

HO CHI MINH UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING



COMPUTER NETWORKS
SEMESTER 202

INSTRUCTOR: NGUYEN LE DUY LAI

Assignment 2 Report: Computer network design for building of the bank

Student name

DOAN ANH TIEN

HO HOANG THIEN LONG

Student ID

1852789

1852161

August 25, 2021

Contents

1	Introduction	3
2	Requirements analysis	3
2.1	Functional requirements	3
2.1.1	Internal LAN	3
2.1.2	WAN	3
2.2	Non-functional requirements	4
2.2.1	Internal LAN	4
3	Survey checklist	4
3.1	Customer information	4
3.2	Facility information	4
3.3	Network and system information	5
3.4	Installation location walkthrough	5
4	Network structure	6
4.1	WAN diagram	6
4.2	Internal LANs diagram	7
4.2.1	HQ	7
4.2.2	Branches	12
5	IP table	16
5.1	WAN	16
5.2	Internal LANs	17
5.2.1	HQ	17
5.2.2	Branches	18
5.2.3	Summary	19
6	Area with high load	21
6.1	WAN	21
6.2	Internal LANs	21
6.2.1	HQ	21
6.2.2	Branches	21
7	List of recommended equipment	22
7.1	HQ	22
7.2	Branches	23
8	Physical setup	24
8.1	HQ	25
8.2	Branches	26

9	Implementation on Packet Tracer	27
9.1	WAN	27
9.2	Internal LANs	29
9.2.1	HQ	29
9.2.2	Branches	39
9.2.3	Internet	39
10	Result	40
10.1	Connect between PCs in the same VLAN	40
10.2	Connect PCs between VLANs	40
10.3	Connect PCs between Headquarters and branches	41
10.4	Connect to servers in the DMZ	42
10.5	No connections from Customers devices to PCs on the LAN	42
10.6	Connect to the Internet to a Web server	43
10.7	bbbank.com webserver	44
10.8	Exchange mails via Mailserver of different branches	45
10.9	Access FTP servers	48
10.10	Check netflow monitor of gateway	50
10.11	Telnet to networking devices from admin workstations	51
11	Evaluation	52
11.1	Advantages	52
11.1.1	Connectivity	52
11.1.2	Scalability	52
11.1.3	Security	52
11.2	Disadvantages	52
11.2.1	Redundancy	52
11.3	Remaining problems	52
12	Conclusion	53

1 Introduction

In semester 202, we are working on Computer Networks and our second assignment is build networking system for a banking system using Packet Tracer, in which implementing the network topology for 3 facility, HQ and 2 branches of the bank name BBBank, implementing some networking applications as well as security services.

2 Requirements analysis

2.1 Functional requirements

2.1.1 Internal LAN

- Each workstations shall be provided with office applications as text editor, email and file transferring and web browsing.
- The servers is used for database, email, file transferring, bank website and network management.
- The networking devices is used to connect different VLANs to each other.
- The network shall be organized as VLANs structure.
- The VLANs shall be organized as VTP (VLAN Trunking Protocol).
- The network shall dynamically assigning private IP address to all devices using DHCP.
- The network shall translate private IP address to public IP address via NAT.
- The network shall have Internet connection.
- The network shall have wireless connection for guests to accessing to Internet.
- The network shall deny all strange IP address connecting to internal network.
- The network shall deny all strange networking devices accessing internal network.
- The network shall allow 2 administrators to monitor traffic and access internal networking devices via telnet.
- The network in 2 branches Da Nang and Nha Trang have similar structure to HQ's.

2.1.2 WAN

- The 2 branches must go through the HQ to access Internet and communicate with each other.
- The WAN must have a private connection line among the 3 buildings.

2.2 Non-functional requirements

2.2.1 Internal LAN

- HQ: The network shall connect around 100 workstations, 5 servers and 12 networking devices.
- The network in each branches shall connect around 50 workstations, 3 servers, 5 or more networking devices.
- The network shall use new networking devices that can handle up to 100/1000 Mbps wired and wireless connection.
- The network shall enable the flow and load parameters to be properly shared between headquarters and branches at peak hours 9-11 AM and 3-4 PM).
- The total upload and download capacity of servers shall be about 500 MB/day.
- The total upload and download capacity of workstations shall be about 100 MB/day.
- The WiFi-connected laptop for guests shall access about 50 MB/day.

3 Survey checklist

The first step in the whole process of network deployment is to ensure that our operation is well-prepared and matched with customer requirements. This lead the site survey, a fundamental process where we assess network properties in a specific environment, to be one of the most important task to be finished.

After comprehend the requirements and other information such as facility type, devices, number of floors, we need to plan our survey checklist in order to obtain more detailed information, details follow as these sections.

3.1 Customer information

- Contact information including name, address, phone number of company and IT chief officer of the bank?

3.2 Facility information

- Facility structure in terms of floors, rooms, departments? (Where is customer area? Where is staff area? Where are workstation rooms, where is IT room)?
- A map of floor plan of the area your network will cover?
- Electricity installation map?
- What is peak hour?
- Average number of customers?

3.3 Network and system information

- Determine client operating systems (workstations)?
- Determine Wireless protocol? (WiFi?)
- Verify the physical environment (cable, outdoor grounding, lightning protection)?
- Location of public router?
- Verify the setup for printing devices network?
- Verify if there is any optional software purchase needed?

3.4 Installation location walkthrough

- Perform a walkthrough in the facility to determine more reality factors.
- Identify and list possible sources of interference. (modular walls and metal equipment racks, for example, can sometimes weaken wireless signals).
- Note the locations where wireless access points can be mounted, such as ceilings and pillars.
- Note the locations of the existing wired network closets and existing access points
- Use wireless site survey software or specialized survey tool to gather data from wireless access point that have been setup in desired locations for testing process.
- Determine the areas to install networking devices to get a high-performing and efficient network.
- Check details of the areas that may not mentioned on the main coverage map.
- Check and anticipate zones that difficult to deploy devices or transmit signals.

4 Network structure

4.1 WAN diagram

The two branches will be connected to Headquarters via the WAN network by using the leased lines (Serial). Between these three locations are the intermediate routers representing for different areas in Vietnam such as Bien Hoa, Da Lat, Pleiku, ... This setup will enable us to create a realistic WAN network with the aid of Cisco Packet Tracer.

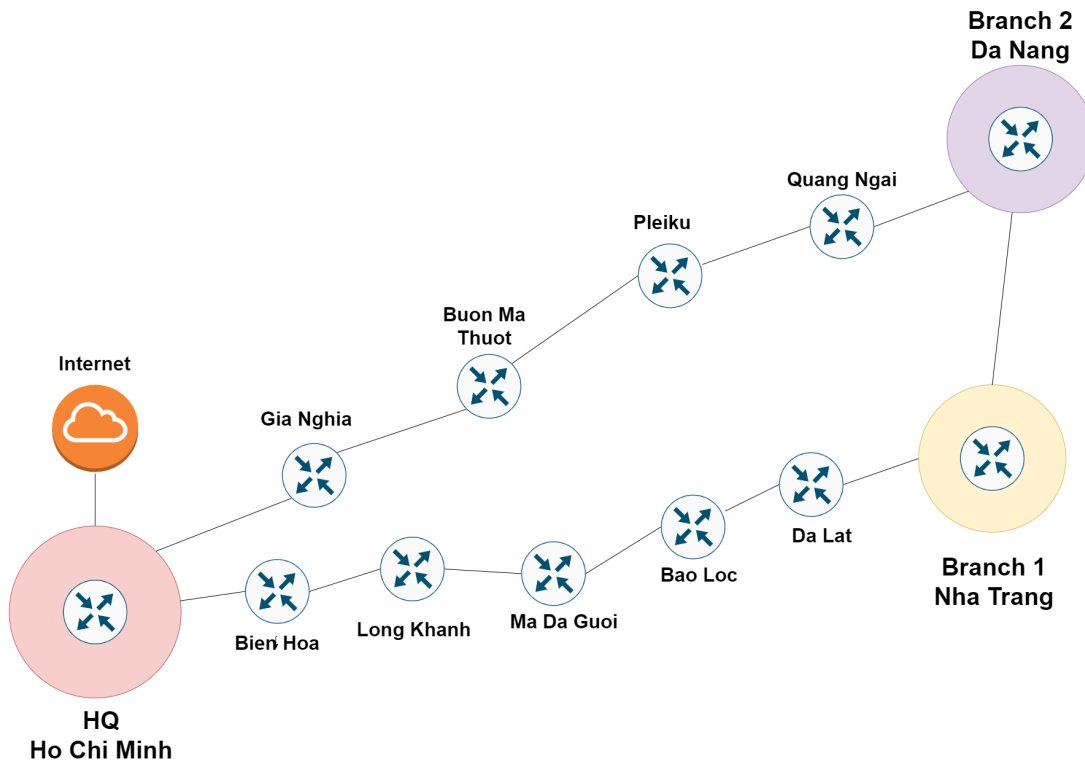


Figure 1: WAN Network

Each routers can forward and receive packets from other. We also add a connection between two branches since this factor is not specified in the requirement of the assignment. Due to that, the load to HQ might be decreased and the bottleneck incident might be prevented.

Although there are multiple connections in this WAN network, it does not give two branches the permission to freely access to the Internet at their own will. The two branches cannot access the Internet via any intermediate routers in different provinces. They must access to the Internet through the gateway of HQ, enabling the HQ can observe the internet activities of their staffs and prevent any unwanted or malicious actions. They cannot access the Internet via any intermediate routers in different provinces.

4.2 Internal LANs diagram

4.2.1 HQ

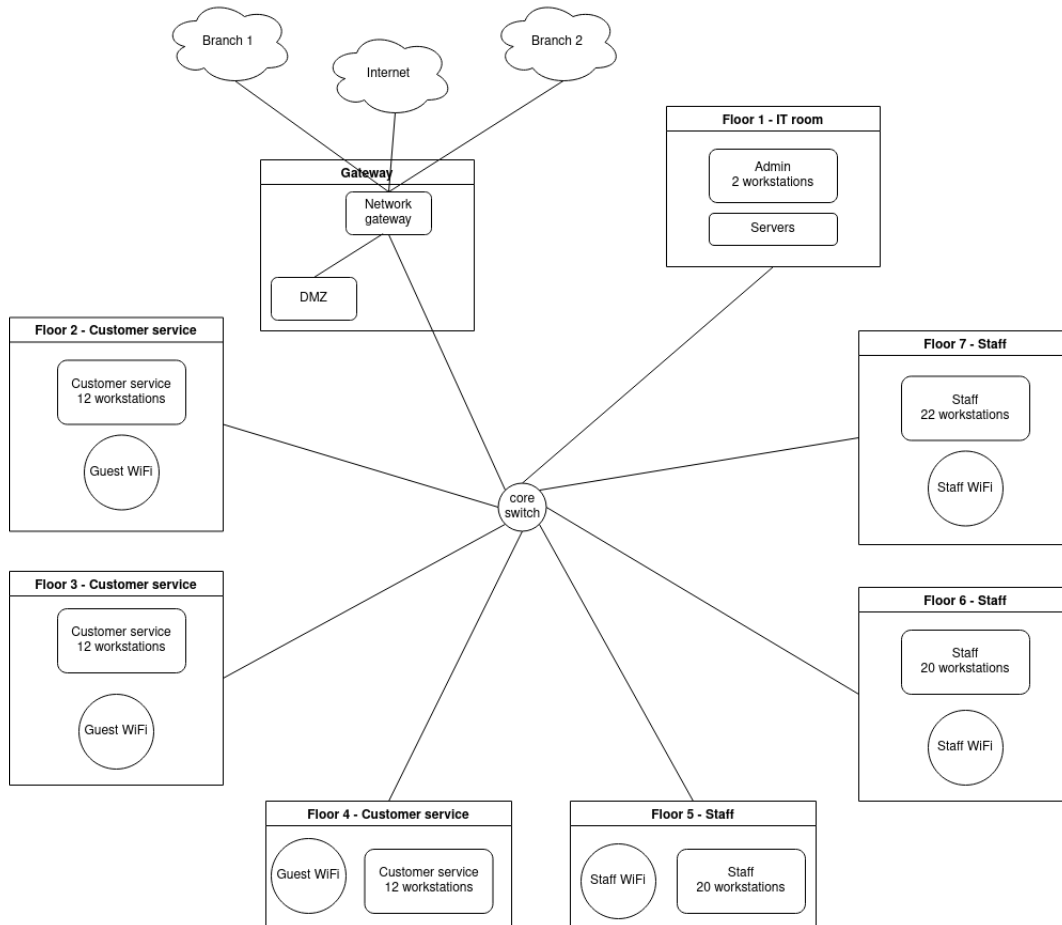


Figure 2: HQ internal network topology

The HQ internal structure follows the tree topology in which core switch is the root. There are 8 main sections connected together via a core switch, 8 sections are

