**NETWORKING CONCEPTS AND CYBER SECURITY**

**Module Code: COMP40002**

**RESEARCH REPORT: NETWORK ARCHITECTURE**

Group Assignment:

HAN23080227

HAN23080577

HAN23080330

HAN23070023

*#Word count: 1917*

**Content**

[I. Network Scenario 3](#_Toc1873522597)

[1. Scenario of our topology 3](#_Toc2066184033)

[2. Multi-site connection 3](#_Toc238918816)

[3. Online work (Topology) 4](#_Toc596560955)

[4. Data security (Access control list - who has access to what) 4](#_Toc353267601)

[5. Administration Control (Admin privilege) 4](#_Toc553181117)

[6. Solution 5](#_Toc1185561905)

[II. Network Requirements 6](#_Toc642042779)

[1. Switches 6](#_Toc1172946948)

[2. Routers 7](#_Toc359894436)

[3. End devices 7](#_Toc124345927)

[4. Servers 7](#_Toc1794947392)

[5. Wireless Devices 7](#_Toc186970313)

[III. OSI model and network configuration 7](#_Toc622334480)

[1. OSI model 7](#_Toc1002438960)

[2. IP address scheme 9](#_Toc1067645106)

[Hoan Kiem HQ: 9](#_Toc805828782)

[Dong Da: 11](#_Toc419107629)

[Cay Giay: 13](#_Toc991641979)

[Thanh Xuan 14](#_Toc573493569)

[Hai Ba Trung 15](#_Toc1175468772)

[3. Access Control Lists 16](#_Toc389517251)

[IV. WAN 17](#_Toc637958385)

[1. WAN connection 17](#_Toc956894669)

[2. Throughput Requirements 17](#_Toc1395724157)

[3. Available WAN Technologies 18](#_Toc100445819)

[a. ISP routers 18](#_Toc478907751)

[b. Ethernet cable to simulate the connection from the routers to the ISP 20](#_Toc1765147385)

[4. Security 20](#_Toc1173896115)

[5. Redundancy 21](#_Toc1528498985)

[6. NAT 21](#_Toc108883991)

[V. VLAN 21](#_Toc1127675767)

[1. How VLANs Work 21](#_Toc1549989595)

[2. Characteristics of VLANs 21](#_Toc912502427)

[3. Configuring VLANs 22](#_Toc910194409)

[4. Benefits of using VLANs 22](#_Toc1999235938)

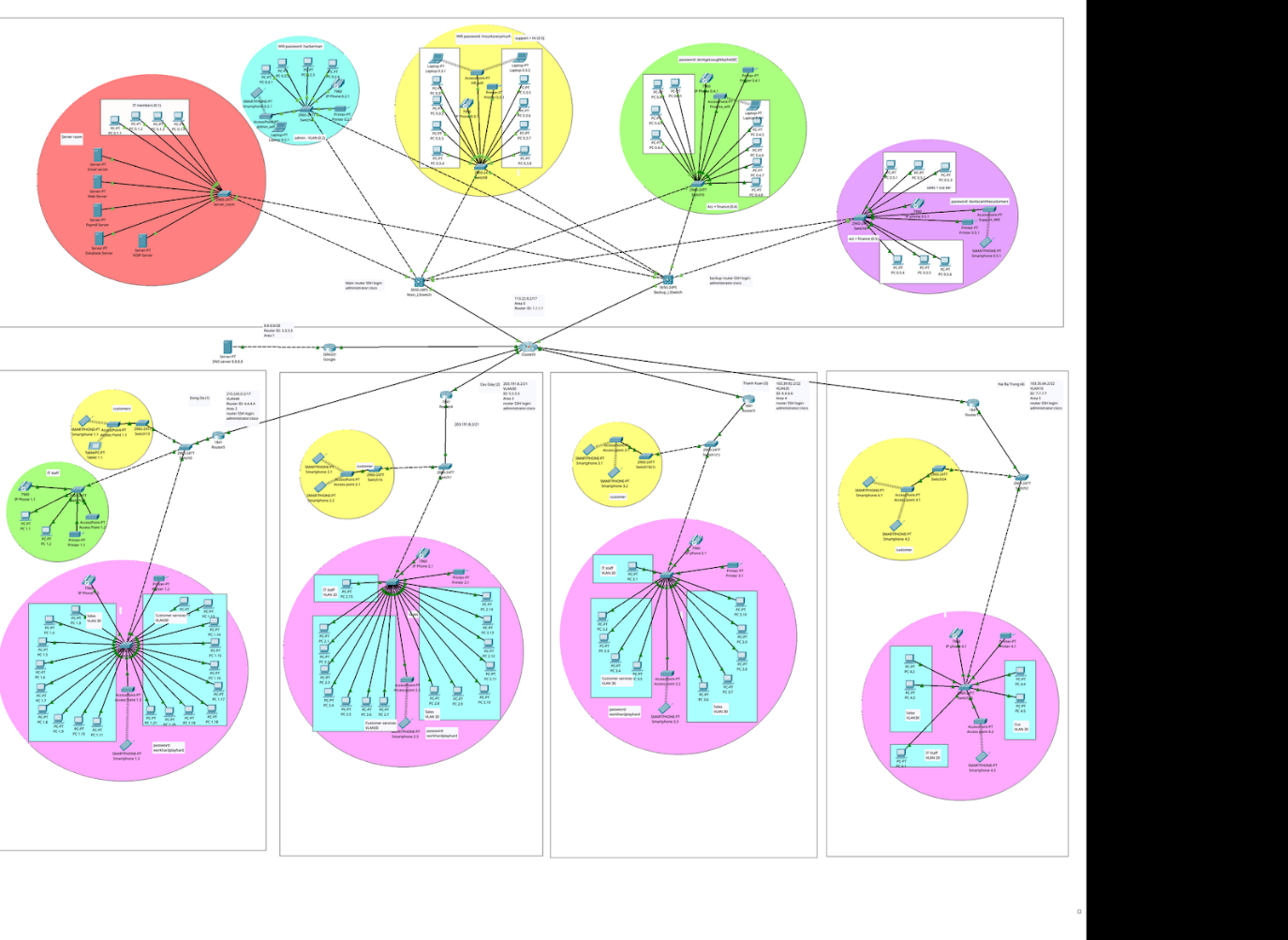
[VI. Cost 22](#_Toc1140156575)

