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

COMPUTER NETWORKS LAB (CO3094)

Assignment 2

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

Advisor: Nguyễn Mạnh Thìn
Students: Phạm Duy Tường Phước - 2252662
Phan Hồng Quân - 2252685

HO CHI MINH CITY, MAY 2024

Contents

1 Member list & Workload

No.	Fullname	Student ID	Problems	Percentage
1	Phạm Duy Tường Phước	2252662	- Configure devices - Write report	50%
2	Phan Hồng Quân	2252685	- Configure devices - Write report	50%

2 Suitable network structures for buildings

2.1 Requirement analysis

- Using new technologies for network infrastructure including wired and wireless connection, fiber cabling (GPON), and GigaEthernet 1GbE/10GbE/40GbE.
- The network is organized according to the VLAN structure: That is, dividing the center's network into sub-networks for departments. Computers in each of these VLANs can access each other, but computers on the outside network will not be able to access the VLANs of these departments.
- The Main Site sub-network connects two other Sites by 2 leased lines (for WAN connection) and 2 DSLs (for Internet access) with a load-balancing mechanism.
- High security, robustness when problems occur, easy to upgrade the system.
- Hospital Network is estimated for a growth rate of 20% in 5 years (in terms of the number of users, network load, branch extensions, ..).

2.2 Solution

The whole network will be a LAN which connect to central router and Internet. This LAN will be divided into VLANS.

2.2.1 Main Site

We have 600 workstations which will be divided into 10 floors (5 floors for each building): each floor has 60 workstations, 3 servers is added for IT room located 50 meters from buildings A and B. Each floor has 10 rooms, therefore we decided to construct a switch for each room, and those switches connect to another switch in order to maintain a whole VLAN for that floor.

Since the number of workstations at each floor is not too much, we will use 20-24 port switches to make access switches for each floor, and the remaining ports can be used for future expansion.

In addition, we have placed servers in the data center 50 meters from the two buildings. Regarding the hospital's servers, our team found out that there are usually the following servers:

- Web server: People can access to get information about their accounts in the bank as well as other services.
- File server: to share the information.
- Mail server: to send and receive mail.
- DHCP Server: provides and assigns IP addresses for network devices.

- DNS server: translate domain names to IP addresses as requested.
- Database server: to store the database.
- Backup server: store backup's information.

For simplicity, we used 2 servers in this assignment. In addition, the company network connects to the Internet through an ASA firewall.

2.2.2 Auxiliary Sites

For 2 Auxiliary Sites, we have created structures for each Site as followed:

- The first floor is equipped with 3 servers. We created a VLAN for these servers by connecting them with a switch.
- The second floor is equipped with devices. Because we didn't know how many rooms and how many devices in each room, we simply assumed the second floor to have about 2 - 3 rooms. Therefore, we use 1 switch to connect all devices and create a VLAN for the floor. Departments can also easily expand their model by installing more PCs and switches in each room.
- We also set up the WiFi network for the second floor, in order to create a surveillance camera system for the Site and allow wireless devices to connect to the Internet.
- Two switchs for the VLANs are connected to another switch, in order to reduce congestion and easy to extend in the future.

Each Site has a router that connects the Site with the Main Site in order to exchange messages. We connect Sites together by 2 leased lines for WAN connection, in this network we used SD-WAN.

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?
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?
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?

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

Before diving into defining areas with high load to place load balancers, lets have a quick definition of a network load balancer.

Network Load Balancers distribute traffic based on variables like destination ports and IP addresses. Operating at OSI Layer 4, they lack context awareness for application-layer cues such as cookie data, content type, user location, custom headers, or application behavior. These balancers focus solely on network-layer information within directed packets.

Key advantages of Network Load Balancers include:

- Scalability to handle millions of requests per second for volatile workloads.
- Support for static IP addresses.
- Ability to assign one elastic IP address per enabled subnet.
- Support for registering targets, even those outside the VPC, using IP addresses.
- Ability to route requests on a single EC2 instance to multiple applications, registering each IP address or instance with multiple ports in the same target group.
- Support for independent monitoring of service health, with health checks defined at the target group level and numerous reported metrics.

Now the definition has been cleared, lets have a look at areas facing high load in this assignment. Areas with high network load include:

- The Internet gateway: all traffic to the internet passes through the hospital network, therefore the gateway of the entire hospital is dependent on this gateway. Therefore, the Internet gateway is a potential congestion point. **A load balancer should be put on the inside of the internet gateway**, to distribute the workload to the servers at the Auxiliary and the Main Site.
- The Main Site's subnet router: the traffic from the Main Site will be distributed to the two Auxiliary Sites, and from the two Auxiliary Sites to the Main Site, therefore, there will be a bottleneck at this position.

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

The implementation plan of the company's network is defined as follows:

1. **MAIN SITE**

   Note that the Main Site has two buildings A and B, therefore we decided to build networks for the two buildings similarly. In particular, each floor will have 10 rooms, each rooms will have the average of 6 devices, including PCs and wireless devices. In addition, two surveillance cameras are placed at two ends of the floor.

2. **OTHER SITES**

   1st floor. Server room and IT department

   - 3 public servers for load balancing with the Main Sites's public servers, 1 private server for internal uses.
   - 05 PCs for IT personnel.
   - 02 switches for cabling between the floors.
   - 01 routers with the leased DSL line.

   2nd floor: Patient services department

   - 20 PCs for nurses and doctors, 10 PCs for patients who do not have WiFi access.
   - 01 switch to connect the PCs.
   - 01 camera surveillance system.

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, ...)

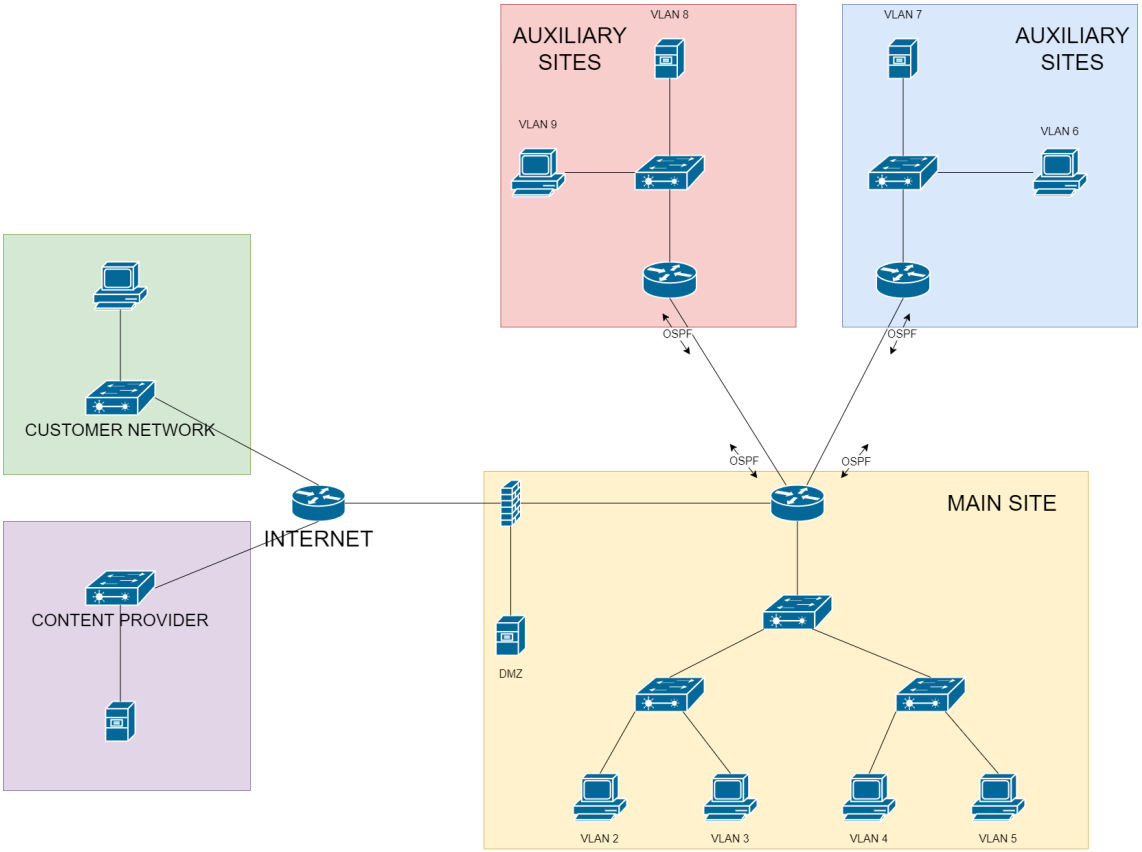

Figure 1: Our network demonstration

The network is partitioned as demonstrated in the above figure.