- Floor 1 - IT: internal servers and 2 workstations for 2 administrators.
- Floor (2 - 4) - Customer service: 12 workstations and a Wi-Fi access point for guests for each floor.
- Floor (5 - 7) - Staff: 20 workstations and a Wi-Fi access point for staff for each floor; except for Floor 7 in which there 22 workstations for staffs and 2 additional workstations for HQ managers.

- Gateway: consists of a DMZ area for public webserver, a network gateway to control the traffic going in and going out the network, access to Internet and connect to other 2 branches.
- Core switch: a VTP server responsible for creating VLANs, synchronizing VLANs, switching and routing packets between VLANs, creating firewall to prevent guests and other outside factors accessing to workstations and essential devices. VLAN subnet is be discussed further in the IP diagram section.

VTP is used for easier configuring client switches, because switches in the same VTP domain synchronize with each other, avoid unwanted devices to access to the switching systems by setting domain name and password.

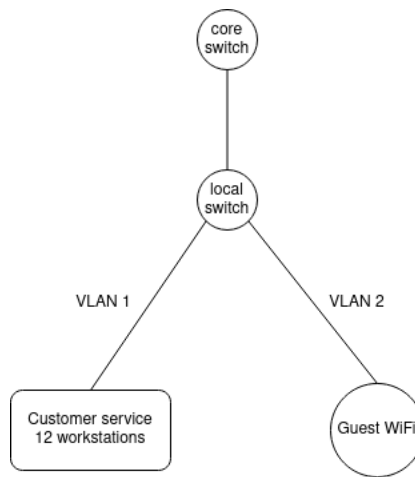


Figure 3: Customer service network topology (Floor 2 - 4)

The local switch is a VTP client.

The customer service network on each floor is formed by the local switch, the local switch is divided into 2 VLANs, one for staff workstations and one for guest Wi-Fi in order to increase security. The VLAN 2 cannot access to VLAN 1 and other staff network, it can only access to Internet and public servers.

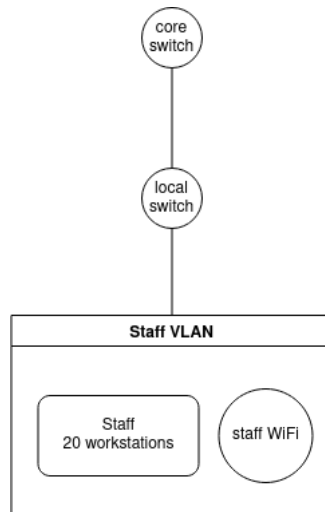


Figure 4: Staff network topology (Floor 5 - 7)

The staff network on each floor is formed by the local switch, because customers is not allowed to come to this floor, so there is no need to divide more VLANs, staff workstations and staff Wi-Fi can be on the same VLAN.

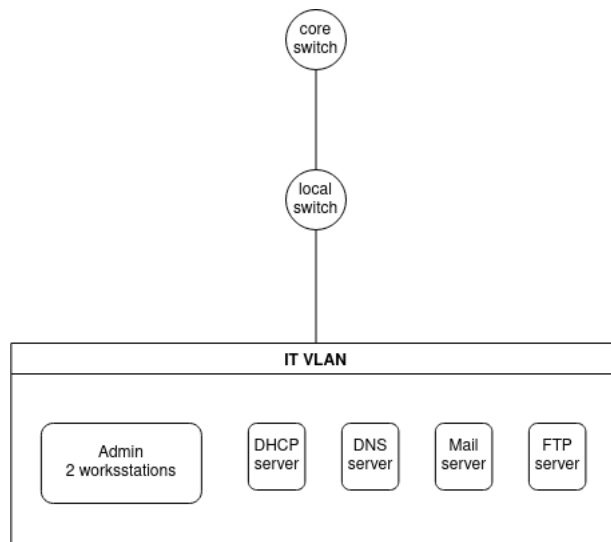


Figure 5: IT network topology (Floor 1)

The IT network including 2 administrator workstations and 4 internal servers is on the same VLAN.

- Administrator workstations: have privilege to access and modify all internal networking devices via telnet; have 2 workstations to increase redundancy, if one workstation is failed, the other workstation can still manage the network.
- DHCP server: dynamically assign IP address to all of end devices joining the network depending on the VLAN they are in.
- DNS server: holds a list of allowed domain names, end devices use this server to translate input domain name to IP address. The 2 branches of the bank also use this server.
- Mail server: Internal mail server for staff of HQ and 2 branches, which mean guests or other unknown end devices cannot access this mail server.
- FTP server: Internal file sharing server for staff of HQ and 2 branches, which mean guests or other unknown end devices cannot access this FTP server.

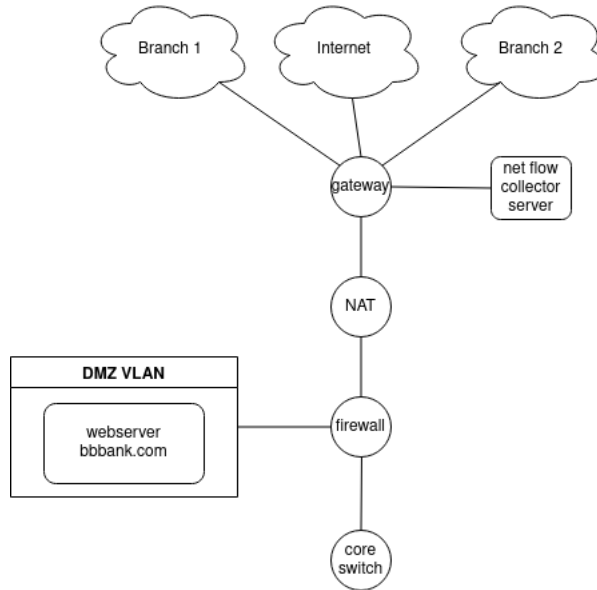


Figure 6: Gateway network topology

The gateway network is the door between internal network and outside network. The gateway consist 5 main parts

- Firewall: block unwanted traffic from outside accessing internal network. Only allow staff of the 2 branches to access the internal network, other traffic can only access the DMZ area.
- DMZ VLAN: consists of the public bank webserver bbbank.com. This area can be accessed by most of end devices.
- NAT: translate internal end devices' private IP address to public IP address. The IP translation will be discussed further in IP diagram section.
- Gateway: The gateway router connect inside and outside network including Internet, 2 branches of the bank. The gateway will record all the traffic (packets) information going in and out of the HQ and send to the net flow collector server.
- Net flow collector server: Monitor traffic information from the gateway and do statistics.

4.2.2 Branches

2 branches' network structure are similar to the HQ, but in smaller scale and the same to each other. Therefore, we will represent only one model used for the 2 branches.

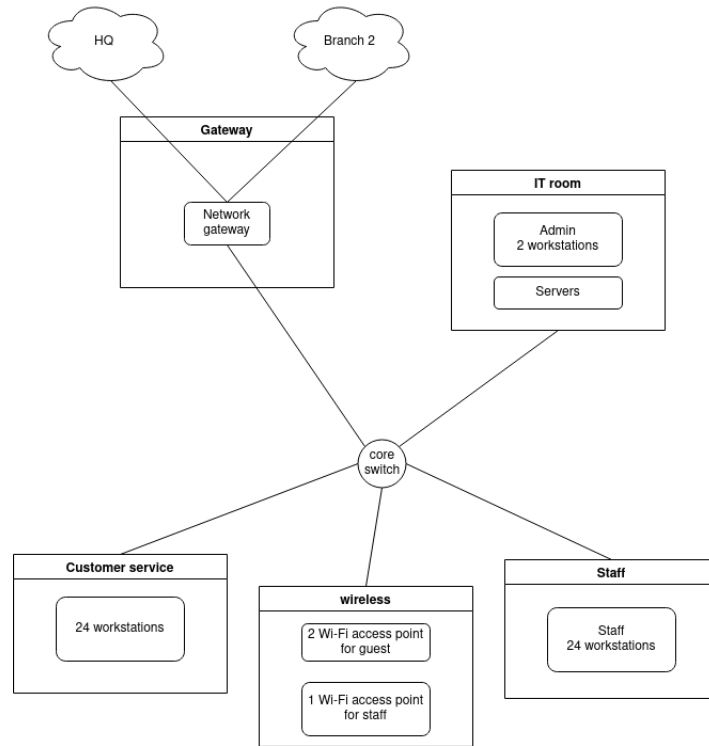


Figure 7: Internal network topology of branches

The branch building only have 2 floors, so we divide floor 2 into 2 seperate sections: customer service and staff

- Floor 1 - IT: internal servers and 2 workstations for 2 administrators.
- Floor 2 - Customer service section: 24 workstations.
- Floor 2 - Staff section: 24 workstations.
- Wireless section: 2 Wi-Fi access point for guests and 1 Wi-Fi access point for staff.
- Gateway: consists of the network gateway to other branch and HQ; there is no DMZ area.

