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

# COMPUTER NETWORK (CO3093)

## Assignment 2

# NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

| | |
|---|---|
| Instructor: | Nguyen Phuong Duy |
| Group: | 6 - CC02 |
| Students: | Mai Tôn Đăng Khánh - 2152122 |
| | Võ Trung Kiên - 2153502 |
| | Cao Chánh Trí - 2153917 |
| | Trần Hoàng Khôi Tuấn - 2012359 |

HO CHI MINH CITY, SEPTEMBER 2023

# Contents

# 1 Suitable network structures for buildings

## 1.1 Network system requirements of Headquarters and Branch

### 1.1.1 Headquarter

- The building consists of 7 floors, the first floor is equipped with one IT room and Cabling Central Local (using patch panels gathering wires).
- Medium-scale: 120 workstations, 5 servers, 12 networking devices (or maybe more with security-specific devices).
- It should support both wired and wireless connections. Fiber cabling should be considered
- It should be organized according to the VLAN structure and GigaEthernet 1GbE/10GbE.
- The network connects to outside by 2 leased lines for WAN connection and 2 xDSL with a load-balancing mechanism.
- All traffic to the Internet passes through the Headquarters subnet.
- It use a mix of licensed and open-source software, office applications, client-server applications, multimedia, and database.
- The network is required to be highly secured, with high availability, robustness and ease of upgrade taken into account.
- The Head Office connects to 2 branches in Da Nang and Ha Noi.
- BB Bank's Network is estimated to have a growth rate of 20% in 5 years (in terms of the number of users, network load, branch extensions, ..)

### 1.1.2 Branches

Each branch is also designed similarly to the headquarters but on a smaller scale.

- The building has 2 floors, the first floor is equipped with 1 IT room and 1 Cabling Central Local.
- BB Branch small-scale: 30 workstations, 3 servers, 5 or more networking devices.

### 1.1.3 System Throughput and Bandwidth

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

- Servers for software updates, web access, and database access, ..... The total download estimate is about 1000 MB/day and the upload estimate is 2000 MB/day.
- Each workstation is used for Web browsing, document downloads, and customer transactions, ... The total download estimate is about 500 MB/day and the upload estimate is 100 MB/day.
- WiFi-connected devices from customers' access for downloading are about 500 MB/day.
- VPN configuration for site-to-site and for a teleworker to connect to LAN.

## 1.2 Surveyed Checklist at the installation locations

Before installing the devices:

1. Check that there is enough physical space for all networking devices and work stations on each floor. The first floor should be given special consideration due to the importance of the devices placed there.
2. The physical security of the IT room should also be taken into account. It should not be accessed by unauthorized people.
3. Ventilation (if required) needs to be taken care of to ensure optimal working condition for servers and networking devices.
4. Edge switches and wireless access points should be placed in such a way that prevent or at least discourage workers and other personnel from tampering with those devices.
5. Check that there is enough devices as is required for the installation.

After installing and configuring the network:

1. Each workstation is able to communicate to other workstations on the same floor, in the same building, and then in the company.
2. Each workstation is able to communicate, upload/download data to/from servers within the same building and possibly those in other buildings, depending on company's policy

## 1.3 Define high load area

- Network Load Balancing: is important feature for computer network. It is the uniform distribution of traffic between two or more servers with the same function in the same system. By using Network Load Balancing, the system will minimize the situation a server is overloaded and down. Or when a server crashes, weigh by load will direct the distribution of the work of that server to the rest of the servers, push system's up-time highest and improve overall operational productivity. This ensures system availability, reliability and can easily and flexibly add or remove servers as required for future upgrades.
- Technically, the web server system allows all Internet users to search for information, exchange information with the bank website. Therefore, it is necessary to ensure access speed and stability.
- We notice, it is on the SECOND and THIRD floors that there is access from plenty of customers and the amount of information here is huge. Therefore, it is necessary to focus on network load balancing here.

## 1.4 Network structure

- The system is arranged in a star-shaped topology, including 100/1000 Mbps switches.

