data Plane

Justification: The Cisco ISR 4331 is selected not as a luxury, but as a necessity to ensure the 'Robustness' and 'High Availability' mandated by the project requirements. It provides the necessary CPU overhead to handle encrypted VPN tunnels and complex ACLs without introducing latency to critical medical data.

3.1.2 Cisco Catalyst 3650-24PS-L

Figure 3: WS-C3650-24PS-L Catalyst 3650 Switch

Key Specifications:

- **Switching Capacity:** 88 Gbps (Easily handles our 509 Mbps peak load).
- **Forwarding Rate:** 41.66 Mpps.
- **PoE Power:** 390W (Sufficient for APs on the floor).

Justification: This Multilayer Switch handles Inter-VLAN routing at hardware speeds (10GbE capable). It supports PoE+ (Power over Ethernet), which is critical for powering the Wireless Access Points and IP Phones without extra electrical cabling.

3.1.3 Cisco Catalyst 2960-24TT-L

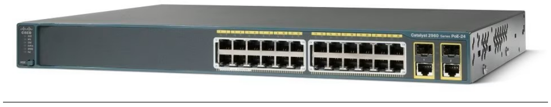


Figure 4: Cisco Catalyst 2960-24TT-L

Key Specifications:

- **Ports:** 24x 10/100 FastEthernet + 2x Gigabit Uplinks.
- **VLANs:** Supports up to 255 active VLANs.

Justification: A cost-effective Layer 2 switch for connecting workstations. It supports VLAN tagging (802.1Q) and Port Security features required to isolate departments (e.g., locking MAC addresses).

3.1.4 Cisco ASA 5506-X with FirePOWER Services

Figure 5: Cisco ASA 5506-X with FirePOWER Services

Key Specifications:

- **Throughput:** 750 Mbps Max (Matches our 509 Mbps requirement).
- **VPN:** Supports 50 IPsec VPN peers (Meets ”Site-to-Site” and ”Teleworker” specs).
- **Concurrent Sessions:** 20,000.

Justification: Explicitly requested in the assignment for ”High Security.” This device provides stateful firewall inspection, Intrusion Prevention System (IPS), and malware protection.

3.1.5 Cisco 3504 Wireless LAN Controller (WLC)

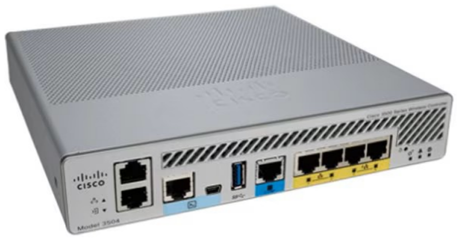


Figure 6: Cisco 3504 Wireless LAN Controller (WLC)

Justification: Essential for a "Critical Large Hospital." It allows centralized management of all Access Points, seamless roaming for doctors moving between floors, and creates separate "Staff" vs "Guest" SSIDs.

3.1.6 Cisco LAP-PT Lightweight Access Point1

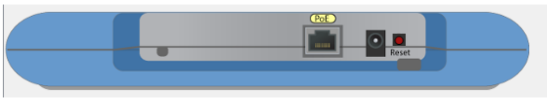


Figure 7: Cisco LAP-PT Lightweight Access Point1

Justification: In the simulation, LAP-PT Lightweight Access Point-1 is chosen to represent enterprise-grade Cisco Aironet lightweight APs. This model follows a controller-based architecture, where all WLAN configuration and security policies are centrally managed on the Cisco 3504 Wireless LAN Controller. Such a lightweight design is appropriate for a large hospital because it simplifies AP deployment, supports multiple SSIDs (Staff and Guest), enables fast roaming between access points, and allows consistent enforcement of security settings across all wireless coverage areas.

3.2 IP Addressing Plan

The IP addressing scheme for the hospital network follows a hierarchical, VLAN-based private IPv4 design. Each major department or functional block is mapped to a dedicated VLAN and IP subnet in order to:

- Isolate broadcast domains and improve performance and security.
- Simplify troubleshooting by keeping a clear mapping between VLAN ID and subnet.
- Reserve enough address space for at least 20% growth in the next few years.

IPv4 private address blocks are used for all internal VLANs, while a small public range is reserved for Internet-facing services and WAN connections. The detailed IP addressing information for each VLAN and site will be filled in later in the following tables.

3.3 Main Hospital Site

Table 2: IP Addressing Plan – Main Hospital Site - Building A

VLAN ID	VLAN / Department Name	Subnet	Default Gateway	Usable IP Range
10	**Management** (IT/NetAdmin)	192.168.10.0/24	192.168.10.1	192.168.10.2 – 192.168.10.254
20	**Administration** (HR, Finance)	192.168.20.0/24	192.168.20.1	192.168.20.2 – 192.168.20.254
30	**Medical Core** (Doctors, Nurses)	192.168.30.0/24	192.168.30.1	192.168.30.2 – 192.168.30.254
40	**Imaging** (Radiology, PACS)	192.168.40.0/24	192.168.40.1	192.168.40.2 – 192.168.40.254
50	**Pharmacy** (Inventory, Sales)	192.168.50.0/24	192.168.50.1	192.168.50.2 – 192.168.50.254
99	**Guest WiFi** (Patients/Visitors)	192.168.99.0/24	192.168.99.1	192.168.99.2 – 192.168.99.254
100	**Server Farm** (Internal: DNS, DHCP)	192.168.100.0/24	192.168.100.1	192.168.100.2 – 192.168.100.254
200	**IoT & Surveillance** (Cameras)	192.168.200.0/24	192.168.200.1	192.168.200.2 – 192.168.200.254
250	**DMZ** (Public Web/Email)	192.168.250.0/29	192.168.250.1	192.168.250.2 – 192.168.250.6

Table 3: IP Addressing Plan – Main Hospital Site - Building B

VLAN ID	VLAN / Department Name	Subnet	Default Gateway	Usable IP Range
110	**Cafeteria**	192.168.110.0/24	192.168.110.1	192.168.110.2 – 192.168.110.254
120	**Emergency**	192.168.120.0/24	192.168.120.1	192.168.120.2 – 192.168.120.254
130	**Laboratory**	192.168.130.0/24	192.168.130.1	192.168.130.2 – 192.168.130.254
140	**Clinic**	192.168.140.0/24	192.168.140.1	192.168.140.2 – 192.168.140.254
150	**Engineering**	192.168.150.0/24	192.168.150.1	192.168.150.2 – 192.168.150.254
160	**Guest WiFi** (Patients/Visitors)	192.168.160.0/24	192.168.160.1	192.168.160.2 – 192.168.160.254

3.3.1 Auxiliary Site 1 (DBP)

Table 4: IP Addressing Plan – Auxiliary Site 1 (DBP)

VLAN ID	Function	Subnet Address	Subnet Mask	Usable IP Range
10	**Staff LAN** (Mixed Departments)	172.16.10.0	/24	172.16.10.2 – .254
20	**Guest WiFi**	172.16.20.0	/24	172.16.20.2 – .254
30	**IoT/Surveillance**	172.16.30.0	/24	172.16.30.2 – .254
99	**Management/IT**	172.16.99.0	/24	172.16.99.2 – .254

3.3.2 Auxiliary Site 2 (BHTQ)

Table 5: IP Addressing Plan – Auxiliary Site 2 (BHTQ)

VLAN ID	Function	Subnet Address	Subnet Mask	Usable IP Range
10	**Staff LAN** (Mixed Departments)	172.16.50.0	/24	172.16.50.2 – .254
20	**Guest WiFi**	172.16.60.0	/24	172.16.60.2 – .254
30	**IoT/Surveillance**	172.16.70.0	/24	172.16.70.2 – .254
99	**Management/IT**	172.16.99.0	/24	172.16.99.2 – .254

3.3.3 WAN Connection Diagram (Site-to-Site)

Table 6: WAN Point-to-Point Links

Connection Description	Subnet Address	Subnet Mask	Router 1 IP (Main)	Router 2 IP (Remote)
Main Site DBP Site	10.0.0.0	/30 (255.255.255.252)	10.0.0.1	10.0.0.2
Main Site BHTQ Site	10.0.0.4	/30 (255.255.255.252)	10.0.0.5	10.0.0.6
ISP Link 1 (Leased Line)	203.0.113.0	/30 (255.255.255.252)	203.0.113.2	203.0.113.1 (ISP)
ISP Link 2 (DSL Backup)	203.0.113.4	/30 (255.255.255.252)	203.0.113.6	203.0.113.5 (ISP)

3.3.4 OSPF Router IDs (Loopback Interfaces)

To ensure stable OSPF elections, Loopback interfaces are configured on each router. These Loopback addresses are also used as the OSPF Router IDs.

- **Main Site Core Router:** 1.1.1.1 /32
- **DBP Site Router:** 2.2.2.2 /32
- **BHTQ Site Router:** 3.3.3.3 /32

4 Throughput Calculation and Configuration Suggestion

4.1 Traffic Analysis

- **Peak Hours:** 3 hours per day (9am-11am and 3pm-4pm) accounting for 80% of total load.
- **Server Load:** 1000 MB download + 2000 MB upload = 3000 MB/day/server.
- **Workstation Load:** 500 MB download + 100 MB upload = 600 MB/day/PC.
- **Wi-Fi Load:** 500 MB/day total for customer access.
- **Growth Factor:** 20% over 5 years.

