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

MẠNG MÁY TÍNH

Assignment 2

MINI PROJECT:
COMPUTER NETWORK DESIGN FOR BUILDING OF THE BANK

GVHD: Nguyễn Quang Sang
Sinh viên: Nguyễn Khắc Bảo - 1912675
Vũ Thành Công - 1912811
Nguyễn Đăng Hải - 1913254
Nguyễn Chí Tuệ - 1915795

HO CHI MINH CITY, 10/2021

Contents

Introduction

Computer & Construction Concept was asked to design a computer network used in the headquarters of a BB Bank which was preparing to build a new one. The bank has 2 branches in Nha Trang and Da Nang with different technical from the headquarters.
In this project, our team would like to propose a network system design to meet the current and expanding needs of the bank based on the actual network usage parameters provided.

1 Step 1: Network Architure

1.1 Analysis of network system requirements

BBB's Computer Network is estimated for a growth rate of 20% in 5 years (in terms of number of users, network load, branch extensions, ..).

1.1.1 Headquarters

- The building consists of 7 floors, each floor is equipped with a network engineering room and Cabling Central Local.
- BBB is a Small Enterprise: 100 workstations, 5 Servers, 10 Network devices.
- Using new technology for network infrastructure, 100/1000 Mbps and Wireless.
- Organize the network according to the VLAN structure.
- Use a combination of Licensed and Open source Software
- Connect to outside by 2 Leased line and 1 ADSL, using Load-balancing
- Office application, client-server, multimedia, database
- High security, safe when problems occur, easy to upgrade the system

1.1.2 Branches

BBB needs to connect to 2 branches in Nha Trang and Da Nang. Branches are smaller.

- The building has two floors, the 1st floor rooms are equipped with one Technical and Network Cabling Central Local.
- Each Branch has 50 Workstations, 3 Servers, 5 Network Equipment

No	Survey Content	Check	Result
Headquarter and two Branches			
1.	The number of network devices in each floor, each room		
2.	Area per floor, per room		
3.	Room layout in each floor, interior layout in each room		
4.	Investment costs for the network system		
5.	Types of connected devices (port type-/bandwidth,...)		
Two Branches			
1.	Distance to headquarters		

Bảng 1: Detailed table of survey

1.1.3 Traffic and system load

The implementation of the connection between headquarters and branches is performed via WAN links of subscribes party father.

- Concentrate about 80% at peak hours 9:00 - 11:00 and 15:00 - 16:00
- Servers used for updates, web access, database access, ... Total upload and download at about 500 MB/day.
- Each workstation is used for browsing the Web, downloading documents, customer transactions, ... General content upload and download amount is about 100 MB/day.
- WiFi-connected laptop for customers to access about 50 MB/day.

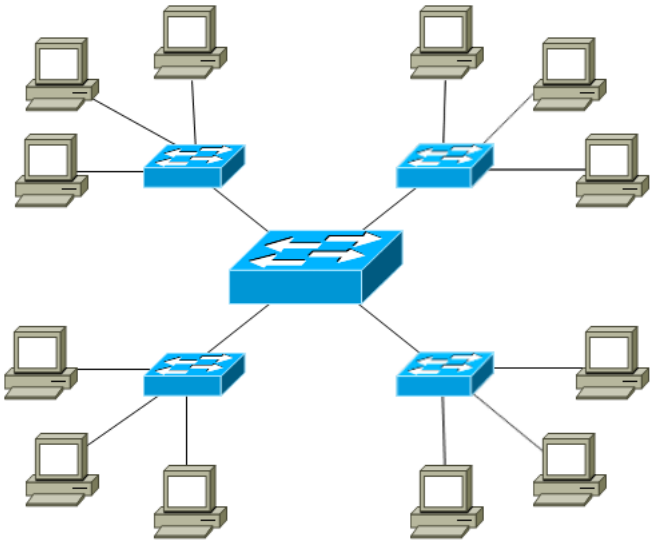
1.2 Detailed table of survey

1.3 Inside building Physical Network Architecture

1.3.1 Network topology

In our design, we use Extended star topology for each building (headquarter and two branches). In this, we have a switch layer 3 in the 1st floor network engineering room connected to the switches layer 2 on the other floors. We choose it because:

- It provides a lower cost.
- It allows for easier management and troubleshooting of a network, extending the network by adding additional devices is much faster and easier to accomplish.
- If one computer goes down it will not affect the entire network.



Hình 1: Extended star topology

Specifically for headquarters and branchs, we calculate in the following section.

1.3.2 Headquarter

There are 100 workstations, 5 Servers, 10 Network devices in headquarter. In each floor has about:

$$\left\lceil \frac{100+5}{7} \right\rceil = 15 \text{ devices}$$

For the above needs, we will use 1 switch layer 2 having 24 ports on each floor. There will be a port that connects to the switchboard in the 1st floor network engineering room.

1.3.3 Branches

There are 50 workstations, 3 Servers, 5 Network Equipment devices in each branch. In each floor has about:

$$\left\lceil \frac{50+3}{2} \right\rceil = 27 \text{ devices}$$

For the above needs, we will use 2 switch layer 2 24 ports connect together on each floor. There will be a port that connects to the switchboard in the 1st floor network engineering room.

1.4 Technique using in Network Architecture

1.4.1 VLAN with VTP

For each department, we will create a separate VLAN for that department. This meets the need for private sharing between departments and increases system performance by reducing broadcast costs, making it easy to spot errors. We have 10 departments1

with 10 VLANs.
Another technique is used is VLAN Trunking Protocol (VTP). This technology makes the management of VLANs (add / delete / edit) synchronous and easier because just make changes on the Server switch, all changes will be updated to the switch Client.

