VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY

HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY

COMPUTER NETWORK

ASSIGNMENT 1

DEVELOP A NETWORK APPLICATION

CC02 — SEMESTER 231

LECTURER : Prof. NGUYEN LE DUY LAI

Student	ID	Marks
Bành Tân Thuận	2153011	100%
Lê Trần Nguyên Khoa	2152674	100%
Trần Minh Triết	2153057	100%

HO CHI MINH CITY – 2023

TABLE OF CONTENTS

1. Step 1 (1 point): Find out suitable network structures for buildings.....3
a. Analyze the network system requirements of Headquarters and Branches.....3
b. Make a checklist to be surveyed at the installation locations.....3
c. Define areas with high load (network load) to select the appropriate device configuration (load balancers are placed in necessary locations).....4
d. Choose a network structure that matches the building's architecture with convenience and aesthetics..... 5
e. 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, ...).....7
2. Step 2 (1 point): List of minimum equipment, IP plan, and wiring diagram (cabling).....9
a. List of recommended equipment and typical specifications & IP plan.....9
b. Schematic physical setup of the network..... 13
c. WAN connection diagram between Headquarters and Branches (using new WAN..... 13
3. Step 3 (1 point): Calculate the required throughput, and expected bandwidth from ISP, then suggest the configuration for the company network..... 15
4. Step 4 (2 points): Design the network map using Packet Tracer or GNS3 simulation software.. 17
1. Overall structure of the network.....17
2. HCM Headquarters & Connection to the internet.....18
3. Danang Branch..... 19
4. Hanoi Branch.....20
5. Connection between branches.....20
6. Internet, ISP and Content Provider.....21
5. Step 5 (2 points): Test the system with popular tools such as ping, and traceroute, etc. on the simulated system. (modify only what have changed)..... 22
1. Connect between PCs in the same VLAN.....22
2. Connect PCs between VLANs..... 22
3. Connect PCs between Headquarters and branches.....23
4. Connect to servers in the DMZ..... 24
5. No connections from Customers' devices to PCs on the LAN..... 26
7. Connect the Internet to a Web server.....26
6. Step 6 (2 points): Re-evaluate the designed network system through the following features: reliability, ease of upgrade, diverse support software, safety, network security, etc.....27
Remaining problems of the project..... 27
Development orientation in the future.....27

1. Step 1 (1 point): Find out suitable network structures for buildings

a. Analyze the network system requirements of Headquarters and Branches

Functional requirements

- *The Headquarters*: network infrastructure must use new technologies including wired and wireless, fiber cabling and GigaEthernet 1GbE/10GbE.
- *The Headquarters*: 7 floors, 120 workstations, 5 servers, 12 networking devices and security devices.
- *The Branches*: 2 floors, 30 workstations, 3 servers, 5 networking devices.
- Use a mix of licensed and open-source software.
- The Headquarters and the Branches are connected through leased WAN links.
- Network is divided into 3 subnets for The Headquarters and the Branches.
- All traffic to the Internet passes through the Headquarters subnet.
- Have separate servers for software updates, web access, and database access, etc.
- Work stations for Web browsing, document downloads, and customer transactions.

Non-functional requirements

- Shared dataflow and workload balancing between the Headquarters and the Branches.
- Cope with the company's growth rate of 20% in 5 years.
- High security, high availability, robustness when problems occur, ease of upgrading
- The total download estimation is about 1000 MB/day and the upload estimate is 2000 MB/day.
- The total download estimation is about 500 MB/day and the upload estimation is 100 MB/day.
- WiFi-connected devices from customers' access for downloading are about 500 MB/day.

b. Make a checklist to be surveyed at the installation locations

On-site survey:

Category 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?

Category 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 banking services need networking facilities, and what are they?

Category 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 (group, department, employee, customer, etc.)
- Does the company accept the proposed list of devices and equipment and associated cost?
- How flexible is the company about the additional cost?

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

Network Load Balancers:

- 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.

Areas with high network load include:

- *Headquarters internet gateway*: all traffic to the internet passes through the Headquarters subnet, therefore the gateway of the entire company WAN is dependent on this gateway. Therefore, the Headquarters 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 branches and the Headquarters.
- *Headquarters subnet router*: the traffic from the headquarters will be distributed to the two branches, and from the two branches to the headquarters, therefore, there will be a bottleneck at this position.

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

Since the installation locations are buildings with many vertical floors, it is better to put a single “brain” in the ground floor (IT Room and Cabling Central Local) for ease of management aesthetics of other floors. (1) Disaster-recovery is also easier, since the ground floor is easier to access for humans. (2) Also the loss could be mitigated in case of fire, which happens frequently in big cities like HCM, Hanoi and Danang, since fire always goes upward.

For the above reasons, we chose the **Star Topology** between the floors. In detail, the servers and core networking devices of a branch are put at the ground floor, each floor contains one switch to distribute the network to hosts, and there will be a central switch that connects all switches from floors.

Instead of using the Multilayer Switch as a central switch, we adopted the **Router on a Stick** method, this provides better separation between the VLANs in the network, and comes with lower cost. Furthermore, routers provide more routing options which we can impose further security policies later on.

Customer public network (including wired and wireless), is used at floor 2 (reception floor) to provide Internet access to customers. The network is **isolated** from the Company network and lies outside the Firewall.

Internal devices in the company network communicates with trusted servers outside the Internet only.

The camera system of the entire company is implemented in a isolated VLAN not accessible from any other internal VLANs and the Internet. All cameras activities are monitored through a central IOT server and only from there the image captures can be retrieved.

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

Headquarters.

1st floor. Central cabling center and IT room.

- 4 servers for public access, 5 PCs for IT personnel.
- 2 camera surveillance devices, one to monitor the servers, one to monitor the IT desk.
- 03 switches, for server network, for IT department network and for central cabling of department’s switches.
- 01 firewall. 02 routers

2nd, 3rd, 4th, 5th, 6th floor. Operational departments.

- Consists of operational departments for a bank such as Reception, Accounting, Marketing, Human Resources and Treasury.
- 2nd - Treasury: 10 PCs, with 5 camera surveillance at this department. 01 central networking switch.

- 3rd - Reception: 20 PCs, 10 for employees and 10 for customers without WiFi connected devices. 01 central networking switch.
- 4th - Accounting: 20 PCs for employees. 01 central networking switch.
- 5th - Marketing: 20 PCs for employees.01 central networking switch.
- 6th - Human Resources: 20 PCs for employees. 01 central networking switch.
- 01 surveillance camera at each department.

7th floor. Directorate.

- 01 surveillance camera IOT server
- 05 PCs for directorates.
- 01 central switch.

Branches.

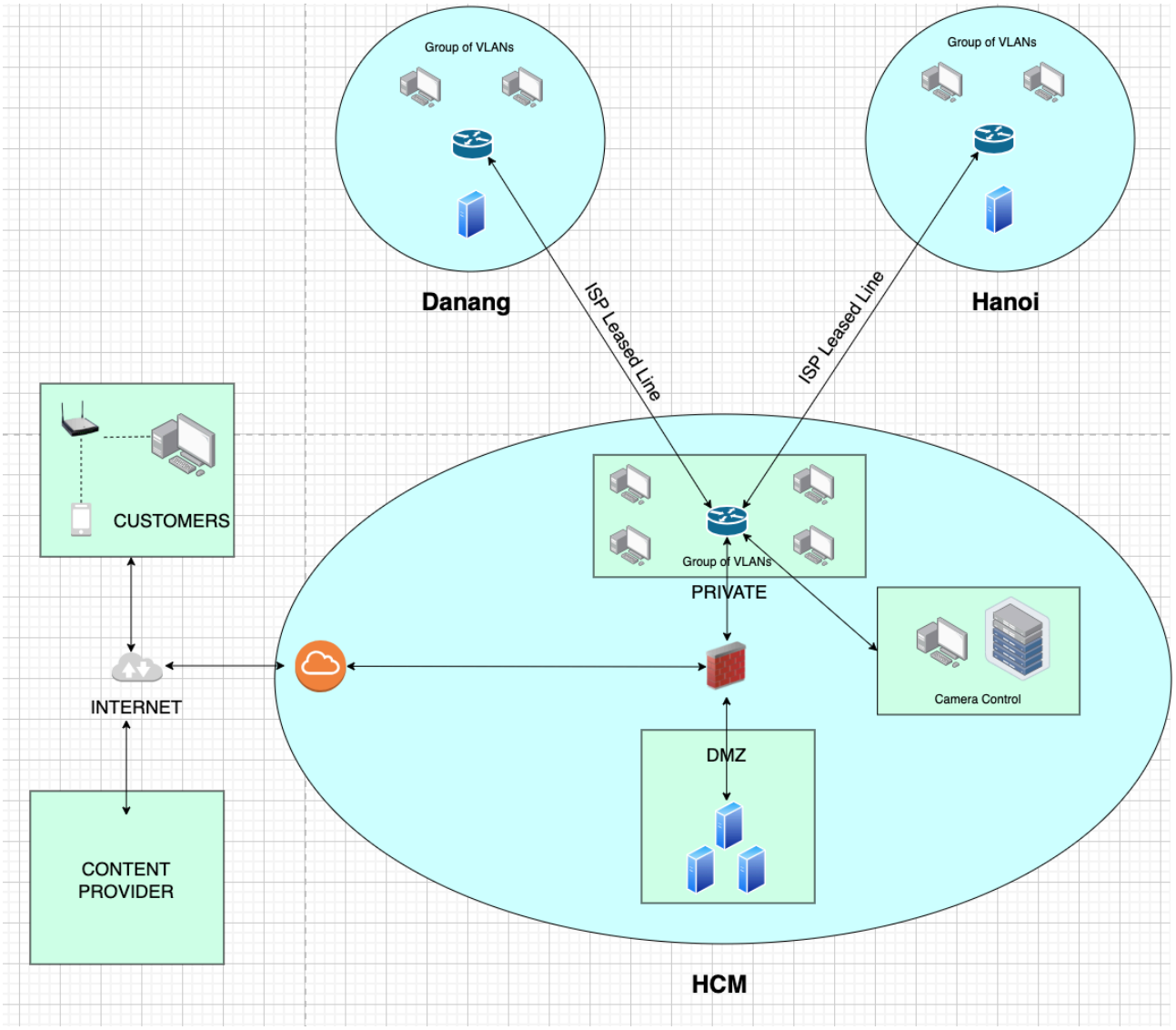
1st floor. Server room and IT department

- 02 public servers for load balancing with the headquarters's public servers. 01 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. Reception and Customer services department

- 20 PCs for employees. 10 PCs for customers who do not have WiFi access.
- 01 switch to connect the PCs.
- 01 camera surveillance system

e. 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, ...)