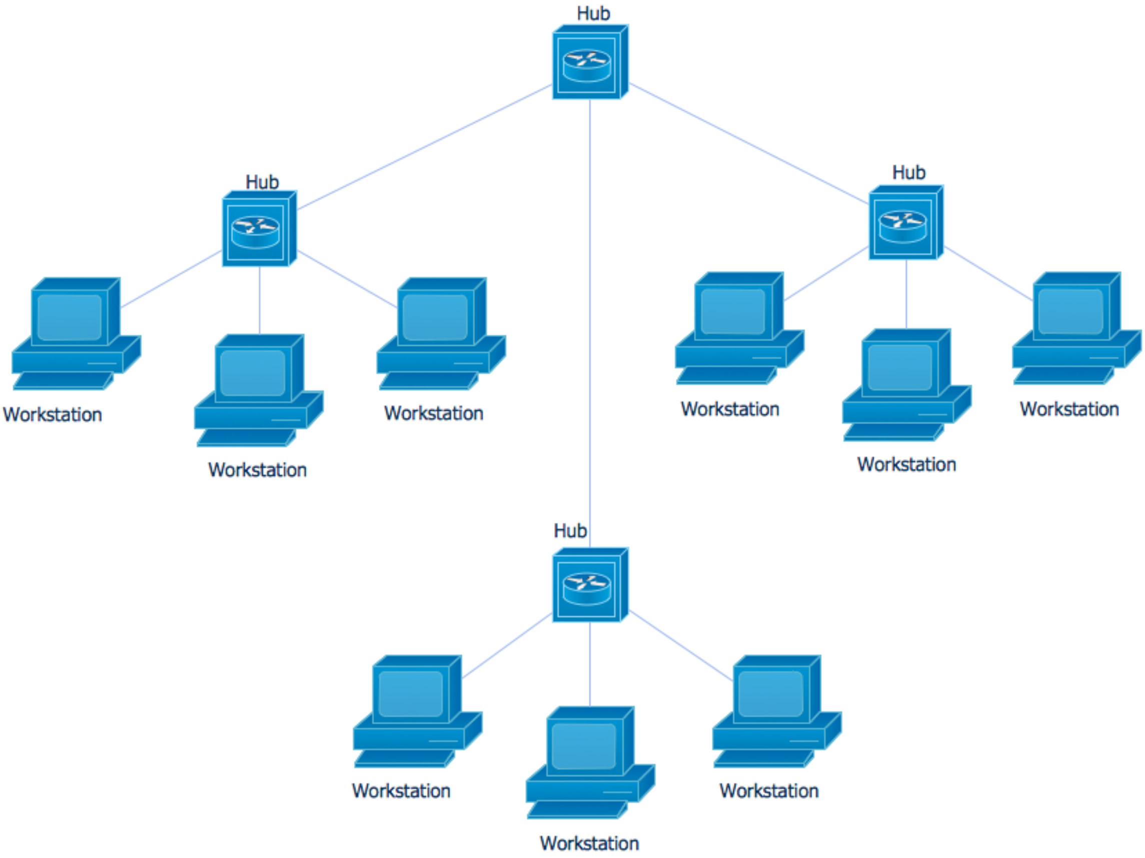


Figure 1. Star topology

Star topology is scalable, enabling the addition or removal of devices without disrupting the entire network. Each device has a dedicated connection to the central hub, providing isolation and localized fault management. The centralized control facilitates efficient monitoring and maintenance, contributing to good network performance. Additionally, the design allows for convenient upgrades and expansions, as new devices can be integrated into the central hub.

- The server system located in the IT room includes:
  - Web Server: the server on which the software is installed for customers.
  - Mail Server: for sending and receiving emails.
  - FTP Server: used for file exchange through TCP/IP (Transmission Control Protocol/Internet Protocol).
  - DNS Server: the domain name resolution server used to map domain names to IP addresses.

- In the network, use Switch Layer 3 to connect to server systems and workstations through Switch Layer 2. Eight Switch Layer 2 devices at the main office and three Switch Layer 2 devices at the branch connect to the Switch Layer 3. The connection from Switch Layer 2 and Access Point to Switch Layer 3 by Fiber Optic Cable ensures transmission quality and speed.

- The connection from another branch enters the company network through the leased line provided by the ISP.

- Connecting to the internet serves the needs of customers and entertains employees. It must not be connected to the company network to ensure security. This connection is transmitted over the ADSL line provided by the ISP.

- It is crucial to combine the inside network, outside network, and DMZ while prioritizing network security standards. Establish a robust firewall to regulate traffic between internal and external domains. Deploy a dedicated DMZ to host public-facing servers like web servers, ensuring that external access is tightly controlled.

## 1.5 Network usage in a wireless environment

- For the convenience of customers, the wireless point will be set at the floor where the customers service located.

- The wireless access point will be in the same subnet as the workstation and switch in the floor that it is on.

- One benefit of wireless access points is that it reduce the need for high-port-count switches and wires on each floor, which can reduce cost and labor.

## 1.6 Propose a VPN configuration and a surveillance camera system

### 1.6.1 Propose a VPN configuration

- Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

- We have split it into two steps that are required to get the Site-to-Site IPSec VPN Tunnel to work. These steps are:
  - Configure ISAKMP(IKC) (ISAKMP Phase 1)
  - Configure IPSec (ISAKMP Phase 2, ACLs, Crypto MAP)

### 1.6.2 Propose a surveillance camera system

In surveillance camera system, the number of camera and its position mostly depend on the architecture of each floor of the building. Therefore we provide some requirements for the system that can be applied to arbitrary number of camera:

- Star topology: Implement a star topology where each surveillance camera connects to a central Ethernet switch of the floor it located.

- Power over Ethernet (PoE): Utilize PoE switches to provide both data connectivity and power to the surveillance cameras over a single Ethernet cable. This reduces cabling complexity and allows for flexible camera placement.
- Bandwidth Requirements: Estimate the bandwidth needs based on the resolution and frame rates of the surveillance cameras. Remember to ensure that the network infrastructure can handle the aggregate bandwidth of all cameras during peak usage.
- Network Switches: Choose managed Gigabit Ethernet switches with sufficient ports to accommodate the number of cameras. Ensure that the switches support PoE for simplified camera power and data connectivity.
- Firewall and Security Appliances: Deploy firewalls and other security appliances to protect the surveillance camera network from unauthorized access.
- VPN for Remote Access: If remote monitoring is required, set up a secure VPN for authorized personnel to access the surveillance camera system remotely.
- Remember to separate the surveillance camera network from the company's regular data network to ensure security isolation and bandwidth management.

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

## 2.1 List of recommended equipment and typical specifications

### 2.1.1 Router: CISCO1941/K9 Cisco 1941

Figure 2. Router CISCO1941/K9 Cisco 1941

**Description:** The Cisco 1941 Integrated Services Router is a versatile networking device designed for small to medium-sized businesses. Offering a throughput of up to 2 Mbps, it supports various WAN interfaces, including T1/E1, xDSL, and Gigabit Ethernet, providing flexible connectivity options. With integrated security features, modular design for scalability, and support for advanced routing and switching protocols, the Cisco 1941 ensures robust performance and adaptability.

