Contents

1 Introduction

The solution presented in this report is a computer network used in the headquarters and two branches of a BBB (BB Bank) under construction.

The table below presents the work assigned for each of our team members.

Name	ID	Works	Percentage
Vu Hoang Hai	1952669	- Write report, design network and test network	100%
Le Nguyen Tan Loc	1952088	- Write report, design network and test network	100%
Nguyen Le Thao Vy	1952536	- Write report, design network and test network	100%

Table 1: Individual workloads

2 Network Structures Analysis

2.1 Given specifications and characteristics

- The 100/1000 Mbps wired and wireless connection are used in the network infrastructure.
- The network is organized based on the VLAN structure, in which packets can only travel from one segment to another if both segments have the same identifiers.
- The network connects to the world outside using 2 leased line (for WAN connection) and 1 ADSL (for Internet access) with a load-balancing mechanism.
- The network must guarantee high security, robustness when problems occur, and the system can be upgraded easily.
- The flows and load parameters of the system:
    - Servers (for updates, web access, database access...): The total upload and download capacity is about 500 MB/day.
    - Workstations (used for web browsing, document downloads, customer transactions...): The total upload and download capacity is about 100 MB/day.
    - WiFi-connected laptops for customers to access: about 50 MB/day.
    - VPN configuration for site-to-site and for a teleworker to connect to LAN.
- The network is estimated to have a growth rate of 20% in 5 years (in terms of the number of users, network load, branch extensions,..).

2.2 Installation locations

According to the given specifications, we have proposed a rough floor-planning design. For the Headquarter, its first floor contains the Reception area, Transaction area, IT room and the Cabling Central Local. Each of the remaining 6 floors is the workplace for 1-2 department(s), all are equipped with a reasonable number of workstations, switch and other network devices. Meanwhile, the 2-floor Branch offices would be built as a smaller scale of the above, yet still provide sufficient equipment that can satisfy the needs of office usages.

2.2.1 Headquarter Floor-plan

The first floor

This floor is dedicated to the Retail Banking Department, where the transaction activities of individual customers are carried out. Along with the given IT room and the Cabling Central Local, it should be designed with a reception section, customer information section (featured WiFi-connected laptops), transaction section and customer service section.

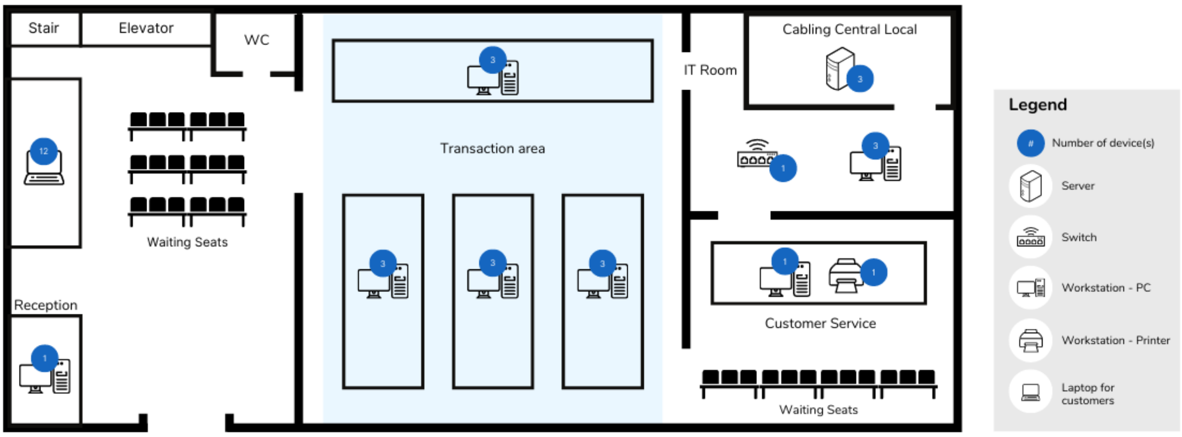


Figure 1: Floor plan of the Headquarter's 1st floor

The 2nd - 7th floors

The 2nd floor is built for 2 departments: the Commercial Banking and the Loan Servicing.

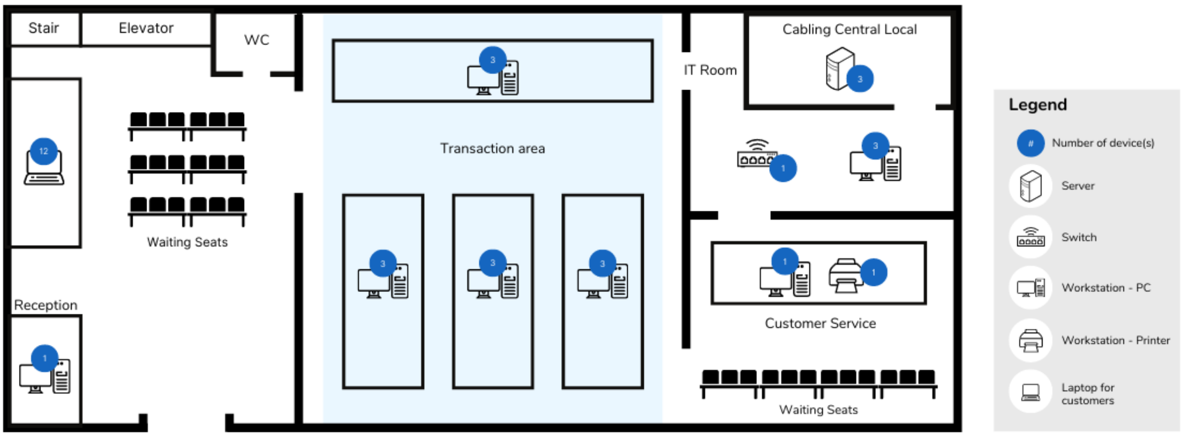


Figure 2: Floor plan of the Headquarter's 2nd floor

The 3rd and 4th floor are for Deposit Operations Department and Investment Banking Department respectively.

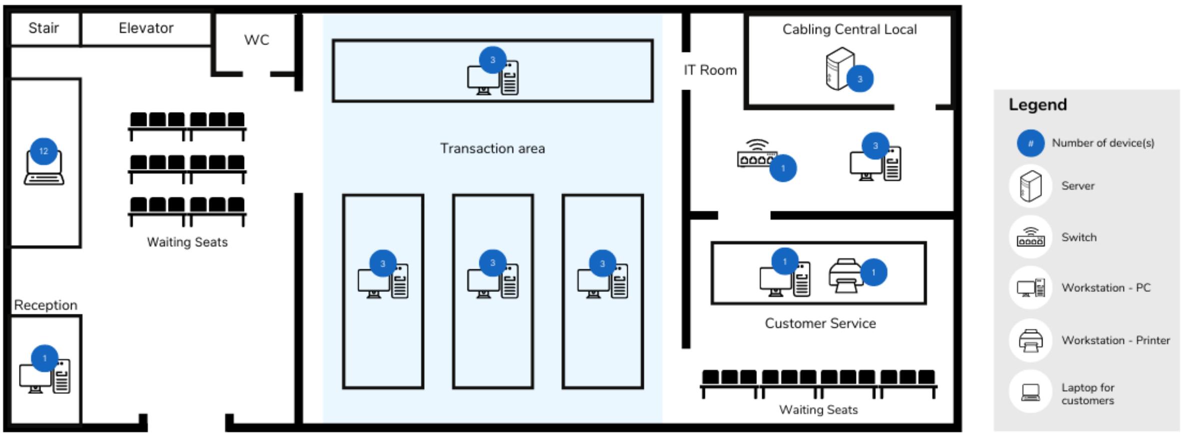


Figure 3: Floor plan of the Headquarter's 3rd floor

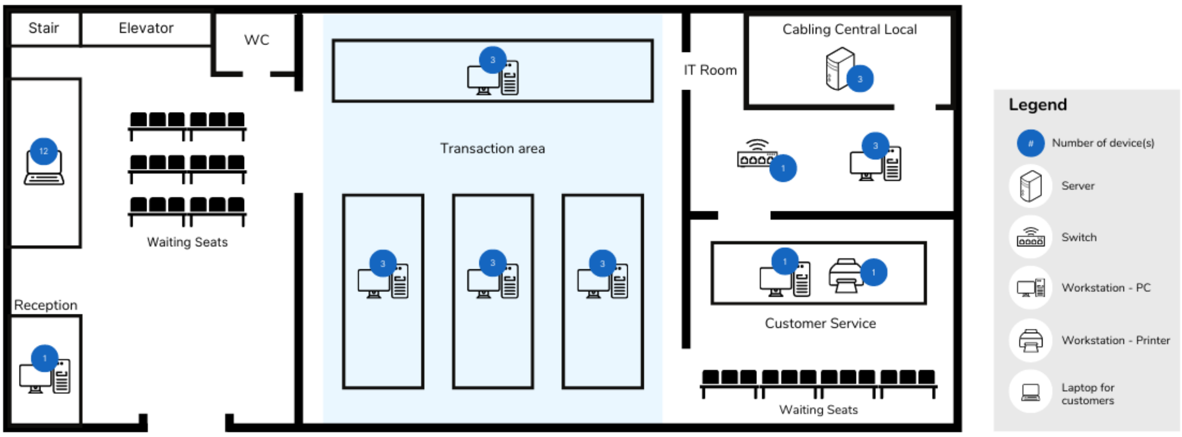


Figure 4: Floor plan of the Headquarter's 4th floor

The 5th floor is made for Human Resources Department, while the 6th one is of the Legal Department and Risk Management Department.