4.2 Bandwidth Calculation

4.2.1 Main Site

- **Devices:** 600 Workstations, 10 Servers.
- **Server Traffic:** 10 servers × 3000 MB = 30,000 MB
- **Workstation Traffic:** 600 PCs × 600 MB = 360,000 MB
- **Wi-Fi Traffic:** 500 MB
- **Total Daily Data:** 390,500 MB
- **Required Bandwidth (Mbps):**

$$\frac{390,500\text{ MB} \times 0.8\text{ (Peak)}}{3\text{ hours} \times 3600\text{ sec}} \times 8\text{ bits} \approx \mathbf{231.41\ Mbps}$$

4.2.2 Auxiliary Sites

- **Devices:** 260 Workstations, 2 Servers.
- **Server Traffic:** 2 servers × 3000 MB = 6,000 MB
- **Workstation Traffic:** 260 PCs × 600 MB = 156,000 MB
- **Wi-Fi Traffic:** 500 MB (Estimated)
- **Total Daily Data:** 162,500 MB
- **Required Bandwidth (Mbps):**

$$\frac{162,500\text{ MB} \times 0.8}{3\text{ hours} \times 3600\text{ sec}} \times 8\text{ bits} \approx \mathbf{96.30\ Mbps}$$

4.2.3 Total Internet Link Requirement

Since ”All traffic to the Internet passes through the main site subnet”, the Main Site ISP link must handle the traffic of the Main Site plus both Auxiliary Sites.

- **Aggregate Bandwidth:** $231.41 + 96.30 + 96.30 = 424.01$ Mbps
- **Future Growth (20%):** $424.01 \times 1.2 \approx$ **508.81 Mbps**

Conclusion: The hospital requires a Leased Line / ISP connection of at least 550 Mbps or 600 Mbps to accommodate peak traffic and future growth.

4.3 Proposed Configuration

Based on the throughput analysis in Section 4.2 and the logical design in previous chapters, the following configuration is proposed to guarantee sufficient performance, scalability and security for the three-site hospital network.

Internet and WAN Edge

- Provision at least a ≥ 600 Mbps symmetric Internet link for the Main Hospital Site. This value is slightly above the calculated peak demand in order to leave headroom for bursts, routing overhead and future growth.
- Terminate the Internet link on the ASA firewall at the Main Site. The firewall performs NAT/PAT for all inside VLANs, enforces security policies and acts as the default route to the Internet.
- Use dedicated /30 point-to-point subnets on the serial links between the Main Site router and the DBP/BHTQ routers, as defined in the WAN addressing plan. Each WAN link should be provisioned at ≥ 100 Mbps to comfortably carry inter-site traffic, backup traffic and control-plane overhead.

Core and Distribution Layer

- Deploy the ISR 4331 router at the Main Site as the central WAN router, connected upstream to the firewall and downstream to the core/distribution switch (Cisco 3650).
- Use the 3650 distribution switch as a Layer–3 switch: it terminates all VLAN SVI interfaces for the Main Site, performs inter-VLAN routing and provides a single summarised default route towards the firewall.
- Trunk links between the 3650 and all access switches should run at 1 Gbps using 802.1Q tagging. Where possible, use EtherChannel bundles for additional bandwidth and redundancy.

Access Layer and VLAN Design

- Each floor/department is served by 2960 access switches. Access ports are configured as access mode and assigned to the appropriate VLAN (Medical, Imaging, Pharmacy, Staff LAN, Guest WiFi, IoT/Surveillance, Management/IT, Servers, etc.).
- Inter-VLAN routing is done centrally on the distribution switch. Default gateways for hosts are the corresponding SVI addresses on the 3650.
- DHCP services are placed on dedicated DHCP servers at each site; the distribution router/switch is configured with `ip helper-address` on each SVI so that DHCP requests can reach the correct server.
- VLAN IDs and IP subnets follow the addressing tables defined in Section 3, ensuring non-overlapping ranges per site and easy summarisation at the core.

Dynamic Routing and Summarisation

- EIGRP (or another IGP chosen in the design) is enabled between the Main Site router, the DBP router and the BHTQ router. All LAN subnets are advertised via the distribution/core devices to their local router.
- At the Main Site, LAN prefixes are summarised towards the remote sites, and each remote site also advertises a summary of its local VLANs. This reduces routing table size, speeds up convergence and improves scalability.

- A default route is injected from the Main Site towards DBP and BHTQ so that auxiliary sites use the Main Site's firewall as their Internet exit.

Wireless and Mobility

- Each site uses LAP-PT Lightweight Access Points controlled by a central Wireless LAN Controller (WLC).
- SSIDs are mapped to existing VLANs (e.g., Staff-WiFi → Staff VLAN, Guest-WiFi → Guest VLAN, IoT-WiFi → IoT VLAN).
- For Guest WiFi, client traffic is placed in an isolated VLAN with restricted access (only to the Internet and specific public services) via ACLs on the distribution switch and firewall.

Security and Policy Enforcement

- The ASA firewall enforces zone-based policies: Inside (hospital LANs), DMZ (public-facing servers) and Outside (Internet). Only required services (HTTPS, VPN, DNS, NTP, etc.) are allowed between zones.
- On internal switches, port-security, BPDU guard, DHCP snooping and dynamic ARP inspection are enabled to mitigate common Layer–2 attacks.
- Access Control Lists (ACLs) on the distribution switch restrict communication between sensitive VLANs: for example, IoT/Surveillance devices cannot directly reach administrative systems; Guest VLAN cannot reach internal servers; Management VLAN has SSH/Telnet/SNMP access to infrastructure devices only.

Quality of Service (QoS)

- Traffic classes are defined to prioritise critical clinical applications (e.g., medical imaging transfers, VoIP between departments, remote consultations) over best-effort traffic such as web browsing.
- At the access layer, DSCP markings from trusted endpoints (IP phones, imaging servers) are preserved; other traffic is remarked at the distribution layer.
- WAN links implement LLQ/CBWFQ so that voice and real-time traffic receive guaranteed bandwidth during congestion, while bulk data transfers use remaining capacity.

High Availability and Future Growth

- Redundant uplinks are provided wherever possible (e.g., distribution switch to firewall and router) with fast convergence mechanisms such as link-state tracking and EIGRP fast hellos.
- The chosen IP addressing scheme reserves unused subnets within each site's block so that new VLANs or departments can be added without redesigning the whole network.
- If Internet demand grows beyond current estimates, an additional ISP link can be added and either load-balanced (Policy-Based Routing / ECMP) or used as a failover path.

This proposed configuration aligns the physical topology, logical IP/VLAN design and security mechanisms with the throughput calculations, ensuring that the hospital network can reliably support daily operations and future expansion.

5 Network Design Simulation (Packet Tracer)

5.1 Topology Implementation

5.1.1 System Overview

The designed hospital network is divided into the following components:

- **Main Hospital Site (Ho Chi Minh City):**
  - Consists of two clinical buildings (A and B) with five floors each; each floor contains consultation rooms, wards, pharmacies and imaging departments with approximately 600 wired workstations and medical devices in total.
  - A separate Data Center / IT room and Cabling Central Local (patch–panel area) is located in an adjacent building about 50 meters away from the clinical blocks; this room hosts the core switches, servers and security devices of the hospital.
  - All inter–departmental connectivity inside the Main Site is organised using VLANs for medical, administrative, guest and IoT/surveillance traffic.
- **Auxiliary Sites (DBP Campus and BHTQ Campus):**
  - Each auxiliary site contains a two–floor building with an IT room and a local Cabling Central Local on the first floor.
  - Each site supports roughly 260 wired workstations and local services (IoT / DHCP servers, wireless APs) for outpatient clinics and satellite offices.
  - Both auxiliary sites are connected back to the Main Hospital Site by dedicated leased lines, forming a hub–and–spoke topology with the Main Site as the hub.
- **Internet Connectivity:**
  - The Main Hospital Site connects to the Internet via two independent DSL links terminated on the firewall and edge routers.
  - A per–packet (or per–session) load–balancing mechanism is applied so that outgoing traffic is distributed across the two DSL lines, increasing available bandwidth and providing redundancy.
  - All Internet traffic from the Auxiliary Sites is backhauled through the WAN links to the Main Site and exits through these two DSL connections; there is no direct Internet breakout at the Auxiliary Sites.

The Main Hospital Site itself is further divided into several logical network segments:

1. **DMZ and Server Farm Zone:**
   - Located in the Data Center on the ground floor, separated from the internal LAN by the firewall.
   - Hosts critical shared services with static IP addresses, such as:
     - hospital information systems (HIS, LIS, RIS/PACS),
     - database and application servers,
     - public web portal and VPN gateway for teleworkers.
   - Servers in this zone can be accessed from internal departments and, in a controlled manner, from the Internet for remote services.

2. **Wireless Access Point Zone:**

   - Also concentrated around the ground floor and vertical shafts, where controller–based lightweight access points are connected to the cable risers.
   - Provides Wi–Fi coverage for all floors of Buildings A and B and the outpatient areas, supporting Staff, Guest and IoT SSIDs.
   - Wireless traffic is tunnelled back to the wireless controller and then bridged into the appropriate VLANs in the internal network.

3. **Internal Clinical and Administrative Zone:**

   - Spans all floors of Buildings A and B and is interconnected through a multilayer core/distribution switch in the Data Center.
   - Protected from the Internet by a firewall and from the DMZ by strictly filtered access lists.
   - **Clinical floors (wards, imaging, pharmacy):**
     - Each floor includes at least one access switch to connect wired workstations, medical devices and VoIP phones using department–specific VLANs (Medical, Imaging, Pharmacy, Staff).
     - Each floor also has one or more wireless access points for doctors' and nurses' mobile devices and for patient Wi–Fi.
   - **IT and Management areas:**
     - Contain the management workstations, network monitoring systems and backup devices in a dedicated Management VLAN.
     - Provide out–of–band access to network devices (routers, switches, firewalls and servers) for configuration and troubleshooting.