1.4.2 Subinterface

Used for routing between VLANs. It helps save the router's physical port. With a physical gate we can divide into multiple logic gates (subinterface).

1.4.3 Access list

Use to control access between VLANs to increase security. Only computer in Director VLAN can ping each other, other VLANs cannot.

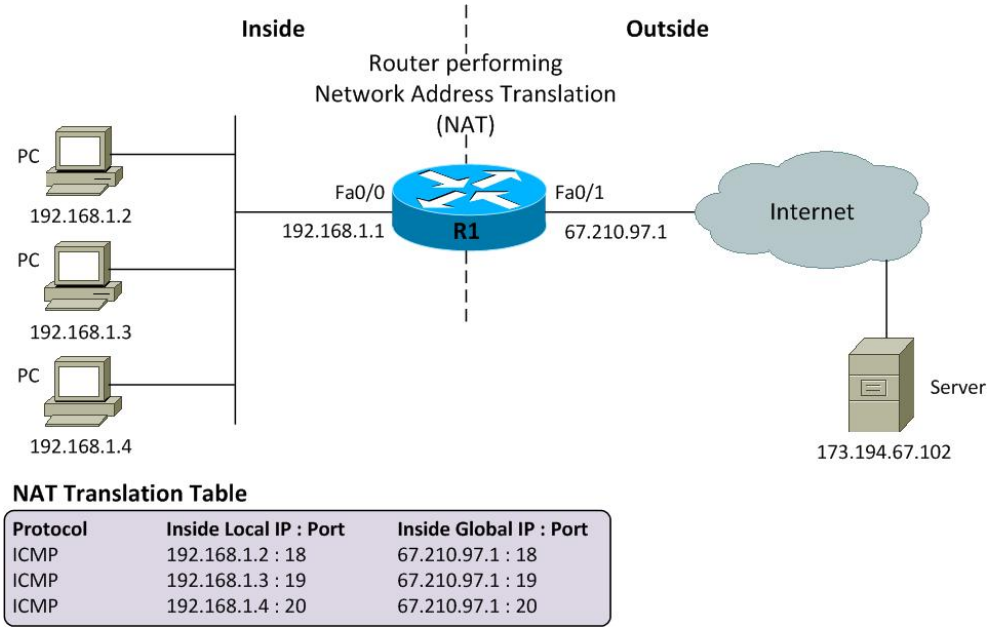
1.4.4 Subnet mask

We using Subnet mask technique for private IP start from 192.168.0.0. Each VLANs will have different IP range. Using this technology, we will have the following advantages:

- Save and optimize IP address allocation.
- Broadcast Domain, optimizing network traffic and improving network performance.

1.4.5 NAT Overload

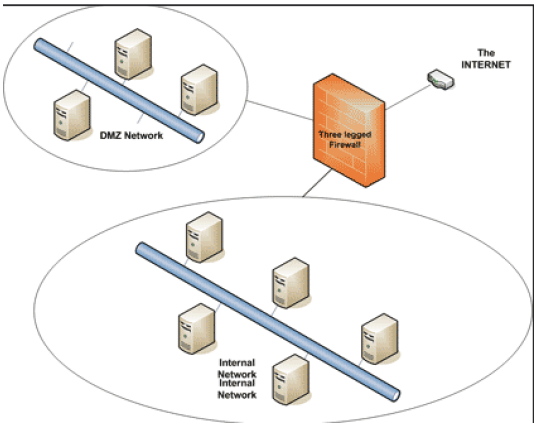
NAT Overloading or Port Address Translation (PAT) is a modified form of dynamic NAT. PAT allows overloading or the mapping of more than on inside local address to the same inside global address. So that, we only need to rent 1 public IP address, minimizing costs incurred.



Hình 2: Port Address Translation (PAT)

1.4.6 DMZ Network

DMZ (Demilitarized Zone) helps us protect servers in internal network. If public servers are attacked, hackers still cannot rely on them to attack servers located inside that contain important information. Server in DMZ include: Web, Mail, FTP, VoIP,...



Hình 3: DMZ Single Firewall

2 Step 2: Equipment list, IP diagram and cabling diagram

2.1 Equipment list

2.1.1 Servers

In a bank it is essential to have the following servers:

1. Web server: For external customers to access to get information about their accounts in banks and other services.
2. Mail server: To send and receive mail.
3. File server: To share information.
4. DNS server: To convert domain name to IP address.
5. Database server: To store information
6. Backup server: To contains backup information

Servers need to be configured strongly enough to accommodate multiple concurrent and continuous access.

2.1.2 Switch layer 2: CISCO Catalyst WS-C2960-24TC-S

- Maximum Port density: 24 x 10/100 + 2 dual-purpose (10/100/1000 or SFP) ports
- DRAM: 64 MB
- Throughput: 6.5 Mbps
- Number of VLANs: 64

Hình 4: Switch CISCO Catalyst WS-C2960-24TC-S

2.1.3 Switch layer 3: CISCO Catalyst WS-C3650-24TS-S

- Maximum Port density: 24 x 10/100/1000 Ethernet
- MAC Address Table Size: 32000 entries
- RAM: 4 GB
- Stack bandwidth: 160 Gbps
- Forwarding Bandwidth: 65.47 Mbps