**Specifications:**

- Manufacturer: Cisco Systems, Inc.
- Manufacturer Part Number: CISCO1941/K9.
- Product Type: Router.
- Form Factor: External - modular - 2U
- Services and Slot Density:

  - Embedded hardware-based crypto acceleration (IPSec): Yes.
  - Total Onboard Gigabit Ethernet 10/100/1000 WAN ports: 2.
  - RJ-45-Based Ports: 2.
  - EHWIC Slots: 2.
  - Double-wide EHWIC slots: 1.
  - DRAM Memory: 512 MB (installed) / 2 GB (max).
  - Flash Memory: 256 MB (installed) / 8 GB (max).
  - Serial Console Port: 1
  - Serial Auxiliary Port: 1
  - Power Supply Options: AC, POE.

- Routing Protocol: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing.
- Data Link Protocol: Ethernet, Fast Ethernet, Gigabit Ethernet.
- Network/Transport Protocol: IPSec.
- Features: Cisco IOS IP Base , firewall protection, VPN support, MPLS support, Syslog support, IPv6 support, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED).
- Compliant Standards: IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag.
- Power: AC 100/240 V ( 47-63 Hz).
- Dimensions (WxDxH): 34.3 x 29.2 x 8.9 cm.
- Weight: 5.8 kg.

### 2.1.2 Switch layer 2: CISCO WS-C2960+24TT-L

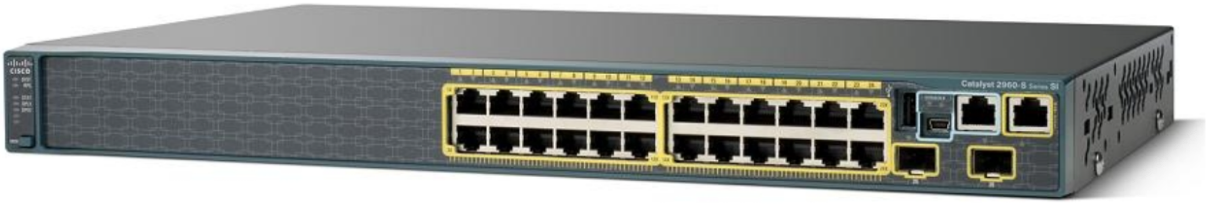


Figure 3. Switch layer 2 CISCO WS-C2960+24TT-L

**Description:** The Cisco Catalyst WS-C2960+24TT-L is a Layer 2 managed switch designed for efficient and secure network connectivity. With 24 Ethernet 10/100 ports, it provides reliable and high-performance connectivity for various devices within a network. The switch supports advanced features such as VLANs like our project to optimize network traffic and enhance overall performance. Additionally, the switch can be easily integrated into a larger network infrastructure, making it a versatile choice for building scalable and reliable networks.

**Specifications:**

- Manufacturer: Cisco Systems, Inc.
- Manufacturer Part Number: Cisco WS-C2960-24TT-L.
- Product Type: Switch - 24 ports - Managed.
- Enclosure Type: Rack-mountable 1U.
- Uplink interface: 2 (SFP or 1000BASE-T).
- Ports: 24 x 10/100Mbps Ethernet.
- Bandwidth forwarding: 16 Gbps.
- DRAM: 128 MB.
- Flash Memory: 64 MB.
- Protocols: SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH.
- Compliant Standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP).
- High Availability / High Responsiveness: PVST, Block Broadcast, Interrupt Unicast, Block Mulitcast, Spanning Tree, Portfast, Fast Uplink, Fast Backbone, 802.1s, 802.1w.

- Management features: SPAN, CiscoView, Cisco Discovery Protocol (CDP), Virtual Trunking Protocol (VTP), Telnet customers, BOOTP, TFTP, CiscoWorks, CWSI, RMON, SNMP, Clustering, Web Management.
- Throughput: 6.5 Mbps.
- Power: AC 120/230 V (50/60 Hz).
- Dimensions (WxDxH) 44.5 cm x 23.6 cm x 4.4 cm
- Weight 3.63 kg

### 2.1.3 Switch layer 3: Cisco WS-C3650-24PS-S

Figure 4. Switch layer 3: Cisco WS-C3650-24PS-S

**Description:** The Cisco Catalyst WS-C3650-24PS-S is a Layer 3 managed switch designed to deliver high-performance, feature-rich networking for organizations of varying sizes. With 24 Gigabit Ethernet ports, PoE+ support, and modular uplink options, this switch provides advanced connectivity for a range of devices. As a Layer 3 switch, it offers IP routing capabilities, enabling efficient inter-VLAN routing and enhancing network segmentation. The WS-C3650-24PS-S also features Power over Ethernet (PoE) support, providing power to connected devices such as IP phones and cameras, and includes advanced security features to safeguard the network.

**Specification:**

- Manufacturer: Cisco Systems, Inc.
- Manufacturer Part Number: Cisco WS-C3560V-24PS-S.
- Enclosure Type: Rack-mountable 1U.
- Gate: 24 gates 10/100/1000 Ethernet.
- Bandwidth forwarding: 41,66Mpps.
- Power conversion: 88 Gb / s.

- RAM: 4 GB.
- Flash memory: 2 GB.
- Routing Protocol: RIP-1, RIP-2, Static IP.
- Features: Layer 3 switching, automatic recognition per device, DHCP support, auto-negotiation, load balancing, VLAN support, auto-linking (MDI/MDI-X), MAC address filtering, IPv6 Support Trunking Protocol (STP), DHCP snooping, DTP support, Port Aggregation Protocol Support (PAgP), TFTP support, Access Control List (ACL), Quality of Service (QoS) support, Jumbo Frames support, Dynamic ARP Inspection (DAI), Time Domain Reflectometry (TDR).
- Compliant Standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s.
- Power: AC 120/230 V (50/60 Hz).
- Dimensions (WxDxH): 44,3 x 29,5 x 4,4 cm.
- Weight: 4.6 kg.