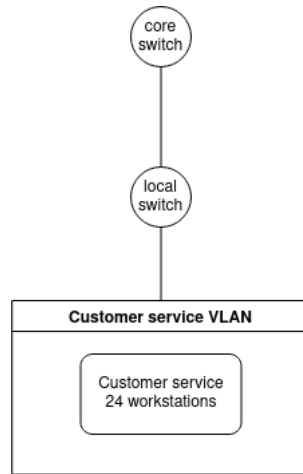


Figure 8: Customer service topology of branches

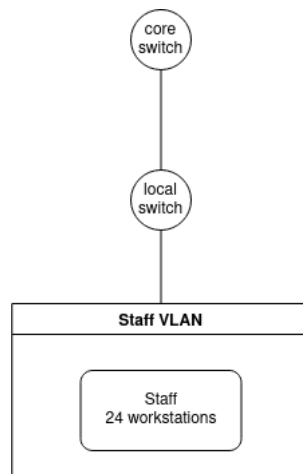


Figure 9: Staff topology of branches

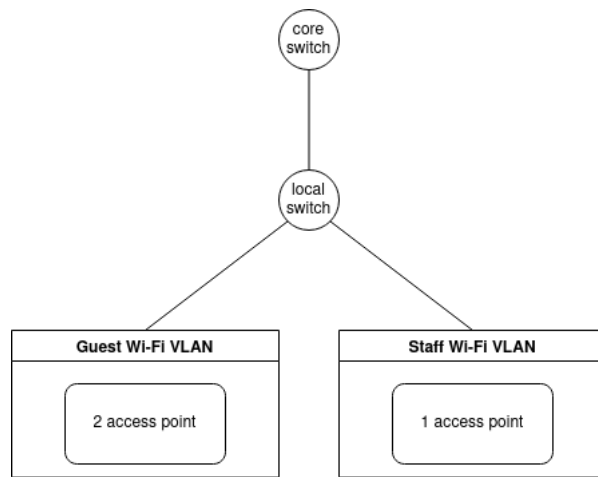


Figure 10: Wireless topology of branches

There are 2 VLANs created on a local switch

- Guest Wi-Fi VLAN: consist of 2 Wi-Fi access points for guests.
- Staff Wi-Fi VLAN: consist of 1 Wi-Fi access point for staff.

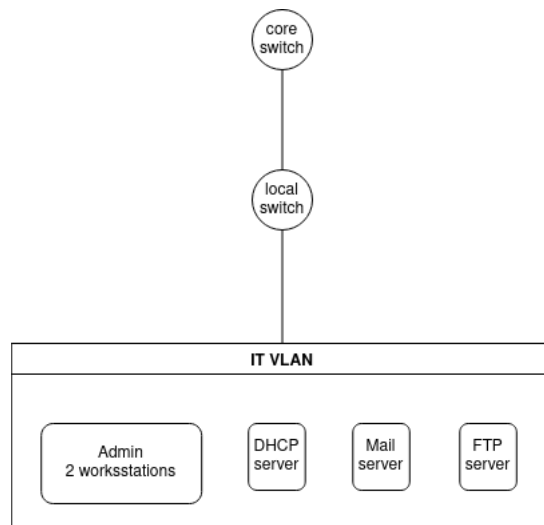


Figure 11: IT and servers network topology of branches

The role of these administrators and servers are similar to IT room in HQ, except there is no DNS server, end devices will use DNS server of HQ to translate domain name to IP address. Mail server, FTP server can be shared with HQ and other branch.

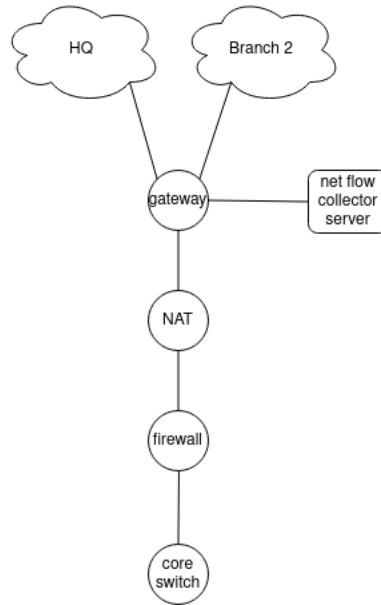


Figure 12: gateway network topology of branches

The structure is the similar to HQ gateway structure, except there is no DMZ area due to the fact that there is no public server can be accessed by unknown end devices; the gateway router connect HQ and other branches, if one internal end devices want to access to Internet, it must pass the gateway of HQ.

5 IP table

5.1 WAN

Area	IP Address	Subnet Mask
HQ - Bien Hoa	10.0.0.1 - 10.0.0.2	255.0.0.0
HQ - Gia Nghia	16.0.0.1 - 16.0.0.2	255.0.0.0
Nha Trang - Da Nang	9.0.0.1 - 9.0.0.2	255.0.0.0
Bien Hoa - Long Khanh	11.0.0.1 - 11.0.0.2	255.0.0.0
Long Khanh - Ma Da Guoi	12.0.0.1 - 12.0.0.2	255.0.0.0
Ma Da Guoi - Bao Loc	13.0.0.1 - 13.0.0.2	255.0.0.0
Bao Loc - Da Lat	14.0.0.1 - 14.0.0.2	255.0.0.0
Da Lat - Nha Trang	15.0.0.1 - 15.0.0.2	255.0.0.0
Gia Nghia - Buon Ma Thuat	17.0.0.1 - 17.0.0.2	255.0.0.0
Buon Ma Thuat - Pleiku	18.0.0.1 - 18.0.0.2	255.0.0.0
Pleiku - Quang Ngai	19.0.0.1 - 19.0.0.2	255.0.0.0
Quang Ngai - Da Nang	20.0.0.1 - 20.0.0.2	255.0.0.0
HQ Gateway - Internet	8.8.8.2, 8.8.8.8	255.255.255.0

HQ and 2 branches public IP subnet

Area	IP Address	Subnet Mask
HQ	161.228.x.x	255.255.0.0
Nha Trang branch	135.35.x.x	255.255.0.0
Da Nang branch	180.20.x.x	255.255.0.0

5.2 Internal LANs

5.2.1 HQ

VLAN IP range assigned by DHCP server, each of VLAN has maximum 253 end devices joining in, except interface IP on core switch.

VLAN	IP Address	Subnet Mask
IT room	192.168.1.2 - 255	255.255.255.0
Floor2 - customer service	192.168.2.2 - 255	255.255.255.0
Floor3 - customer service	192.168.3.2 - 255	255.255.255.0
Floor4 - customer service	192.168.4.2 - 255	255.255.255.0
Floor5 - staff	192.168.5.2 - 255	255.255.255.0
Floor6 - staff	192.168.6.2 - 255	255.255.255.0
Floor7- staff	192.168.7.2 - 255	255.255.255.0
Floor2 - guest	192.168.12.2 - 255	255.255.255.0
Floor3 - guest	192.168.13.2 - 255	255.255.255.0
Floor4 - guest	192.168.14.2 - 255	255.255.255.0

Note: Core switch create VLANs and have IP address 192.168.x.1 on each of VLAN interface x.

Special internal devices with static IP address.

Device	IP Address	Subnet Mask
Admin 1	192.168.1.11	255.255.255.0
Admin 2	192.168.1.12	255.255.255.0
DHCP server	192.168.1.2	255.255.255.0
DNS server	192.168.1.3	255.255.255.0
Mail server	192.168.1.4	255.255.255.0
FTP server	192.168.1.5	255.255.255.0

Gateway area

Area	IP Address	Subnet Mask
Core switch - firewall	192.168.101.1 - 2	255.255.255.0
DMZ VLAN	192.168.102.1 - 255	255.255.255.0
bbb.com webserver	192.168.102.2	255.255.255.0
NAT inside	192.168.103.2	255.255.255.0
NAT outside	161.228.1.1	255.255.0.0
Gateway	161.228.1.2	255.255.0.0
Net flow collector server	161.227.1.2	255.255.0.0

NAT translation

Device	Inside local	Inside global	NAT type
Admin 1	192.168.1.11	161.228.101.11	static
Admin 2	192.168.1.12	161.228.101.12	static
DNS server	192.168.1.3	161.228.101.3	static
Mail server	192.168.1.4	161.228.101.4	static
FTP server	192.168.1.5	161.228.101.5	static
bbbank.com webserver	192.168.102.2	161.228.102.2	static
other internal end devices	192.168.x.x	161.228.10.x	dynamic pool

5.2.2 Branches

The 2 branches internal IP subnet are similar to each other, except the NAT translation.

VLAN IP range assigned by DHCP server.

VLAN	IP Address	Subnet Mask
IT room	192.168.1.2 - 255	255.255.255.0
Customer service	192.168.2.2 - 255	255.255.255.0
Staff	192.168.3.2 - 255	255.255.255.0
Guest - wireless	192.168.11.2 - 255	255.255.255.0
Staff - wireless	192.168.12.2 - 255	255.255.255.0

Note: Core switch create VLANs and have IP address 192.168.x.1 on each of VLAN interface x.

Special internal devices with static IP address.

Device	IP Address	Subnet Mask
Admin 1	192.168.1.11	255.255.255.0
Admin 2	192.168.1.12	255.255.255.0
DHCP server	192.168.1.2	255.255.255.0
Mail server	192.168.1.4	255.255.255.0
FTP server	192.168.1.5	255.255.255.0

Gateway area of Nha Trang branch.

Area	IP Address	Subnet Mask
Core switch - firewall	192.168.101.1 - 2	255.255.255.0
NAT inside	192.168.103.2	255.255.255.0
NAT outside	135.35.1.1	255.255.0.0
Gateway	135.35.1.2	255.255.0.0
Net flow collector server	135.34.1.2	255.255.0.0

NAT translation of Nha Trang branch.

Device	Inside local	Inside global	NAT type
Admin 1	192.168.1.11	135.35.101.11	static
Admin 2	192.168.1.12	135.35.101.12	static
Mail server	192.168.1.4	135.35.101.4	static
FTP server	192.168.1.5	135.35.101.5	static
other internal end devices	192.168.x.x	135.35.10.x	dynamic pool

Gateway area of Da Nang branch.

Area	IP Address	Subnet Mask
Core switch - firewall	192.168.101.1 - 2	255.255.255.0
NAT inside	192.168.103.2	255.255.255.0
NAT outside	180.20.1.1	255.255.0.0
Gateway	180.20.1.2	255.255.0.0
Net flow collector server	180.19.1.2	255.255.0.0

NAT translation of Da Nang branch.

Device	Inside local	Inside global	NAT type
Admin 1	192.168.1.11	180.20.101.11	static
Admin 2	192.168.1.12	180.20.101.12	static
Mail server	192.168.1.4	180.20.101.4	static
FTP server	192.168.1.5	180.20.101.5	static
other internal end devices	192.168.x.x	180.20.10.x	dynamic pool

5.2.3 Summary

- Using DHCP to dynamically assigning IP.
- Some public servers have static IP addresses.
- Each for have its own subnet.
- Each subset can scale up to average 253 end devices (workstations, etc.).

- NAT translates private IP addresses to public IP addresses pool with 255 different values.

6 Area with high load

6.1 WAN

- HQ LAN: it has to load the traffic of HQ internal network and traffic from the 2 branches accessing to the Internet.

6.2 Internal LANs

6.2.1 HQ

- Core switch: every communication among VLANs must pass the core switch.
- Gateway router: load traffic from HQ internal network, traffic from the 2 branches and Internet.

6.2.2 Branches

- Core switch: every communication among VLANs must pass the core switch.
- Gateway router: load traffic from branch internal network, HQ and other branch.

7 List of recommended equipment

The list of device implemented and their quantity will be demonstrated in the following tables. Since we are only focusing on the bank company structure, other devices in the WAN network or outside company will not be taken in to account. The WAN network has been discussed in the previous section and they can be flexibly adjusted.