Hình 5: Switch CISCO Catalyst WS-C3650-24TS-S

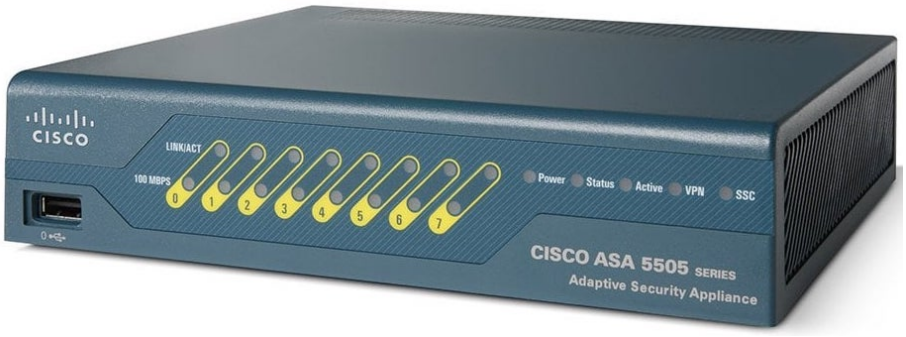
2.1.4 Router: CISCO 2911-SEC/K9

- Port: 3 integrated 10/100/1000 Ethernet ports (RJ-45 only)
- Routing: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, static IPv4 IPv6
- DRAM: 512 MB (installed) / 2 GB (max)
- Embedded hardware-accelerated VPN encryption for secure connectivity and col-laborative communications
- Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering

Hình 6: Router CISCO 2911-SEC/K9

2.1.5 Firewall: CISCO ASA5505-BUN-K9

- Firewall Users: 10
- Maximum firewall throughput: 150 Mbps
- Maximum connections: 10.000
- Packets per second (64 byte): 85.000
- Maximum VLANs: 3 (trunking disabled)



Hình 7: Firewall CISCO ASA5505-BUN-K9

2.1.6 Access Point: Cisco Business 240AC WiFi

- Max data rate: 1733 Mbps
- LAN port: 2 GbE
- Security: WPA/WPA2, WPA3, WPA2 - Enterprise, RADIUS Server

Hình 8: Cisco Business 240AC WiFi

2.2 Cable

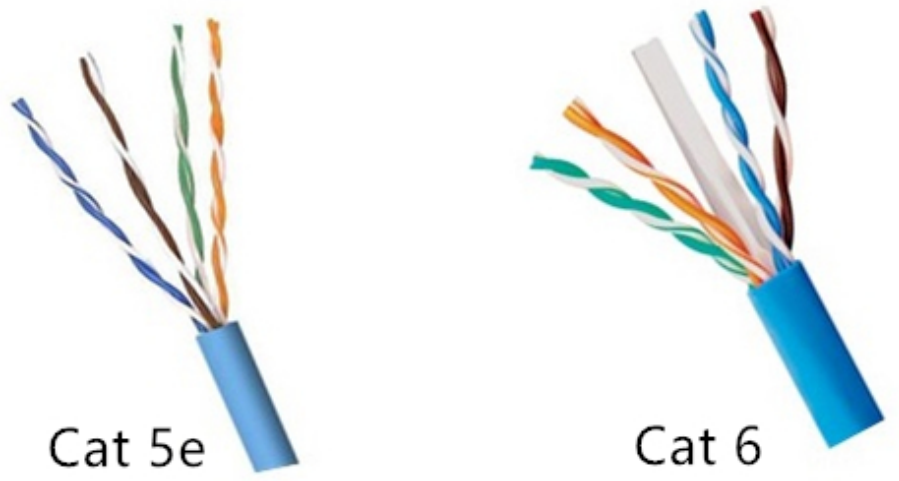
We using AMP Cat 5e UTP:

- All requirements of Gigabit Ethernet (IEEE 802.3ab) are satisfied (1000 Mbps).
- Bandwidth: supports up to 200 MHz

MP Netconnect Cat 6 UTP

- Meets and exceeds the Category 6 standard performance requirements according to TIA/EIA-568-B and ISO/IEC 11801 Class E

- Bandwidth: supports up to 600 MHz



Hình 9: Cable cat 5e and cat 6

2.3 IP diagram

We using 16-bit block private IP has range from 192.168.0.0 →192.168.255.255 (65 536 addresses) and Subnet mask 255.255.255.0/24. Therefore, we will have the details of the subnet:

- $2^8 = 256$ subnet
- $2^8 = 256$ host/subnet. In this, we have 2 host for network and broadcast.

VLAN	Department	Network	IP range
10	Server	192.168.1.0	192.168.1.1 → 192.168.1.254
20	Director	192.168.2.0	192.168.2.1 → 192.168.2.254
30	Financial & Accountant	192.168.3.0	192.168.3.1 → 192.168.3.254
40	Human Resource	192.168.4.0	192.168.4.1 → 192.168.4.254
50	Administration	192.168.5.0	192.168.5.1 → 192.168.5.254
60	Customer Relations	192.168.6.0	192.168.6.1 → 192.168.6.254
70	Capital Management & Business	192.168.7.0	192.168.7.1 → 192.168.7.254
80	Risk management	192.168.8.0	192.168.8.1 → 192.168.8.254
90	Money Management	192.168.9.0	192.168.9.1 → 192.168.9.254
100	Inspection & Supervision	192.168.10.0	192.168.10.1 → 192.168.10.254

Bảng 2: VLANs and IP range in Headquarter

VLAN	Department	Network	IP range
10	Server	192.168.20.0	192.168.20.1 → 192.168.20.254
20	Financial & Accountant	192.168.21.0	192.168.21.1 → 192.168.21.254
30	Human Resource	192.168.22.0	192.168.22.1 → 192.168.22.254
40	Administration	192.168.23.0	192.168.23.1 → 192.168.23.254
50	Money Management	192.168.24.0	192.168.24.1 → 192.168.24.254

