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

COMPUTER NETWORKS (CO3094)

Assignment

Computer Network Design For Building Of The Bank

Advisor: Nguyễn Mạnh Thìn
Students: Trần Việt Hoàng - 1852145
Hoàng Nhật Quang - 1852691

HO CHI MINH CITY, NOVEMBER 2021

Contents

1 Requirements analysis

1.1 Functional requirements

- Three separated local network of BB Bank: one headquarter in HCM city and two branches in Nha Trang and Da Nang.
- Headquater
  - The building consists of 7 floors, the first floor is equipped with one IT room and Cabling Central Local (for the gathering of wires and patch panels).
  - Small-scale BBB: 100 workstations, 5 servers, 12 (or maybe more with security- specific devices) networking devices.
  - Using new technologies for network infrastructure including 100/1000 Mbps wired and wireless connection.
  - The network is organized according to the VLAN structure
  - The network connects to outside by 2 leased line (for WAN connection) and 1 ADSL (for Internet access) with a load-balancing mechanism
  - Using a combination of licensed and open-source software, office applications, client-server applications, multimedia, and database.
  - Requirements for high security, robustness when problems occur, easy to upgrade the system.
- Branches
  - The building is about 2 floors high, the first floor is equipped with 1 IT room and Cabling Central Local.
  - BBB Branch: 50 workstations, 3 servers, 5 or more networking devices.

1.2 Non-functional requirements

- High security:Configured networks for higher working environments should have ad- vanced security algorithms to prevent attacks such as DDOS, SQL Ejection,... to manipulate the data or harm the servers.
- Robustness:Easy to back up data when the server crashed or when problems occurred.And provide a high available network so that the users can access the network withoutfacing any interruption.
- Scalability:The network for the bank is scalable, which means that the network can be modified by adding more devices to the network.
- Total upload and download of each Server: 500 MB/day, Workstation: 100 MB/day, Wifi-guest connection: 50 MB/day with the flows and load parameters of the system of about 80% at peak hours (9g-11g and 15g-16g).
- Growth rate must be above 20% in 5 years.

2 Requirement analysis

2.1 Analysis

- ***High security:*** Configured networks for higher working environments should have advanced security algorithms to prevent attacks such as DDOS, SQL Ejection,... to manipulate the data or harm the servers.
- ***Internet connection:*** use 2 leased lines (WAN connection) to connect 2 branches to the headquarters, and ADSL connection to connect to the Internet.

2.2 Solution

Our solution is to divide the network into small and independent clusters for easy management:

- ***Arrange separate departments:*** use VLAN structure to divide each floor as a department, connect all VLANs to the central switch at floor 1.
- ***Connection between headquarters and branches:*** through routers located in the Cabling Cantral Local Room of each location.
- ***Connection between ISP and Bank:*** connection through the Firewall located in the IT room of the headquarters
- ***Connect to Server:*** Servers are located in the DMZ partition at the headquarters, branch servers are located on a VLAN in that branch
- ***Wireless network connection:*** located at the 1st floor of branches, does not allow Trunk to prevent customers from accessing the system.

2.3 Survey Checklist

Headquarter

- Check for location of the servers, workstation, network devices and their distribution within the building.
- Check for number of the servers, workstation, network devices and connection within them and connection to the branches.

Branches

- Check for location of the servers, workstation, network devices and their distribution within the building.
- Check for number of the servers, workstation, network devices and connection within them and connection to the other branch, headquarter.

2.4 Area Definition - High Load area

- Typically, the office area where most of our workstations and devices will be located in a building. Due to the high number of workstations and their upload/download capacity, this area will have high load.
- To handle large traffic volumes, companies often place a load balancer in front of a group of servers connected to the same LAN and running the same applications (sometimes referred to as a server farm). For even greater redundancy, a company might distribute requests across the servers on multiple LANs aggregated into a WAN. One of the goals of load balancing is to maximize application reliability by eliminating single points of failure. Deploying network load balancers to load balance across servers on multiple LANs or even multiple WANs ensures that even if all servers in a LAN fail (or a network partition isolates the LAN), users don't experience failure, because traffic is redirected to accessible LANs where servers are still online.

2.5 Network Structure

The BB bank's network use the Star topology which is a type of network topology in which all the nodes are connected to the central hub or router. For example:

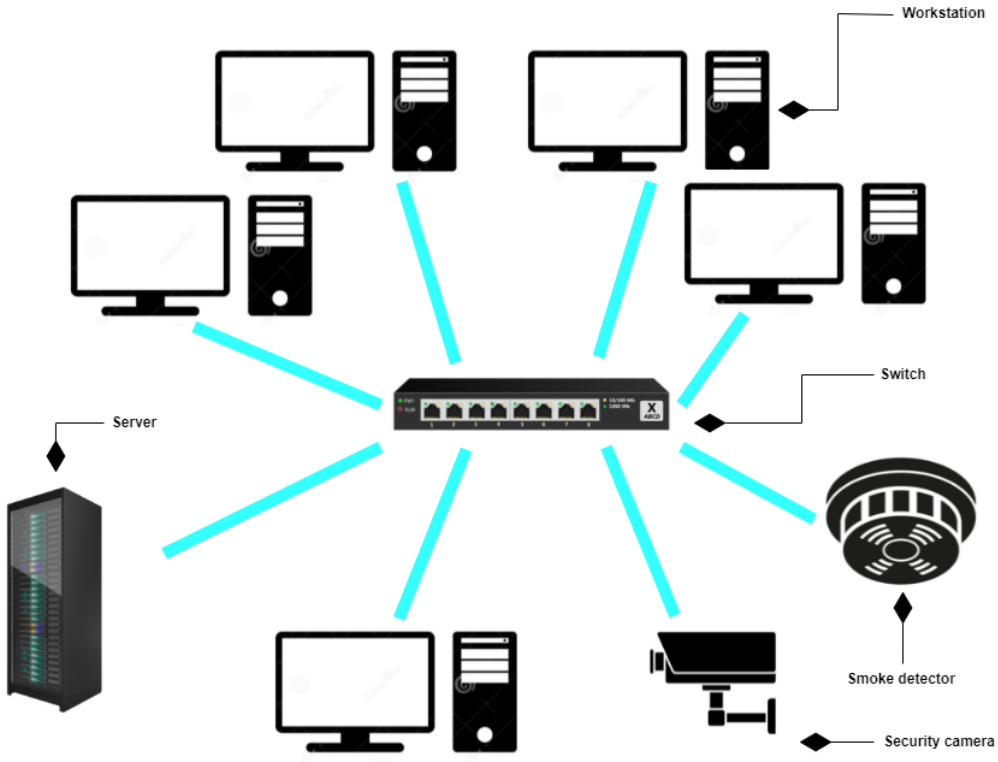

Figure 1: Star Network Topology

2.6 Wireless Coverage

- The wireless network on the first floor will be available to customers.

- We offer a wireless network that can be used by up to 100 people with standard channels from 1-2.412GHz.
- All wireless network devices use WPA2-PSK authentication to set a password for each device.
- Finally, all devices connected to the wireless network cannot be pinged by other devices outside the area. For example, devices in Nha Trang branch cannot ping devices in Da Nang branch and to headquarters. However, devices in the same branch can ping each other except for those used by Clients on tier 1.
- For the devices on the first floor that are allowed to be used by customers, we use their own VLAN protocol but do not allow them to access the local PCs and servers.

3 Network paper design

3.1 Technologies usage

3.1.1 VLAN (virtual local area network)

- ***A LAN*** (virtual local area network) is a subnetwork which can group to- gether collections of devices on separate physical local area networks. A local area network (LAN) is a collection of computers and devices that share a commu- nications line or wireless link with a server located within the same geographic area.
- ***Types of VLANs***
  - The building consists of 7 floors, the first floor is equipped with one IT room and Cabling Central Local (for the gathering of wires and patch panels).
  - Small-scale BBB: 100 workstations, 5 servers, 12 (or maybe more with security- specific devices) networking devices.
  - Using new technologies for network infrastructure including 100/1000 Mbps wired and wireless connection.
- ***Advantages and Disadvantages of VLAN***
  - **Advantages**
    - VLAN include reduced broadcast traffic, security, ease of administration and broadcast domain confinement.
  - **Disadvantages**
    - A packet can leak from one VLAN to other.
    - An injected packet may lead to a cyber-attack.
    - Threat in a single system may spread a virus through a whole logical network.
    - A VLAN cannot forward network traffic to other VLANs.

3.1.2 VLAN (virtual local area network)

- ***LAN Trunking Protocol (VTP)*** is a Cisco proprietary protocol that propagates virtual local area network (VLAN) definitions throughout the whole local area network.

3.1.3 RIP (Routing Information Protocol)

- ***Routing Information Protocol (RIP)*** is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network.
- ***RIP versions***
  - There are three versions of routing information protocol – RIP Version1, RIP Version2, and RIPng.
- ***Features of RIP***
  - Network updates are exchanged on a regular basis.
  - Routing information (updates) are always broadcast.
  - Full routing tables are sent in updates.
  - Routers always trust routing information received from neighbor routers.

3.1.4 VPN (Virtual private network)

- ***A virtual private network, or VPN,*** is an encrypted link between a device and a network via the Internet. The encrypted connection aids in the secure transmission of sensitive data.
- ***Types of VPNs***
  - **Remote access:** a remote access VPN establishes a secure connection between a device and the corporate network. Endpoints are computing devices such as laptops, tablets, and smartphones.
  - **Site-to-site:** over the Internet, a site-to-site VPN connects the corporate office to branch offices. When distance makes direct network connections between these offices impractical, site-to-site VPNs are employed. To create and maintain a connection, specialized equipment is necessary.
- ***Advantages and Disadvantages***
  - **Advantages**
    - A VPN hides your online identity.
    - VPNs help you bypass Geo-Blocks.
    - VPN services secure your online connections.
    - VPNs make online gaming better.
  - **Disadvantages**
    - VPNs can sometimes slow down your online speeds.
    - Using the wrong VPN can put your privacy in danger.
    - VPNs of high quality come at a price.
    - VPNs aren't supported by all devices out of the box.

3.1.5 DHCP, DNS Server

- **DHCP (Dynamic Host Configuration Protocol):** Dynamic Host Configuration Protocol DHCP is a network protocol that helps us to assign an IP address and related IP information to the devices such as servers, desktops, or mobile equipment in the network.
- **DNS (Domain Name System):** The Domain Name System (DNS) converts a website's name, such as FS.COM, to its IP address and vice versa, allowing users to access to websites by matching human-readable domain names with the server's unique ID.

3.1.6 Network Address Translation (NAT)

NAT is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on **a router or firewall.**
Advantages

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantages

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec. evolves.
- Also, the router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

3.2 Equipment usage

We used a variety of Cisco network devices. We'll go through each gadget in detail in this section.

