

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH TRƯỜNG ĐẠI HỌC BÁCH  
KHOA KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH (CO3094)

---

ASSIGNMENT 2  
**Network Design And Simulation  
For A Critical Large Company**

---

Giáo viên hướng dẫn: Thầy Bùi Xuân Giang  
Sinh viên: Bùi Hoàng Quang Huy - 2153372 (NT)  
Nguyễn Đức Huy - 2152592  
Nguyễn Minh Hiếu - 2153343  
Nguyễn Hữu Nhật Minh - 2153575

THÀNH PHỐ HỒ CHÍ MINH, THÁNG 11 NĂM 2023

# Mục lục

<b>1</b>	<b>STEP 1</b>	<b>3</b>
1.1	Phân tích yêu cầu về hệ thống mạng của Trụ sở (Headquarter) và các chi nhánh (Branches)	3
1.2	Cấu trúc hạ tầng mạng của công ty . . . . .	3
1.3	Mô hình . . . . .	4
<b>2</b>	<b>STEP 2</b>	<b>5</b>
2.1	Schematic Physical Setup for the network . . . . .	5
2.1.1	Headquarter . . . . .	5
2.1.2	Branches . . . . .	7
2.2	List of devices required . . . . .	9
2.3	WAN Diagram . . . . .	12
<b>3</b>	<b>STEP 3</b>	<b>13</b>
3.1	Calculate the required throughput, and expected bandwidth from ISP . . . . .	13
3.1.1	Headquarter . . . . .	13
3.1.2	Branches . . . . .	13
3.2	Suggest the configuration for the company network . . . . .	14
3.2.1	Router . . . . .	14
3.2.2	Switch/Multilayer Switch . . . . .	15
3.2.3	Access Point . . . . .	15
<b>4</b>	<b>STEP 4</b>	<b>16</b>
4.1	Network Map using Packet Tracer . . . . .	16
<b>5</b>	<b>STEP 5</b>	<b>19</b>
5.1	Connect between PCs in the same VLAN . . . . .	19
5.2	Connect PCs between VLANs . . . . .	19
5.3	Connect PCs between Headquarters and branches . . . . .	21
5.4	Connect to server in the DMZ . . . . .	23
5.5	No connections from Customers' devices to PCs on the LAN . . . . .	26
5.6	Connect to the Internet to a Web Server . . . . .	26
<b>6</b>	<b>STEP 6</b>	<b>27</b>
6.1	Re-evaluate the designed network system . . . . .	27

## Danh sách Thành viên & Phân công Công việc

No.	Full name	ID	Duty in the assignment	Percentage of work
1	Bùi Hoàng Quang Huy	2153372	Kết nối PCs trong cùng VLAN, PCs giữa các VLAN, PCs giữa HQ và Chi nhánh, step 2, step 3 (Assignment 2)	25%
2	Nguyễn Minh Hiếu	2153343	Kết nối các server trong DMZ, ngăn kết nối từ máy khách tới LAN, kết nối internet đến web server, step 1, step 6 (Assignment 2)	25%
3	Nguyễn Đức Huy	2152592	Làm code, kiểm thử chương trình và tạo github (Assignment 1)	25%
4	Nguyễn Hữu Nhật Minh	2153575	Làm report, vẽ architecture, class diagram và gõ LaTeX (Assignment 1)	25%

## 1 STEP 1

### 1.1 Phân tích yêu cầu về hệ thống mạng của Trụ sở (Headquarter) và các chi nhánh (Branches)

Đối với Trụ sở chính:

- Tòa nhà trụ sở chính gồm 7 tầng, trong đó tầng 1 là nơi được chỉ định đặt phòng IT và Trung tâm cấp quang.
- Quy mô lắp đặt ở mức trung bình bao gồm: 120 máy trạm, 5 máy chủ và 12 thiết bị mạng hoặc nhiều hơn.
- Bảo đảm sử dụng kỹ thuật mới cho cả kết nối có dây và không dây. Trong đó, kết nối có dây sử dụng công nghệ cáp GPON và yêu cầu về kết nối hạ tầng mạng là 1GbE/10GbE.
- Hệ thống tổ chức theo VLAN, với mỗi tầng thì sẽ dùng 1 VLAN khác nhau, bảo đảm cả về bảo mật, xác thực và quyền truy cập. Tức là các máy trong nội bộ có thể truy cập dữ liệu lẫn nhau nhưng máy ở ngoài mạng thì không.
- Về kết nối Internet: mạng trung tâm kết nối với hệ thống Internet bên ngoài đường truyền ADSL và sử dụng 2 đường truyền Leased Line cho phép kết nối WAN.
- Công ty dùng kết hợp giữa Licensed và Open-Source SoftWare, ứng dụng văn phòng, ứng dụng client-server, cơ sở dữ liệu, ....
- Có hệ thống camera giám sát.
- Tỷ lệ phát triển của ngân hàng BB là 20 % trên 1 năm cho việc tăng cường số lượng nhân viên, số máy, ....

Đối với chi nhánh:

- Tòa nhà gồm 2 tầng, tầng 1 cũng trang bị 1 phòng IT và 1 Trung tâm Cấp quang.
- Quy mô nằm ở mức nhỏ: 30 máy trạm, 3 máy chủ, ít nhất 5 thiết bị mạng.

### 1.2 Cấu trúc hạ tầng mạng của công ty

- **Phân hệ theo kết nối Internet và truy cập từ xa:**

Phần này được trang bị các thiết bị kết nối Gateway Cisco Router riêng kết nối mạng Internet, cho phép nâng cấp và mở rộng tốc độ cổng kết nối khi cần phát triển. Người dùng truy cập mạng được xác thực để xác định quyền truy cập cho phép vào mạng nội bộ hoặc cơ sở dữ liệu hoặc Internet phục vụ khách hàng.

- **Phân hệ mạng DMZ:**

Gồm hệ thống máy chủ web, e-mail dành cho khách hàng, hệ thống giao dịch và tiện ích trên trang web của ngân hàng, internet banking, home banking, hệ thống đào tạo và dạy học điện tử cho nhân viên nội bộ, .... Máy chủ email cho các tài khoản khách hàng, máy chủ web có cài bộ lọc theo đề mục, nội dung và tại khu vực này cũng được trang bị các máy chủ virus để phòng chống mã độc hay virus xâm nhập thông tin thông qua đường truyền internet.

- **Phân hệ mạng nội bộ:**

Bao gồm các client đặt mọi nơi trong tòa nhà của cả trụ sở và chi nhánh, dành cho mọi nhân viên làm việc, duyệt web, gửi email, ....

- **Phân hệ máy chủ và ứng dụng:**

Các máy chủ ứng dụng chứa cơ sở dữ liệu cho các ứng dụng nên được bảo mật cao

- **Phân hệ quản trị mạng:**

Bao gồm máy chủ quản trị an ninh, máy chủ xác thực, máy chủ quét các dịch vụ trên mạng.

- **Phân hệ kết nối bên ngoài:**

Dành cho các kết nối đến từ các đơn vị bên ngoài hoặc bên ngoài truy cập vào mạng của ngân hàng

- **Phân hệ máy chủ cơ sở dữ liệu:**

Được đặt ở an ninh cao nhất vì đây là nơi chứa chứa toàn bộ dữ liệu quan trọng.

- **Phân hệ kết nối WAN:**

Kết nối mạng với cổng GateWay FireWall để bảo vệ các giao dịch từ bên ngoài đi vào mạng nội bộ.

### 1.3 Mô hình

Toàn bộ mạng của công ty được chia thành 1 LAN. Mạng này sẽ kết nối ra Router Trung tâm và Router chi nhánh, tại mỗi đầu Router tổng của cả trụ sở sẽ kết nối với FireWall GateWay rồi đi ra Internet.

