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

## Computer Networks Lab (CO3094)

# Assignment 2

## Section CC06

| | | |
|---|---|---|
| **Advisor**: | Nguyễn Mạnh Thìn | |
| **Group Members**: | Nguyễn Hải Đăng | 1952652 |
| | Lưu Nguyễn Hoàng Minh | 1952845 |
| | Nguyễn Phú Nghĩa | 1952355 |

HO CHI MINH CITY, NOVEMBER 2021

# Contents

# Member list

| No. | Fullname | Student ID |
|---|---|---|
| 1 | Nguyễn Hải Đăng | 1952652 |
| 2 | Lưu Nguyễn Hoàng Minh | 1952845 |
| 3 | Nguyễn Phú Nghĩa | 1952355 |

# 1 Overview of the project

The purpose of this project is to help CCC (Computer Construction Concept) to design a computer network for a headquarter and two branches of a BBB (BB Bank), which is a bank being under construction.

# 2 Requirements analysis

## 2.1 Requirements

### 2.1.1 Functional requirements

1. The Headquarters (H) building consists of 7 floors, the first floor is equipped with 1 IT room and the Cabling Central Local. It is in small-scale BBB: 100 Workstations, 5 Servers, 12 Network devices (switches, routers, wireless AP, modem, etc.).

2. The 2 branches in 2 big cities like Nha Trang (NT) and Da Nang (DN) are designed similarly to the Headquarters, but at a smaller scale. It is about 2-floor high, the first floor is equipped with 1 IT room and the Cabling Central Local. The BBB Branch consists of 50 Workstations, 3 Servers, 5 Network devices.

3. The system has 3 separated local networks: one for the headquarters and 2 smaller-scale networks for the branches in Nha Trang and Da Nang:

   - Using new technologies for network infrastructure that should support 100/1000 Mbps wired and wireless connection.
   - Using a combination of licensed and open-source software, office applications, client-server applications, multimedia, and database.
   - Requiring high security, robustness when problems occur, easy-to-upgrade system.
   - Using VLAN structure network organization.

4. The system has the network connection from the headquarters and branches to the outside.

5. The network connections between the headquarters and the 2 branches are set up through 2 leased lines (for WAN connections) and 1 ADSL (for Internet connection) with a load-balancing mechanism.

### 2.1.2 Non-functional requirements

1. **High security.** Configured networks for our working environments should be able to prevent unauthorized data manipulation, server harm, etc. through attacks such as DDoS, SQL injection, etc.

2. **Robustness.** Data are backed up occasionally in case the server crashes or problems occur. The network is highly available so that the users can access the network without facing any interruption.

3. **Scalability.** The network for the bank is scalable, which means that the network can be modified by adding more devices to it.

4. **Balanced load.** The flows and load parameters of the system (about 80% at peak hours 9 a.m. - 11 a.m. and 15 p.m.-16 p.m.) can be shared for Head Office and Branch.

5. **Usability.** Licensed and open-source software, office applications, client-server applications, multimedia, and database.

6. **High upload and download capacity.** Each server consumes 500 MB/day, each workstation consumes 100 MB/day and each WiFi-connected laptop for customers to access consumes 50 MB/day.

7. **Teleworkability.** VPN configuration for site-to-site and for a teleworker to connect to LAN.

8. **High growth rate.** 20% in 5 years.

### 2.2 Checklist

This checklist is used for the headquarters and two branches, but the scale of branches is smaller than the headquarters' one.

1. **Planning**

| | |
|---|---|
| How many on-site devices (computers, servers, scanners, printers, etc.) will require a network card? | |
| Which server-based applications (e.g. database, email) does the Bank need to run on the network? | |
| What are the desired specifications of the servers the Bank intends to install on the network (e.g. amount of memory, processor speed, etc.)? | |

2. **Network hardware requirements**

| | |
|---|---|
| Do the hubs or switches have enough ports for the number of connections the Bank will require? Is there room for growth? | |

3. **Network design**

| | |
|---|---|
| What network topology will the Bank use? | |
| Which network operating system will the Bank use? | |
| Which type of cabling will the Bank use? Would a wireless network be suitable? | |
| Where will the network cables be located? | |
| Where will the Bank locate the following devices: servers, hubs, switches, printers, firewalls, routers, modems, etc.? | |

4. **Security, backup, and power**

| | |
|---|---|
| What security measures will the Bank be putting in place? | |
| Does the Bank need to physically secure its servers (e.g. locking them away in cupboards)? | |
| How will the Bank back up data on its network? | |
| What is the capacity of the backup solution? | |
| Is it capable enough to support all the data on the servers and network devices? | |
| Does the backup solution have the capacity to grow as the data grows? | |
| How frequently will files be backed up and how long will the Bank keep backup files? | |
| Where will the Bank store backed-up tapes? Would it be fireproof safe? Or off-site? Or any other locations? | |
| What devices will require an uninterruptible power supply (e.g. servers)? | |
| Is there sufficient ventilation around the servers? | |

### 2.3 Area with high load

High load areas should be at floor 1 of the headquarters as well as the two branches where the servers are located. These zones are where large amount of data goes through since the servers have to execute many operations.

### 2.4 Network topology

In general, network topology is the link to connect the end users to the data center, and the devices within the data center. The choice of the network topology for a system is often determined by two main factors: the cost and the criticality of the services provided. Given these factors, there are two extremes of this decision:

1. **Bus topology.**

   In this topology, all nodes of the network are connected to a single cable called the backbone. It is inexpensive, and prone to failure because of its centralized property.

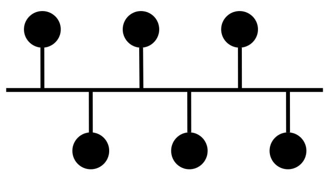

Figure 1: Bus topology

2. **Full-mesh topology.**

In this topology, all nodes are directly connected to every other nodes. It is costly, yet it is the most reliable topology.

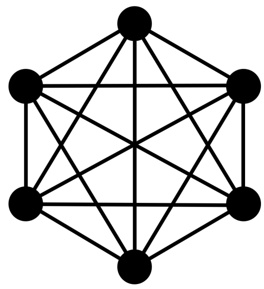

Figure 2: Full-mesh topology

There is also a topology that tries to combine the advantages of the two, that is the star topology. In this topology, all nodes are connected to a central hub or switch. It is the balance between bus and full-mesh topology both in terms of cost and reliability.

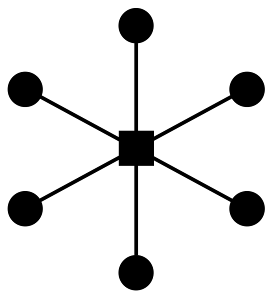

Figure 3: Star topology

In this project, we use *extended star topology* for our system, which is an extended version of star topology, for its balance between cost and reliability. From the star topology, the extended star topology adds sub-central devices that are connected to the central devices to scale up the idea of the star topology to be used in many buildings, etc.

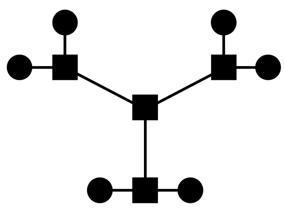

Figure 4: Extended star topology - our choice

Obviously, the pros and cons of this topology is not only confined in just its cost and reliability, which are compiled and presented as follows:

| Pros | Cons |
|---|---|
| • Easy to setup, maintain, and monitor<br>• Relatively inexpensive compare to full-mesh topology<br>• Resilient to nodes and cables failure<br>• Easy to scale up by adding more sub-central devices<br>• High-performing since no data collisions can occur and data take shorter path compared to bus topology<br>• Adding and removing nodes are easy | • More redundancy than bus topology<br>• More expensive than bus topology (more cables, more devices, etc.)<br>• Sentitive to central/sub-central devices failure<br>• The central device's load is shared between nodes |

### 2.5 WiFi coverage

- The design for WiFi coverage in each of the two branches is similar to the design in headquarters.
- The network is designed for floor 1 and 2 of the headquarters and floor 1 of the branch where customers mainly use WiFi.
- The wireless routers are directly connected to the gateway router so that it can act as the DHCP and provide the IP for wireless devices (smartphones, laptops).
- The standard channel is 2.4 GHz.
- We also use the WPA2-PSK with AES for the authentication method to set up the password for each device that wants to connect to the wireless.
- All devices that connect to WiFi networks cannot access the internal network. They only can connect to the router and use the service provided by the ISP.

### 2.6 Security

In terms of network security, Demilitarized Zone (DMZ) is used to improve the security of an organization's network by segregating devices, such as computers and servers, on the opposite sides of a firewall.