3.2.1 Router

Theoretical basis: A router is a network or subnetwork device that connects two or more packet-switched networks or subnetworks. It has two main functions: it manages traffic between these networks by forwarding data packets to their intended IP addresses, and it allows several devices to share the same Internet Routers use packets to guide and steer network data, which can include files, communications, and simple transfers like web interactions. According to the docu- mentation from Cisco, there are 5 main types of routers:

- ***Core router:*** Service providers (such as AT&T, Verizon, and Vodafone) and cloud providers are the most common users of core routers (i.e. Google, Amazon, Microsoft). They provide the highest possible bandwidth for connecting additional routers or switches. Core routers are not necessary for most small organizations. Core routers, on the other hand, may be used as part of the net- work architecture of very big organizations with numerous employees working in various buildings or locations.
- ***Edge router:*** An edge router, often known as a gateway router or simply "gateway," is a network's outermost point of access to other networks, such as the Internet.
- ***Distribution router:*** A distribution router, also known as an interior router, receives data over a wired connection from the edge router (or gateway) and transmits it to end users, usually via Wi-Fi, though it may also have physical (Ethernet) connections for connecting users or additional routers.
- ***Wireless router:*** Residential gateways, often known as wireless routers, in- tegrate the operations of edge and distribution routers. For home networks and Internet access, these are common routers.
- ***Virtual router:*** Virtual routers are software components that enable some router services to be virtualized and supplied as a service in the cloud. Large businesses with sophisticated network requirements will benefit from these routers. They provide flexibility, scalability, and a lower barrier to entry. Another advantage of virtual routers is that local network hardware management is simplified.

In this assignment, we use router Router-PT:

- ***Port:***
  - 2 Serial Ports
  - 2 Fast Ethernet Ports
- ***Modules:***
  - **PT-ROUTER-NM-1FGE:** the single-port Cisco Gigabit Ethernet Net- work Module provides Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.
  - **PT-ROUTER-NM-1S:** provides a single port serial connection to re- mote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.
  - **The PT-ROUTER-NM-1CFE:** provides one Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.
- ***Quantity:*** 3 (one for headquarter and the others for Nha Trang and Da Nang branch each).
- ***Description:*** We use Fast Ethernet ports to connect to the switches and routers in the same area. For connection to other branches over the WAN network, we use Serial port.

3.2.2 Wireless Router

Theoretical basis: A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.

- ***Model:*** WRT300N
- ***Bandwidth:*** 2.4 GHz
- ***Integrated Switch:*** 4-port switch
- ***Features:*** DHCP support, DMZ port, MAC address filtering.
- ***Quantity:*** 3 (one for headquarter and the others for Nha Trang and Da Nang branch each in the 1st Floor).
- ***Description:*** Wifi router provides wireless connection to wireless devices with WEP authentication. This serves internet service to the guest of each building as well as the staff.

3.2.3 Firewall

Theoretical basis: A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Types of firewalls

- ***Next-generation firewalls (NGFW):*** combine traditional firewall technol- ogy with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Most notably, it includes deep packet inspection (DPI). While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious data.
- ***Proxy firewalls:*** filter network traffic at the application level. Unlike basic firewalls, the proxy acts an intermediary between two end systems. The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked.
- ***Network address translation (NAT) firewalls:*** allow multiple devices with independent network addresses to connect to the internet using a single IP ad- dress, keeping individual IP addresses hidden. As a result, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks. NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.
- ***Stateful multilayer inspection (SMLI) firewalls:*** filter packets at the net- work, transport, and application layers, comparing them against known trusted packets. Like NGFW firewalls, SMLI also examine the entire packet and only allow them to pass if they pass each layer individually. These firewalls examine packets to determine the state of the communication (thus the name) to ensure all initiated communication is only taking place with trusted sources.

- ***Model:*** ASA 5506X
- ***Port:*** 8 Gigabit Ethernet, 1 RJ-45 and Mini USB console
- ***Quantity:*** 1
- ***Description:*** In this assignment, we use firewall to filter the packets from the internet service provider as well as controlling the input and output of the flow.

3.2.4 Cable

In this system, we use three types of cable to connect our network: Copper straight through, Copper crossover, leased line.

- ***Copper straight through:*** A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. Both pins on both ends match each other. This type of cable is usually used for connecting different types of devices.
- ***Copper crossover cable:*** An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. The crossover cable pinout crosses the pair at the transmit pins on each device to the receive pins on the opposite device.
- ***Serial cable:*** the serial cables normally used between a router and an external CSU/DSU are called data terminal equipment(DTE) cables, plus a similar but slightly different matching data communications equipment(DCE) cable.

3.3 Schematic physical setup

- Our bank has a headquarters in Ho Chi Minh City and two branches in Nha Trang (NT) and Da Nang (DN).
- Using a WAN link, we were able to connect the branches to the headquarters.
- These areas transfer information and data by means of WAN links. From the headquarter in Ho Chi Minh city, we use 2 leased line to communicate with other branches and one ADSL to the Internet service provider.

ID	Floor	Room	Device inside	
			Device	amounts
1	1	IT room	Server	5
			Switch	2
			Camera	1
			Firewall	1
			Smoke Detector	1
		Cabling Central Local	Router	1
			Switch	1
			Camera	1
			Smoke Detector	1
2	2	R201&202	Workstation	24
			Smoke Detection	1
			Switch	1
			Camera	1
3	3	R301&302	Workstation	24
			Smoke Detection	1
			Switch	1
			Camera	1
3	4	R401&402	Workstation	24
			Smoke Detection	1
			Switch	1
			Camera	1
5	5-6	R501-601	Workstation	10 x 2
			Smoke Detection	1 x 2
			Switch	1 x 2
			Camera	1 x 2
7	7	Room 701	Workstation	8
			Smoke Detection	1
			Switch	1
			Camera	1

3.4 WAN connection diagram

3.4.1 Wide Area Networks

A wide area networks are a form of telecommunication networks that can connect devices from multiple locations and across the globe. WANs are the largest and most expansive forms of computer networks available to date.