Bảng 3: VLANs and IP range in Brach 1

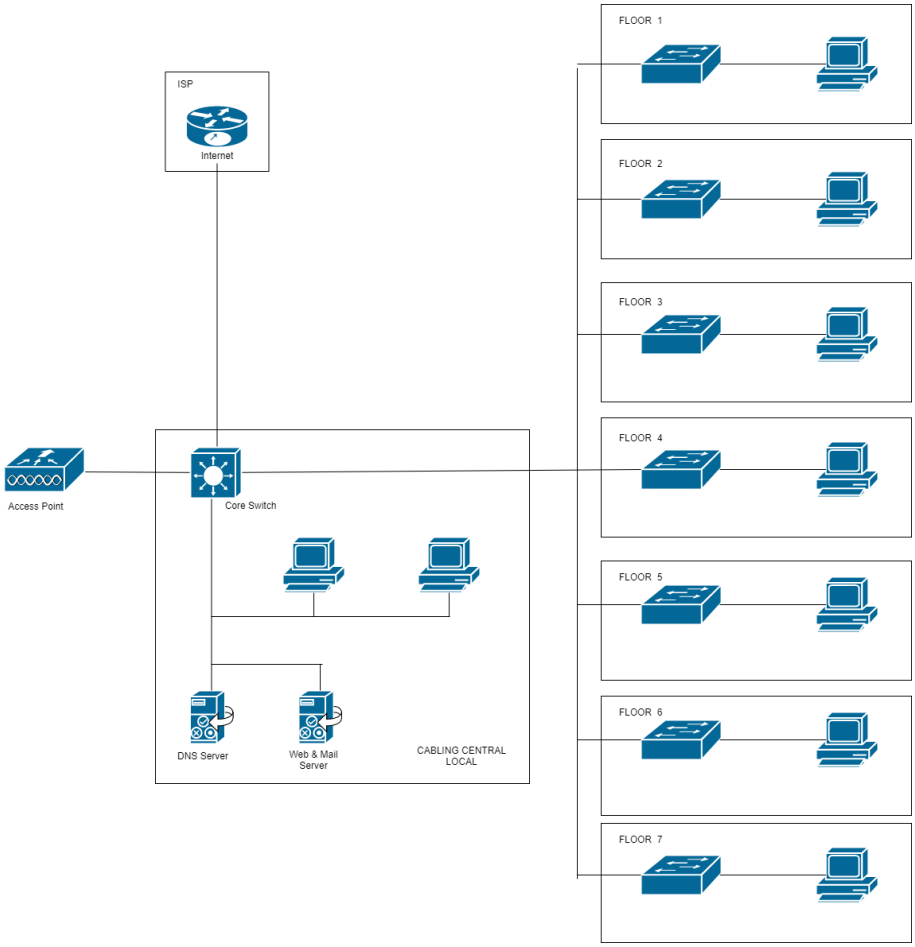
VLAN	Department	Network	IP range
10	Server	192.168.30.0	192.168.30.1 → 192.168.30.254
20	Financial & Accountant	192.168.31.0	192.168.31.1 → 192.168.31.254
30	Human Resource	192.168.32.0	192.168.32.1 → 192.168.32.254
40	Administration	192.168.33.0	192.168.33.1 → 192.168.33.254
50	Money Management	192.168.34.0	192.168.34.1 → 192.168.34.254

Bảng 4: VLANs and IP range in Brach 2

2.4 Cabling Diagram

2.4.1 Headquarter

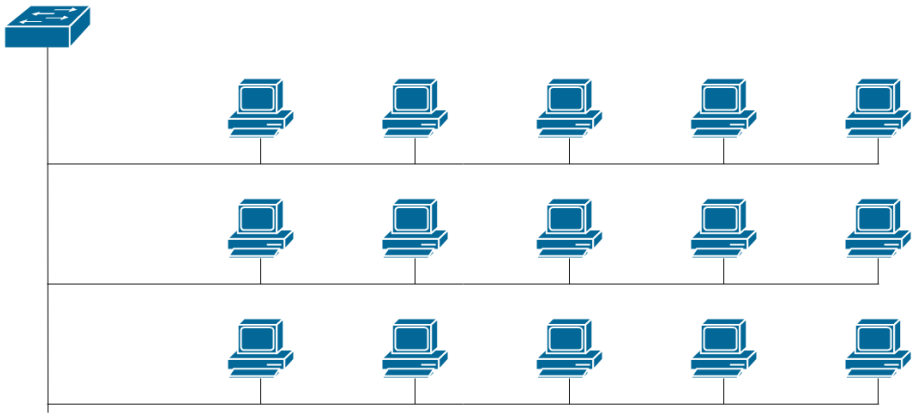
- 1 Cabling Central Local in floor 1.
- 7 floors in the building.