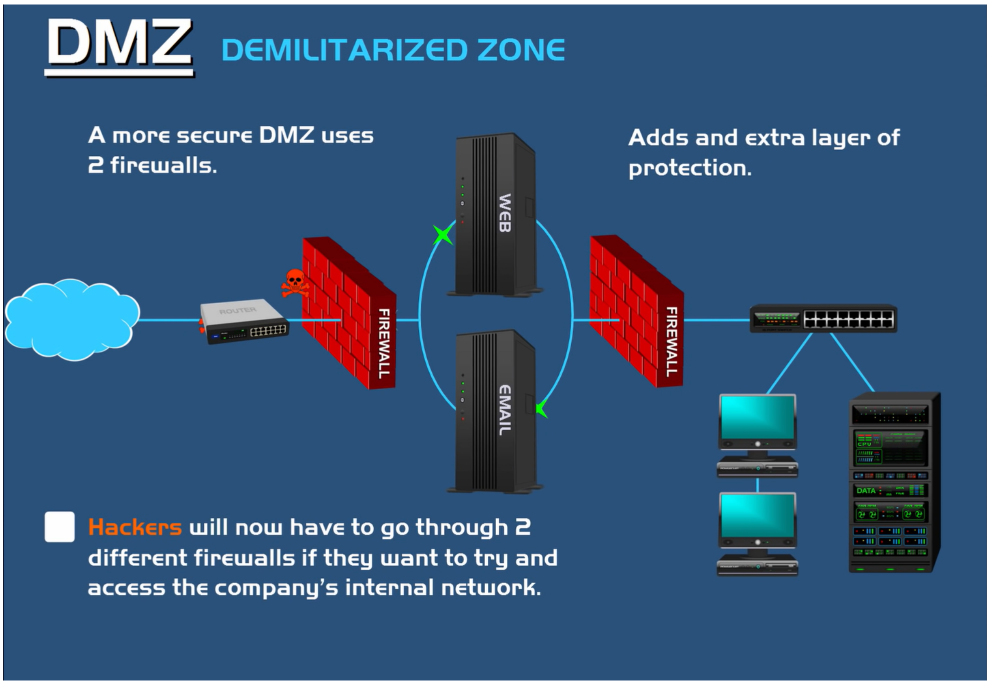


Figure 5: Demilitarized Zone

# 3 Equipment & diagram

## 3.1 Recommended equipment

The following hardware choices are based on the devices available in Cisco PacketTracer.

### 3.1.1 Router: 2911

- Quantity: 3
- Specification: 3 Gigabit Ethernet Port, 2 Serial Port
- Ethernet connects the switches and routers in the same area
- Serial connects to devices in other areas

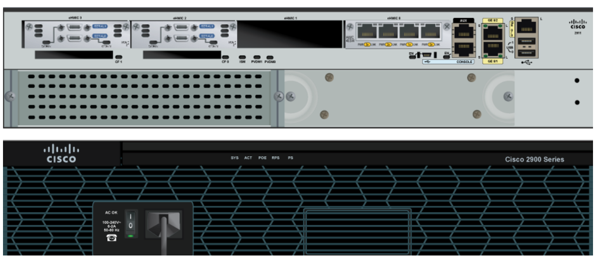


Figure 6: Router 2911

### 3.1.2 Router: 2811

- Quantity: 1
- Specification: 18 Fast Ethernet Port
- Used to connect from headquarter and branches to the internet

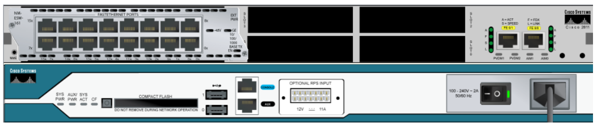

Figure 7: Router 2811

### 3.1.3 DSL modem

- Quantity: 3
- Specification: 1 Phone line port, 1 Fast Ethernet Port
- Used to connect a network to a telephone company digital subscriber line (DSL) service for Internet access.

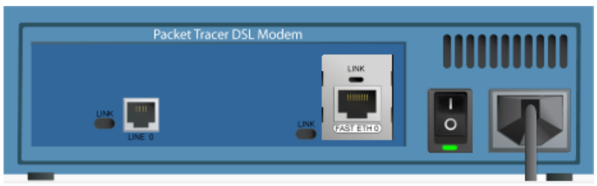


Figure 8: DSL modem

### 3.1.4 Cloud

- Quantity: 1
- Specification: 3 Modem port, 1 Fast Ethernet Port
- the ISP connect to the internet can be represent as the cloud. We need cloud to have the phone line connect to the DSL modem. Some time we represent ISPs just a whole bunch of different routers that make up that cloud.

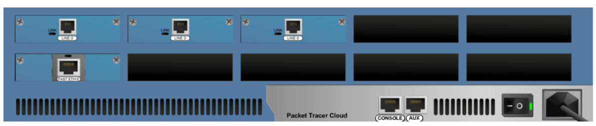


Figure 9: Cloud

### 3.1.5 Switches: 2960 24TT

- Quantity: 15
- Specification: 24 Fast Ethernet Port, 2 Gigabit Ethernet Port
- For headquarter, we need 7 switches for 100 workstations, 4 servers, 1 DHCP server and growth rate of 20% in 5 years
- For branches, we need 4 switches for each branch correspond to 50 workstations, 2 servers, 1 DHCP server and growth rate of 20% in 5 years

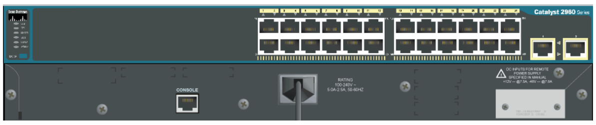

Figure 10: Switches 2960 24TT

### 3.1.6 Wifi Router: WRT300N

- Quantity: 4
- Specification: 2.4GHz channel WPA2-PSK built-in DHCP server
- Provide wireless connection through WPA2-PSK authentication
- In headquarter, we need 2 wifi routers for floor 1 and floor 2
- In branch, we only need 1 wifi routers for floor 1

Figure 11: Wifi Router WRT300N

### 3.1.7 Server

- Quantity: 11
- Specification: 5 servers for Headquarter, 3 for each branch
- To provide the DHCP services, each headquarter or branch will need 1 server for doing that

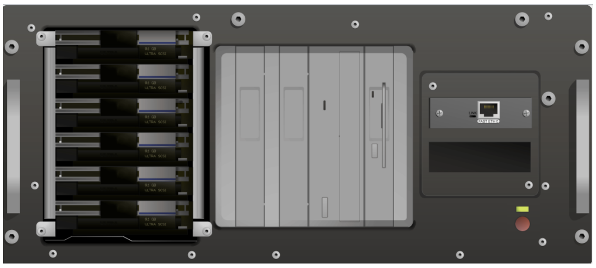

Figure 12: Server

#### 3.1.8 Cables

Figure 13: Straight-through copper cable

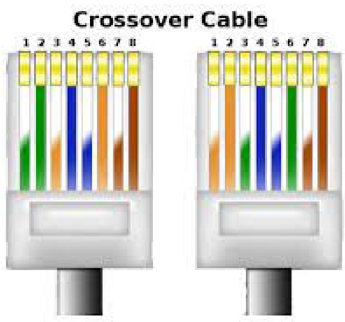


Figure 14: Crossover copper cable

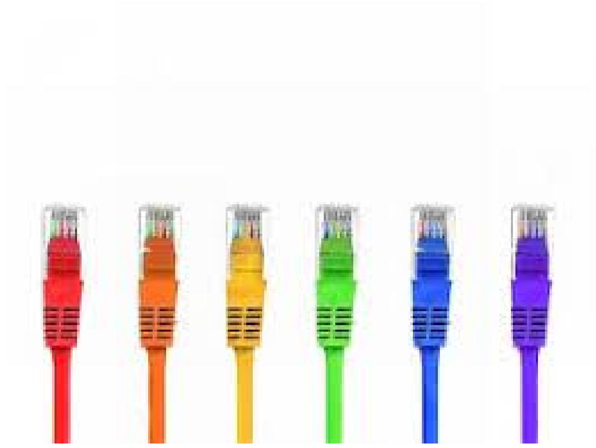

Figure 15: Leased line cable

### 3.2 Schematic physical setup

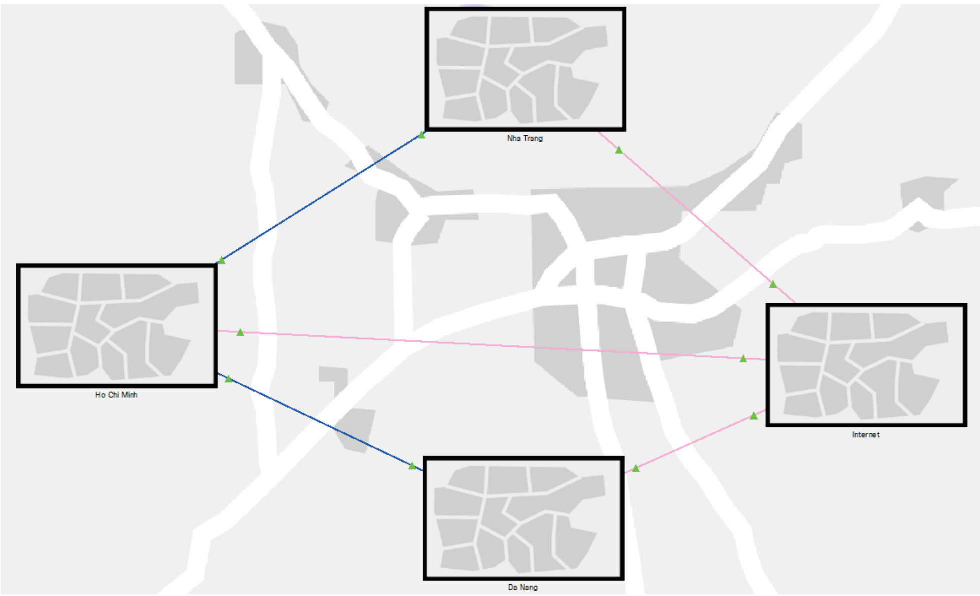


Figure 16: Connection diagram between Headquarters, Branches and the Internet

In this diagram, the red lines are DSL connection between the headquarters or a branch and the Internet. The blue lines are the leased lines between the headquarters and two branches. We eliminated the leased line between two branches because they can communicate the headquarters, which reduces the cost for the cable between the two branches.

### 3.3 IP Diagram

Because our network is very big so we choose to use the IP address table instead of diagram for showing the IP address. In here, we are using CIDR notation which is a compact representation of an IP address and its associated network mask.