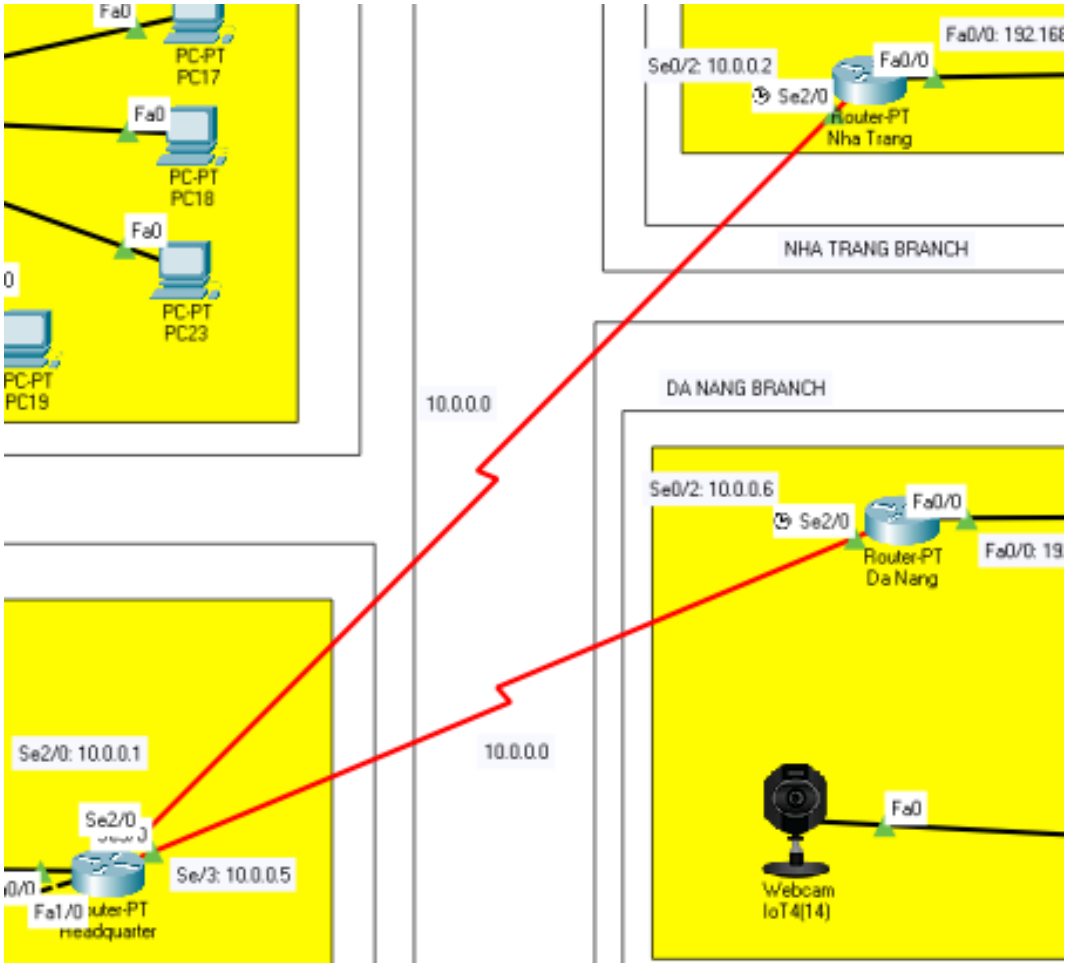

Figure 2: WAN connection diagram (using OSPF protocol)

Location	Department	IP	Default Gateway	VLAN
HCM City	Floor 1	192.168.10.0/24	192.168.10.1/24	10
	Floor 2	192.168.20.0/24	192.168.20.1/24	20
	Floor 3	192.168.30.0/24	192.168.30.1/24	30
	Floor 4	192.168.40.0/24	192.168.40.1/24	40
	Floor 5	192.168.50.0/24	192.168.50.1/24	50
	Floor 6	192.168.60.0/24	192.168.60.1/24	60
	Floor 7	192.168.70.0/24	192.168.70.1/24	70
	HQ Gateway router Se2/0	10.0.0.1	N.A	N.A
	HQ Gateway router Se3/1	10.0.0.5	N.A	N.A
	DMZ server	17.16.200.3-7	17.16.200.1	N.A
NT City	Floor 1	192.168.80.0/24	192.168.80.1/24	80
	Floor 2	192.168.90.0/24	192.168.90.1/24	90
	NT Gateway router Se2/0	10.0.0.2	N.A	N.A
DN City	Floor 1	192.168.100.0/24	192.168.100.1/24	100
	Floor 2	192.168.110.0/24	192.168.110.1/24	110
	HQ Gateway router Se2/0	10.0.0.6	N.A	N.A
ISP	DNS	8.8.8.0/24	8.8.8.1/24	8
	Google	10.10.10.0/24	10.10.10.1/24	10
	ISP Gateway router Fa0/0	20.110.24.1	N.A	N.A

- When the local network wants to connect to the Internet, they will have to go through the Firewall (IP port is 20.110.24.2), we use NAT protocol to convert the address to the network provider's address (IP port is 20.110 .24.1)
- For the internal network (local) we set the security level to 100, for the network in the DMZ zone it is 50 and outside the Internet it is 0 to keep the system safe. Allows packets to be returned locally, but does not allow outside access.

3.4.2 WAN connection diagram

- ***Pros:***
  - Data can be shared easily from one device to another and so on connected in a loop
  - WANs cover far distances, for the same business operating at different geographies to connect on a single forum.
  - Using Wan, users can access application software and other resources over the Internet.
- ***Cons:***
  - WANs are subject to more security issues and can face more cyber-attacks than LAN.
  - Setting up a WAN to automate your businesses across the globe is highly costly.
  - Strong firewalls and high security are needed to ensure safe transfer of Information and for the protection of data.