### 2.1.4 Access-point: Cisco-Linksys WRT300N Wireless-N Broadband Router

Figure 5. Multilayer Switch Layer 3

**Description:** The Cisco-Linksys WRT300N Wireless-N Broadband Router is an access point designed to deliver reliable and high-speed wireless networking. Equipped with four Ethernet ports for wired connections and advanced security features such as WPA and WPA2 encryption, it ensures secure and seamless connectivity for a variety of devices. With an intuitive web-based interface for configuration and management, the WRT300N allows users to easily set up and customize their wireless network settings, making it a user-friendly solution for those seeking a reliable and feature-rich wireless access point.

**Specification:**

- Throughput: 540 Mbps.
- Data process with Layer 7 application fingerprinting and QoS.

- Integrate with firewall.
- Air Marshal: Real-time WIPS (Wireless intrusion prevention system) with alarm.
- Each device is designed for high-density access to more than 100 users per device without bottlenecks, or processor crashes like conventional products. In addition, the device has traffic shapping technology to ensure that bandwidth is shared fairly between users.
- With Plug and Play technology, administrators only need to plug a new device into a power source, which will automatically tune in to devices of the same network and transmit waves to create an extended broadcast area without having to go through complicated configuration steps.
- Avoid common configuration errors of most wireless networks today. Devices without controllers when set to the same frequency band located close to each other will interfere with each other, which affect the performance and stability of the wireless network.

### 2.1.5 Cisco Firewall ASA 5540

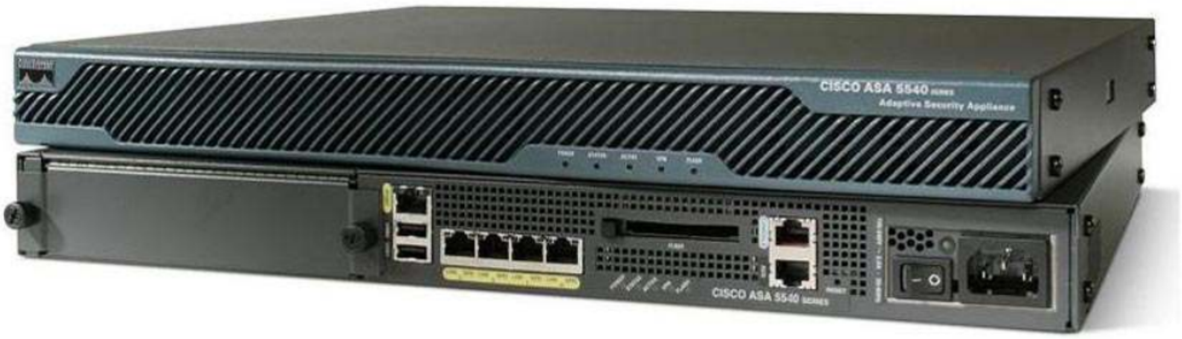


Figure 6. Cisco Firewall ASA 5540

**Description:** The Cisco ASA 5540 is a robust firewall appliance designed to provide advanced security features for medium to large-scale enterprise networks. Operating within the Adaptive Security Appliance (ASA) family, it combines firewall capabilities with VPN (Virtual Private Network) functionality and intrusion prevention features. With a high firewall throughput and VPN performance, the ASA 5540 offers reliable protection against a wide range of threats. It supports multiple security contexts, allowing the creation of virtual firewalls within a single physical appliance, enhancing network segmentation and security policy enforcement. The appliance includes features such as stateful inspection, application layer filtering, and advanced threat detection to safeguard network traffic.

**Specification:**

- Firewall Throughput: Up to 650 Mbps
- Maximum Firewall and IPS: Up to 500 Mbps with AIP SSM-20, Up to 650 Mbps with AIP SSM-40

- VPN Throughput: Up to 325 Mbps
- IPsec VPN Peers: 5000
- Virtual interfaces (VLANs): 200
- Concurrent sessions : 400000

## 2.2 Schematic physical setup of the network

### 2.2.1 The Headquarters:

| VLAN | Name | Network address | IP range |
|---|---|---|---|
| VLAN2 | SERVERLAN | 192.168.1.0/24 | 192.168.1.10 ⟶ 192.168.1.109 |
| VLAN10 | HQ_1 – IT | 192.168.10.0/24 | 192.168.10.10 ⟶ 192.168.10.109 |
| VLAN20 | HQ_2 | 192.168.20.0/24 | 192.168.20.10 ⟶ 192.168.20.109 |
| VLAN30 | HQ_3 | 192.168.30.0/24 | 192.168.30.10 ⟶ 192.168.30.109 |
| VLAN40 | HQ_4 | 192.168.40.0/24 | 192.168.40.10 ⟶ 192.168.40.109 |
| VLAN50 | HQ_5 | 192.168.50.0/24 | 192.168.50.10 ⟶ 192.168.50.109 |
| VLAN60 | HQ_6 | 192.168.60.0/24 | 192.168.60.10 ⟶ 192.168.60.109 |
| VLAN70 | HQ_7 | 192.168.70.0/24 | 192.168.70.10 ⟶ 192.168.70.109 |
| VLAN80 | GUEST | 192.168.80.0/24 | 192.168.80.10 ⟶ 192.168.80.109 |

Figure 7. VLAN Schematic of The Headquarters

### 2.2.2 First Branch (DA NANG):

| VLAN | Name | Network address | IP range |
|---|---|---|---|
| VLAN2 | SV_BR1 | 172.168.1.0/24 | 172.168.1.10 ⟶ 172.168.1.109 |
| VLAN10 | IT_BR1 – IT | 172.168.10.0/24 | 172.168.10.10 ⟶ 172.168.10.109 |
| VLAN20 | BR1_2 | 172.168.20.0/24 | 172.168.20.10 ⟶ 172.178.20.109 |
| VLAN30 | BR1_3 | 172.168.30.0/24 | 172.168.30.10 ⟶ 172.168.30.109 |
| VLAN40 | BR1_4 | 172.168.40.0/24 | 172.168.40.10 ⟶ 172.168.40.109 |
| VLAN50 | BR1_GUEST | 172.168.50.0/24 | 172.168.50.10 ⟶ 172.168.50.109 |