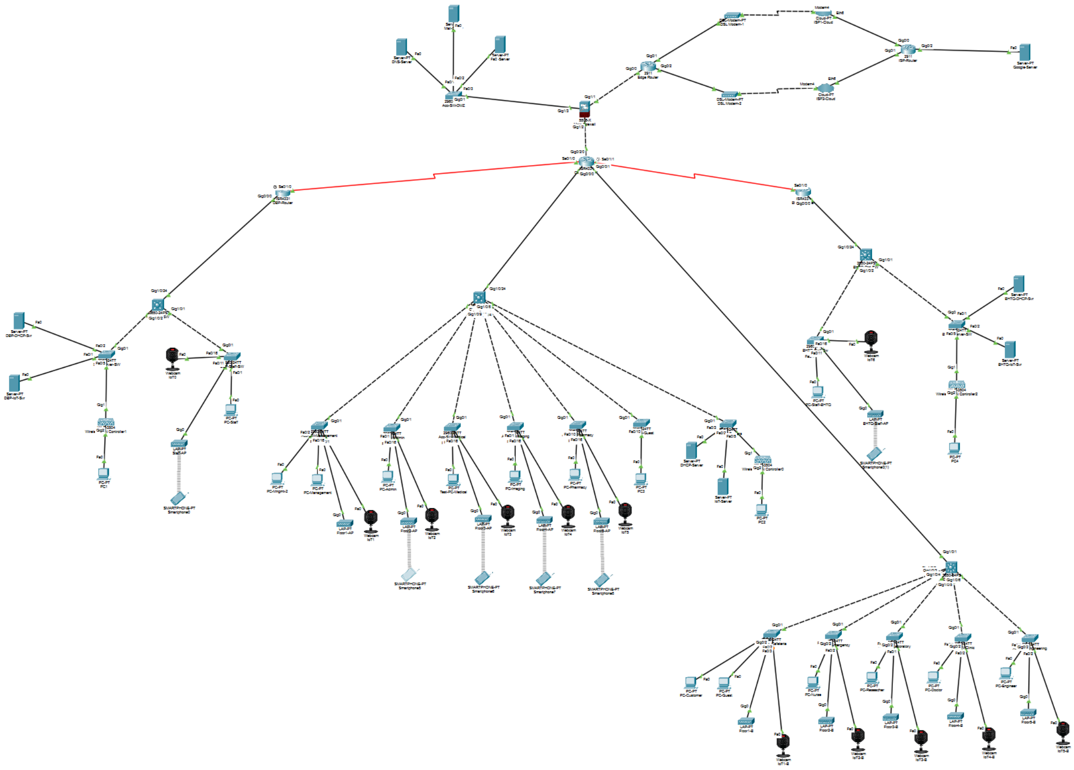


Figure 8: Logical Connection Diagram

5.1.2 Main Hospital Site - Building A

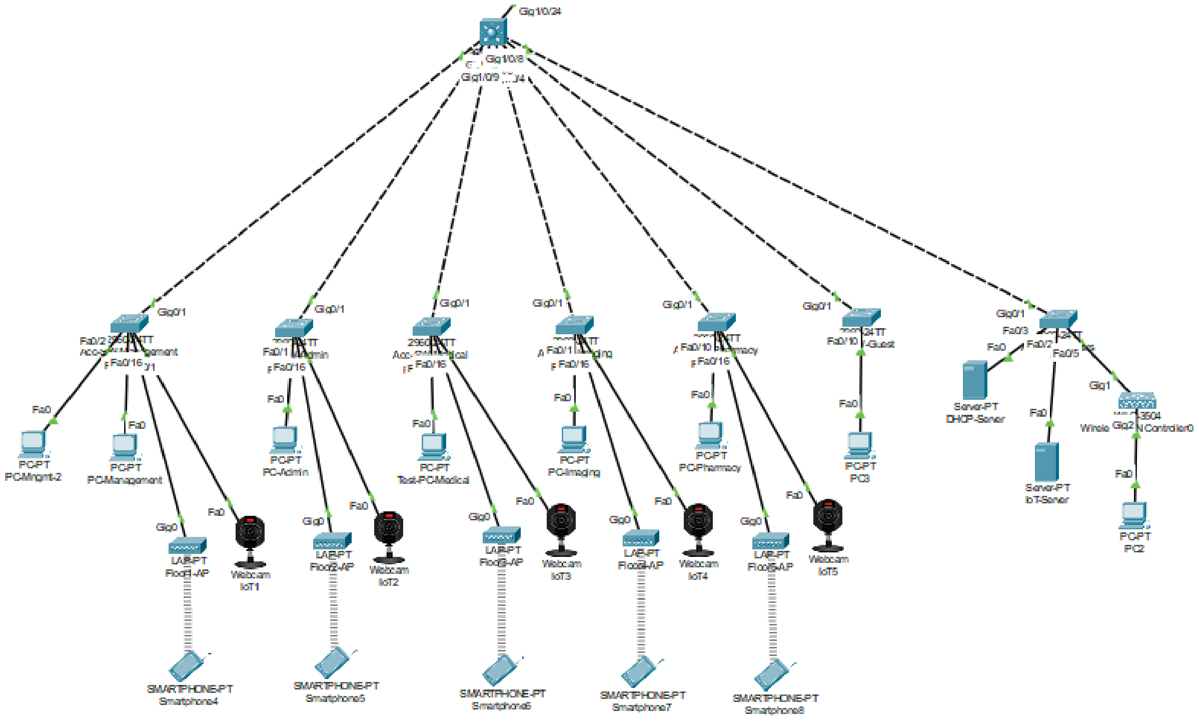


Figure 9: Main Hospital Site - Building A

5.1.3 Main Hospital Site - Building B

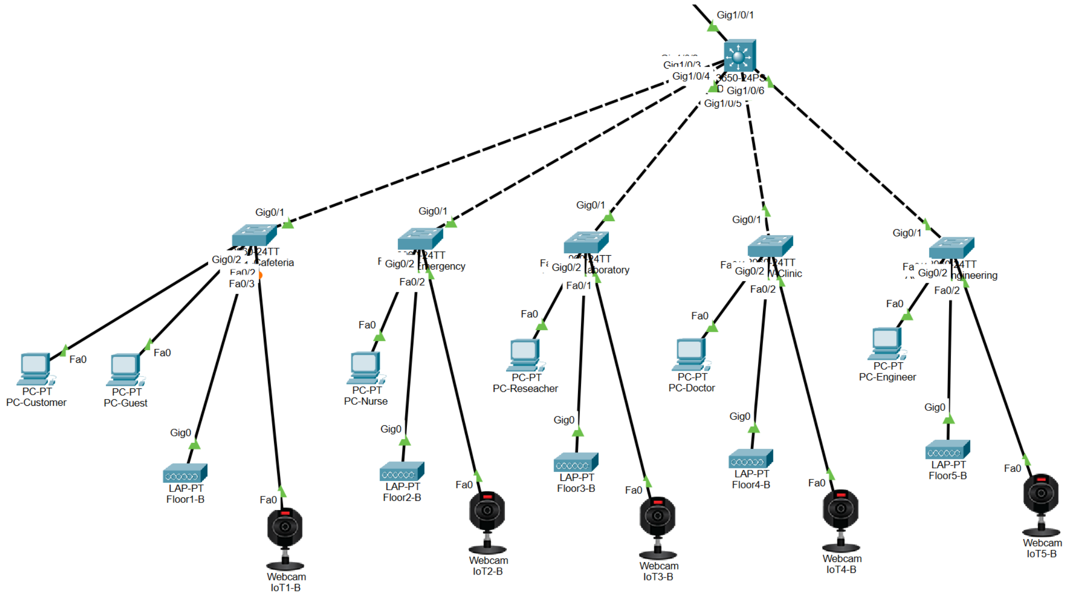


Figure 10: Main Hospital Site - Building B

5.1.4 DBP Site

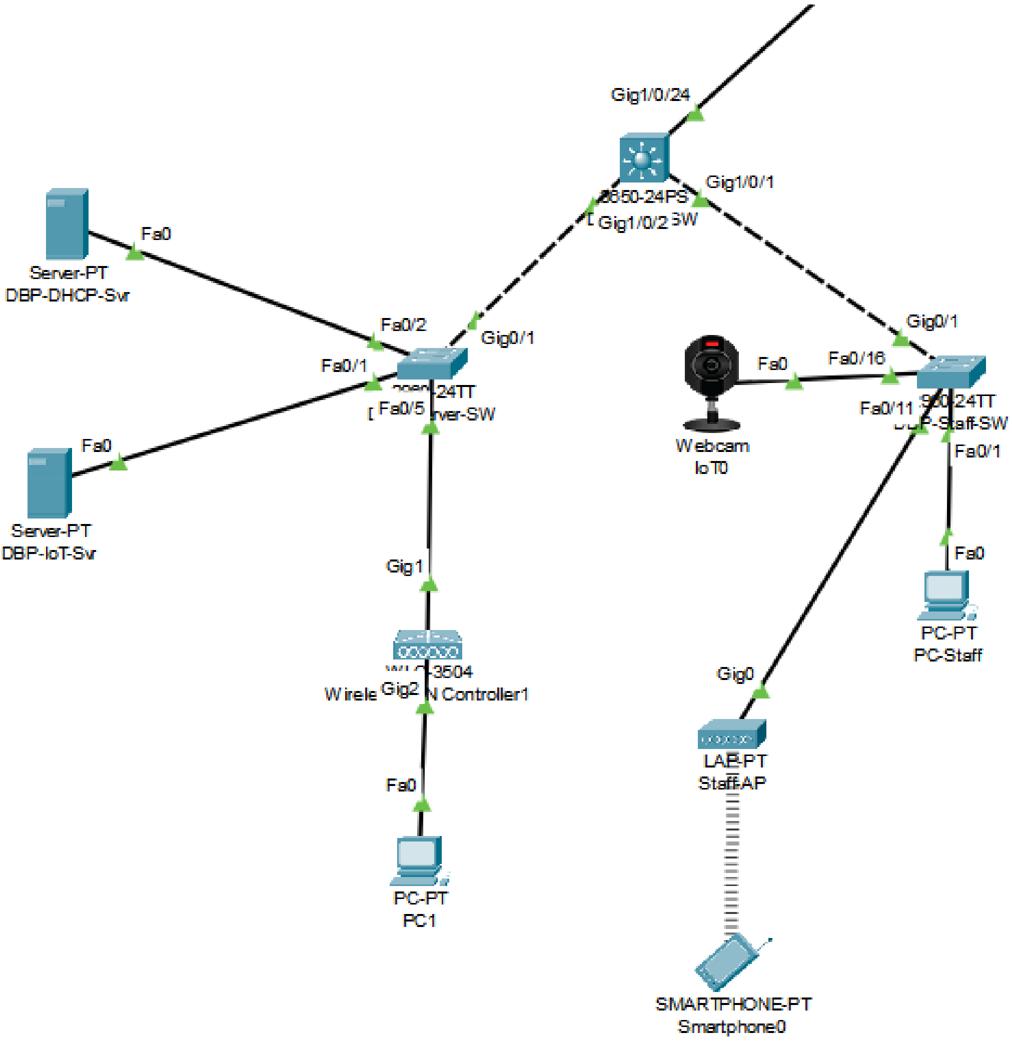


Figure 11: DBP Site

5.1.5 BHTQ Site

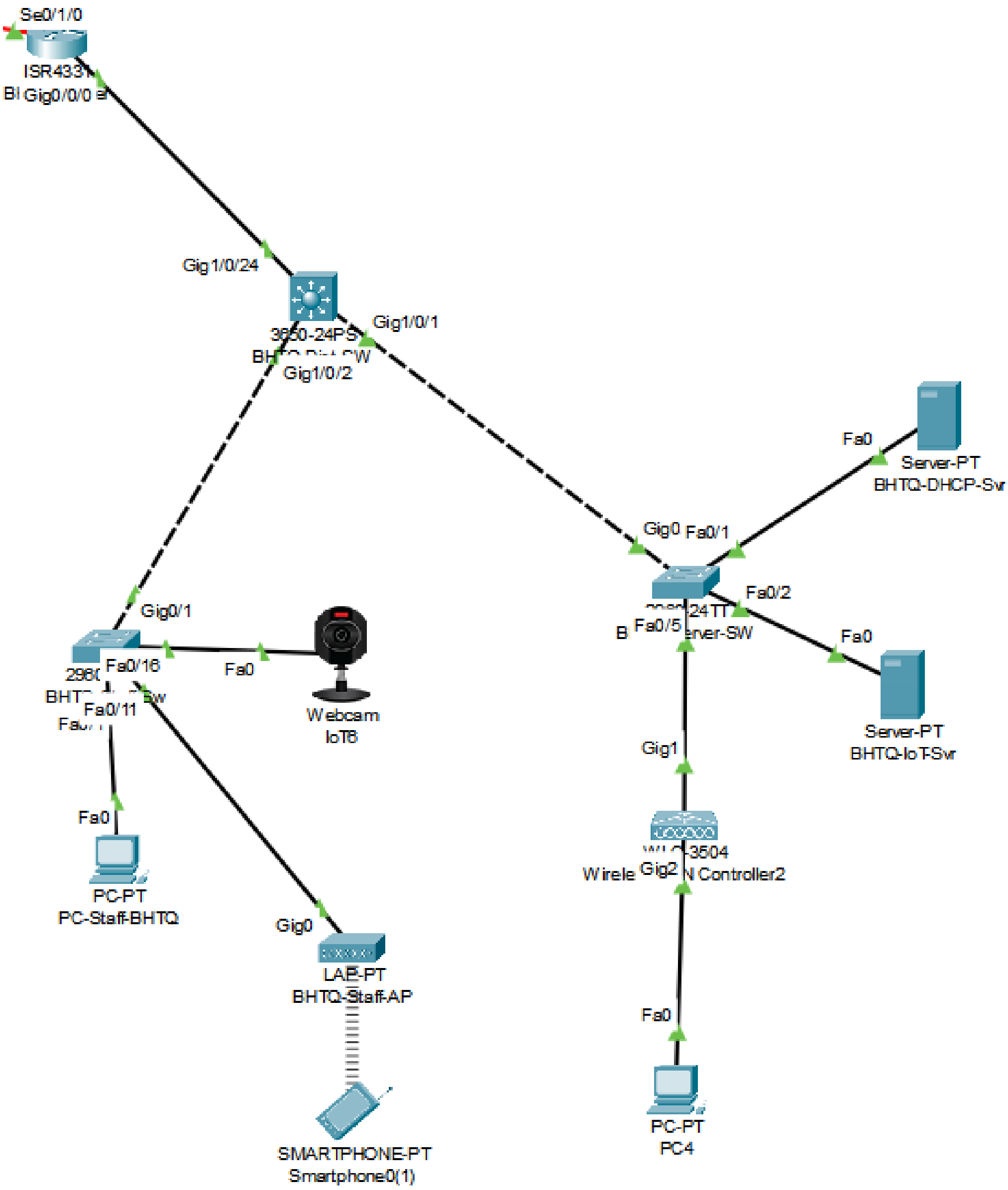


Figure 12: BHTQ Site

5.1.6 DMZ Server

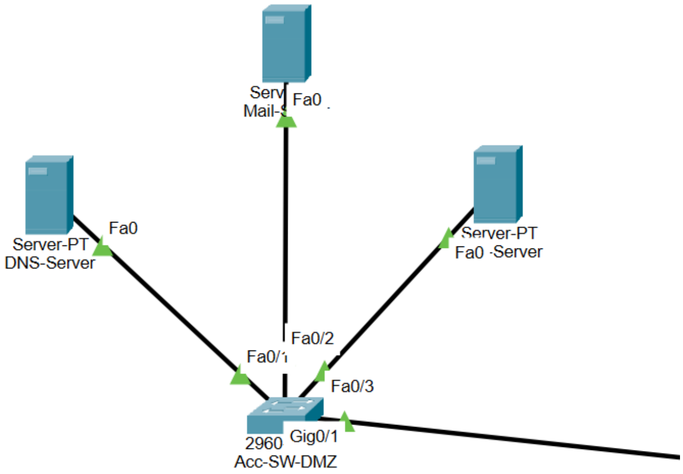


Figure 13: DMZ Server

5.1.7 Internet

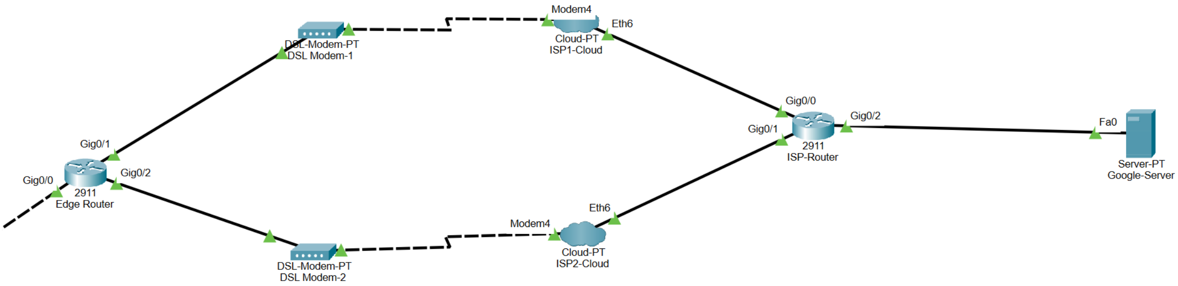


Figure 14: DSL and Internet

6 System Testing and Verification

6.1 Test Scenarios

This section presents the test plan and key verification steps used to validate the designed network. For each test, we specify the objective, test method, expected result and actual observation.

6.1.1 Internal Connectivity

Objective: Verify connectivity between devices in same and difference VLANs at each site.

#	Test Description	Expected Result	Actual Result
DV-01	PCs from same department	Successful	Successful
DV-02	PCs from different departments	Successful	Successful
DV-03	PCs and mobile devices	Successful	Successful
DV-04	PCs and cameras	Successful	Successful
DV-05	PCs and public servers	Successful	Successful
DV-06	PCs and private servers	Successful	Successful

Table 15: Test Scenario: Devices Across VLANs

6.1.2 WAN Connectivity

Objective: Verify that end hosts at the Main Site, DBP Site and BHTQ Site can reach each other through the configured WAN links and dynamic routing

#	Test Description	Expected Result	Actual Result
SS-01	PCs from Main Site to Auxilary Site	Successful	Successful
SS-02	PC and Mobile Device	Successful	Successful
SS-03	PCs and cameras	Successful	Successful
SS-04	Mobile and Cameras	Successful	Successful

6.1.3 Servers in DMZ

Objective: Verify connectivity between servers in the DMZ and other devices

#	Test Description	Expected Result	Actual Result
SD-01	Between servers within the DMZ	Successful	Successful
SD-02	DMZ servers ping to PCs	Failed	Failed
SD-03	PCs ping to DMZ Server	Successful	Successful

Table 17: *Test Scenario: Servers in DMZ*

6.1.4 Camera Surveillance System

Objective: Verify the functionality of the camera surveillance system at the Main Site, DBP Site and BHTQ Site.