Ở trụ sở chính:

- LAN được chia thành 7 LAN nhỏ cho mỗi tầng (7 VLAN):  
Tầng 1 (VLAN 10), tầng 2 (VLAN 20), tầng 3 (VLAN 30), tầng 4 (VLAN 40), tầng 5 (VLAN 50), tầng 6 (VLAN 60), tầng 7 (VLAN 70).
- Mỗi tầng cho 1 ban và chia ra n máy kết nối chung 1 switch layer 2 và các layer 2 sẽ được tổng hợp đường truyền dữ liệu vào một switch layer 3 vì số lượng workstation là khá nhỏ (chỉ mang quy mô trung bình). Khi cần thiết mở rộng thì ta sẽ thêm 1 switch layer 2 cho mỗi tầng và thêm 1 layer 3 để tổng hợp đường truyền (dùng LACP).
- Ta cũng sẽ cho lắp đặt hệ thống modem để phát mạng không dây cho toàn bộ tòa nhà, kết hợp với các access point để mở rộng vùng phủ sóng. Do đó chỉ thiết kế để đặt modem tại các tầng số lẻ của tòa nhà trụ sở.
- Ta sẽ dùng 1 switch tổng cho cả tòa nhà. Switch này là 1 switch layer 3 và được nối ra Router trung tâm (router này khi kết nối với server có đi qua Firewall). Switch này cho phép ta có thể cấu hình để nó cho phép hoặc không cho phép các VLAN truy cập lẫn nhau và được định tuyến rõ ràng cho các VLAN.
- Tầng 1 là nơi ta đặt toàn bộ server và các thiết bị mạng. Các tầng khác đều chứa 1 lượng các workstation tương đương nhau và ta xác định các máy này đều thuộc máy nội bộ (inside) nên cần được Firewall bảo vệ và đặt ở mức bảo mật cao nhất.

Ở chi nhánh: Sẽ được thiết kế tương tự trụ sở chính.

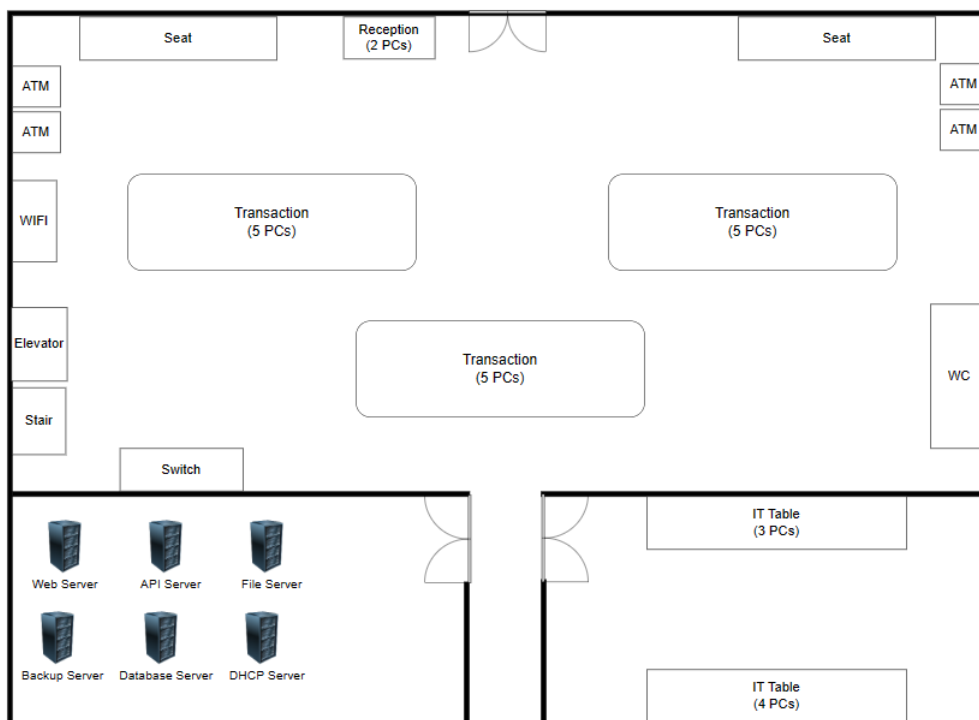
## 2 STEP 2

### 2.1 Schematic Physical Setup for the network

#### 2.1.1 Headquarter

##### Tầng 1

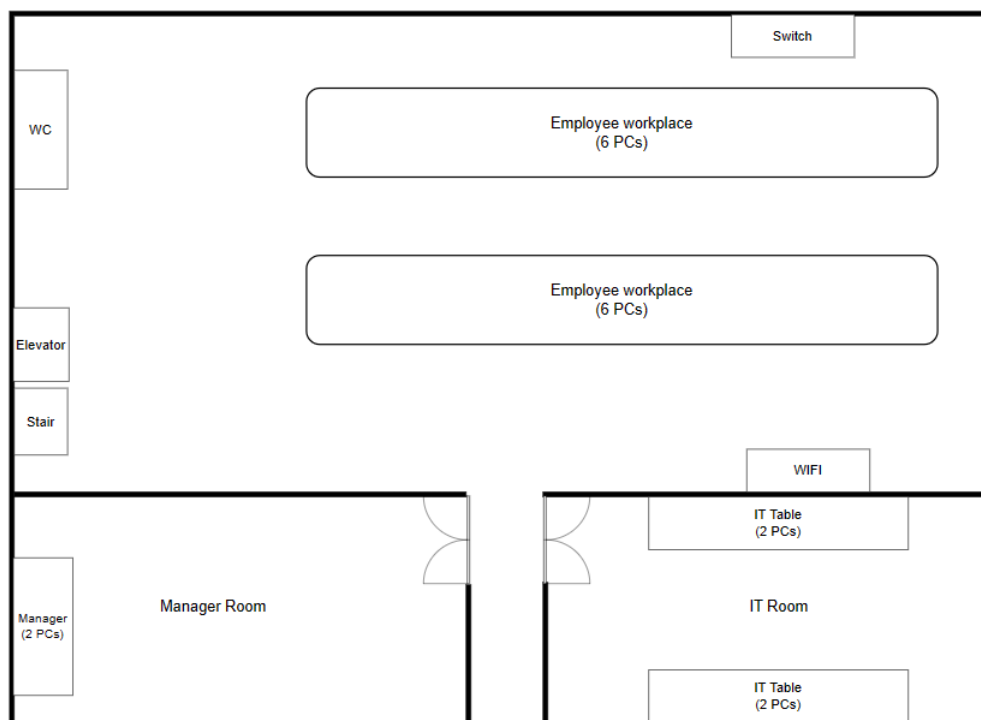
Tầng trệt của ngân hàng chủ yếu dùng cho giao dịch với khách hàng, bao gồm một khu vực tiếp tân và các quầy giao dịch. Mỗi quầy giao dịch được trang bị 5 máy tính để hỗ trợ tra cứu thông tin khách hàng và xử lý các dịch vụ tài chính như chuyển tiền, thanh toán hóa đơn, và mở tài khoản mới. Quầy lễ tân có 2 máy tính để cung cấp dịch vụ nhanh chóng cho khách hàng, như đặt lịch hẹn với tư vấn viên và hỗ trợ thông tin cơ bản. Ngoài ra, ngân hàng còn đặt các cây ATM ở hai bên cửa ra vào, cho phép khách hàng rút tiền, kiểm tra số dư, và thực hiện các giao dịch không cần đến quầy. Khu vực này cũng được trang bị màn hình hiển thị thông tin và quảng cáo về các sản phẩm, dịch vụ mới, cũng như cung cấp khu vực chờ thoải mái với ghế ngồi và tạp chí.