Figure 8. VLAN Schematic of The First Branch

### 2.2.3 Second Branch (HA NOI:

| VLAN | Name | Network address | IP range |
|---|---|---|---|
| VLAN2 | SV_BR2 | 182.168.1.0/24 | 182.168.1.10 ⟶ 182.168.1.109 |
| VLAN10 | IT_BR2 – IT | 182.168.10.0/24 | 182.168.10.10 ⟶ 182.168.10.109 |
| VLAN20 | BR2_2 | 182.168.20.0/24 | 182.168.20.10 ⟶ 182.178.20.109 |
| VLAN30 | BR2_3 | 182.168.30.0/24 | 182.168.30.10 ⟶ 182.168.30.109 |
| VLAN40 | BR2_4 | 182.168.40.0/24 | 182.168.40.10 ⟶ 182.168.40.109 |
| VLAN50 | BR2_GUEST | 182.168.50.0/24 | 182.168.50.10 ⟶ 182.168.50.109 |

Figure 9. VLAN Schematic of The Second Branch

## 2.3 WAN connection diagram between Headquarters and Branches ((using new WAN technology such as SD-WAN, MPLS and OSPF routing protocol)

### 2.3.1 Features of each routing protocol

The choice between SD-WAN (Software-Defined Wide Area Network), MPLS (Multiprotocol Label Switching), and OSPF (Open Shortest Path First) routing protocol depends on various factors, including the specific requirements of the network, the level of control and visibility needed, and the organization's budget considerations. Below is the comparasion between multiple WAN connection:

**SD-WAN:**

- Advantages:
  - Flexibility: SD-WAN is like a networking superhero, using smart software to adapt easily.
  - Cost Savings: It can use different internet types, saving money and boosting performance.
  - Easy Control: Management is like having a central command center, making things simpler.
  - Better Apps: It directs traffic smartly, making applications work faster and smoother.
- Disadvantages:
  - Overlay Challenge: It relies on another layer, so the quality depends on the base network.
  - Learning Curve: Getting used to it might take some time and effort.

**MPLS:**

- Advantages:
  - Built-in Security: Adds a safety layer, keeping things secure.
  - Traffic Priority: Can prioritize important data for better service.
  - Secure Connections: Links multiple places securely.
- Disadvantages:
  - Costly Choice: Can be pricier, especially for big setups.
  - Takes Time: Setting up may take longer compared to SD-WAN.

**OSPF:**

- Advantages:
  - Adaptable Routes: Like a flexible GPS, it adjusts paths based on network changes.
  - Good for Bigger Networks: Works well for medium to large setups with complex designs.
  - Quick Adaptation: Responds fast to network changes.
  - Inside the Company Roads: Usually used for routes within a company.
- Disadvantages:
  - Plan Well: Needs careful design to avoid confusion in routes.
  - Not a Traffic Expert: Doesn't specialize in managing different types of data like SD-WAN.

**Conclusion:** We want to optimize the suggestion options with the development in the next 5 years therefore Scalability is vital for our design connection which OSPF is scalable and can support large and complex networks. It is suitable for organizations with multiple branches and a hierarchical structure, making it a good choice for connecting branch offices to headquarters. Moreover, the dataflows and workload of the system (about 80% at peak hours 9g-11g and 15g-16g) can be shared for Head Office and Branch so OSPF supports load balancing, allowing the distribution of traffic across multiple paths. This is beneficial in scenarios where multiple links connect branch offices to the headquarters, as OSPF can intelligently balance the traffic load to optimize network performance.