Purpose	**#**	**Test Description**	**Expected Result**	**Actual Result**
Verify functionality of the camera surveillance system at the Main Site	CM-01	Devices access the camera server.	Successfully observe camera statuses.	Observed successfully
Verify functionality of the camera surveillance system at the BHTQ and DBP Site	CM-02	Devices access the camera server at the BHTQ and DBP Site.	Successfully observe camera statuses.	Observed successfully

Table 18: ***Test Scenario: Camera Surveillance System***

6.1.5 Security Testing

Finally, we verify that the implemented security policies (firewall, ACLs, and NAT) behave as intended and that unauthorized access is blocked.

Test Objectives

- Ensure that Guest WiFi clients cannot reach internal Staff or Management VLANs.
- Ensure that only DMZ servers are accessible from the Internet (simulated), while internal servers are protected.
- Confirm that NAT is correctly translating internal addresses to public IPs at the edge.

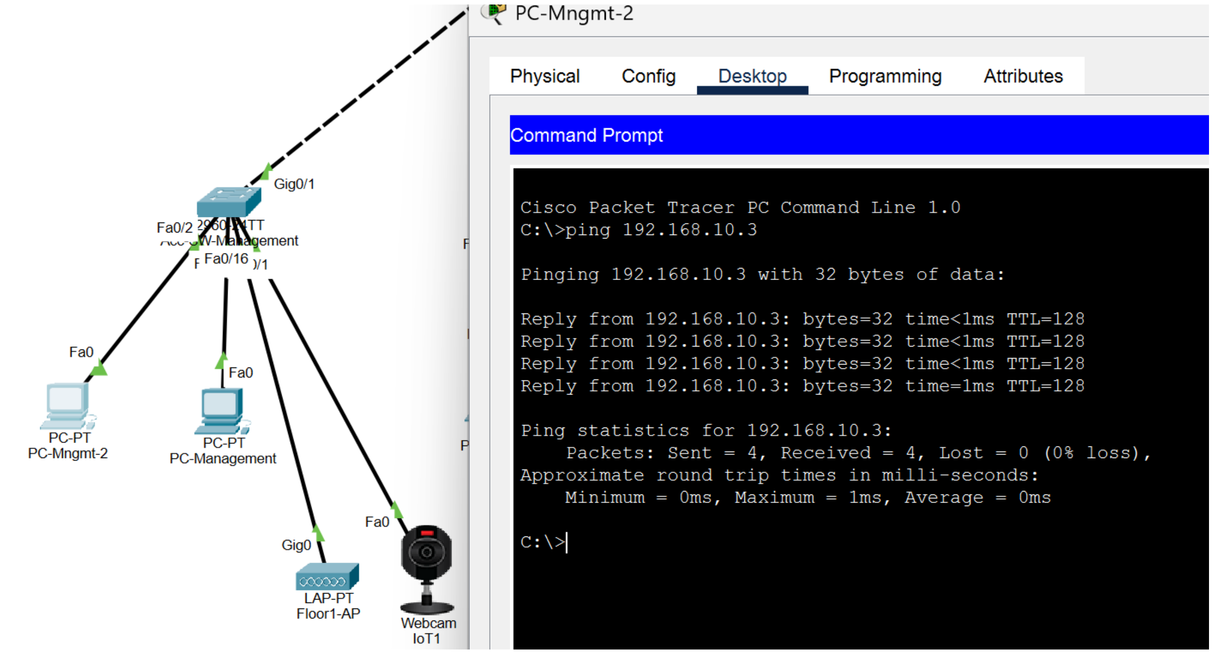
Test Cases

Table 9: Security Testing Test Cases

#	**Source**	**Destination**	**Method**	**Expected Result**
SEC-01	Guest WiFi Client	PC–Staff (Main)	`ping` / RDP	**Blocked**
SEC-02	Guest WiFi Client	Web Server (DMZ)	HTTP	Allowed
SEC-03	Internet Host (simulated)	Internal DB Server	HTTP/SQL	**Blocked**
SEC-04	PC–Staff (Main)	Public Server (Internet)	`ping` / HTTP	Allowed, IP translated by NAT

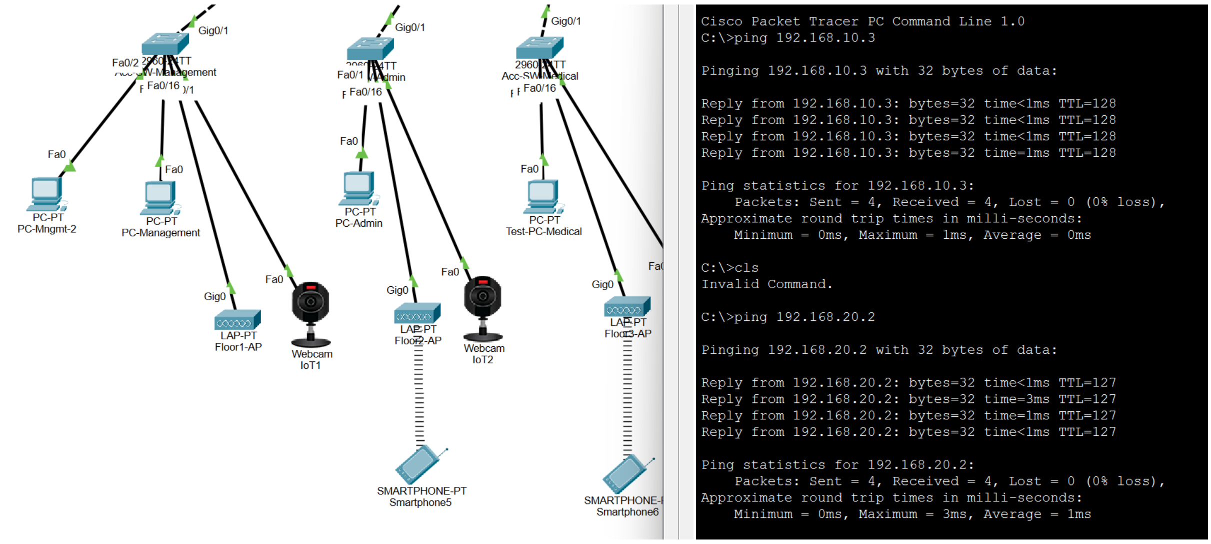
6.2 Test Result:

6.2.1 Devices across VLANs at the same and different site:



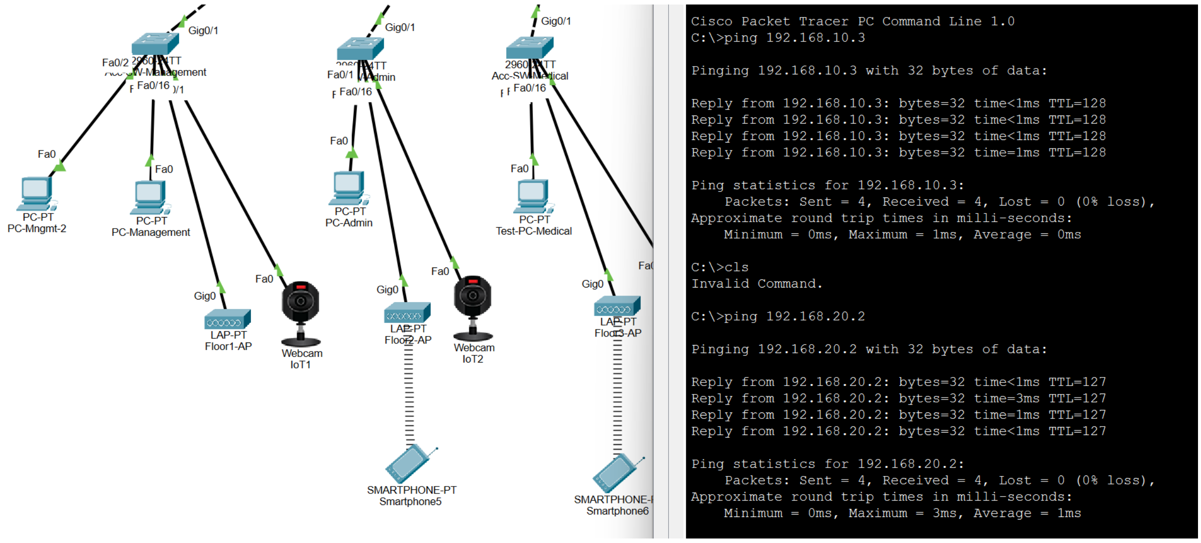
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 15: 2 PC from the same department and floor



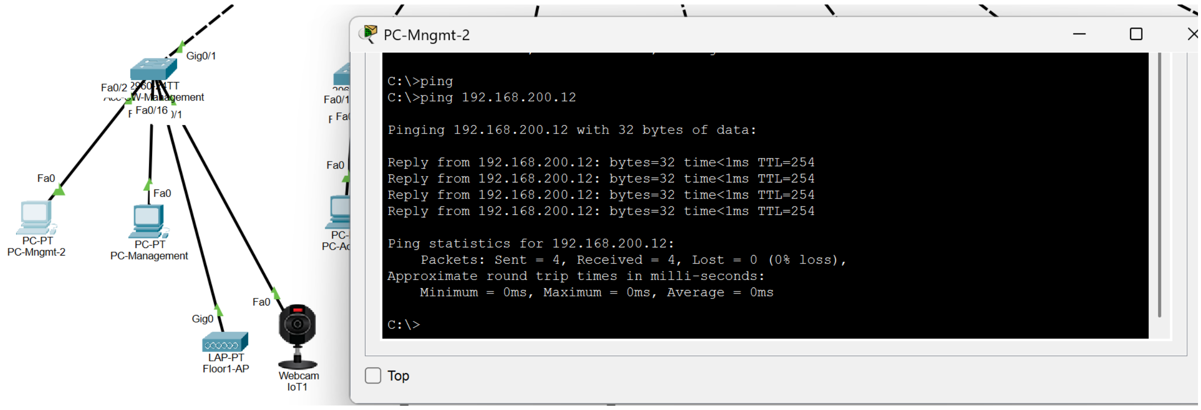
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>cls
Invalid Command.