Hình 1: Floor 1

##### Tầng 2-6

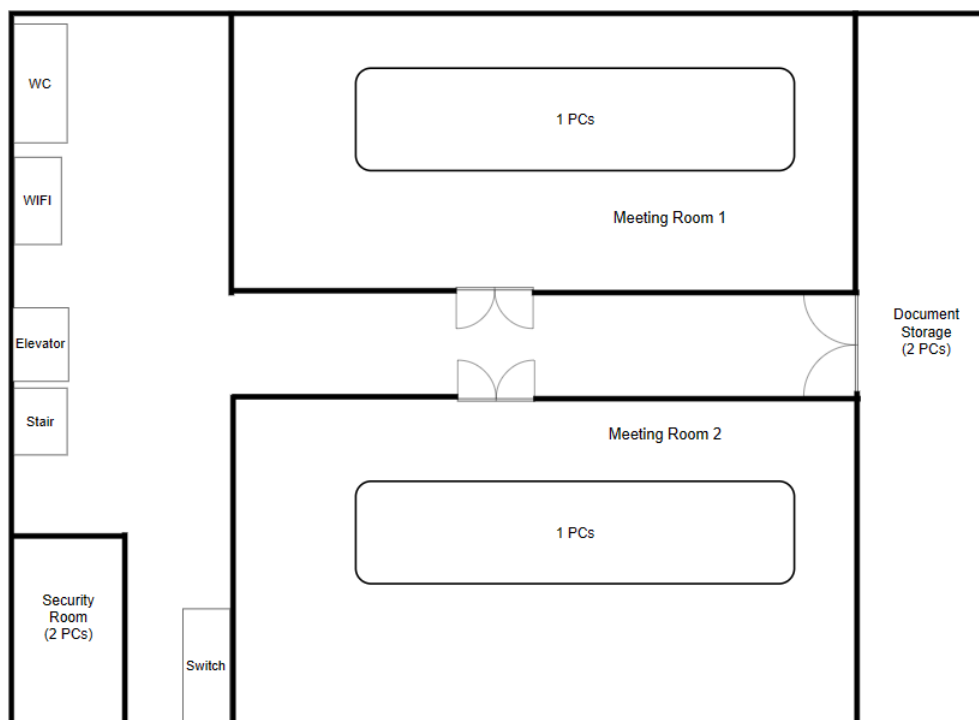
Khu vực làm việc của nhân viên bao gồm bàn làm việc được trang bị tổng cộng 14 máy tính, cho phép nhân viên thực hiện các nhiệm vụ hàng ngày như xử lý giao dịch và hỗ trợ khách hàng. Phòng quản lý với 2 máy tính dành cho các nhà quản lý để thực hiện công việc lãnh đạo và quản lý chiến lược. Phòng IT được thiết kế để hỗ trợ cơ sở hạ tầng kỹ thuật và giải quyết sự cố, cũng như quản lý hệ thống thông tin của ngân hàng. Khu vực IT có bàn làm việc với 2 máy tính dành cho kỹ thuật viên IT để giám sát và duy trì hệ thống mạng. Khu vực WiFi đảm bảo kết nối không dây liên tục cho cả khách hàng và nhân viên. **Tuy nhiên, các Access Point để mở rộng phạm vi của Wifi chỉ được đặt tại các tầng lẻ.** Các switch mạng được phân bố khắp không gian để cung cấp kết nối mạng ổn định và dễ dàng truy cập cho tất cả thiết bị.



**Hình 2:** Floor 2-6

## Tầng 7

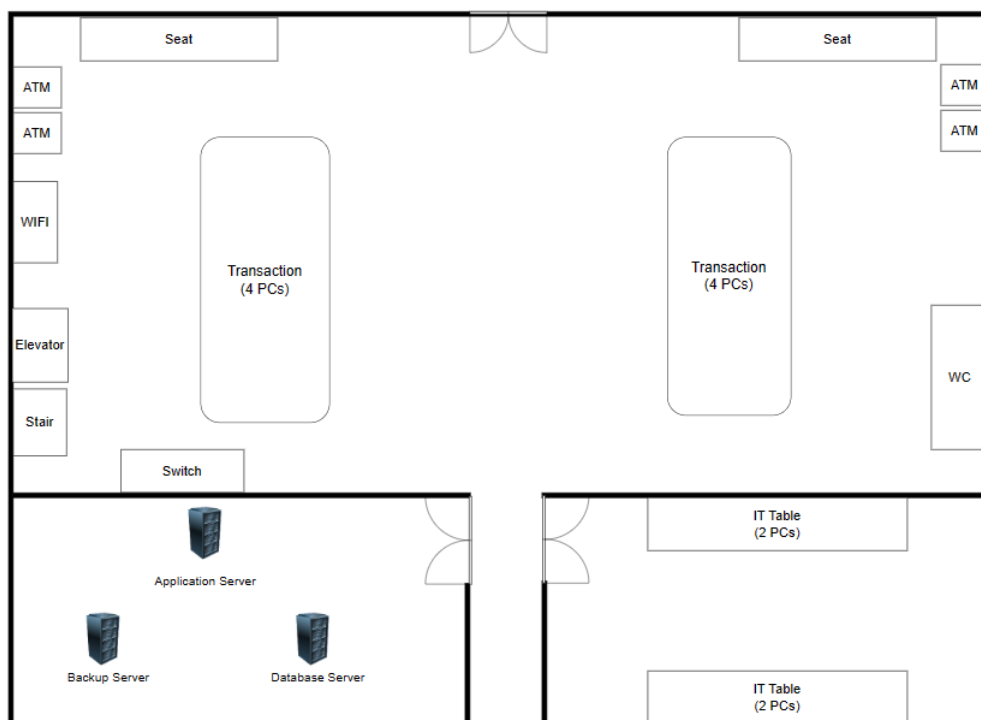
Tầng cao nhất của trụ sở ngân hàng này được thiết kế một cách chiến lược để tăng hiệu quả và bảo mật. Khu vực WiFi riêng biệt cho thấy một không gian dành cho nhân viên kết nối và thực hiện các nhiệm vụ kỹ thuật số dễ dàng. Hai phòng họp, mỗi phòng được trang bị ba máy tính, được sử dụng như những không gian hợp tác cho cuộc họp nhân viên, tư vấn khách hàng hoặc thuyết trình. Phòng an ninh, với hai máy tính, đóng vai trò quan trọng trong việc giám sát toàn bộ tòa nhà và đảm bảo an toàn cho hoạt động của ngân hàng. Phòng lưu trữ tài liệu, cũng với hai máy tính, cần thiết để xử lý an toàn các tài liệu tài chính nhạy cảm, được trang bị các công cụ kỹ thuật số để quản lý hồ sơ một cách chính xác. Các switch được đặt khắp nơi để duy trì một cơ sở hạ tầng dữ liệu vững chắc và an toàn, đảm bảo kết nối liền mạch trên mạng của ngân hàng. Bố cục này nhấn mạnh cam kết của ngân hàng đối với bảo mật hoạt động, tích hợp kỹ thuật số và môi trường làm việc hợp tác.