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

Network usage in a wireless environment:

- All devices are able to connect to the Customer network in a range of 50.0 meters within the building through an Access Point device connected to the switch.
- The device will connect to the wireless network named BB_CUSTOMER, no password was required.
- The IP is allocated automatically using DHCP. The IP is private IP and will be translated into public IP using NAT.

- There are also prepared PCs in the bank to provide wired access to customers who don’t have wireless devices.

2. Step 2 (1 point): List of minimum equipment, IP plan, and wiring diagram (cabling)

a. List of recommended equipment and typical specifications & IP plan

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 (Dec 2023)
Cisco 4321 Integrated Services Router	Product Code: Cisco ISR4321/K9 Total throughput: 50 Mb/s-100 Mb/s Total number of on-board 10/100/1000 WAN or LAN ports: 2 Network Interface Module (NIM) slots: 2 Power Supply Options: External - AC and PoE Rack Height: 1U Dimensions (H x W x D): 44.55 x 369.57 x 294.64 mm Package Weight: 9.19 Kg	03	$3,482
Cisco 2911	Cisco CISCO2911/K9 2911 3 Ports onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base.	01	$1,567.40
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 ASA5505-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)	01	$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	04	$399.99
Optical fiber cable & Copper cable supporting GigabitEthernet			
Optical fiber cable & Copper cable supporting FastEthernet			

Servers & Workstations	Selected by the bank.		
Total devices cost		$57243.36	

IP Addressing plan.

Assume the company was assigned a CIDR block `10.0.0.0/16`.
The line used to connect ISP to Company's Gateway is `8.8.8.0/8`.

For **private network**, all *hosts* have IP address format as:

`192.168.[VLAN].[host]`

where,

`[VLAN]` ranges from `2 .. 254`
`[VLAN] = 1` is reserved for management
`[host]` ranges from `1 .. 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.

For **Customer Public Network**, all hosts have IP address format as:

`192.168.0.[host]`

where,

`[host]` ranges from `10 .. 254`
`[host]` in `1 .. 9` is preserved for networking devices.

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 HCM and Danang.
2. Network `10.0.2.0/24` is for WAN communication on leased DSL between HCM and Hanoi
3. Network `192.168.1.0/24` is for communication between Headquarters subnet router and the firewall.
4. Network `172.168.2.0/24` is for communication between the firewall and Internet Gateway.
5. Network `172.168.0.0/24` is for communication between the Customer Public Network and Internet Gateway.
6. Network `10.0.0.0/24` is for public servers. (CIDR block assigned to the company)

The summary of IP addresses is as follows:

List of Access VLANs

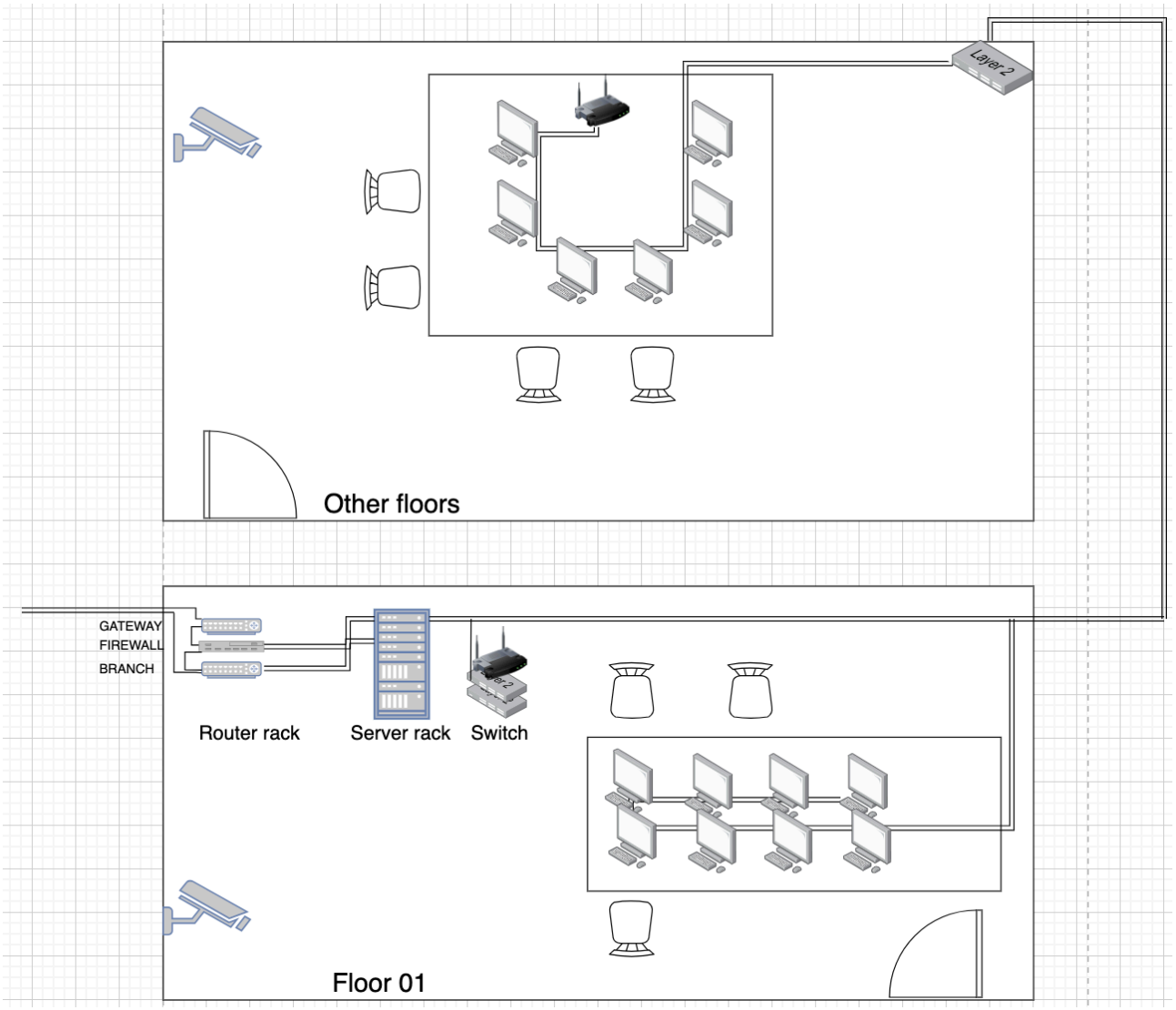
Location	VLAN	Network IP address	Default Gateway
HCM	002	192.168.2.0/24	192.168.2.1/24
HCM	003	192.168.3.0/24	192.168.3.1/24
HCM	004	192.168.4.0/24	192.168.4.1/24
Danang	008	192.168.8.0/24	192.168.8.1/24
Danang	009	192.168.9.0/24	192.168.9.1/24
Danang	010	192.168.10.0/24	192.168.10.1/24
Hanoi	005	192.168.5.0/24	192.168.5.1/24
Hanoi	006	192.168.6.0/24	192.168.6.1/24
Hanoi	007	192.168.7.0/24	192.168.7.1/24

List of Company Public Servers

DNS is resolved at 9.9.9.9

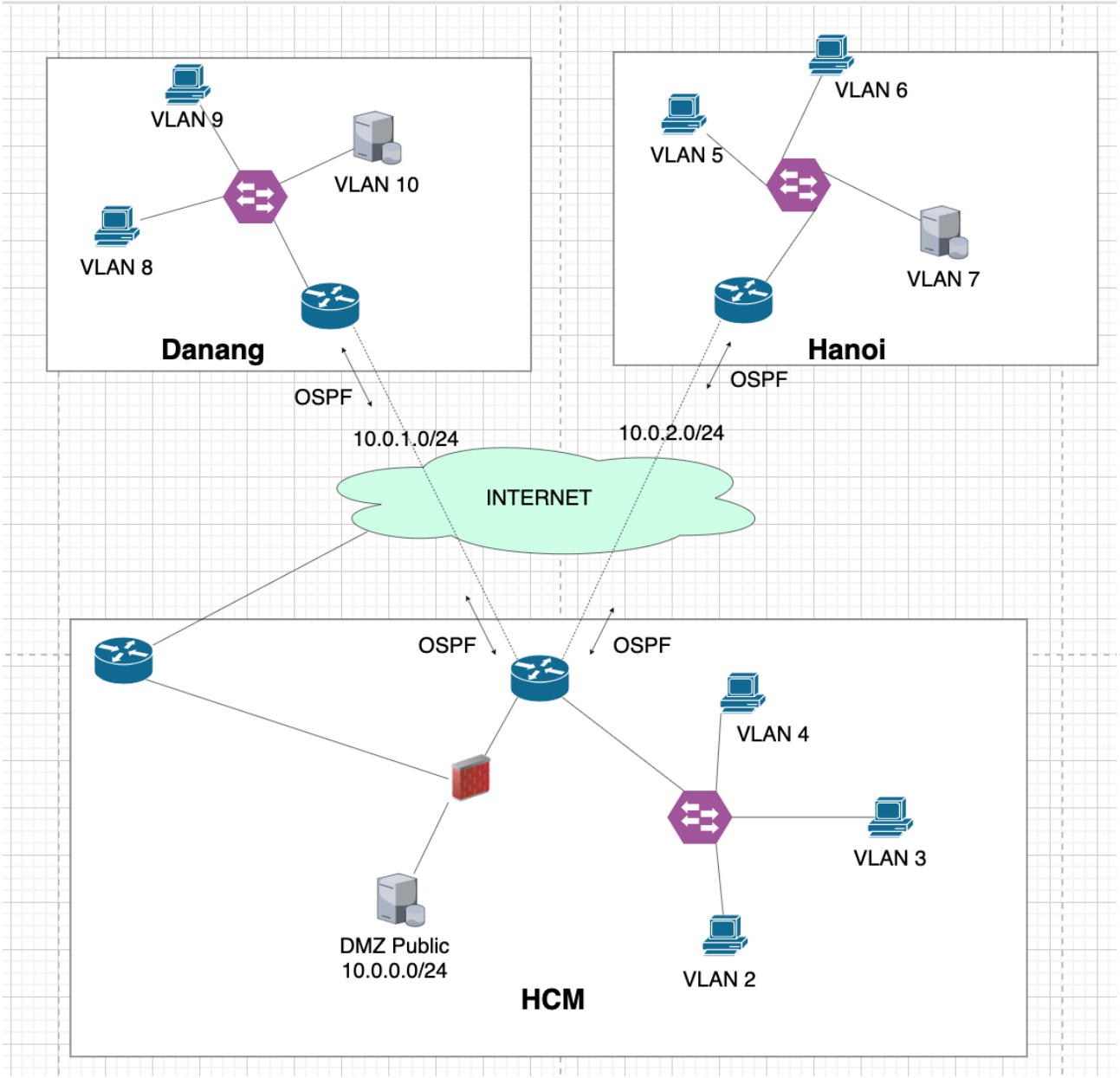
Location	SERVER NAME	IP address	Domain name
HCM	WEB_SERVER	10.0.0.3/24	www.bbank.com
HCM	SOFTWARE_UPDATES	10.0.0.4/24	update.bbank.com
HCM	DATABASE	10.0.0.5/24	database.bbank.com
HCM	MAIL_SERVER	10.0.0.6/24	mail.bbank.com
Danang	WEB_SERVER_DN	10.0.0.8/24	www.bbank.com
Danang	SOFTWARE_UPDATES_DN	10.0.0.9/24	update.bbank.com
Hanoi	WEB_SERVER_HN	10.0.0.10/24	www.bbank.com
Hanoi	SOFTWARE_UPDATES_HN	10.0.0.11/24	update.bbank.com