C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time=3ms TTL=127
Reply from 192.168.20.2: bytes=32 time=1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Figure 16: 2 PC from the different department and floor



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>cls
Invalid Command.

C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time=3ms TTL=127
Reply from 192.168.20.2: bytes=32 time=1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

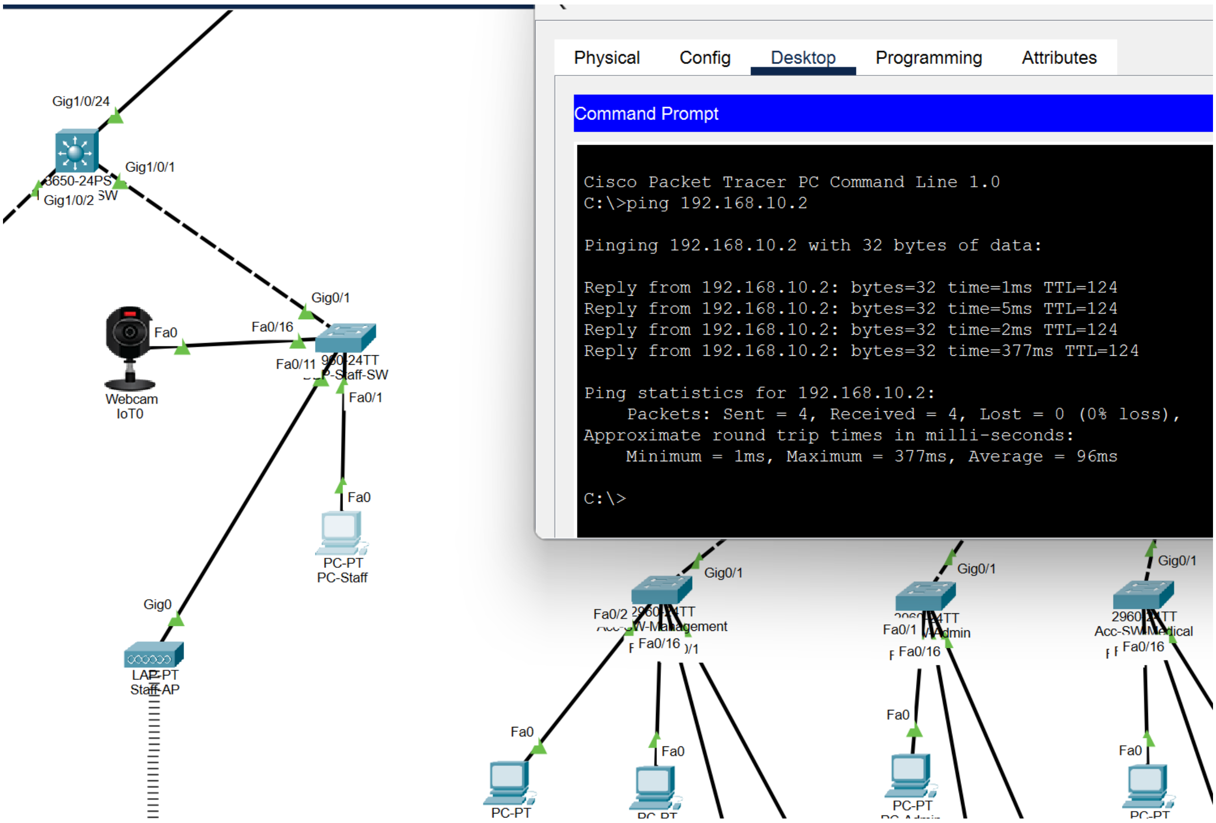
Figure 17: PC and Mobile Devices



```
C:\>ping
C:\>ping 192.168.200.12

Pinging 192.168.200.12 with 32 bytes of data:

Reply from 192.168.200.12: bytes=32 time<1ms TTL=254
Reply from 192.168.200.12: bytes=32 time<1ms TTL=254
Reply from 192.168.200.12: bytes=32 time<1ms TTL=254
Reply from 192.168.200.12: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.200.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

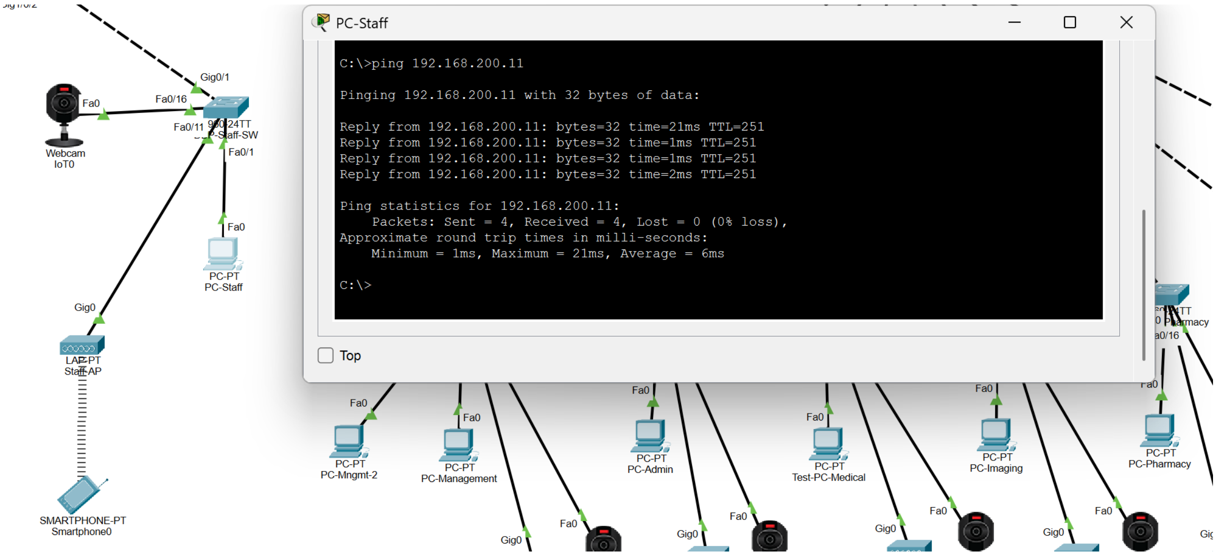
Figure 18: PC and Camera at the Main Site

6.2.2 Devices across WAN



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=124
Reply from 192.168.10.2: bytes=32 time=5ms TTL=124
Reply from 192.168.10.2: bytes=32 time=2ms TTL=124
Reply from 192.168.10.2: bytes=32 time=377ms TTL=124

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 377ms, Average = 96ms

C:\>
```

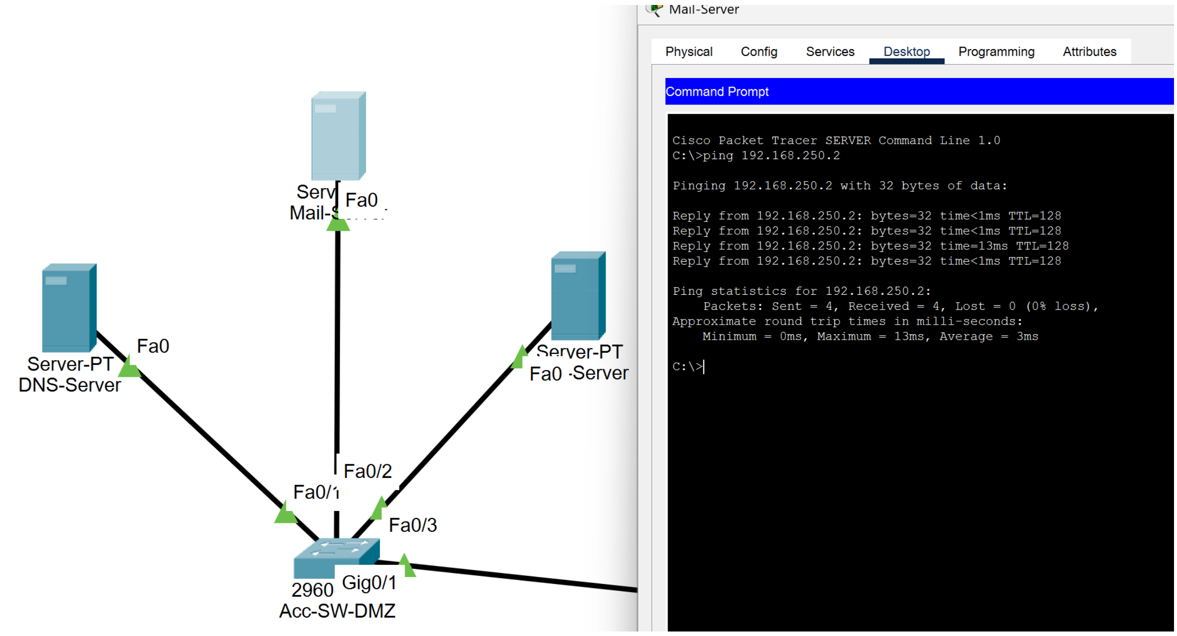
Figure 19: 2PCs from Main Site to DBP Site



```
C:\>ping 192.168.200.11

Pinging 192.168.200.11 with 32 bytes of data:

Reply from 192.168.200.11: bytes=32 time=21ms TTL=251
Reply from 192.168.200.11: bytes=32 time=1ms TTL=251
Reply from 192.168.200.11: bytes=32 time=1ms TTL=251
Reply from 192.168.200.11: bytes=32 time=2ms TTL=251

Ping statistics for 192.168.200.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 6ms

C:\>
```