3.5 Network Calculation

The specification for the upload and download capacity for each type of networking devices is as follow:

- The total upload and download capacity forserver is 500 MB/day.
- The total upload and download capacity for workstation is 100 MB/day.
- WiFi-connected laptop for customers to access about 50 MB/day.

Note that we also take into account the fact that the Bank can grow up to 20% in the next 5 years. Also, The flow of the system reaches its peak with the duration of 3 hours (from 9h to 11h and 15h to 16h)

3.5.1 Network Throughput

For the headquarter:

- There are 5 servers:
  Average data usage: $500 * 5 = 2500(MB/day)$
- There are 100 Workstations:
  Average data usage: $100 * 100 = 10000(MB/day)$
- Access points for 100 users:
  Average data usage: $100 * 50 = 5000(MB/day)$
- Total Average data usage: $2500 + 10000 + 5000 = 17500(MB/day)$
- Total Average data usage during peak hours (80 % in 3h):
  Throughput: $(17500 * 80\%)/(3 * 3600) = 1.2963(MB/s) = 10.3704(Mbps)$

3.5.2 Network Bandwidth

All the inner buildings are connected through Ethernet ports with 100/1000 MBps. With this speed, all connection inside the building will be handled perfectly fine.

For outside connection: since all devices are connected outside through the gateway router, the WAN links from this router will be their bottleneck. Our buildings have 2 leased lines and 1 ADSL connection to the outside. Since 2 leased lines are used for connections to the 2 branches. it leaves only the ADSL line for internet connection.

Assuming the serial DTE connection to other branches is 1544 Kb per second. Therefore the total bandwidth through the branch connections is:

$$1544/8 * 3600 * 24 = 16675200(KB/day) = 16284.375(MB/day)$$

For Internet connection, assuming ADSL2+M (ITU G.992.5 Annex M) with 24Mbit/s downstream and 3.3Mbit/s upstream. The total bandwidth for both download and upload is:

$$(24 + 3.3)/8 = 3.4124(MB/s) = 294840(MB/day)$$

We can see that the ADSL link is more than enough to handle the bank Internet needs. However the serial links might have trouble keeping up with the inter-branch network demands.

3.5.3 Network Bandwidth

Implementation of an integrated safety management system can reduce and control injury rates as well as related expenses. Following are nine key parameters of a safety management system.

- ***A Written Safety and Health Policy:*** signed by the top company official that expresses the employer's values and commitment to workplace safety and health.
- ***Visible Senior Management Leadership:*** that promotes the belief that the management of safety is an organizational value.
- ***Employee Involvement and Recognition:*** that affords employees opportunities to participate in the safety management process.
- ***Safety Communication:*** keep all employees informed and to solicit feedback and suggestions.
- ***Orientation and Training:*** for all employees.
- ***Documented Safe Work Practices:*** so that employees have a clear understanding of how to safely accomplish their job requirements.
- ***Safety Program Coordination:*** assigning an individual the role of coordinating safety efforts for the company.
- ***Early Return to Work strategies:*** to help injured or ill workers return to work as soon as possible.
- ***Internal Program Verification:*** to assess the success of company safety efforts, including audits, surveys, and record analysis.

4 Network map using packet tracer

In this design of BB Bank's banking network, we design the following structure: Headquarters and branches are connected to each other via serial cables connected between the routers of each building. There are a total of 3 routers, the headquarters router plays a central role. In addition, to enhance the security of the bank, we use firewalls and ACLs to prevent access to the bank. The headquarters servers are located in the DMZ partition to limit access from outside the Internet as well as internally to ensure safety. The firewall acts as a bridge between the bank, the server and the ISP and it is located on the first floor in the IT room of the headquarters.
For the headquarters:

7 floors are divided from the central switch located on the 1st floor. In addition, 100 workstations are equally divided on each floor except the 1st floor. The 2nd to 4th floors each floor 24 workstations are divided equally among 2 rooms. Floors 5 to 7 each floor 12 workstations are located in one room. At each floor, workstations are connected to a switch and this switch is connected to the central switch on layer 1:

- ***VLAN10:*** 1st floor of headquarters
- ***VLAN20:*** 2nd floor of headquarters
- ***VLAN30:*** 3rd floor of headquarters

- ***VLAN40:*** 4th floor of headquarters
- ***VLAN50:*** 5th floor of the headquarters
- ***VLAN60:*** 6th floor of headquarters
- ***VLAN70:*** 7th floor of the headquarters

For branches:

Two floors are divided from the central switch located on the ground floor and the division structure is similar to the headquarters. However, on the 2nd floor, there are a total of 42 workstations divided equally among 3 rooms and the remaining machines are located in the IT room of the 1st floor.

- ***VLAN80:*** 1st floor of Nha Trang branch
- ***VLAN90:*** 2nd floor of Nha Trang branch
- ***VLAN100:*** 1st floor of Da Nang branch
- ***VLAN110:*** 2nd floor of Da Nang branch

In addition, on each floor, there are additional security devices such as Camera and Smoke Detector connected to the switches on that floor. It allows staff to be able to access and manage incidents if they occur.

Split VLANs between layers to ensure that each department is isolated from each other but can still access each other's data. When the problem occurs on one VLAN, the other VLANs will not be affected. The use of VLANs in the system also allows the bank to expand further in the next 5 years.

The system also provides wireless network access for customers in branches. The wireless IP address is a subnet port of the router, and the switch it connects to cannot be trunked on that connection to ensure that customers cannot access the corporate LAN.

In addition, each workstation can also connect to the Internet securely through the firewall we have designed.