- A DMZ was set up to provide public access from the internet to the service servers.
- A firewall was set up between the Company private WAN and the external public network.
- Only permitted traffic (trusted server on the internet) from outside is able to go into 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. For core devices such as routers and firewalls, we proposed Cisco devices for reliability. For minor devices like access points, we

preferred using less expensive options like the one from Linksys. Edge devices like servers and workstations can be chosen by the bank themselves to suit their particular needs.

Device name	Technical specifications	Amount	Cost (May 2024)
The Cisco 1941 Router	**Product Code:** CISCO1941/K9 **Rack Units:** 2 RU **Interfaces:** 2 integrated 10/100/1000 Ethernet ports: GE0/0&GE0/1 **Expansion Slot(s):** • 2 enhanced High-Speed WAN Interface Card slots • 1 Internal Services Module slot **RAM:** 512 MB (installed) / 2 GB (max) **Flash Memory:** 256 MB (installed) / 8 GB (max) **Dimensions:** 34.3 cm x 29.2 cm x 8.9 cm **Package Weight:** 10.48 Kg	06	$3,482
Cisco WS-C2960-24TT L Switch	**Product Code:** Cisco WS-C2960-24TT-L **Ports:** 24 Ethernet 10/100 ports **Uplinks:** 2 Ethernet 10/100/1000 ports **VLAN IDs:** 4000 **Dimensions (H x W x D):** 4.4 x 44.5 x 23.6 cm **Weight:** 3.6 kg **Rack Height:** 1 RU	15	$2,869
Cisco ASA5506-BUN-k 9 Firewall	**Firewall Users:** 10 **Maximum firewall throughput (Mbps):** 150 **Maximum connections:** 10,000 **Maximum connections/second:** 3,000 **Packets per second (64 byte):** 85,000 **Integrated ports:** 8 port 10/100 switch with 2 Power over Ethernet ports **Maximum virtual interfaces (VLANs):** 3 (trunking disabled)	1	$595
Linksys Cloud Managed AX3600 WiFi 6 Indoor Wireless Access Point	• Dual-Band 802.11AX (2.4GHz + 5GHz) • 4x4:4 Internal Antennas for AX3600 Speeds (1200Mbps + 2400Mbps) • UL/DL OFDMA, 1024-QAM, Target Wake Time • BSS Coloring, Tx Beamforming • 802.3at PoE+ Support • Limited Lifetime Cloud Management • TAA Compliant	1	$399.99
Optical fiber cable & Copper cable supporting GigabitEthernet			
Optical fiber cable & Copper cable supporting FastEthernet			
Servers & Workstations	Selected by the hospital.		

Figure 2: Devices's information

IP addressing plan:
The connection between the IT cable room of the the Main Site and the firewall is 10.0.0.0/24. For private network, all hosts have IP address format as:

192.168.[VLAN].[HOST], where:

[**VLAN**] ranges from 1.. 254
[**host**] ranges from 2 .. 254

Additional rule:

- **Networking devices:** first available addresses within the range
- **Hosts:** last available addresses within the range
- All hosts in the Company private network are **assigned with a static IP address**.

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

1. Network **10.0.1.0/24** is for WAN communication on leased DSL between Main Site and the Auxiliary Site 1.
2. Network **10.0.2.0/24** is for WAN communication on leased DSL between Main Site and the Auxiliary Site 2.
3. Network **12.12.12.0/24** is for communication between the hospital and the firewall.
4. Network **8.8.8.0/24** is for communication between the firewall and Internet Gateway.

The summary of IP addresses is as follows:

Location	VLAN	Network IP address	Default Gateway
Main Site	002	192.168.1.0/24	192.168.1.1/24
Main Site	003	192.168.2.0/24	192.168.2.1/24
Main Site	004	192.168.10.0/24	192.168.10.1/24
Main Site	005	192.168.11.0/24	192.168.11.1/24
Auxiliary 1	006	192.168.6.0/24	192.168.6.1/24
Auxiliary 1	007	192.168.7.0/24	192.168.7.1/24
Auxiliary 2	008	192.168.8.0/24	192.168.8.1/24
Auxiliary 2	009	192.168.9.0/24	192.168.9.1/24
IT Cable Room (Main Site)	010	10.0.0.0/24	10.0.0.1/24