[VII. Reference 30](#_Toc1292135805)

# 

# **Network Scenario**

## **Scenario of our topology**



*#Packet tracer topology*

## **Multi-site connection**

The multi-site connection allows an interconnection between different regions. This type of network is used to meet different business requirements, and most of them are Layer 2 (Data link) needs.

In the group's resolution, the multi-site connection was an obligatory and crucial requirement for the success of the project, since the *X company* was previously operating five physical stores across different districts and decided to close them in favor of launching online portals, with particular emphasis on the internal communication and remote workers. Consequently, all district portals must connect to each other, mainly with the Hoan Kiem, since it is the Internet and server's provider

## **Online work (Topology)**

Network topology refers to the physical and logical arrangement of a network (Referring to the connected computing devices). It illustrates the connections and positioning of various nodes, such as routers and switches, and how they are placed and interconnected.

The *X company*’s topology was organized, firstly, by dividing the five districts. In this district division, a separate VLAN (Virtual local area network) was created for each district. Inside each VLAN, the organization structure was based on departmental and functional divisions such as sales, customer services, support, IT members, finance, accounts, HR. So, for each one of them, there is a separate VLAN. Another noticeable common point in each district is the presence of end-devices (IP phones, printers, and computers) and network devices (Routers, switches, multilayer switches, access points).

## **Data security (Access control list - who has access to what)**

Securing a network, especially data, involves recommended deployment techniques as access control lists (ACLs), which are implemented to minimize the risks of direct attacks on the infrastructure, by allowing only authorized traffic to access the infrastructure equipment. The ACL functions by establishing a series of rules that dictate which network traffic is allowed or not.

The data security established for the X company was based on implementing stringent access controls to prevent unauthorized individuals from gaining access to the payroll and database servers. The ACL configuration was established only in the Hoan Kiem district, Using the ACL in the multilayer switch, it was configured the blocking access for the VLANs 30 and 50 (Any other department besides the IT, account & finance, and admin departments) in relation to the IP Addresses 192.168.1.6 (Payroll servers) and 192.168.1.7 (Database servers).ACL information from CLI

## **Administration Control (Admin privilege)**

The Administration control, often referred to as admin privileges, grants the user access and authority to the network’s system’s settings, resources, and security. In the X company’s situation, it was decided to use the SSH (Secure Shell) protocol to provide a secure, remote connection to a device over an unsecured network (such as the Internet).

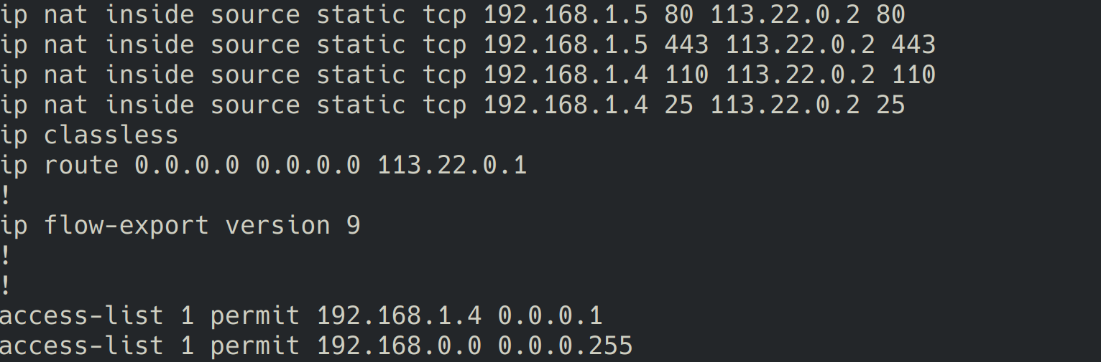
In *X company*’s topology, the protocol SSH was configured in the terminal CLI, configured with the layer 3 switches (For Hoan Kiem) and routers (Other Branches). It basically created a necessary username (administrator) and password (cisco) for the server, router and layer 3 switches.

## **Solution**

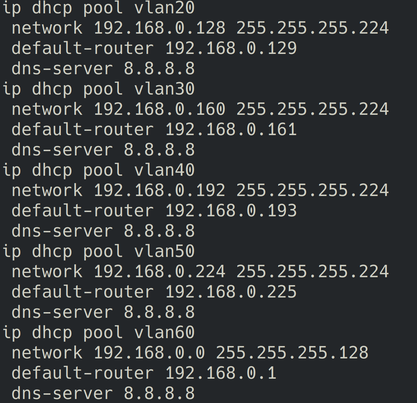
According to the *X company*’s requirements, all five online portals need to be connected to each other, all employees are going to work remotely, and all customers will have access to the e-sales system. Besides, it is necessary that our group develop a design for the network design, and documentation with the network equipment specifications, network configuration, and internal communication.

For the three first requirements of *X company,* it was decided to handle the online portals, employees working remotely and the access for all customers to the e-sales system, creating a main website that hosts the portals, the employees will have a specific login, and the customers are going to have a different login to access the e-sales.