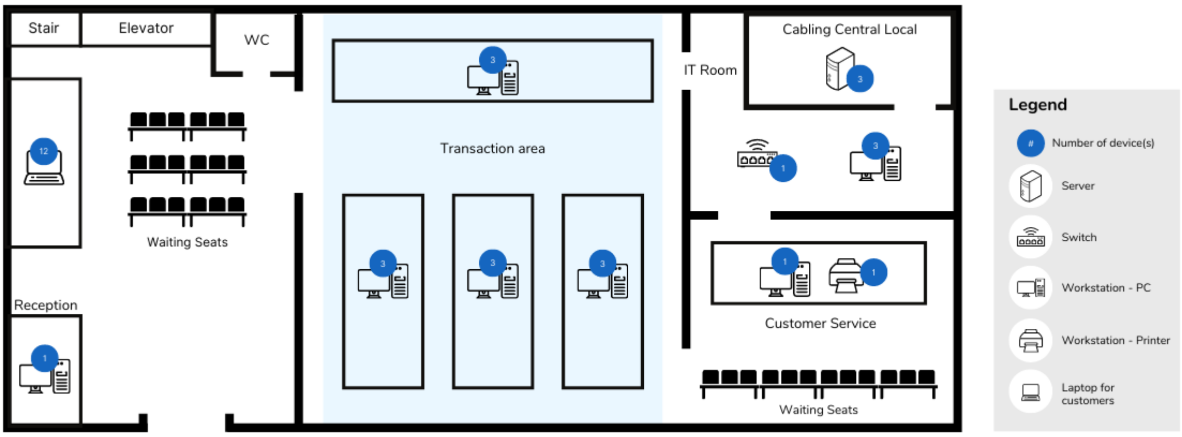


Figure 5: Floor plan of the Headquarter's 5th floor

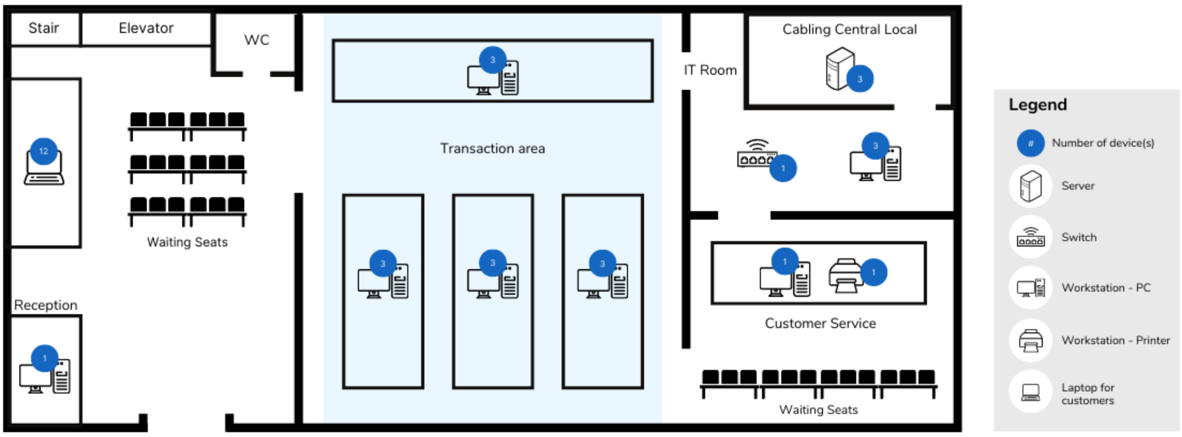


Figure 6: Floor plan of the Headquarter's 6th floor

On the highest floor, beside an office of the Managing Director, there would be a large meeting room.

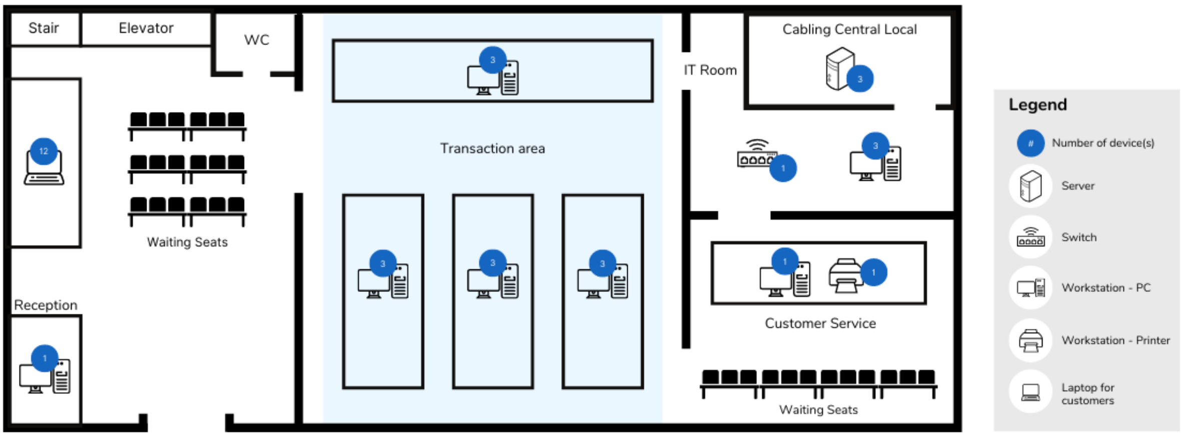


Figure 7: Floor plan of the Headquarter's 7th floor

2.2.2 Branch Office(s) Floor-plan

The branches have the same construction with each other. Therefore their floor planning for network is at most similar in design. This section shall discuss one of the branches as illustrative purposes.

The first floor

The following image illustrate the first floor of the branches.

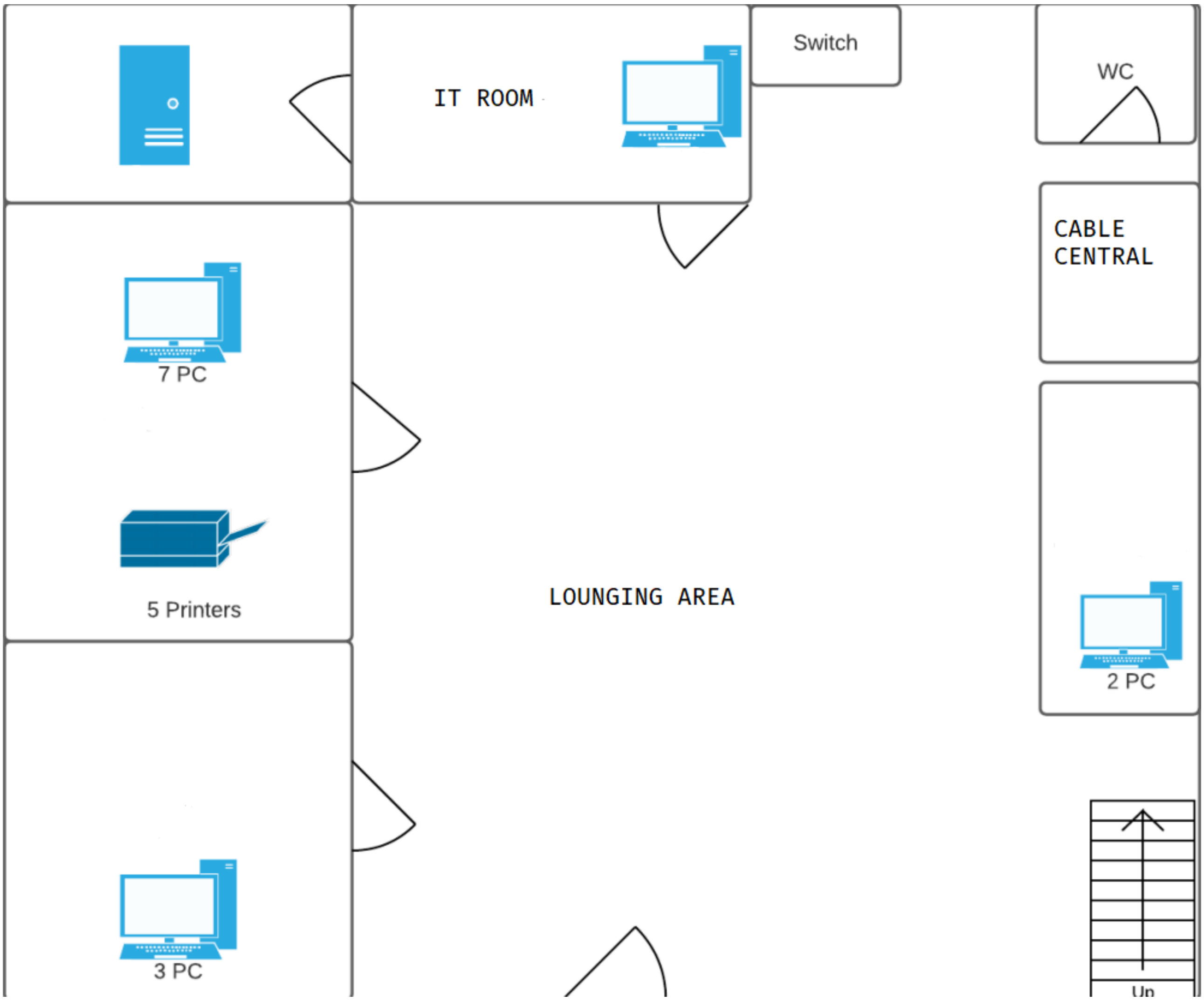


Figure 8: Branches first floor.

The second floor

The following image illustrate the first floor of the branches.

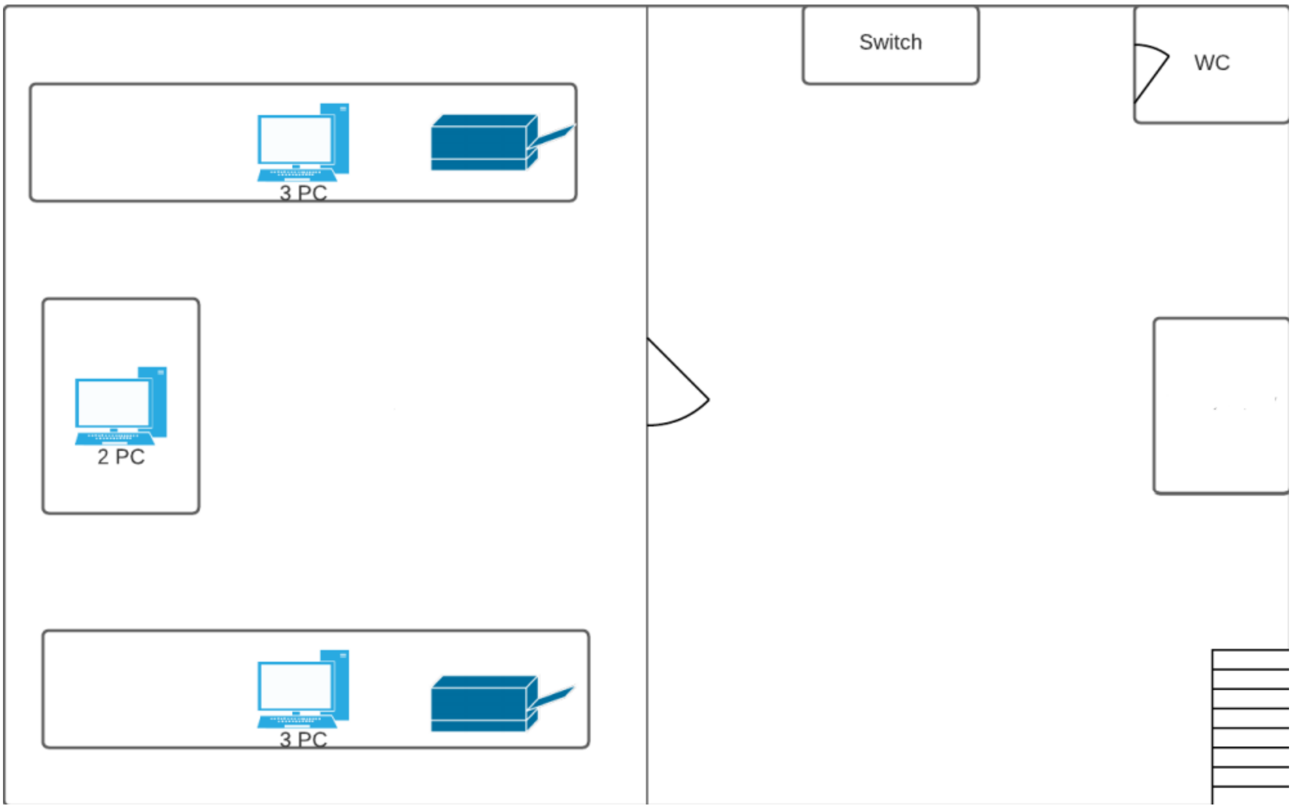


Figure 9: Branches second floor.