7.1 HQ

No.	Device	Quantity	Info
Headquarters			
1	ISR 4331 Router	3	The device that routing data packets among computer networks. There are 3 routers: one for firewall, one for public gateway and one for NAT IP translation. The router support adding gigabitEthernet switch ports with bandwidth up to 1000Mbps which improve the traffic load of gateway area.
2	Server PT	6	The device that share data or resources among multiple clients. There are 6 servers: DHCP server, DNS server, Mail server, FTP server, Web server, Net flow collector server
3	Switch PT-Empty	8	The device that connect workstations and other end devices together forming a network. There are 7 switches for workstations in 7 different floors and 1 switch for the public webserver in DMZ area. This model have 10 empty ports which allow adding more gigabitEthernet ports as needed.
4	Core Switch 3650 24PS	1	The device that responsible for creating VLANs, routing among VLANs. This model support 24 gigabitEthernet ports, which improve the high traffic at core switch.
5	Access Point	6	The device that provides the local wireless connection for guests or staffs in each floor, support WPA2-PSK encryption.
6	PC (Bank)	100	The workstations used in floors of customer service, staff and IT room, support multiple office application on GUI.
7	Laptop	6+	Represent the device that guests use to access Internet via Wi-Fi.

Figure 13: List of recommended device in HQ

7.2 Branches

No.	Device	Quantity	Info
Branch 1 and 2			
1	ISR 4331 Router	3	The device that forwards data packets between computer networks. There are 3 routers: one for internal network, one for public gateway and one for NAT IP translation. The router support adding gigabitEthernet switch ports with bandwidth up to 1000Mbps which improve the traffic load of gateway area.
2	Server PT	4	The device that share data or resources among multiple clients. There are 4 servers: DHCP server, Mail server, FTP server, Net flow collector server
3	Switch PT-Empty	4	The device that connects workstations and other devices together. There are 3 switches for workstations in customer service, staff and IT area; one switch for common LAN wireless connection. This model have 10 empty ports which allow adding more gigabitEthernet ports as needed.
4	Core Switch 3650 24PS	1	The device that responsible for creating VLANs, routing between VLANs and establish a firewall. This model support 24 gigabitEthernet ports, which improve the high traffic at core switch.
5	Access Point	3	The device that provides the local wireless internet for guests or staffs in different VLANs, support WPA2-PSK encryption.
6	PC (Bank)	50	The workstations used in department of customer service, staff and IT room, support multiple office application on GUI.
7	Laptop	3+	Represent the device that guests use to access Internet via Wi-Fi.

Figure 14: List of recommended device in two branches

Note: As the number of workstations for each specific area has been discussed in the internal LANs diagram section, we do not put the reparation in the above list of equipment.

8 Physical setup

8.1 HQ

The physical setup may not look similarly as in Cisco Packet Tracer since it is the prior step we need to do in order to visualize the implementation. Extra devices might be added into the implementation for testing purposes or to improve our ideas during this assignment.

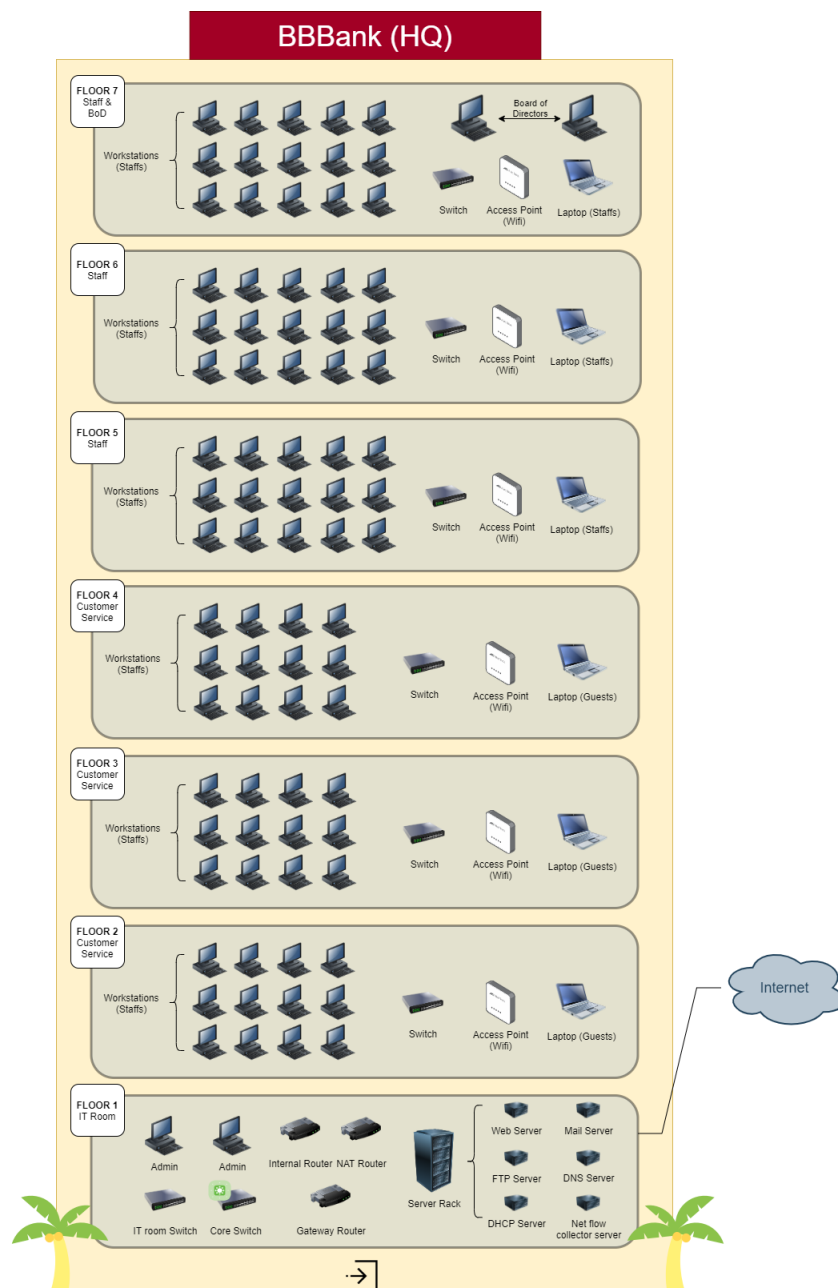


Figure 15: Physical setup of HQ

8.2 Branches

Since the two branches have a similar network structure, we only demonstrate it in one physical setup figure.

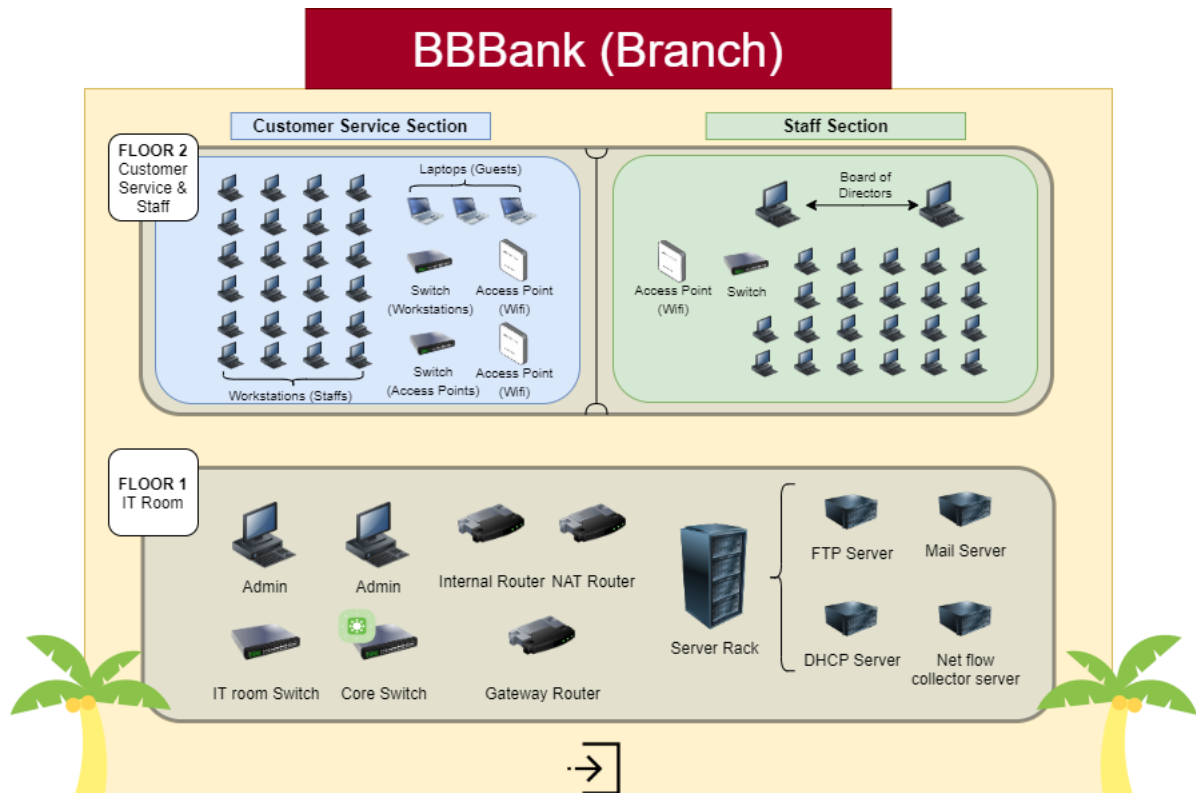


Figure 16: Physical setup of branches

9 Implementation on Packet Tracer

9.1 WAN

Wiring

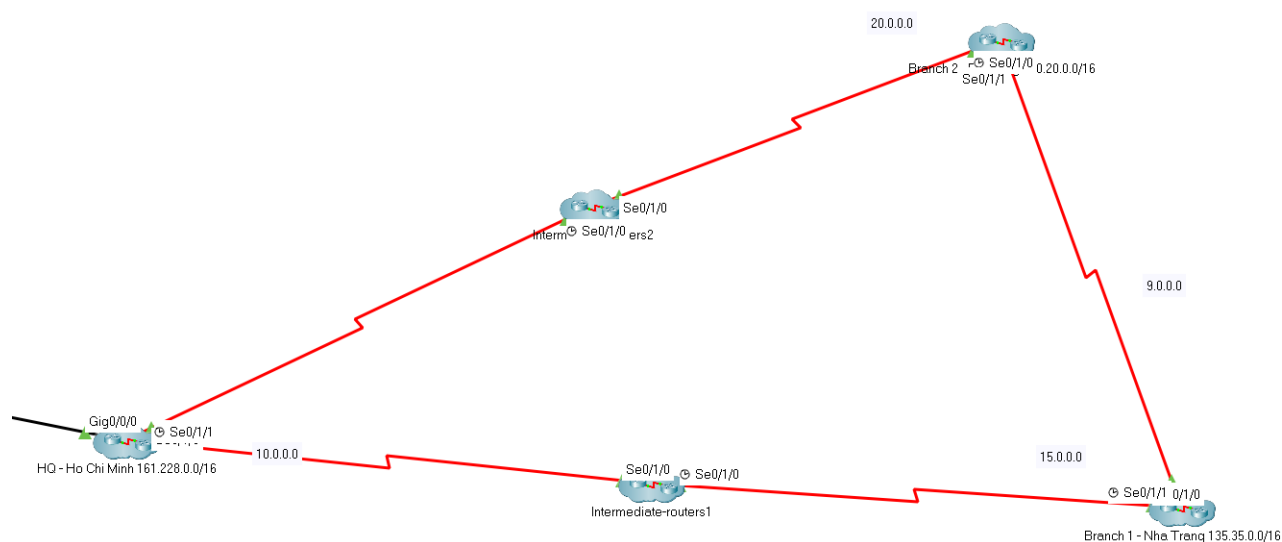


Figure 17: WAN connection

The WAN topology has a shape similar to a triangle, in which the HQ connects to two branches via leased lines using Serial ports. These connections involve the intermediate routers (inside two clusters in the middle) placed across the provinces in Vietnam.