Figure 3: List of IP Subnets and Gateways

3.2 Schematic physical setup of the network

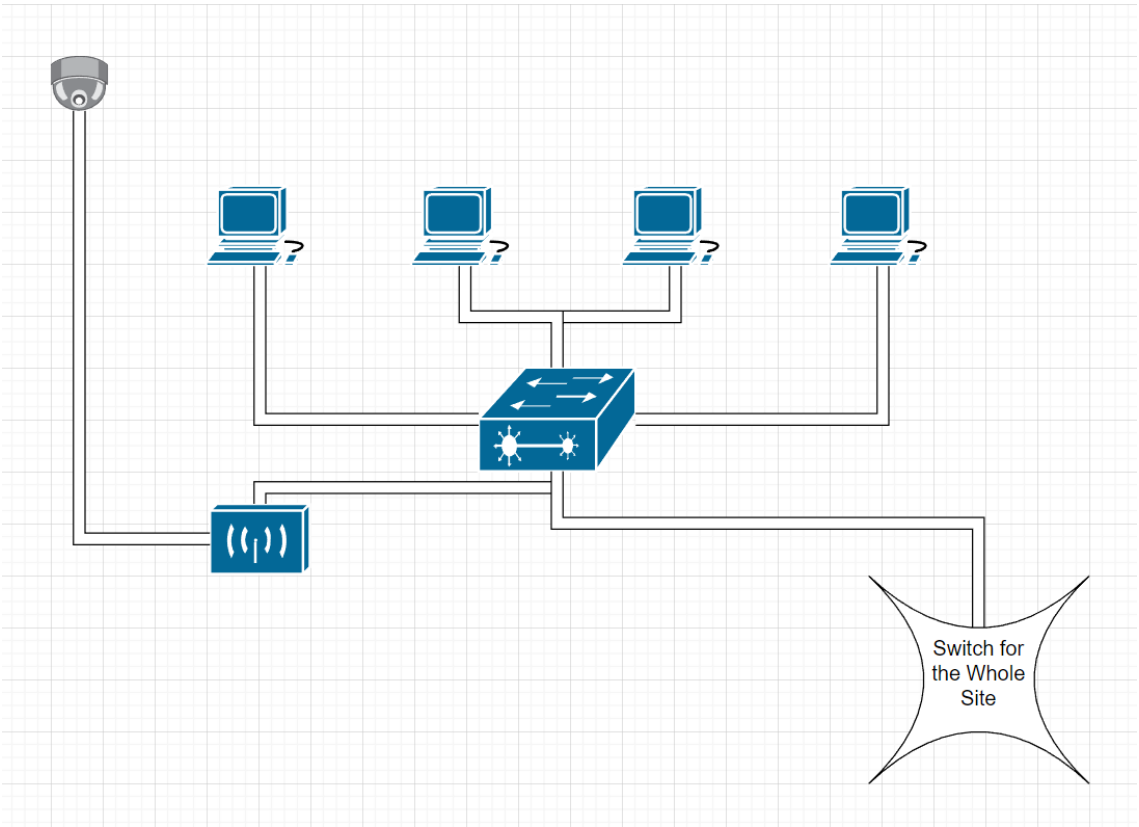

Figure 4: Physical wiring diagram of a typical building

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

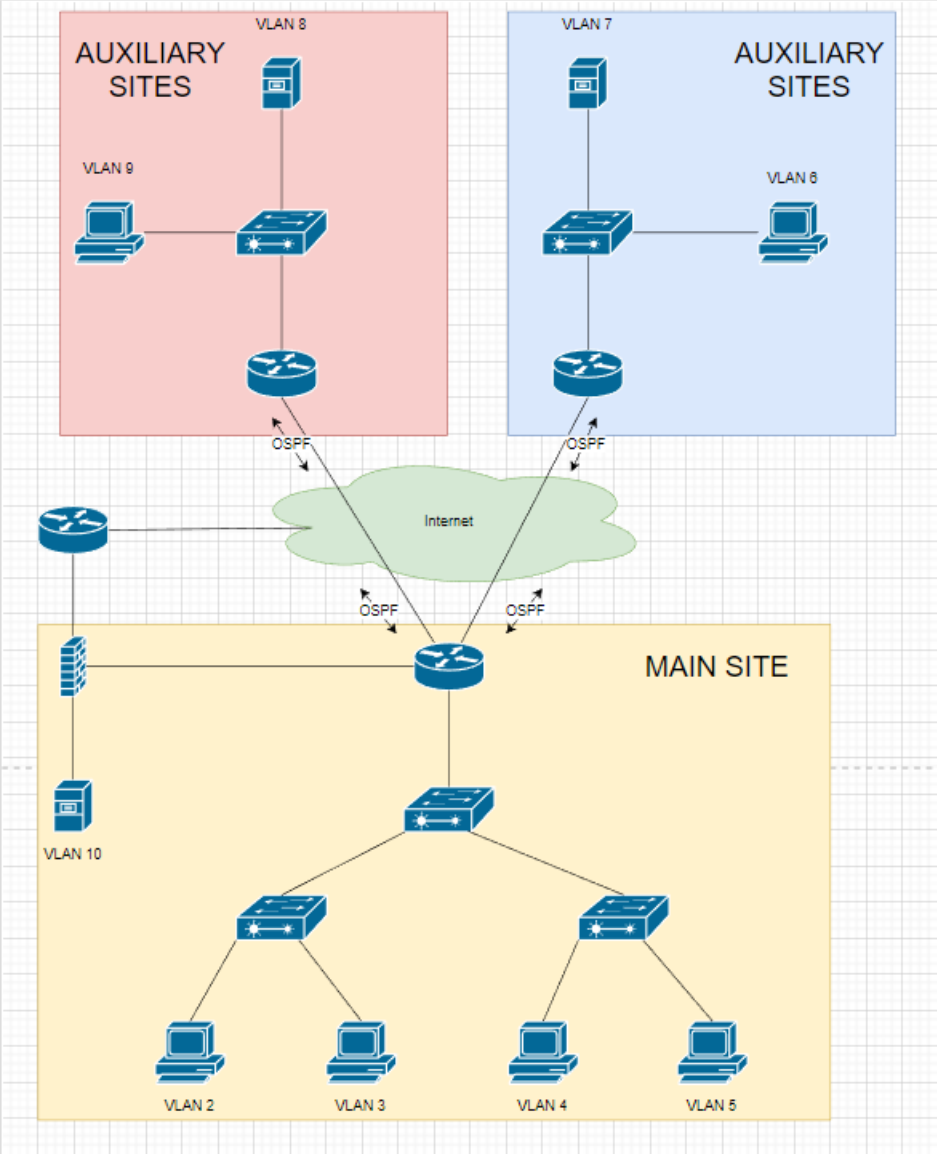

Figure 5: WAN Connection Diagram

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

Summary of the estimated data-flows and workload of the system:

- Each server total download: $D_s = 1000MB/day$
- Each server total upload: $U_s = 2000MB/day$
- Each workstation total download: $D_w = 500MB/day$
- Each workstation total upload: $U_w = 100MB/day$
- Total WiFi-connected devices download: $Data_WiFi = 500MB/day$
- Peak hours : 3 hours
- Network peak rate is 80% at peak hours
- Hospital's growth rate of 20% in 5 years

The formula of network:

- 1 MBps = $1MBps = \frac{8*2^{20}}{10^6}Mbps$
- The total data transfer:

$$Data = Number * (Upload + Download)$$

- Peak Hour Throughput (PHT):

$$Throughput = Data * \frac{Peak\ Rate}{Peak\ Time} = Data * \frac{0.8}{3*60*60} = \frac{Data}{13500}$$

- The minimum bandwidth for the next 5 years:

$$Bandwidth = Throughput * Growth\ Rate = Throughput * 1.2$$

4.1 Main Site

In wired Internet, there are

- **Number of server:** $N_s = 10$
- **Number of workstation:** $N_w = 600$:

The total data transfer by server:

$$\sum Data_{server} = N_s(D_s + U_s) = 12 * (1000 + 2000) = 36000(MB/day)$$

The total data transfer by workstation:

$$\sum Data_{workstation} = N_w(D_w + U_w) = 600 * (500 + 100) = 360000(MB/day)$$

The total data transfer in the Main Site:

$$\sum Data_{Main\ Site} = \sum Data_{server} + \sum Data_{workstation} + \sum Data_{WiFi} = 36000 + 360000 + 500 = 396500(MB/day)$$

The peak hour throughput in Main Site:

$$Throughput_{Main\ Site} = \sum \frac{Data_{Main\ Site}}{13500} = \frac{396500}{13500} = 29.3704(MBps)$$

The minimum bandwidth of the Main Site:

$$Bandwidth_{Main\ Site} = Throughput_{Main\ Site} * 1.2 = 29.3704 * 1.2 = 35.2444(MBps)$$

4.2 Auxiliary Sites

In wired Internet, there are

- **Number of servers:** $N_s = 2$
- **Number of workstations:** $N_w = 60$:

The total data transfer by server:

$$\sum Data_{server} = N_s(D_s + U_s) = 2 * (1000 + 2000) = 6000(MB/day)$$

The total data transfer by workstation:

$$\sum Data_{workstation} = N_w(D_w + U_w) = 60 * (500 + 100) = 36000(MB/day)$$

The total data transfer in an Auxiliary Site:

$$\sum Data_{Auxiliary\ Site} = \sum Data_{server} + \sum Data_{workstation} + \sum Data_{WiFi} = 6000 + 36000 + 500 = 42500(MB/day)$$

The peak hour throughput in Auxiliary Site:

$$Throughput_{Auxiliary\ Site} = \sum \frac{Data_{Auxiliary\ Site}}{13500} = \frac{42500}{13500} = 3.1481(MBps) = 25.1852(Mbps)$$

The minimum bandwidth of headquarters:

$$Bandwidth_{Auxiliary\ Site} = Throughput_{Auxiliary\ Site} * 1.2 = 3.1481 * 1.2 = 3.7777(MBps) = 30.2218(Mbps)$$

4.3 Suggest the configuration for the hospital network

- From the expected bandwidth, the ISP lease line from each branch should be 40 Mbps, which scales well for the company for the next ten years.
- From the FPT internet leased line, we could rent the 16 millions VNĐ/month package

Bảng giá dịch Internet Leased Line FPT

Gói	Tốc độ kênh	Cước phí
Cước thuê Leased Line Internet	512 Kbps quốc tế và 10 Mbps trong nước	10,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 10 Mbps trong nước	12,000,000
Cước thuê Leased Line Internet	512 Kbps quốc tế và 20 Mbps trong nước	12,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 20Mbps trong nước	14,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 30Mbps trong nước	15,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 40Mbps trong nước	16,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 50Mbps trong nước	17,000,000
Cước thuê Leased Line Internet	02 Mbps quốc tế và 30Mbps trong nước	17,500,000
Cước thuê Leased Line Internet	02 Mbps quốc tế và 40Mbps trong nước	18,000,000

Figure 6: Price for Internet leased line by FPT

5 Design the network map using Packet Tracer

Due to limited space on Cisco Packet Tracer, the simulation network does not contain all floors, all workstations and servers. Instead, the design was simplified only for demonstration purposes. However, this network contains enough characteristics to simulate the actual network, supporting sufficient networking features.