2.3 Appropriate network structure

DMZ Network

DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks. The primary benefit of using a DMZ is that it offers users from the public internet access to certain secure services, while maintaining a buffer between those users and the private internal network. However, in this project, it is better to wholefully secure servers in the "inside" zone of the network so as to maximally prevent security breaches.

LAN

A local area network (LAN) is a collection of devices connected together in one physical location, in this case is either the Headquarter or the Branch office.

WAN

A wide area network (WAN) is a telecommunications network that extends over a large geographic area. Wide area networks are often established with leased telecommunication circuits

VLAN

VLAN is an advertised region created by a Swith or Multilayer Switch. It can be understood as a virtual LAN.

The purpose of virtual LAN is creating independent LANs on a different logical interface but same physical interface ports. VLANs are used to protect advertised region, increase security, flexible in using 1 switch for multiple virtual switches, and using the same application on a broadcast domain.

The strength of VLAN accounts for better and wasteless bandwidth of the network since it divides LAN into smaller broadcast domains, only one VLAN shall received an adverised packet without transmitting to others all at once.

DHCP

DHCP (Dynamic Host Configuration Protocol) is an interface designed to reduce configuration hassles for TCP/IP networks by automatically assigned designated IP addresses to same network computers.

NAT

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. It is used across firewalls to mask the original IP address from the "inside" to the "outside", it is also a signature that identifies packets originally sent form the "inside" region of the firewall to pass through.

3 List of Minimum Equipment, IP Diagram, and Wiring Diagram (cabling)

The list of equipment used to build the required network is presented as follows:

- Server: The network contains several type of servers as below.
  - DNS server
  - Web server
  - Database server
  - Transaction server
  - ...
- Core switch: A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to a wide area network (WAN) or the Internet.
- Switch: Switch is a hardware device that filters and forwards network packets from one networking device (switch, router, computer, server, etc.) to another.
- Router: A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.
- Firewall: Firewall is a necessary part of any network security architecture. Its job includes monitoring and filtering incoming and outgoing network traffic based on a previously established security policies.
- Access point: Access point is deployed to create wireless local area network, or WLAN in the offices. It can be connected to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.
- Workstation:
  - PC: A network PC is a small, low-cost computer designed to be centrally managed and support businesses using network applications.
  - Printer: A network printer is part of a workgroup or network of computers that can all access the same printers at the same time.
- Laptop: WiFi-connected laptops are provided for customers.

Table of IP addresses

VLAN	Floor	IP address	Default gateway	Possible IP addresses
VLAN10	IT room	192.168.1.0/24	192.168.1.1	192.168.1.2 - 192.168.1.100
VLAN20	G	192.168.2.0/24	192.168.2.1	192.168.2.2 - 192.168.2.100
VLAN30	1	192.168.3.0/24	192.168.3.1	192.168.3.2 - 192.168.3.100
VLAN40	2	192.168.4.0/24	192.168.4.1	192.168.4.2 - 192.168.4.100
VLAN50	3	192.168.5.0/24	192.168.5.1	192.168.5.2 - 192.168.5.100
VLAN60	4	192.168.6.0/24	192.168.6.1	192.168.6.2 - 192.168.6.100
VLAN70	5	192.168.7.0/24	192.168.7.1	192.168.7.2 - 192.168.7.100
VLAN80	6	192.168.8.0/24	192.168.8.1	192.168.8.2 - 192.168.8.100
VLAN13	Customer WiFi	192.168.13.0	192.168.13.1	192.168.13.2 - 192.168.13.100

- Web server: 201.11.51.11
- DNS server: 7.7.7.7
- Database server: 192.168.1.2 - 192.168.1.6
- Backup server: 192.168.1.7 - 192.168.1.11
- ISP public IP: 20.40.60.0/24
- Network Routing: 200.100.40.0/24; 200.100.50.0/24; 200.100.60.0/24

VLAN	Floor	IP address	Default gateway	Possible IP addresses
VLAN90 VLAN100	Nha Trang branch	192.168.9.0/24 192.168.10.0/24	192.168.9.1 192.168.10.1	192.168.9.2 - 192.168.9.100 192.168.10.2 - 192.168.10.100
VLAN110 VLAN120	Da Nang branch	192.168.11.0/24 192.168.12.0/24	192.168.11.1 192.168.12.1	192.168.11.2 - 192.168.11.100 192.168.12.2 - 192.168.12.100

WAN connection diagram

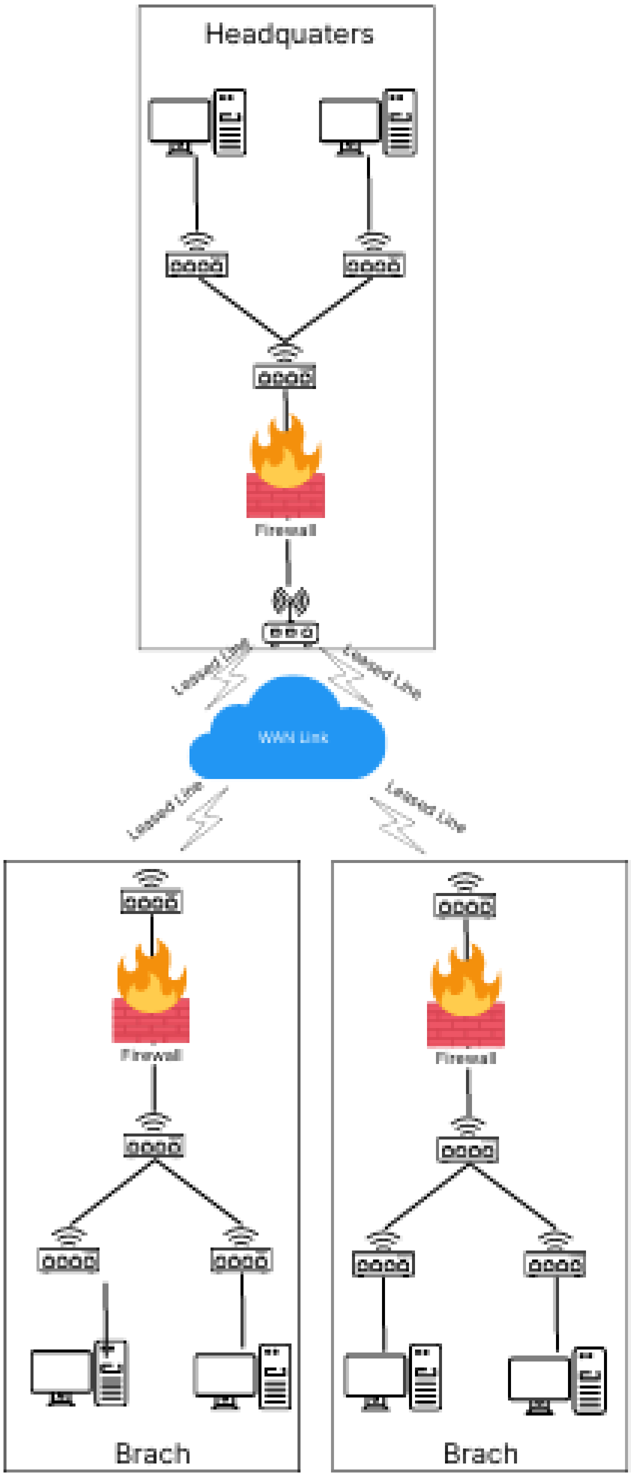


Figure 10: WAN connection diagram between Headquarters and Branches (using OSPF protocol)

4 Throughput - Bandwidth - Safety parameters

4.1 Theoretical basis

- **Throughput:** Throughput is a practical metric that measures the number of messages successfully transmitted during a specified time period via a network, interface or channel. Measuring throughput is a way to assess, troubleshoot and improve network performance, as it can help to reveal the causes of a poor or slow connection.

  The unit of measurement for this metric can be bits per second (bps), which has evolved to bytes per second(Bps), kilobytes per second(KBps), megabytes per second(MBps) and gigabytes per second(GBps).

- **Bandwidth:** Bandwidth is a theoretical metric that measures the (potential) maximum rate at which data transfer occurs across any particular path of the network. It reflects how high a network's throughput could be at peak performance levels, or how much throughput it could possibly handle.

  The unit of measurement for this metric is typically bits per second (bit/s or bps), megabits per second (Mbps) or gigabits per second (Gbps).

4.2 Parameters' calculation

Throughput and bandwidth are important components of any network and data transmission systems. Knowing how both of them are performing is crucial for administrators hoping to get a comprehensive view of their network's performance.

In this project, we are given the following parameters:

- Peak periods: 9:00 to 11:00 and 15:00 to 16:00; 80% of the network communication occurs in these peak hours.
- The total upload and download capacity of server, workstation and laptop for customer are 500 MB/day, 100 MB/day and 50 MB/day respectively.