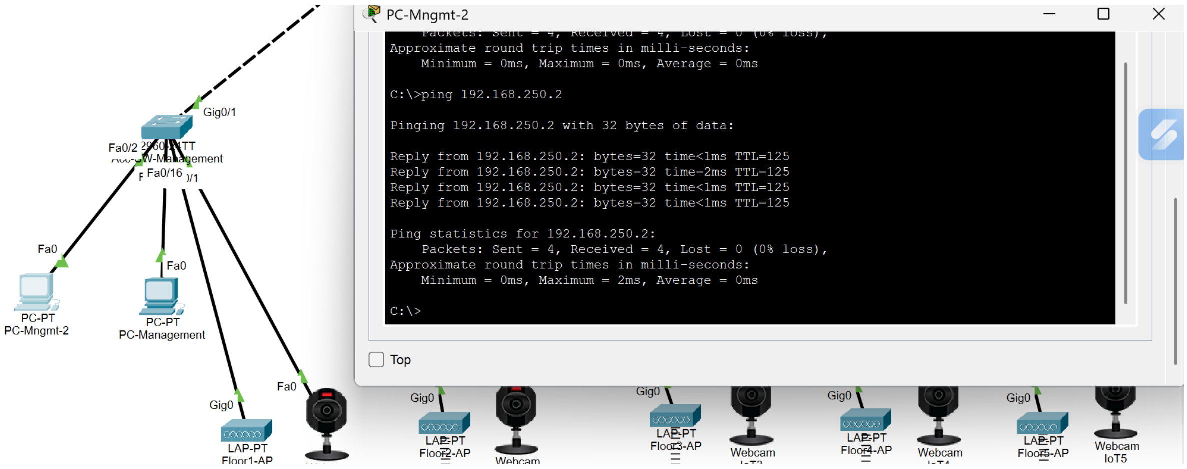
Figure 20: PC and Camera from Main Site to DBP Site

6.2.3 Connection between Server in DMZ



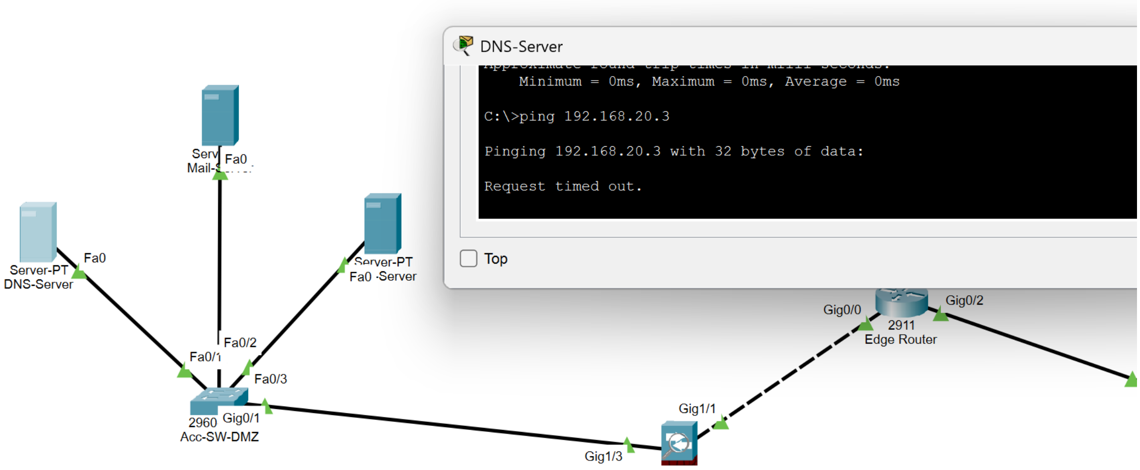
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.250.2

Pinging 192.168.250.2 with 32 bytes of data:

Reply from 192.168.250.2: bytes=32 time<1ms TTL=128
Reply from 192.168.250.2: bytes=32 time<1ms TTL=128
Reply from 192.168.250.2: bytes=32 time=13ms TTL=128
Reply from 192.168.250.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.250.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>
```

Figure 21: Servers in DMZ Servers



```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.250.2

Pinging 192.168.250.2 with 32 bytes of data:

Reply from 192.168.250.2: bytes=32 time<1ms TTL=125
Reply from 192.168.250.2: bytes=32 time=2ms TTL=125
Reply from 192.168.250.2: bytes=32 time<1ms TTL=125
Reply from 192.168.250.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.250.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

Figure 22: Ping from PCs to Server



```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
```

Figure 23: Ping from Server to PC

6.2.4 Camera Surveillance System

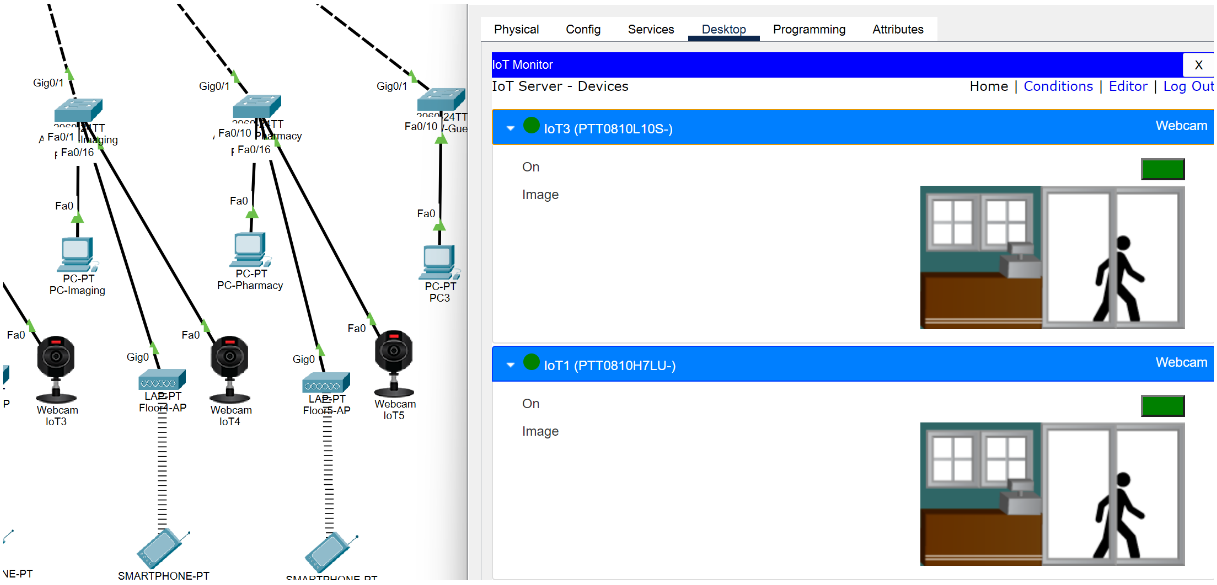
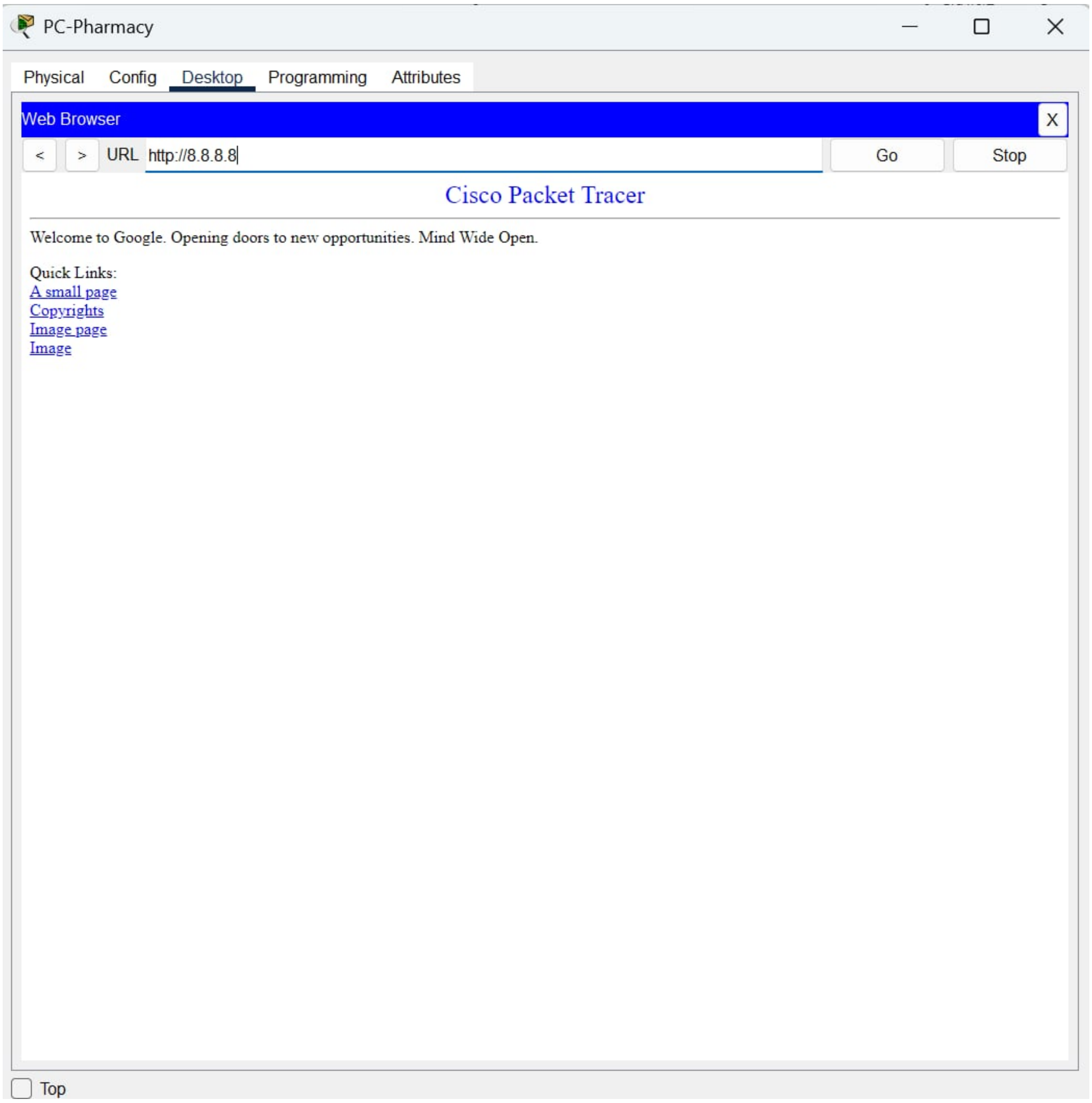