Hình 10: Cabling diagram in Headquarter

In each floor, we have:

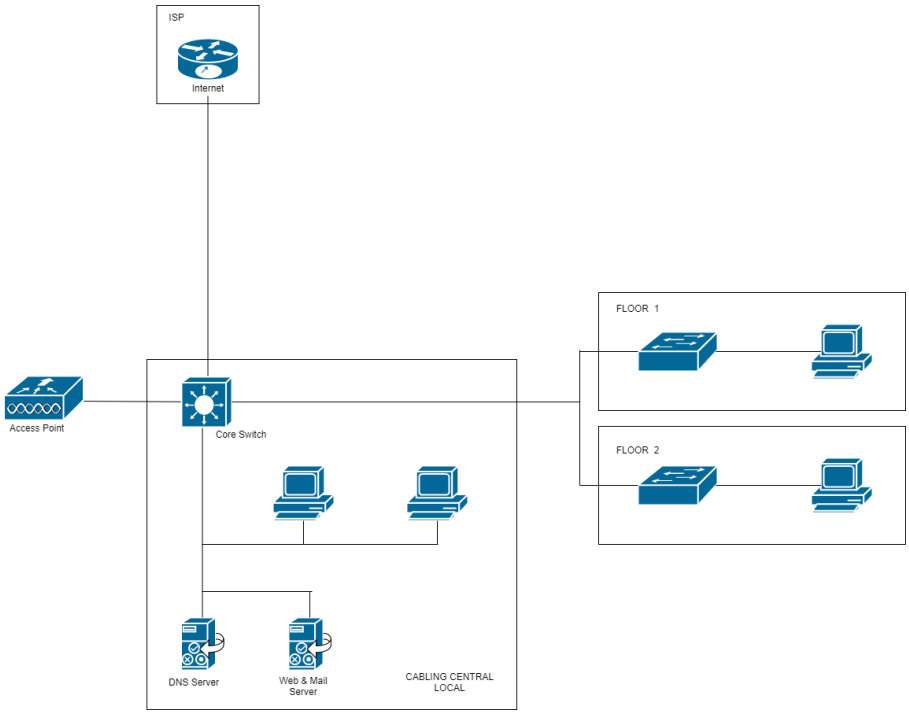
- 15 workstations.
- 1 switch connects to all workstations.



Hình 11: Cabling diagram at each floor in Headquarter

2.4.2 Branches

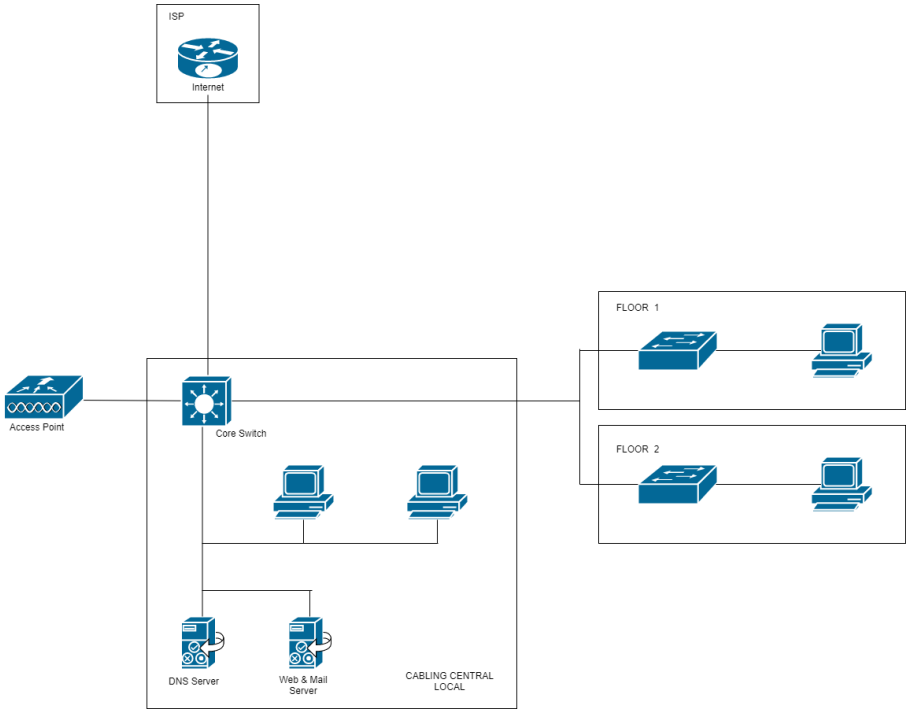
- 1 Cabling Central Local in floor 1.
- 2 floors in the building.



Hình 12: Cabling diagram in Branch

In each floor, we have:

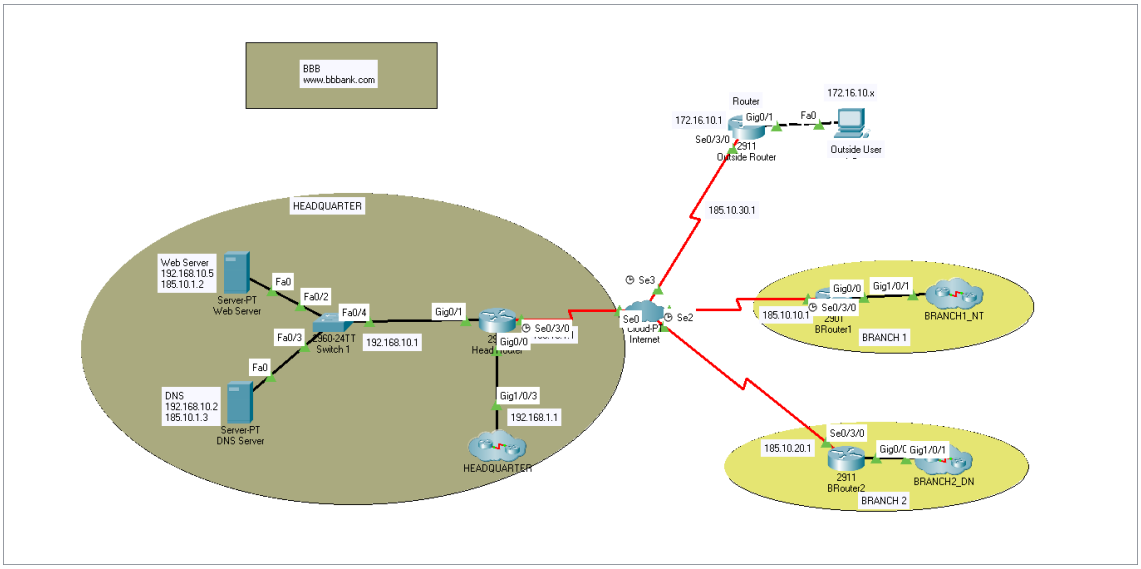
- 27 workstations .
- 2 switch connects to all workstations.



