

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



Computer Networks (Lab) (CO3094)

ASSIGNMENT 2

Computer Network Design For Building Of The Bank

Lecturer: Nguyễn Mạnh Thìn

Students:	Nguyễn Trúc Phương	1952402
	Nguyễn Võ Hoàng Thi	1952996
	Trần Hưng Cường	1952606

HO CHI MINH CITY, 2021



Contents

1	Find out suitable network structures for buildings	3
1.1	Requirements analysis	3
1.1.1	Functional requirements	3
1.1.2	Non-functional requirements	3
1.1.3	The flows and load parameters of the system	4
1.2	Survey checklist	4
1.2.1	Planning	4
1.2.2	Network hardware requirements	4
1.2.3	Network design	5
1.2.4	Security, back-up and power	5
1.2.5	Support services	5
1.2.6	Costs and maintenance	6
1.3	High Network Load Area	6
1.3.1	What is High Load	6
1.3.2	Network Load Balancing - The solution for High Load Problem	6
1.3.3	Define areas with high load (network load) in BBB Computer Network	7
1.4	Computer Network Design	7
1.4.1	Network Structure	7
1.4.1.a	In headquarter	7
1.4.1.b	In branches	8
1.4.2	Computer Network Design	8
1.4.3	Specific arrangement	10
1.4.3.a	Headquarter	10
1.4.3.b	Branch	10
1.4.4	Network hierarchy	10
1.5	Network security of the system	10
1.6	Wireless coverage	11
1.7	Development prediction	12
2	List of minimum equipment, IP diagram and wiring diagram (cabling)	12
2.1	List of recommended equipment	12
2.1.1	Server	12
2.1.2	Router	12
2.1.3	Switch	13
2.1.4	Core Switch	14
2.1.5	Firewall	15
2.1.6	Access Point	15
2.1.7	Cable	16
2.1.8	End Devices	17
2.1.9	Checkpoint	17
2.2	Schematic physical setup	17
2.3	WAN connection diagram	18
2.4	IP address table	20



3	Calculate throughput, bandwidth, and safety parameters for computer networks	21
3.1	In headquarter	21
3.1.1	Server	21
3.1.2	Workstation	21
3.1.3	User	21
3.1.4	Total	22
3.2	In branch	22
3.2.1	Server	22
3.2.2	Workstation	22
3.2.3	User	22
3.2.4	Total	23
4	Design the network map using Packet Tracer or GNS3 simulation software	23
5	Test the system with popular tools such as ping, traceroute, ... on the simulated system.	24
5.1	Connect between PCs in the same VLAN	25
5.2	Connect PCs between VLANs	25
5.3	Connect PCs between Headquarters and branches	25
5.4	No connections from Customers devices to PCs on the LAN	26
6	Re-evaluate the designed network system through the following features: reliability, easy to upgrade, diverse support software, safety, the security of data, ...	26
6.1	Reliability	26
6.2	Easy to upgrade	27
6.3	Safety	27
6.4	Diversity in Software support	27
6.5	Problems	28
6.6	Development Orientation	28

1 Find out suitable network structures for buildings

1.1 Requirements analysis

1.1.1 Funtional requirements

- **Three** separated local networks a BBB (BB Bank):
 - IT usage at a Headquarter:
 - * A 7-floor building, the first floor is equipped with one IT room and Cabling Central Local.
 - * Small-scale BBB: 100 workstations, 5 servers, 12 (or maybe more with security specific devices) networking devices.
 - IT usage at 2 Branches (designed similarly to the headquarters but with a smaller scale):
 - * A 2-floor building, the first floor is equipped with 1 IT room and Cabling Central Local.
 - * 50 workstations, 3 servers, 5 or more networking devices.
- Connections between the headquarters and the branches: by 2 leased line (for WAN connection) and 1 ADSL (for Internet access) with a load-balancing mechanism.
- 100/1000 Mbps wired/wireless connection for network infrastructure.
- The network is organized according to the VLAN structure

1.1.2 Non-funtional requirements

- **High security:** Networks configured for work environments need advanced security algorithms to protect client data and information, keep shared data secure, avoid server harm and ensure reliable access and network performance as well as protection from cyber threats. **Firewall** is the network security protections that we intend to use in this project.
- **Robustness:** The ability to withstand failures and perturbations. Network robustness can help to evaluate the resilience of infrastructure networks, ensure that the network is highly available so that users can access it without interruption.
- **Growth potential:** The network for the bank is scalable which means that the network can be modified by adding more devices to the network. BB Bank's Computer Network is estimated for a growth rate of **20%** in 5 years (in terms of the number of users, network load, branch extensions,...)
- **Flexibility:** The network is capable of using a combination of licensed and open source software, office applications, client-server applications, multimedia, and databases.
- **Performance:** The speed of a web resource affects user satisfaction with the service, as well as ranking in search results (which is reflected in traffic).



1.1.3 The flows and load parameters of the system

The flows and load parameters of the system (about 80% at peak hours 9h-11h and 15h-16h) can be shared for Head Office and Branch as follows:

- Servers 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 transactions, ... The total upload and download capacity is about **100 MB/day**.
- WiFi connected laptop for customers to access about **50 MB/day**.
- VPN configuration for site to site and for a teleworker to connect to LAN.

1.2 Survey checklist

1.2.1 Planning

- ☐ How many people will use the network?
- ☐ How many users are local or on-site?
- ☐ How many users are remote or off-site and will require access to the network?
- ☐ How many on-site computers will be connected to the network?
- ☐ How many on-site devices (computers, servers, scanners, printers, etc) will require a network card?
- ☐ How do you intend remote users to access the network?
- ☐ Which server based applications (e.g. databases, email) do you plan to run on the network?
What are the minimum hardware requirements of these server based applications?
- ☐ What are the specifications of the servers you intend to install on the network?
- ☐ Have you purchased sufficient licenses to run all the software on servers and client machines?
- ☐ Check for available network devices.
- ☐ Location of servers, workstations, and network devices and their distribution to the building's network.

1.2.2 Network hardware requirements

- ☐ What other devices will your network support (e.g. back-up devices, Uninterruptible Power Supplies, Network printers, etc.)?
- ☐ Do you have enough network points for these network devices?
- ☐ Do the hubs or switches have enough ports for the number of connections you will require?
And is there room for growth?



1.2.3 Network design

- ☐ What network topology will you use
- ☐ Do all workstations have the correct Network interface cards (NICs) to support this technology?
- ☐ Which network operating system will you use?
- ☐ Which type of cabling will you use (e.g. CAT 5, fibre optic) or will a wireless network be suitable?
- ☐ Where will network cables be located?
- ☐ Are there any building or leasing regulations that may affect cable placement?
- ☐ Where will you locate the following devices, servers, hubs or switches, printers, firewalls and routers, modems etc.?
- ☐ Ensure network connectivity and stability.
- ☐ Check for impact of the surrounding environment.

1.2.4 Security, back-up and power

- ☐ What security measures will you be putting in place? Virus protection, user passwords, firewalls, data encryption etc.
- ☐ Do you need to physically secure your server?
- ☐ How will you back up data on your network?
- ☐ What is the capacity of your back up solution?
- ☐ Is it large enough to support all the data on your servers and network devices?
- ☐ Does your back up solution have the capacity to grow as your data grows?
- ☐ How frequently will files be backed up and how long will you keep backed up files?
- ☐ Where will you store backed up tapes?
- ☐ What devices will require an uninterruptible power supply?
- ☐ Is there sufficient ventilation around your servers?