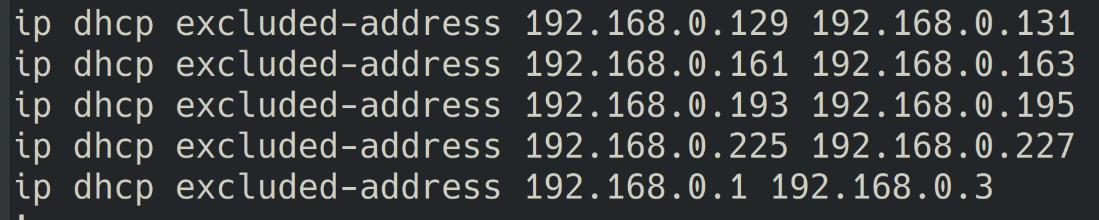
About the solution with the website, we decided to, via the web server, host the HTML file. Configure the port address translation (PAT) to the second ISP router. About the PAT configuration, we configured port 80 and 443 for the web server, and port 25 and 110 for the email server. Then we employed Port Address Translation to globally translate all end-devices on the second WAN IP address. Additionally, we utilized DHCP to automatically allocate the 8.8.8.8 DNS server to each end device on the layer 3 (network) switches.



*#PAT information from the CLI*



*#DHCP configuration 1*



*#DHCP configuration 2*

# **Network Requirements**

This section illustrates the network equipment that is utilized in the topology, followed by a brief explanation of these devices:

## **Switches**

In a small business network, switches create a connection between computers and other devices. A switch enables communication and exchange of data between internal devices.In the topology, it plays as an essential factor of network hardware for establishing connection between devices in the network, including [Switch 2960] and [Multi Switch 3650]. (Cisco, n.d.)

## **Routers**

A router device acquires and transmits data in a single area or across multiple locations. Routers are the combination of network switches and modems in terms of functionality. It connects these devices’ networks and forms a larger network. In the case of a network that works across multiple locations, the router allows devices and users access to the internet, or to create a business network. There are three types of routers used in the topology: [Router1841], [Router4331], [Router2621XM]. (Cisco, n.d.)

## **End devices**

End devices operate as an interface, allowing users to access the communication network. Each end device is identified by an address, transmitting messages from a source to the destination. In general, it creates transmission by using the address to locate the destination device. There are three types of end devices used in the topology: [Printer], [VoIP Phone], [Smart Phone & Laptop]. (Cisco, n.d.)

