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

COMPUTER NETWORK

PROJECT REPORT

COMPUTER NETWORK ASSIGNMENT 2

Advisor(s):	Dr. Nguyen Phuong Duy	
Student(s):	Nguyen Hoang Quan	2252681
	Le Trung Kien	2252394
	Nguyen Sy Hung	2252271
	Tran Chi Tai	2252727

HO CHI MINH CITY, DECEMBER 2024

Table of Content

---

5. Network Map Design Using Packet Tracer

- **5.1 Overall Network Structure**: A top-level view of the network.
- **5.2 Main Site Setup**: Connection of the main site to the internet.
- **5.3 Auxiliary Sites Setup**: Detailed diagrams for Auxiliary 1 and 2.
- **5.5 Site Connections**: Connectivity between the main site and auxiliary sites.
- **5.6 Internet Connection**: Integrating internet access.

---

6. System Testing

- **6.1 Connect PCs Within VLANs**: Verifying intra-VLAN communication.
- **6.2 Inter-VLAN Connectivity**: Ensuring communication across VLANs.
- **6.3 Site-to-Site Connectivity**: Testing connections between the main and auxiliary sites.
- **6.4 DMZ Server Access**: Verifying access to servers within the DMZ.
- **6.5 Customer Device Restrictions**: Blocking customer devices from accessing LAN PCs.
- **6.6 Web Server Internet Connectivity**: Ensuring web servers are reachable from the internet.

---

7. Network System Re-evaluation

- **7.1 Remaining Issues**: Addressing unresolved challenges in the design or implementation.
- **7.2 Future Development**: Recommendations for scalability and upgrades.

1. Member List & Workload

No	Full Name	Student ID	Responsibility	Percentage
1	Le Trung Kien	2252394	2,3	25%
2	Nguyen Hoang Quan	2252681	4,5	25%
3	Tran Chi Tai	2252727	6,7	25%
4	Nguyen Sy Hung	2252271	File, report	25%

2. Suitable network structures for buildings

2.1 Requirement analysis

- **Technology Stack**: The network infrastructure will utilize modern technologies, including wired and wireless connections, fiber cabling (GPON), and GigaEthernet (1GbE/10GbE/40GbE).
- **VLAN Structure**: The network will be organized using VLANs to segment the center's network into department-specific sub-networks. Devices within each VLAN can communicate freely, while external networks will be restricted from accessing department VLANs.
- **WAN and Internet Access**: The Main Site sub-network will connect to two Branch Sites through two leased lines for WAN connectivity and two DSLs for Internet access, with a load-balancing mechanism to ensure efficiency and redundancy.
- **Security and Robustness**: The network design prioritizes high security, system robustness in case of failure, and scalability for future growth.
- **Future Growth**: The network is estimated to grow by 20% over the next five years in terms of users, load, and branch expansions, and is designed to accommodate this growth with minimal disruption.

2.2 Solution

The network will be implemented as a LAN connected to a central router and the Internet, segmented into VLANs for security and management purposes.

2.2.1 Main Site

- **Workstation Layout**: The Main Site comprises 600 workstations spread over two buildings with 10 floors in total (5 floors per building). Each floor will house 60 workstations divided among 10 rooms. Each room will have a dedicated switch, with all switches connected to a central switch on each floor to form a VLAN for that floor.

- **Switch Selection**: To accommodate current and future needs, each room switch will be a 20-24 port model, allowing room for additional devices. For high-usage floors, 48-port switches may be considered to simplify future expansion.
- **Data Center**: A data center located 50 meters from both buildings will house critical hospital servers. Fiber cabling will connect the buildings and data center to ensure low latency and high throughput. Servers include:
    - **DNS Server**: Resolves domain names to IP addresses.
    - **Web Server**: Provides access to patient account information and other services.
    - **File Server**: Shares files and data within the hospital.
    - **Mail Server**: Manages internal and external email communications.
    - **DHCP Server**: Dynamically assigns IP addresses across the network.
    - **Database Server**: Stores critical hospital data.
    - **Backup Server**: Secures backup data for recovery purposes.
- **Firewall and Security**: The network connects to the Internet via an ASA firewall, providing perimeter security with Network Address Translation (NAT), VPN capabilities, and threat management.

2.2.2 Branch Sites

For the two Branch sites, we structured each site as follows:

- **First Floor**: This floor is equipped with two servers, connected through a switch within a dedicated VLAN for efficient server management.
- **Second Floor**: This floor accommodates devices across 3 rooms, as we assumed given the lack of specific room and device numbers. A switch connects all devices on the second floor, creating a single VLAN for the entire floor. This setup allows for easy expansion, with departments able to add PCs and additional switches as needed.
- **Wi-Fi Network**: We implemented a Wi-Fi network on the second floor, supporting a surveillance camera system for security monitoring and enabling wireless devices to connect to the Internet.
- **VLAN Connectivity**: The two switches for the VLANs are linked to an additional switch to help reduce congestion and to support future scalability.
- **Site Connectivity**: Each site is equipped with a router connecting it to the main site, enabling communication. The sites are interconnected through two leased lines for a WAN connection, utilizing SD-WAN to manage network traffic.

2.3 Make a checklist to be surveyed at the installation locations

1. Physical Infrastructure

- What physical topology does the company prefer? (Bus, Star, Ring, Mesh, Tree)
- The new network will integrate to the existing networking infrastructure, or it will be built from scratch?
- How is conduit between floors carried out?
- What standards for structured cabling does the company use?

- How many departments are there, what are they, where they are physically located in each building?

Summary solutions: The network will adopt a **Star Topology** for scalability and fault tolerance, simplifying maintenance and troubleshooting by isolating faults to specific segments. Structured cabling pathways, such as **cable trays or vertical risers**, will facilitate efficient inter-floor connections, adhering to modern standards with **Category 6/6A cables for copper** and **fiber optics for backbone links**. A comprehensive site survey will map departmental locations and physical layouts to ensure the infrastructure meets specific connectivity needs while evaluating whether to integrate with existing systems or design a new setup from scratch.

2. Logical infrastructure

- What WAN connection does the company prefer? (SD-WAN or MLPS)
- Discuss VPN configuration in more detail.
- Discuss camera systems in more detail.
- How many hospital services (or tasks) need networking facilities, and what are they?

Summary solution: The network will use **SD-WAN** for flexible, cost-efficient, and centrally managed WAN connectivity. **Site-to-site VPNs** will secure communication between main and branch sites, while **remote access VPNs** will enable secure connections for off-site employees. Surveillance cameras will leverage a **centralized NVR system**, and **VLANs** will isolate their traffic from the main network. Networking needs for patient data, scheduling, device integration, and administrative tasks will be supported by VLAN segmentation to ensure security and manageability.

3. Cost, Security & Risks

- What are the issues with existing infrastructure, if any?
- What are the previous issues and disasters the company has met in the past?
- What security policy for each networking unit in the company?
- Does the company accept the proposed list of devices and equipment and associated cost?
- How flexible is the company about the additional cost?

Summary solution: Potential bottlenecks, outdated equipment, or non-compliance issues in the current infrastructure will be addressed. Past incidents, such as outages or breaches, will inform proactive security measures. A comprehensive **security policy** will be developed for each VLAN, incorporating **firewalls, intrusion prevention systems (IPS), and endpoint security solutions**. Approval will be sought for the proposed equipment and budget, with allowances for unanticipated costs to support scalability and organizational goals.