At Headquarter

- **Servers:** 5 servers, with a total upload and download capacity of 500 MB/day.
  - Throughput = $\frac{5*500}{8*3600}$ = 0.0868 (MB/s) = 0.6944 (Mbps)
  - Bandwidth = $\frac{5*500*0.8}{3*3600}$ = 0.1852 (MB/s) = 1.4815 (Mbps)
- **Workstations:** 100 workstations, with a total upload and download capacity of 100 MB/day.
  - Throughput = $\frac{100*100}{8*3600}$ = 0.3472 (MB/s) = 2.7778 (Mbps)
  - Bandwidth = $\frac{100*100*0.8}{3*3600}$ = 0.7407 (MB/s) = 5.9259 (Mbps)
- **WiFi-connected laptops for customer:** Assume that there are 12 laptops in total, in which 8 of them operating at peak hours, with a total upload and download capacity of 50 MB/day.
  - Throughput = $\frac{12*50}{8*3600}$ = 0.0208 (MB/s) = 0.1667 (Mbps)
  - Bandwidth = $\frac{8*50*0.8}{3*3600}$ = 0.0296 (MB/s) = 0.2370 (Mbps)

- Total throughput of Headquarter's network = 0.6944 + 2.7778 + 0.1667 = 3.6389 (Mbps)

- Total bandwidth of Headquarter's network = 1.4815 + 5.9259 + 0.2370 = 7.6444 (Mbps)

At Branch office

- **Servers:** 3 servers, with a total upload and download capacity of 500 MB/day.
  - Throughput = $\frac{3*500}{8*3600}$ = 0.0521 (MB/s) = 0.4167 (Mbps)
  - Bandwidth = $\frac{3*500*0.8}{3*3600}$ = 0.1111 (MB/s) = 0.8889 (Mbps)

- **Workstations:** 50 workstations, with a total upload and download capacity of 100 MB/day.
  - Throughput = $\frac{50*100}{8*3600}$ = 0.1736 (MB/s) = 1.3889 (Mbps)
  - Bandwidth = $\frac{50*100*0.8}{3*3600}$ = 0.3704 (MB/s) = 2.9629 (Mbps)

- **WiFi-connected laptops for customer:** Assume that there are 5 laptops in total, in which 3 of them operating at peak hours, with a total upload and download capacity of 50 MB/day.
  - Throughput = $\frac{5*50}{8*3600}$ = 0.0087 (MB/s) = 0.0694 (Mbps)
  - Bandwidth = $\frac{3*50*0.8}{3*3600}$ = 0.0111 (MB/s) = 0.0889 (Mbps)

- Total throughput of Branch Office's network = 0.4167 + 1.3889 + 0.0694 = 1.875 (Mbps)

- Total bandwidth of Branch Office's network = 0.8889 + 2.9629 + 0.0889 = 3.9407 (Mbps)

5 Network Map Design

The following section show how the network is planned out according to the infrastructure stated in the previous sections. The construction begins with a headquarter located in Ho Chi Minh City and two branches of the bank, one is in Da Nang, and the other is in Nha Trang. Intercommunication within headquarter and branches shall be initiated as well as connection to the public Internet for all locations.

5.1 Ho Chi Minh City headquarter

The figure below demonstrates the network system in the bank's headquarter.

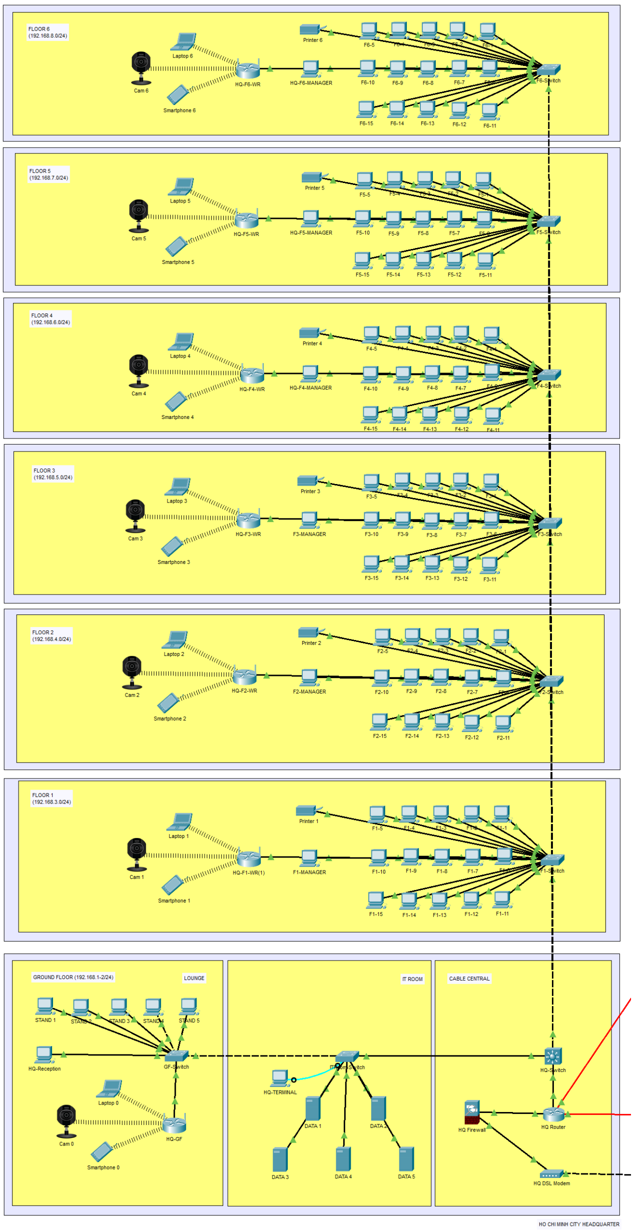


Figure 11: BB Bank's headquarter topology

The Ho Chi Minh city headquarters is a large campus with 7 floors total - one ground floor and six upper-ground floors. The first floor has three separate rooms, the *main lounge* for carrying out transactions, an *IT room* for server storage, and the *cable central* room to control intranet to other branches.

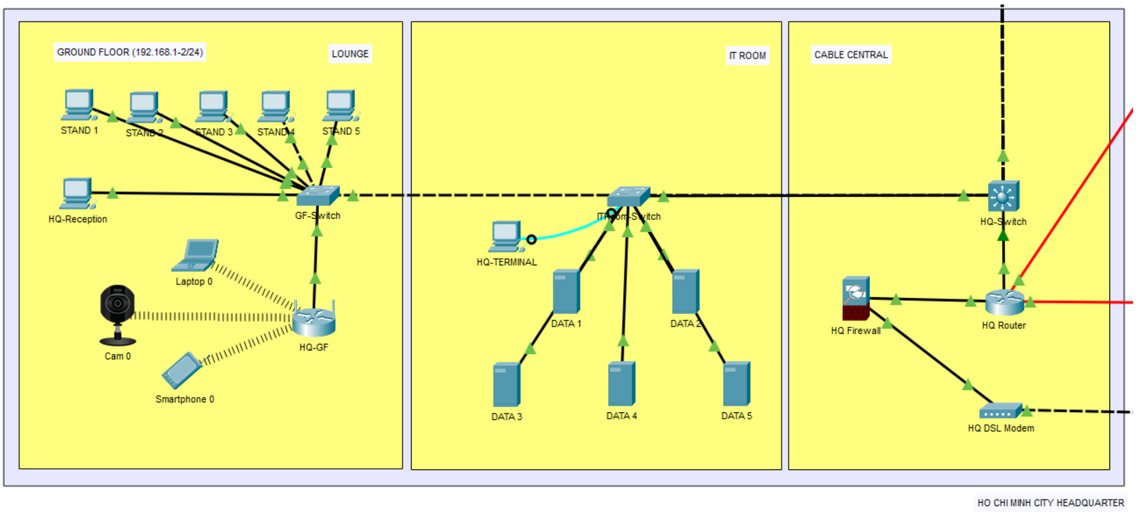


Figure 12: Ground floor planning

The upper floors have the same architectural positioning with 15 workstations each and device peripherals. Every floor offers wireless connectivity as needed.

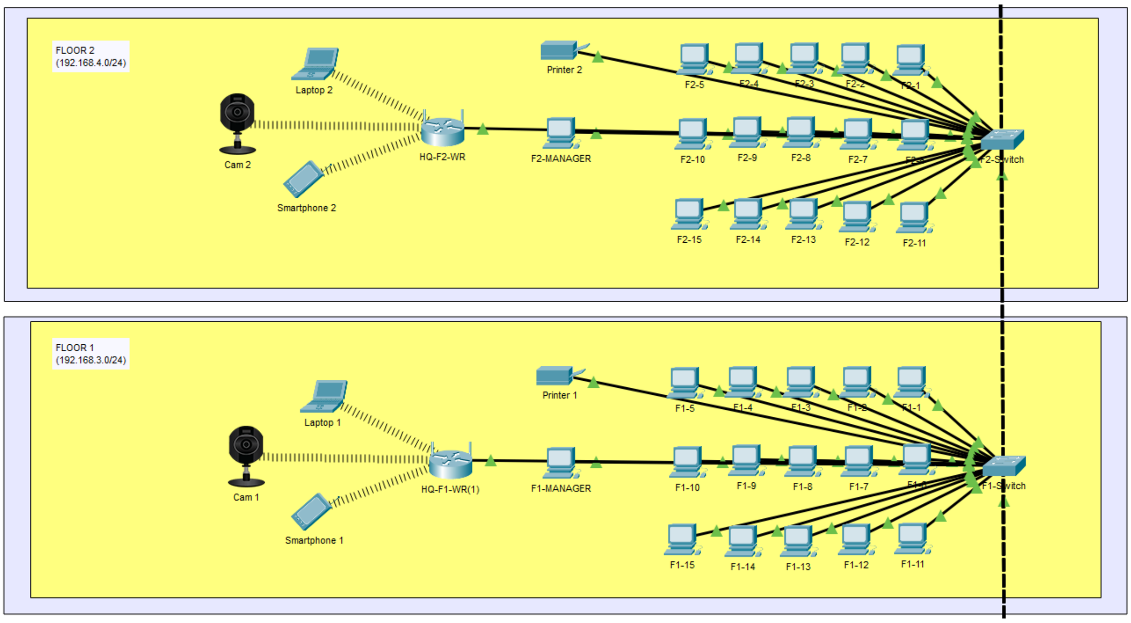


Figure 13: First and second floors planning

All floors can access each other's network interchangeably via switchers and multi-layer switching units. They also can retrieve servers data from the ground floor, if needed. All headquarter LANs can access the Internet provided by the internet service provider via an ADSL modem connected to the provider.

Accessing WAN to other branches in Vietnam requires a central routing unit in the *Cable Central* room on the ground floor to perform communication port-wise. The ISP Internet is also routed via this unit.
A security firewall is placed in the same room after the modem unit to safeguard unauthorized

access and malicious breaches from the outside to the bank's internals.

5.2 Nha Trang Branch

The Nha Trang branch of the bank is a small campus with only two floors, one ground and one upper. The figure below demonstrates the network system in said branch.