### 2.3.2 Wiring diagram the connection between Headquarters and Branches

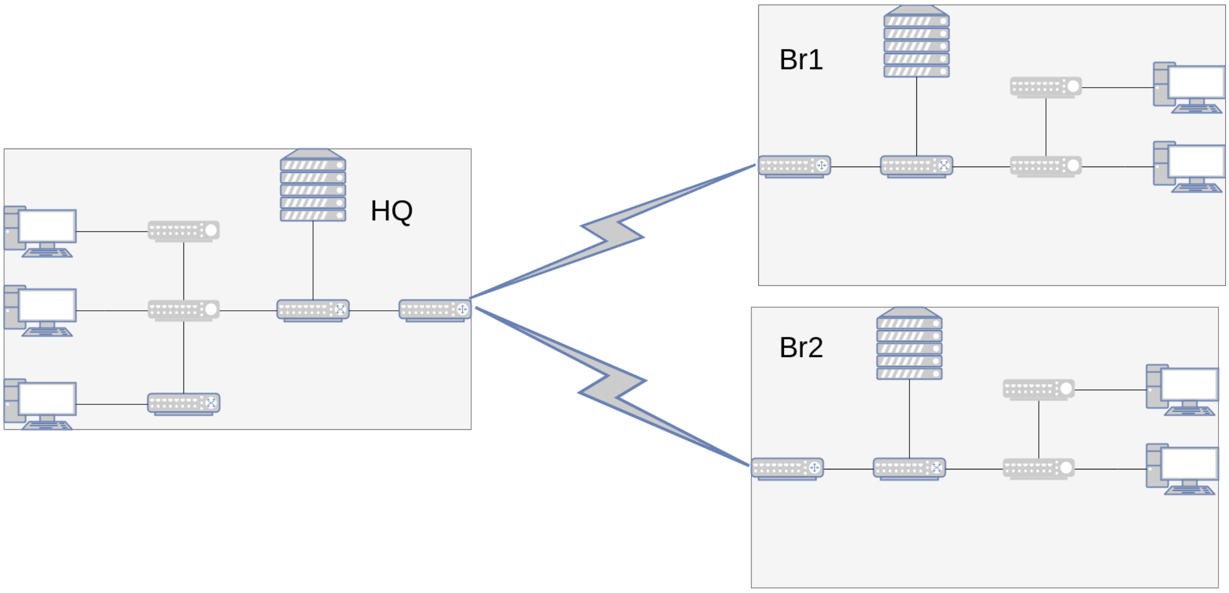


Figure 10. Wiring diagram the connection between Headquarters and Branches

# 3 Calculate the necessary throughput and bandwidth for the system

As given in the requirements:

- Each server's download estimate is 1000 MB/day and the upload estimate is 2000 MB/day. Therefore total is 3000 MB/day.
- Each workstation's download estimate is 500 MB/day and the upload estimate is 100 MB/day. Therefore total is 600 MB/day
- WiFi-connected devices from customers' access make up about 500 MB/day of upload and download.
- About 80 percent of the load is at the peak hours from 9am to 11am and from 3pm to 4pm.

## 3.1 Headquarter

The headquarter hosts 120 workstations and 5 servers. We can estimate the daily throughput of the headquarter's network to be:

$$\text{Throughput}_{\text{Headquarter}} = 600 \times 120 + 3000 \times 5 + 500 = 87500(\text{MB})$$

The bandwidth required at peak hours should then be:

$$\text{Bandwidth}_{\text{Headquarter}} = \frac{87500 \times 2^3 \times 0.8}{3 \times 3600} \approx 51.9 \text{ (Mbps)}$$

With the 20% growth in the future in mind, using 100Mbps interfaces on the routers should suffice as the peak bandwidth required will be $51.9 \times 1.2 \approx 62.28$(Mbps).

## 3.2 Branch

The branch hosts 30 workstations and 3 servers. We can estimate the daily throughput of the headquarter's network to be:

$$\text{Throughput}_{\text{Branch}} = 600 \times 30 + 3000 \times 3 + 500 = 27500(\text{MB})$$

The bandwidth required at peak hours should then be:

$$\text{Bandwidth}_{\text{Branch}} = \frac{27500 \times 2^3 \times 0.8}{3 \times 3600} \approx 16.3 \text{ (Mbps)}$$

With the 20% growth in the future in mind, using 100Mbps interfaces on the routers should suffice as the peak bandwidth required will be $16.3 \times 1.2 \approx 19.6$ (Mbps).

# 4 Design the network map using Packet Tracer

## 4.1 Headquarters

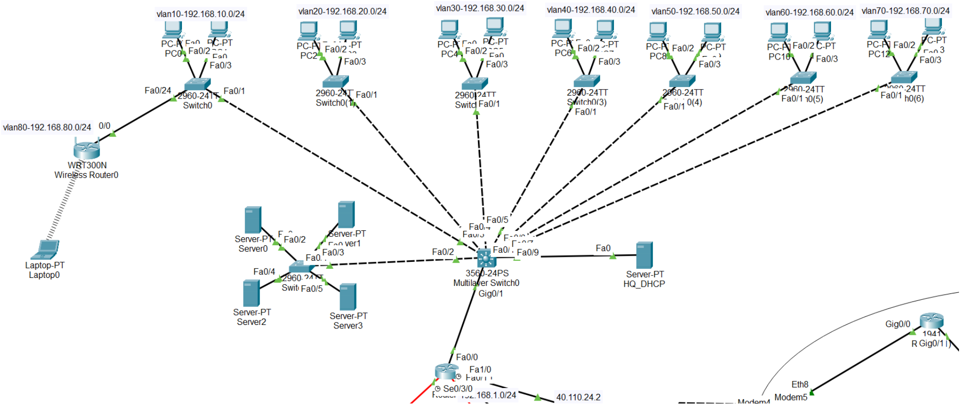


Figure 11. The Headquarters

## 4.2 Branch 1(DA NANG)

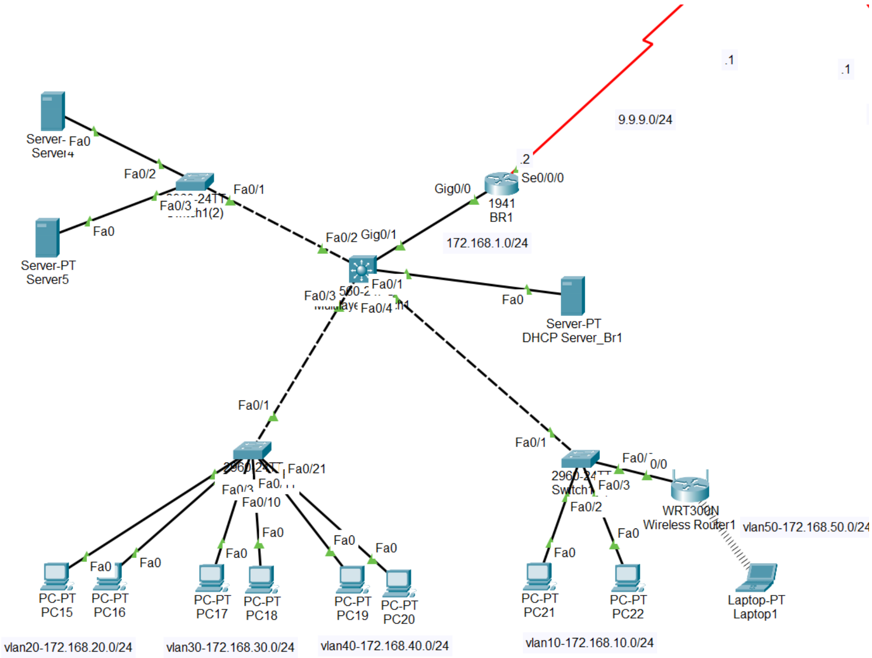


Figure 12. Branch 1(DA NANG)