5.1 Overall structure of the network

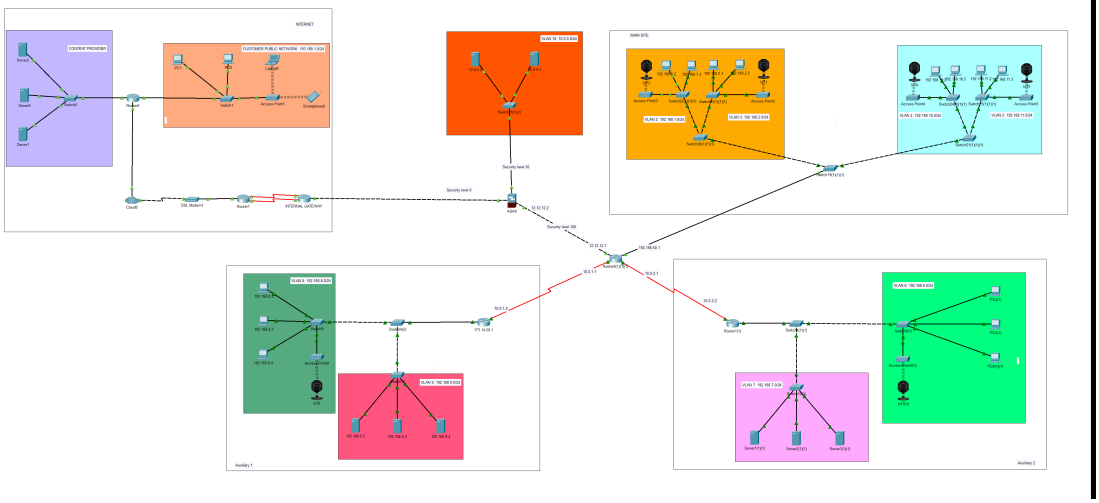

Figure 7: The structure of our network

5.2 Main Site and Connection to the Internet

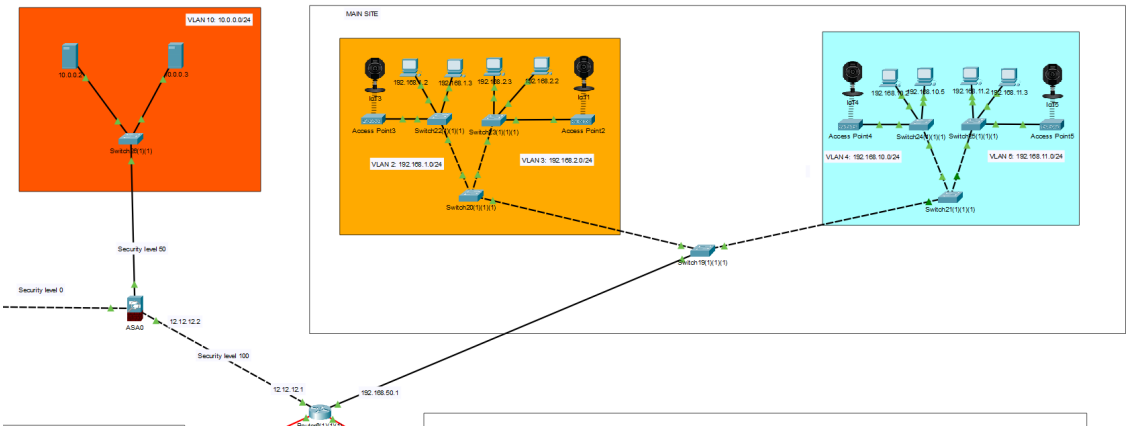

Figure 8: The Main Site

5.3 Auxiliary 1

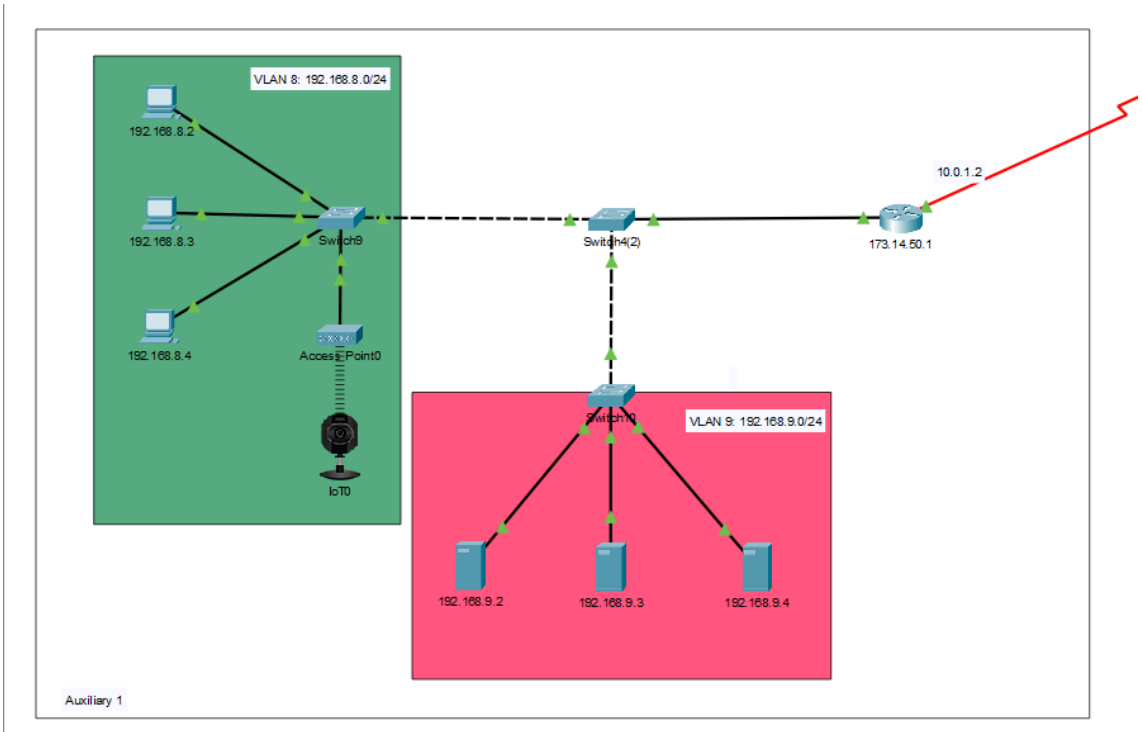

Figure 9: The Auxiliary 1

5.4 Auxiliary 2

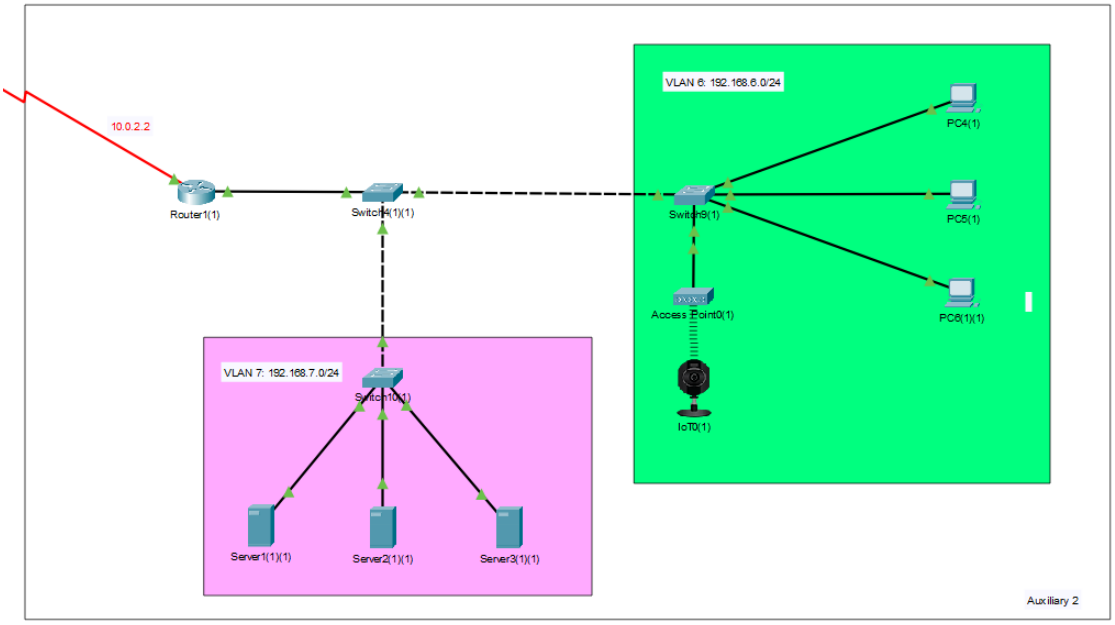

Figure 10: The Auxiliary 2