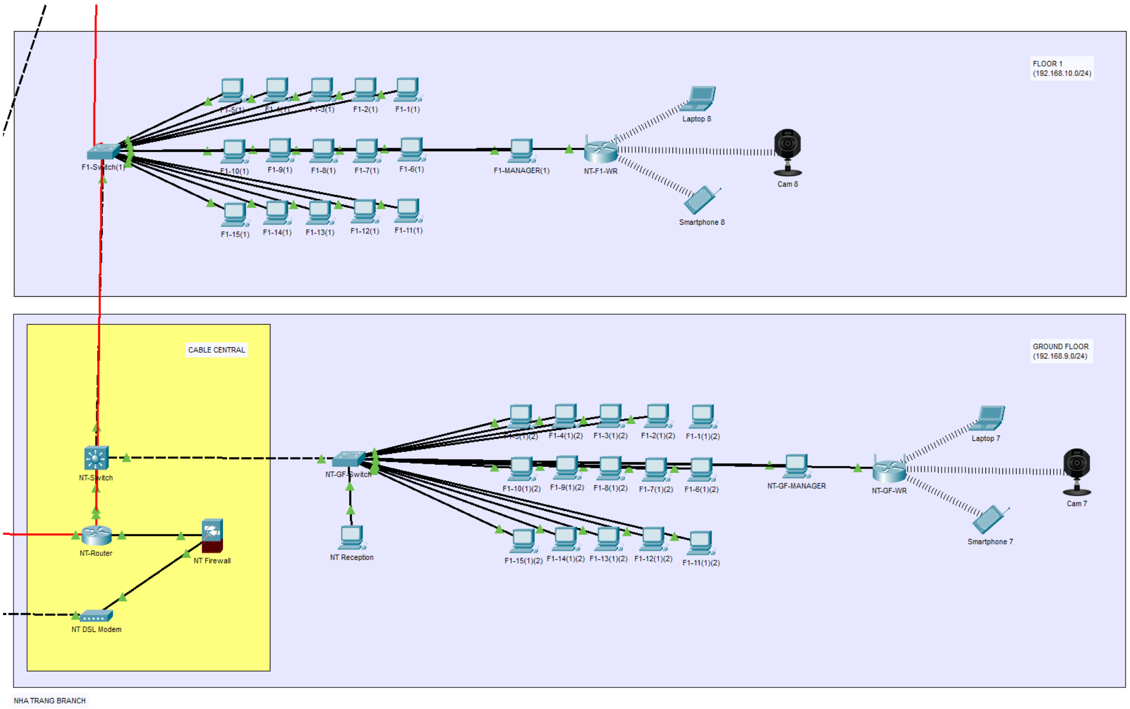


Figure 14: BB Bank's Nha Trang branch

The ground floor consists of two separate rooms, one *Cable Central* for managing WAN connections and internal wirings, and one lounge area with 15 terminals. The upper floor is an entire workspance floor also with 15 computers equipped with necessary devices.

Just like the headquarter, all devices are inter-connected via switchers and multilayer switchers. To access the Internet, they are equipped with modem cabling and a firewall. To manage routing between networks, a router is needed to accomplish said task.

5.3 Da Nang branch

This branch is similar to Nha Trang campus. All networking peripherals are done in an exact fashion as the counterpart. The figure below demonstrates the network system in said branch.

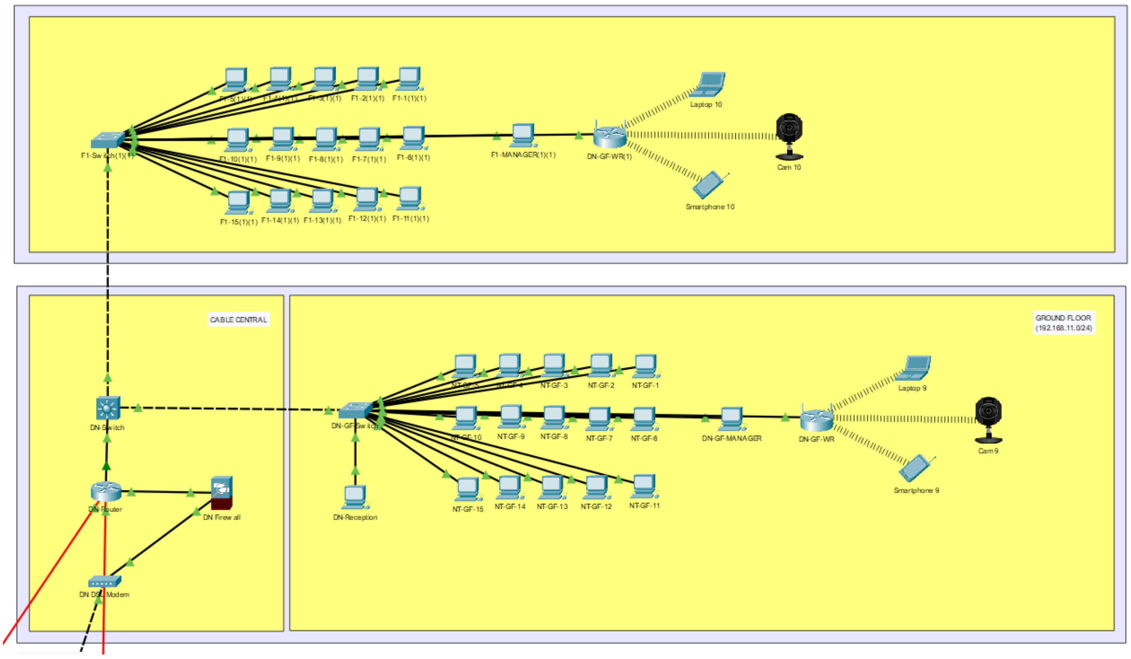


Figure 15: BB Bank's Da Nang branch

5.4 The Internet Service Provider

Below is the depiction of what an Internet Service Provider (ISP) should look like.

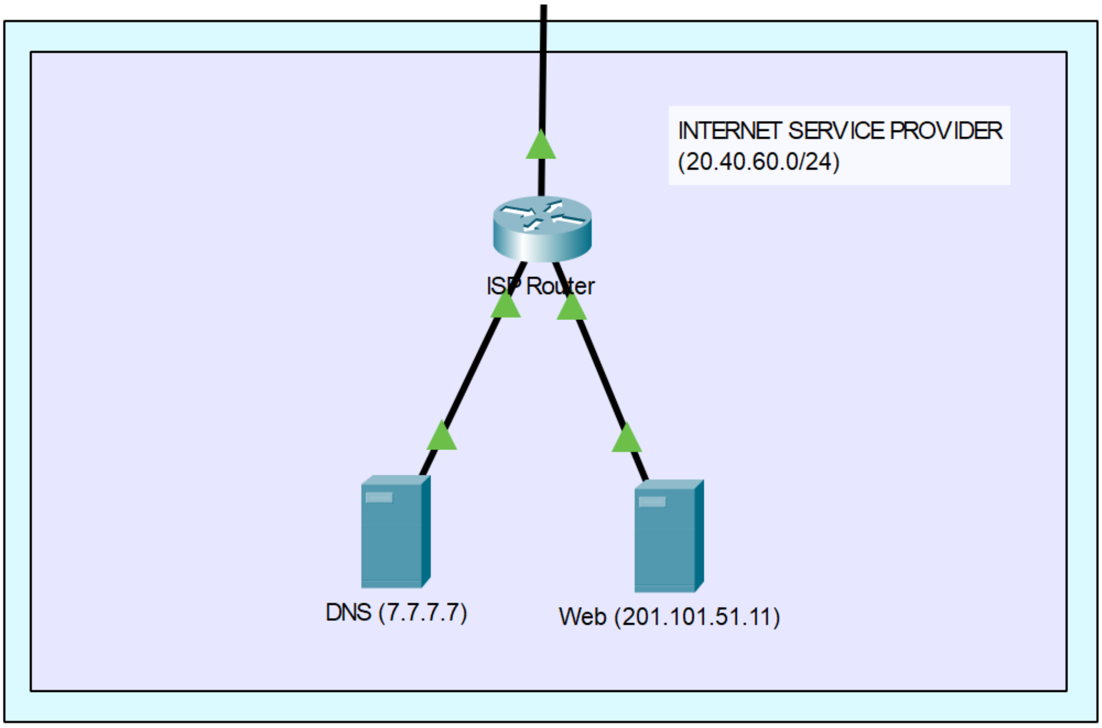


Figure 16: ISP interpretation

An ISP contains an HTTP web server accompanied with a DNS service server. These network components are routed to the Internet and the customers then subscribe to the network via a modem protocol. A DNS server is a resolution server to map key addresses to their respected IP address of the server which contains the web contents. In this case, whenever a request is made to the DNS, it is routed to the HTTP web server.

5.5 Network topology

The following figure summarizes the overall network topology of the entire network.

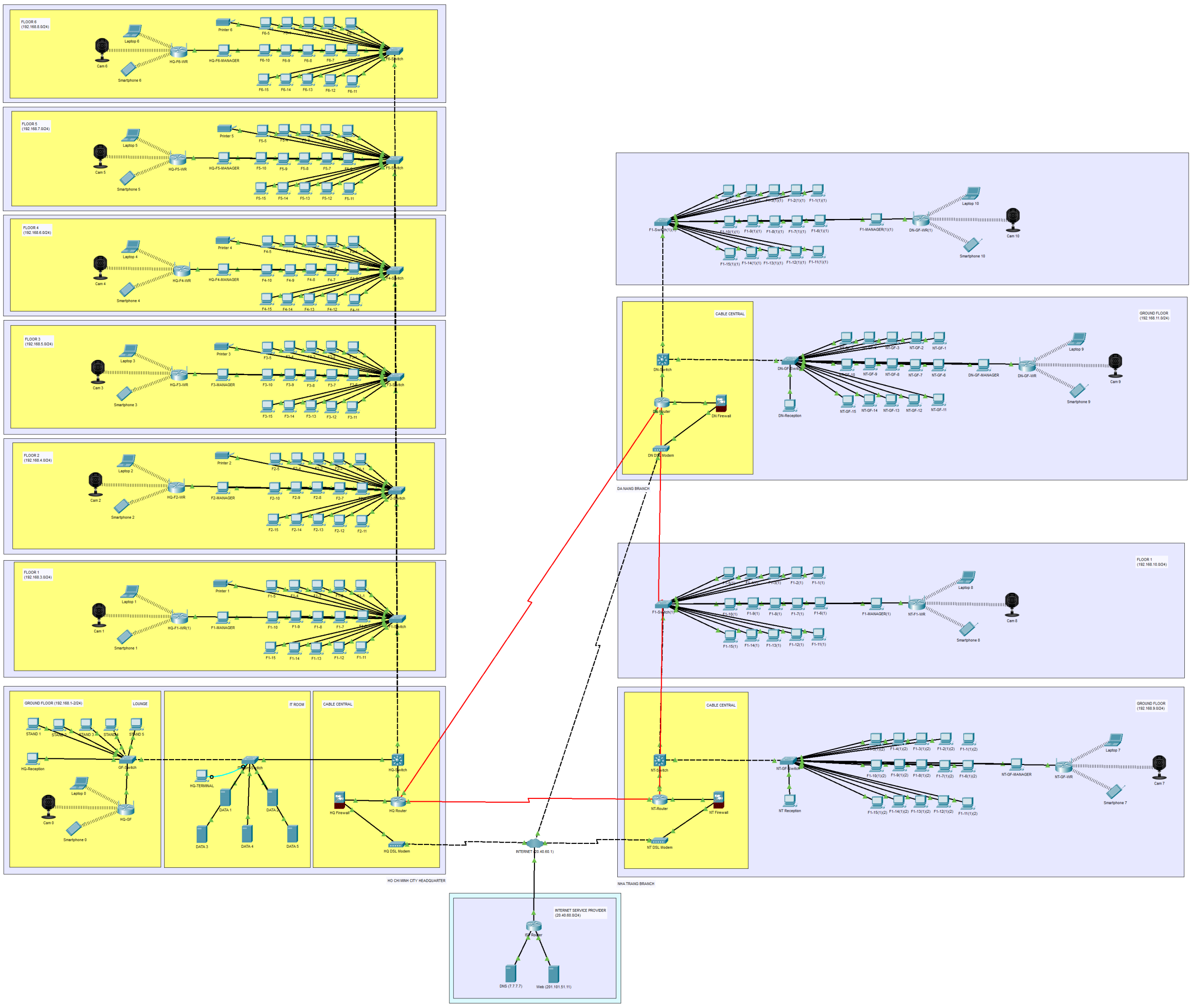


Figure 17: Network topology

To connect inter-VLANs of computers from branches and headquarter, a triangular routing method is introduced in the network via serial connections. Jumping between router is done using RIP routing. Each branch has their own set of network using DHCP from the central routing unit and is allowed to communicate to the ISP via NAT protocol of the installed firewall.