## **Servers**

Email server: POP3 and SMTP

Web server: HTTP and HTTPS

Payroll server: SQL

Database Server: SQL

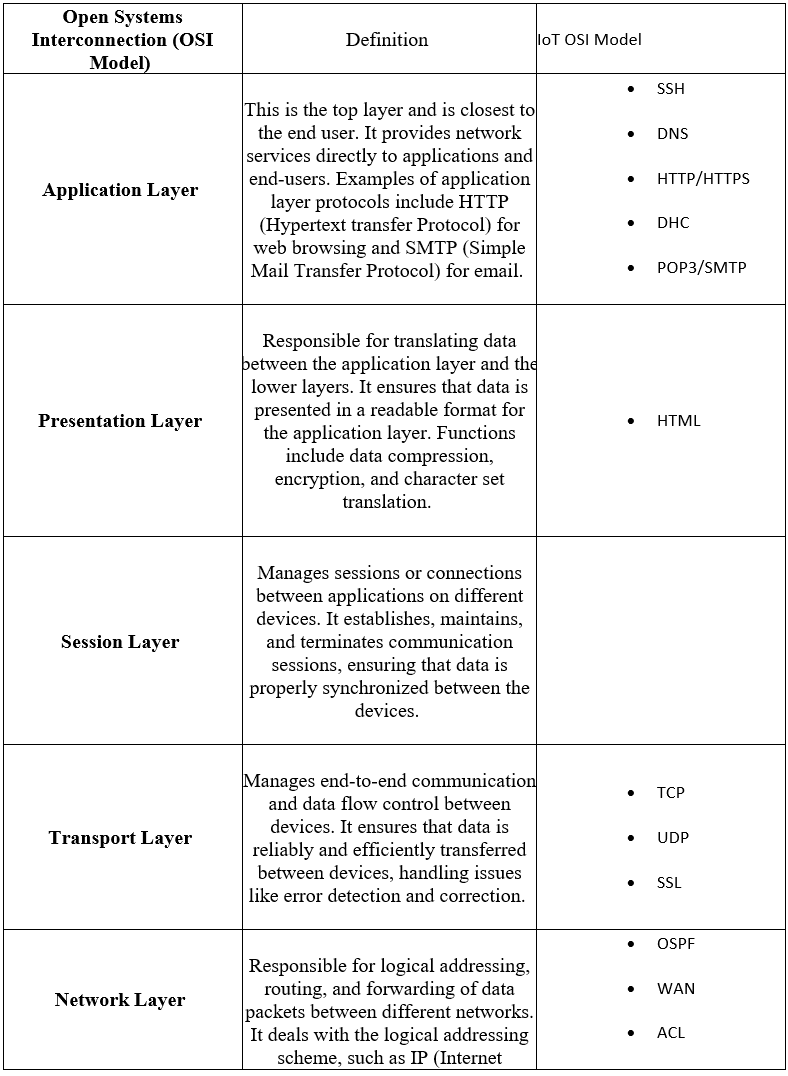
VIOP Server – serves Cisco VOIP

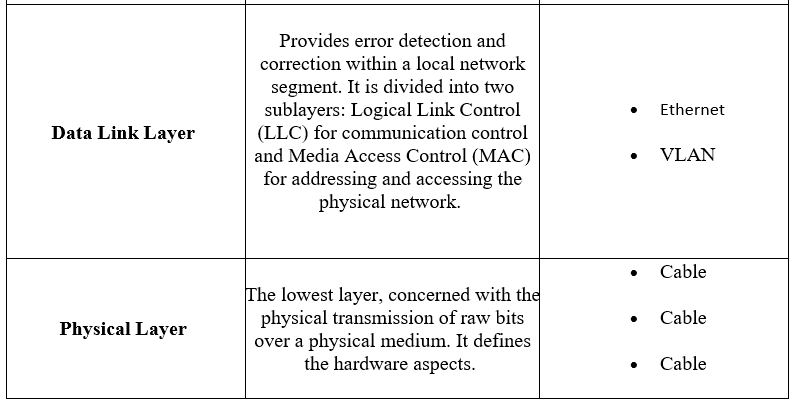
## **Wireless Devices**

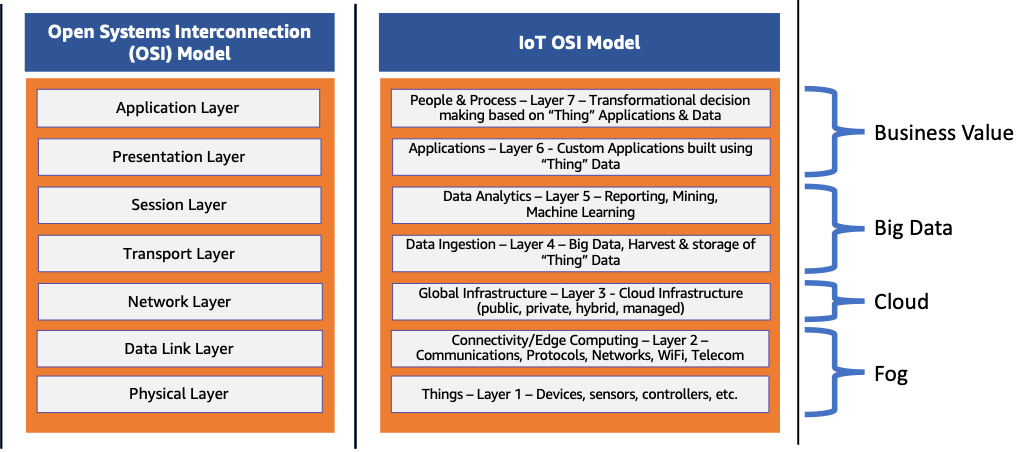
Light Weight Access Point – generic

# **OSI model and network configuration**

## **OSI model**







*#OSI Model layers* (AWS, n.d.)