As for the Internet connection, we use a DSL service that is connected from the firewall before connecting to the Cloud and connecting to the ISP.

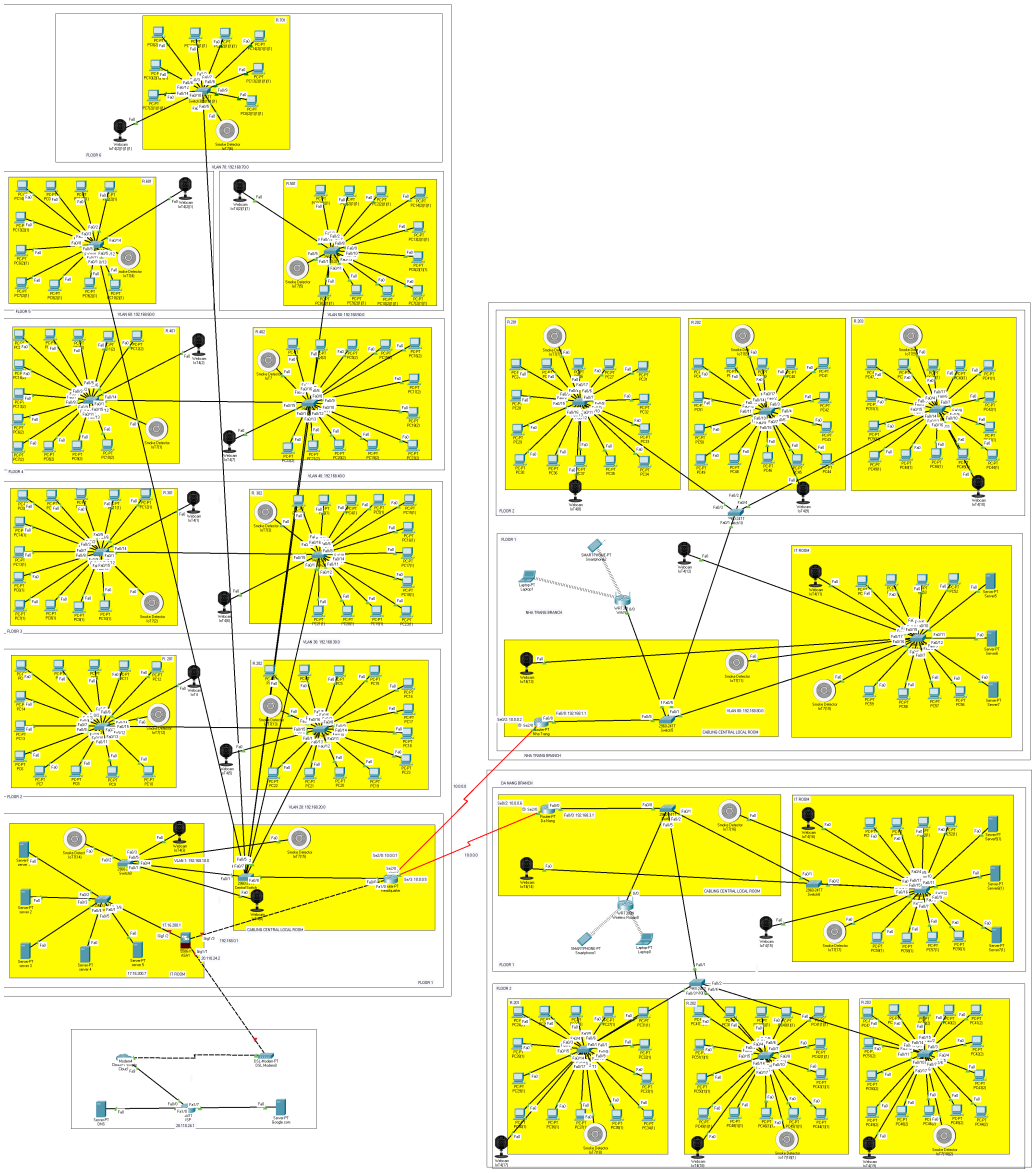

Figure 3: BB Bank Network Map Design

5 Testing and results

5.1 Test with Ping

Connect between PCs in the same VLAN

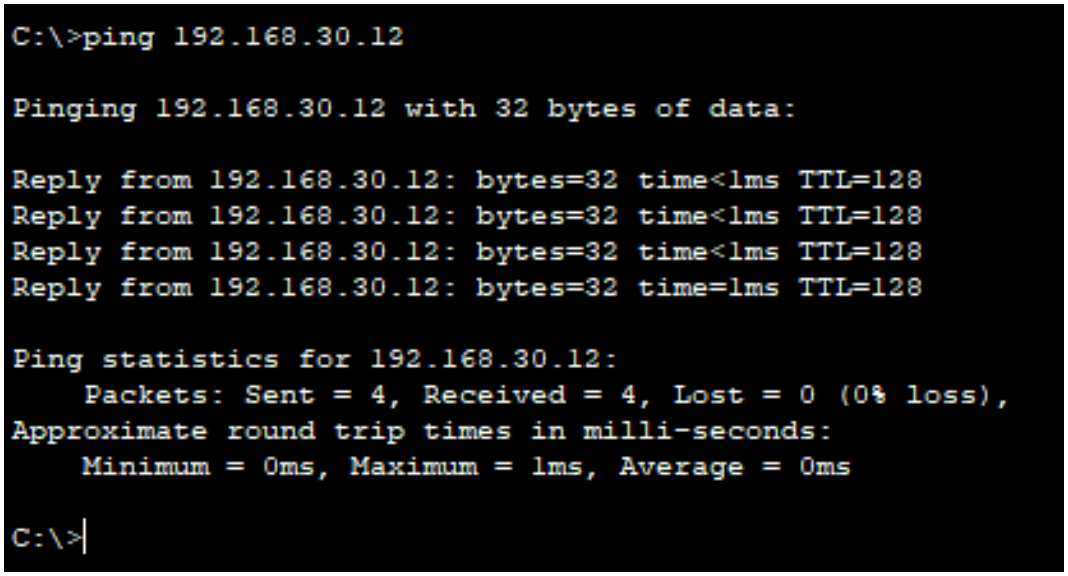