5.5 Connection between Sites

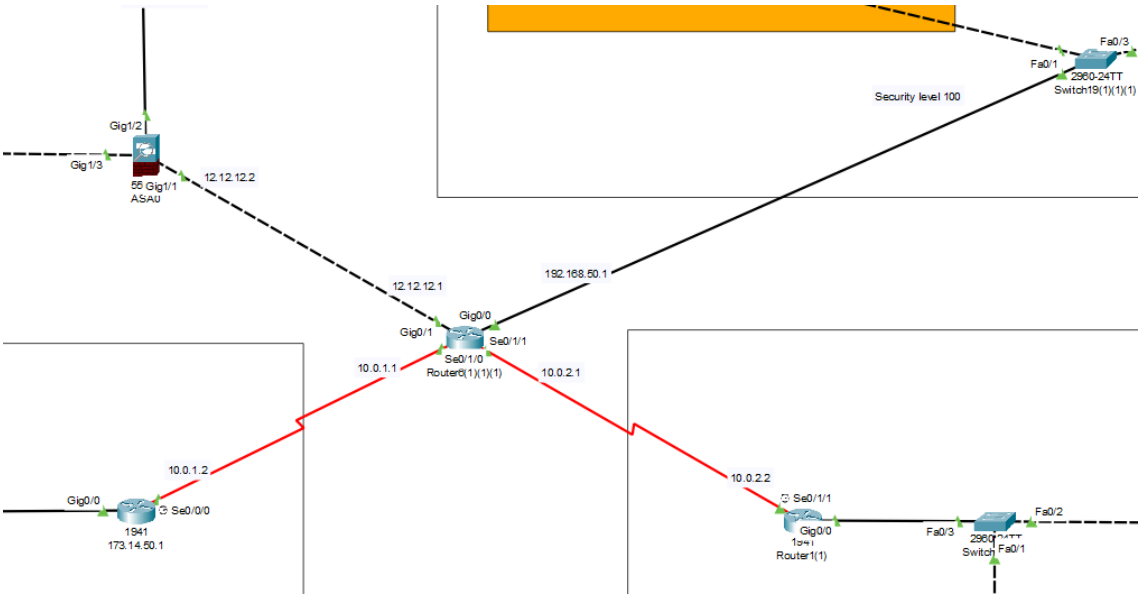

Figure 11: Connection between three Sites

5.6 Internet

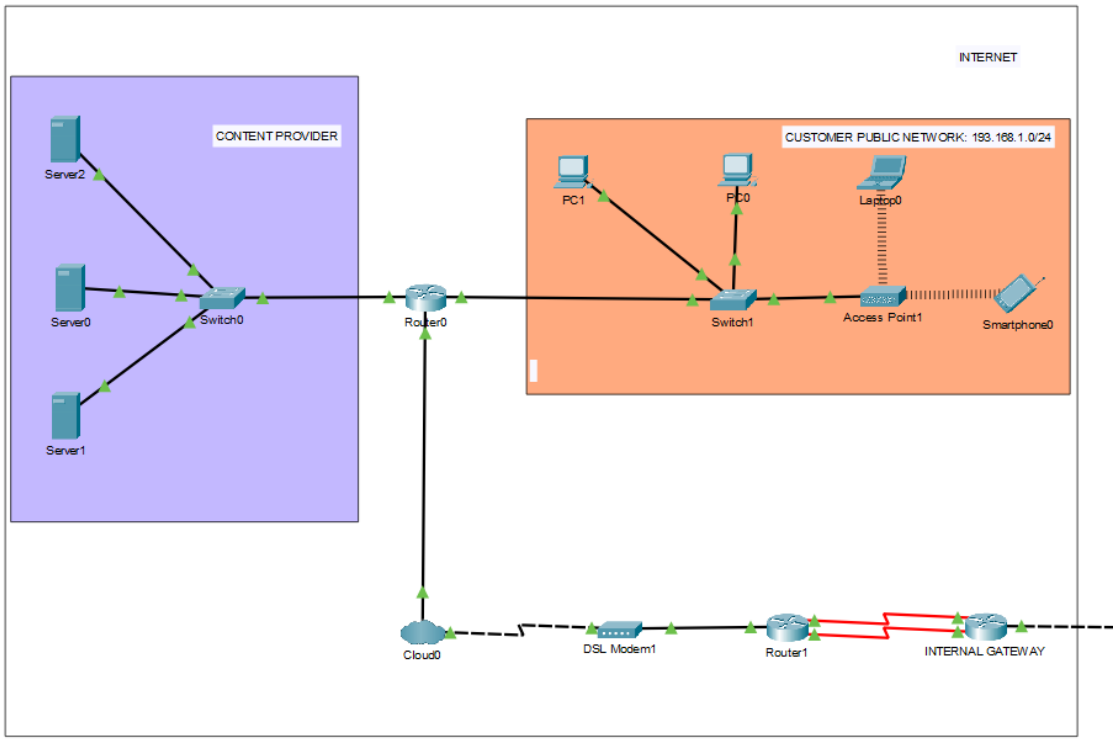

Figure 12: The Internet

6 Test the system

6.1 Connect between PCs in the same VLAN

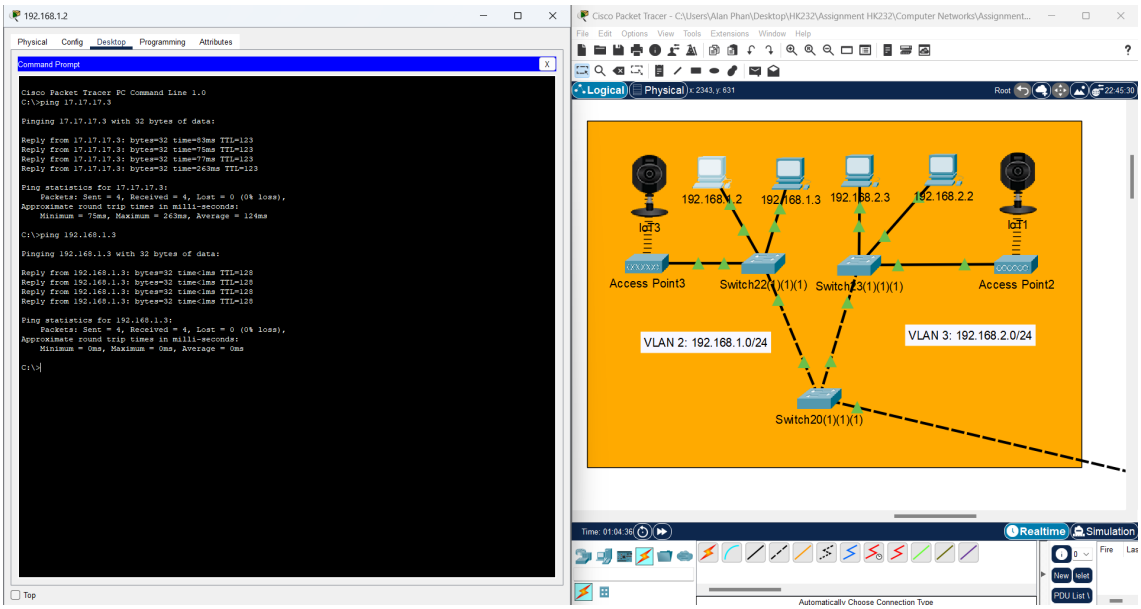

Figure 13: Ping PCs in the same VLAN

- The experiment was carried out within VLAN 2 (192.168.1.0/24) computers.