The details of the intermediate routers can be seen inside the clusters as follows:

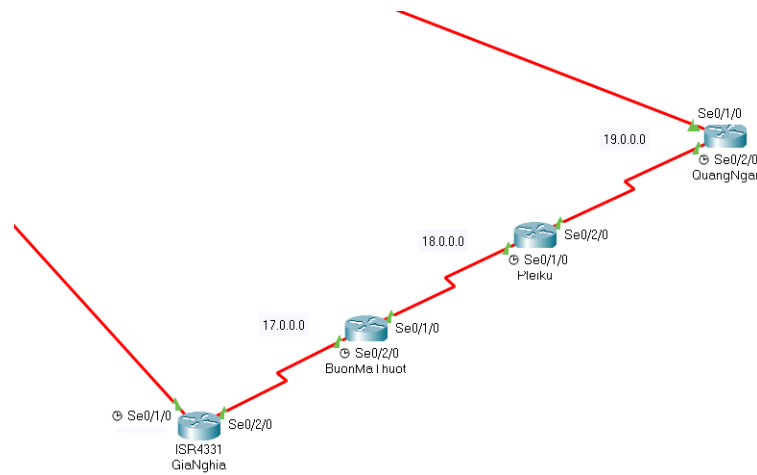


Figure 18: WAN connection line from HQ to Branch 2 (Da Nang)

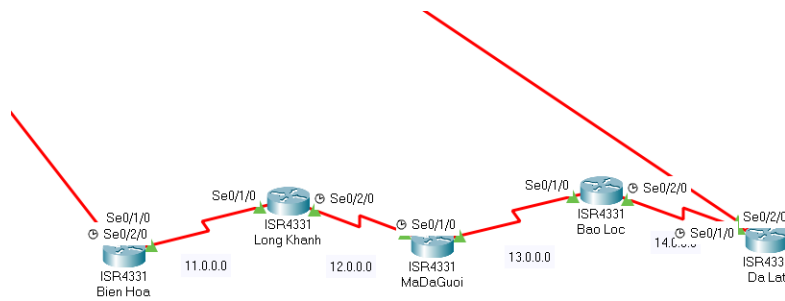


Figure 19: WAN connection line from HQ to Branch 3 (Nha Trang)

The whole WAN is using RIP for routing the desired connection from HQ to two branches. Each router contains the RIP information of interface network, enabling them to create a consecutive connection throughout this WAN.

9.2 Internal LANs

9.2.1 HQ

Wiring

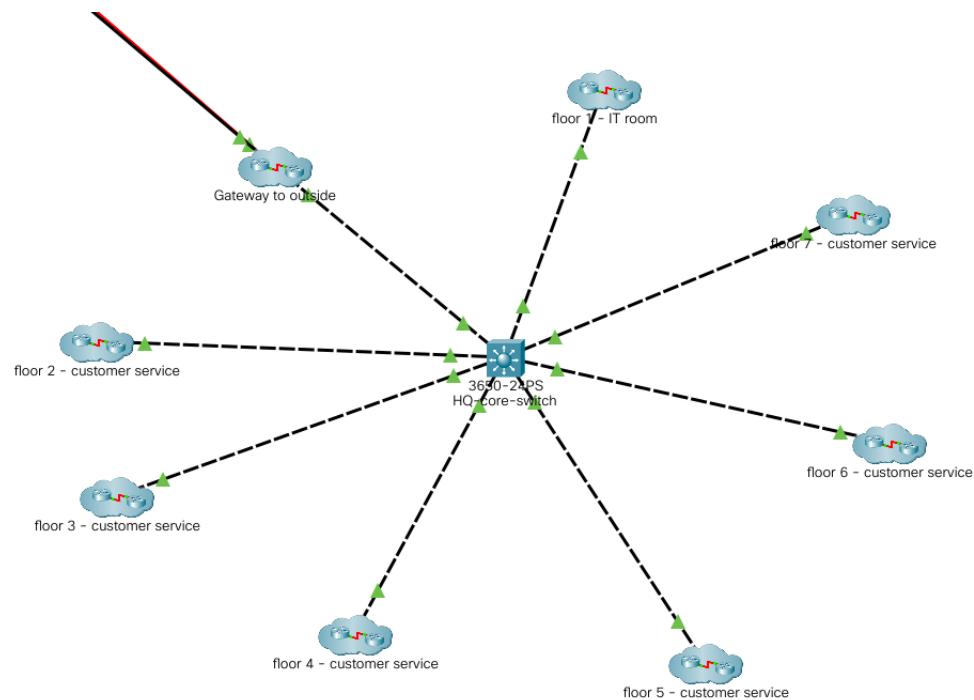


Figure 20: HQ core network topology implementation

There is a core switch connecting 7 VLANs via GigabitEthernet ports setting to trunk port, and connecting gateway using GigabitEthernet port.

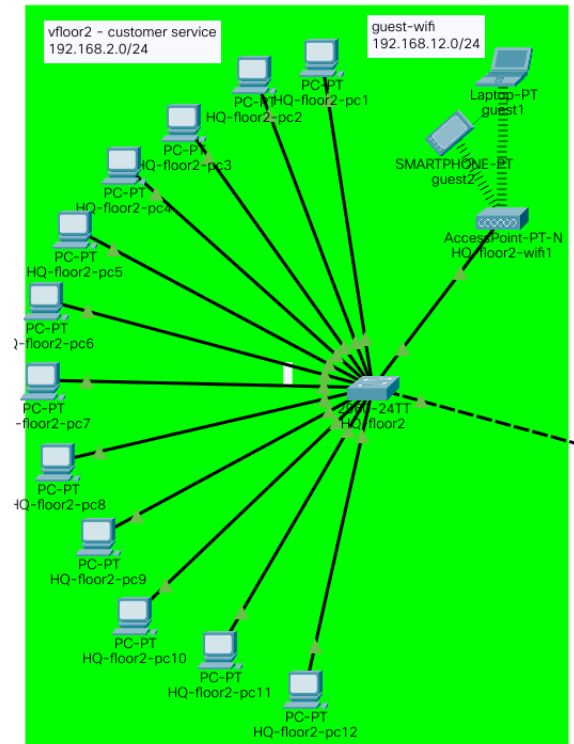


Figure 21: Customer service topology implementation

There is a switch connect 12 workstations as a VLAN as well as an access points for guest as another VLAN. Workstations connect with the switch using FastEthernet port; the access point connects with the switch using FastEthernet port; The client end devices connect to the network using Wi-Fi. The local switch then connect with the core switch using GigabitEthernet port.

Floor 2, 3, 4 wiring are similar to each other.

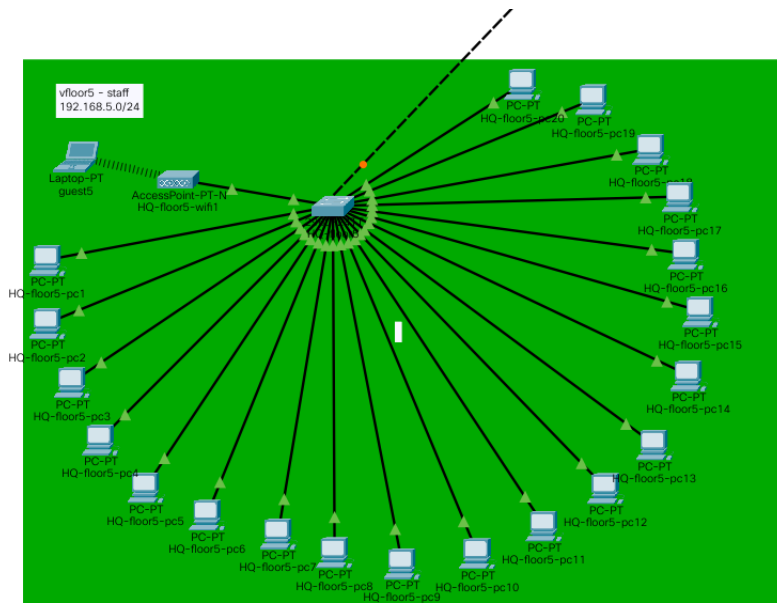


Figure 22: Staff topology implementation

There is a switch connect 20 workstations as well as an access points for staff as a VLAN. Workstations connect with the switch using FastEthernet port; the access point connects with the switch using FastEthernet port; The staff end devices connect to the network using Wi-Fi. The local switch then connect with the core switch using GigabitEthernet port.

Floor 5, 6, 7 wiring are similar to each other.

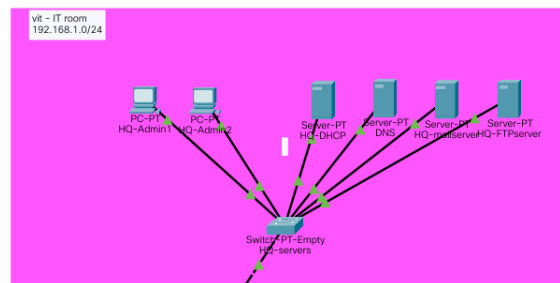


Figure 23: IT topology implementation

There is a switch connect 4 servers 2 administrator workstations as a VLAN. Workstations connect with the switch using FastEthernet port; 4 servers connect with the switch using GigabitEthernet port; the local switch then connect with the core switch using GigabitEthernet port.

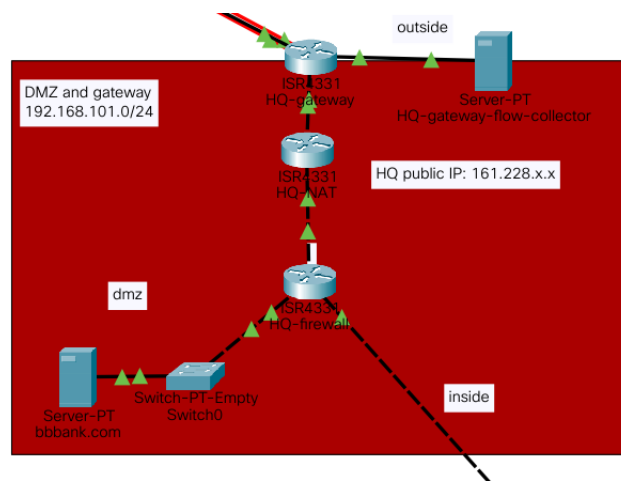


Figure 24: Gateway area topology implementation

VTP

The VTP configuration

- Domain name: BBBANK_HQ
- Password: BBBANK_HQ

```
VTP Version capable : 1 to 2
VTP version running : 2
VTP Domain Name : BBBANK_HQ
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0090.0C7A.1500
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 192.168.2.1 on interface VI2 (lowest numbered VLAN interface found)

Feature VLAN :
-----
VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 15
Configuration Revision : 638
MD5 digest : 0x30 0x14 0xCB 0x7D 0x31 0x6B 0xCA 0xE4
            0x20 0xAD 0x14 0xB4 0x8C 0x0C 0x3B 0x83
```

Figure 25: Core switch VTP configuration

Core switch is the VTP server.

```
VTP Version capable : 1 to 2
VTP version running : 2
VTP Domain Name : BBBANK_HQ
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0030.A3E2.9100
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
-----
VTP Operating Mode : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 15
Configuration Revision : 638
MD5 digest : 0x30 0x14 0xCB 0x7D 0x31 0x6B 0xCA 0xE4
            0x20 0xAD 0x14 0xB4 0x8C 0x0C 0x3B 0x83
```

Figure 26: Local switches VTP configuration

Local switches act as the VTP client.