Hình 3: Floor 7

## 2.1.2 Branches

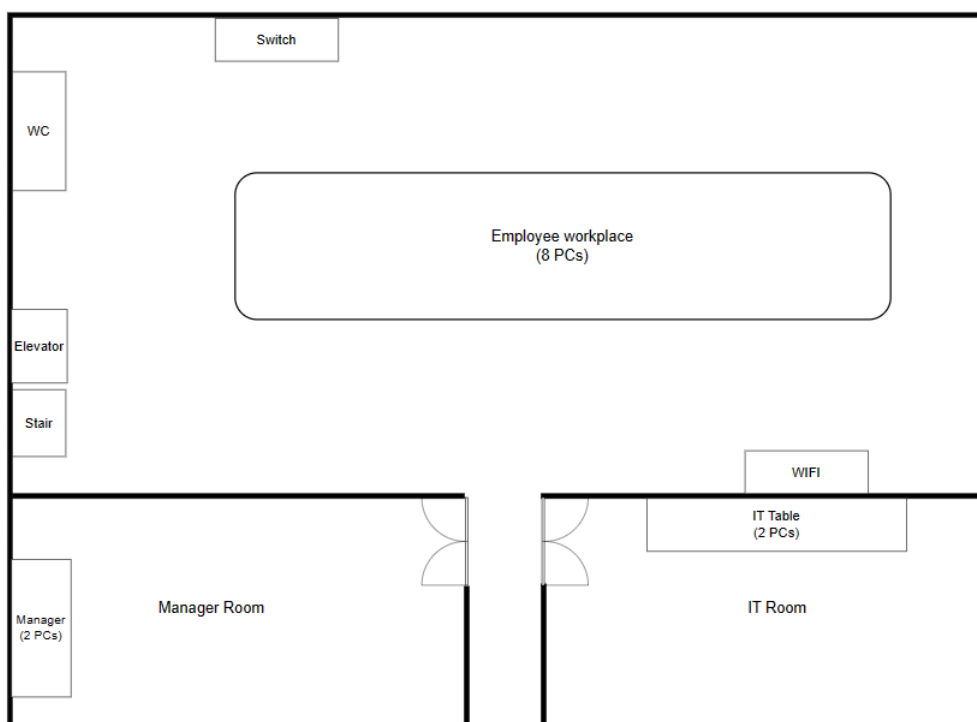
### Tầng 1



Hình 4: Floor 1

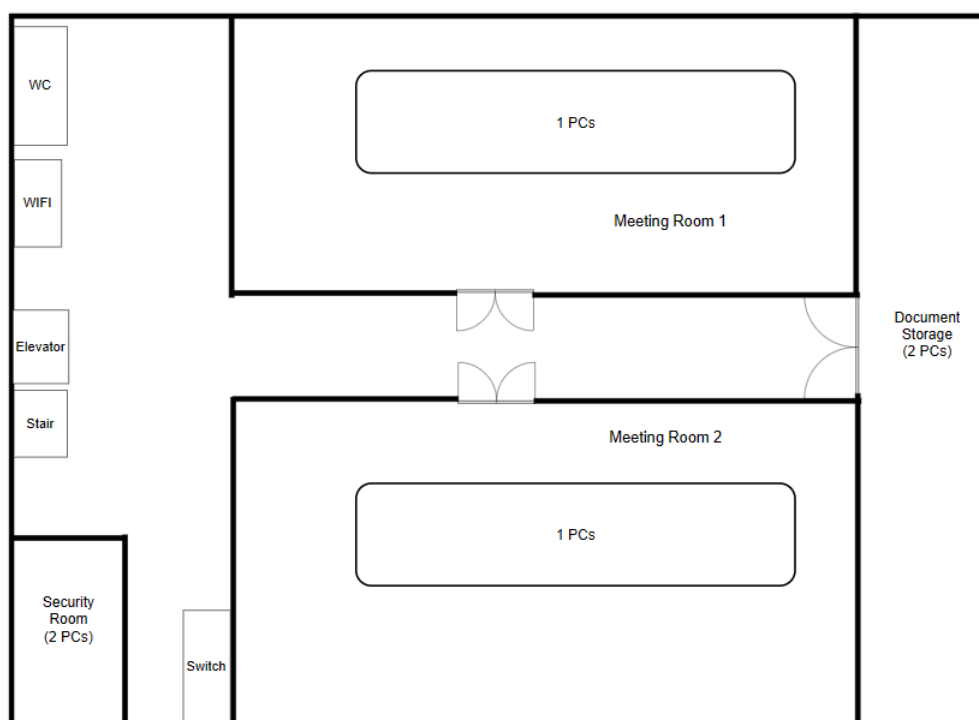


## Tầng 2



Hình 5: Floor 2

## Tầng 3



Hình 6: Floor 3

## 2.2 List of devices required

### Server

- **FTP Server:** FTP (File Transfer Protocol) là một trong những phương thức cổ điển nhất được sử dụng để truyền tải dữ liệu giữa client và server trên mạng. Server FTP cung cấp một cách dễ lưu trữ và chia sẻ file qua mạng. Người dùng có thể kết nối đến server FTP thông qua các ứng dụng client FTP, đăng nhập (nếu cần), và sau đó tải lên (upload) hoặc tải xuống (download) file. Server FTP thường được sử dụng trong các doanh nghiệp để chia sẻ và quản lý file lớn, hoặc cho phép người dùng truy cập từ xa vào một kho lưu trữ dữ liệu. FTP có thể hoạt động ở hai chế độ: active và passive, tùy thuộc vào cách thiết lập kết nối giữa client và server.
- **Web Server:** Server web là một máy chủ phần cứng hoặc phần mềm (ứng dụng server) lưu trữ, xử lý và phục vụ các trang web. Khi một người dùng truy cập một website thông qua trình duyệt, trình duyệt sẽ gửi yêu cầu đến server web, và server này sau đó phản hồi bằng cách gửi lại dữ liệu trang web, thường là trong dạng HTML, CSS, và JavaScript. Server web phổ biến như Apache và Nginx hỗ trợ một loạt các công nghệ và ngôn ngữ lập trình để xây dựng các ứng dụng web phức tạp, từ trang web đơn giản đến các ứng dụng web đầy đủ chức năng.
- **DHCP server:** DHCP (Dynamic Host Configuration Protocol) là một giao thức mạng được sử dụng để tự động cấp phát các thông số cấu hình mạng cho các thiết bị trên mạng (clients), bao gồm địa chỉ IP, subnet mask, default gateway và thông tin DNS. Server DHCP quản lý một pool địa chỉ IP và gán chúng cho các thiết bị mỗi khi chúng kết nối với mạng, giúp quản lý mạng trở nên dễ dàng và hiệu quả hơn. Ngoài việc cấp phát địa chỉ IP, DHCP cũng cho phép cấu hình tự động các thông số mạng khác, giúp giảm bớt công việc cấu hình mạng thủ công và giảm nguy cơ xung đột địa chỉ IP trong mạng.
- **Email Server:** Server email là một loại máy chủ chuyên dụng để xử lý, lưu trữ và gửi/nhận thư điện tử. Nó là một phần quan trọng của hệ thống gửi và nhận email trên Internet. Server email hoạt động dựa trên các giao thức như SMTP (Simple Mail Transfer Protocol) cho việc gửi thư, IMAP (Internet Message Access Protocol) hoặc POP3 (Post Office Protocol) cho việc nhận và đọc thư. SMTP được sử dụng để đẩy email từ client email tới server email và từ server này sang server khác, trong khi IMAP và POP3 cho phép người dùng cuối truy cập và quản lý thư của họ từ server email. Server email có thể là dịch vụ cung cấp bởi một nhà cung cấp dịch vụ email (như Gmail của Google, Outlook của Microsoft), hoặc được tổ chức tự lập trình và quản lý nội bộ (ví dụ, sử dụng Microsoft Exchange hoặc server email mã nguồn mở như Postfix).
- **DNS Server:** DNS (Domain Name System) là một hệ thống cho phép người dùng truy cập các website bằng tên miền thân thiện thay vì phải nhớ các địa chỉ IP phức tạp. Server DNS hoạt động như một danh bạ của Internet, chuyển đổi tên miền (như www.example.com) thành địa chỉ IP tương ứng mà máy tính có thể hiểu và truy cập. Khi một người dùng gõ tên miền vào trình duyệt, yêu cầu truy vấn DNS được gửi tới server DNS. Server này sẽ tra cứu thông tin trong bảng ghi DNS của mình hoặc hỏi các server DNS khác trên Internet để tìm địa chỉ IP tương ứng với tên miền đó. Một khi tìm thấy, địa chỉ IP được trả về cho máy trạm của người dùng, cho phép trình duyệt kết nối tới server hosting website đó.