6.2 Connect PCs between VLANs

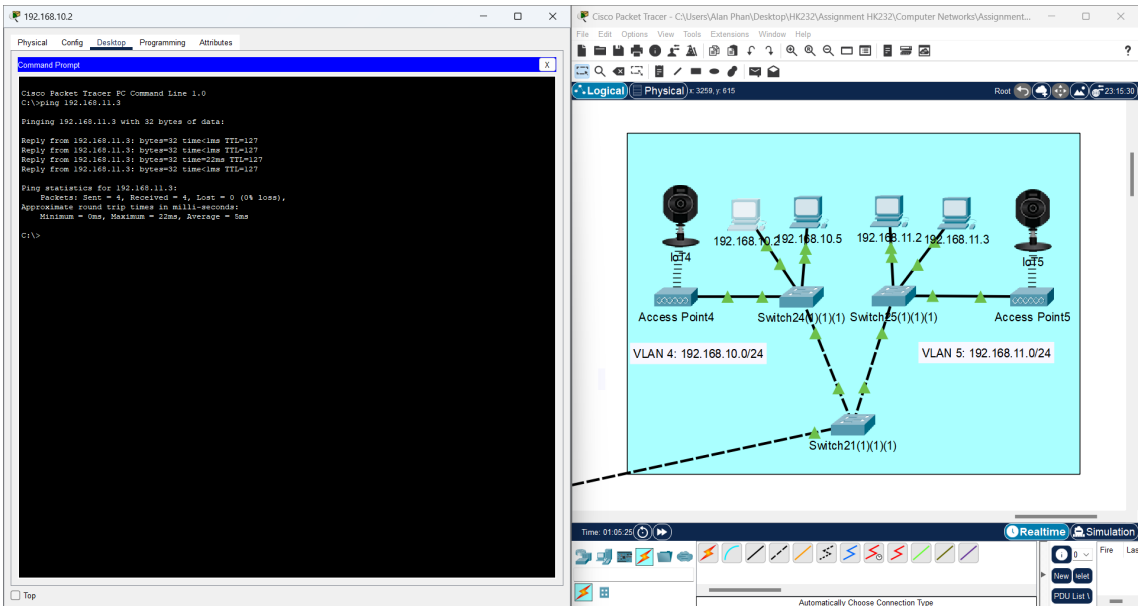

Figure 14: Ping PCs between VLANs

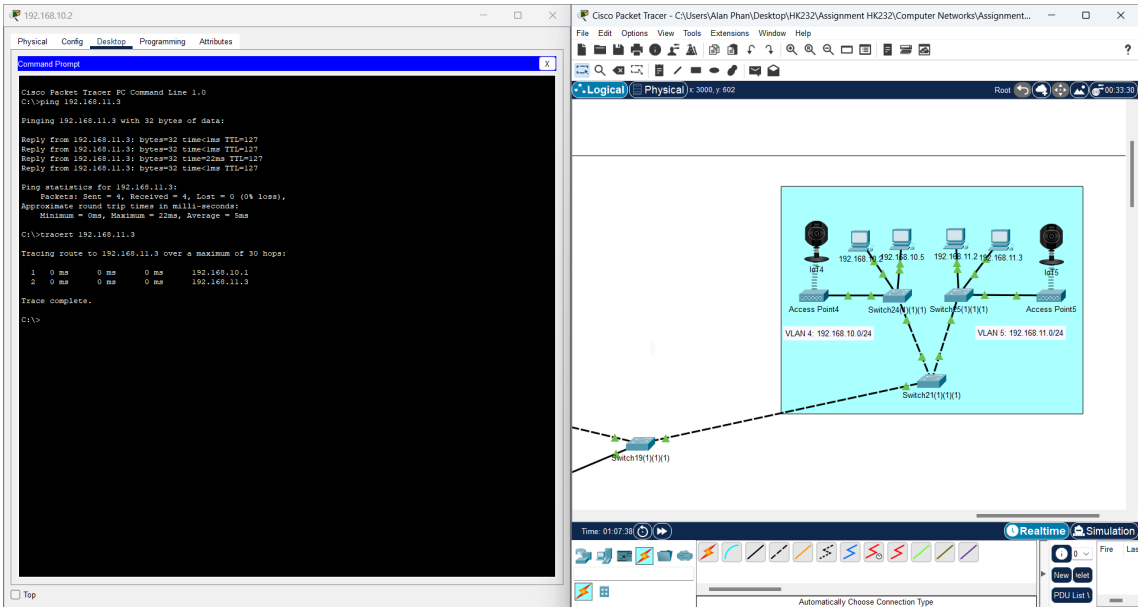

Figure 15: Tracert PCs between VLANs

- The experiment was carried out between VLAN 2 (192.168.1.0/24) and VLAN 3 (192.168.2.0/24) in the Main Site using ping and traceroute.