b. Schematic physical setup of the network



Physical wiring diagram of a typical building

c. WAN connection diagram between Headquarters and Branches (using new WAN technology such as SD-WAN, MPLS and OSPF routing protocol)


VLAN 9
VLAN 10
VLAN 8
Danang
VLAN 6
VLAN 5
VLAN 7
Hanoi
OSPF
OSPF
10.0.1.0/24
10.0.2.0/24
INTERNET
OSPF
OSPF
VLAN 4
VLAN 3
DMZ Public
10.0.0.0/24
VLAN 2
HCM

3. **Step 3 (1 point): Calculate the required throughput, and expected bandwidth from ISP, then suggest the configuration for the company network**

- **Summarize the estimated dataflows 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
  - BB Bank's growth rate of 20% in 5 years

- **The formula of network:**
  - 1 MBps = $\frac{8*2^{20}}{10^6}$ 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:

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

a) Headquarters

- In wired Internet, there are
  - Number of server : $N_s = 5$
  - Number of workstation : $N_w = 120$

- The total data transfer by server:

$$\sum Data_{server} = N_s(D_s + U_s) = 5 * (1000 + 2000) = 15000\ (MB/day)$$

- The total data transfer by workstation:

$$\sum Data_{workstation} = N_w(D_w + U_w) = 120 * (500 + 100) = 72000\ (MB/day)$$

- The total data transfer in headquarters:

$$\sum Data_{headquarter} = \sum Data_{server} + \sum Data_{workstation} + Data_{wifi} = 87500\ (MB/day)$$

- The peak hour throughput in headquarters:

$$Throughputt_{headquarter} = \frac{\sum Data_{headquarter}}{13500} = 6.481\ (MBps) = 54.3706\ (Mbps)$$

- The minimum bandwidth of headquarters:

$$Bandwidth_{headquarter} = Throughput_{headquarter} * 1.2 = 65.24472\ (Mbps)$$

b) Branches

- In wired Internet, there are
  - Number of server : $N_s = 3$
  - Number of workstation : $N_w = 30$

- The total data transfer by server:

$$\sum Data_{server} = N_s(D_s + U_s) = 3 * (1000 + 2000) = 9000\ (MB/day)$$

- The total data transfer by workstation:

$$\sum Data_{workstation} = N_w(D_w + U_w) = 30 * (500 + 100) = 18000\ (MB/day)$$

- The total data transfer in a branch:

$$\sum Data_{branch} = \sum Data_{server} + \sum Data_{workstation} + Data_{wifi} = 27500\ (MB/day)$$

- The peak hour throughput in branch:

$$Throughput_{branch} = \frac{\sum Data_{branch}}{13500} = 2.037\ (MBps) = 17.088 (Mbps)$$

- The minimum bandwidth of branch:
  $Bandwidth_{branch} = Throughput_{branch} * 1.2 = 20.505486\ (Mbps)$

c) Summary

- From the expected bandwidth, the ISP lease line from each branch should be 30 Mbps, which scales well for the company for the next ten years.
- From the FPT internet leased line, we could rent the 15 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**

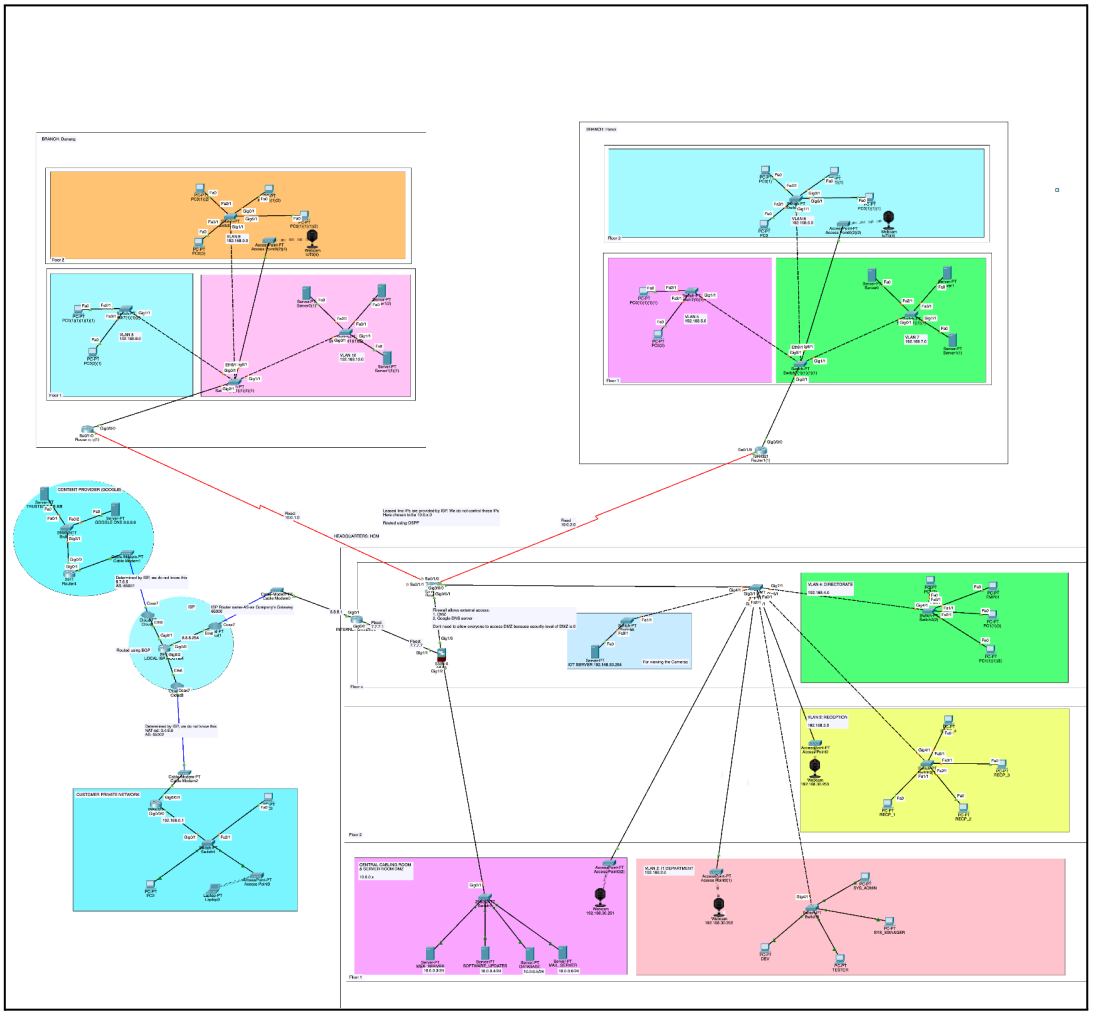
Price for Internet leased line by FPT[1]