1.2.5 Support services

Do you have resources allocated for the following areas?

- ☐ Network installation
- ☐ Cable installation
- ☐ Network technical support
- ☐ Network management

- ☐ Network security
- ☐ Network maintenance
- ☐ Training

1.2.6 Costs and maintenance

- ☐ Estimated installation cost.
- ☐ Does the budget satisfy all the requirements and plan?
- ☐ Anticipate maintenance, upgrade and security costs cost per year

1.3 High Network Load Area

1.3.1 What is High Load

High load is when one server is not enough for customer service, the IT-system ceases to cope with the current load. A key source of problems in high load infrastructure is the volume of data, complexity and rate of change.

1.3.2 Network Load Balancing - The solution for High Load Problem

- What is Network Load Balancing?

Load balancing is a method of taking multiple requests or processes and distributing them across multiple devices depending on how busy each device is.

Load balancing techniques distribute methodically and efficiently application or network traffic across multiple servers. Each load balancer sits between the client devices and the back-end server, receiving and then delivering requests to any available servers that are capable of responding to them.

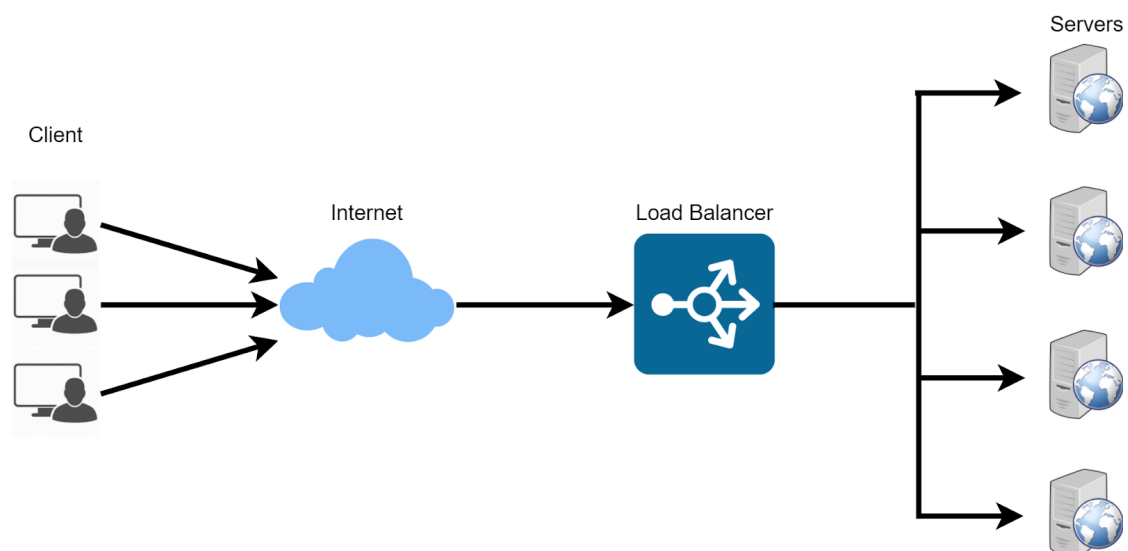


Fig. 1: Load balancing distributes traffic to servers

1.3.3 Define areas with high load (network load) in BBB Computer Network

- We need to use load balancing at **Headquarters**, where the web server and other important servers are located because the traffic to the web server can be overloaded, or experience other problems.
- The solution here is to install a Cisco RV082 load balancer, or install load balancing software that connects directly to important servers to ensure that the banking system's particular servers are not overloaded.
- Usually, the first floor is where transactions with customers are made, leading to an unexpected amount of traffics. It also includes IT room as required. Therefore, we should pay attention to load balancing in this area.
- The whole building should have a load balancer right after the WAN connections(in the bottleneck) to balance load between the workstations and servers. Ensuring that they will all get at least part of the bandwidth (although not necessarily evenly distributed).

1.4 Computer Network Design

1.4.1 Network Structure

1.4.1.a In headquarter

Headquarter of BBB includes 100 workstations, 5 servers, 12 (or maybe more with security specific devices) networking devices arranged in a 7-floor building.

- The 1st floor: IT room and transactions room.
 - IT room contains 5 servers of the headquarters and Router, Switch, ... and 6 workstations for IT staff.
 - There are 20 workstations for transactions.
- The 2nd floor: contains 13 workstations for HR and Sales Department
- The 3rd floor contains 13 workstations for Investment and Financial institution Department
- The 4th floor contains 13 workstations for Financial accounting Department
- The 5th floor contains 13 workstations for Administration and Marketing Department.
- The 6th floor contains 8 workstations for Conference room and meeting rooms.
- The 7th floor: Director's Department and legal department
 - Director's Department contains 4 workstations for directors and 8 workstations for secretaries.
 - There are 2 workstations for legal department.

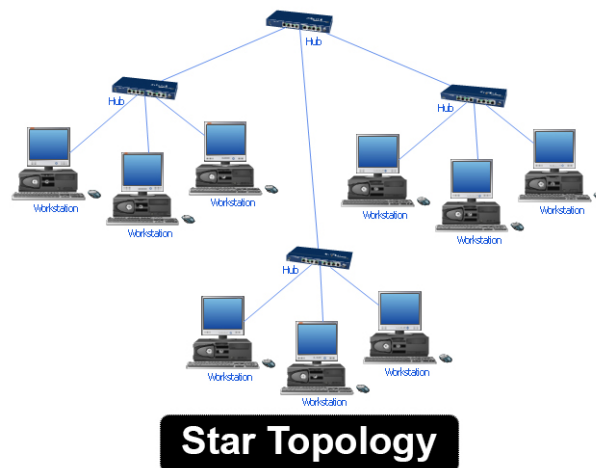
1.4.1.b In branches

BBB Branches include 50 workstations, 3 servers, 5 or more networking devices:

- The 1st floor: IT room and Transaction room
 - IT room contains 3 servers and routers, switches,... and 4 workstations for IT staff
 - 12 workstations for transaction
- The 2nd floor: Investment, business, administration, human resources, accounting department contains 32 workstations for employees and 2 workstations for directors

1.4.2 Computer Network Design

- Network design according to the client-server model.
- The system is arranged in a **star topology**, including 100/1000 Mbps switches.



- Many workstations connect to a single switch. Workstations are indirectly connected through the switch.
 - If the switch has an interrupt, the computers will not be able to connect to each other.
 - When using this topology, it requires accept more expensive wiring due to long-distance. We accept this shortcoming.
 - Using a star structure makes it easier to expand more workstations in each building and floor in the future because we only need to connect new machines to the switch. And we can also add more switch to the router if we don't have enough ports in the switch.
 - Star network is very sensitive in error detection since any computer connected to the network has a point-to-point connection to the central switch. It is also easy to install and reconfigure the network.
 - As data is transferred through the switch so there is no data collision in the network.
- The company leases 2 Leased Lines and 1 ADSL line.