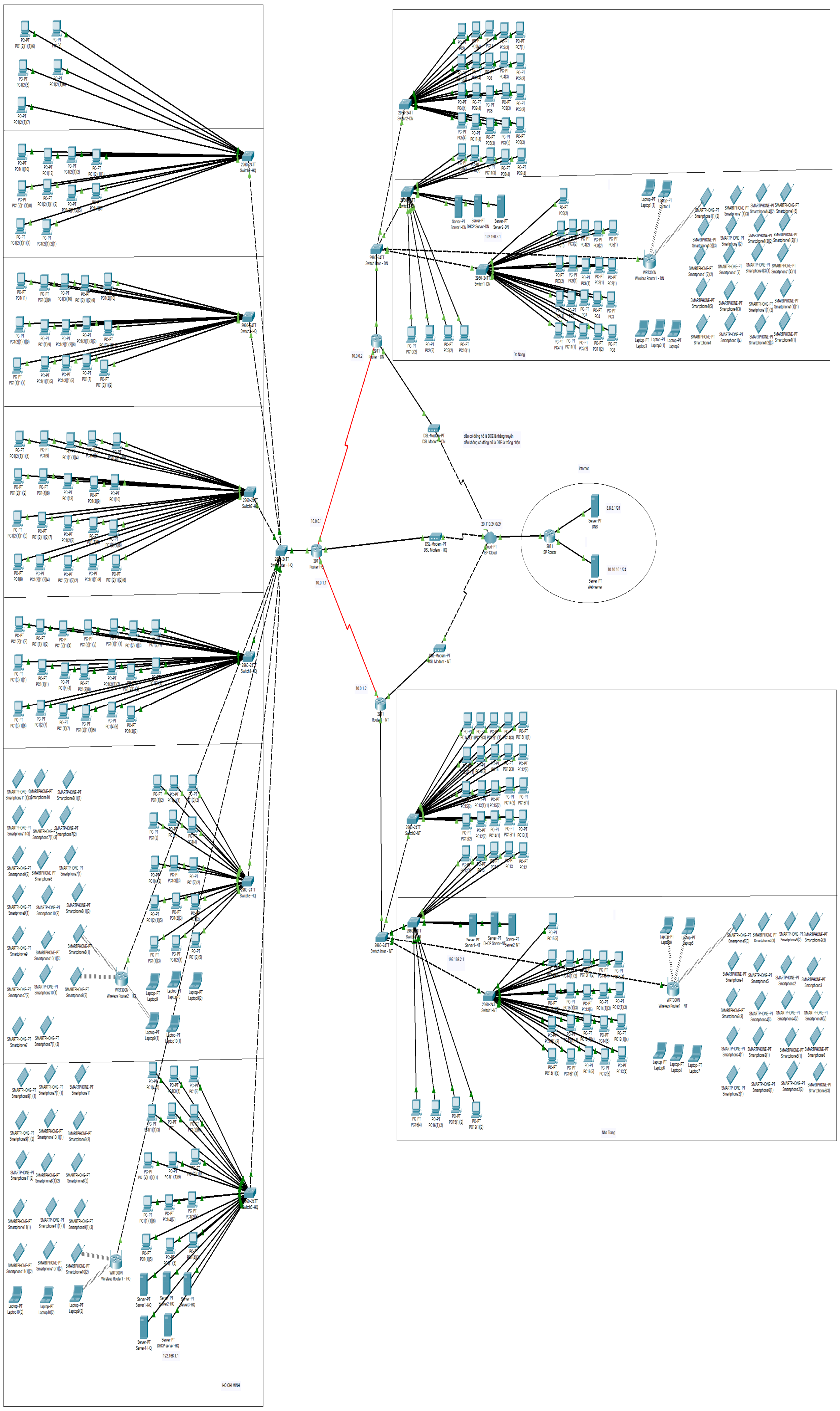

Figure 17: The whole picture of network design for our Bank

### 3.3.1 Headquarter

| VLAN | Dept | Network ID | Default Gateway |
|---|---|---|---|
| 10 | IT/Work Station | 192.168.1.0/24 | 192.168.1.1/24 |
| 50 | IT/Server | 192.168.1.0/24 | 192.168.1.1/24 |
| 10 | DHCP/Server | 192.168.1.2/32 | 192.168.1.1/24 |
| N.A | Wifi Router floor1 | 172.168.10.0/24 | 172.168.10.1/24 |
| N.A | Wifi Router floor2 | 172.168.20.0/24 | 172.168.20.1/24 |

### 3.3.2 Nha Trang branch

| VLAN | Dept | Network ID | Default Gateway |
|---|---|---|---|
| 10 | IT/Work Station | 192.168.2.0/24 | 192.168.2.1/24 |
| 50 | IT/Server | 192.168.2.0/24 | 192.168.2.1/24 |
| 10 | DHCP/Server | 192.168.2.2/32 | 192.168.2.1/24 |
| N.A | Wifi Router floor1 | 172.168.30.0/24 | 172.168.30.1/24 |

### 3.3.3 Da Nang branch

| VLAN | Dept | Network ID | Default Gateway |
|---|---|---|---|
| 10 | IT/Work Station | 192.168.3.0/24 | 192.168.3.1/24 |
| 50 | IT/Server | 192.168.3.0/24 | 192.168.3.1/24 |
| 10 | DHCP/Server | 192.168.3.2/32 | 192.168.3.1/24 |
| N.A | Wifi Router floor1 | 172.168.40.0/24 | 172.168.40.1/24 |