### Router

Router Cisco 2620XM, khi được trang bị mô-đun mạng NM-2FE2W và thẻ giao diện WAN WIC-2T, trở thành một thiết bị mạng linh hoạt. Mô-đun mạng NM-2FE2W cung cấp hai cổng Fast Ethernet, nâng cao khả năng kết nối của router với khả năng thông lượng cao hơn. Trong khi đó, thẻ WIC-2T cung cấp hai cổng serial bổ sung cho kết nối WAN, mỗi cổng có khả năng hỗ trợ đồng bộ với tốc độ tối đa 2.048 Mbps mỗi cổng. Cấu hình này phù hợp cho nhiều môi trường mạng khác nhau, cung cấp sự cân bằng giữa kết nối Ethernet và serial cho các yêu cầu mạng đa dạng.



**Hình 7:** Router 2620xm with WIC 2T

### Switch

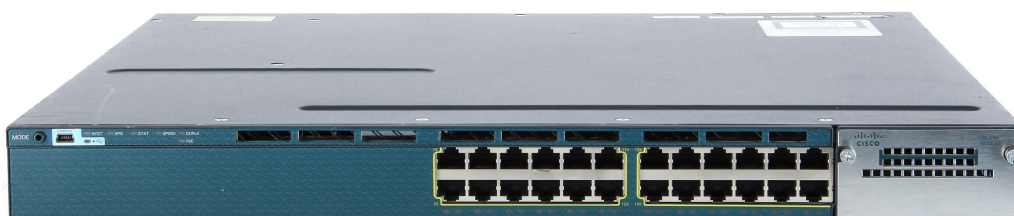
Các switch dòng Cisco Catalyst 2960-X, hoạt động trên Cisco IOS 15, là các switch Gigabit Ethernet có khả năng gắn kết (stackable), cung cấp truy cập cấp doanh nghiệp cho các ứng dụng trên khuôn viên và chi nhánh. Chúng hỗ trợ quản lý thiết bị đơn giản và quản lý mạng, cung cấp các tính năng tiên tiến Layer 2 và Layer 3, với khả năng cung cấp điện qua Ethernet Plus (PoE+). Các switch này được thiết kế để đơn giản hóa vận hành và giảm tổng chi phí sở hữu, đồng thời cho phép vận hành kinh doanh có khả năng mở rộng, bảo mật và tiết kiệm năng lượng với các dịch vụ thông minh. Chúng có tính năng lên đến 48 cổng Gigabit Ethernet, hỗ trợ PoE+, tùy chọn quản lý linh hoạt và các tính năng nâng cao về bảo mật và đáng tin cậy mạng.



**Hình 8:** Switch 2960 IOS 15

### Multilayer-Switch

Multilayer switch 3560-24PS là một thiết bị switch trong dòng 3560 của Cisco, được thiết kế để hỗ trợ kết nối mạng đa người sử dụng. Nó có 24 cổng Ethernet, cho phép kết nối nhiều thiết bị mạng cùng một lúc. Switch này hỗ trợ tính năng định tuyến Layer 2 và Layer 3, giúp tối ưu hóa việc chuyển tiếp dữ liệu trong mạng. Nó cũng tích hợp tính năng Power over Ethernet (PoE), cho phép cấp nguồn điện cho các thiết bị mạng như điện thoại IP hoặc camera IP. Multilayer switch 3560-24PS cung cấp hiệu suất ổn định và đáng tin cậy cho mạng đa người sử dụng trong các môi trường doanh nghiệp hoặc tổ chức.



**Hình 9:** Multiplayer Switch 3560 24PS

### Access Point

Access Point là một thiết bị tạo ra một mạng không dây trong khu vực cục bộ (WLAN), thường là trong một văn phòng hoặc tòa nhà lớn. AP kết nối với mạng có dây và có thể phát sóng Wi-Fi trong một khu vực đã chỉ định.



**Hình 10:** Access-Point Netgear WAC540

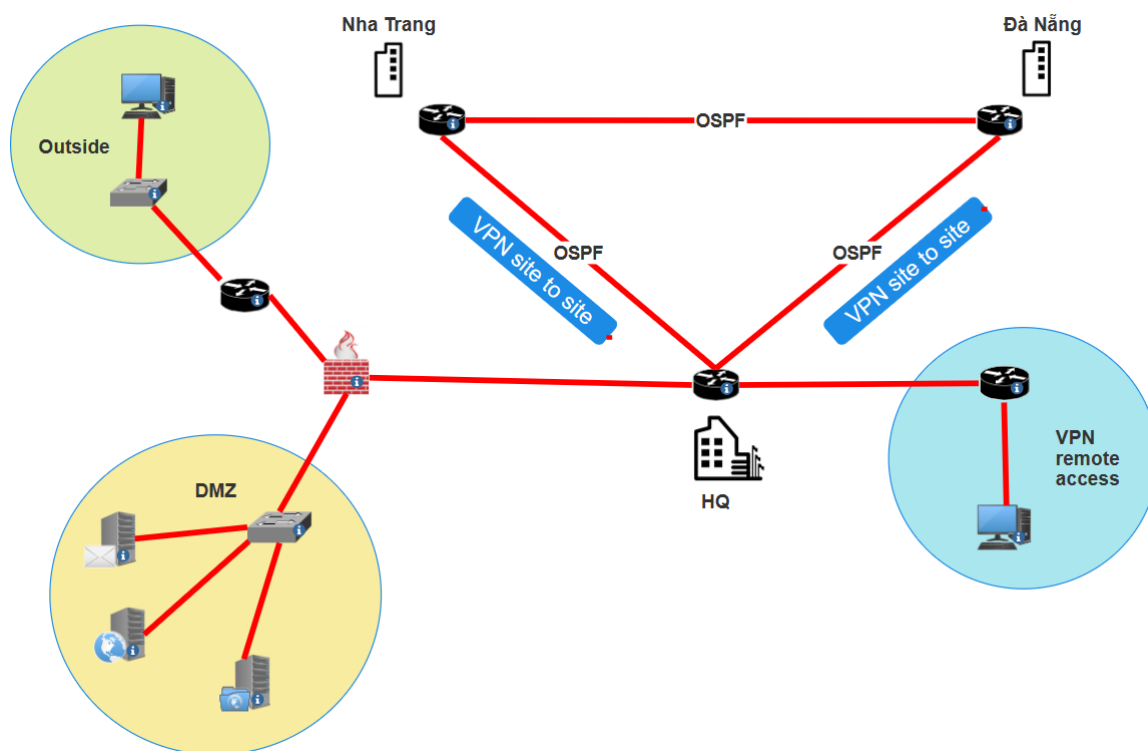
### Firewall

Firewall là một thiết bị bảo mật mạng giám sát và lọc lưu lượng mạng đi vào và đi ra dựa trên các chính sách bảo mật đã được thiết lập trước đó của tổ chức. Ở mức cơ bản nhất, tường lửa chính là rào cản đặt giữa một mạng nội bộ riêng tư và Internet công cộng. Hiệu quả của một tường lửa trong bảo mật mạng nằm ở khả năng lọc lưu lượng từ các nguồn không an toàn hoặc đáng ngờ để ngăn chặn các cuộc tấn công và xâm nhập.