- The need for high-speed network connection is very urgent. We will use 2 Leased Lines to connect the center with branches, ensuring stable and high-speed communication and data transmission between branches and centers.
 - Using copper cable ADSL lines to connect to the Internet, allowing devices outside the network to access the company's website.
- The server system is located in the technical room including:
 - **Web server:** is a server on which web server software is installed for customers,...
 - **Mail server:** to send-receive email messages.
 - **Database Server:** the server on which the database management system software is installed, and the bank's data is stored.
 - **FTP server** (File Transfer Protocol server): is used to exchange files over a communication network using the TCP/IP protocol.
 - **DNS Server:** is an ordered naming system for computers and services participating in the Internet. The DNS is used to map domain names to IP addresses.
- At the headquarters and branches, there are general multilayer switches located on the 1st floor (IT room) to connect the switches of each floor (for the head office) or switches of the second floor (for the branch) together.
- The server system is separated into 2 parts on the system:
 - The servers located in the DMZ: Web Server, Mail Server, FTP Server. Servers connected to the Layer 2 Switch
 - The servers located in the LAN includes: Database Server, DNS Server.
- The connection from Switch Layer 2 and Access Point to Switch Layer 3 uses Optical Cable to ensure performance and speed of transmission.
- The LAN system is protected by Firewall (To reduce the risk of attacks from outside).
- The network system is divided into VLANs, facilitating increased security for different network segments of different departments.
- Connecting to the internet from the outside into the banking network through the gateway device and the firewall to increase the security of the bank's network. This connection is transmitted over a leased line provided by the ISP.
- Connections from other branches enter the banking network through the firewall to prevent forgery. This connection is transmitted over a leased line provided by the ISP.
- Connecting to the internet to serve the needs of customers, and entertainment of bank staff,... not connected to the bank's network to ensure security. This connection is carried over an ADSL line provided by the ISP.

1.4.3 Specific arrangement

1.4.3.a Headquarter

- The entire network of the company is divided into 8 small VLAN networks (details presented in the IP diagram). This network will connect to the central router and out to the Internet.
- If there is a need to expand the number of workstations and devices by about 20% in 5 years, we can still reach it because the number of empty ports is quite large.
- A layer 3 switch will be used as the controlling switch of the whole building, this switch connects the total switches of each floor and is connected to the central router. Using Switch layer 3, we can configure it to allow or not allow VLANs to access each other and can routes for VLANs.
- Because transaction activities take place on the first floor, it is necessary to install a Wireless network to provide the network for guests. Each client laptop will access about 50Mb/day.

1.4.3.b Branch

- Using 2 48-port switches to connect to the devices and workstations and need 1 multilayer switch located on the 1st floor to connect to 2 child switches. If there is a need to expand the number of machines by about 20% in 5 years, we can still reach it because the number of empty ports is quite large.
- Use Switch layer 3 as the controlling switch similar to the headquarter.
- Floor 1 is where we put 3 Servers, network devices. Need to install Wifi modem for guests to access the network.

1.4.4 Network hierarchy

We divide the network into 4 layers:

- Layer 1: Central router, branch router and Internet network.
- Layer 2: The multilayer/layer 3 switch of the building.
- Layer 3: Switch of each floor.
- Layer 4: VLAN network of each department.

This 4-Layer network applies to branches and the headquarter.

1.5 Network security of the system

Applying the DMZ network area for essential servers, the Firewall ensures the safety of the system before receiving connections from the outside.

When discussing networks that are connected to a firewall, there are some general terms to consider:

- Outside Network - The network/zone that is outside the protection of the firewall

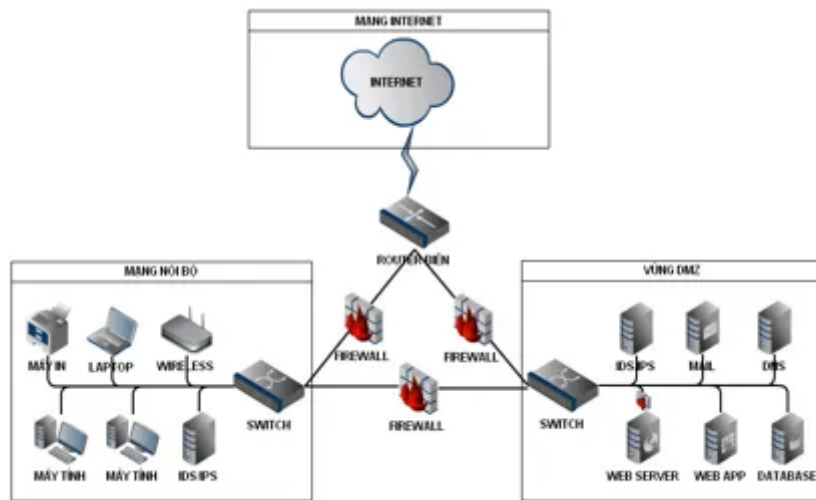


Fig. 2: Simulate the security model of the system

- Inside Network - The network/zone that is protected and behind the firewall
- DMZ - The demilitarized zone that allows both inside and outside users access to protected network resources.

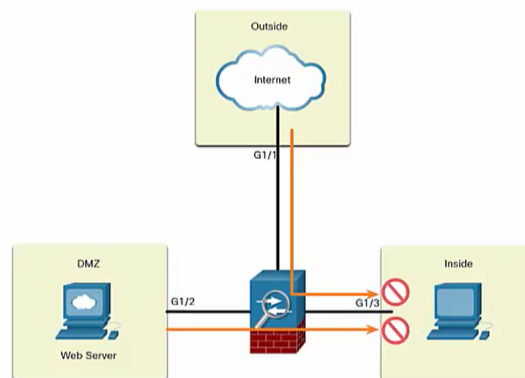


Fig. 3: DMZ

Regions with higher security values have access to regions with lower security values. Areas with smaller security values that want to access areas with higher security values must be allowed by the firewall, that is, must write rules for it.

1.6 Wireless coverage

- We design the same wireless device in headquarter and two branches.



- We design the network so that each floor has an access point to the wireless.
- We also use the WPA2-PSK authentication method to set up the password for each device that wants to connect to the wireless.
- All the devices connected to this wireless network can not be ping by other devices which are not in the same subnet area . However, the devices connected to this wireless can ping other devices from different subnet areas.

1.7 Development prediction

- **Branch expansion:** we need to rent a new Leased Line to connect the headquarter with the new branch.
- **Department expansion:** we have planned to use Switch 48 ports, so the installation of additional PCs if the number of ports is not exceeded is still satisfactory. If the need for expansion is too great, we only need to add Switch 48 ports to the central multilayer/layer 3 switch.

2 List of minimum equipment, IP diagram and wiring diagram (cabling)

2.1 List of recommended equipment

We have taken all the products of the Cisco company and further made a table of required equipment for this project.

We have used various types of network devices which includes : routers, switches, Below shows the description of all the devices:

2.1.1 Server

- Web server
- Mail server
- File server
- DNS server
- Database server

The servers need to be configured strong enough to handle many simultaneous and continuous accesses (eg thousands of transactions per day).