## **IP address scheme**

### **Hoan Kiem HQ:**















### **Dong Da**:











### **Cay Giay**:









### **Thanh Xuan**








### **Hai Ba Trung**



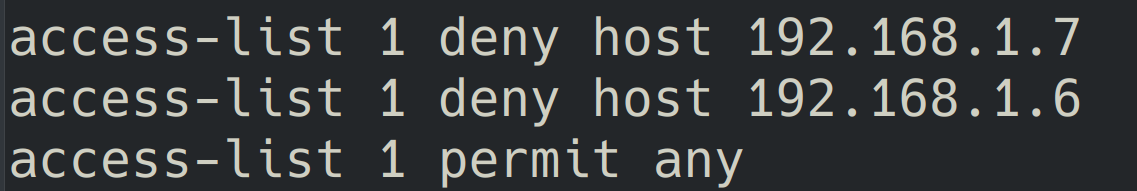








## **A**ccess Control Lists



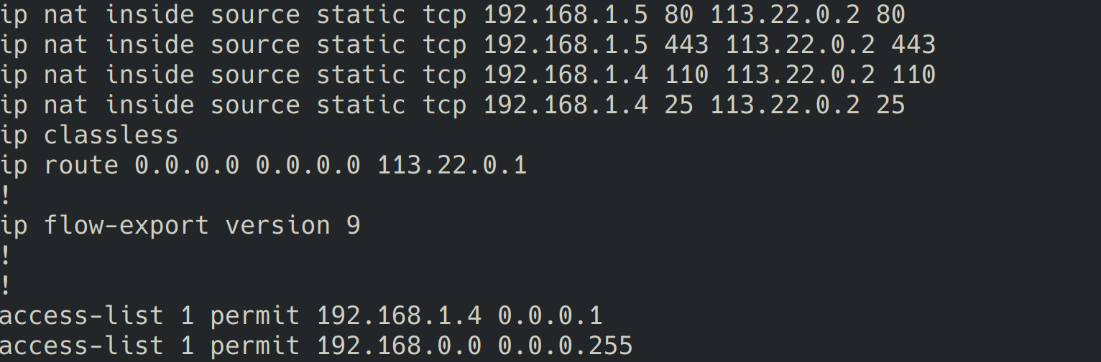
*#ACL configuration*

Admin: All Access

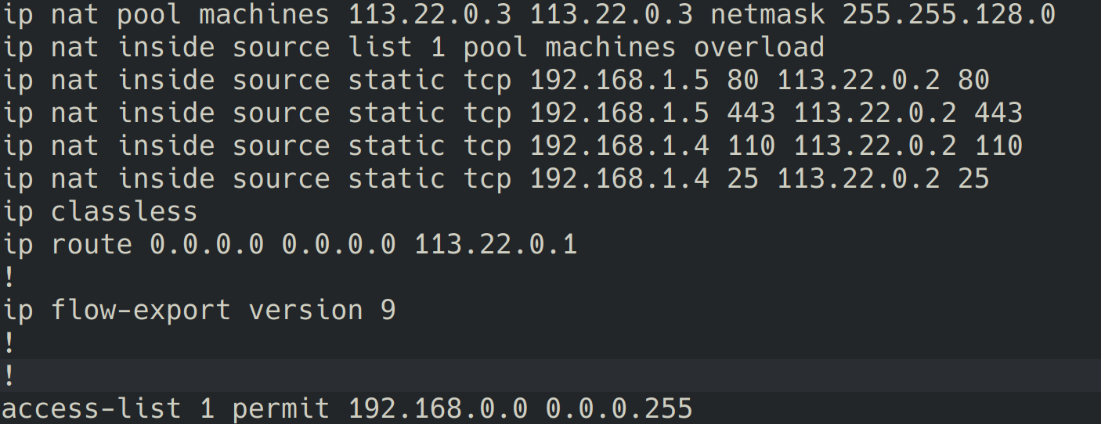
Database: Admin and IT members only

Payroll: Admin and Finance department only

1. NAT and PAT configuration



*#PAT config for the Servers*



*#PAT config for the end devices*

# **WAN**

## **WAN connection**

Overall, the WAN (Wide-area network) is a compilation of local-area networks (LANs) and networks that communicate with one another. (Cisco, n.d.)

In the topology, WAN is organized by dividing the districts into branches, then, defines the internal division of networks in each branch. The implementation of the VLAN segmentation strategy (Each department is associated with a VLAN and a specific network address) is applied to divide accordingly to each department.

The connection between the districts (branches) is defined by interconnectivity among the network devices (Routers, cluster, and multilayer switches). Firstly, the utilization of the protocol OSPF (Open Shortest Path First) is applied to route and create the connections between the routers inside the topology. Also, NAT (Network Address Translation) was used to assign a temporary public address to a private device for the duration of the communication.  
  
The multilayer switches function as the primary router, and there is a backup switch that activates in case the primary one goes offline.  
  
The cluster represents the WAN of the Internet service provider (ISP), and inside of it, we added 2 routers as the hub to connect all branches together.

## **Throughput Requirements**

The throughput requirements are related to the amount of data that the network can transmit within a specific time. Some factors that influence the throughput in the network are the network bandwidth, Packet loss, Network equipment performance, and Network latency.

## **Available WAN Technologies**

* 1. **ISP routers**

An Internet Service Provider (ISP) connects with a transmit provider to provide global internet access to customers. The ISP router, referred to as the “gateway” is a device that facilitates access to the internet.

The simulation of the internet was implemented mainly in the middle of the network topology. The cluster represents the public WAN/ISP. The 2 routers inside of the cluster are used as a hub to connect all branches. And connected to the cluster, the DNS server is utilized to translate the human-readable domain name (URL) into IP addresses. During the test processes, we pinged the DNS server and tried to ping the domain. After achieving this connection, we tested in the web browser by typing the domain and tested the email server by sending some emails from one device to another.   
  
A screenshot of a computer

Description automatically generated

*#The website*

A screenshot of a computer

Description automatically generated

*#The remote email*

* 1. **Ethernet cable to simulate the connection from the routers to the ISP**

The Ethernet cables are usually made of copper and used to connect devices in a wired LAN and WAN. As mentioned before, the idea was to simulate a connection with the internet with the DNS server and cluster. About the connection itself, we used the routers inside the cluster as hubs to connect all branches using the Ethernet cables.

## **Security**

The security related to the topology was based on the Access Control List (ACL), Admin privilege (Associated to login credentials - usernames & passwords),

## **Redundancy**

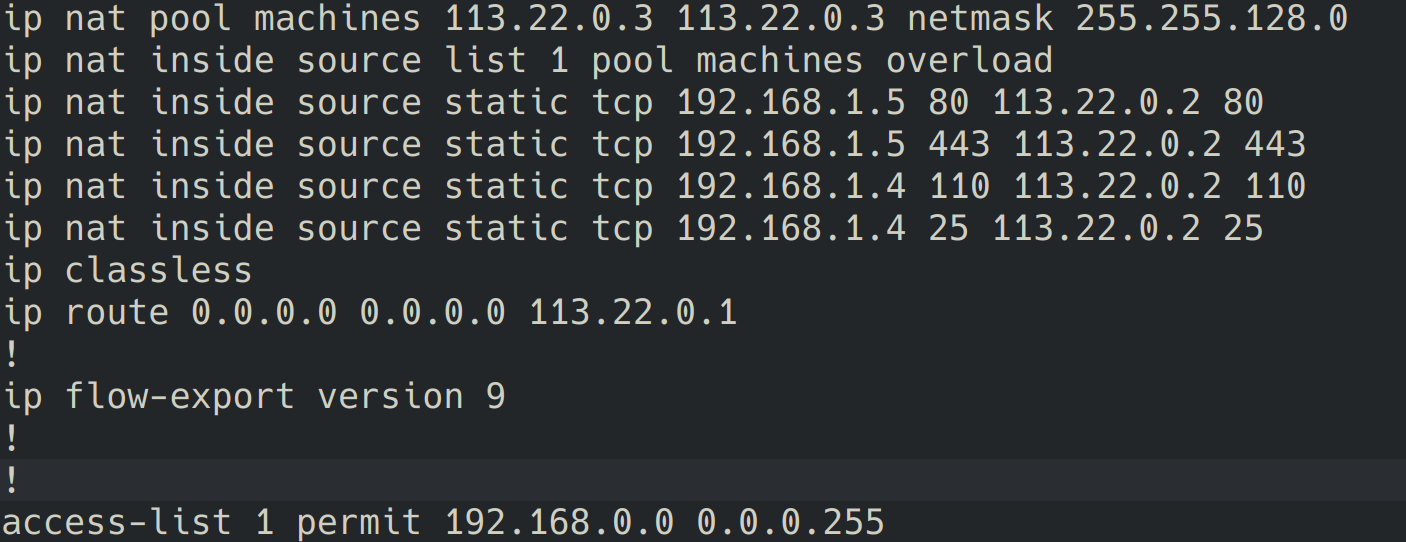
Configuring redundancy prevents open connections to failure or disruption, by connecting and replicating the information forwarding to the standby and extra network devices such as switches, routers, or multilayer switches.