## 3.4 Wiring diagram

### 3.4.1 Headquarters

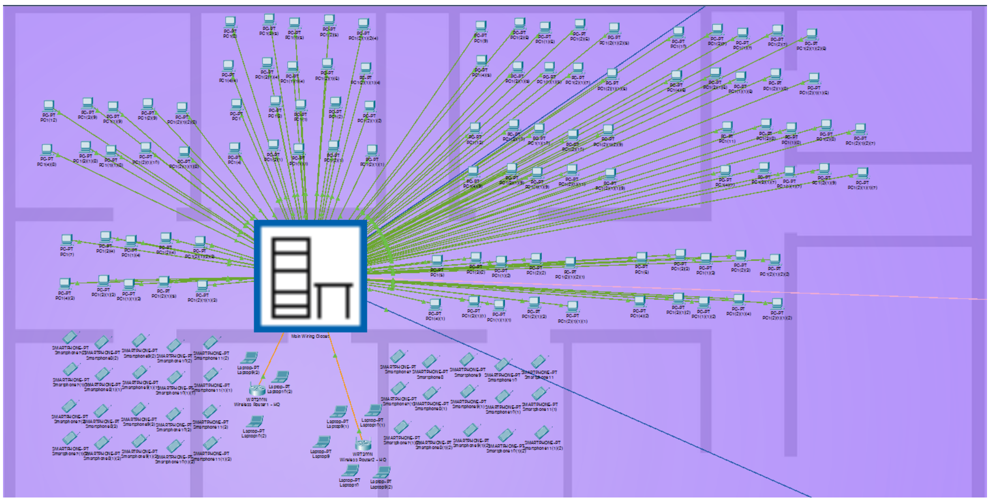

Figure 18: Overview of Wiring diagram at headquarters

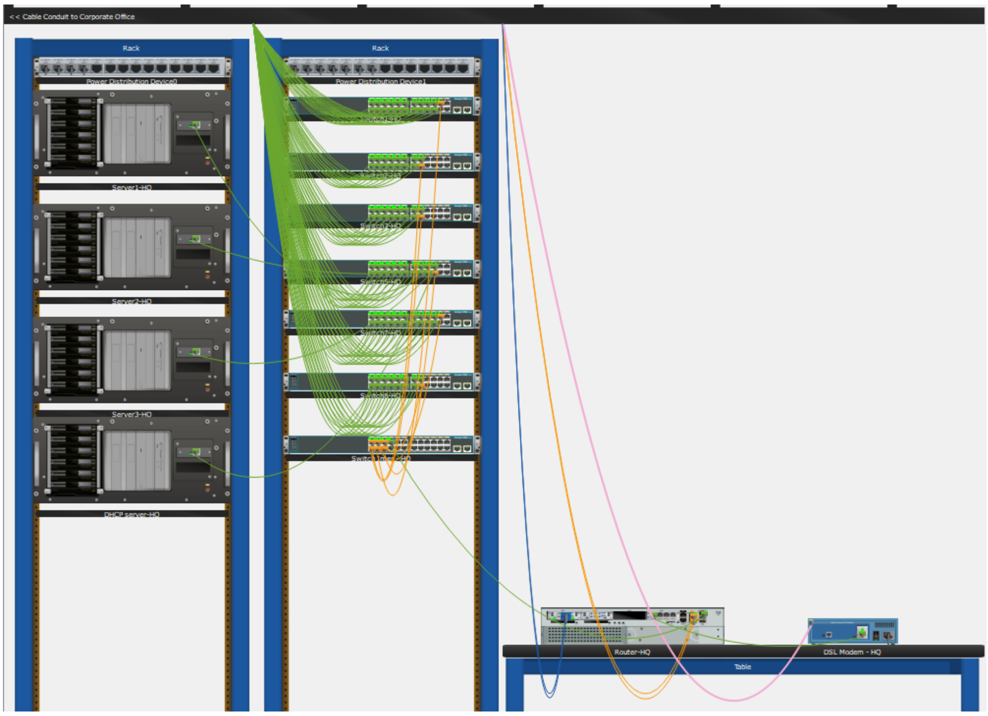


Figure 19: Wiring diagram of main wiring closet at headquarters

### 3.4.2 Branches

Nha Trang branch

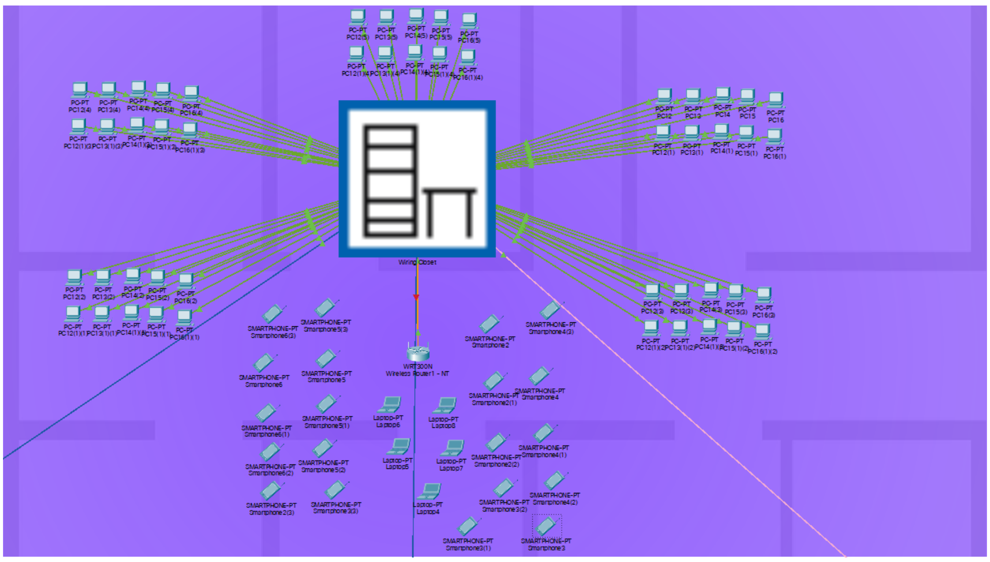


Figure 20: Overview of Wiring diagram at Nha Trang branch

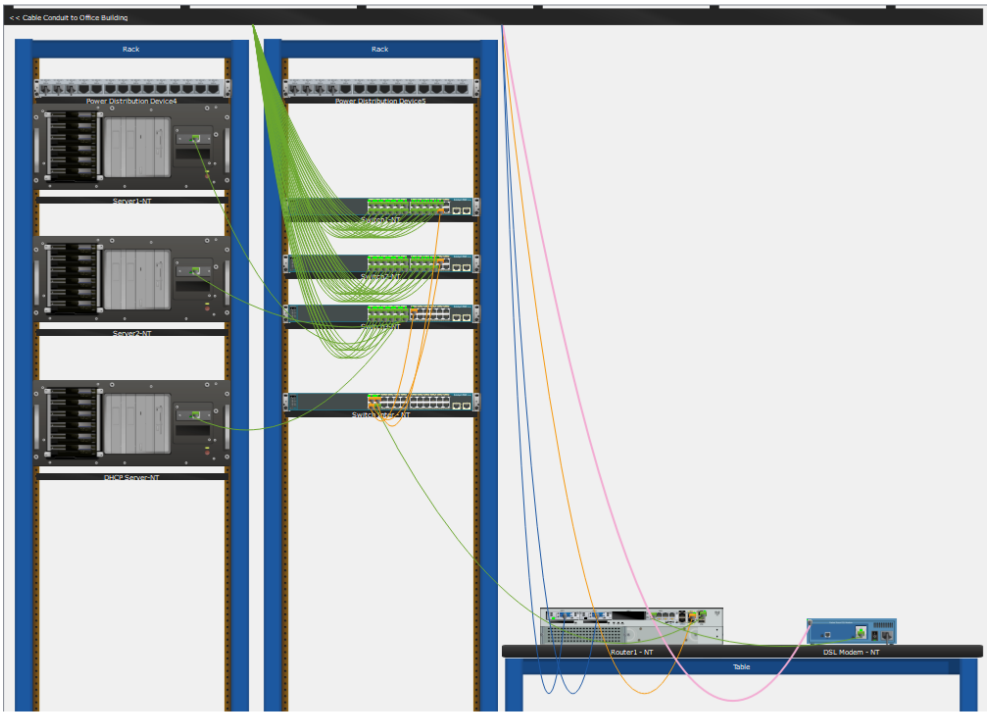


Figure 21: Wiring diagram of main wiring closet at Nha Trang branch

Da Nang branch

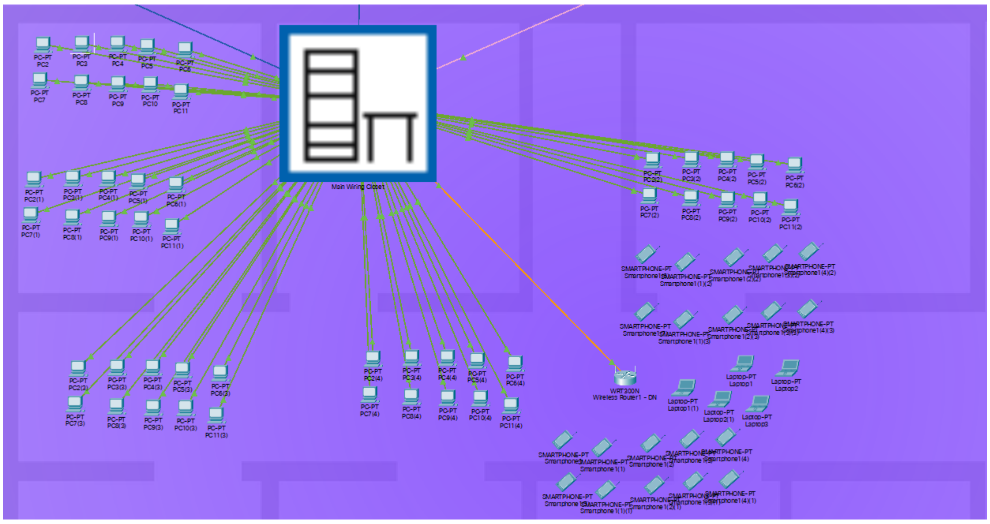

Figure 22: Overview of Wiring diagram at Da Nang branch

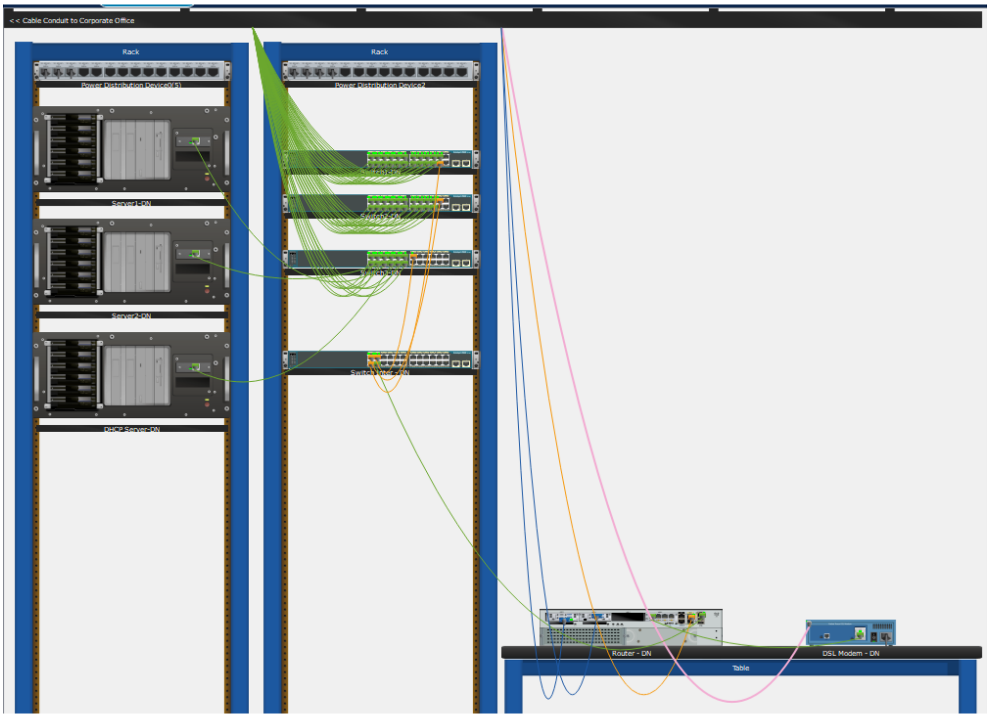


Figure 23: Wiring diagram of main wiring closet at Da Nang branch

# 4 Calculation

## 4.1 Overview

Throughput is how much data actually does travel through the 'channel' successfully. This can be limited by a ton of different things including latency, and what protocol you are using.

Bandwidth is the maximum amount of data that can travel through a 'channel'.

The flows and load parameters of the system reach the peak at about 80% at two specific durations in a day (9 a.m.-11 a.m. and 3 p.m.-4 p.m. => 3 hours total) and can be shared for Head Office and Branches as follows:

- Each server for updating, web access, database accessing, etc. has a total upload and download capacity of about 500 MB/day.
- Each workstation used for web browsing, document downloading, customer transactions, etc. has the total upload and download capacity of about 100 MB/day.
- Each wifi-connected laptop for customers to access uses about 50 MB/day.

**Assumption:** The web server needs to keep running 24/7. The bank (headquarters and branches) opens 8 hours a day (8 a.m. to 4 p.m.), which means that remaining servers, workstations and devices (wifi-connected laptops and smartphones) for customers' use can be shut down after a day of work.

## 4.2 Headquarters

Headquarters in Ho Chi Minh City contains 5 servers and 100 workstations. Assume that there are about 200 customers visiting the headquarter pers day and 100 customers in peak time.