Hình 13: Cabling diagram at each floor in Branch

2.5 WAN connection diagram between Headquarter and Branches

Between the headquarters and the branch, we will use the WAN connection and the OSPF (Open Shortest Path First) protocol. OSPF supports VLSM (Variable Length Subnet Mask), allows load balancing and has better bandwidth usage.



Hình 14: WAN connection diagram between Headquarter and Branches

3 Step 3: Parameter calculation

Throughput is the determination of how much data is actually transferred during a time period through a network, interface or channel.
Bandwidth can be defined as the theoretical potential of the data that is to be trans- mitted in a specified period of time.
Determining throughput and bandwidth in a network is very important because it helps the network administrator to determine the connection for the network to run smoothly while saving costs on rental. Services used in network are:

- Sending and receiving mail.
- Browsing the Web.
- Providing web server services for external access.
- Synchronizing database with other headquarters.

The parameters of the flow and load of the system (about 80and 15h-16h) can be shared for Headquarter and Branches as follows:

- Servers used for updates, web access, database access, ... The total upload and download capacity is about 500 MB / day.
- Each workstation is used for Web browsing, document downloads, customer trans-actions, ... The total upload and download capacity is about 100 MB / day.
- WiFi-connected laptop for customers' accesses about 50 MB / day.

The total peak hours time in a days is 3 hours (9h-11h and 15h-16h)
Assume that the bank works 8 hours per days.

3.1 Headquarter

3.1.1 Wired network

1. Server: 5 servers with total upload and download capacity 500MB / day

- Bandwidth = $\frac{5*500*0.8}{3*3600} = 0.185$ MB/s
- Throughput = $\frac{5*500}{8*3600} = 0.087$ MB/s

2. Workstation: 100 workstations with total upload and download capacity 100MB / day

- Bandwidth = $\frac{100*100*0.8}{3*3600} = 0.741$ MB/s
- Throughput = $\frac{100*100}{8*3600} = 0.347$ MB/s

3.1.2 Wireless network

WiFi-connected laptop for customers to access about 50 MB / day.
Assume that the number of customers in one day is about 150 customers, and in peak time is 80 customers.

- Bandwidth = $\frac{8*100}{3*3600}$ = 0.370 MB/s = 2.963 Mbps
- Throughput = $\frac{150*50}{8*3600}$ = 0.260 MB/s = 2.083 Mbps

Total Bandwidth = 0.185 + 0.741 + 0.370 = 1.296 MB/s = 10.368 Mbps.
Total Throughput = 0.087 + 0.347 + 0.260 = 0.694 MB/s = 5.552 Mbps
To ensure the system works stably when there are more developments in the next 5 years. We'll stock up with 20% more:

- Bandwidth = 10.368 * 1.2 = 12.4416 Mbps.
- Throughput = 5.552 * 1.2 = 6.6624 Mbps.

3.2 Branches

3.2.1 Wired network

1. Server: 3 servers with total upload and download capacity 500MB / day.

- Bandwidth = $\frac{3*500*0.8}{3*3600}$ = 0.111 MB/s
- Throughput = $\frac{3*500}{8*3600}$ = 0.052 MB/s

2. Workstation: 50 workstations with total upload and download capacity 100MB / day

- Bandwidth = $\frac{50*100*0.8}{3*3600}$ = 0.370 MB/s
- Throughput = $\frac{100*100}{8*3600}$ = 0.174 MB/s

3.2.2 Wireless network

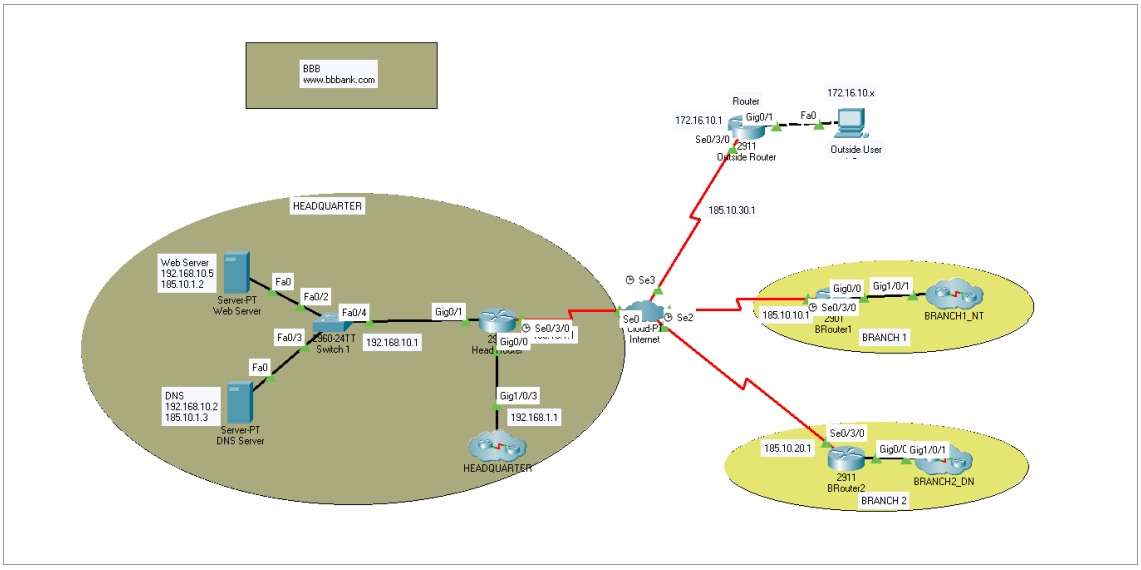
WiFi-connected laptop for customers to access about 50 MB / day.
Assume that the number of customers in one day is about 100 customers, and in peak time is 50 customers.