## 4.3 Branch 2(HA NOI)

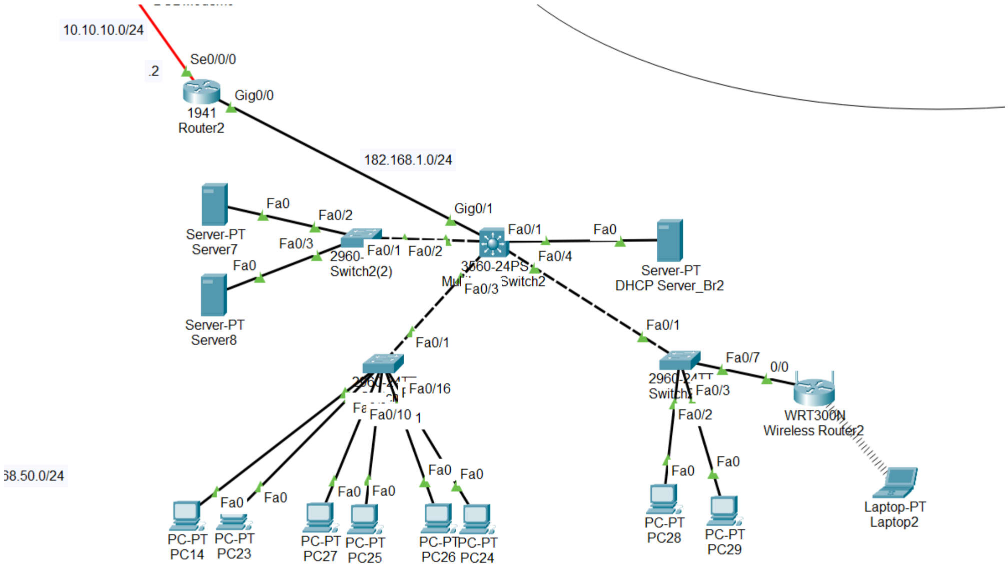
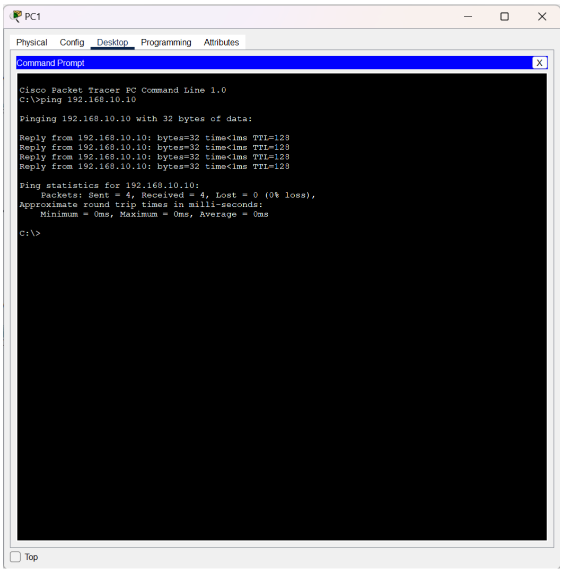


Figure 13. Branch 2(HA NOI)

# 5 Test on simulated system

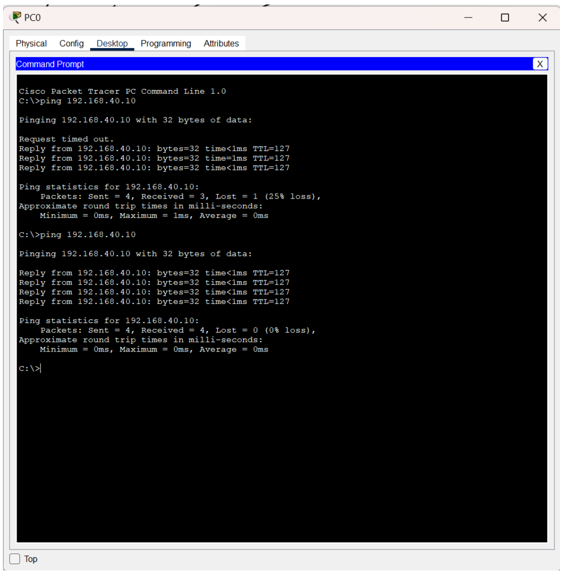
## 5.1 Connection in the same VLANS in Headquarter



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 14. Connection in the same VLAN in Headquarter

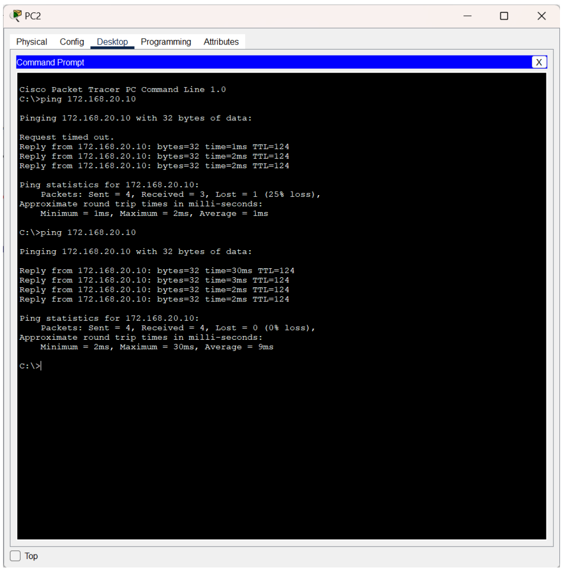
## 5.2 Connection between different VLANS in Headquarter