2.1.2 Router

We choose the Cisco ISR 4321 (2GE,2NIM,4G FLASH,4G DRAM,IPB)
CODE: ISR4321/K9

- Total throughput: 50 Mbps to 100 Mbps
- Total number of onboard 10/100/1000 WAN or LAN ports: 2



Fig. 4: Router Cisco ISR4321/K9

- Port based on RJ-45: 2
- SFP-based port: 1
- NIM (Network Interface Module) slots: 2
- Integrated Services Card (ISC) slots: 1
- Default/max DRAM: 4 GB / 8 GB
- Default/max Flash: 4 GB / 8 GB
- Power supply type:
External: AC, PoE
- Rack height: 1 RUES

Gigabit Ethernet port to connect to the switches and routers in the same area.

Serial Port provides serial communication (gateway) with other devices in other areas.

2.1.3 Switch

Although in the tracer we have already use the but in reality, we intend to use Cisco SRW248G4-K9 (SF300-48) to maximize the number of ports.



Fig. 5: Cisco SRW248G4-K9 (SF300-48) switch

- Cisco SF300-48 is an important device used to connect network segments with each other according to the star topology.
- Product ID Number: SRW248G4-K9

- 48-port 10/100Mbps + 4-Port Gigabit Switch with WebView.
- 48 10/100Mbps; 2 10/100/1000Mbps ports; 2 Combo mini-GBIC ports.
- Performance: Switching capacity 17.6 Gbps, nonblocking, Forwarding rate 13.10 mpps wire-speed performance.
- 48 x 10Base-T / 100Base-TX - RJ-45 - PoE; 1 x control panel - 9 pins D-Sub (DB-9) - management; 4 x 10Base-T / 100Base-TX / 1000BaseT - RJ-45; 2 x SFP (mini-GBIC)
- Flash Memory: 16MB
- RAM: 128MB

In Headquarter: the building has 100 workstations, so we use 1 switch on each floor Cisco SRW248G4-K9 (SF300-48) (each switch has 48 ports).

Branch: The number of machines in the branch is 50 workstations, so we use 2 Cisco Switches SRW248G4-K9 (SF300-48) (each switch has 48 ports), and are connected to Core Switch.

The computer system for the bank is located on a different interface of the firewall.

2.1.4 Core Switch

Use layer 3 switch to connect the switches on different floors together because there are more features than switch layer 2, providing high speed, better security. We choose the core-switch Cisco Catalyst 9300 Series Switches to do core-switch for the system.

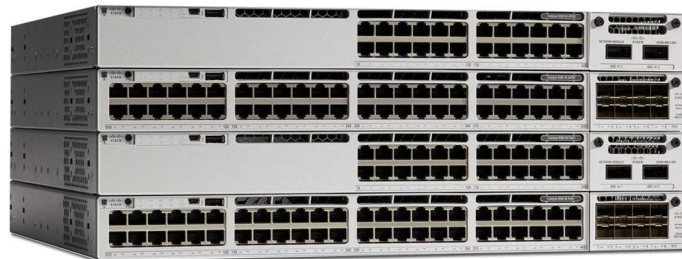


Fig. 6: Cisco Catalyst 9300 Series Switches

- x86 CPU complex with 8-GB memory, and 16 GB of flash and external USB 3.0 SSD pluggable storage slot (delivering up to 240GB of storage with an option SSD drive) to host containers. C9300X models support 16GB of memory. The x86 CPU architecture and more memory allow them to host and run third-party applications.
- Up to 1 TBps of local stackable switching bandwidth.

- IPv6 support in hardware, providing wire-rate forwarding for IPv6 networks
- USB 2.0 slot to load system images and set configurations.
- Highest wireless scale for Wi-Fi 6 and 802.11ac Wave 2 access points supported on a single switch with select models.

2.1.5 Firewall

To ensure information security, it is imperative to build a firewall system, especially for banks. We use Cisco ASA5506-K9 with FirePOWER service as firewall.



Fig. 7: Cisco ASA5506-K9

- Product Code: ASA5506-K9
- Interfaces: 8 x 1 Gigabit Ethernet interface, 1 management port
- Stateful inspection throughput (multiprotocol): 300 Mbps
- Maximum 3DES/AES VPN throughput: 100 Mbps
- IPsec site-to-site VPN peers: 10; 50 with Security Plus license
- Virtual interfaces (VLANs): 5; 30 with Security Plus license
- Memory: 4GB
- Flash: 8GB
- Power: (AC or DC) AC

Filter URLs and categories, provide comprehensive alerts and control web traffic, and enforce policies on hundreds of millions of URLs in over 80 categories.

Granular application visibility and control (AVC) supporting over 4,000 application layers and operations based on tailored intrusion threat detection (IPS) policies to optimize security performance.

2.1.6 Access Point

It is possible to arrange 1 or more access-points to serve the entertainment needs as well as information retrieval of customers. Its advantage is to ensure the convenience of accessing the network without going through the network wiring. We choose Wireless Access Point Meraki CISCO MR66.



Fig. 8: Wireless Access Point Meraki CISCO MR66

- Layer 7 application fingerprinting and QoS.
- Max throughput rate 600 Mbit/s.
- Integrated policy firewall (Identity Policy Manager)
- Real-time WIPS with Air Marshal.

2.1.7 Cable

Include Copper Straight through, Cross-over, Serial connection through leased line to other branches. They are used for connection between switches, PCs, servers and routers.

For the Ethernet cable, we use Cat5e which is capable of transmitting large data at a speed of up to 1000 Mbps and significantly reducing noise during signal transmission.

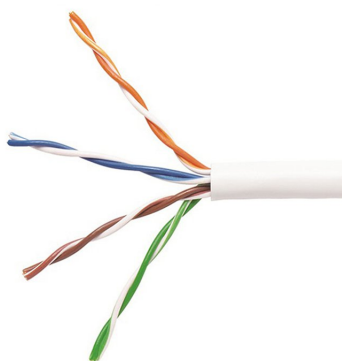


Fig. 9: Cat5e cable



2.1.8 End Devices

Computers (work stations, laptops, file servers, web servers), printers, VoIP phones, fax machines,...

2.1.9 Checkpoint

Identity Awareness (IA) in Checkpoint allows us to add user, user groups, and machine identity to your security layer. Traditionally, firewalls used IP addresses to monitor traffic and were unaware of the user and computer identities behind those IP addresses.

Identity Awareness maps user and computer identities to IP addresses, allowing you to enforce identity-based data access and auditing.

Identity Awareness is an easy to deploy and scalable solution. It is applicable to both Active Directory and non-Active Directory-based networks, as well as to employee and guest users. Check Point supports both local and external users. Local users are defined on the Security Management Server. External users are those managed by Active Directory, RADIUS, LDAP server.

The Access Role identifies users, computers, and network as an object and can be used as the source or destination in the rule.