- Bandwidth = $\frac{50*50}{3*3600}$ = 0.231 MB/s = 1.852 Mbps
- Throughput = $\frac{100*50}{8*3600}$ = 0.174 MB/s = 1.389 Mbps

Total Bandwidth = 0.111 + 0.370 + 0.231 = 0.712 MB/s = 5.969 Mbps.
Total Throughput = 0.052 + 0.174 + 0.174 = 0.4 MB/s = 3.2 Mbps.
To ensure the system works stably when there are more developments in the next 5 years. We'll stock up with 20% more.

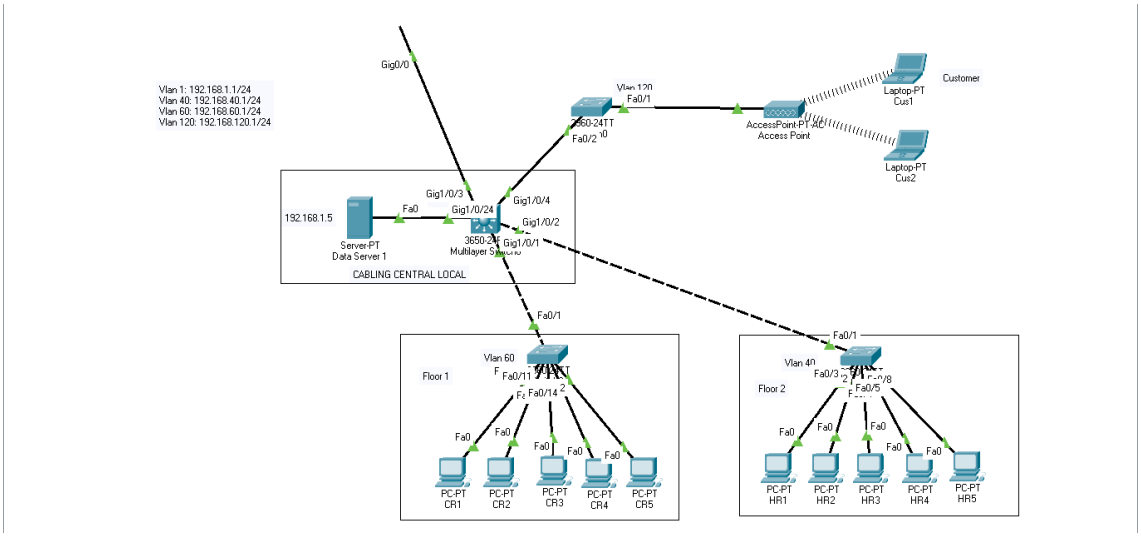
- Bandwidth = 5.969 * 1.2 = 7.1628 Mbps.
- Throughput = 3.2 * 1.2 = 3.84 Mbps

4 Step 4: Network design using Packet Tracer



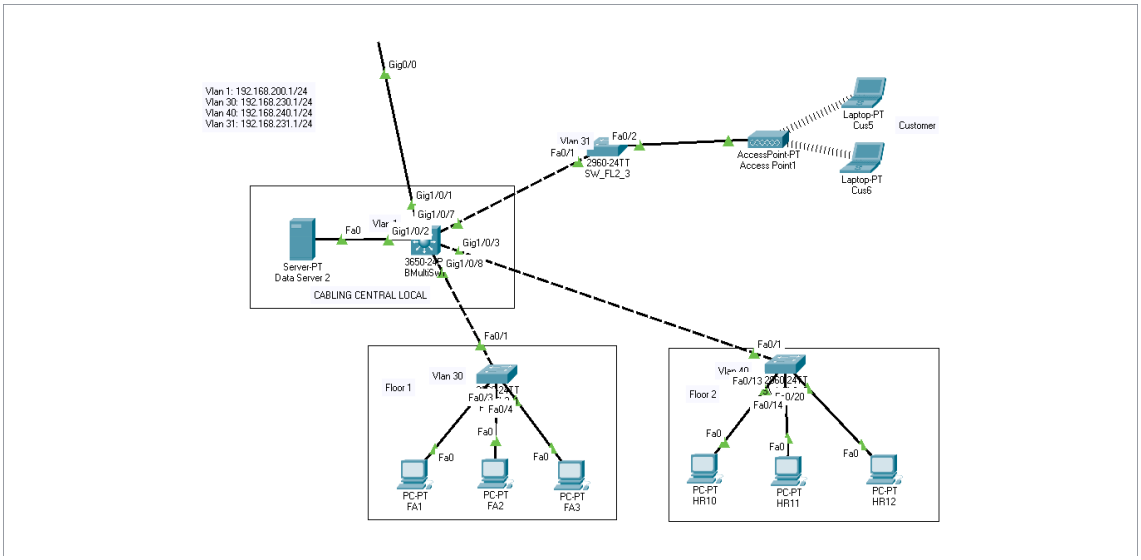
Hình 15: Design of WAN connection between Headquarter and Branches