[1]https://mangfpt.vn/leased-line-fpt/

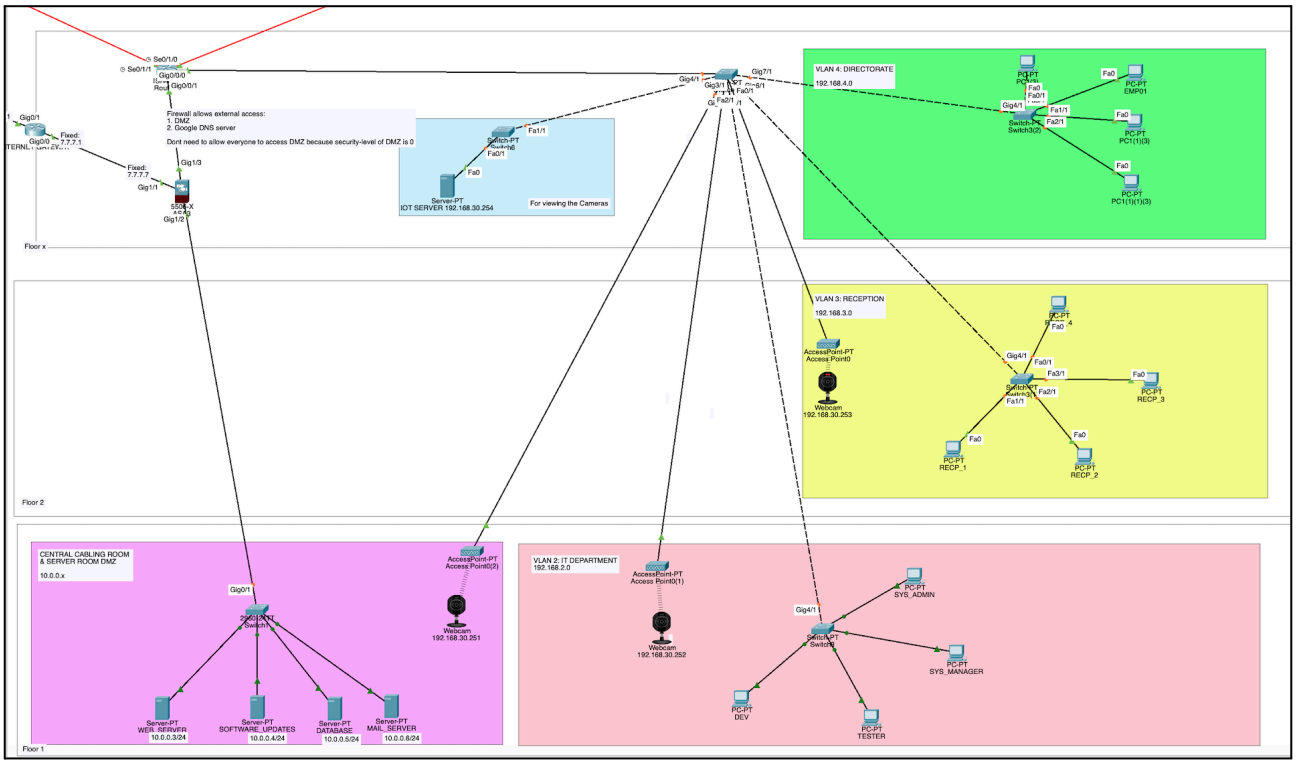
4. **Step 4 (2 points): Design the network map using Packet Tracer or GNS3 simulation software**

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.

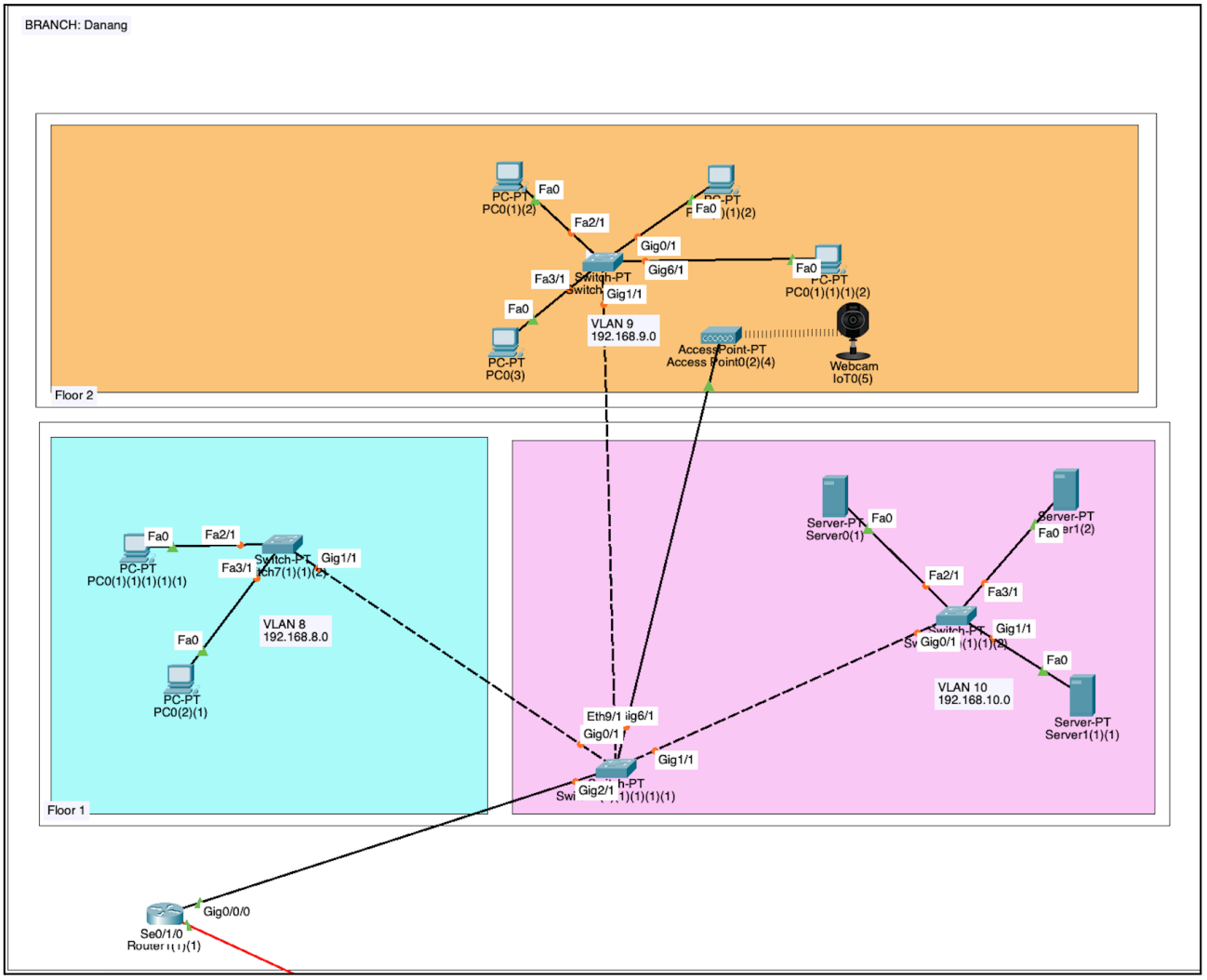
1. *Overall structure of the network*



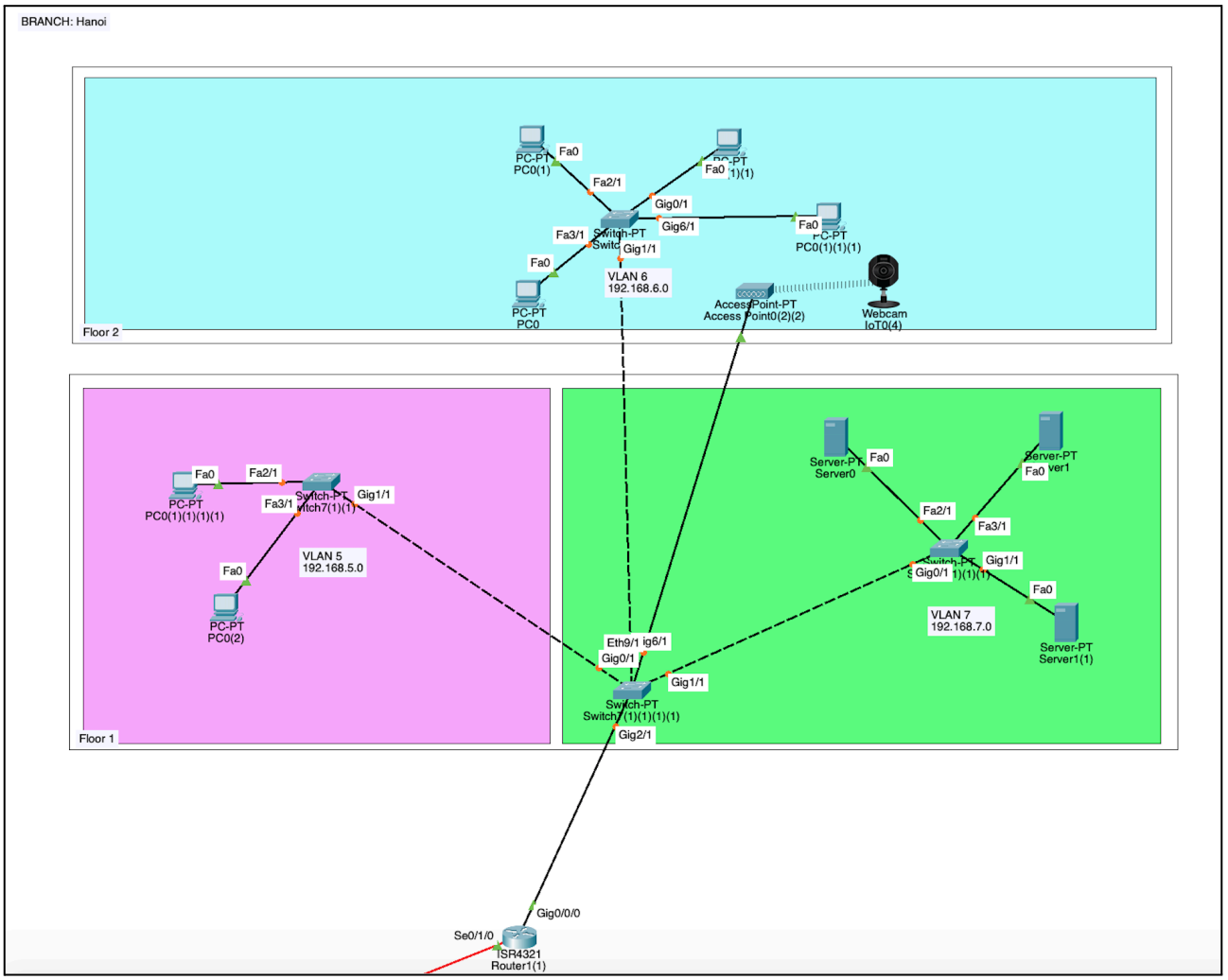
2. HCM Headquarters & Connection to the internet