Hình 11: Cisco Asa 5506

### 2.3 WAN Diagram



Hình 12: WAN Diagram

### 3 STEP 3

#### 3.1 Calculate the required throughput, and expected bandwidth from ISP

Các luồng dữ liệu và khối lượng công việc của hệ thống (khoảng 80% trong giờ cao điểm từ 9g đến 11g và từ 15g đến 16g) có thể được chia sẻ cho Trụ sở chính và Chi nhánh như sau:

- Các máy chủ để cập nhật phần mềm, truy cập web và truy cập cơ sở dữ liệu, .... Ước tính tổng lượng tải xuống là khoảng 1000 MB/ngày và lượng tải lên là 2000 MB/ngày.
- Mỗi máy trạm được sử dụng để duyệt web, tải xuống tài liệu và giao dịch với khách hàng, ... Ước tính tổng lượng tải xuống là khoảng 500 MB/ngày và lượng tải lên là 100 MB/ngày.
- Các thiết bị kết nối WiFi từ khách hàng để tải xuống là khoảng 500 MB/ngày.

##### 3.1.1 Headquarter

###### Wired network

Tại tầng 1, tổng cộng có 10 Servers. Dung lượng upload cả download khoảng 3000 MB/ngày. Ta tính được Throughput vào lúc sử dụng đường truyền cao nhất (Tập trung 80%) trong 3h:

- Số lượng server: 6
$$-Bandwidth = \frac{6 \times 3000 \times 80\%}{3 \times 3600} = 1.33(MB/s)$$
$$-Throughput = \frac{6 \times 3000}{8 \times 3600} = 0.625(MB/s)$$
- 120 workstation với tổng lượng tải xuống và lượng tải lên là 600 MB/ngày.
$$-Bandwidth = \frac{120 \times 600 \times 80\%}{3 \times 3600} = 5.33(MB/s)$$
$$-Throughput = \frac{120 \times 600}{8 \times 3600} = 2.5(MB/s)$$

Total Bandwidth =  $1.33 + 5.33 = 6.66(MB/s)$

Total Throughput =  $0.625 + 2.5 = 3.125(MB/s)$

###### Wireless network

- 4 Access Point
$$-Bandwidth = \frac{4 \times 500 \times 80\%}{3 \times 3600} = 0.148(MB/s)$$
$$-Throughput = \frac{4 \times 500}{8 \times 3600} = 0.069(MB/s)$$

##### 3.1.2 Branches

###### Wired network

Tại tầng 1, tổng cộng có 10 Servers. Dung lượng upload cả download khoảng 3000 MB/ngày. Ta tính được Throughput vào lúc sử dụng đường truyền cao nhất (Tập trung 80%) trong 3h:

- Số lượng server: 3
$$-Bandwidth = \frac{3 \times 3000 \times 80\%}{3 \times 3600} = 0.667(MB/s)$$
$$-Throughput = \frac{3 \times 3000}{8 \times 3600} = 0.313(MB/s)$$

- 30 workstation với tổng lượng tải xuống và lượng tải lên là 600 MB/ngày.

$$-Bandwidth = \frac{30 \times 600 \times 80\%}{3 \times 3600} = 1.33(MB/s)$$

$$-Throughput = \frac{30 \times 600}{8 \times 3600} = 0.625(MB/s)$$

$$\text{Total Bandwidth} = 0.667 + 1.33 = 1.997(MB/s)$$

$$\text{Total Throughput} = 0.625 + 0.313 = 0.938(MB/s)$$

### Wireless network

- 1 Access Point

$$-Bandwidth = \frac{1 \times 500 \times 80\%}{3 \times 3600} = 0.037(MB/s)$$

$$-Throughput = \frac{1 \times 500}{8 \times 3600} = 0.017(MB/s)$$

## 3.2 Suggest the configuration for the company network

### 3.2.1 Router

- **OSPF (Open Shortest Path First):** Đây là một giao thức định tuyến nội bộ (IGP) được sử dụng để tự động tính toán đường đi tối ưu giữa các router trong cùng một khu vực OSPF. OSPF được sử dụng để định tuyến giữa trụ sở chính và các chi nhánh.
- **IPsec (Internet Protocol Security):** Là một tập hợp các giao thức bảo mật để bảo vệ giao tiếp thông qua mạng IP, thường được sử dụng trong VPN site-to-site để mã hóa và xác thực dữ liệu.
- **VPN Site-to-Site:** Là một kết nối an toàn giữa các mạng tại các vị trí địa lý khác nhau thông qua mạng công cộng như Internet, sử dụng IPsec để mã hóa dữ liệu truyền giữa các địa điểm.
- **VPN Remote Access:** Cho phép người dùng từ xa kết nối an toàn vào mạng nội bộ của công ty, có thể thông qua IPsec hoặc SSL VPN.
- **Serial Interfaces:** Các giao diện Serial (Se0/0/0, Se0/0/1, v.v.) thường được sử dụng cho kết nối WAN giữa các địa điểm.
- **GigabitEthernet Interfaces:** Các giao diện GigabitEthernet (Gi0/0, Gi0/1, v.v.) được sử dụng cho kết nối LAN tốc độ cao nội bộ hoặc kết nối đến các thiết bị mạng khác như switch hoặc router.
- **FastEthernet Interfaces:** Sử dụng cho các kết nối LAN tốc độ thấp hơn hoặc kết nối với các thiết bị đầu cuối như máy tính để bàn hoặc máy chủ.
- **NAT (Network Address Translation):** Sử dụng để dịch địa chỉ IP nội bộ sang địa chỉ IP công cộng cho việc truy cập Internet, thường được cấu hình trên router biên (ở khu vực OUTSIDE).
- **Firewall Rules:** Các quy tắc tường lửa được áp dụng trên router hoặc thiết bị bảo mật khác để kiểm soát lưu lượng vào và ra, đặc biệt là trong DMZ và kết nối từ bên ngoài vào.
- **ACLs (Access Control Lists):** Được sử dụng để kiểm soát lưu lượng truy cập và có thể được áp dụng để định cấu hình VPN và các quy tắc bảo mật khác.



### 3.2.2 Switch/Multilayer Switch

- **VLANs (Virtual Local Area Networks):** Mỗi switch cấu hình với một VLAN duy nhất để phân chia mạng lưới thành các phân đoạn riêng biệt. Mỗi VLAN tạo ra một miền quảng bá riêng, giúp cải thiện hiệu suất mạng và cung cấp tính bảo mật thông qua sự cô lập lưu lượng mạng.
- **Inter-VLAN Routing:** Multilayer switch sử dụng cơ chế này để cho phép giao tiếp giữa các VLAN. Thông thường, mỗi VLAN sẽ có một địa chỉ IP trên một sub-interface hoặc SVI (Switched Virtual Interface) trên multilayer switch, và IP routing được kích hoạt để chuyển mạch lưu lượng giữa các VLAN này.
- **IP Routing:** Trên multilayer switch, cấu hình IP routing (thông qua lệnh ip routing) cho phép nó chức năng như một router, định tuyến lưu lượng giữa các mạng khác nhau được kết nối với nó.
- **OSPF (Open Shortest Path First):** OSPF là một giao thức định tuyến nội bộ dùng để quảng bá thông tin định tuyến giữa các thiết bị trong cùng một AS (Autonomous System). Trong trường hợp này, multilayer switch tham gia vào OSPF để định tuyến và quảng bá các mạng VLAN đến các router khác trong mạng.
- **DTP (Dynamic Trunking Protocol):** DTP có thể được sử dụng để tự động đàm phán việc cấu hình trunking giữa các switch. Trunking là cần thiết khi có giao tiếp giữa các VLAN khác nhau trên cùng một đường link vật lý.
- **DHCP (Dynamic Host Configuration Protocol):** DHCP thường được sử dụng trên một server hoặc router để tự động cấp phát địa chỉ IP cho các thiết bị trong mạng.
- **Access Control Lists (ACLs):** ACLs có thể được áp dụng trên multilayer switch để kiểm soát quyền truy cập vào mạng hoặc giữa các VLAN.
- **QoS (Quality of Service):** Đối với môi trường có các webcam CCTV, QoS có thể được sử dụng để đảm bảo băng thông cho video surveillance traffic, đặc biệt quan trọng trong việc đảm bảo chất lượng video không bị giảm sút khi mạng bận rộn.