4.1 Design in Headquarter



Hình 16: Design of network in Headquarter

4.2 Design in Branches



Hình 17: Design of network in each Branches

5 Step 5: System Testing

Testing standards:

- Computers in the same VLAN can ping each other.
- Computers in different VLAN can ping each other (except for the VLAN director).
- All computers on the network can connect to the internet through the bank's public IP address.
- Branch / user can ping the bank's headquarter server (web, ...).
- The wireless connection is working properly.

6 Step 6: Re-evaluate the network system

6.1 Investment costs

Investment costs for Headquarter and Branches(using VND)

Model	Unit price	Number	Total
Switch CISCO Catalyst WS-C2960-24TC-S	18.750.000	10	187.500.000
Switch CISCO Catalyst WS-C3650-24TS-S	166.450.000	3	499.350.000
Router CISCO 2911-SEC/K9	131.550.000	3	394.500.000
Access Point Cisco Business 240AC WiFi	4.800.000	3	14.400.000
Cable AMP Cat 5e UTP 305m	1.600.000	14	22.400.000
Cable AMP Netconnect Cat 6 UTP 305m	2.100.000	10	21.000.000
Sum			1.139.150.000
Costs incurred(10%)			113.915.000
Total costs			1.253.065.000

Bảng 5: Expense statistics table

6.2 Security

6.2.1 Requirement

The bank's operations always have a huge amount of information processed in real time. However, not everyone has access to these repositories. Therefore, the bank has the need to build a secure system for the computer network to serve operations and business. This security system must ensure:

1. On the internal network it is impossible to change the network structure (physical, logical) unless authorized.
2. Safe for all information on the network, against all illegal access to the network.
3. Control of user access.
4. Ensuring safety of data transmitted and received via line services to the internet.
5. Sensitive data is kept confidential when there are packet theft attacks.

6.2.2 Solution

For the above security requirements, we take the following measures:

1. **Device and server level security:** Network devices such as routers, switches, ... are very important network nodes and need to be protected physically and software.
2. **OS and application level security:** Regularly back up and update patches of operating system, applications. Use error detection software for timely handling.
3. **Database-level security:** It can be said that the database is the core of the entire system and contains extremely important information (transactions, customers, ...). In design, database security takes the highest priority.

4. **Firewall / IDS:** In areas where access servers are provided, firewalls and IDS attack detectors should be arranged to prevent unauthorized access or attacks from the gateway to the network.
5. **Network-level security:** Using tools to encrypt information on the transmission line, determine integrity and authenticity of information.

6.3 System scalability

The network system built must ensure easy upgrade when needed, such as the bank increasing its staff, the number of branches and partners increasing, the more accessible servers ...
Therefore in the design we have also taken into account these issues. Currently at the headquarters we are equipped with 100 workstations and assume that it is divided equally among floors, each floor is 15 machines. Currently, each floor uses a 24-port switch (except for 1 port to connect to the switch in the network room), so when there are more staff, we do not need to redesign or buy more switches.
For the bandwidth problem, we have also taken into account the safety factor of 20% to ensure the system operates stably and when there is a need to increase bandwidth, just register to change the package with the service provider (ISP). Regarding the IP address, we use private IP for the entire internal network and only need to rent 1 public IP based on PAT technology. Moreover, the system is designing on an address range with 256 subnets (currently only using 20 subnets) so we do not worry about the IP shortage problem.
In addition, the use of network equipment from Cisco - the leader in network equipment helps us to have better technical support, more stable equipment, and especially in Cisco products that are often integrated. available new technologies, suitable for use requirements ...

6.4 Licensed and Open source Software

Licensed Software:

- OS: Microsoft Window 10 (20H1) and Microsoft Office for Work station.
- Banking software: T24 Core Banking.

Open source/free Software:

- OS: Ubuntu server 18.04 for server.
- Web browser: Google Chrome, Microsoft Edge.
- Anti virus: Window defender.
- Default multimedia software on Window 10.
- Mail: Microsoft Outlook software and Gmail on web.
- Server setting: LAMP (Linux + Apache + MySQL + PHP).

6.5 Limitations of the system

There are some limitations in our design:

1. The system is using 1 layer DMZ to save costs, but the firewall will bear a large load. If the firewall goes down, it will affect the entire system.
2. Poses many design hypotheses so it may not be close to reality.
3. Equipment cost is designed high (ensuring good quality always, but not optimal choice).
4. Not tightening network security measures and real-time anti-attack design.

6.6 Oriented development

We will outline further measures to be implemented in the future to address the above limitations.

1. Build 2 layers DMZ to reduce the load, arrange more redundant firewalls (redirect to the same class firewall).
2. Conduct a detailed actual survey of the lines, structure of the wall and floor to install the equipment.
3. Select equipment with parameters suitable for actual use in each different location.
4. Use professional security measures, build a network security room to detect and resolve situations in real time.

7 Reference

Tài liệu tham khảo

[1] Cisco devices price and detail
https://www.router-switch.com/

[2] Computer Networking: A Top-Down Approach, James F. Kurose, Keith Ross, 2000, Pearson Education