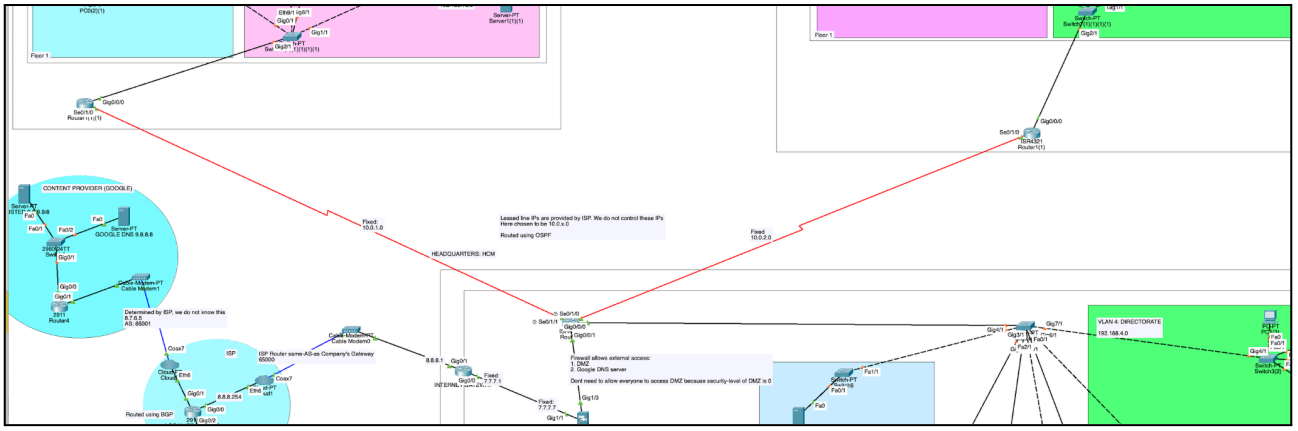
3. Danang Branch



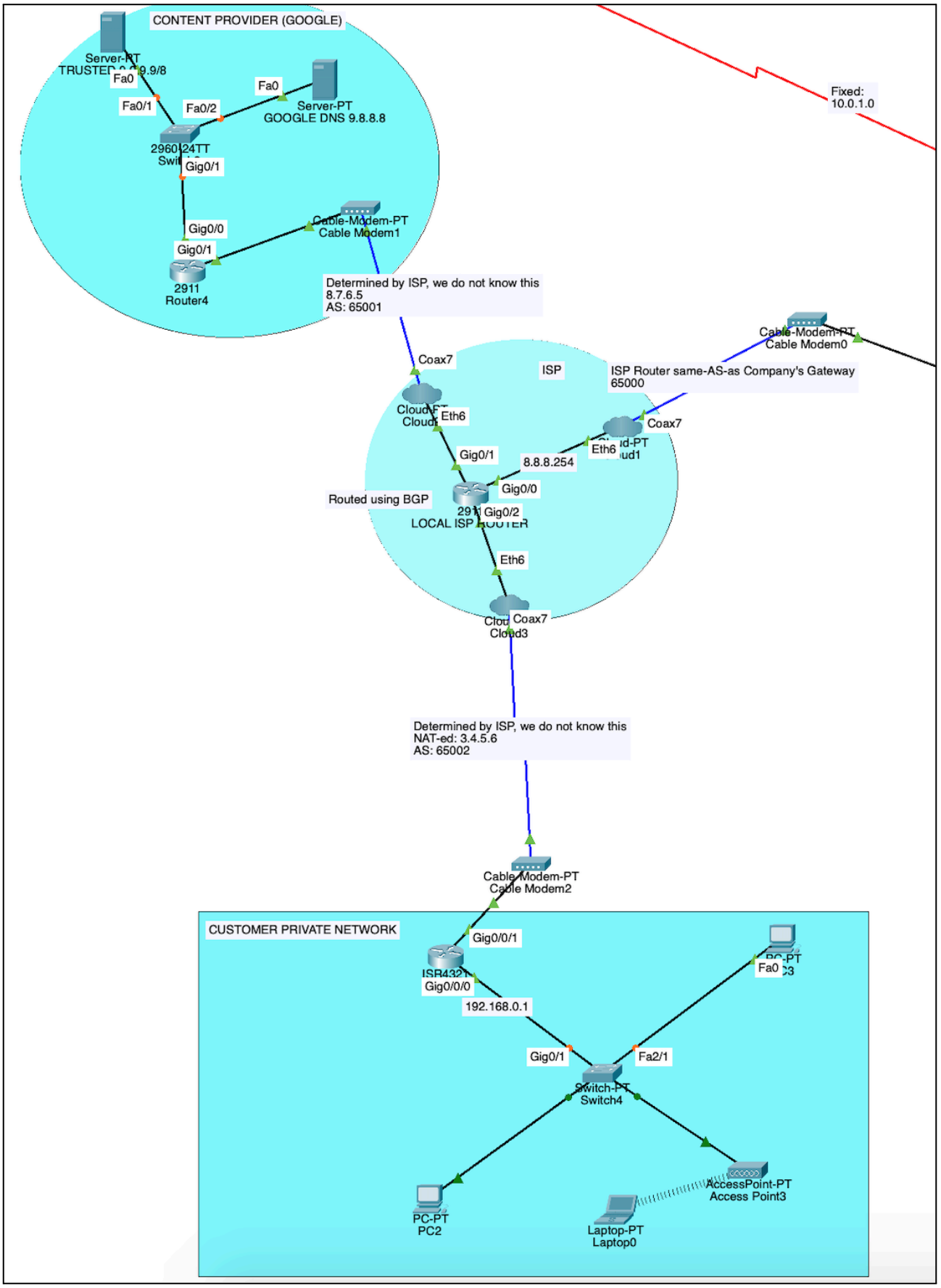
4. Hanoi Branch



5. Connection between branches

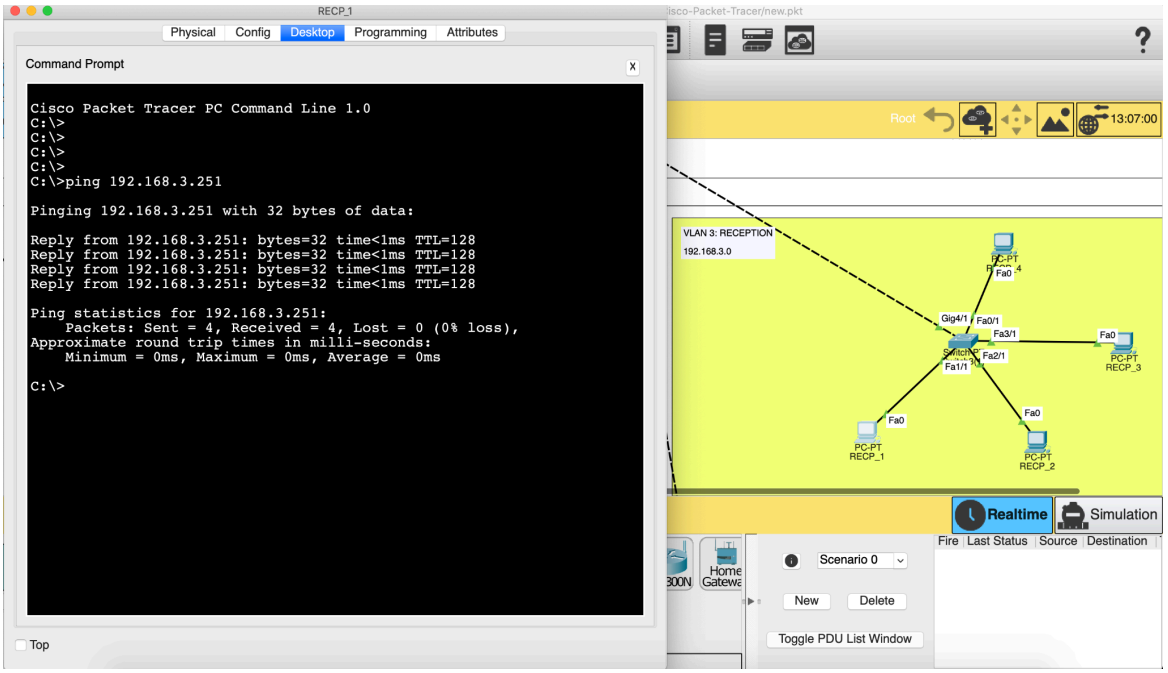


6. Internet, ISP and Content Provider



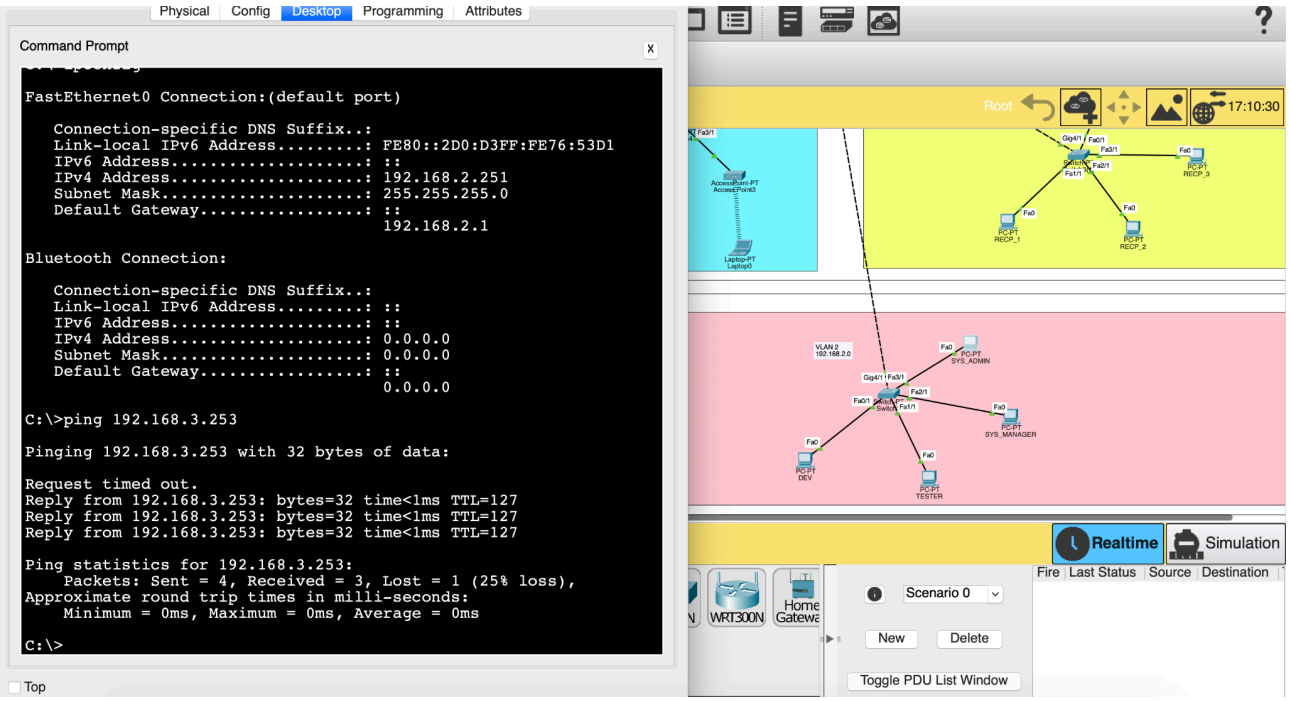
5. **Step 5 (2 points): Test the system with popular tools such as ping, and traceroute, etc. on the simulated system.**