2.4 Define areas with high load (network load) to select the appropriate device configuration (load balancers are placed in necessary locations)

Before identifying high-load areas for load balancer placement, let's briefly define a network load balancer.

Network Load Balancers (NLBs) operate at OSI Layer 4, distributing traffic based on network-layer attributes like destination ports and IP addresses. Unlike application-aware load balancers, NLBs do not process application-layer data such as cookies, content types,

user location, custom headers, or application behavior, instead focusing solely on network-level information in packet headers.

Key Advantages of Network Load Balancers:

- Scalability to handle millions of requests per second, suitable for fluctuating workloads.
- Support for static IP addresses.
- Ability to assign an elastic IP address for each enabled subnet.
- Flexibility to register targets by IP addresses, even if they are outside the VPC.
- Capacity to route multiple applications on a single EC2 instance, registering each IP or instance with multiple ports in the same target group.
- Independent monitoring of service health, with health checks and metrics reported at the target group level.

Now that the definition is clear, let's identify high-load areas in this assignment:

- **Internet Gateway:** All traffic to the internet flows through the hospital network's internet gateway, which acts as the central access point. This gateway is a potential bottleneck. Placing a load balancer behind the internet gateway can help distribute incoming traffic across servers located at the Branch and Main Sites, reducing congestion.
- **Main Site's Subnet Router:** Traffic between the Main Site and the Branch Sites flows through the Main Site's subnet router, creating a potential bottleneck. A load balancer here would help manage traffic distribution between the Main Site and the Branch Sites, balancing the load effectively.

2.5 Choose a network structure that matches the building's architecture with convenience and aesthetics

The implementation plan for the company's network is outlined as follows:

1. Main Site

The Main Site consists of two buildings, A and B, with each building following a similar network setup. Specifically:

- Each floor contains 10 rooms, with each room averaging 6 devices, including PCs and wireless devices.
- Two surveillance cameras are installed at each end of each floor for monitoring.

2. Branch Sites

First Floor - Server Room and IT Department:

- 2 public servers for load balancing in coordination with the Main Site's public servers.
- 1 private server dedicated to internal functions.
- 5 PCs for IT personnel.
- 2 switches to manage connections between floors.
- 1 router connected to a leased DSL line for external communication.

Second Floor - Patient Services Department:

- 20 PCs for use by nurses and doctors, plus an additional 10 PCs for patients without WiFi access.
- 1 switch connecting all PCs.
- 1 surveillance camera and speaker system for security monitoring.

2.6 Design the network usage in a wireless environment, applying network security standards and setting up partitions for network servers and devices (e.g., Server farm, DMZ, Firewall, ...)

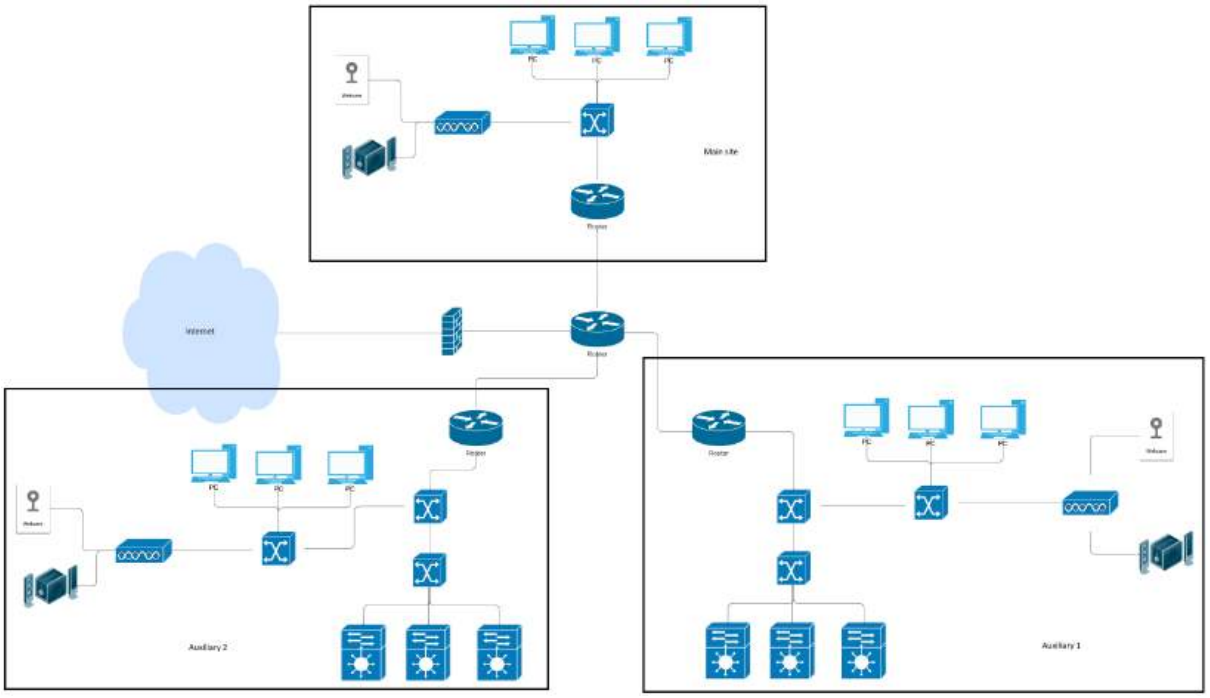


Figure 1: Our network demonstration

The network is segmented as shown in the figure above:

- A DMZ (Demilitarized Zone) was established to provide public access to service servers from the internet.
- A firewall was implemented between the company's private WAN and the external public network.
- Only authorized traffic from trusted internet servers is allowed to enter the private network.

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

3.1 List of recommended equipment and typical specifications

Here we present the device stack needed for the network setup.

Device Name	Technical specifications	Amount	Cost (November 2024)
The Cisco 2901 Router	Device Code: CISCO2901-V/K9 Form Factor: External – modular – 1U Dimensions: 43.9 – 43.8 – 4.5 (cm) Weight: 6.1 kg DRAM Memory: 512 MB (installed) / 2 GB (max) Flash Memory: 256 MB (installed) / 8 GB (max) Routing Protocol: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing Data Link Protocol: Ethernet, Fast Ethernet, Gigabit Ethernet Remote management Protocol: SNMP, RMON Power: AC 120/230 V (50/60 Hz)	06	1050$
Cisco ASA5508-K9 FireWall	Product ID: ASA5516-FPWR-K9 Interfaces: 8 x 1 Gigabit Ethernet 1 RJ-45 and Mini USB console Memory: 8 GB Flash: 8 GB Features: VLAN support, VPN support, firewall protection Application control (AVC) throughput: 250 Mbps VPN throughput (3DES/AES): 250 Mbps Stateful inspection throughput: 1.8 Gbps IPsec site-to-site VPN peers: 300 Stateful inspection throughput (multiprotocol): 900 Mbps Maximum 3DES/AES VPN throughput: 250 Mbps Dimensions: 4.3 x 43.6 x 28.7 cm Weight: 3 kg Power: AC only	01	2000$
Switch Cisco WS-C2960L-16TS-LL	Product ID: WS-C2960L-16TS-LL IOS: LAN Lite Ethernet Gate 10/100/1000: 16 Forwarding bandwidth: 18 Gbps Switching bandwidth: 36 Gbps DRAM: 512 MB Flash: 256 MB	15	8000$
Cisco Aironet 1700 Series Access Points	Product ID: AIR-CAP1702I-H-K9 Max Data Rate 5GHz MIMO Radio Design: Spatial Streams	01	250$
Severs & Workstations	Selected by the hospital		