Figure 24: Camera Testing

6.2.5 Connection From Internet



http://8.8.8.8

Cisco Packet Tracer

Welcome to Google. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Figure 25: Internet Connection

7 System Re-evaluation

7.1 Reliability and Safety

The proposed network for the three hospital sites is designed on a hierarchical (top–down) topology with clear separation between core, distribution, and access layers. This structure helps localize failures: a problem at one access switch or one floor will not affect the whole hospital, while issues at the distribution layer can be quickly isolated and bypassed through redundant links and multiple Layer 3 switches at each site.[1]

At Layer 2, VLANs are used to logically separate different types of traffic: *Staff LAN*, *Guest WiFi*, *IoT/Surveillance*, and *Management/IT*. Each VLAN has its own IP subnet and default gateway, and inter-VLAN routing is strictly controlled at Layer 3. This reduces the broadcast domain size, limits the impact of faults, and improves both performance and security for critical applications such as EMR, PACS, and internal management systems.

At Layer 3, dynamic routing is provided by an interior gateway protocol (EIGRP in the current design) together with carefully planned point-to-point /30 links between routers. Route convergence is therefore fast when a WAN link fails, helping to maintain connectivity between the main hospital site and the two auxiliary campuses. Loopback interfaces have been reserved as router IDs, which simplifies future migration to OSPF if required by the hospital or the course specification.

WAN reliability is further enhanced by using multiple leased lines between sites and two separate DSL links for Internet connectivity. Even though the Packet Tracer simulation cannot fully emulate real ISP behaviour, the design allows traffic to be redistributed if one leased line or one ISP link fails, thereby improving availability for telemedicine, remote access, and cloud services.

Regarding safety and security, several mechanisms are deployed:

- A Cisco ASA firewall separates the network into *Inside*, *DMZ*, and *Outside* zones. Only required ports are opened from the Internet to the web server in DMZ; internal servers remain protected in the Inside zone.
- Access Control Lists (ACLs) on distribution switches and routers prevent Guest WiFi clients from accessing hospital workstations or management devices, while still allowing them to reach Internet services.
- NAT is applied at the main site edge so that internal addresses are hidden from the public network, reducing the exposed attack surface.
- Critical services (DHCP, DNS, web server, and IoT server) are placed in controlled segments, making it easier to monitor and secure them.

Overall, the combination of hierarchical design, VLAN segmentation, dynamic routing, redundant WAN connections, and layered security (Firewall + ACLs + NAT) provides a reliable and reasonably safe network for a medium–large hospital environment.

7.2 Ease of Upgrade

The addressing and naming schemes are intentionally simple and scalable. Each VLAN uses a /24 subnet, with consistent patterns across the three sites (e.g. 172.16.x.10.0/24 for Staff LAN, 172.16.x.20.0/24 for Guest WiFi, etc.). Point-to-point links use the 10.0.0.x/30 range. This regular structure makes it

[1] The overall hierarchical and redundant structure is summarized in Sections 1–4 of the report.

straightforward to add new floors, new buildings or even new auxiliary sites by allocating the next available subnet according to the same convention.

Because of the hierarchical topology, upgrades can often be performed per layer. For example, access switches on one floor can be replaced by higher capacity models or PoE switches for new medical devices without changing the core or WAN design. Similarly, wireless coverage can be improved by adding more LWAPs and updating the Wireless LAN Controller configuration, without touching routing or security policies.

Dynamic routing also simplifies scaling. When additional subnets are added at a site, only the local distribution switches and router need to be updated. Routes are then automatically propagated to the rest of the network. The use of loopback interfaces and summarizable address blocks reduces the need for frequent changes in the core.

The system also supports a diverse set of networked applications and platforms: wired PCs, WiFi clients, web and database servers, surveillance cameras, and IoT devices. Standard IP services such as DHCP, DNS and HTTP are used, so new software systems can be integrated without redesigning the whole infrastructure.

7.3 Remaining Issues

Despite the above strengths, several limitations remain in the current simulation and design:

- **Single points of failure.** The design still relies on single firewall and edge-router instances at the main site. If one of these devices fails, Internet access or inter-site connectivity may be lost until manual intervention occurs.
- **Limited security depth.** Only basic firewall rules and ACLs are configured. Advanced features such as IDS/IPS, URL filtering, anti-malware inspection, and detailed logging to a central SIEM are not implemented in Packet Tracer.
- **Wireless security.** The Wireless LAN in the simulation uses simplified security (e.g. WPA2-PSK). In a real hospital, stronger mechanisms such as 802.1X authentication with RADIUS and per-user credentials would be required.
- **QoS and performance guarantees.** Quality of Service mechanisms for voice, video, and critical medical applications are not configured. All traffic currently shares the same priority, which may affect performance during peak hours.
- **Monitoring and management.** A full network management system (SNMP monitoring, NetFlow, configuration backup, alerting) is not part of the simulation, although it is essential in production.

These issues do not prevent the network from operating in the simulated environment, but they highlight aspects that must be addressed before deploying a similar design in a real hospital.

7.4 Future Development

Based on the above evaluation, several directions for future improvement can be proposed:

- Deploy high-availability pairs for the main firewall and core routers (e.g. using failover pairs and HSRP/VRRP) to remove single points of failure at the main site.

- Strengthen security by enabling advanced firewall features, adding IDS/IPS sensors, implementing 802.1X authentication for both wired and wireless access, and applying more granular ACLs per department.
- Introduce end-to-end QoS policies to prioritise real-time traffic (voice over IP, telemedicine video, medical imaging transfers) over non-critical traffic such as general web browsing.
- Extend the addressing plan to support IPv6 dual-stack operation, in line with modern hospital information systems and national IPv6 deployment roadmaps.
- Integrate a centralized network management and monitoring platform (e.g. SNMP-based NMS, Syslog, NetFlow) to improve visibility, fault detection, and capacity planning.
- Consider adding VPN services for remote doctors and administrators, ensuring secure access to internal systems from outside the hospital.

These developments would gradually turn the current academic design into a production-ready hospital network with higher resilience, better security, and easier operation.

8 Conclusion and Deliverables

8.1 Summary of Achievements

In this assignment, we have designed and simulated a complete network infrastructure for a large hospital with one main site and two auxiliary campuses. Starting from the functional and non-functional requirements, we proposed a hierarchical topology, defined the role of each building and network device, and produced detailed IP addressing plans for all VLANs and WAN links.

We selected suitable Cisco equipment (routers, Layer 2/Layer 3 switches, firewall, LWAPs, and Wireless LAN Controller) and showed how they are interconnected through structured cabling diagrams. The bandwidth and throughput calculations confirmed that the chosen links are adequate for estimated traffic at peak hours.

The logical design was implemented in Cisco Packet Tracer using VLANs, dynamic routing, ACLs, firewall policies, NAT, DHCP, DNS, DMZ web servers, and an IoT surveillance subsystem. A series of tests (pings between VLANs and sites, Internet access, web server access, NAT verification, and IoT camera connectivity) demonstrated that the network satisfies the basic connectivity and security requirements.

Finally, we re-evaluated the system in terms of reliability, safety, ease of upgrade, and remaining issues, and suggested several directions for future development. The main deliverables of this project are:

- The written report describing requirements, design rationale, IP planning, wiring diagrams, configurations, and evaluation.
- The Cisco Packet Tracer simulation file of the complete hospital network.
- Supporting configuration snippets and test screenshots that verify the correct operation of the proposed design.

Overall, the project achieves the learning objectives of the course: applying computer networking knowledge to analyse requirements, design a scalable and secure network, implement it in a simulation environment, and critically evaluate its strengths and limitations.