6.3 Connect PCs between the Main Site and the two Auxiliary Sites

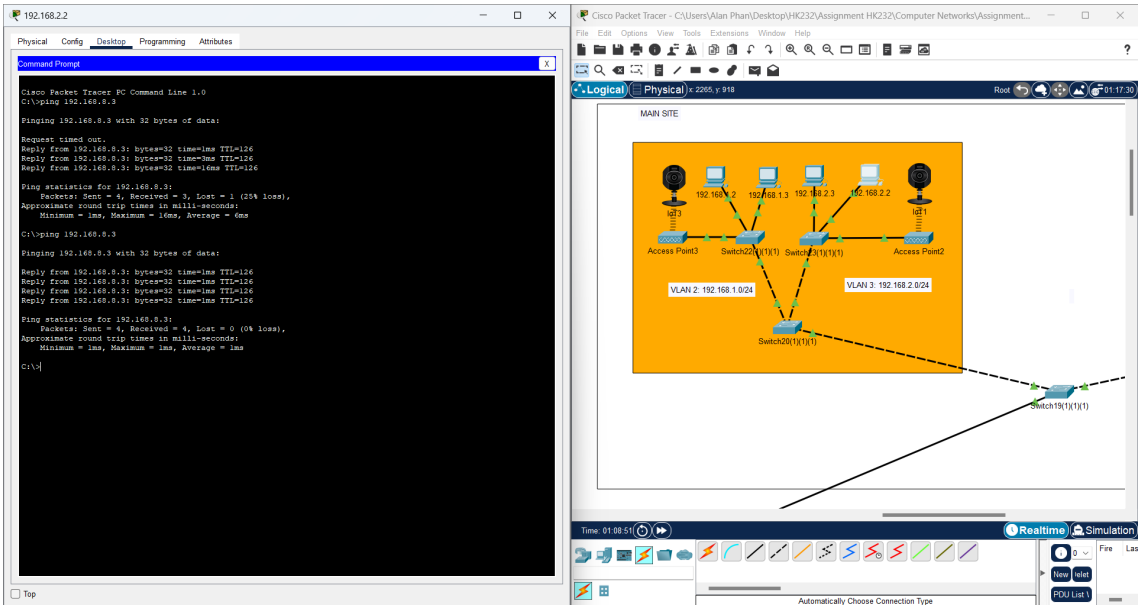

Figure 16: Ping PCs between Sites

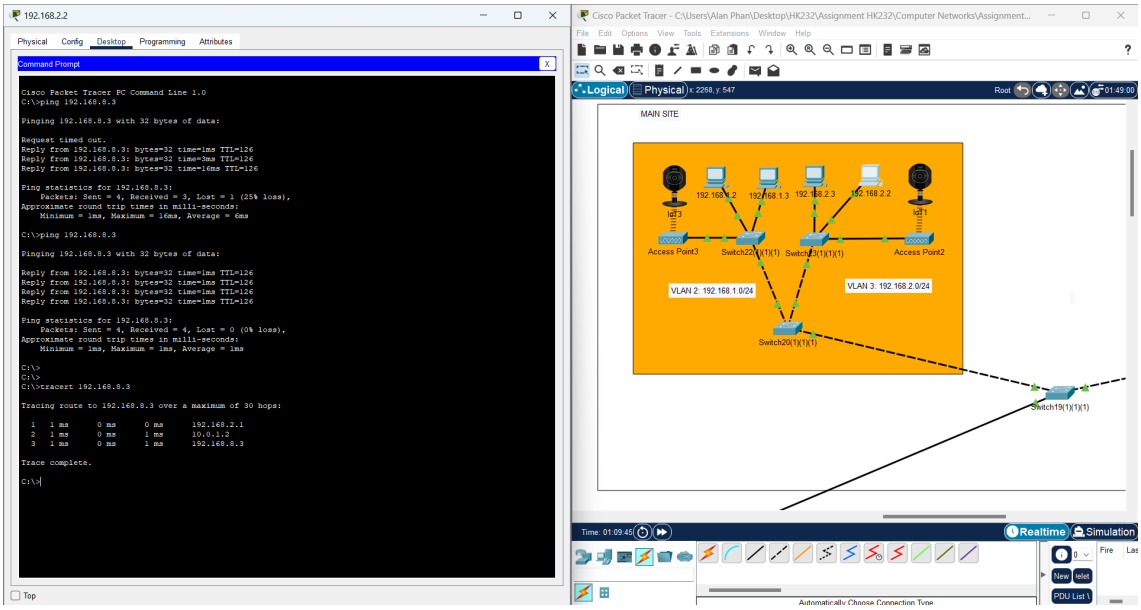

Figure 17: Tracert PCs between Sites

- The experiment was carried out between VLAN 3 (192.168.2.0/24) of the Main Site and VLAN 8 (192.168.8.0/24) of Auxiliary 1 using both ping and traceroute.

6.4 Connect to servers in the DMZ

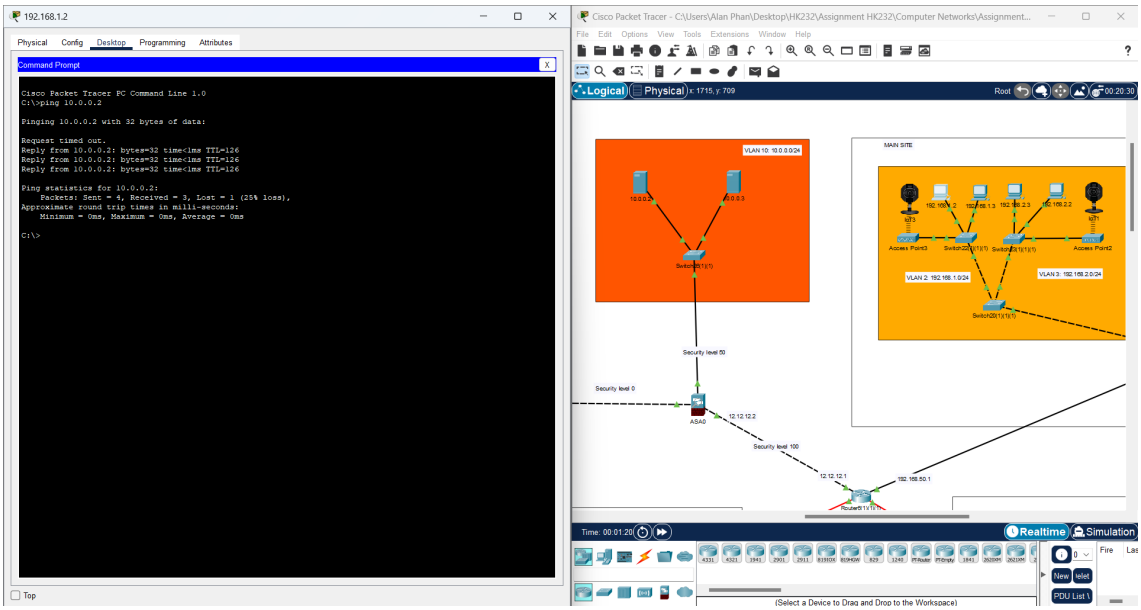

Figure 18: Ping servers in the DMZ

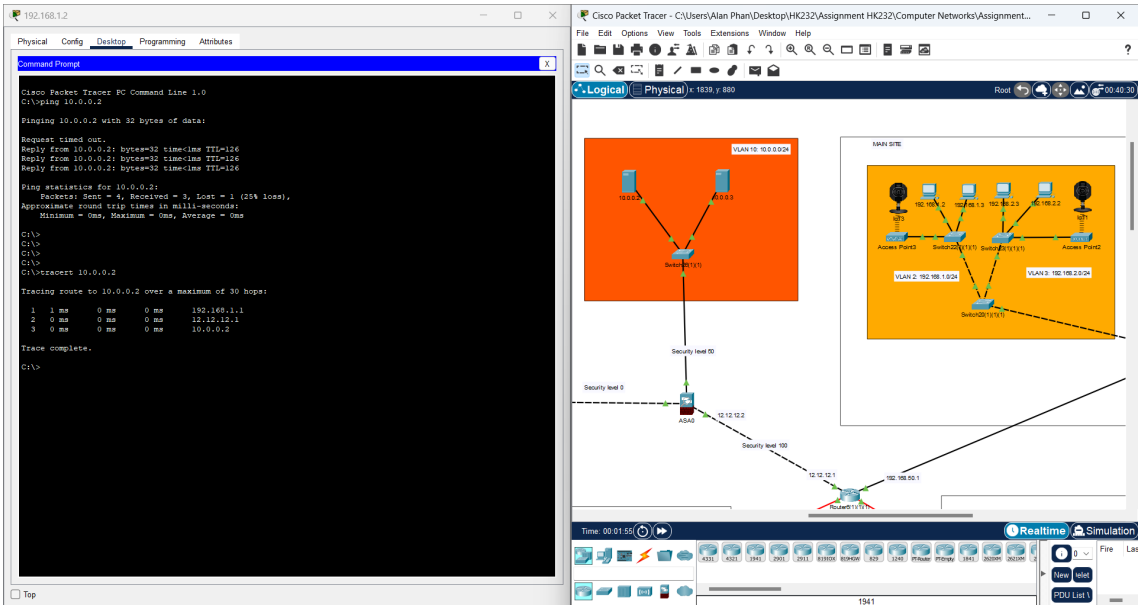

Figure 19: Tracert servers in the DMZ

- The experiment was carried out between VLAN 2 (192.168.1.0/24) of the Main Site and VLAN 10 (10.0.0.0/24) of the DMZ using both ping and traceroute.