Firewall is 11.0.0.0 / 24

IP address format: **138.165.[VLAN].[HOST]** where [VLAN] from 1 to 254 and [HOST] from 2 to 254

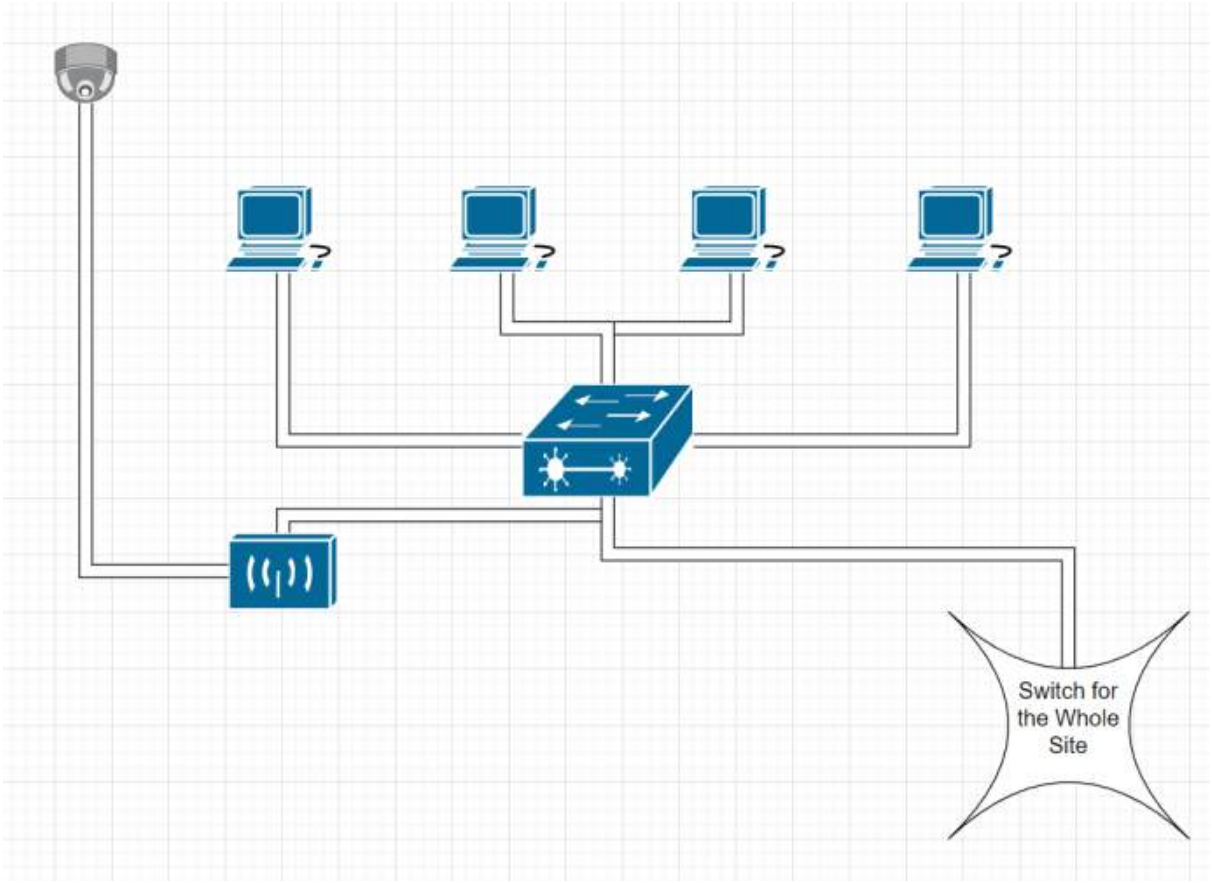
There are special IP addresses and VLANs used for routing and network management:

- Network 11.0.1.0/24 is for WAN communication on leased DSL between Main Site and Branch Site 1.
- Network 11.0.2.0/24 is for WAN communication on leased DSL between Main Site and Branch Site 2.
- Network 12.12.12.0/24 is for communication between the hospital and the firewall.
- Network 8.8.8.0/24 is for communication between the firewall and Internet Gateway.

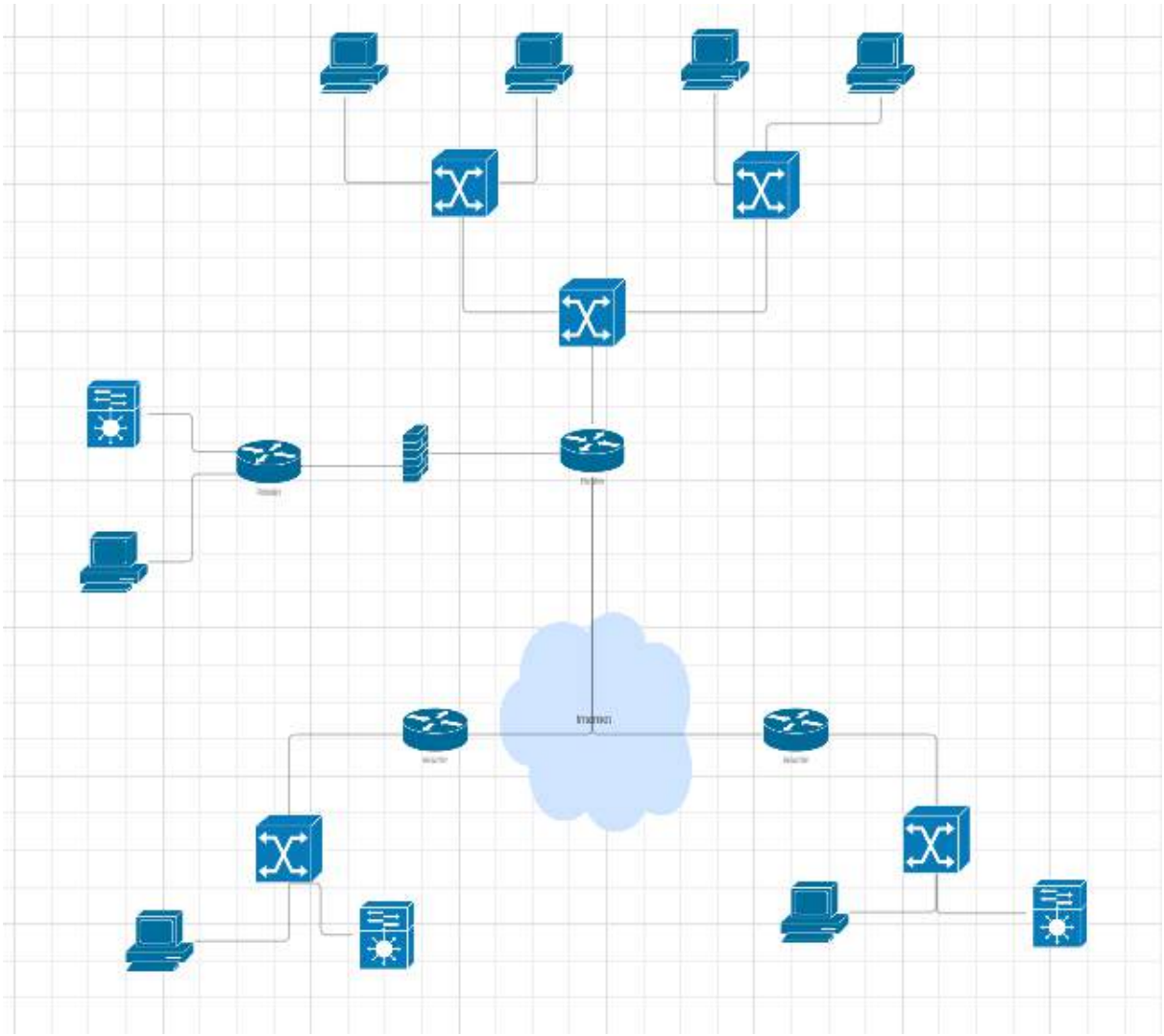
Here is the summary of IP address:

Location	VLAN	Network IP Address	Default Gateway
Main Site	001	138.165.1.0 / 24	138.165.1.1 / 24
Main Site	002	138.165.2.0 / 24	138.165.2.1 / 24
Main Site	003	138.165.3.0 / 24	138.165.3.1 / 24
Main Site	004	138.165.4.0 / 24	138.165.4.1 / 24
Auxiliary 1	005	138.165.8.0 / 24	138.165.8.1 / 24
Auxiliary 1	006	138.165.9.0 / 24	138.165.9.1 / 24
Auxiliary 2	007	138.165.10.0 / 24	138.165.10.1 / 24
Auxiliary 2	008	138.165.11.0 / 24	138.165.11.1 / 24
IT Cable Room (Main Site)	009	11.0.0.0 / 24	11.0.0.1 / 24

3.2 Schematic physical setup of the network



3.3 WANconnection diagram between the main Site and the two Branch Sites (using new WAN technology such as SD-WAN, MPLS, and OSPF routing protocol)



4.Calculate the required throughput, and expected bandwidth from ISP, then suggest the configuration for the hospital network

This section details the calculation of the required throughput and expected bandwidth from the Internet Service Provider (ISP). Based on these calculations, a suitable network configuration for the hospital is suggested.

Summary of estimated data flows and system workload:

- Each server total download: Ds = 1000MB/day
- Each server total upload: Us = 2000MB/day
- Each workstation total download: Dw = 500MB/day
- Each workstation total upload: Uw = 100MB/day
- Total WiFi-connected devices download: DataWiFi = 500MB/day
- Peak hours: 3 hours
- Network peak rate is 80% at peak hours

- Hospital's growth rate of 20% in 5 years

Network calculation formulas:

- 1 MBps = 1MBps = 8 * 2^20 / 10^6 Mbps
- Total data transfer: Data = Number * (Upload + Download)
- Peak Hour Throughput (PHT): Throughput = Data * Peak Rate / Peak Time = Data * 0.8 / (3 * 60 * 60) = Data / 13500
- Minimum bandwidth for the next 5 years: Bandwidth = Throughput * Growth Rate = Throughput * 1.2

4.1 Main Site

Wired Internet:

- Number of servers: Ns = 102
- Number of workstations: Nw = 6002

Total data transfer by server:

∑Dataserver = Ns * (Ds + Us) = 12 * (1000 + 2000) = 36000 (MB/day)2

Total data transfer by workstation:

∑Dataworkstation = Nw * (Dw + Uw) = 600 * (500 + 100) = 360000 (MB/day)2

Total data transfer at the Main Site:

∑DataMain Site = ∑Dataserver + ∑Dataworkstation + ∑DataWiFi = 36000 + 360000 + 500 = 396500 (MB/day)3

Peak hour throughput at the Main Site:

ThroughputMain Site = ∑DataMain Site / 13500 = 396500 / 13500 = 29.3704 (MBps)3

Minimum bandwidth of the Main Site:

BandwidthMain Site = ThroughputMain Site * 1.2 = 29.3704 * 1.2 = 35.2444 (MBps)3

4.2 Branch Sites

Wired Internet:

- Number of servers: Ns = 24
- Number of workstations: Nw = 604

Total data transfer by server:

∑Dataserver = Ns * (Ds + Us) = 2 * (1000 + 2000) = 6000 (MB/day)4

Total data transfer by workstation:

∑Dataworkstation = Nw * (Dw + Uw) = 60 * (500 + 100) = 36000 (MB/day)4

Total data transfer at an Auxiliary Site:

∑DataAuxiliary Site = ∑Dataserver + ∑Dataworkstation + ∑DataWiFi = 6000 + 36000 + 500 = 42500 (MB/day)4

Peak hour throughput at the Auxiliary Site:

ThroughputAuxiliary Site = ∑DataAuxiliary Site / 13500 = 42500 / 13500 = 3.1481 (MBps) = 25.1852 (Mbps)5

Minimum bandwidth of the Auxiliary Site:

BandwidthAuxiliary Site = ThroughputAuxiliary Site * 1.2 = 3.1481 * 1.2 = 3.7777 (MBps) = 30.2218 (Mbps)5

4.3 Suggest the configuration for the hospital network

- From the expected bandwidth, the ISP lease line from each branch should be 100 Mbps, which scales well for the company for the next ten years.
- From the VNPT internet leased line, we could rent the cheapest selection, about 418.000 VNĐ/month package.

Gói cước	Tốc độ trong nước/ Quốc tế **	Thiết bị	Giá cước (vnđ)
FiberS1	400Mbps/2Mbps	01 WIFI	**418.000**
FiberS2	800Mbps/5Mbps	01 WIFI	**660.000**
FiberS3	1000Mbps/12Mbps	01 WIFI	**814.000**
Fiber WIFI 1	400Mbps/2Mbps	03 WIFI	**473.000**
Fiber WIFI 2	800Mbps/5Mbps	04 WIFI	**748.000**
Fiber WIFI 3	1000Mbps/12Mbps	04 WIFI	**902.000**

5. Design the network map using Packet Tracer simulation software

5.1 Overall Structure of the Network

Network Segments and Zones

- Design multiple zones, each representing a department (Admin, IT, HR, etc.), with unique IP subnet ranges. Assign VLANs based on departments to help organize and secure the network traffic.
- Color-code these zones in Packet Tracer or GNS3 to easily identify departments visually (e.g., blue for Admin, green for IT).

Core Network

- Place a core switch (or router) at the center of your design to act as the network backbone.
- Connect this core device to distribution switches or routers that lead to each departmental subnet.
- Ensure high-speed links between the core device and distribution layer to handle inter-departmental traffic.

Departmental Segments

- For each department (Admin, IT, HR, etc.), create a subnet with a unique VLAN ID and IP range.
- Each department's router or switch connects local devices to the core network, while isolating departmental traffic for better security and efficiency.
- Set IP ranges for each VLAN (e.g., VLAN 2: 192.168.1.0/24, VLAN 3: 192.168.2.0/24, VLAN 6: 192.168.6.0/24 for a Branch site).

Devices within Segments

- Add devices like workstations, servers, and IP phones to each departmental subnet.
- Configure the IP addresses within each department's subnet and ensure device roles are assigned according to departmental needs.
- Set up peripheral devices (e.g., printers, scanners) specific to departments that need them.