In our topology, redundancy is specially implemented through the utilization of multilayer switches, comprising the main switch and its corresponding backup. Both have the same configuration, but the main switch periodically dispatches a “hello” messenger to the backup, to validate the standby status and maintain synchronization.

## **NAT**

The Network Address Translator (NAT) is a service that permits the private IP networks to use the internet and cloud. The NAT translates the private IP address of an internal network to a public IP address.

In our networking solution, for NAT we assigned the first IP to servers and then to devices.

*#NAT for Servers and devices*

# **VLAN**

## **How VLANs Work**

Virtual local area networks (VLAN) are groups of LANs (Local area networks) that are switched to each other. The VLANs are LANs that logically segment networks with physical networks.

## **Characteristics of VLANs**

VLAN are used to organize and logically segment the network, to isolate them, and to be flexible and scale. Also, they are usually associated with IP subnetworks.

In our network topology, we decided to create and divide the VLANs by the department division in each district. It is possible to see the division of each VLAN by the background circle colours and how each of them possesses a switch to connect to the other VLAN of the same branch.

## **Configuring VLANs**

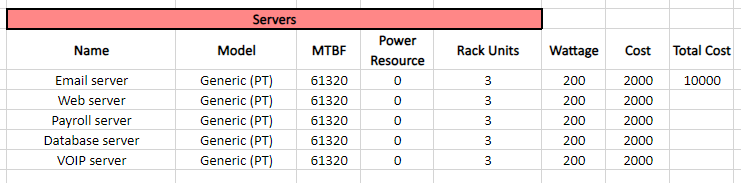
The VLAN configuration of our topology was, first, configured in the low-level routers (Each router in each district + The layer 3 switches), then, we decided to set the VLANs for the individual ports. Later, we set up the trunk port to the routers and layer 3 switches on a sticky (To allow the passage of multiple VLANs over a single). Afterward, we would set up all the VLANs on the router and layer 3 switches, DHCP, and HSRP too.

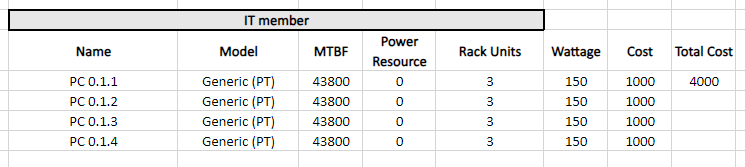
## **Benefits of using VLANs**

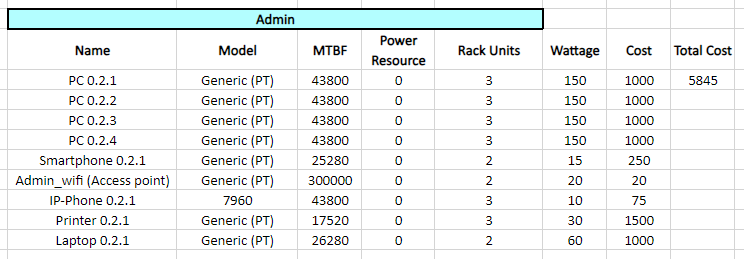
By dividing the network into separate logical areas, it is possible to organize the topology according to the criteria, and have more control of the division of each VLAN, it is also possible to isolate a specific VLAN, they are flexible and scalable.

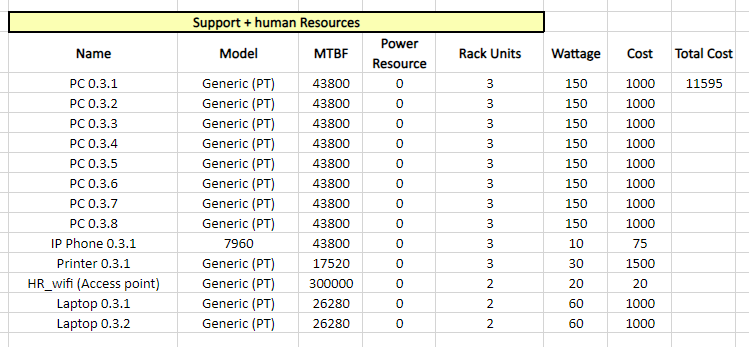
The benefits in our topology were related to the better organization by departments, the better control over each VLAN, the isolation of each department, and the association with the subnetwork.