The Access Role can include one or more of these objects:

- Networks
- Users and user groups
- Computers and computer groups
- Remote access clients

Identity Awareness Software Blade provides many methods to obtain the user's identity, including:

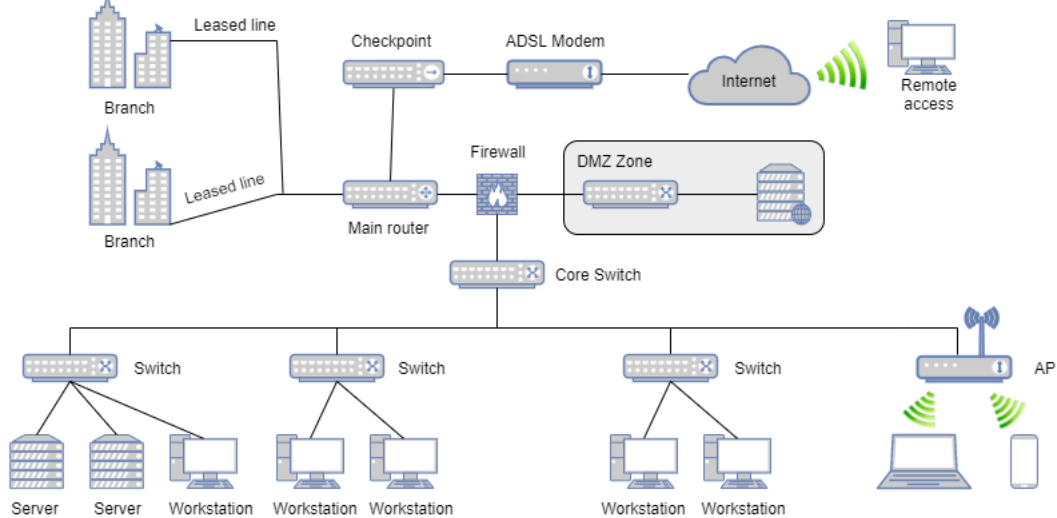
- AD Query
- Browser-Based
- Identity Agents
- RADIUS Accounting
- Remote Access clients
- Identity Collector and the Identity Web API.

2.2 Schematic physical setup

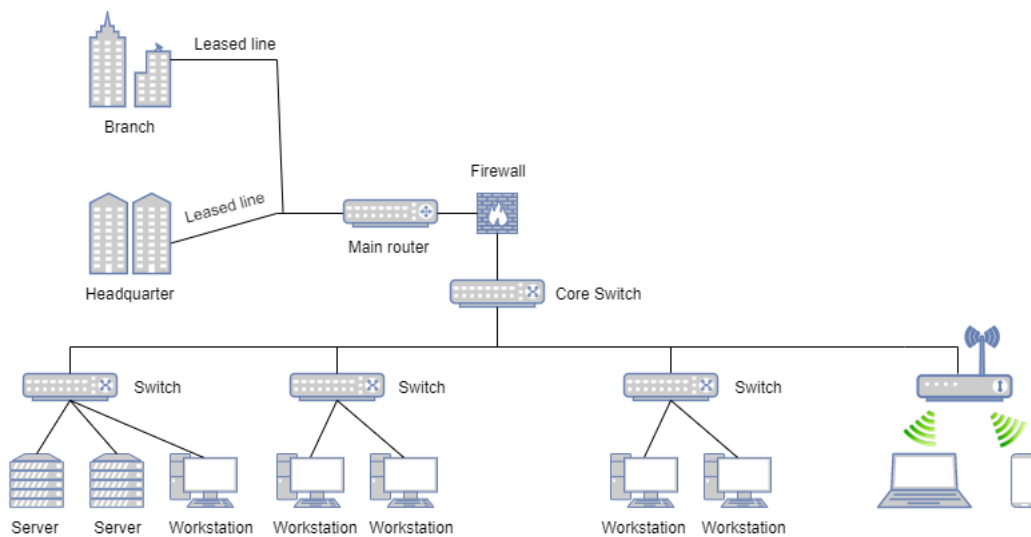
The BBBank has 2 branches in Nha Trang(NT) and Da Nang(DN). The Headquarter of BBBank is located in HCM City.

We also manage to make the Branches and Headquarter to communicate with each other using

WAN links.



HQ diagram

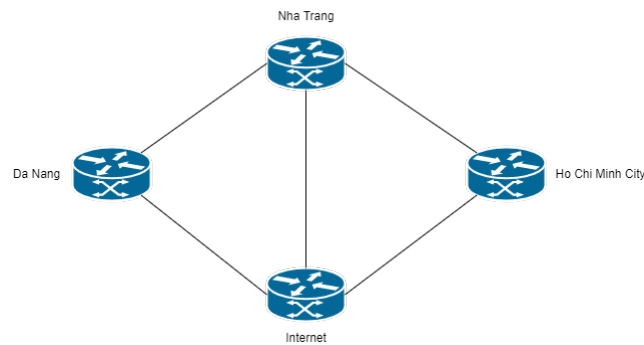


Branch diagram

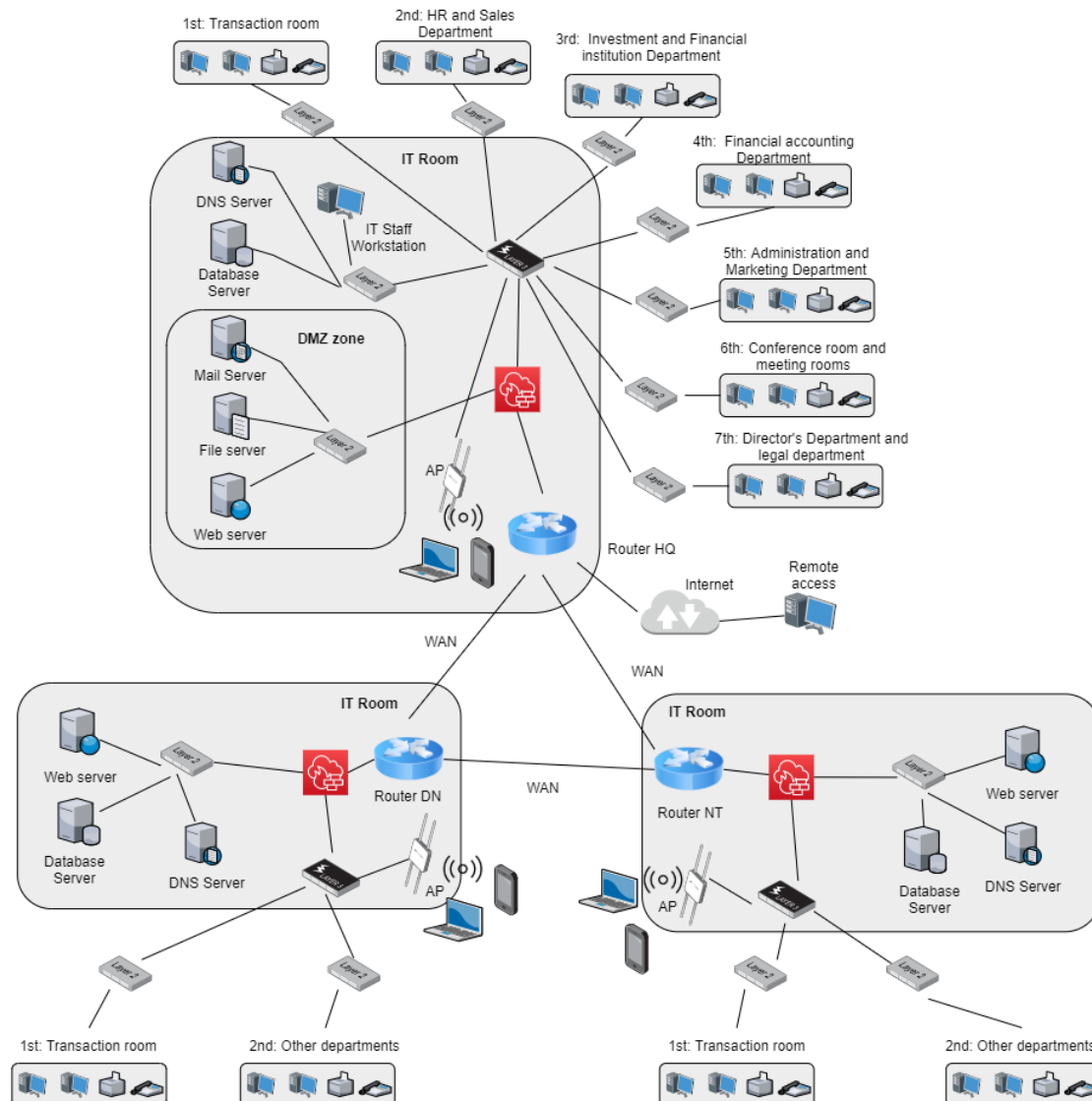
The main structure is using one core router for WAN connection and one core switch for manage all the switches of each floor.