Inter-Segment Communication

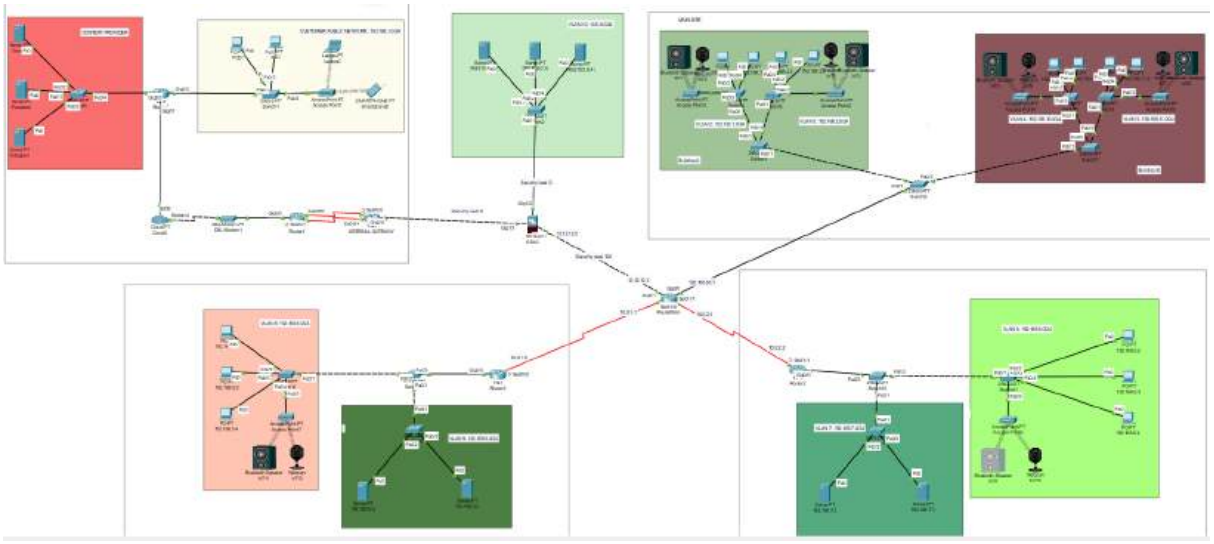
- Configure firewall rules and access control lists (ACLs) at the core device to restrict sensitive data access.
- Set routing and inter-VLAN communication policies on core and distribution routers to control communication flow between different segments.

External Connections

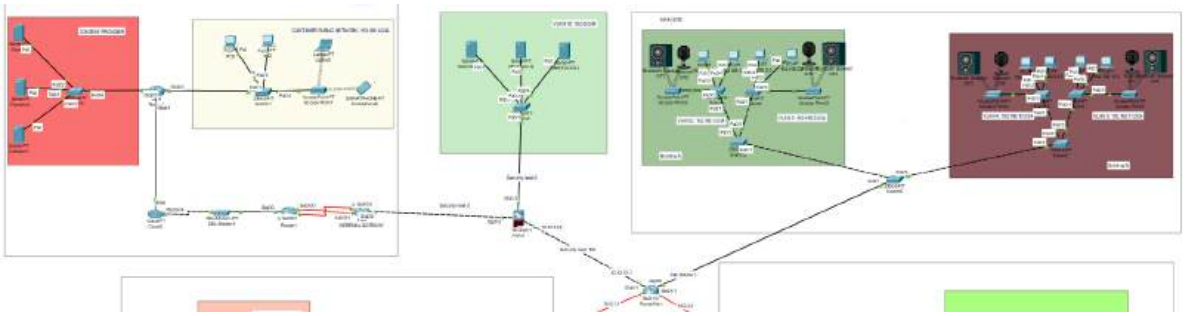
- Connect the core network device to an internet-facing router with firewall settings to secure external communication.
- Set up VPN configurations for secure remote access as needed for employees or remote departments.
- Test and configure NAT to allow internal devices to access the internet safely.

Simplified Design for Simulation

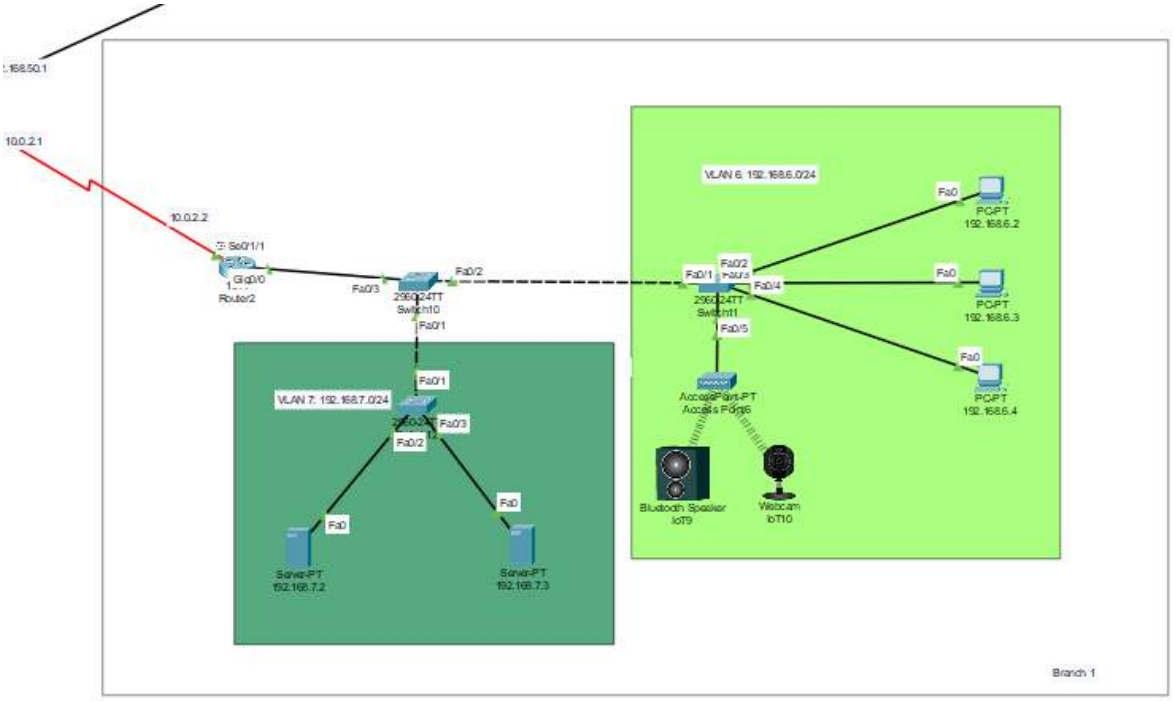
- Omit excessive workstations or servers for each department in the simulation software to manage complexity.
- Focus on essential components, routers, switches, and a few sample devices per department to validate connectivity and routing functionality.