Figure 4: Connect between PCs in one floor in Headquater

Connect PCs between VLANs

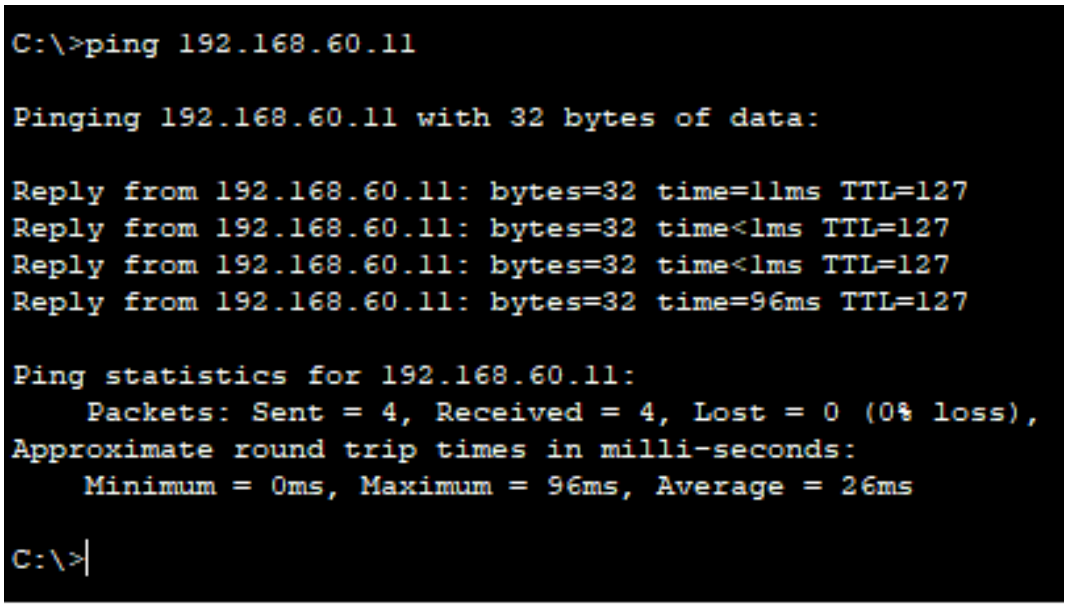

Figure 5: Connect between PCs in 4th floor and 6th floor in Headquater

Connect PCs between Headquarter and branches

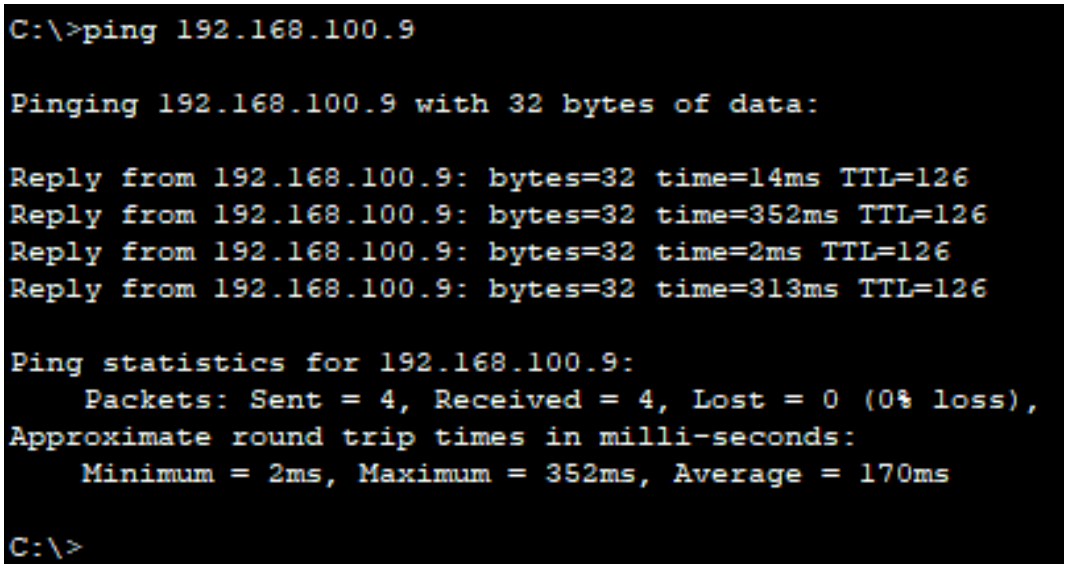

Figure 6: Connect between PCs from 3rd floor in Headquater to 1st floor in Da Nang branch