Telnet access

```
Standard IP access list telnet-access
10 permit host 192.168.1.11
20 permit host 192.168.1.12
30 deny any
```

Figure 27: Telnet access configuration

Using access-list to allow only 2 administrators workstation IP to telnet to networking devices including core switch, firewall router, NAT router, gateway router.

To telnet to the networking devices, issuing the command: telnet <IP_interface_of_device>

Telnet password for each devices

- Core switch: HELLO_CORE_SWITCH
- Firwall router: HELLO_HQ_FIREWALL
- NAT router: HELLO_HQ_NAT
- Gateway router: HELLO_HQ_GATEWAY

DHCP server

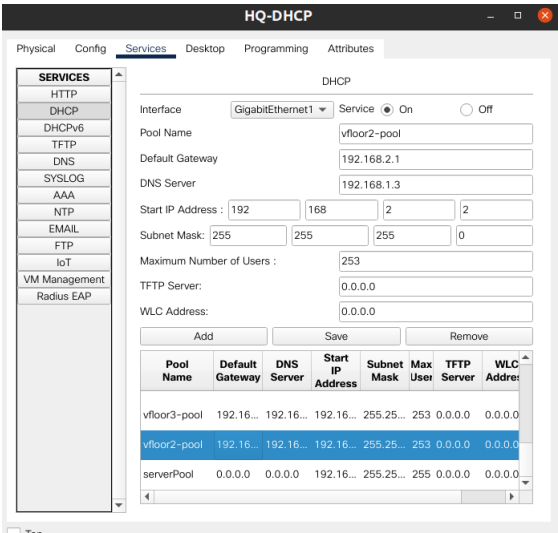


Figure 28: DHCP server configuration

Each VLAN has it own IP pool. Core switch act has a relay agent forwarding IP request whenever an end device request for an IP.

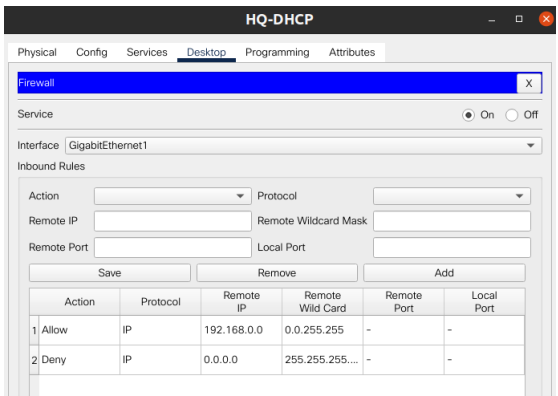


Figure 29: DHCP server firewall configuration

DHCP servers has a firewall which only allow internal IP to access and make requests, deny other IP.

DNS server

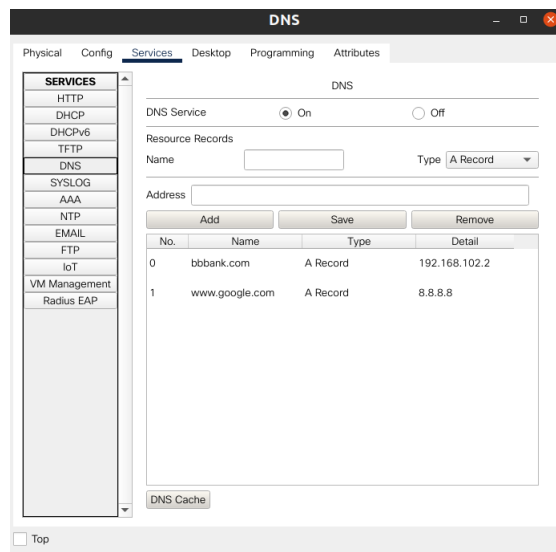


Figure 30: DNS server configuration

Mail server

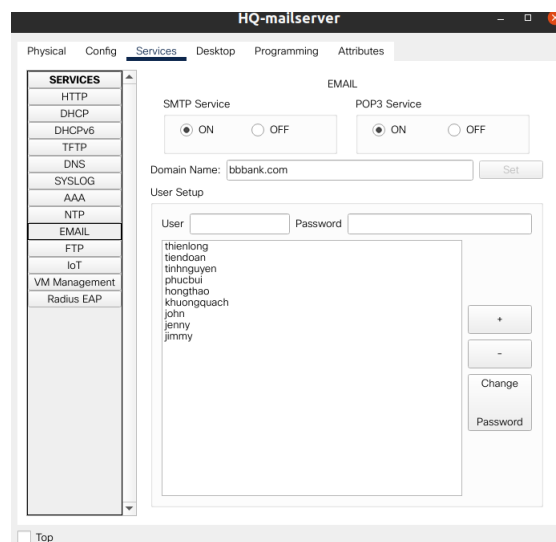


Figure 31: Mail server configuration

Mail server have a domain name bbbank.com, allow SMTP and POP3 service. There are many accounts for staff to use the mail server. This account is replicated to the mail servers of the 2 branches, allow staff to send email to different branches.

Mail server has a firewall which only allow staff IP and staff IP of the 2 branches to access, guests or unknown IP are not allowed.

To use email application, click on the email icon on GUI of the workstation.

FTP server

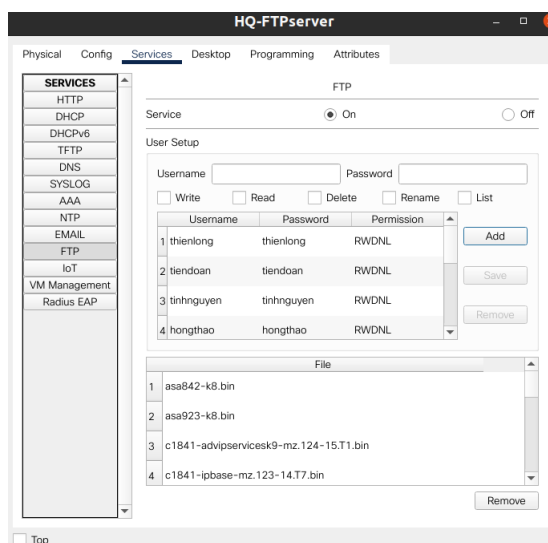


Figure 32: FTP server configuration

The network structure for FTP servers is similar to Mail servers.

There are accounts for staff to use the FTP server. This account is replicated to other FTP servers of the 2 branches, allow staff to download, upload, modify files in different branches.

To use FTP application, go to command prompt and issue the command: `vtp <IP_of_the_FTPserver>`

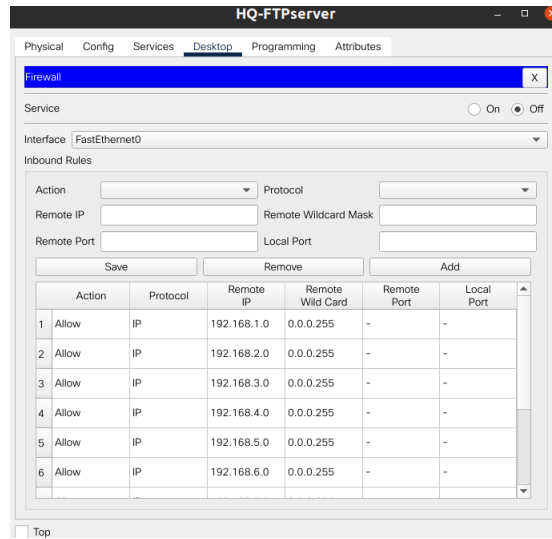


Figure 33: FTP server firewall configuration

FTP server has a firewall which only allow staff IP and staff IP of the 2 branches to access, guests or unknown IP are not allowed.

Wi-Fi

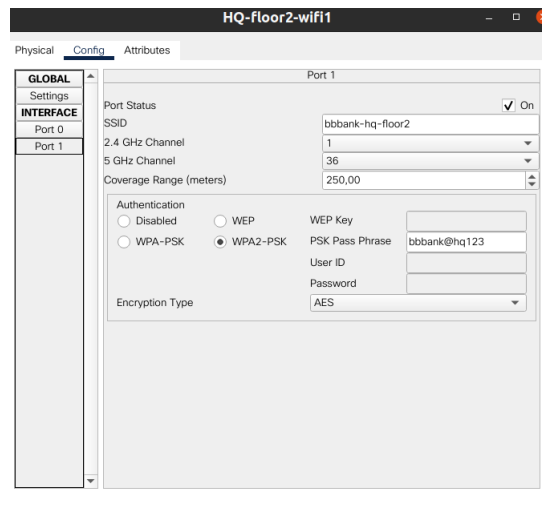


Figure 34: Wi-Fi configuration

Wi-Fi access point support 2 band rate 2.4 and 5 GHZ, using WPA2-PSK authentication, AES encryption, with SSID and PSK Pass Phrase (password).

Security Deny guests' subnets, allow any others to access; setting on core switch.

```
Standard IP access list staff-access
10 deny 192.168.12.0 0.0.0.255
20 deny 192.168.13.0 0.0.0.255
30 deny 192.168.14.0 0.0.0.255
40 permit any
```

Figure 35: Access-list to staff PC

9.2.2 Branches

There is similar configuration to the HQ. Therefore, please visit other branches and check the configuration.

9.2.3 Internet

The Internet is connected to Headquarters through the ISP (Internet Service Provider) router. At this intersection, there are also have anonymous network user from outside that can access to the Internet or the webserver of BBBank.

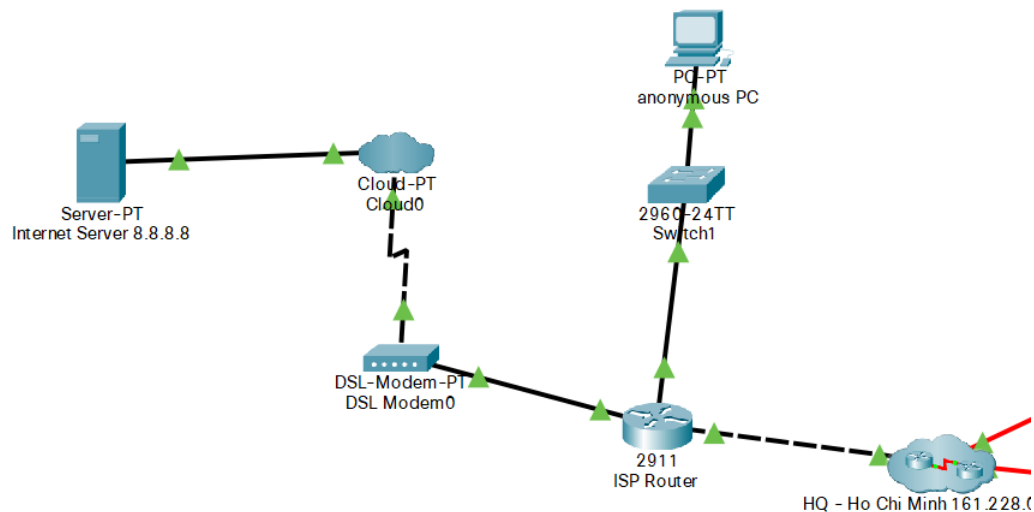


Figure 36: Internet Connection

For the simulation of the Internet, we implement a website that looks like Google with the server address as 8.8.8.8. Staffs from the two branches Nha Trang and Da Nang who want to access to this page must have their computer connection go through the gateway of the Headquarters. With that, the policy and requirements of security and safe contents in BBBank would have been met.