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.40.10

Pinging 192.168.40.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.10: bytes=32 time<1ms TTL=127
Reply from 192.168.40.10: bytes=32 time=1ms TTL=127
Reply from 192.168.40.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.40.10

Pinging 192.168.40.10 with 32 bytes of data:

Reply from 192.168.40.10: bytes=32 time<1ms TTL=127
Reply from 192.168.40.10: bytes=32 time<1ms TTL=127
Reply from 192.168.40.10: bytes=32 time<1ms TTL=127
Reply from 192.168.40.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 15. Connection between different VLANS in Headquarter

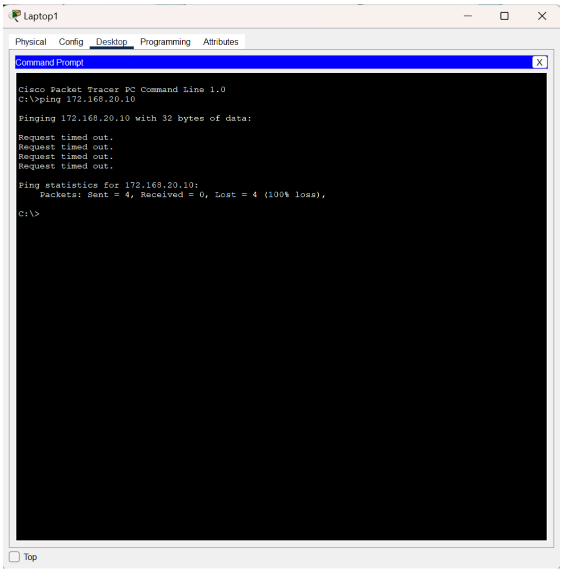
## 5.3 Connection between Headquarters and Branches



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.168.20.10

Pinging 172.168.20.10 with 32 bytes of data:

Request timed out.
Reply from 172.168.20.10: bytes=32 time=1ms TTL=124
Reply from 172.168.20.10: bytes=32 time=2ms TTL=124
Reply from 172.168.20.10: bytes=32 time=2ms TTL=124

Ping statistics for 172.168.20.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 172.168.20.10

Pinging 172.168.20.10 with 32 bytes of data:

Reply from 172.168.20.10: bytes=32 time=30ms TTL=124
Reply from 172.168.20.10: bytes=32 time=3ms TTL=124
Reply from 172.168.20.10: bytes=32 time=2ms TTL=124
Reply from 172.168.20.10: bytes=32 time=2ms TTL=124

Ping statistics for 172.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 30ms, Average = 9ms

C:\>
```

Figure 16. Connection between Headquarters and Branches

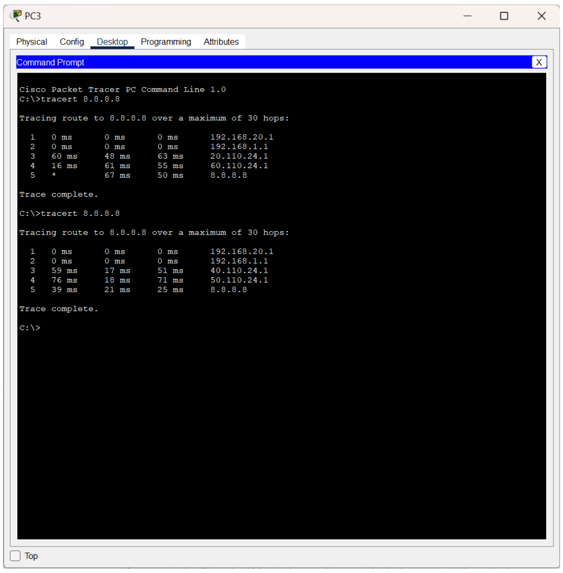
## 5.4 No connections from Customers' devices to PCs on the VLAN



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.168.20.10

Pinging 172.168.20.10 with 32 bytes of data:

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

Ping statistics for 172.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 17. No connections from Customers' devices to PCs on the VLAN

### 5.5 Connect to the Internet



```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.20.1
  2   0 ms      0 ms      0 ms      192.168.1.1
  3   60 ms     48 ms     63 ms     20.110.24.1
  4   16 ms     61 ms     55 ms     60.110.24.1
  5   *         67 ms     50 ms     8.8.8.8

Trace complete.

C:\>tracert 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.20.1
  2   0 ms      0 ms      0 ms      192.168.1.1
  3   59 ms     17 ms     51 ms     40.110.24.1
  4   76 ms     18 ms     71 ms     50.110.24.1
  5   39 ms     21 ms     25 ms     8.8.8.8

Trace complete.

C:\>
```

Figure 18. Connect to the Internet

# 6 Re-evaluate the designed network system

## 6.1 The remaining problems

- We have not configured any firewall and DMZ, so the security of the system is extremely weak and traffic from the Internet can access enterprises's network.
- We only apply access control list for customer's wireless network.
- Although capable of expanding the network, this entirely depends on the operation ability of the central department. Once the center encounters an issue (total switch or router), the entire network system will not be able to function.
- We don't have specific knowledge about a particular enterprise network, so when designing, we encounter difficulties in deciding which models, technologies, and devices should be used.
- Inadequate background knowledge about networking standard makes the system messy and hard to debug.

## 6.2 Development orientation in the future

- The network architecture should be re-designed to provide a more structured and organized topology that allows for better traffic management and control.
- Access control policies should be implemented to control who has access to the network and what they are authorized to do. This can help prevent unauthorized access and reduce the risk of data breaches.