### 3.2.3 Access Point

WEP, viết tắt của Wired Equivalent Privacy, là một giao thức bảo mật không dây được thiết kế để cung cấp một mức độ bảo mật so sánh được với mạng có dây cho mạng LAN không dây (WLAN). Mô tả về WEP trong cấu hình một Access Point (AP) trong môi trường công ty có thể như sau:

- **Khóa Mã Hóa:** WEP sử dụng một khóa mã hóa tĩnh (cố định) để bảo mật dữ liệu truyền giữa AP và thiết bị không dây. Khóa này cần được cấu hình trước và phải giống nhau trên AP và tất cả thiết bị không dây muốn kết nối.
- **Mã Hóa Dữ Liệu:** Khi một thiết bị không dây cố gắng kết nối với mạng, dữ liệu truyền đi sẽ được mã hóa bằng khóa WEP. Mã hóa này giúp bảo vệ dữ liệu khỏi bị nghe lén hoặc truy cập trái phép trong quá trình truyền qua không gian mở.
- **Xác Thực:** Trong quá trình xác thực, AP sẽ yêu cầu thiết bị không dây cung cấp khóa WEP. Nếu khóa được cung cấp khớp với khóa đã cấu hình trên AP, xác thực sẽ thành công và thiết bị sẽ được phép kết nối với mạng.

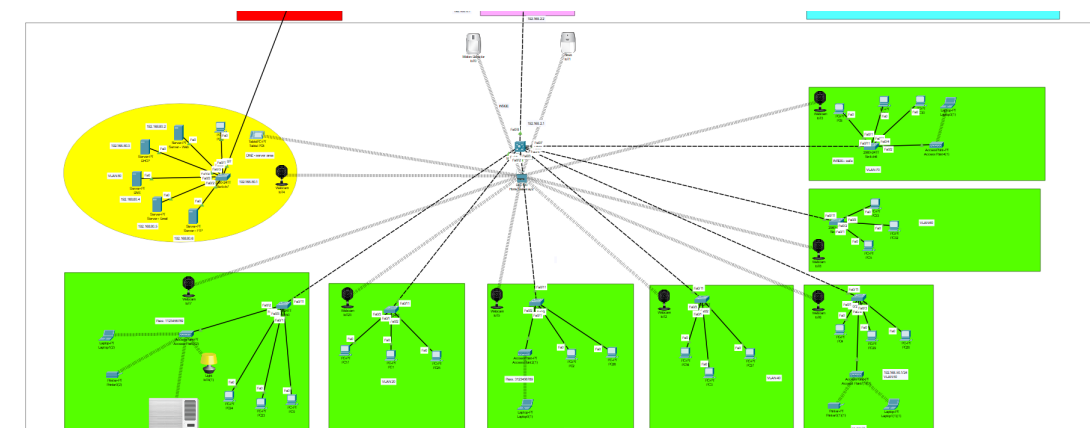


## 4 STEP 4

### 4.1 Network Map using Packet Tracer

#### Headquarter

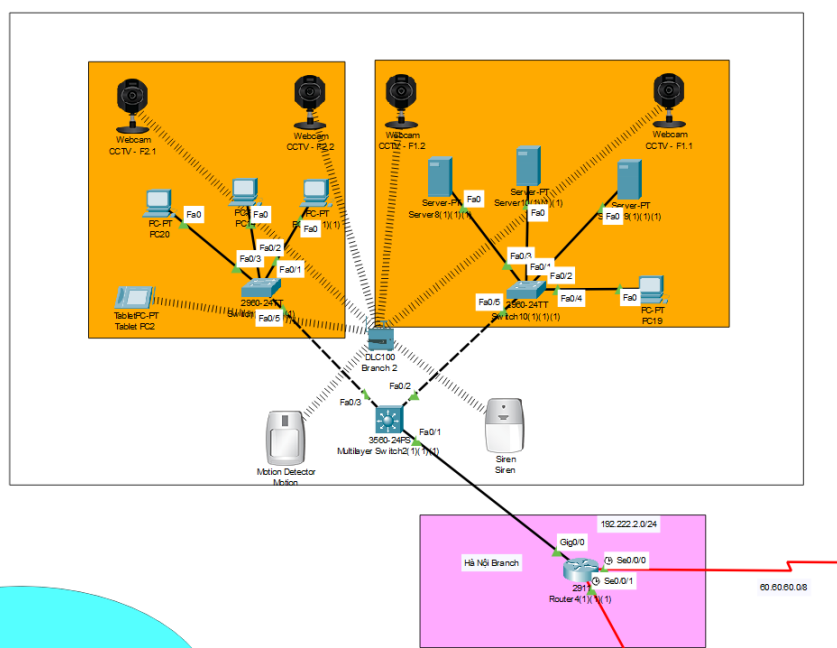
Trụ sở chính có thể được xem như trung tâm điều hành của mạng. Nó sẽ có trung tâm dữ liệu chính với các máy chủ và giải pháp lưu trữ có khả năng cao để xử lý các ứng dụng và dữ liệu quan trọng của công ty. Trụ sở chính sẽ được trang bị biện pháp bảo mật mạnh mẽ, bao gồm tường lửa tiên tiến, hệ thống phòng ngừa xâm nhập để bảo mật mạng.



Hình 13: Headquarter

#### Hà Nội Branch

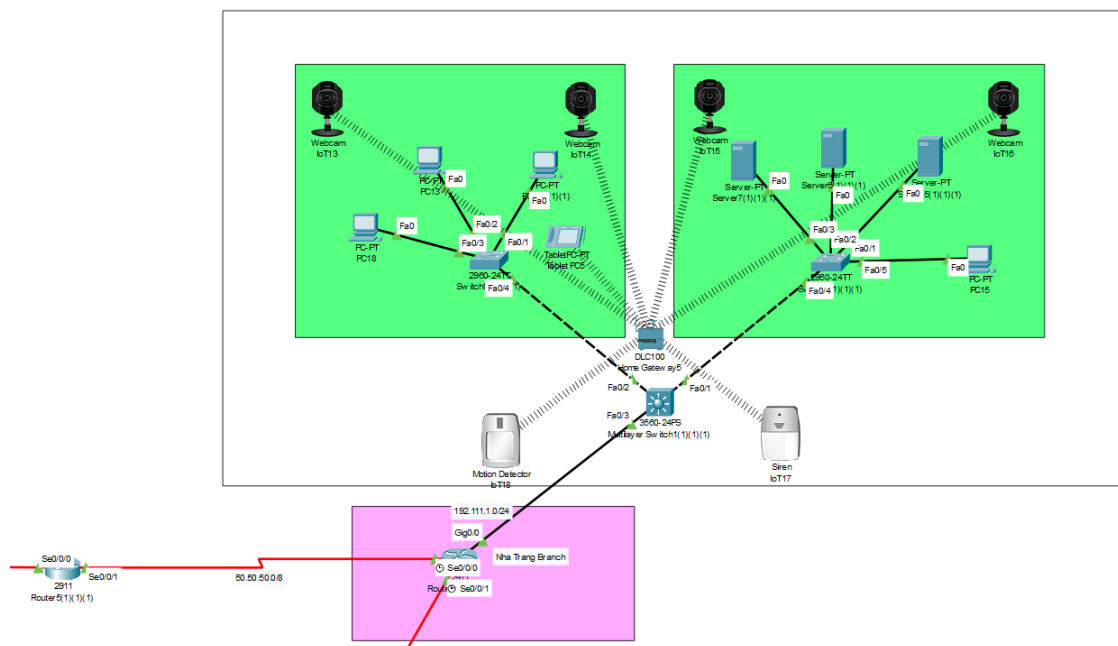
Chi nhánh tại Hà Nội sẽ là một chi nhánh kết nối với trụ sở chính. Nó sẽ duy trì các máy chủ và thiết bị mạng địa phương để xử lý các hoạt động hàng ngày, nhưng vẫn phụ thuộc vào trụ sở chính để sử dụng tài nguyên và dịch vụ tập trung. Chi nhánh sử dụng phương thức OSPF đến trụ sở chính để đảm bảo việc truy cập liên tục và đáng tin cậy vào tài nguyên doanh nghiệp.