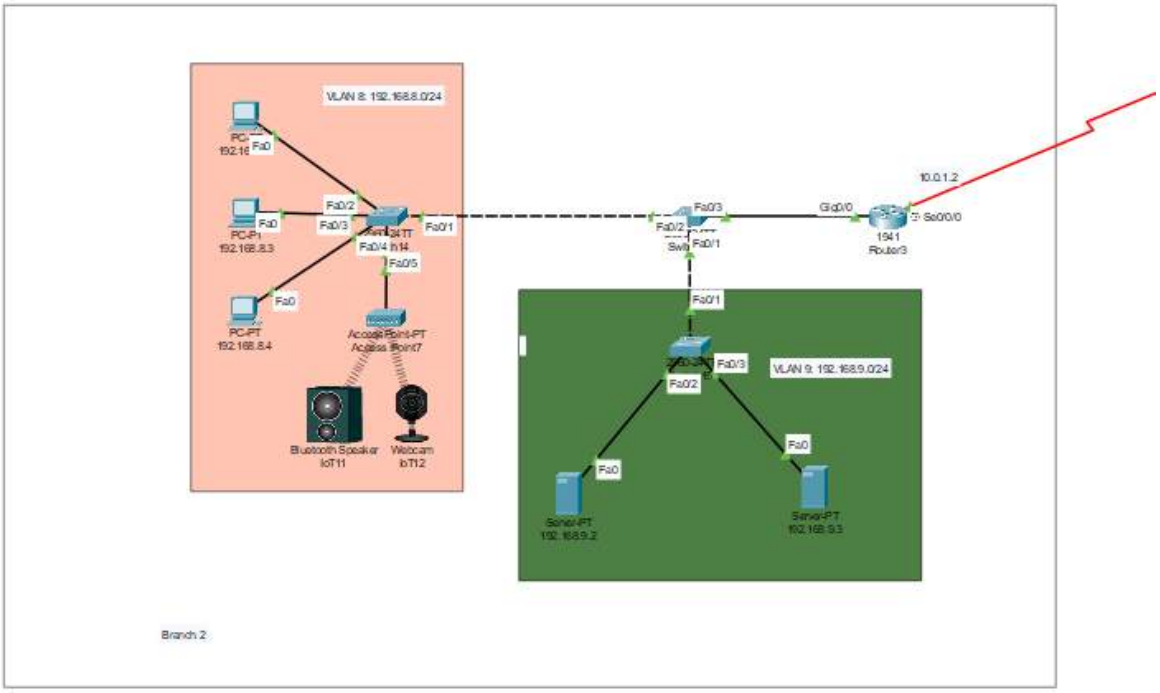
5.2 Main Site and Connection to the Internet