### 4.2.1 Server

The throughput of the server is:

$$\frac{5 * 500}{8 * 3600} * 8 = 0.694 \text{ (Mbps)}$$

The bandwidth of the server is:

$$\frac{5 * 500 * 80\%}{3 * 3600} * 8 = 1.852 \text{ (Mbps)}$$

### 4.2.2 Workstation

The throughput of the workstations is:

$$\frac{100 * 100}{8 * 3600} * 8 = 2.778 \text{ (Mbps)}$$

The bandwidth of the workstations is:

$$\frac{100 * 100 * 80\%}{3 * 3600} * 8 = 5.926 \text{ (Mbps)}$$

### 4.2.3 User

The throughput of the users' devices is:

$$\frac{200 * 50}{8 * 3600} * 8 = 2.778 \text{ (Mbps)}$$

The bandwidth of the users' devices is:

$$\frac{200 * 50 * 80\%}{3 * 3600} * 8 = 5.926 \text{ (Mbps)}$$

### 4.2.4 Total

The total throughput is:

$$0.694 + 2.778 + 2.778 = 6.250 \text{ (Mbps)}$$

The total bandwidth is:

$$1.852 + 5.926 + 5.926 = 13.704 \text{ (Mbps)}$$

### 4.2.5 Safety parameters

Due to the growth rate of 20% every 5 years, the total throughput and total bandwidth need to be recalculated. After the first 5 years, since the bank was established, these two parameters increase by 20%. After the second 5-year period, these two parameters increase by 20% one more time and so on. The recalculated total throughput after the first 5 years is:

$$6.250 + 6.250 * 20\% = 6.250 * 1.2 = 7.500 \text{ (Mbps)}$$

The recalculated total bandwidth after the first 5 years is:

$$13.704 + 13.704 * 20\% = 13.704 * 1.2 = 16.445 \text{ (Mbps)}$$

Generally, the recalculated total throughput after the nth year is:

$$6.250 * 1.2^{\frac{n}{5}} \text{ (Mbps)}$$

And the recalculated total bandwidth after the nth year is:

$$13.704 * 1.2^{\frac{n}{5}} \text{ (Mbps)}$$

## 4.3 Branch

In terms of Branches in Nha Trang City and Da Nang City, each branch contains 3 servers and 50 workstations. Assume that there are about 100 customers visiting each branch per day and 50 customers in peak time.

### 4.3.1 Server

The throughput of the server is:

$$\frac{3 * 500}{8 * 3600} * 8 = 0.417 \text{ (Mbps)}$$

The bandwidth of the server is:

$$\frac{3 * 500 * 80\%}{3 * 3600} * 8 = 0.889 \text{ (Mbps)}$$

### 4.3.2 Workstation

The throughput of the workstations is:

$$\frac{50 * 100}{8 * 3600} * 8 = 1.389 \text{ (Mbps)}$$

The bandwidth of the workstations is:

$$\frac{50 * 100 * 80\%}{3 * 3600} * 8 = 2.963 \text{ (Mbps)}$$

### 4.3.3 User

The throughput of the users' devices is:

$$\frac{100 * 50}{8 * 3600} * 8 = 1.389 \text{ (Mbps)}$$

The bandwidth of the users' devices is:

$$\frac{100 * 50 * 80\%}{3 * 3600} * 8 = 2.9630 \text{ (Mbps)}$$

#### 4.3.4 Total

The total throughput is:

$$0.417 + 1.389 + 1.389 = 3.195 \text{ (Mbps)}$$

The total bandwidth is:

$$0.889 + 2.963 + 2.9630 = 6.815 \text{ (Mbps)}$$

#### 4.3.5 Safety parameters

Due to the growth rate of 20% every 5 years, the total throughput and total bandwidth need to be recalculated. After the first 5 years, since the bank was established, these two parameters increase by 20%. After the second 5-year period, these two parameters increase by 20% one more time and so on. The recalculated total throughput after the first 5 years is:

$$3.195 + 3.195 * 20\% = 3.195 * 1.2 = 3.834 \text{ (Mbps)}$$

The recalculated total bandwidth after the first 5 years is:

$$6.815 + 6.815 * 20\% = 6.815 * 1.2 = 8.178 \text{ (Mbps)}$$

Generally, the recalculated total throughput after the nth year is:

$$3.195 * 1.2^{\frac{n}{5}} \text{ (Mbps)}$$

And the recalculated total bandwidth after the nth year is:

$$6.815 * 1.2^{\frac{n}{5}} \text{ (Mbps)}$$

# 5 Packet Tracer

## 5.1 Switch and VLAN Configuration

In each building, we set up the VLAN configuration as follows:

- **VLAN 10:** Workstations and DHCP servers.
- **VLAN 50:** Servers.

We need to get the workstations and the DHCP servers to be in the same VLAN since its the only way the server can send DHCP response to reply to the workstation's request (or else the DHCP server need to know the workstation's IP address, which is not assigned yet!).

Device Name: Switch5-HQ
Custom Device Model: 2960 IOS15
Hostname: Switch

| Port | Link | VLAN | IP Address | MAC Address |
|---|---|---|---|---|
| FastEthernet0/1 | Up | 10 | -- | 0001.97A6.6E01 |
| FastEthernet0/2 | Up | 10 | -- | 0001.97A6.6E02 |
| FastEthernet0/3 | Up | 10 | -- | 0001.97A6.6E03 |
| FastEthernet0/4 | Up | 10 | -- | 0001.97A6.6E04 |
| FastEthernet0/5 | Up | 10 | -- | 0001.97A6.6E05 |
| FastEthernet0/6 | Up | 10 | -- | 0001.97A6.6E06 |
| FastEthernet0/7 | Up | 10 | -- | 0001.97A6.6E07 |
| FastEthernet0/8 | Up | 10 | -- | 0001.97A6.6E08 |
| FastEthernet0/9 | Up | 10 | -- | 0001.97A6.6E09 |
| FastEthernet0/10 | Up | 10 | -- | 0001.97A6.6E0A |
| FastEthernet0/11 | Up | 10 | -- | 0001.97A6.6E0B |
| FastEthernet0/12 | Up | 10 | -- | 0001.97A6.6E0C |
| FastEthernet0/13 | Up | 10 | -- | 0001.97A6.6E0D |
| FastEthernet0/14 | Up | 10 | -- | 0001.97A6.6E0E |
| FastEthernet0/15 | Up | 10 | -- | 0001.97A6.6E0F |
| FastEthernet0/16 | Up | 10 | -- | 0001.97A6.6E10 |
| FastEthernet0/17 | Up | 50 | -- | 0001.97A6.6E11 |
| FastEthernet0/18 | Up | 50 | -- | 0001.97A6.6E12 |
| FastEthernet0/19 | Up | 10 | -- | 0001.97A6.6E13 |
| FastEthernet0/20 | Up | 10 | -- | 0001.97A6.6E14 |
| FastEthernet0/21 | Down | 1 | -- | 0001.97A6.6E15 |
| FastEthernet0/22 | Down | 1 | -- | 0001.97A6.6E16 |
| FastEthernet0/23 | Down | 1 | -- | 0001.97A6.6E17 |
| FastEthernet0/24 | Down | 1 | -- | 0001.97A6.6E18 |
| GigabitEthernet0/1 | Down | 1 | -- | 0001.97A6.6E19 |
| GigabitEthernet0/2 | Down | 1 | -- | 0001.97A6.6E1A |
| Vlan1 | Down | 1 | <not set> | 0003.E4CA.3E49 |

Physical Location: Intercity > Ho Chi Minh > Corporate Office > Main Wiring Closet > Rack > Switch5-HQ

Figure 24: Configuration of `Switch5_HQ` on the first floor of Headquarters

I just take some example code for VLAN configuration as blow:

```
 en
conf t

vlan 10
name VLAN10
exit

vlan 50
name VLAN50
exit

int range f0/1-16
sw mode acc
sw acc vlan 10
spanning-tree portfast
no shut
exit

int range f0/17-18
sw mode acc
sw acc vlan 50
spanning-tree portfast
no shut
exit

do wr
```

## 5.2 Wireless Router Configuration

In our system, the Wireless Routers are set up using WPA2-PSK authentication algorithm with AES encryption to ensure the security of the connections.