2.3 WAN connection diagram

This is the connection between the headquarter and branches by WAN.



Below is a simulation of the general connection diagram of a computer network.





2.4 IP address table

Headquarter: IP router: 10.0.0.1, IP switch layer 3: 10.0.0.2.

Da Nang: IP router: 10.1.0.1, IP switch layer 3: 10.1.0.2.

Da Nang: IP router: 10.2.0.1, IP switch layer 3: 10.2.0.2.

Location	DEPT	Network ID	Default Gateway	VLAN
HO CHI MINH	IT/Workstation	10.0.10.0/24	10.0.0.1	VLAN 10
	IT/Server	10.0.10.0/24	10.0.0.1	VLAN 10
	HR and Sales Department	10.0.20.0/24	10.0.0.1	VLAN 20
	Investment and Financial Institution Department	10.0.30.0/24	10.0.0.1	VLAN 30
	Financial accounting Department	10.0.40.0/24	10.0.0.1	VLAN 40
	Administration and Marketing Department	10.0.50.0/24	10.0.0.1	VLAN 50
	Conference room and meeting rooms	10.0.60.0/24	10.0.0.1	VLAN 60
	Director's Department and legal department	10.0.70.0/24	10.0.0.1	VLAN 70
	HQ Router serial link 0	192.168.0.0/24	N.A	N.A
	HQ Router serial link 1	192.168.10.0/24	N.A	N.A
DA NANG	IT/Workstation	10.1.10.0/24	10.1.0.1	VLAN 10
	IT/Server	10.1.10.0/24	10.1.0.1	VLAN 10
	Other deparments	10.1.20.0/24	10.1.0.1	VLAN 20
	DN Router serial link 0	192.168.0.0/24	N.A	N.A
NHA TRANG	IT/Workstation	10.2.10.0/24	10.2.0.1	VLAN 10
	IT/Server	10.2.10.0/24	10.2.0.1	VLAN 10
	Other deparments	10.1.20.0/24	10.1.0.1	VLAN 20
	NT Router serial link 1	192.168.10.0/24	N.A	N.A

3 Calculate throughput, bandwidth, and safety parameters for computer networks

We should focus on the system parameters to ensure that the design can handle the amount of load capability required for the bank to operate. The parameters that we are interested in are the amount of data transferred over time (in Mbps). In which two concepts include:

- **Throughput** measures the amount of load of the system during the operation time, namely a day.
- **Bandwidth** measures the amount of data the system can handle during peak hours.

As the requirement:

- Servers 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 transactions, ... The total upload and download capacity is about 100 MB/day.
- WiFi connected laptop for customers to access about 50 MB/day.

3.1 In headquarter

3.1.1 Server

5 Server: Total upload and download capacity 500 MB/day. The total peak time of a day is 3 hours (9:00 - 11:00 and 15:00 - 16:00) and can consume up to 80%.

$$Bandwidth_S = \frac{5 \times 500 \times 0.8}{3 \times 3600} = 0.185 \text{ (MB/s)} = 1.481 \text{ (Mbps)}$$

$$Throughput_S = \frac{5 \times 500}{8 \times 3600} = 0.087 \text{ (MB/s)} = 0.695 \text{ (Mbps)}$$

3.1.2 Workstation

100 Workstations: Total upload and download capacity is 100 MB/day. At peak hours (for 3 hours) exchange 80% of data during the day.

$$Bandwidth_W = \frac{100 \times 100 \times 0.8}{3 \times 3600} = 0.741 \text{ (MB/s)} = 5.925 \text{ (Mbps)}$$

$$Throughput_W = \frac{100 \times 100}{8 \times 3600} = 0.347 \text{ (MB/s)} = 2.78 \text{ (Mbps)}$$

3.1.3 User

We assume about 200 clients in a day, 120 at peak. Total upload and download capacity is 50 MB/day

$$Bandwidth_U = \frac{120 \times 50}{3 \times 3600} = 0.556 \text{ (MB/s)} = 4.444 \text{ (Mbps)}$$

$$Throughput_U = \frac{200 \times 50}{8 \times 3600} = 0.347 \text{ (MB/s)} = 2.78 \text{ (Mbps)}$$

3.1.4 Total

We get the required total bandwidth:

$$Bandwith_{HQ} = 0.185 + 0.741 + 0.556 = 1.389 \text{ (MB/s)} = 11.856 \text{ (Mbps)}$$

$$Throughput_{HQ} = 0.087 + 0.347 + 0.347 = 0.781 \text{ (MB/s)} = 6.248 \text{ (Mbps)}$$

To ensure the growth rate at 20%, the computer network must ensure:

$$Bandwidth = 11.856 \times 1.2 = 14.2272 \text{ (Mbps)}$$

$$Throughput = 6.248 \times 1.2 = 7.498 \text{ (Mbps)}$$

3.2 In branch

3.2.1 Server

3 Server: Total upload and download capacity 500 MB/day. The total peak time of a day is 3 hours (9:00 - 11:00 and 15:00 - 16:00) and can consume up to 80%.

$$Bandwidth_S = \frac{3 \times 500 \times 0.8}{3 \times 3600} = 0.111 \text{ (MB/s)} = 0.889 \text{ (Mbps)}$$

$$Throughput_S = \frac{5 \times 500}{8 \times 3600} = 0.052 \text{ (MB/s)} = 0.417 \text{ (Mbps)}$$

3.2.2 Workstation

50 Workstations: Total upload and download capacity is 100 MB/day. At peak hours (for 3 hours) exchange 80% of data during the day.

$$Bandwidth_W = \frac{50 \times 100 \times 0.8}{3 \times 3600} = 0.37 \text{ (MB/s)} = 2.963 \text{ (Mbps)}$$

$$Throughput_W = \frac{50 \times 100}{8 \times 3600} = 0.174 \text{ (MB/s)} = 1.389 \text{ (Mbps)}$$

3.2.3 User

We assume about 100 clients in a day, 50 at peak. Total upload and download capacity is 50 MB/day

$$Bandwidth_U = \frac{50 \times 50}{3 \times 3600} = 0.231 \text{ (MB/s)} = 1.852 \text{ (Mbps)}$$

$$Throughput_U = \frac{100 \times 50}{8 \times 3600} = 0.174 \text{ (MB/s)} = 1.389 \text{ (Mbps)}$$