10 Result

10.1 Connect between PCs in the same VLAN

```
C:\>tracert 192.168.2.4

Tracing route to 192.168.2.4 over a maximum of 30 hops:

  1  0 ms   0 ms   0 ms   192.168.2.4

Trace complete.
```

Figure 37: Test connection between 2 workstations on the same VLAN 192.168.2.0/24

10.2 Connect PCs between VLANs

```
C:\>tracert 192.168.7.24

Tracing route to 192.168.7.24 over a maximum of 30 hops:

  1  0 ms   0 ms   0 ms   192.168.2.1
  2  *      0 ms   0 ms   192.168.7.24

Trace complete.
```

Figure 38: Test connection between 2 workstations on different VLANs 192.168.2.0/24 with 192.168.7.0/24

10.3 Connect PCs between Headquarters and branches

```
C:\>tracert 135.35.101.11

Tracing route to 135.35.101.11 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.2.1
  2  0 ms    0 ms    0 ms    192.168.101.2
  3  0 ms    0 ms    0 ms    192.168.103.2
  4  *        0 ms    0 ms    161.228.1.2
  5  0 ms    1 ms    2 ms    10.0.0.2
  6  1 ms    2 ms    0 ms    17.0.0.2
  7  2 ms    29 ms   10 ms   12.0.0.2
  8  2 ms    3 ms    3 ms    19.0.0.2
  9  7 ms    2 ms    10 ms   14.0.0.2
 10  5 ms    10 ms   10 ms   15.0.0.2
 11  *        5 ms    30 ms   135.35.101.11
 12  6 ms    2 ms    4 ms    135.35.101.11
 13  3 ms    4 ms    29 ms   135.35.101.11
 14  *        2 ms    1 ms    135.35.101.11

Trace complete.
```

Figure 39: Test connection between HQ - Nha Trang

```
C:\>tracert 180.20.101.11

Tracing route to 180.20.101.11 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    192.168.2.1
  2  0 ms    0 ms    0 ms    192.168.101.2
  3  0 ms    0 ms    0 ms    192.168.103.2
  4  0 ms    1 ms    0 ms    161.228.1.2
  5  0 ms    1 ms    28 ms   16.0.0.2
  6  1 ms    1 ms    2 ms    17.0.0.2
  7  1 ms    1 ms    10 ms   18.0.0.2
  8  3 ms    2 ms    0 ms    19.0.0.2
  9  3 ms    2 ms    7 ms    20.0.0.2
 10  *        2 ms    2 ms    180.20.101.11
 11  5 ms    29 ms   4 ms    180.20.101.11
 12  11 ms   10 ms   10 ms   180.20.101.11
 13  *        4 ms    28 ms   180.20.101.11

Trace complete.
```

Figure 40: Test connection between HQ - Da Nang

10.4 Connect to servers in the DMZ

```
C:\>tracert 161.228.102.2

Tracing route to 161.228.102.2 over a maximum of 30 hops:

  1  0 ms   0 ms   0 ms   192.168.2.1
  2  0 ms   0 ms   0 ms   192.168.101.2
  3  0 ms   0 ms   0 ms   192.168.103.2
  4  *       0 ms   0 ms   180.20.1.2
  5  1 ms   1 ms   1 ms   20.0.0.1
  6  2 ms   2 ms   3 ms   19.0.0.1
  7  2 ms   2 ms   2 ms   18.0.0.1
  8  1 ms   2 ms   3 ms   17.0.0.1
  9  10 ms  4 ms   6 ms   16.0.0.1
 10  *       2 ms  28 ms   161.228.102.2
 11  4 ms   10 ms  0 ms   161.228.102.2
 12  *       3 ms  11 ms   161.228.102.2

Trace complete.
```