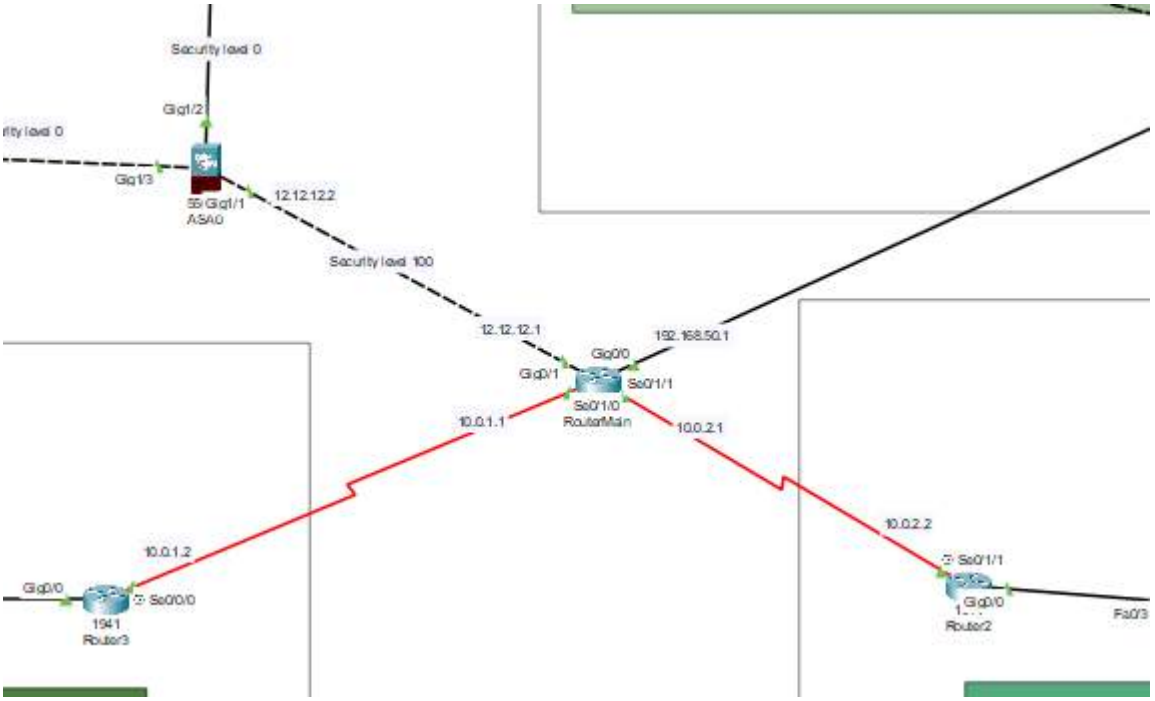
5.3 Branch 1



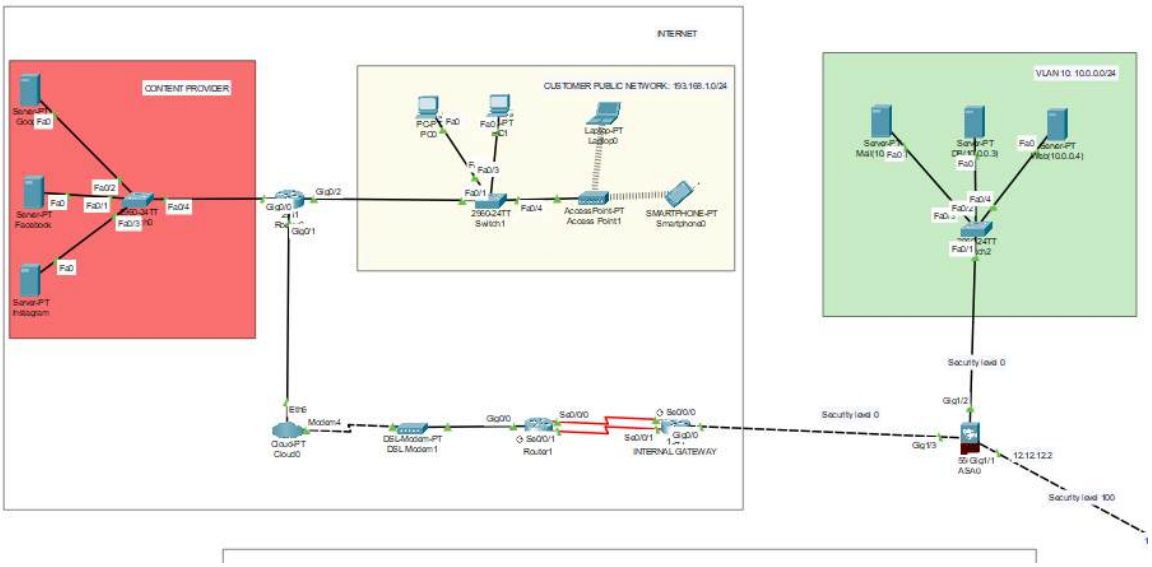
5.4 Branch 2



5.5 Connection between Sites



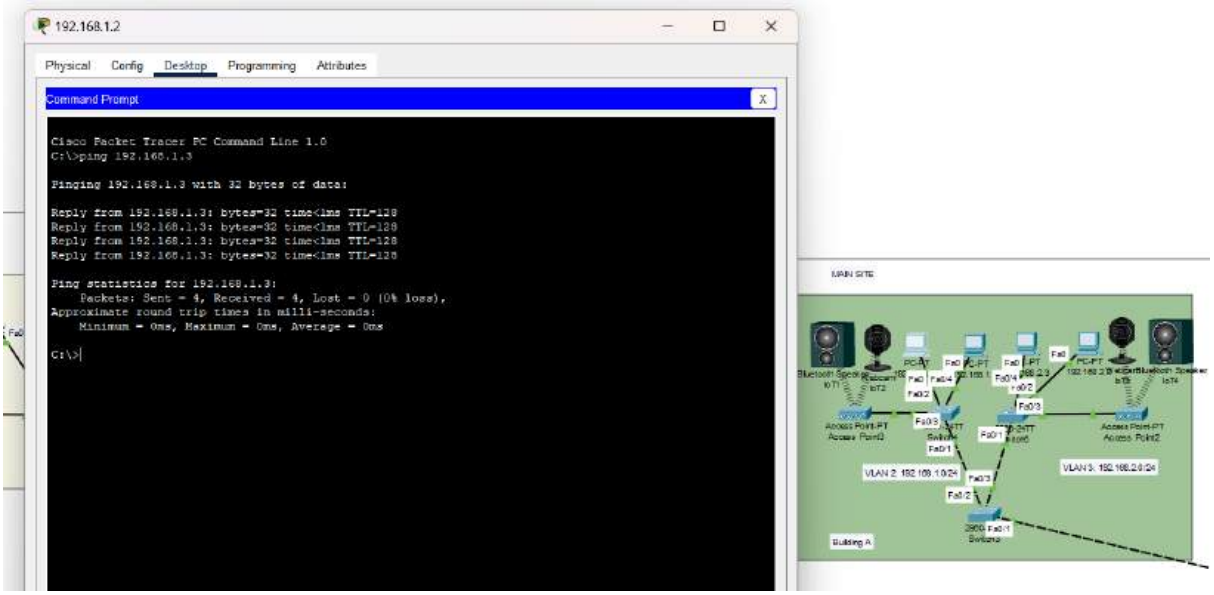
5.6 Internet



6. Test the System

6.1 Connect Between PCs in the Same VLAN

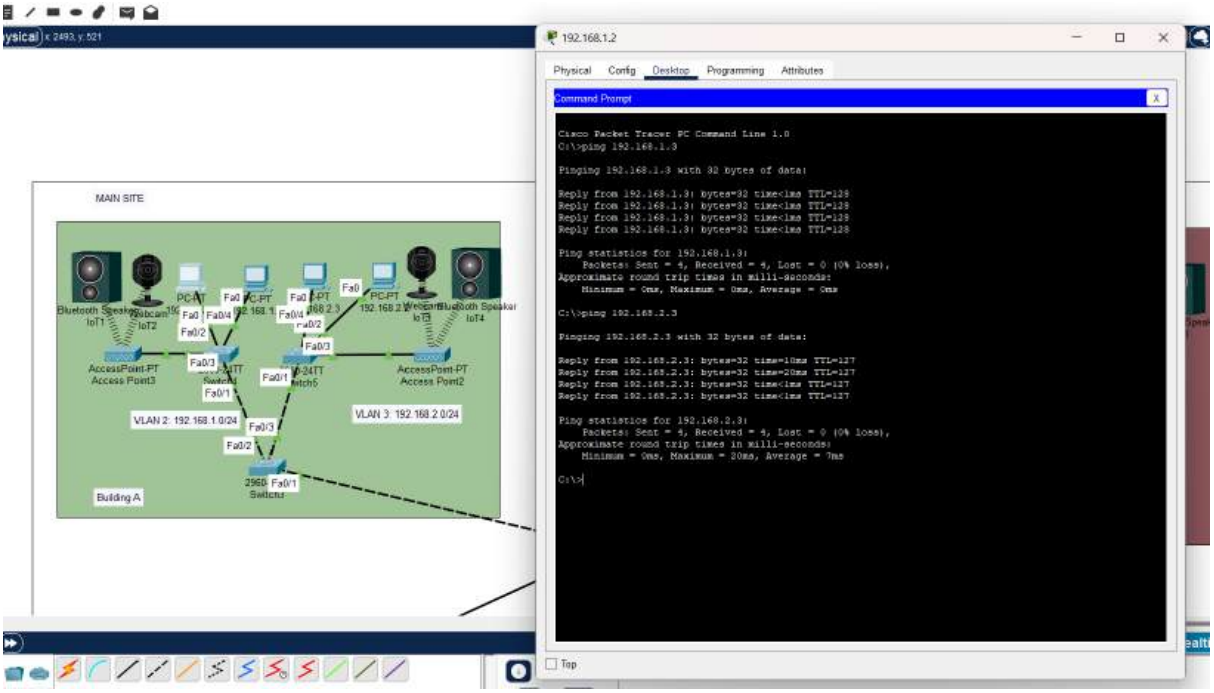
- Use `ping` between PCs in VLAN 2 (192.168.1.0/24) to test connectivity within the same subnet.
- If configured correctly, the ping should succeed, confirming basic internal connectivity.



6.2 Connect PCs Between VLANs

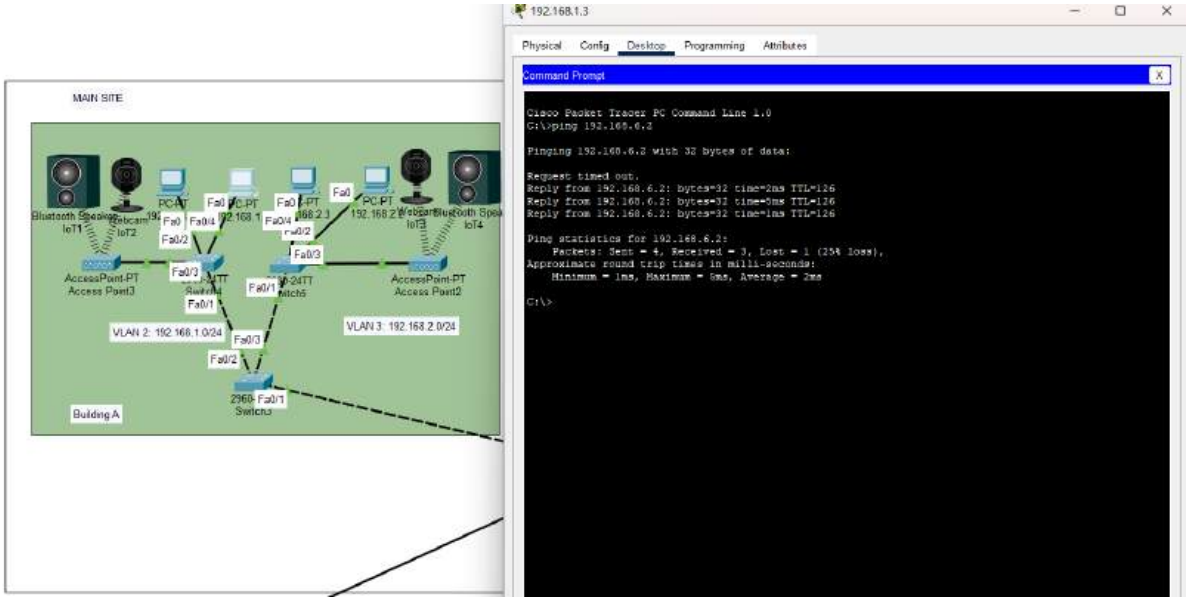
- Perform a `ping` test between PCs in VLAN 2 (192.168.1.0/24) and VLAN 3 (192.168.2.0/24).