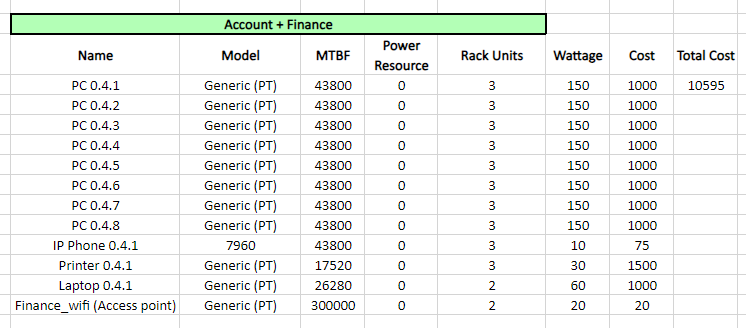
# **Cost**

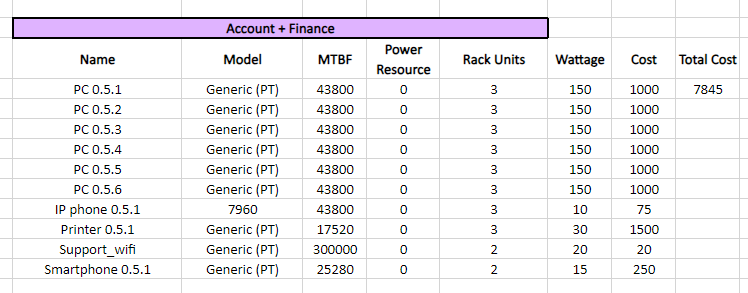






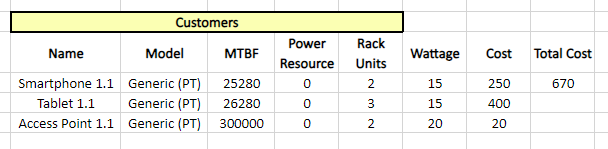


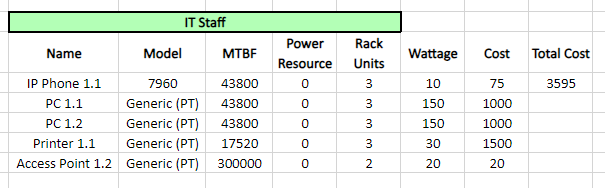


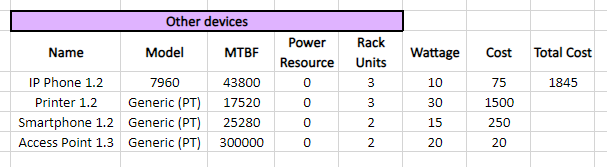


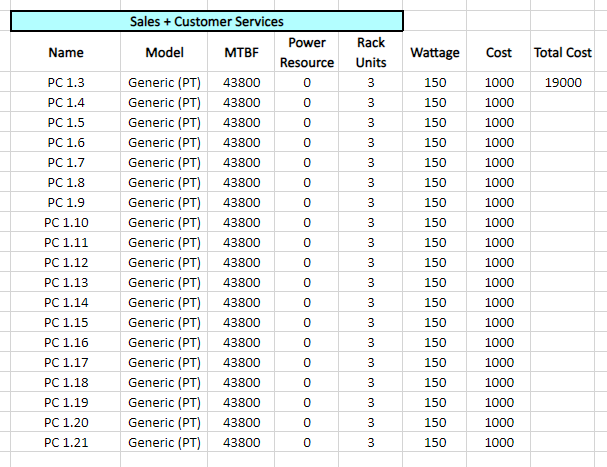


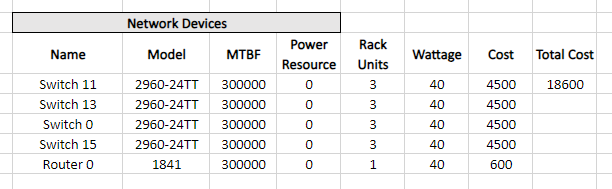
*#Branches Dong Da:*



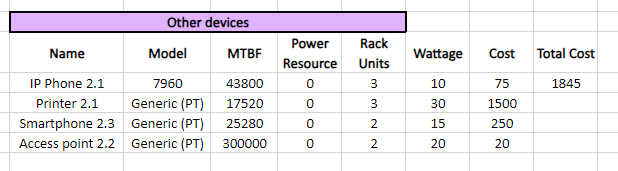
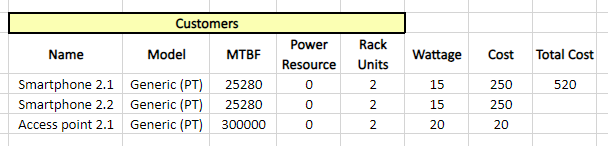