6 Testing and Evaluation

This section will test communication protocols between networks that we have set up in the previous section to ensure proper operation. The network shall meet the demands of:

- Computer-to-computer in the same VLAN.
- Computer-to-computer in different VLANs.
- Computer-to-computer from headquarter to branches.
- Computer-to-server from headquarter/branches to the ISP.
- Load testing with multiple packet sources.
- Fastest and shortest path in the network topology.

6.1 Inter-VLAN testing

With the given topology in this figure, we'll test ping a random computer who has an IP of 192.168.4.2 and a station with an IP address of 192.168.4.5, all of which are generated using DHCP of the headquarter's router.

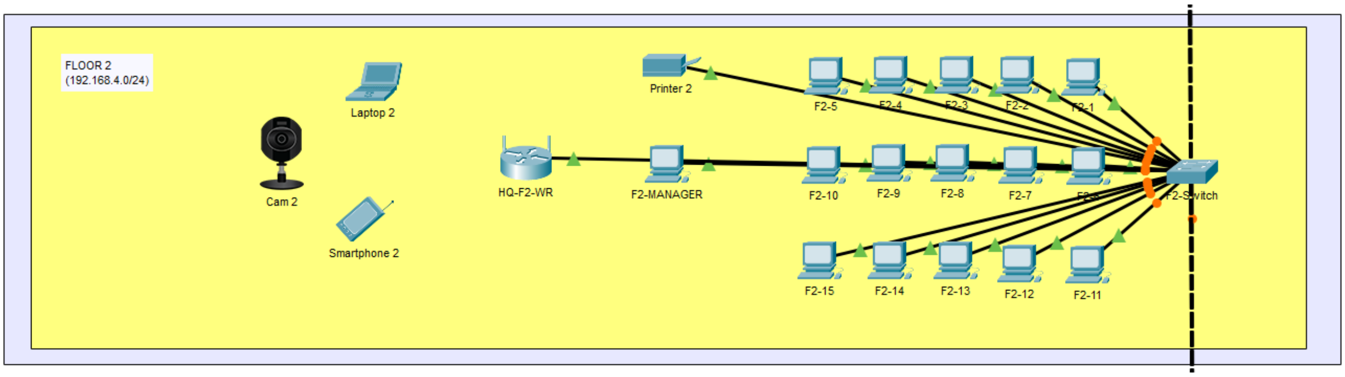
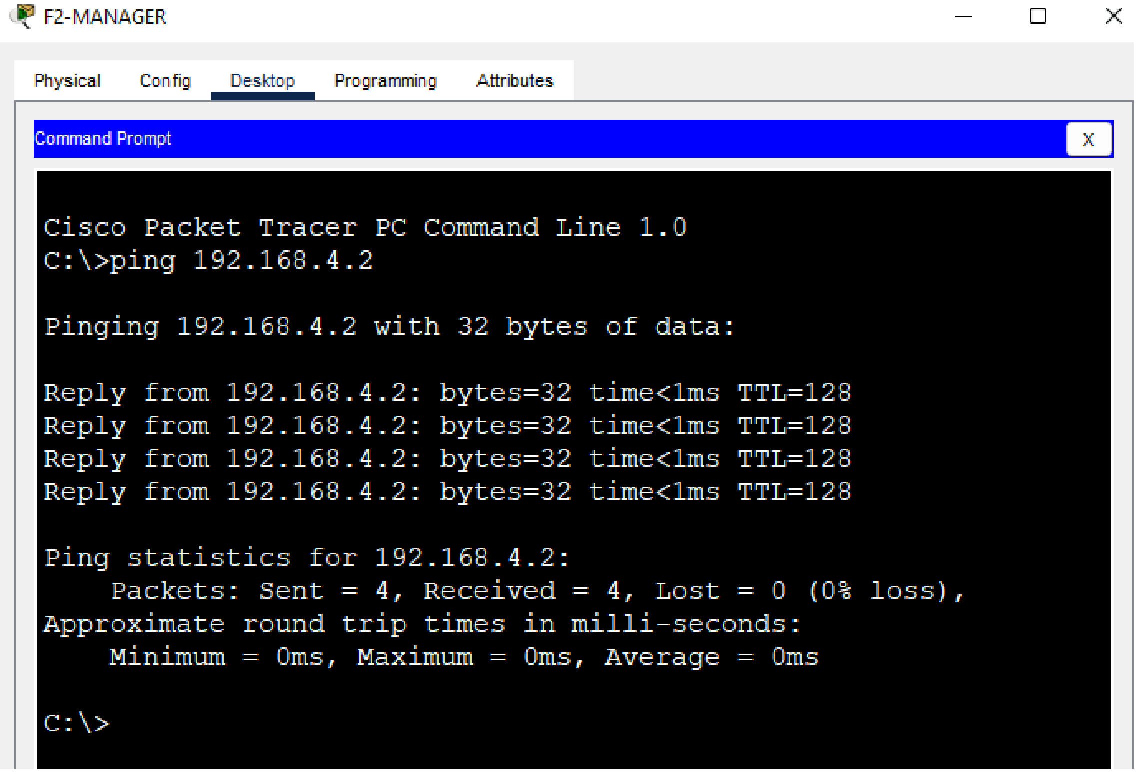


Figure 18: Network topology of HQ floor 2.

The result is shown below which displays successful connection.

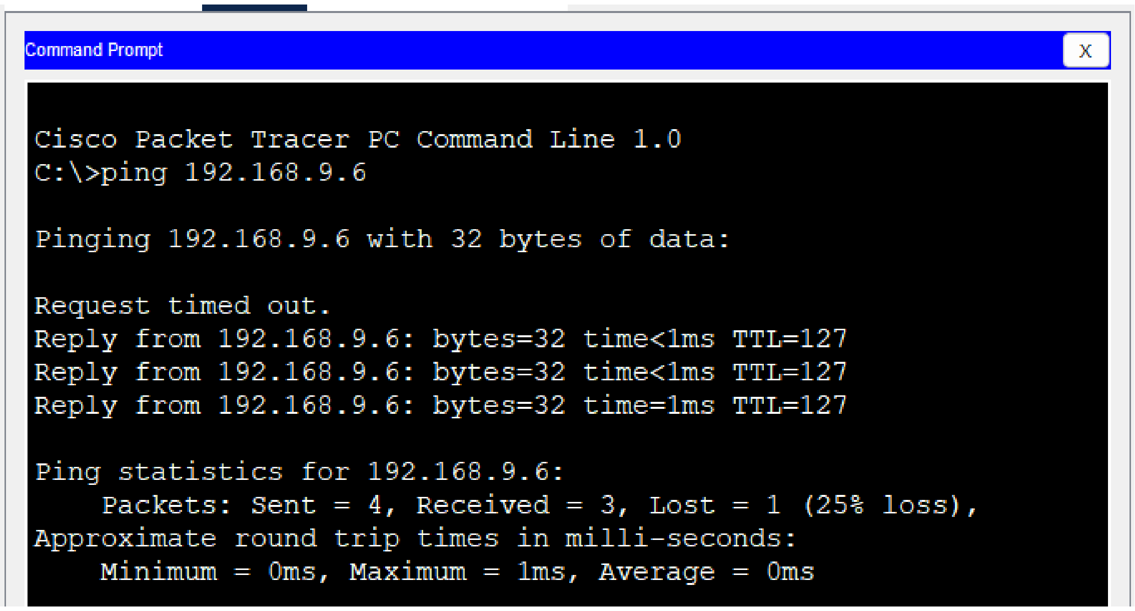


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time<1ms TTL=128
Reply from 192.168.4.2: bytes=32 time<1ms TTL=128
Reply from 192.168.4.2: bytes=32 time<1ms TTL=128
Reply from 192.168.4.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 19: Result of pinging 192.168.4.2.

6.2 Outer-VLAN testing

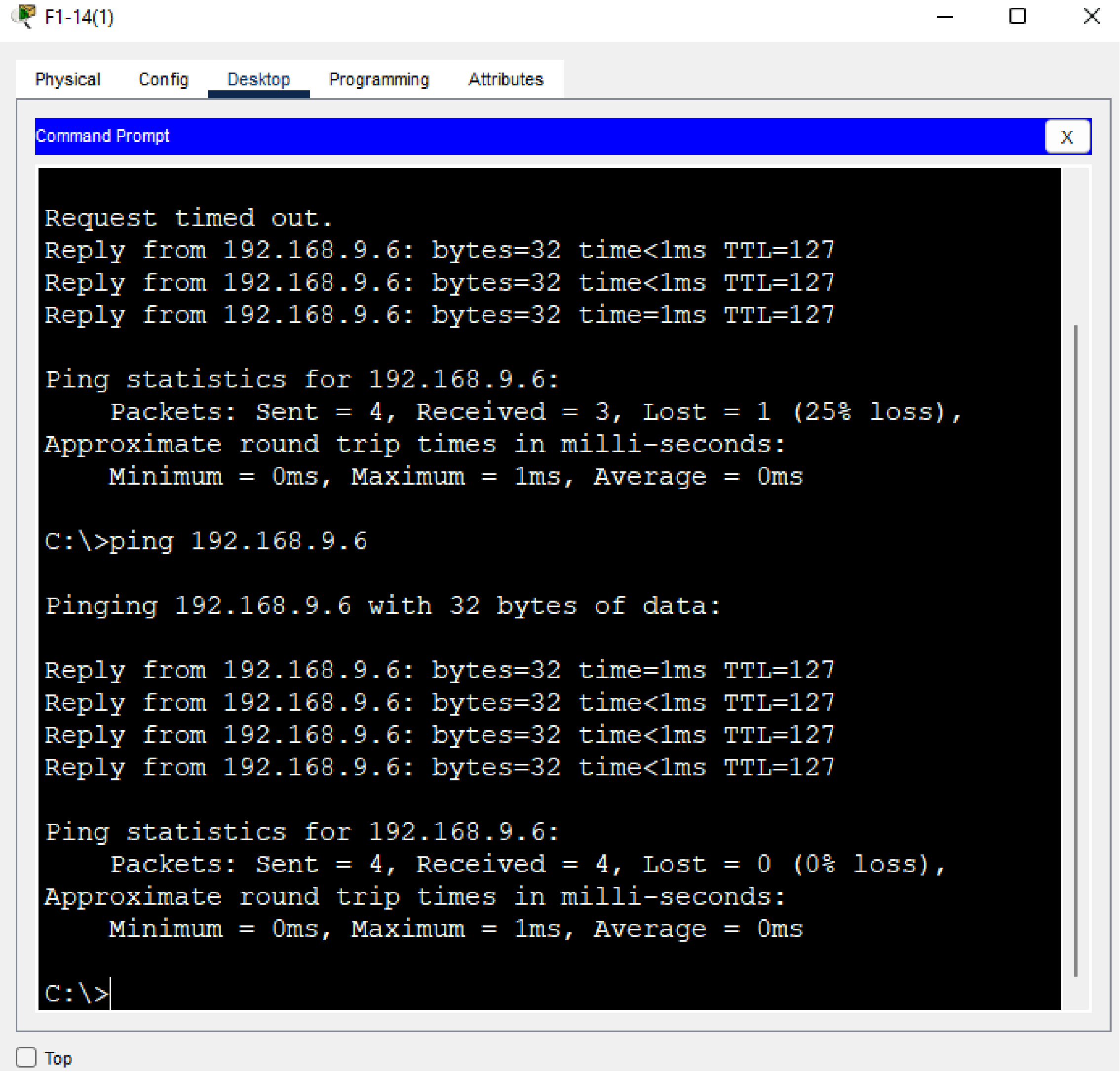
We will use the Nha Trang branch's floor-planning in figure 12 to test connection from first floor down to the ground floor.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.9.6