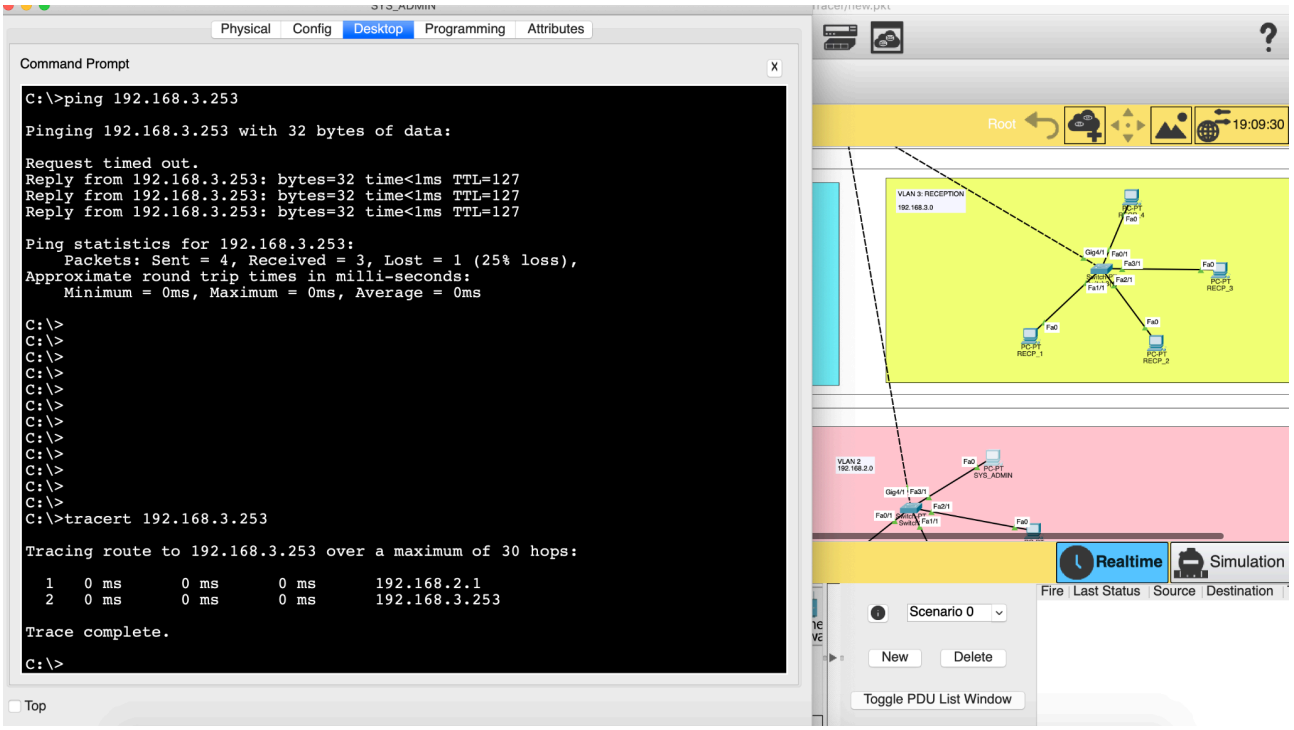
1. Connect between PCs in the same VLAN



- The experiment was carried out within **VLAN 3: Reception** computers.

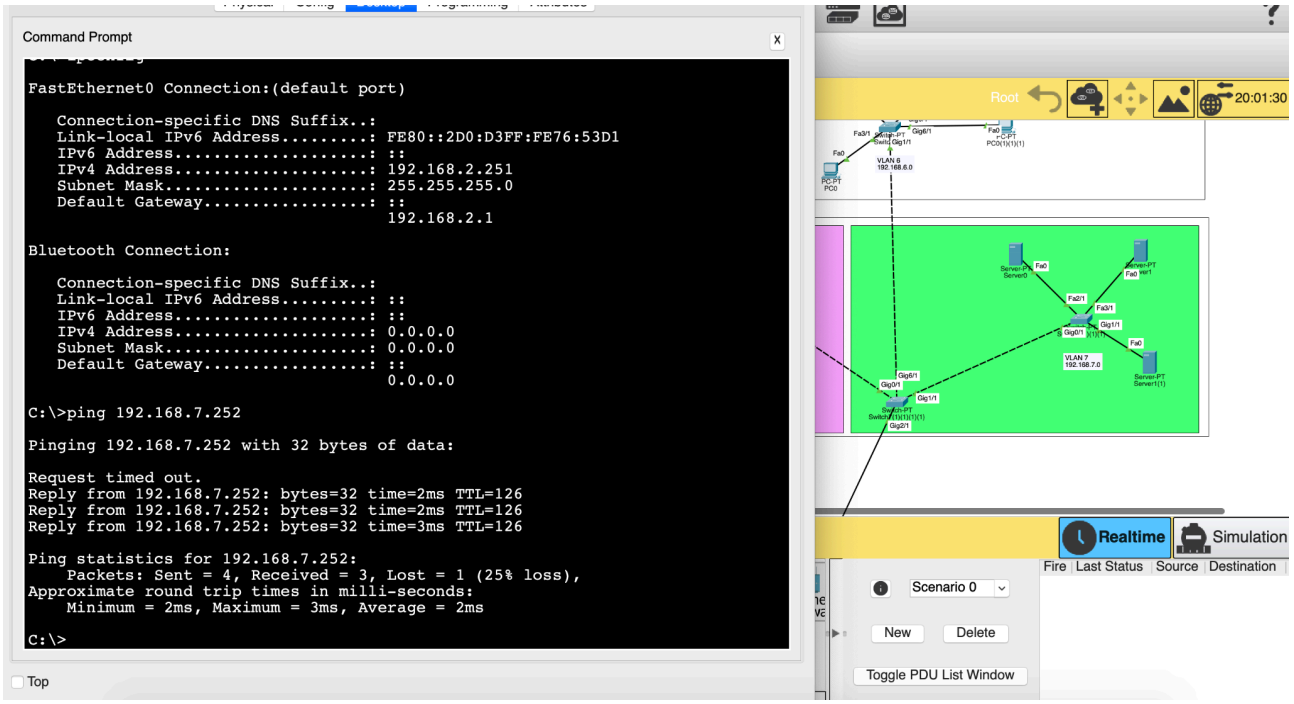
2. Connect PCs between VLANs

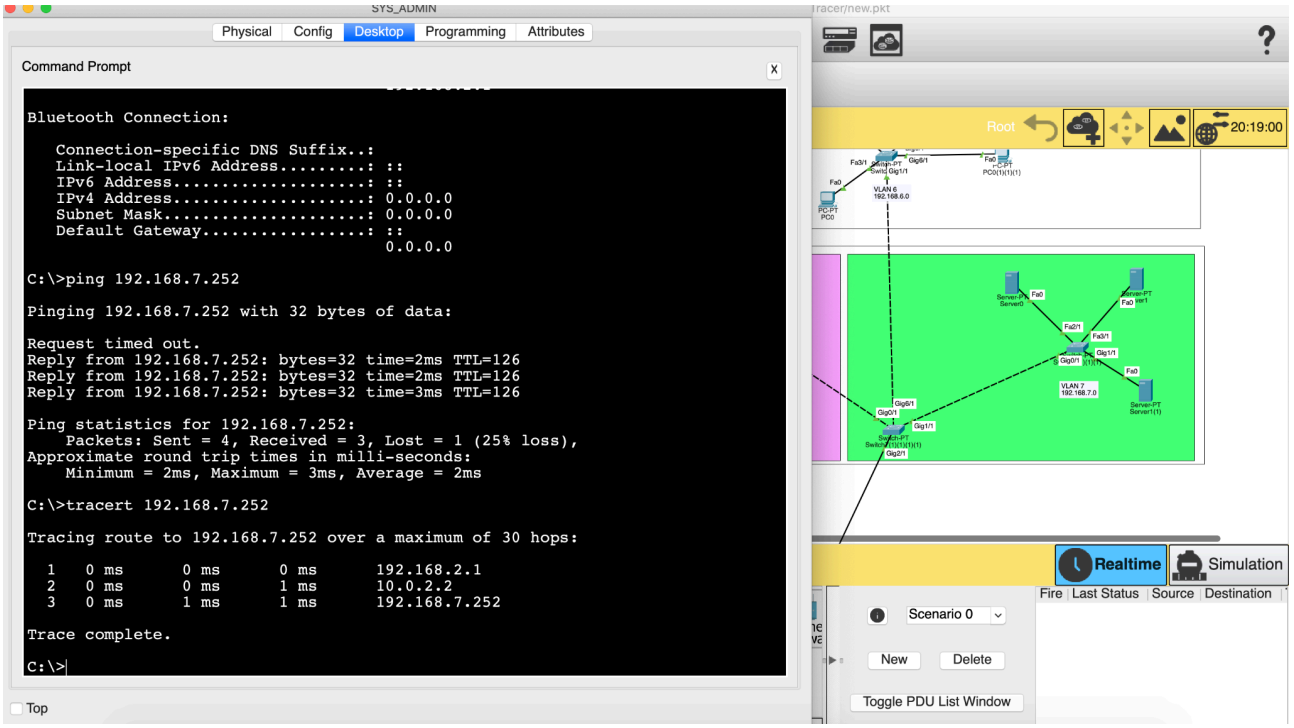




- The experiment was carried out between **VLAN 2: IT DEPARTMENT** and **VLAN 3: RECEPTION** using both ping and traceroute.