3.2.4 Total

We get the required total bandwidth:

$$Bandwidth_{Br} = 0.111 + 0.37 + 0.231 = 0.712 \text{ (MB/s)} = 5.700 \text{ (Mbps)}$$

$$Throughput_{Br} = 0.052 + 0.174 + 0.174 = 0.4 \text{ (MB/s)} = 3.2 \text{ (Mbps)}$$

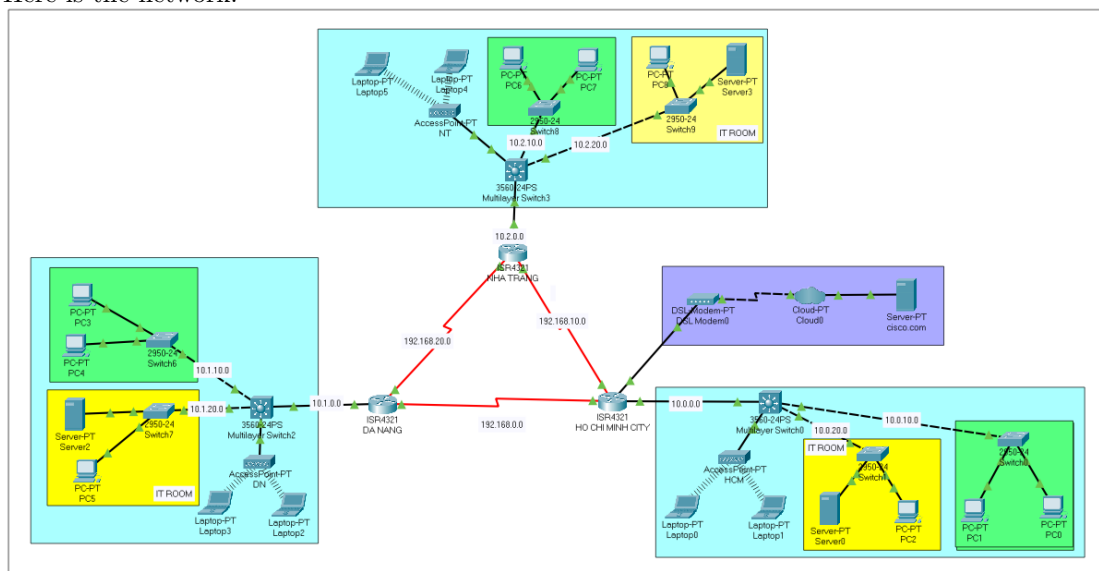
To ensure the growth rate at 20%, the computer network must ensure:

$$Bandwidth = 5.700 \cdot 1.2 = 6.8398 \text{ (Mbps)}$$

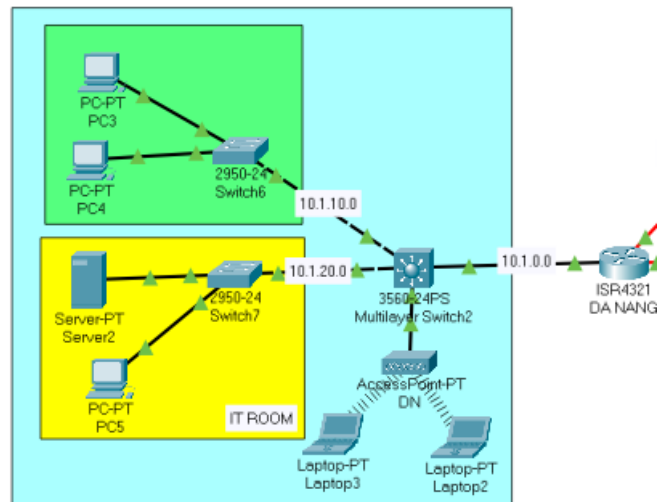
$$Throughput = 3.2 \cdot 1.2 = 3.84 \text{ (Mbps)}$$

4 Design the network map using Packet Tracer or GNS3 simulation software

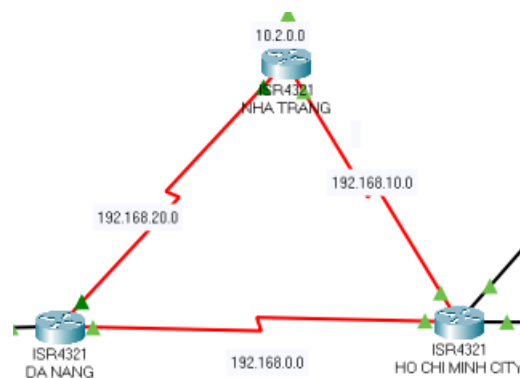
The design is attached with the report submission which named **tracer.pkt**.
Here is the network:



In this design, we simulate these following parts: The first room is IT room, in this room, servers will be placed and also there are some computers for IT staffs to manage the network. The IT room and access point will be placed in the first floor, as mentioned before. And the remained part of the branches represent for all remained floors with workstation.

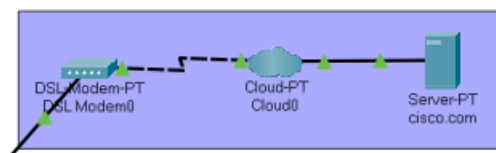


All of it will be connected to a multi-layer switch and that switch will be connected to a router to join with the WAN.



Also, as the requirements, customer's devices is configured so that it cannot join in the workflow of the system.

The branches have the similar design and so for the headquarter. Besides, the headquarter is equipped with an ADSL connection for internet connection.

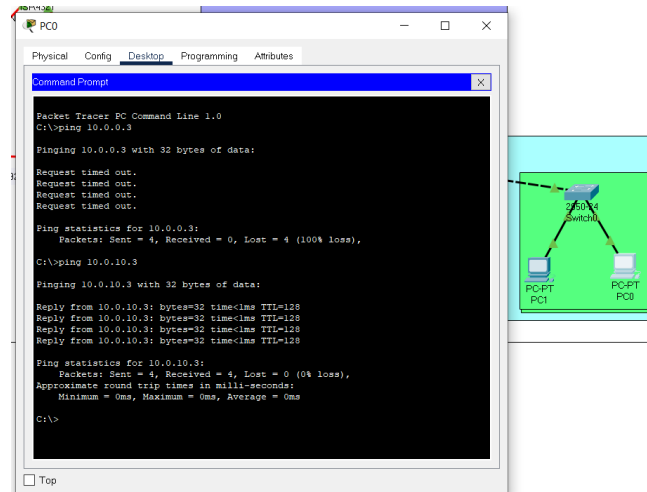


5 Test the system with popular tools such as ping, traceroute, ... on the simulated system.

Here, I will tests the connections of the simulated system by using **ping** command:

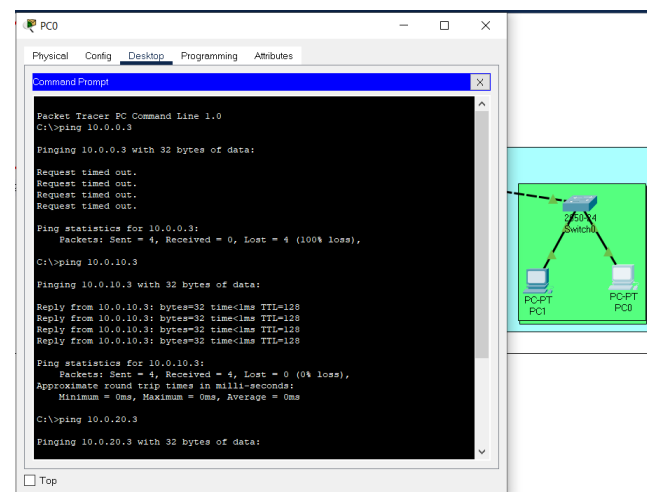
5.1 Connect between PCs in the same VLAN

We use **ping** command to test the connection between PCs in VLAN 10 in headquarter.