Figure 41: Test connection from a workstation in Da Nang to server in DMZ of HQ

10.5 No connections from Customers devices to PCs on the LAN

```
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.13.1: Destination host unreachable.
Reply from 192.168.13.1: Destination host unreachable.
Reply from 192.168.13.1: Destination host unreachable.
Reply from 192.168.13.1: Destination host unreachable.

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 42: Test connection from a guests to staff PC 192.168.2.4

No connection.

10.6 Connect to the Internet to a Web server

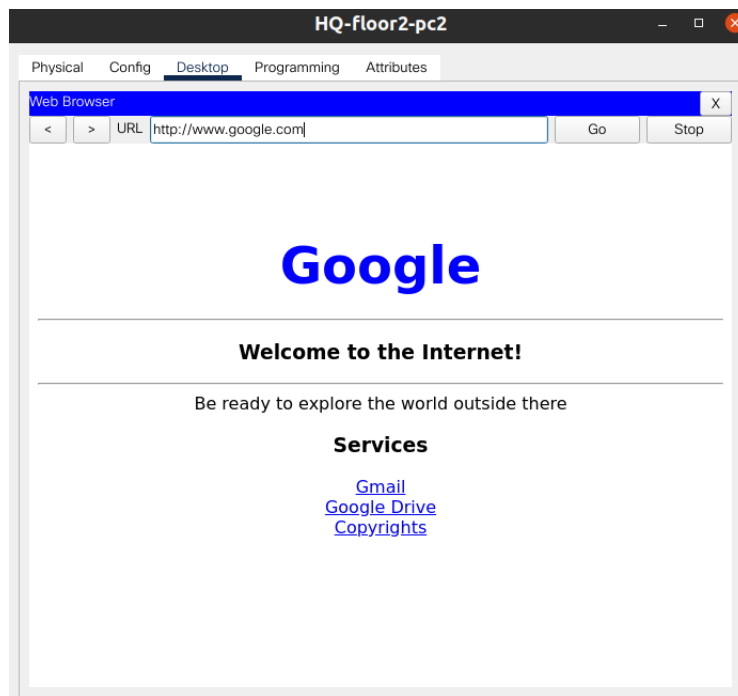


Figure 43: Test connection to www.google.com

10.7 bbbank.com webserver

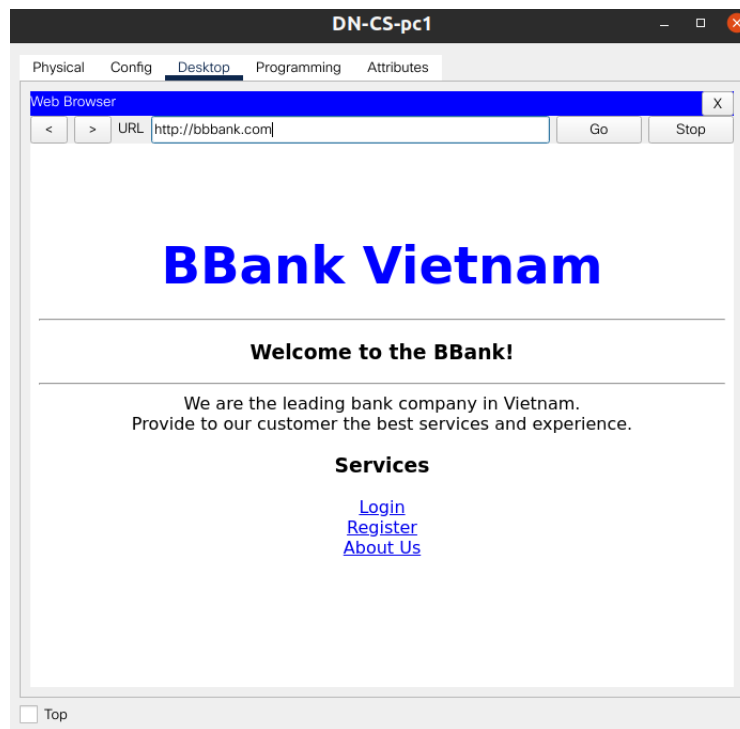


Figure 44: Test connection to bbbank.com in DMZ

10.8 Exchange mails via Mailserver of different branches

Suppose a guy name Thien Long at HQ want to send an email to Hong Thao in Nha Trang branch.

The screenshot shows a window titled "HQ-floor2-pc1" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Configure Mail" dialog box. The dialog box is divided into three sections: User Information, Server Information, and Logon Information. In the User Information section, "Your Name" is "thienlong" and "Email Address" is "thienlong@bbbank.com". In the Server Information section, "Incoming Mail Server" is "192.168.1.4" and "Outgoing Mail Server" is "135.35.101.4". In the Logon Information section, "User Name" is "thienlong" and "Password" is masked with dots. At the bottom of the dialog are "Save", "Clear", and "Reset" buttons. A "Top" button is located at the bottom left of the window.

Section	Field	Value
User Information	Your Name	thienlong
	Email Address	thienlong@bbbank.com
Server Information	Incoming Mail Server	192.168.1.4
	Outgoing Mail Server	135.35.101.4
Logon Information	User Name	thienlong
	Password

Figure 45: Outgoing mailserver is at Nha Trang

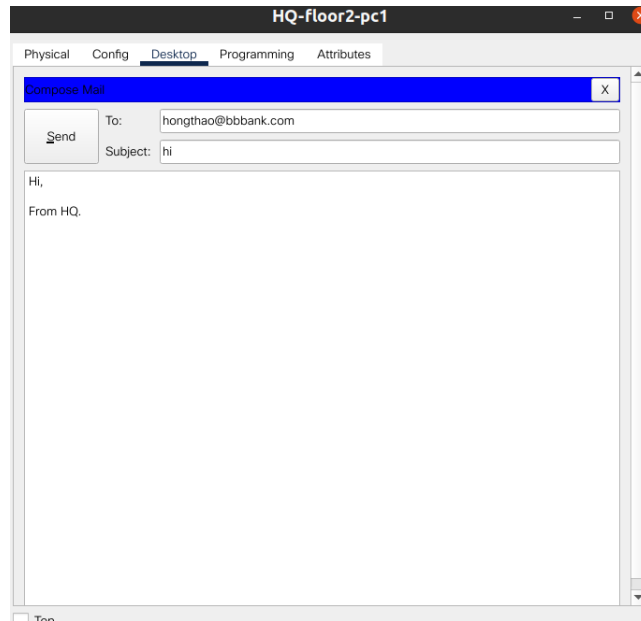


Figure 46: write email to hongthao@bbbank.com

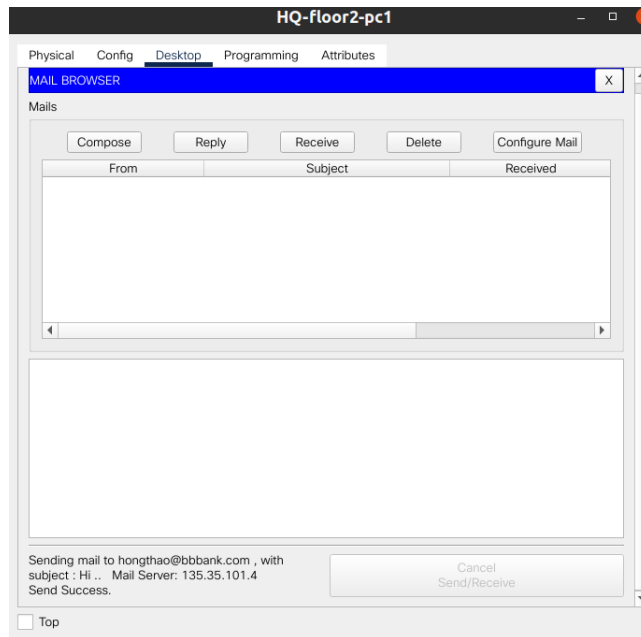


Figure 47: The email is sent successfully!

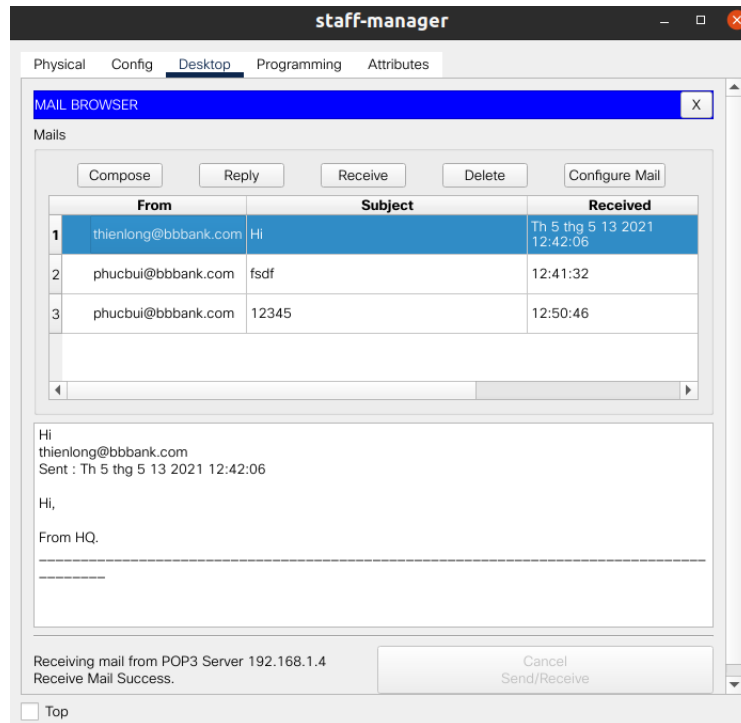


Figure 48: Hong Thao press receive, check her mailbox and read email from Thien Long

10.9 Access FTP servers

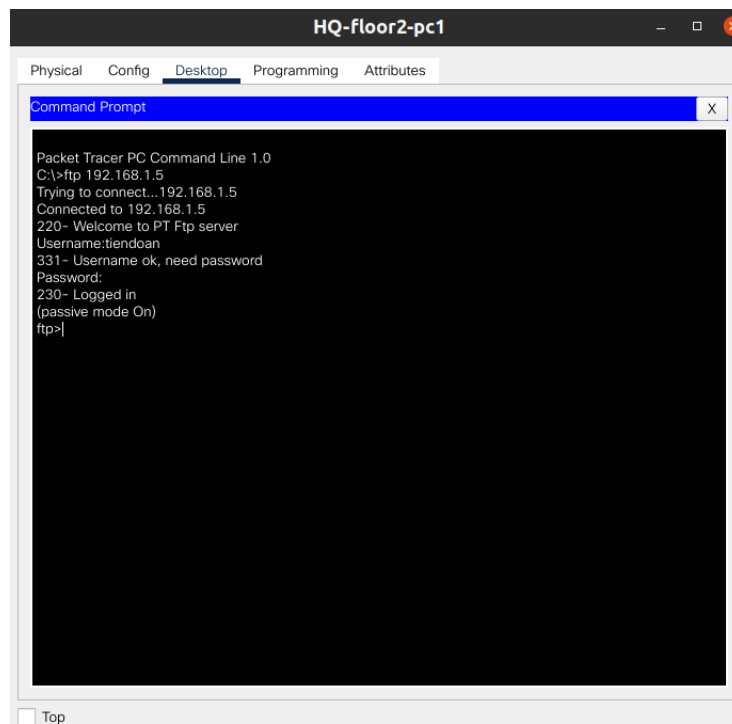


Figure 49: Let's use a staff PC and access to the internal FTP server which has the IP address 192.168.1.5. By entering username and password of a user, we can access to the FTP file system

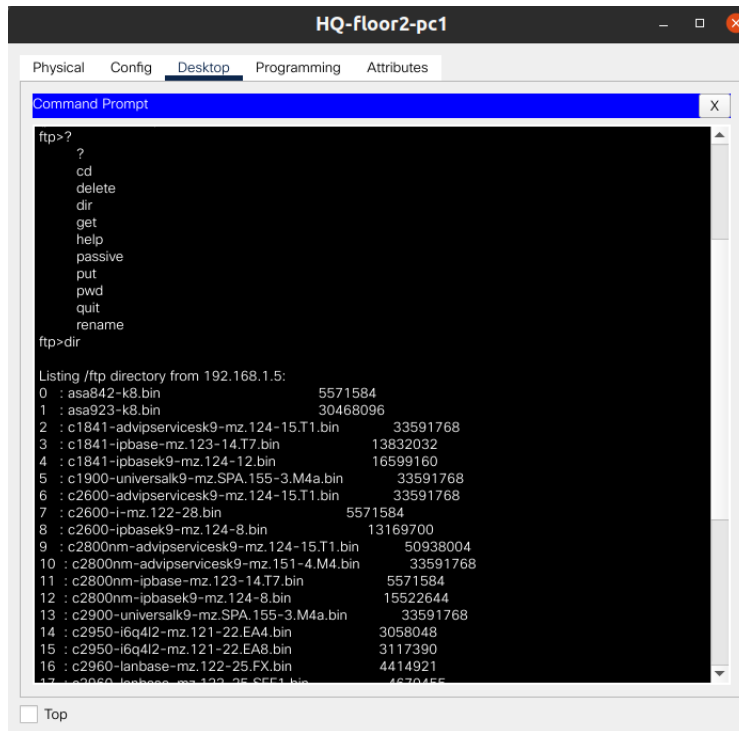


Figure 50: Try *dir* command, which list many files in a certain directory

10.10 Check netflow monitor of gateway

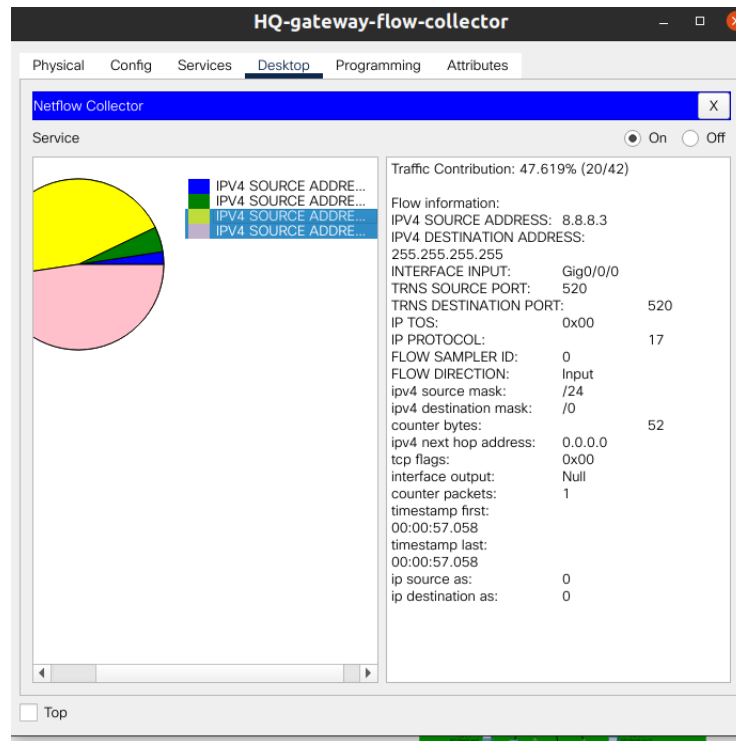


Figure 51: Netflow information of the gateway monitored by the server

The network monitor can record the information about the packets going in and out the network, including source and destination IP addresses, and do statistics, etc.

10.11 Telnet to networking devices from admin workstations

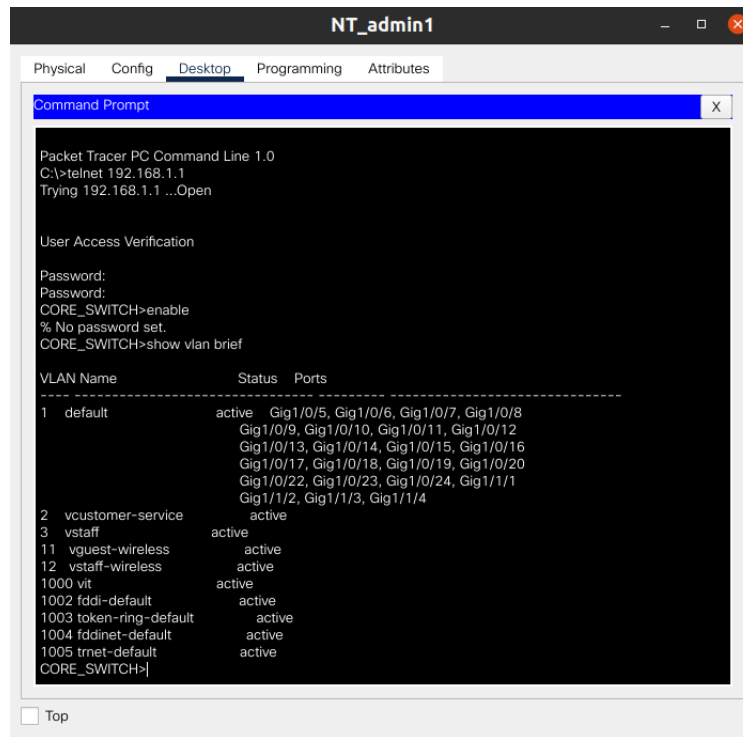


Figure 52: Let's use one admin machine and telnet to the core switch which has the IP address 192.168.1.1. After entering the correct password, we can access to the terminal of the core switch and do operation, in this case we call the command *show vlan brief*

11 Evaluation

11.1 Advantages

11.1.1 Connectivity

- Can connect the HQ with 2 branches and the Internet.
- Using high-speed ports GigabitEthernet to transfer data at high load area such as core switch and gateway.

11.1.2 Scalability

- using private IP with high range of IP addresses for each subnet.
- VTP make scaling easier when more switches is needed.

11.1.3 Security

- Guarantee internal network, servers, staff workstation can be only accessed by trusted factors.
- Branches can only access to the internet via HQ, which easily be controlled and monitored traffic of the bank's network.
- Telnet help administrators to control and modify networking devices on just one PC.

11.2 Disadvantages

11.2.1 Redundancy

- There is only one core switch, which means there is one point of failure, if the core switch is down, the whole internal network is down.
- There is no backing-up devices in high load area such as core switch, servers, gateways.

11.3 Remaining problems

- Improving the realisticity by involving other networks from the outside.
- The project does not cope with the required OSPF network due to its complexity.
- Add more testcases about the performance and non-functional requirements of the network.

12 Conclusion

We have build the bank networking model with an HQ and 2 branches meeting most of the requirements, providing office applications, successfully connecting the facility together and connecting to the Internet. There are advantages in security and scalability, but there are some disadvantages such as low level of redundancy. The project still have some spaces for improvement in the future.