- Ensure inter-VLAN routing is enabled on the router or Layer 3 switch for this communication to succeed.



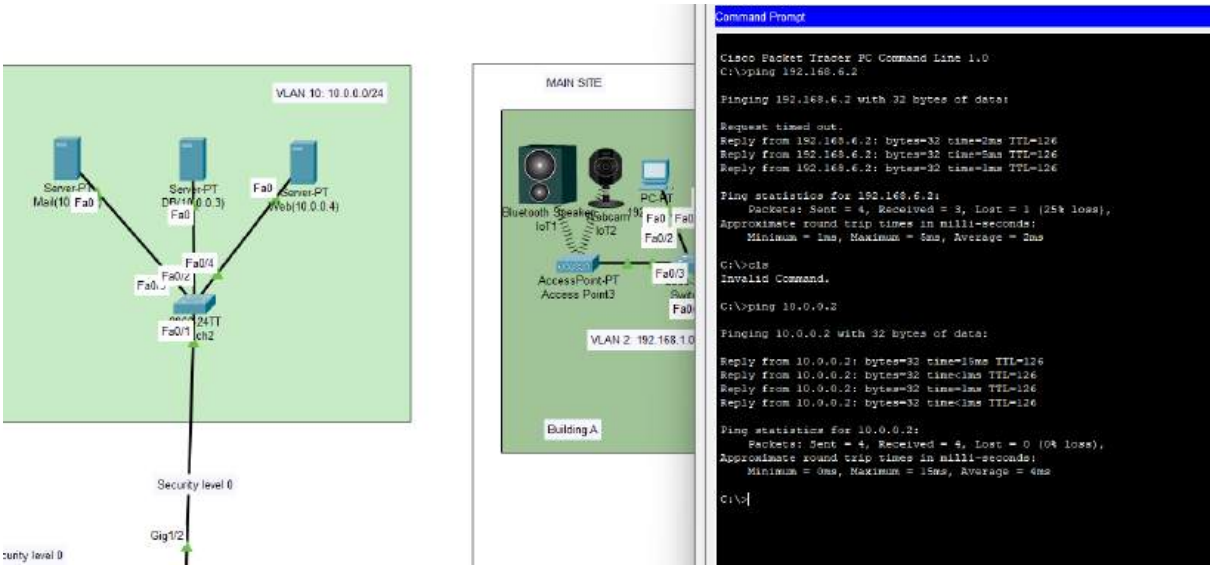
6.3 Connect PCs Between Main Site and Branch Sites

- Test connectivity between VLAN 2 (192.168.1.0/24) at the Main Site and VLAN 6 (192.168.6.0/24) at Branch Site 1.
- If using Packet Tracer, simulate this by placing routers between VLANs and adding appropriate routing entries to allow cross-site communication.



2. **Connect to Servers in the DMZ:**
   - Use `tracert` from a PC in VLAN 2 to a server in VLAN 10 (10.0.0.0/24).

- Configure the DMZ firewall rules to permit tracer packets, ensuring connectivity and controlled access to DMZ resources.



3. **No Connections from Customer Devices to PCs on the LAN:**
   - Test to confirm that customer devices, if present, cannot access internal LAN PCs by simulating a `ping` or `tracert` test.
   - Set up ACLs on the firewall or core router to block any unauthorized customer access to internal resources.

PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2E0:B0FF:FE79:C404
   IPv6 Address.....: ::
   IPv4 Address.....: 193.168.1.4
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 193.168.1.2

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.8.2

Pinging 192.168.8.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.8.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

7. Re-evaluate the designed network system through the following features: reliability, ease of upgrade, diverse support software, safety, network security, etc.

Reliability:

- **Strengths**: The network uses a star topology, which simplifies connections and provides centralized management for each branch.
- **Weaknesses**: The reliance on single routers and switches creates single points of failure at each branch. If any of these devices fails, the entire branch could lose connectivity.
- **Improvements**: Adding redundant paths or implementing failover mechanisms would improve reliability by providing alternative routes in case of hardware failure.

Performance:

- **Strengths**: The network design includes VLANs for segmenting traffic, which can reduce broadcast domains and improve internal traffic management.
- **Weaknesses**: VLAN routing depends on the "Router on a Stick" configuration, which can create a bottleneck, especially during high traffic loads. Additionally, the absence of load balancing at the gateway can lead to uneven traffic distribution between branches.
- **Improvements**: Replacing the Router on a Stick setup with multi-layer switches would enhance VLAN routing performance, while implementing load balancers at key points (such as the gateway) would help distribute traffic more evenly and reduce congestion.

Scalability:

- **Strengths**: The VLAN structure allows for some flexibility in expanding the network by adding more devices within existing VLANs.
- **Weaknesses**: The lack of redundancy and the reliance on legacy devices may hinder future network expansions and the integration of new technologies.
- **Improvements**: Upgrading legacy devices and ensuring that new equipment is compatible with current network protocols would enhance scalability. Additionally, implementing modular and redundant components would facilitate future network growth.

Security:

- **Strengths**: The design includes a firewall to filter traffic, providing a basic layer of protection for branch networks.
- **Weaknesses**: The firewall setup lacks advanced threat detection, and the network is vulnerable to IP spoofing attacks due to reliance on IP filtering alone. Additionally, only the DMZ at the Main Site is configured, while branch

servers are placed behind firewalls without a centralized DMZ, limiting resource sharing.
    - **Improvements**: Implementing a dual firewall system with an enhanced DMZ shared across branches would improve security. Introducing intrusion detection and prevention systems (IDPS) and implementing VPNs for secure remote access would further strengthen security.

Ease of Maintenance and Upgrades:

- **Strengths**: The centralized topology at each branch simplifies network management and maintenance.
- **Weaknesses**: Some legacy devices are no longer supported by the manufacturer, which complicates upgrades and limits the adoption of new technologies.
- **Improvements**: Replacing outdated devices with newer, supported models would simplify future upgrades and ensure compatibility with advanced features.

Redundancy and Backup:

- **Strengths**: The design has centralized connections, which can facilitate control over network traffic.
- **Weaknesses**: The network currently lacks backup servers and redundancy mechanisms, making it vulnerable to data loss and downtime in case of device failure.
- **Improvements**: Adding backup servers and redundant routing paths would enhance data availability and fault tolerance, ensuring continuous network operation even if a primary component fails.

Support for Additional Services:

- **Strengths**: The network design accommodates VLANs, which can support different types of traffic for services such as VoIP and internal communications.
- **Weaknesses**: There is no VPN solution for remote access, and the camera system is isolated within each branch, lacking centralized monitoring.
- **Improvements**: Implementing a VPN solution would enable secure remote access for teleworkers, and centralizing the camera system would improve security monitoring and provide a unified view across all branches.