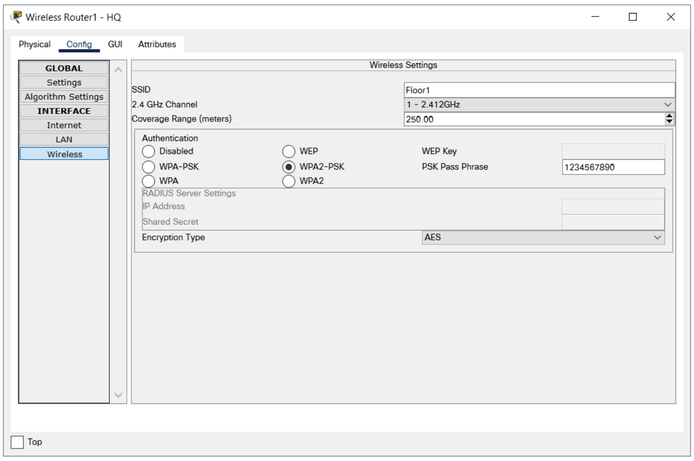


Figure 25: Wireless Settings of `Wireless Router1 - HQ` on the first floor of Headquarters

Here is the Internet and Network Setup of the same router:

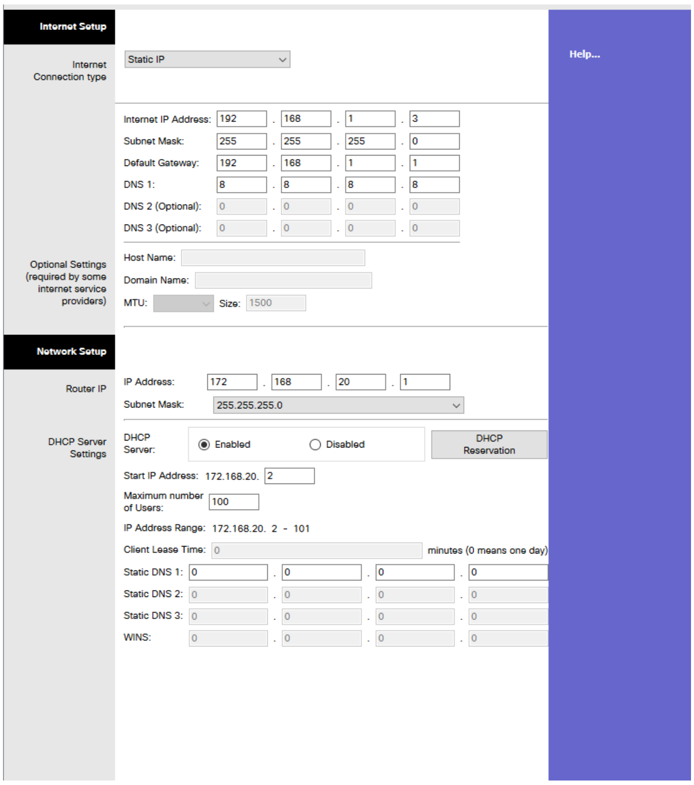


Figure 26: Internet and Network Setup of `Wireless Router1 - HQ` on the first floor of Headquarters

### 5.3 OSPF Protocol Setup

The connection between the Headquarters and the Branches can be enhanced by using OSPF protocol.

We use the following commands to configure the edge routers at the Headquarters, the 2 Branches.

```
en
conf t
router ospf ID
area AREA
```

where ID depends on the area.

We let AREA = 0 as these routers are of the backbone area. Next, the ID is set to 1 for the Headquarters, 2 for the Nha Trang Branch, and 3 for the Da Nang Branch.

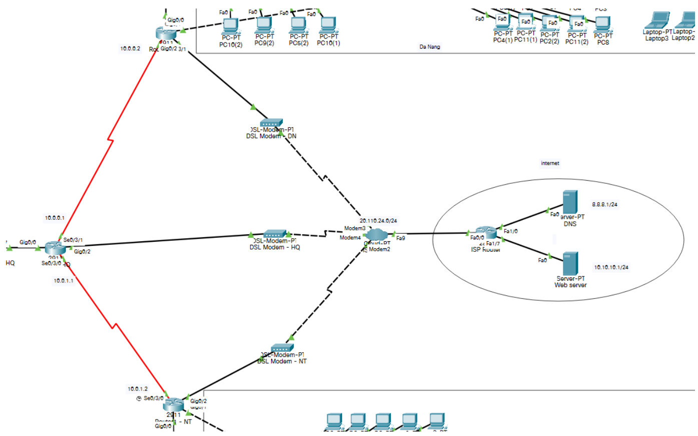

Figure 27: Core network devices and the devices on the other side of the cloud

### 5.4 Security Setup

In this section, we are going to use access control list (ACL) to limit the activity at the APs by prevent reaching the workstations from other area networks.

The following commands are applied to the 3 edge routers of the 3 buildings:

```
en
conf t
ip access-list standard BBBank
deny 10.0.1.2 0.0.0.0
deny 10.1.1.2 0.0.0.0
deny 10.2.1.2 0.0.0.0
permit 10.0.0.0 0.255.255.255
deny any
exit
```

Next, we apply the ACL to the workstations:

```
int GigabitEthernet0/0
ip access-group BBBank out
exit
```

Now we apply the ACL to the servers:

```
int GigabitEthernet0/1
ip access-group BBBank out
exit
```

Finally, we can save this configuration:

```
copy running-config startup-config
write
```

# 6 System testing

In this section, we are going to test our system using 2 tools.

- The first is `ping`, which uses ICMP messages, to test the connectivity between any two nodes.
- The second tool is `tracert`, which uses ICMP messages with suitable `TTL` field, to test if the actual routing is the same as our design. Since we use *static routing* as our routing strategy, the routing observed should always stay constant.

## 6.1 Testing with Ping

In the first test, we test the connection between workstations in our Headquarters. The result is captured as follows:

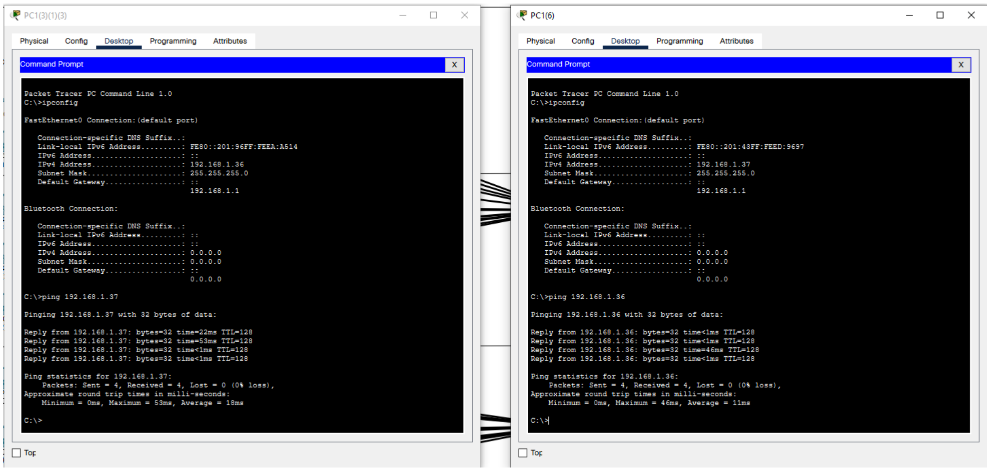


Figure 28: Between workstations in Headquarters

As we can see, the two arbitrarily chosen workstations can `ping` each other at relatively low average RTT (18ms and 11ms respectively) and 0% loss rate. This performant result roots from the fact the workstations are in close vicinity of each other.

In the second test, we test the connection between workstations in our Nha Trang Branch. The result is captured as follows:

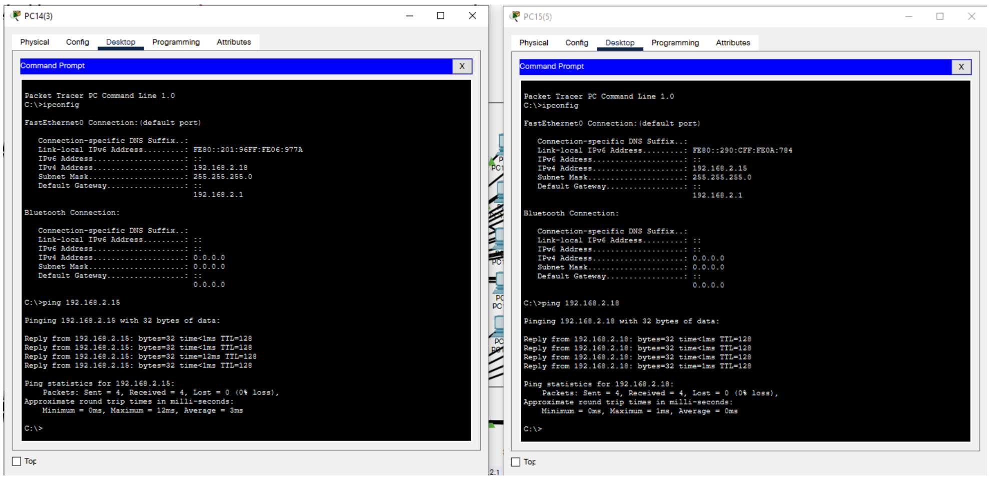


Figure 29: Between workstations in Nha Trang Branch

As we can see, the two arbitrarily chosen workstations can `ping` each other at relatively low average RTT (3ms and 0ms respectively) and 0% loss rate. This performant result roots from the fact the workstations are in close vicinity of each other.

In the third test, we test the connection between workstations in our Da Nang Branch. The result is captured as follows:

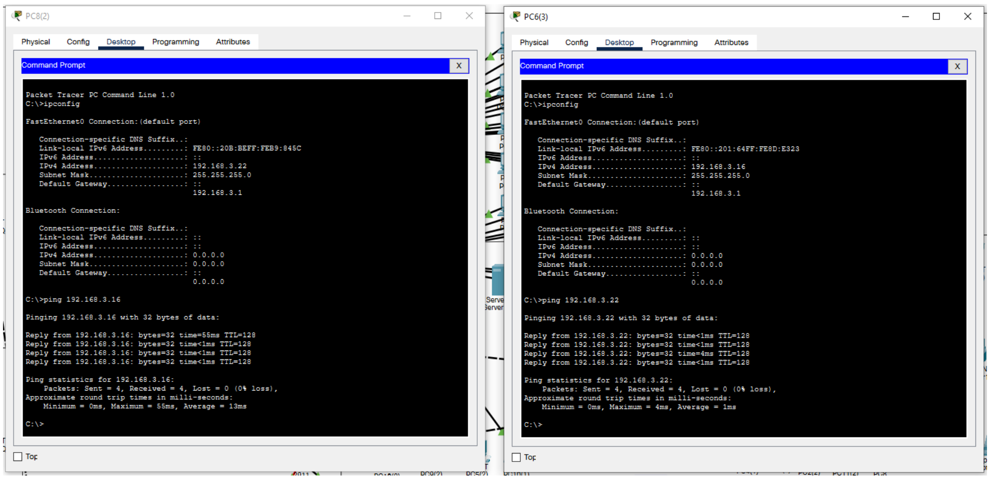


Figure 30: Between workstations in Da Nang Branch

As we can see, the two arbitrarily chosen workstations can `ping` each other at relatively low average RTT (13ms and 1ms respectively) and 0% loss rate. This performant result roots from the fact the workstations are in close vicinity of each other.