6.5 No connections from Customers' devices to PCs on the LAN

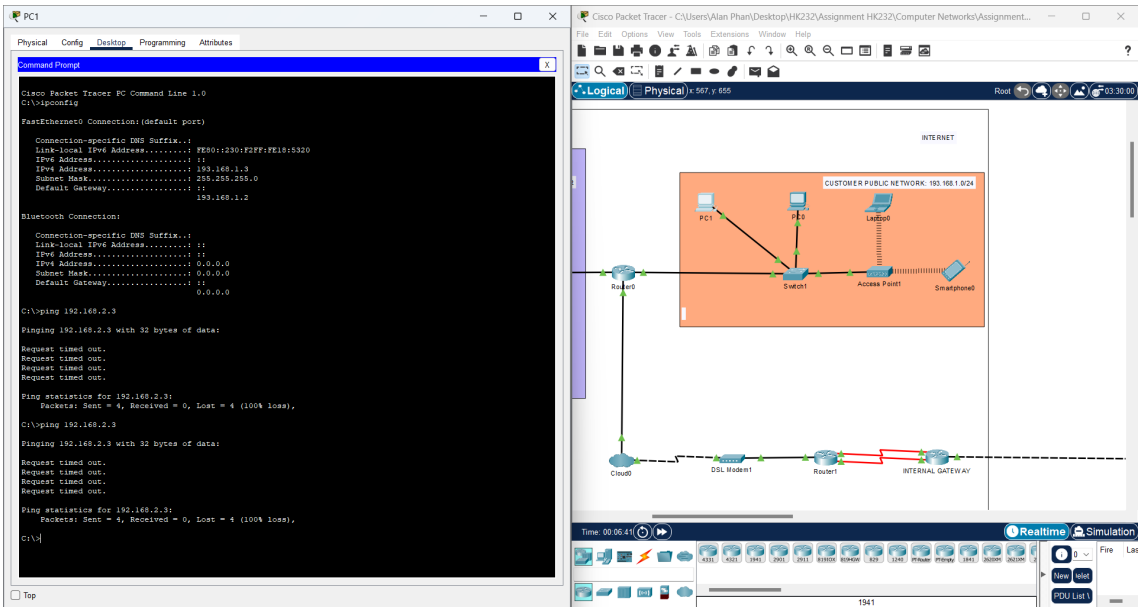

Figure 20: Ping from Customer's network to PCs on the LAN

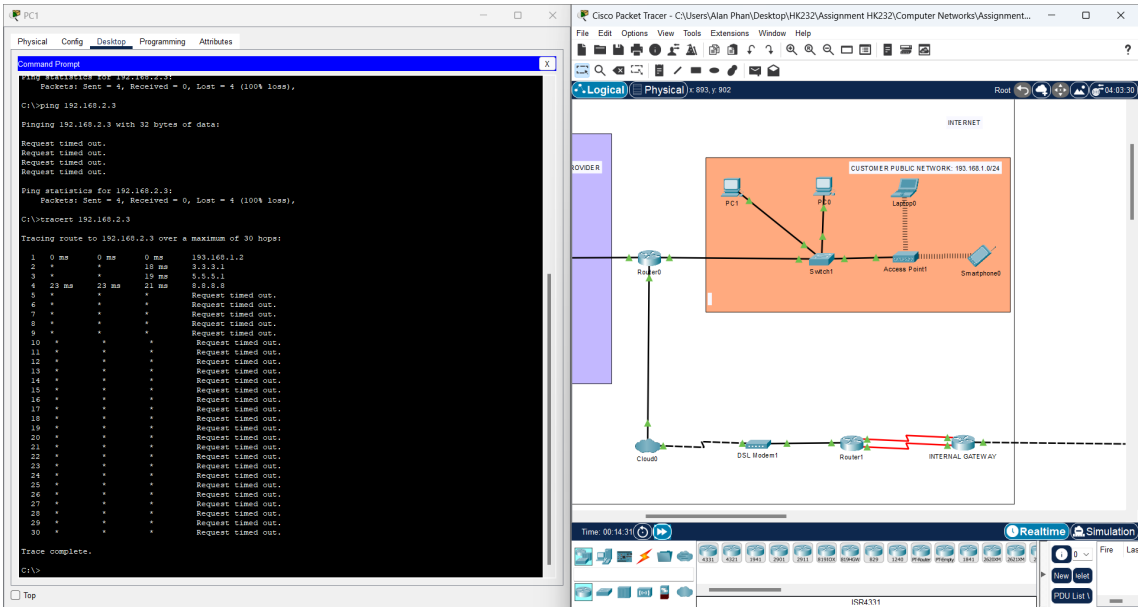

Figure 21: Tracert from Customer's network to PCs on the LAN

- The experiment was carried out between a PC in Customer's network (193.168.1.0/24) and VLAN 3 (192.168.2.0/24) of the Main Site using both ping and traceroute.

6.6 Connect the Internet to a Web server

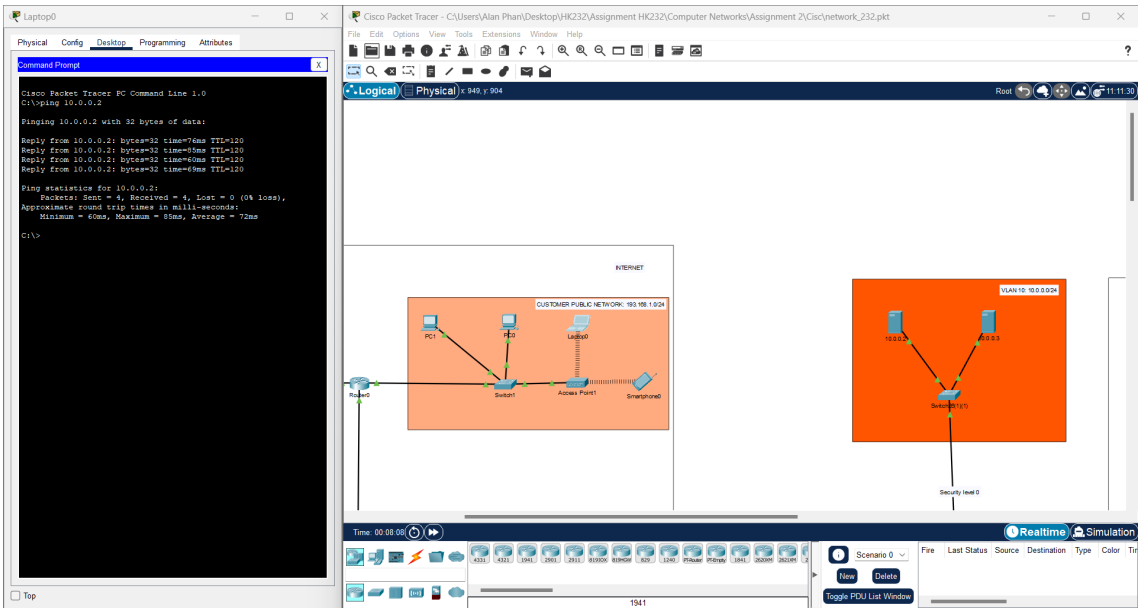

Figure 22: Ping from laptop of the customer network to DMZ

- The experiment was carried out between a wireless laptop in Customer Public Network, pinging to the server in the DMZ.

7 Re-evaluate the designed network system through the features:

7.1 The remaining problems for the project

1. ***Reliability***
   - There is a single point of failure at the switches and routers due to Star Topology.
   - The network does not possess a backup mechanism. Thus, the chance of losing the packet is high.
   - The VLANs routing heavily depends on one-armed routers.
2. ***Performance***
   - The routing between VLANs is done using the Router on a Stick method, creating a potential bottleneck at these one-armed routers.
   - There is no load balancer implemented at the Gateway, the workload is not distributed between the branches.
   - All traffic passes through one router at the Main Site, making it a potential congestion point.

3. ***Ease of Upgrade***
    - The network contains some legacy Cisco devices no longer supported by Cisco, upgrading the network to adopt new technologies could be a challenge.
4. ***Security***
    - Only the DMZ at the Main Site can be simulated, the servers at the branches were put behind the firewall thus they do not belong to the DMZ, and the workload can not be shared.
    - Firewall filters the IP traffic, thus making the network vulnerable to IP spoofing.
5. ***Features***
    - Lack of VPN for teleworkers.
    - Load balancing not yet implemented due to single firewall mechanism.
    - Cross-branch camera system not yet implemented, each branch has its own camera system.

7.2 Development orientation in the future

1. Router on a Stick method should be replaced by Multi-layer Switches. This reduces the congestion point on one-armed routers and provides better performance via wire-speed data traversal when routing between VLANs.
2. Implement Dual Firewall mechanism for proper separation DMZ, allowing DMZ to be shared across branches for load balancing.
3. Implement a load balancing mechanism to ensure the availability of the network during peak hours.
4. Implement multiple routes between the network to avoid congestion and connection risks.
5. Implement Backup Servers to maintain reliable data transfer on the network.

References

[1] Price for Internet leased line by FP - https://mangfpt.vn/leased-line-fpt/

[2] "Configuring an ASA Firewall on Cisco Packet Tracer - Part One" - https://www.youtube.com/watch?v=SLZS1mSc_VY

[3] "Configuring an ASA Firewall on Cisco Packet Tracer - Part TWO" - https://www.youtube.com/watch?v=uJfI69mGUeU

[4] "Configuring an ASA Firewall on Cisco Packet Tracer - Part THREE" - https://www.youtube.com/watch?v=IQI-Rv8cmYM

[5] "Configuring an ASA Firewall on Cisco Packet Tracer - Part FOUR" - https://www.youtube.com/watch?v=pBW1X6r5kNM

[6] "Cisco Packet Tracer Tutorial For Beginners [FULL COURSE]" - https://www.youtube.com/watch?v=ty0HMs48U1k&list=PLVFyjfF2Drdt7aqDk8XdTEPUXcDu5ePg7

[7] "Lab 1- Hướng dẫn cấu hình Router" - https://www.youtube.com/watch?v=uA4NKQQ002s

[8] "Cisco Packet tracer Router configuration step by step" - https://www.youtube.com/watch?v=69bT6bRM-LQ