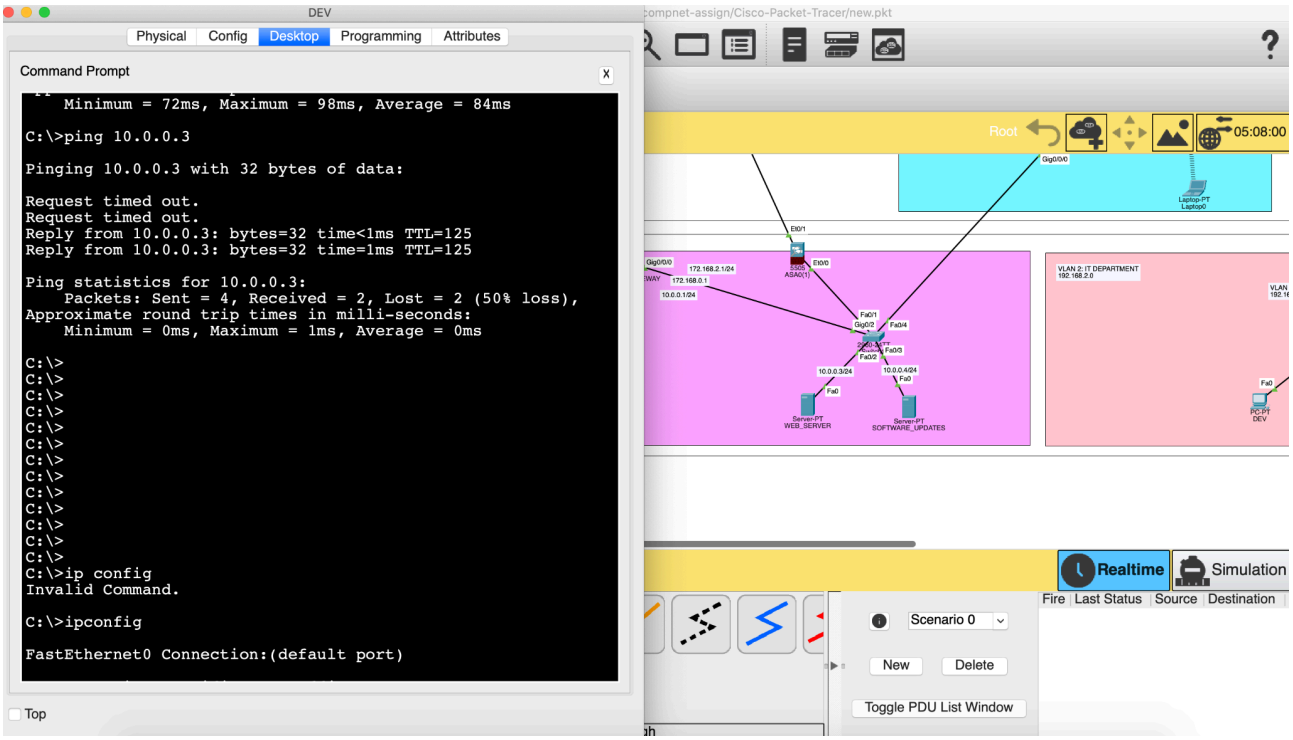
3. *Connect PCs between Headquarters and branches*

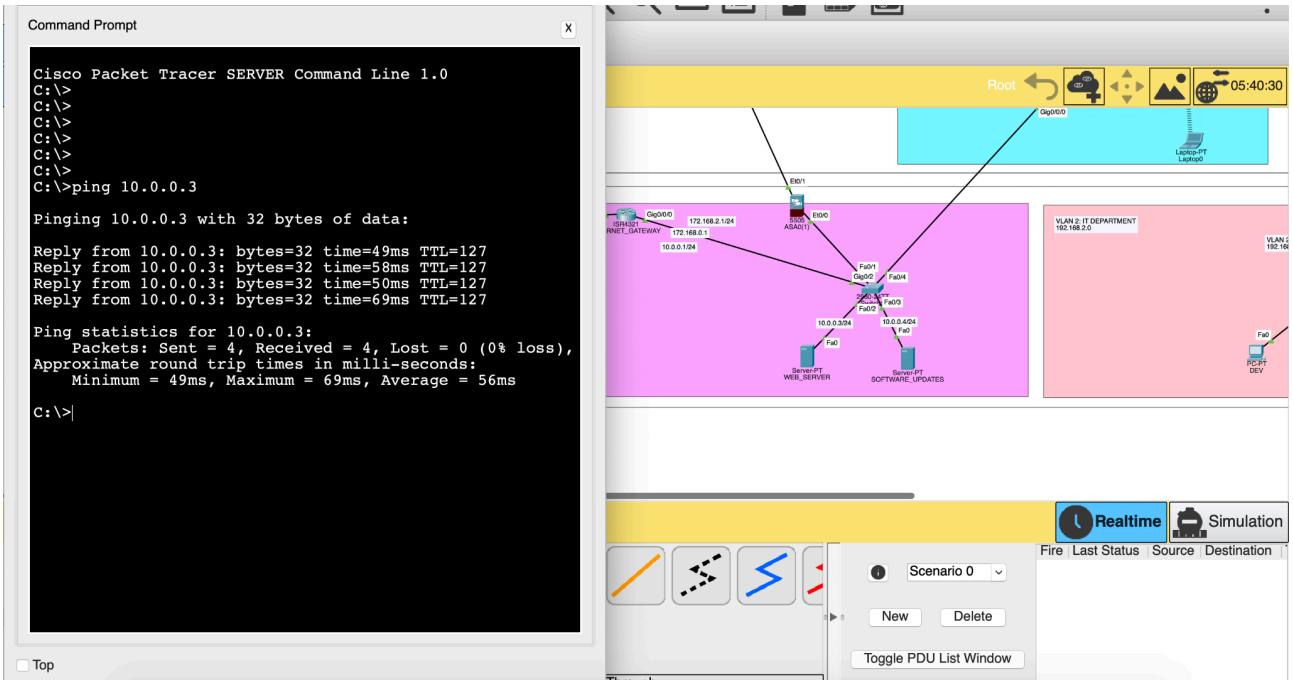




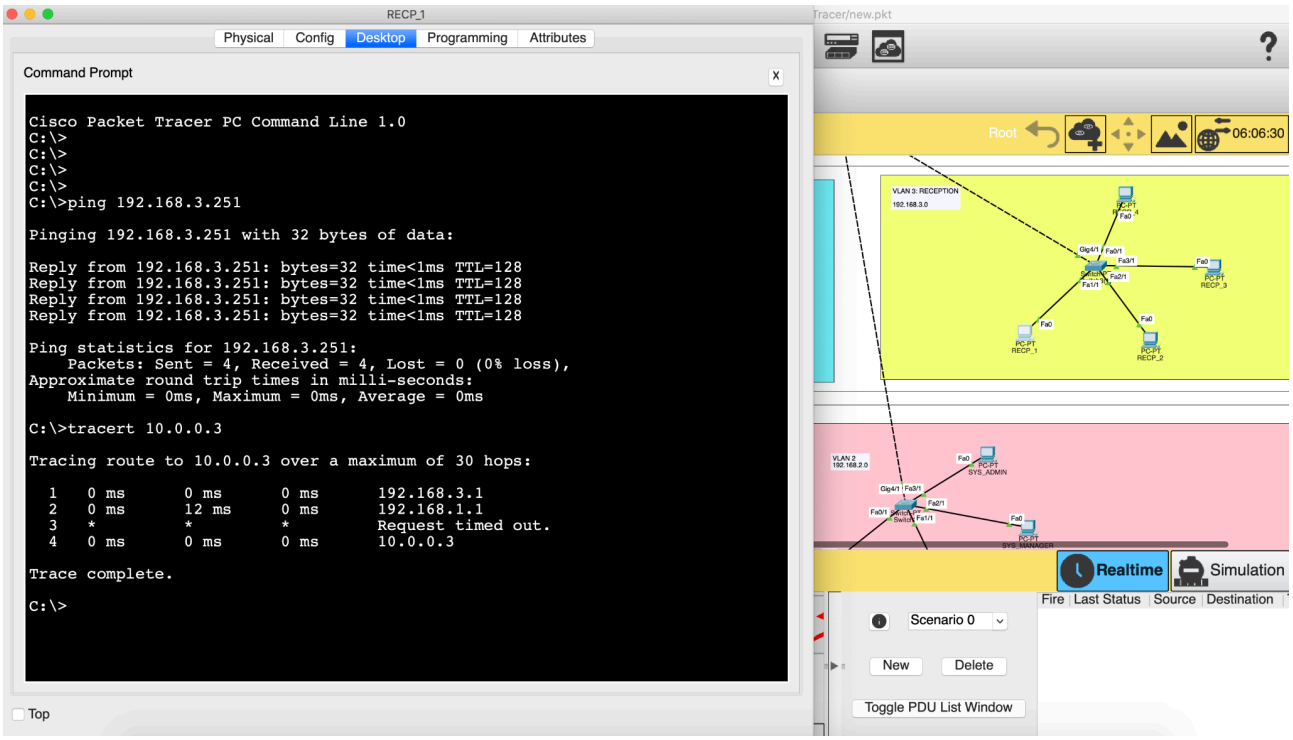
- The experiment was carried out between **VLAN 2: IT DEPARTMENT** in HCM Headquarters and **VLAN 7: SERVERS** in Hanoi using both ping and traceroute.