In the next test, we test the connection between a workstation in our Headquarters and a workstation in the Nha Trang Branch. The result is captured as follows:

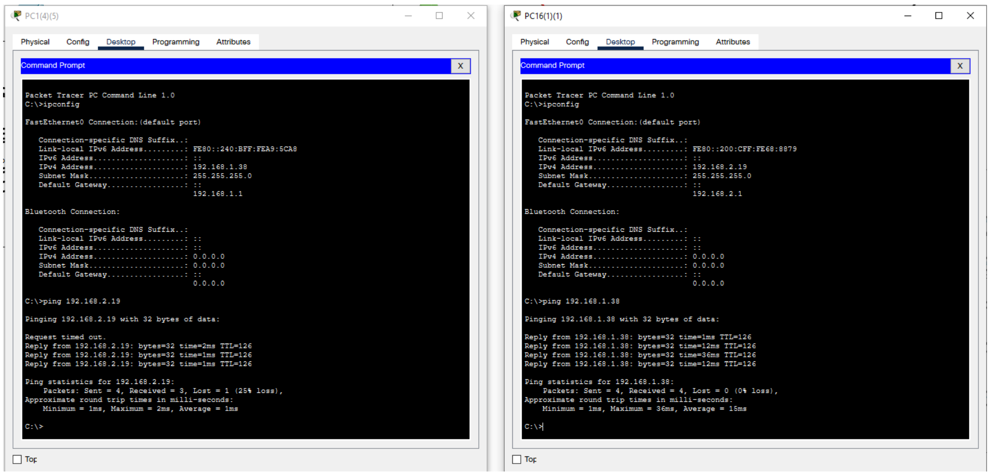

Figure 31: Between workstations in Headquarters and Nha Trang Branch

As we can see, the two arbitrarily chosen workstations can `ping` each other at relatively low average RTT (1ms and 15ms respectively) and 1 lost packet. The lost packets are often observed in our model when we test for connectivity across buildings as we will cover in the next parts.

Now, we test the connection between a workstation in our Headquarters and a workstation in the Da Nang Branch. The result is captured as follows:

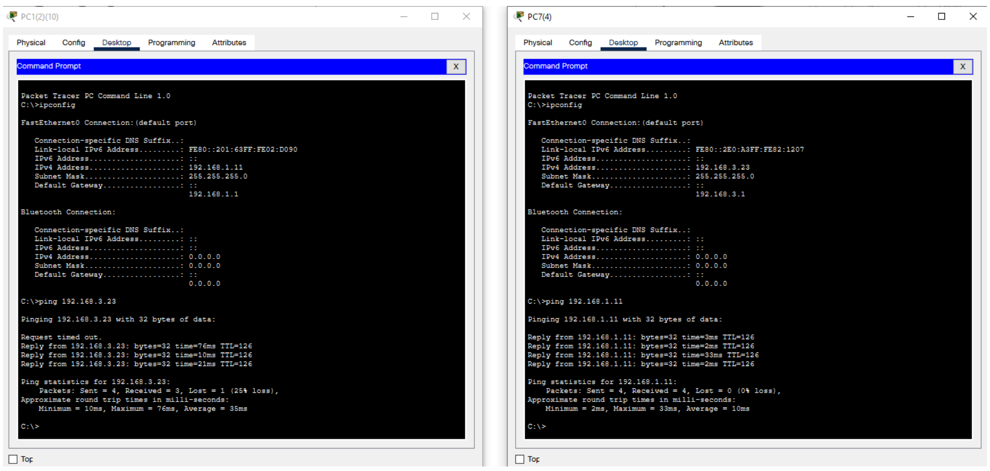

Figure 32: Between workstations in Headquarters and Da Nang Branch

As we can see, the two arbitrarily chosen workstations can `ping` each other at relatively low average RTT (35ms and 10ms respectively) and 1 lost packet.

Now, we test the connection between a workstation in the Nha Trang Branch and a workstation in the Da Nang Branch. The result is captured as follows:

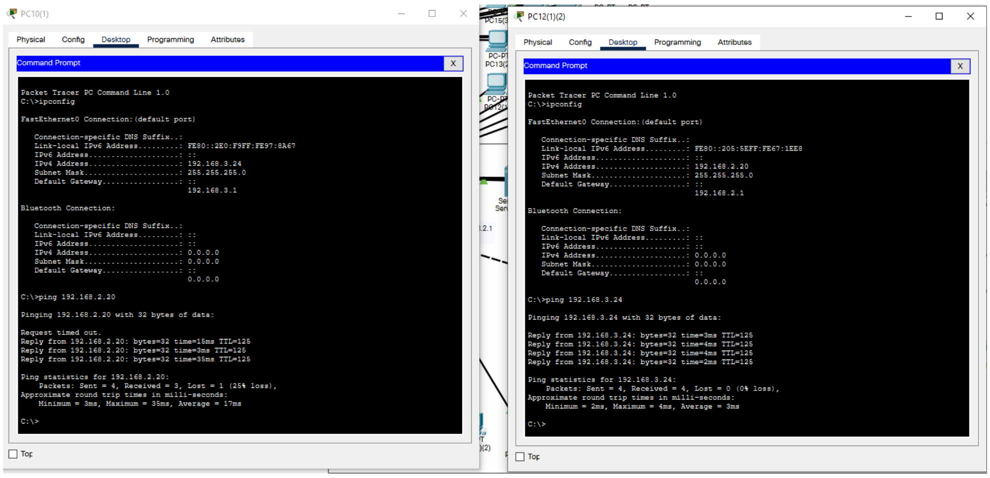

Figure 33: Between workstations in Nha Trang Branch and Da Nang Branch

As we can see, the two arbitrarily chosen workstations can `ping` each other at relatively low average RTT (17ms and 3ms respectively) and 1 lost packet.

Now, we test the connection between a smartphone and a laptop in the Headquarters. The result is captured as follows:

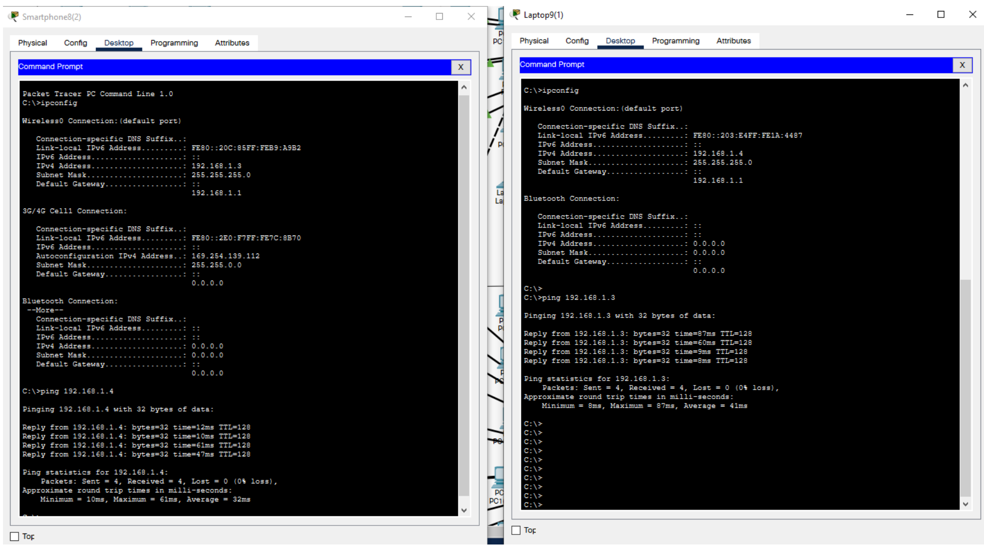

Figure 34: Between smartphones and laptops in Headquarters

As we can see, the two arbitrarily chosen devices can `ping` each other at relatively low average RTT (32ms and 41ms respectively) and 0 lost packets. One prominent fact here is that the RTT is considerably higher in the case of `ping`ing from 2 workstations. This fact could result from the 2 devices tested here having wireless connection, while the 2 workstations have wired connection, which provides more speed.

Now, we test the connection between a smartphone and a workstation in the Headquarters. The result is captured as follows:

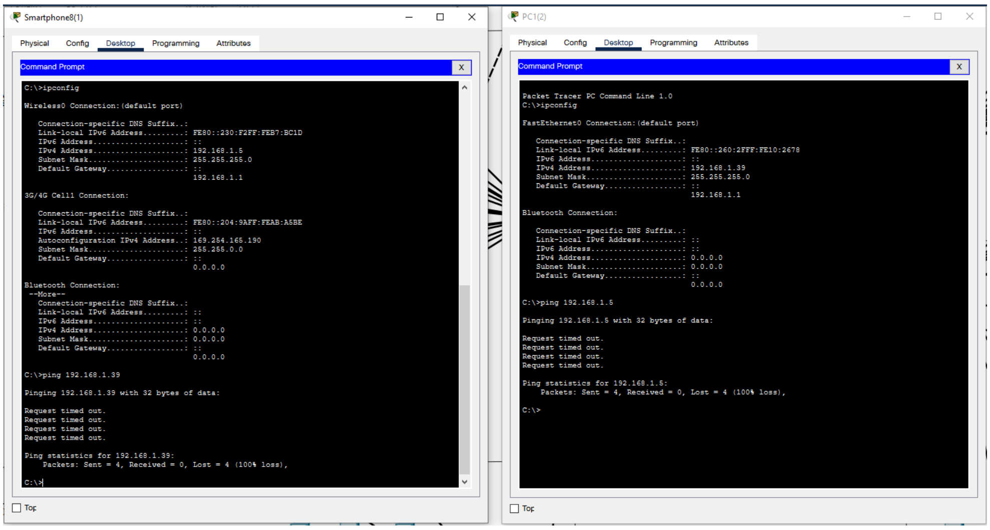

Figure 35: Between smartphones and workstations in Headquarters

The 2 devices cannot `ping` each other. This behaviour is expected as we do not want unauthorized devices to be able to reach our workstations.