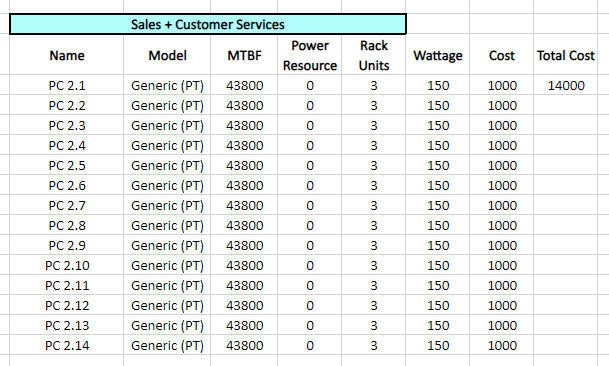


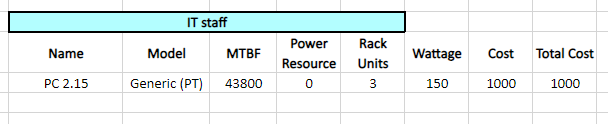


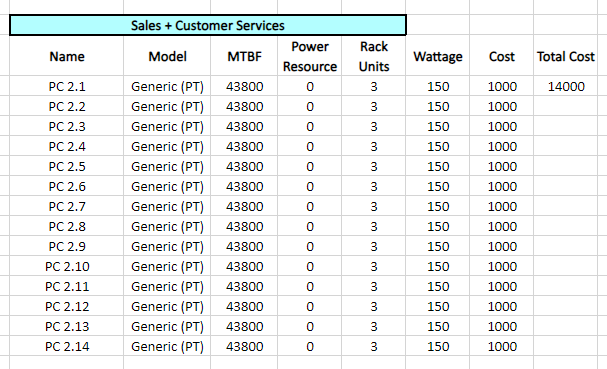


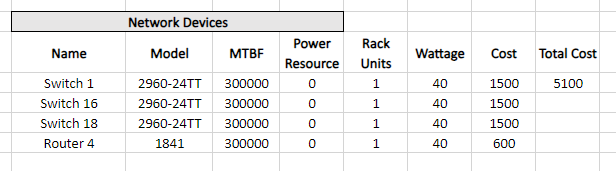
*#CAU GIAY:*



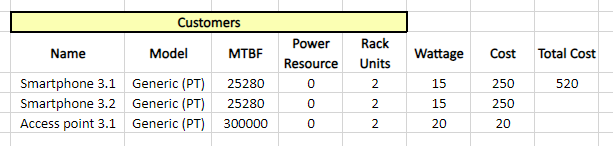


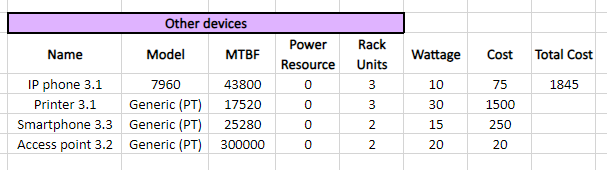


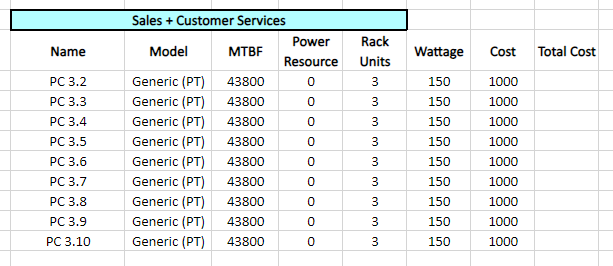


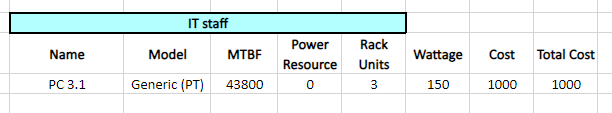


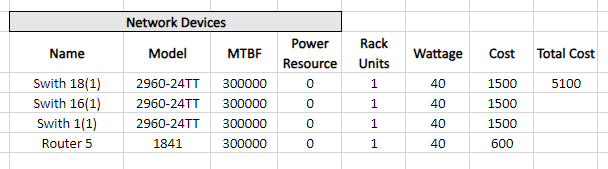
*#THANH XUAN:*



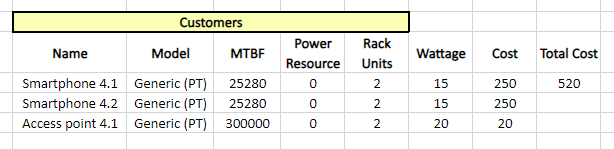


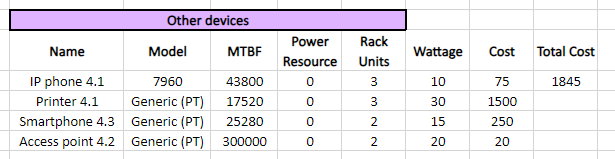


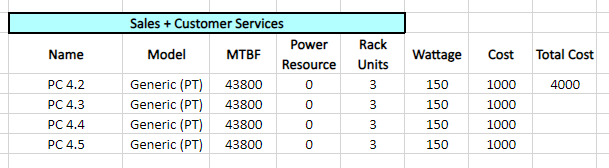


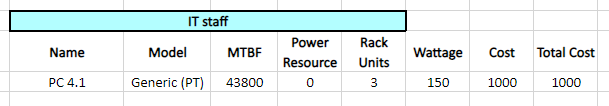


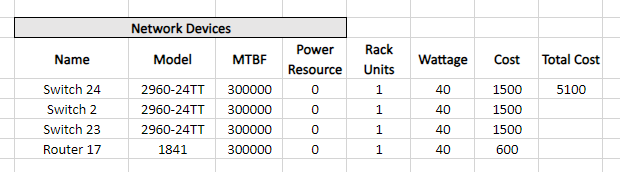
*#HAI BA TRUNG:*











# **Reference**

Cisco (2023a) *Cisco Access Control Lists (ACL)*, *Cisco Community*. Available at: <https://community.cisco.com/t5/networking-knowledge-base/cisco-access-control-lists-acl/ta-p/4182349> (Accessed: 15 December 2023).

Cisco (2023a) *Configure Network Address Translation*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html> (Accessed: 15 December 2023).

Cisco (2017) *Security configuration guide, Cisco Ios XE Release 3SE (Catalyst 3650 switches) - configuring Secure Shell (SSH) [Cisco Catalyst 3650 series switches]*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3se/security/configuration_guide/b_sec_3se_3650_cg/b_sec_3se_3650_cg_chapter_01000.html> (Accessed: 15 December 2023).

*Network switches* (2023) *Cisco*. Available at: <https://www.cisco.com/site/us/en/products/networking/switches/index.html> (Accessed: 15 December 2023).

*Configuring redundant connections* (2013) *Cisco*. Available at: https://www.cisco.com/c/en/us/td/docs/interfaces\_modules/services\_modules/csms/1-11/configuration/guide/redun.html#:~:text=With%20connection%20redundancy%2C%20the%20active,Purpose (Accessed: 15 December 2023).

Cisco (2023) *What is Network Address Translation (nat)?*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/products/routers/network-address-translation.html> (Accessed: 15 December 2023).

Cisco (2015) *Configuring vlans*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html#:~:text=A%20VLAN%20is%20a%20group,on%20the%20same%20LAN%20segment>. (Accessed: 15 December 2023).

Cisco (2015) *Configuring vlans*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html#:~:text=A%20VLAN%20is%20a%20group,on%20the%20same%20LAN%20segment>. (Accessed: 15 December 2023).

Cisco (2023c) *What is a wan? wide-area network*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html> (Accessed: 15 December 2023).

Cisco (no date) *Understanding and configuring Vlans - cisco*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.pdf> (Accessed: 15 December 2023).