Pinging 192.168.9.6 with 32 bytes of data:

Request timed out.
Reply from 192.168.9.6: bytes=32 time<1ms TTL=127
Reply from 192.168.9.6: bytes=32 time<1ms TTL=127
Reply from 192.168.9.6: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.9.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 20: Result of pinging 192.168.9.6.

We see that the first time it pinged 192.168.9.6, it resulted in a timed-out session. This is the because the ARP protocol was doing its job to mark the packet trace in the network. It got sent back by the multi-layer switch because the it does not know where to forward this packet due to VLAN routing, however, a trace was left and the second time the ICMP protocol started to transmit, the multilayer switch knows where to route the packet to its correct destination.



```
Request timed out.
Reply from 192.168.9.6: bytes=32 time<1ms TTL=127
Reply from 192.168.9.6: bytes=32 time<1ms TTL=127
Reply from 192.168.9.6: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.9.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.9.6

Pinging 192.168.9.6 with 32 bytes of data:

Reply from 192.168.9.6: bytes=32 time=1ms TTL=127
Reply from 192.168.9.6: bytes=32 time<1ms TTL=127
Reply from 192.168.9.6: bytes=32 time<1ms TTL=127
Reply from 192.168.9.6: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.9.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 21: Pinging 192.168.9.6 a second time

After the second ping, the multilayer switch learns where to communication with the packets and the station received replies from the other station downstairs successfully.

6.3 WAN testing

We will now test a random WAN connection from the headquarter to a branch, say, Da Nang in the North of Vietnam. The target IPs will be the circled stations in the figure below.

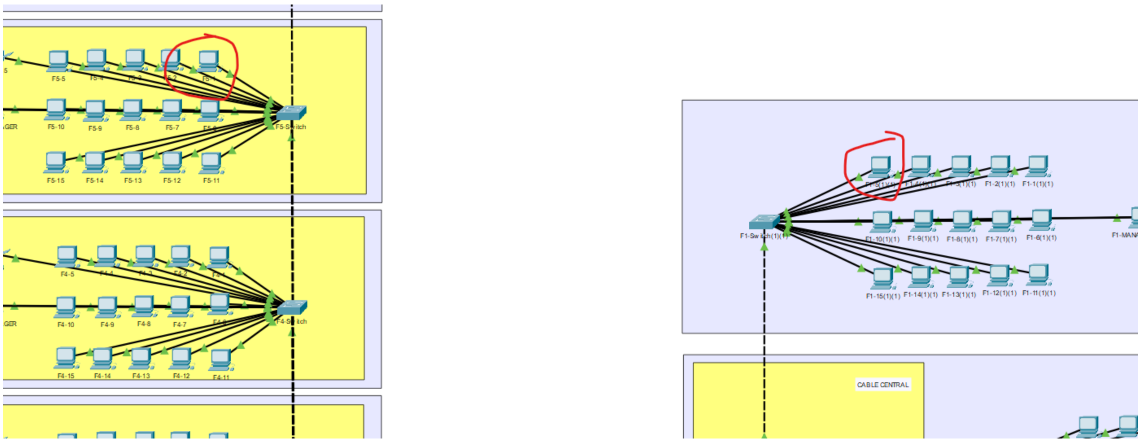
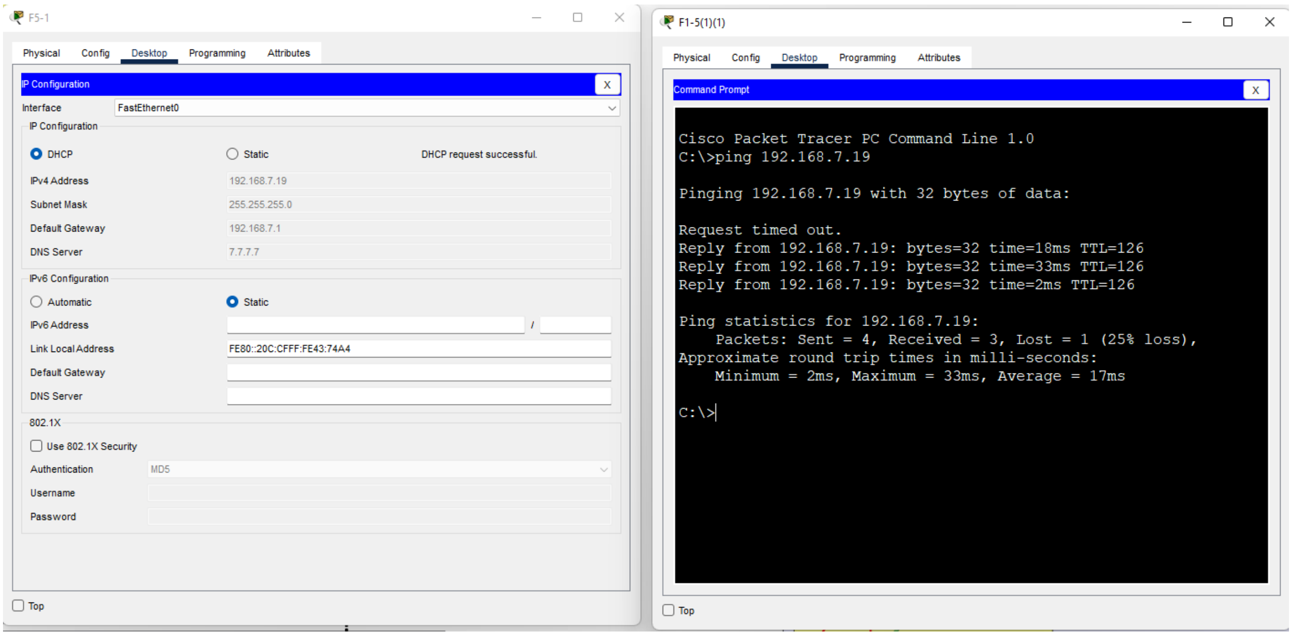


Figure 22: Targets for pinging.

The result is shown below. Aforementioned, the first request shall be a denied ARP request, however, multiple pingings afterwards ensure proper connection.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.7.19
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.7.1
DNS Server: 7.7.7.7

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /
Link Local Address: FE80::20C:CFFF:FE43:74A4
Default Gateway:
DNS Server:

802.1X

□ Use 802.1X Security

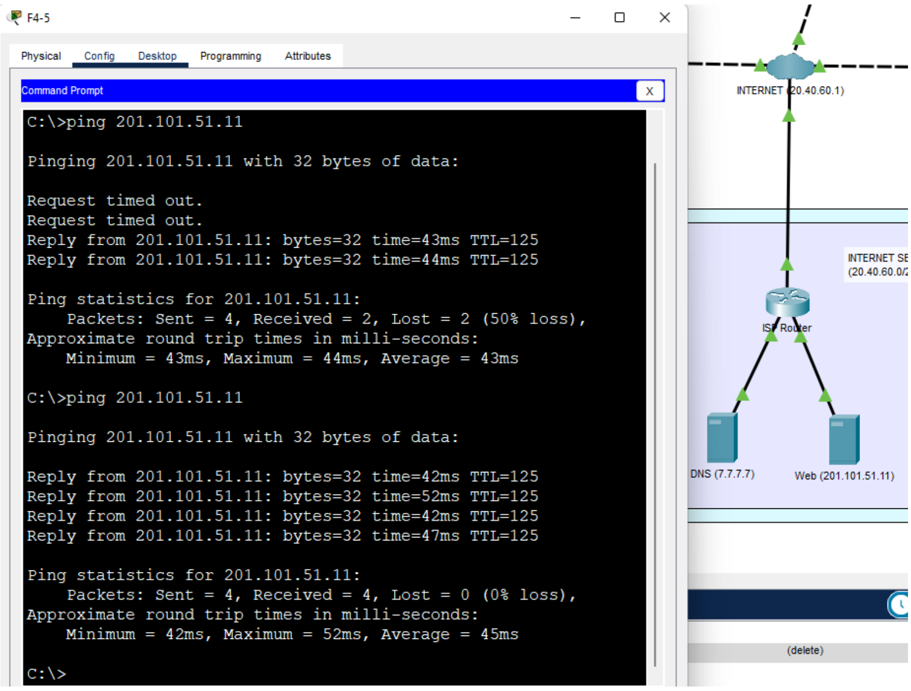
Authentication: MD5
Username:
Password:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.7.19

Pinging 192.168.7.19 with 32 bytes of data:

Request timed out.
Reply from 192.168.7.19: bytes=32 time=18ms TTL=126
Reply from 192.168.7.19: bytes=32 time=33ms TTL=126
Reply from 192.168.7.19: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.7.19:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 33ms, Average = 17ms

C:\>
```

Figure 23: Result of pinging 192.168.7.19.