### 6.2 Testing with Tracert

In the first `tracert` test, we test the routing from a workstation in the Headquarters and a workstation in the Da Nang Branch. The result is captured as follows:

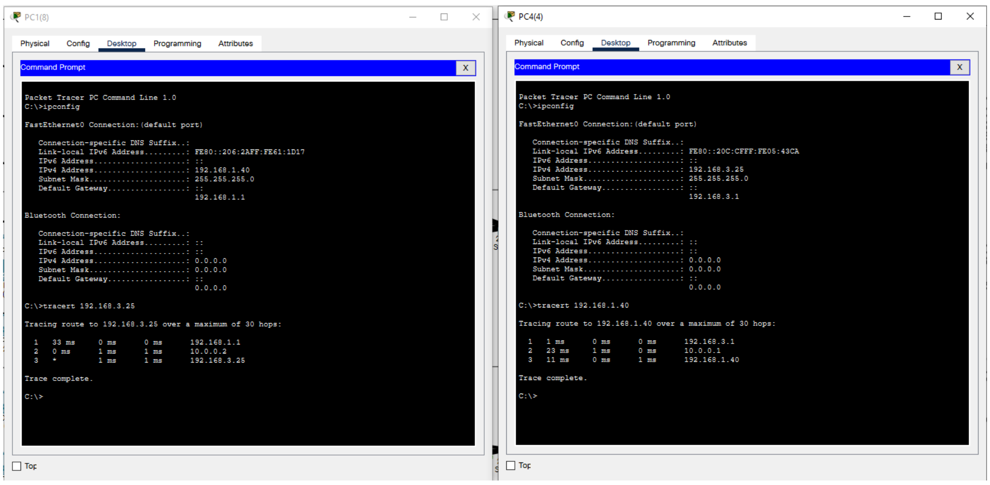

Figure 36: Between workstations in Headquarters and Da Nang Branch

We can see that it took 3 hops for the packets to reach the destination, which is as we have expected. It took the first hop to the edge router, the second hop to the router at the destination, and the last hop to the destination workstation.

In the second `tracert` test, we test the routing from a workstation in the Headquarters and a workstation in the Nha Trang Branch. The result is captured as follows:

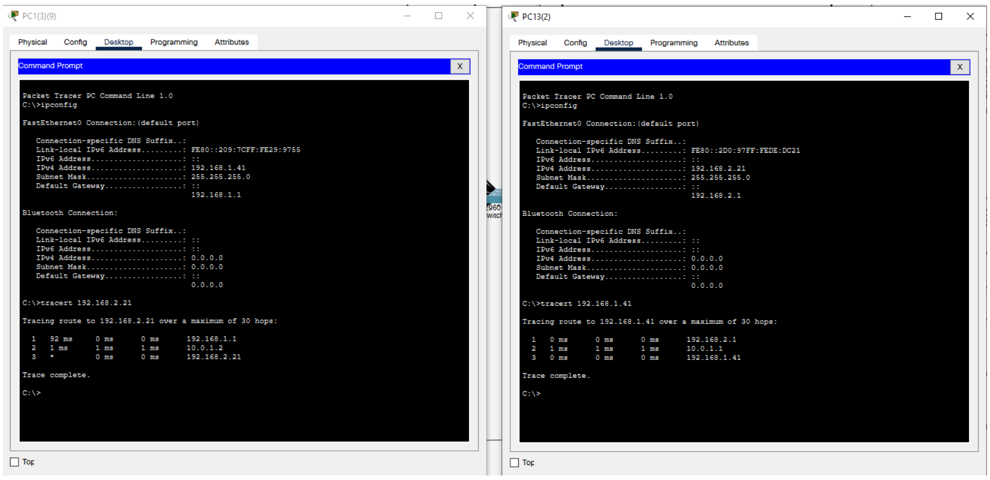

Figure 37: Between workstations in Headquarters and Nha Trang Branch

We can see that it took 3 hops for the packets to reach the destination, which is also as we have expected. The hops are equivalent to the aforementioned case.

In the last `tracert` test, we test the routing from a workstation in the Nha Trang Branch and a workstation in the Da Nang Branch. The result is captured as follows:

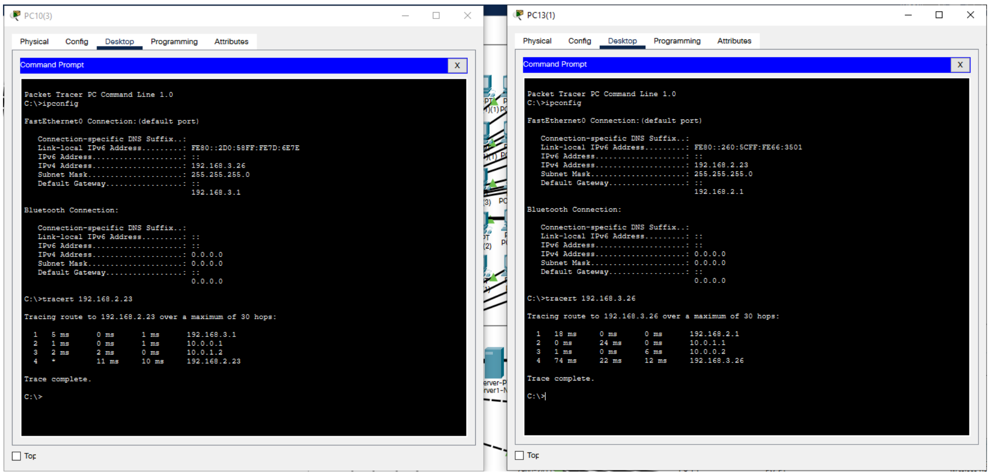

Figure 38: Between workstations in Nha Trang Branch and Da Nang Branch

We can see that it took 4 hops for the packets to reach the destination, which is also as we have expected as we only use 2 leased lines between the buildings' routers for economical purpose. It took the first hop to the edge router at one Branch, the second hop to the router at the Headquarters, the third hop to the router at the destination Branch, and the last hop to the destination workstation.

# 7 Result

## 7.1 Re-evaluation of the designed network system

### 7.1.1 Reliability

- Receivable: The receivers can receive the messages sent by network devices.
- It's possible that our system is experiencing packet loss. This could happen during the first route or ping because the network has to fill the switch's MAC table. After this period, our system will be able to deliver packets with minimal packet loss.

### 7.1.2 Ease of upgrade

- Due to extended star topology, it is easy to scale up by adding more sub-central devices.
- When a branch is added to the network, we simply install and configure a new router for it, then connect it to the headquarters by a leased line and to the Internet by DSL.

### 7.1.3 Diverse support software

- The network system provides Ethernet and wireless connections for devices to access the Internet.

### 7.1.4 Safety

- Prevent the wireless devices ping to other devices.
- Support the method for limiting IP address entry and exit from the Internet.

### 7.1.5 Security of data

- When there are packet theft assaults, sensitive data is kept private.

### 7.1.6 Scalability

- For the problem of bandwidth and throughput, with the growth rate of 20% per 5 years, we provide the formular to recalculate these two parameters annually to prepare for the network having good performance in the future.

## 7.2 Remaining Problems

### 7.2.1 Scalability

- In the future, if the bank grows unexpectedly, more branches need establishing, there should be another enhancement in the network to adapt the scalability of the bank.
- Serial link for headquarters-branch may cause bottleneck problem when the bank grower bigger.

#### 7.2.2 Security

- Servers are not placed in a separate switch with their own VLANs and connecting to gateway routers through a separate port, which help the system implement network configurations to enhance the network's security more conveniently.
- Not applying ACL tables to limit the access from wireless devices to other devices.

### 7.3 Development orientation in the future

- Enhance security of the network to protect customer's data.
- Build a network security room to detect and resolve situations in real time.
- Implement the ping from the internal network to the Web server.
- When the bank grows larger, find strategies to improve the network at the lowest cost while maintaining good performance. A bank typically has a lengthy life period, thus we need to design the network to have as long a life span as feasible while keeping maintenance to a minimum.

## 8 Conclusion

Through this assignment, we knew how to design a network for a real business. The theory on class can be applied for deeper understanding. Cisco packet tracer is a really good software helping us complete this assignment although there were a lot of difficult to be acquainted with at the beginning. After all, we did our best and learnt a lot about computer network.

# References

[1] LearnTech Training. Connecting Cisco Router to DSL Modem with ISP Configurations. https://www.youtube.com/watch?v=MXNM7_Kykaw&t=892s, 2018. [Online; accessed 9-Feb-2018].

[2] Electrical Computer Engineering Project. Static routing with Connecting 4 routers with explanation | Cisco Packet Tracer Tutorial 3. https://www.youtube.com/watch?v=rZw_b0wpQ00&t=672s, 2019. [Online; accessed 21-Jul-2019].

[3] Phil Karn. Classless Inter-Domain Routing. https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing, 1980.