4. *Connect to servers in the DMZ*



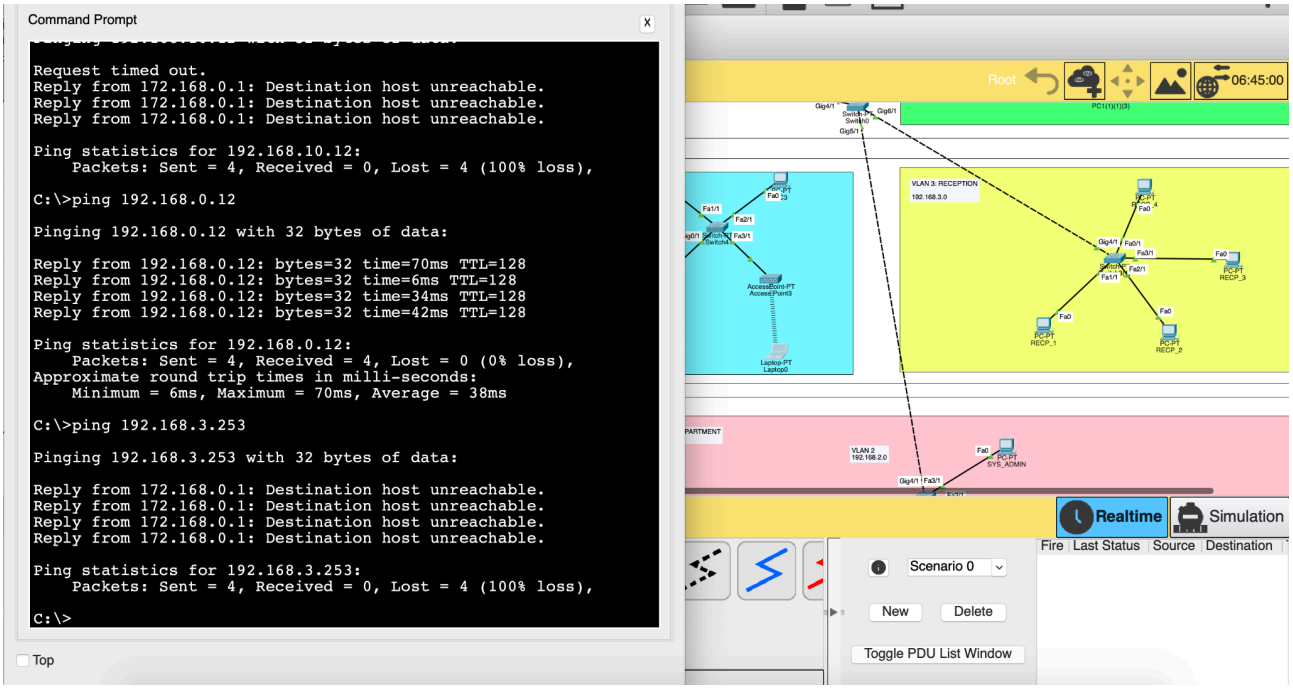


- The experiment was carried out between **VLAN 2: IT DEPARTMENT** in HCM Headquarters, **Public Server** from the internet and the servers in the **DMZ** of HCM Headquarters. We can observe a few "Request timed out" in the beginning due to ARP requests being broadcasted by the routers in the network.
- Two images associated with pinging from VLAN 2 and pinging from the Public Server from the internet.



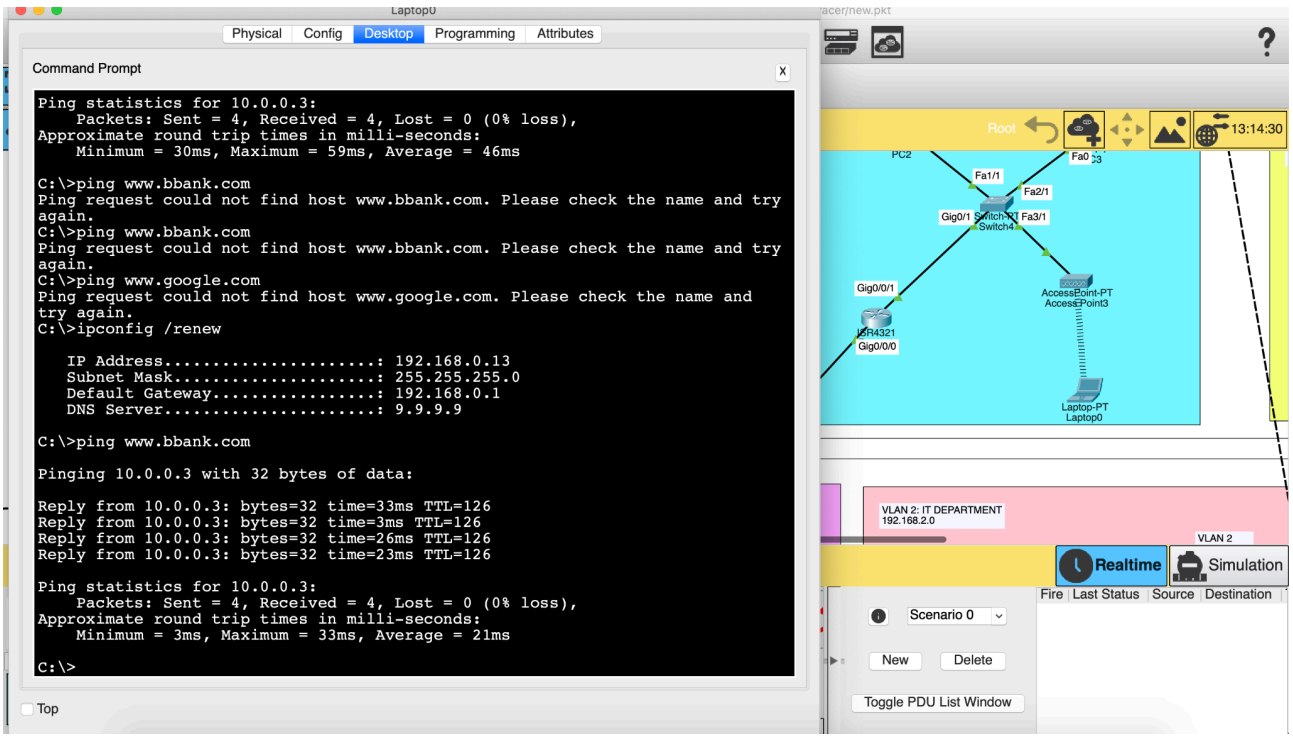
- Experiment with traceroute from an internal computer tracing out.

5. *No connections from Customers' devices to PCs on the LAN*



- Pinging from one computer from the **Customer Public Network** to an internal computer.

7. *Connect the Internet to a Web server.*



- The experiment was carried out between a wirelessly connected device in Customer Public Network, pinging to the WEB SERVER in the DMZ. The DNS service for this network is set up at 9.9.9.9 server.

6. **Step 6 (2 points): Re-evaluate the designed network system through the following features: reliability, ease of upgrade, diverse support software, safety, network security, etc.**

Remaining problems of the project

Reliability
(1) There is a single point of failure at the switches and routers due to Star Topology. (2) The network does not possess a backup mechanism thus the chance of losing the package is high. (3) The VLANs routing is heavily dependent on one-armed routers.

Performance
(1) The routing between VLANs is done using the Router on a Stick method, creating a potential bottleneck at these one-armed routers. (2) There is no load balancer implemented at the Gateway, the workload is not distributed between the branches. (3) All traffic passes through one router at HCM headquarters, making it a potential congestion point.

Ease of Upgrade
(1) The network contains some legacy Cisco devices no longer supported by Cisco, upgrading the network to adopt new technologies could be a challenge.

Security
(1) Only the DMZ at HCM headquarters 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. (3) Firewall filters the IP traffic, thus making the network vulnerable to IP spoofing.

Features
(1) Lack of VPN for teleworkers. (2) Load balancing not yet implemented due to single firewall mechanism. (3) Cross-branch camera system not yet implemented, each branch has its own camera system.

Development orientation in the future

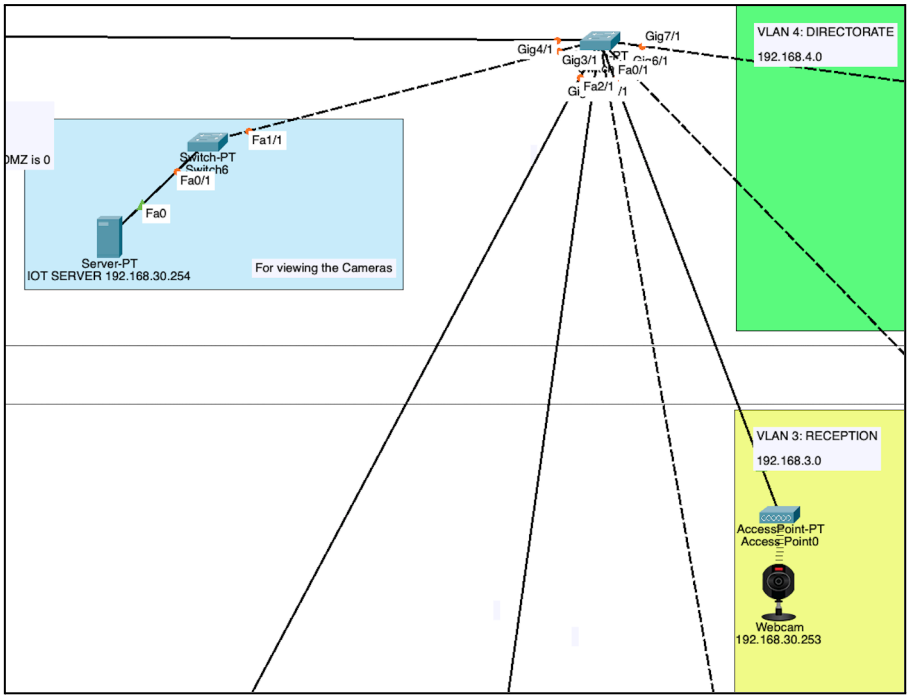
(1) Router on a Stick method should be replaced by Multilayer Switches. This reduces the congestion point on one-armed routers and provides better performance via wire-speed data traversal when routing between VLANs.
(2) Implement Dual Firewall mechanism for proper separation DMZ, allowing DMZ to be 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.

(Additional proposal) Propose a VPN configuration for site-to-site and for a teleworker to connect to Company LAN

To provide VPN access, we can configure an IPsec VPN tunnel from the subnet routers to trusted routers on the external network. From there the teleworker can connect to the Company private LAN via these trusted routers.

Propose a surveillance camera system for the Company

The surveillance camera system for the company should be a separate VLAN of the branch's private network, connected to the central switch. There will be a central IOT server to view and manage the operations of cameras and their captured videos. This VLAN is completely private and can not be accessed anywhere even the internal devices. The camera is remotely accessed via a wireless access point at each floor, making additional physical wiring not necessary thus improve the aesthetic.



A simulation of our camera surveillance system.