6.4 ISP testing

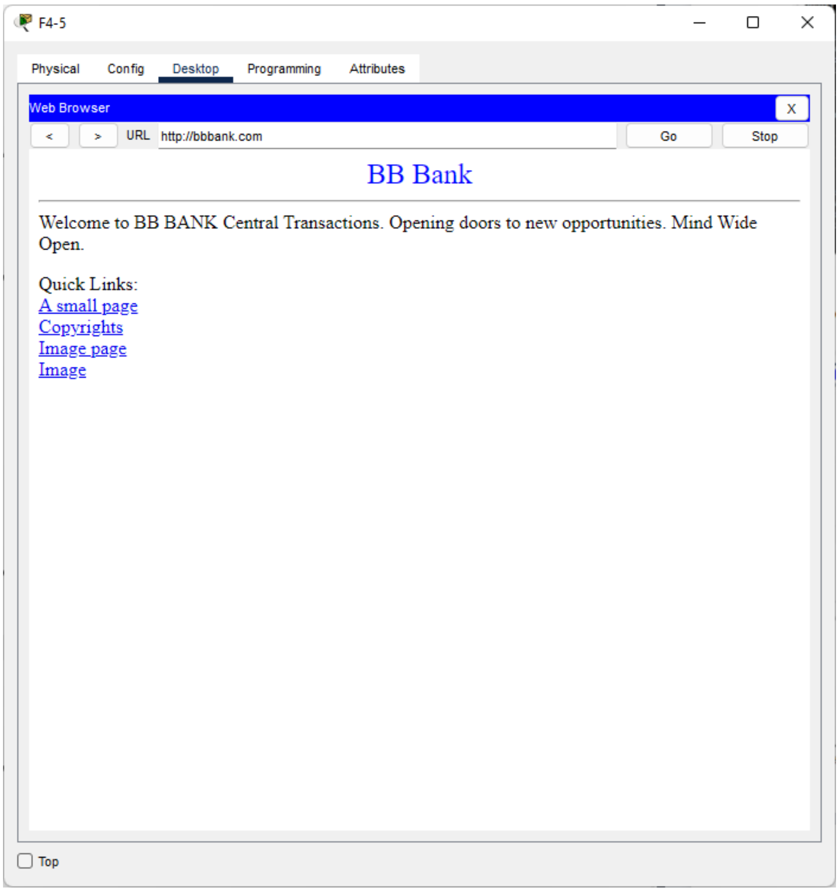
Let's try to access a random website from the ISP. To connect, first we will try to ping the server.



```
C:\>ping 201.101.51.11

Pinging 201.101.51.11 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 201.101.51.11: bytes=32 time=43ms TTL=125
Reply from 201.101.51.11: bytes=32 time=44ms TTL=125

Ping statistics for 201.101.51.11:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 43ms, Maximum = 44ms, Average = 43ms

C:\>ping 201.101.51.11

Pinging 201.101.51.11 with 32 bytes of data:

Reply from 201.101.51.11: bytes=32 time=42ms TTL=125
Reply from 201.101.51.11: bytes=32 time=52ms TTL=125
Reply from 201.101.51.11: bytes=32 time=42ms TTL=125
Reply from 201.101.51.11: bytes=32 time=47ms TTL=125

Ping statistics for 201.101.51.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 52ms, Average = 45ms

C:\>
```

Figure 24: Pinging to ISP server.

The result shown above illustrate two failed ARP requests but successful afterward. We will now try to access the server via a string address to test DNS protocol. The test is successful below.



URL http://bbbank.com

BB Bank

Welcome to BB BANK Central Transactions. Opening doors to new opportunities. Mind Wide Open.

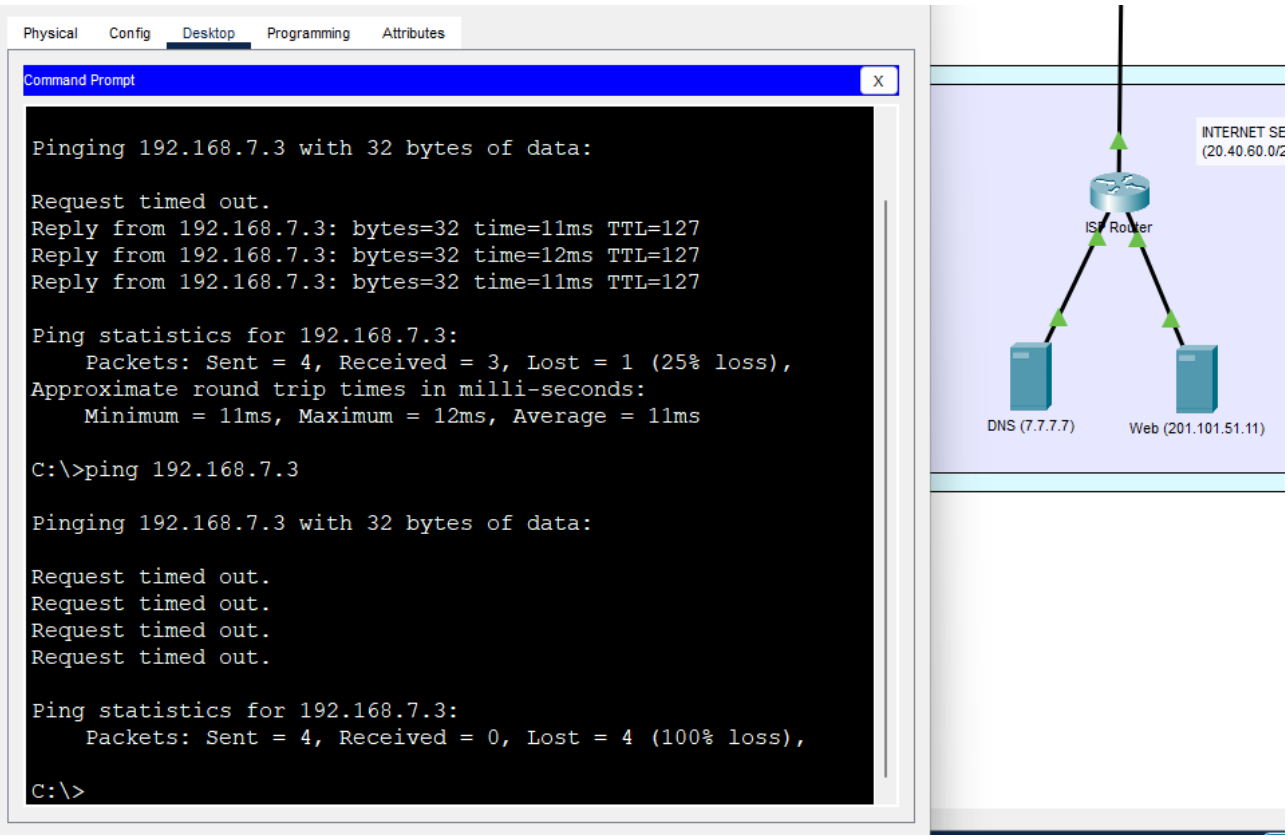
Quick Links:
A small page
Copyrights
Image page
Image

Figure 25: Result of accessing bbbank.com.

6.5 Firewall testing

Firewall only allows communication from the "inside" part of the network to the "outside" part of the network. The tests above have successfully demonstrated pinging from the headquarter to the ISP, which is inside to outside. We shall now try to ping from the ISP server back to the station in the headquarter, which should do be do-able because it is not allowed by the firewall.

The following image illustrates the assertion.



```
Pinging 192.168.7.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.7.3: bytes=32 time=11ms TTL=127
Reply from 192.168.7.3: bytes=32 time=12ms TTL=127
Reply from 192.168.7.3: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.7.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms

C:\>ping 192.168.7.3

Pinging 192.168.7.3 with 32 bytes of data:

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

Ping statistics for 192.168.7.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 26: Firewall prevents outside from pinging inside.

7 Conclusion - Future Work

7.1 Network evaluation

7.1.1 Security apparatuses

The following resources need to be protected:

- Hardware: hosts, servers, networking devices and stations.
- Software: operating systems, programs such as bank account managers, credits, accountant software, ATM.
- Data: crucial banking data such as transaction scripts, customers accounts, documentations, reports, accounting datas, etc.

Looking at the possible threats and attacks to the system, the following can be listed:

- Illegal access from unauthorized personnel. The system shall be administered to specific groups of people with their respective rights to access banking information internally. Any attempted illegal access shall be denied by the firewall.
- Threats of mass data collecting, this can affect the entire system due to the critical errors of storing data unmanageable, passing data (packets) from one system to another, and stored copy datas from servers.
- Threats that affect normal functionalities of the network includes: untraceable packets, packets wandering in the network without knowing where to head next, overloaded bandwidth, segregation due to critical device shutdown, virus existence, and damaged security apparatus.

What the network has solved? The following lists out the security layers of the suggested network system:

- Network layer security.
- Access layer security.
- Peripherals and devices security.
- Host protection.
- Operating system protection.
- Application protection.
- Maximum database security.

In summarizing, the proposed network has ensured complete to almost prone-free of internal networking, preventing all types of unauthorized access both internally and outside from Internet services. It can also account for users management and ensure bandwidth safety during heavy load. The design fits the budget of the bank.

7.1.2 Networking solutions

We propose several solutions to the proposed network in case of random malfunctioning of the network as follows:

- Internet connection mishaps: we use leased-line and ADSL with load balancing mechanism in order to divide evenly the bandwidth via leased-line to ADSL in case leased-line encounters error.
- Networking devices malfunction: backup devices on storage, setting priority to devices (central devices gets higher priority). When the main device encounters issue, the network immediately switch to backup devices ensuring proper network activity.
- Servers in the DMZ: backup servers ready to operate with mirrored data technology, frequent backups to prevent down times.
- Internal LAN: Use switches, multi-layer switches with spanning tree and dot1Q encapsulation to make backup connections in case of issues.
- Constructing a Cable Central and IT room for technical replacements.

7.1.3 Subscribing to high speed and stable Internet

After calculating the speed for the entire network of the bank, accounting current network structure, cost and current workload of the headquarter and the branches, the subscription of the Internet should meet the following requirements:

- Minimum bandwidth speed for headquarter: 500Mbps
- Minimum bandwidth speed for branches: 200Mbps

7.1.4 Communication usages

- Each floor communicates to the server via a main switching unit. Each branch communicates with each other via a mainn HQ web server.
- Guest devices shall not access server address, only HTTP servers from the ISP.
- Server VLAN 10 allows all branches to ping to it.
- Load balancing mechanisms is applied on routing paths to branches.
- Configurations in branches in similar to that of the HQ.

7.2 Future upgrades for the system

At the current point of time, the system meets the demand of the banking corporate. However, a lot more can be done to efficiently build a better network for the bank, namely:

- The bandwidth safety percentage is 25% for network stability. When the need for higher bandwidth arises, we shall subscribe to the ISP a higher bandwidth data plan.

- In the future, we aim to use more Cisco networking devices to assist in better technicality, better device stability. Especially corporates, universities are using Cisco devices everyday for their networking needs.
- Adding more ADSL lines that connect directly from the HQ to the ISP.
- Preparing more devices in case of emergency.
- Upgrading for better networking routes.
- Server and backup servers upgrade.

- End of report -