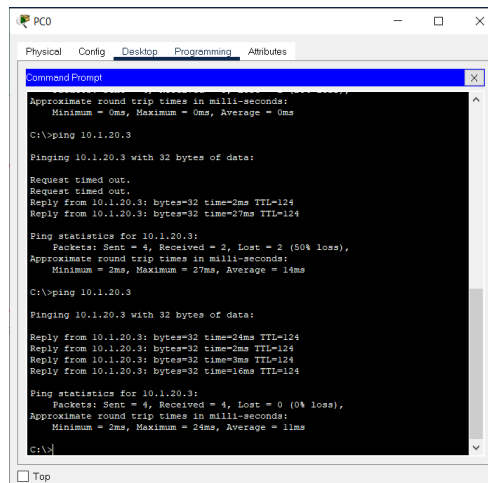
5.2 Connect PCs between VLANs

Here is the connection between PCs in VLAN 10 and VLAN 20 at headquarter.



5.3 Connect PCs between Headquarters and branches

Testing the connection of PC headquarter and PC in Da Nang:



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.1.20.3

Pinging 10.1.20.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.1.20.3: bytes=32 time=2ms TTL=124
Reply from 10.1.20.3: bytes=32 time=27ms TTL=124

Ping statistics for 10.1.20.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 27ms, Average = 14ms
C:\>ping 10.1.20.3

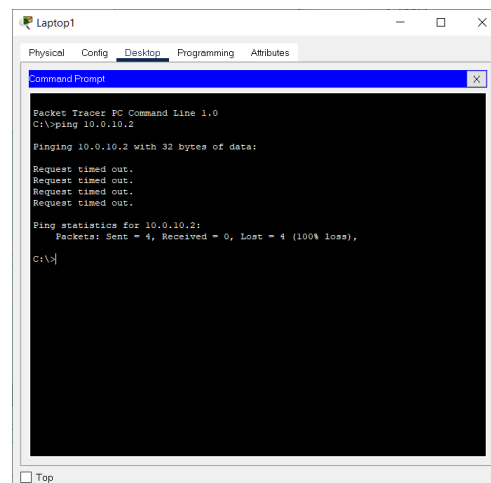
Pinging 10.1.20.3 with 32 bytes of data:

Reply from 10.1.20.3: bytes=32 time=24ms TTL=124
Reply from 10.1.20.3: bytes=32 time=2ms TTL=124
Reply from 10.1.20.3: bytes=32 time=3ms TTL=124
Reply from 10.1.20.3: bytes=32 time=16ms TTL=124

Ping statistics for 10.1.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 24ms, Average = 11ms
C:\>
```

5.4 No connections from Customers devices to PCs on the LAN

Pretend that the Laptop1 is customer's device, here is the result when using **ping** command to one PC in the system.



```
Laptop1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.10.2

Pinging 10.0.10.2 with 32 bytes of data:

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

Ping statistics for 10.0.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Some packet loss have occurred because the network needs to fill in the MAC table of the switch. When all the MAC addresses are filled, packets are delivered without any loss.

6 Re-evaluate the designed network system through the following features: reliability, easy to upgrade, diverse support software, safety, the security of data, ...

6.1 Reliability

Because the purpose of the network is designed for a bank so the security is the first and foremost issue. So, the network should meet some minimum requirements about the security such as:

- Keep track and control the access of customer.
- Personal information and transaction are guaranteed.
- Prevent the illegal access from both inside and outside.
- Multi-layer security is needed for sensitive information.
- The system can be recovered after being attacked.

Also, there are more requirements for the system due to the bank's need, and it will be updated when issues arrive.

The bandwidth and throughput, the design estimate when there will be high network load so that it ensure the provide high quality of network for users. Also for the IP address, the subnet has large amount of IP address so it can meet the requirements when the system need to be enlarged.

6.2 Easy to upgrade

As the system is not perfect when first created, so it need to be updated whenever problems are found or raised. So, the system need to be easy to upgrade.

- Firewall and reliable security approach to prevent illegal activities. Regularly testing and update to get rid of security problems.
- Back up data in server and update attack method to avoid the system from being trespassed.

One more thing is about the increment of users in the system. Because there are still empty ports in the routers and the core switches, when it is needed to create a new branch or connect with more devices, the system can still handle after re-configuration.

6.3 Safety

- The server is connected to IT room so that there will always be a group of staffs to handle the issue (if any).
- Leased line to connect in the WAN which guarantees the safe and strong connection between branches and headquarter.

To be honest, there are also some security requirements that we cannot do it perfectly so we cannot fully rate the safety of the system that we have simulated.

6.4 Diversity in Software support

- Our system not only supports Ethernet connection devices but also have the wireless router, which allows wireless devices (such as smartphones, laptops, etc) to connect to the Internet.
- Use the combination of Licensed and Open source Software.

6.5 Problems

There are also some remaining problems of the system that we have recognized.

- The system will be affected whenever a part of the system has issue, because the network has many centrally connected nodes (routers, core switches).
- The cost of devices of Cisco are affordable with small scale, but it will raise a problem when the system enlarge. Considering to cut down some part is essential to save the budget.
- Due to many assumptions, the solution is not close to reality.
- Despite the firewall, there is still a high risk of viruses because an infected system can spread the virus through the entire network.
- The firewall will be under a heavy load. If the firewall fails, the entire system will be affected.
- The serial link for inter-branch connections will soon become a bottleneck should our bank demand for that grow any larger.

6.6 Development Orientation

- We will provide some security mechanism in order to protect the system from DDOS, SQL, etc.
 - The orientation will incorporate an additional IDS intrusion detection system into the firewall to increase the overall level of protection.
 - Install voip system to chat directly from the director's room to the departments. This system will have its own connection to the voip server.
 - Security in the operating system and applications, regularly backing up, updating patches of the operating system, using additional software (Patch) to close vulnerabilities on operating systems, ensuring that the system works properly. stabilization work.
 - Orientation to develop backup server for servers in the DMZ, especially the database server to ensure risks.
 - Access layer security: secure dial-up user access: Create VPN channels for dial-up connections.
 - Design to reduce system load by building redundant nodes, double-layer DMZ.
 - Enhance security with multiple layers of firewall, measure and prevent all kinds of network attacks, especially zero-day attacks.
- We will also provide some hashing mechanism so that only customers can know their information, and even the bank does not know the information not provided by the customer.
- We will continue learning some mechanisms to expand the bank in many different ways in security, robustness and maintainance and also to provide more services for the users.
- Carefully survey the needs and design of the buildings at the headquarters and branches to arrange the equipment in a reasonable way.
- Design to expand the number of devices in case the bank's size increases by more than 20%. Developing workstations in departments with the use of 48 port switches, even doubling the number of workstations can still meet the requirements.