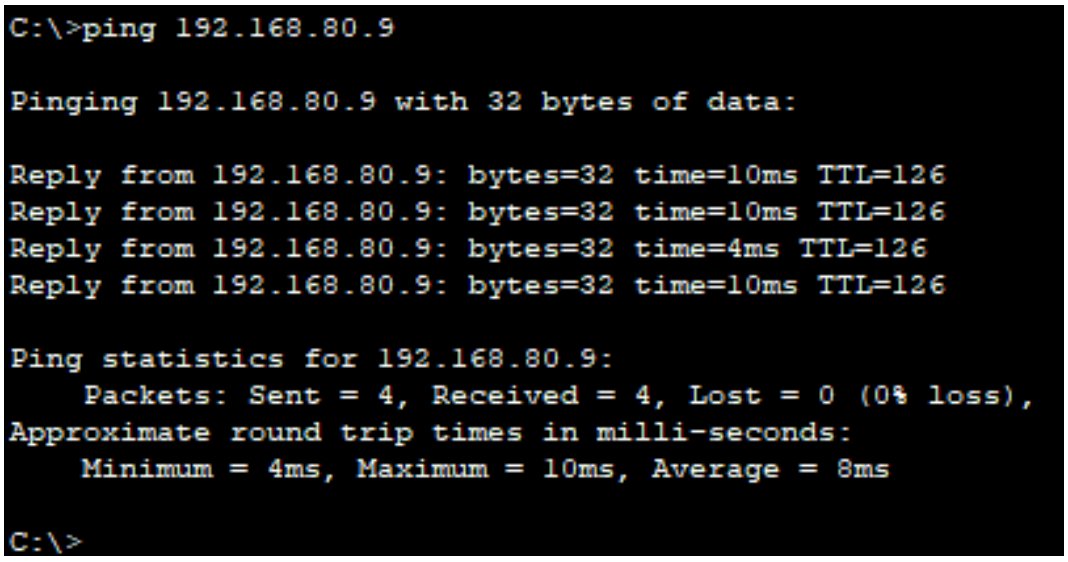

Figure 7: Connect between PCs from 3rd floor in Headquater to 1st floor in Nha Trang branch

Connect to servers in the DMZ

```
Packet Tracer PC Command Line 1.0
C:\>ping 17.16.200.3

Pinging 17.16.200.3 with 32 bytes of data:

Request timed out.
Reply from 17.16.200.3: bytes=32 time=47ms TTL=126
Reply from 17.16.200.3: bytes=32 time=33ms TTL=126
Reply from 17.16.200.3: bytes=32 time<1ms TTL=126

Ping statistics for 17.16.200.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 47ms, Average = 26ms
```

Hình 1: Connect from PC in Headquater to servers in DMZ

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=33ms TTL=254
Reply from 192.168.0.2: bytes=32 time<1ms TTL=254
Reply from 192.168.0.2: bytes=32 time<1ms TTL=254
Reply from 192.168.0.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 33ms, Average = 8ms
```

Hình 2: Connect from servers in DMZ to PCs in Headquater

Connect to the Internet to a Web server

```
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=118ms TTL=125
Reply from 10.10.10.10: bytes=32 time=39ms TTL=125
Reply from 10.10.10.10: bytes=32 time=58ms TTL=125
Reply from 10.10.10.10: bytes=32 time=76ms TTL=125

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 118ms, Average = 72ms
```

Hình 3: Connect from PCs in Headquarter to Internet

5.2 Test the system with Tracert

```
Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.110.15

Tracing route to 192.168.110.15 over a maximum of 30 hops:

  1    7 ms      0 ms      12 ms     192.168.20.1
  2    8 ms      1 ms      1 ms      10.0.0.6
  3    *         1 ms      7 ms      192.168.110.15

Trace complete.

C:\>
```

Figure 8: Tracert from PCs in Headquarter to PCs in Da Nang branch

```
C:\>tracert 192.168.80.10

Tracing route to 192.168.80.10 over a maximum of 30 hops:

  1    5 ms      1 ms      0 ms      192.168.20.1
  2    33 ms     1 ms      1 ms      10.0.0.2
  3    *         1 ms      9 ms      192.168.80.10

Trace complete.

C:\>
```

Figure 8: Tracert from PCs in Headquarter to PCs in Nha Trang branch

6 Conclusion

6.1 Re-evaluate the designed network system

Reliability

- Our system is very reliable, message packets sent from devices are always installed according to the router to know where the traffic is going.
- The system is clearly divided between headquarters and branches based on VLAN structure and OSPF protocol, without interference between branches and branches.

Easy to upgrade

- Thanks to the architecture designed according to the structure of each VLAN for each floor, we can expand more floors if we want, just connect more switches to the central switch on floor 1.
- In addition, we can expand the bank to add more branches, just connect the router of that branch to the router of the headquarters, we can easily access the data system of the bank.
- For a floor, if we want more workstations, we can connect more to the switch of that floor. In case the number of ports of that switch is exceeded, we can add a switch to the switch of that floor to use more workstations.
- Because of the above reasons, our system can guarantee a growth rate of about 20% every 5 years. It is possible to increase the number of workstations, security devices as well as servers,...

Diverse support software

For software, our system supports all office applications. In addition, the system also provides wireless network for customers to use to access.

Safety and security of data

- Thanks to the Firewall set up at the headquarters, our system can control which packets are accessed in the system.

- Using NAT table we can convert private IP address to public IP and vice versa. This can help the system to hide the IP inside the LAN as well as save the number of IP addresses to use.
- In addition, application ACLs also help create a basic layer of protection for the system, ensuring who is allowed to access the server as well as the workstations.
- The creation of the DMZ makes the system able to secure data based on the level of security provided by the Firewall, preventing hackers from being able to access the bank's data, which is considered very important.

6.2 The remaining problems

Although our system fully meets the requirements set forth, there are still certain limitations that have not yet been achieved.

- First, the system can only connect to the Internet from the headquarters, but at the branches, it is still not able to connect.
- Second, haven't set up a VPN for the bank yet.

6.3 Development orientation in the future

In the future, it is expected that the system will be updated with outstanding issues, and add some new features.

- Add web server for the system.
- Decentralize data access based on the employee's position hierarchy (currently only divided by department).
- Allow customers to access some banking services without affecting system data
- Speed up Internet access.
- Applying IoT into the system makes it easier for employees to work.
- Remote networking for employees who can work from home.