Hình 14: Hà Nội branch

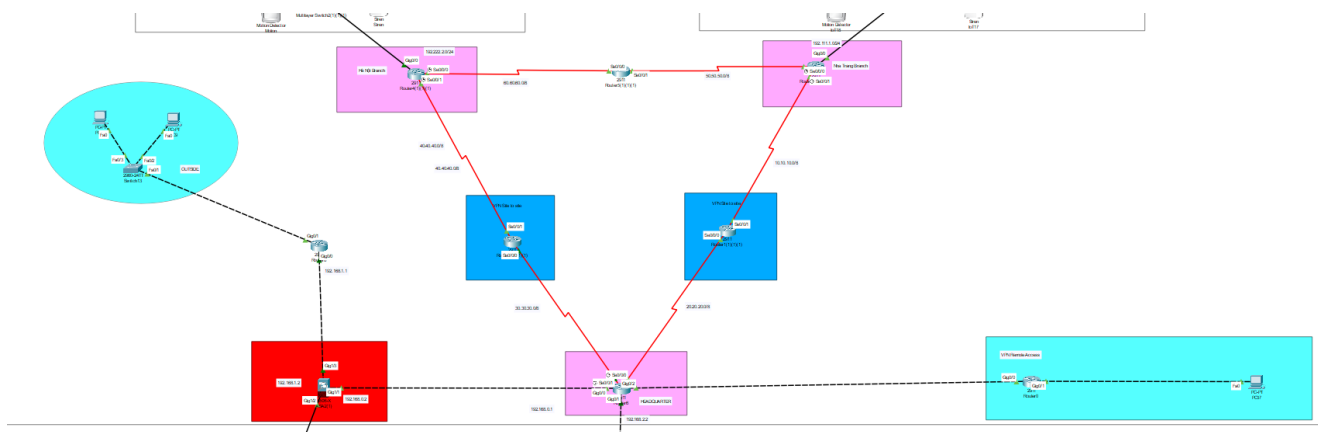
#### Dà Nẵng Branch

Tương tự như chi nhánh Hà Nội, chi nhánh Đà Nẵng sẽ hoạt động như một điểm kết nối khác trong mạng. Nó sẽ có cơ sở hạ tầng mạng địa phương phù hợp với nhân viên và hoạt động tại Nha Trang, với các kết nối an toàn trở lại trụ sở chính để truy cập dịch vụ chia sẻ, dữ liệu và ứng dụng.



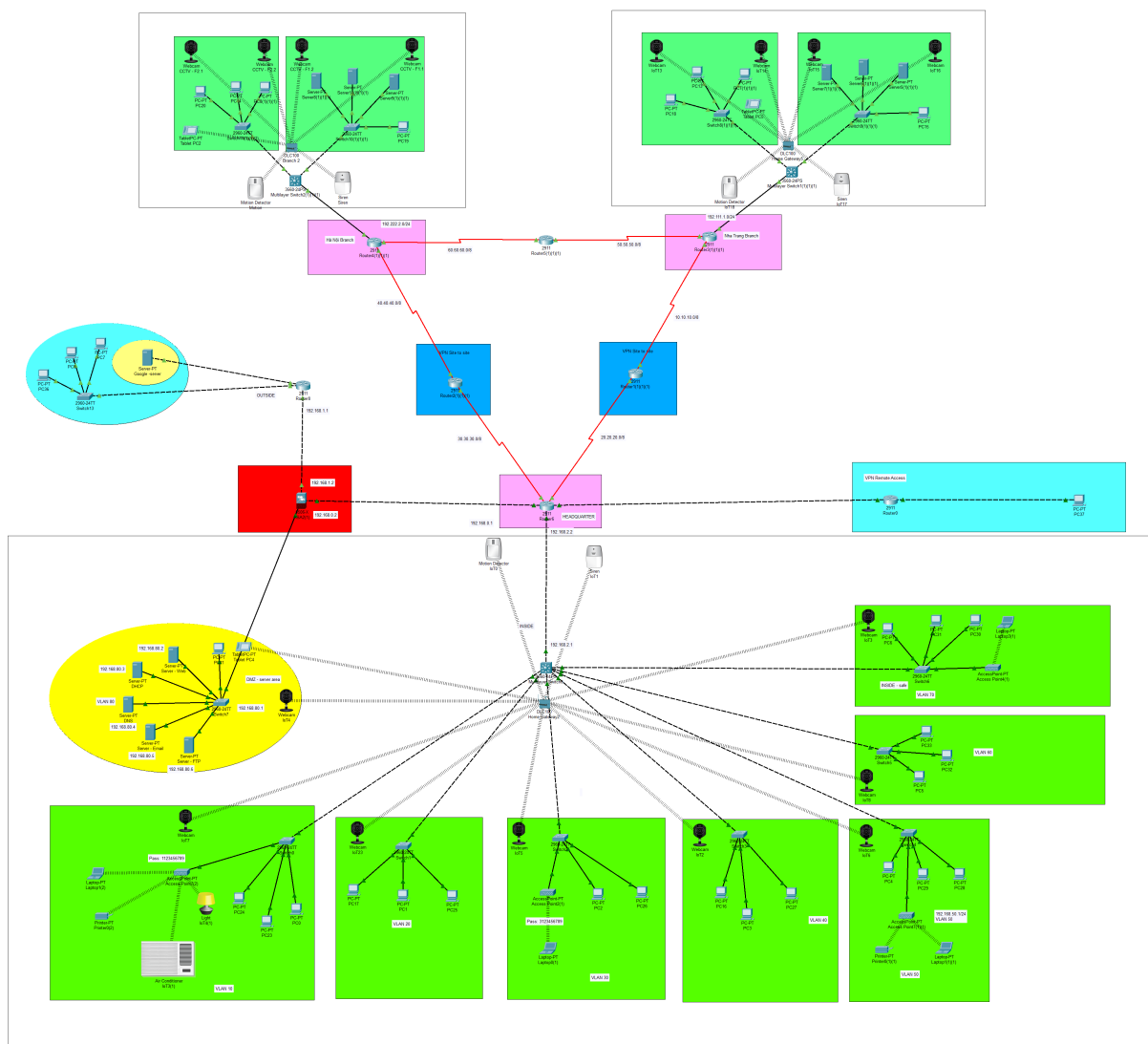
Hình 15: Da Nang branch

## WAN Connection



Hình 16: WAN connection

Chúng ta có thể tổng hợp tất cả các cấu hình trên vào một nơi duy nhất. Trong hình, có 3 khu vực chính: nhánh Đà Nẵng (phía trên bên trái), nhánh Hà Nội (phía trên bên phải) và trụ sở chính (phía dưới). Mỗi khu vực được đánh dấu bằng một màu sắc khác nhau, giúp cung cấp cái nhìn toàn cảnh rõ ràng về toàn bộ cấu hình. Việc sử dụng lệnh ping để xác định vấn đề là một bước rất quan trọng có thể được đánh giá trong tệp final.pkt.

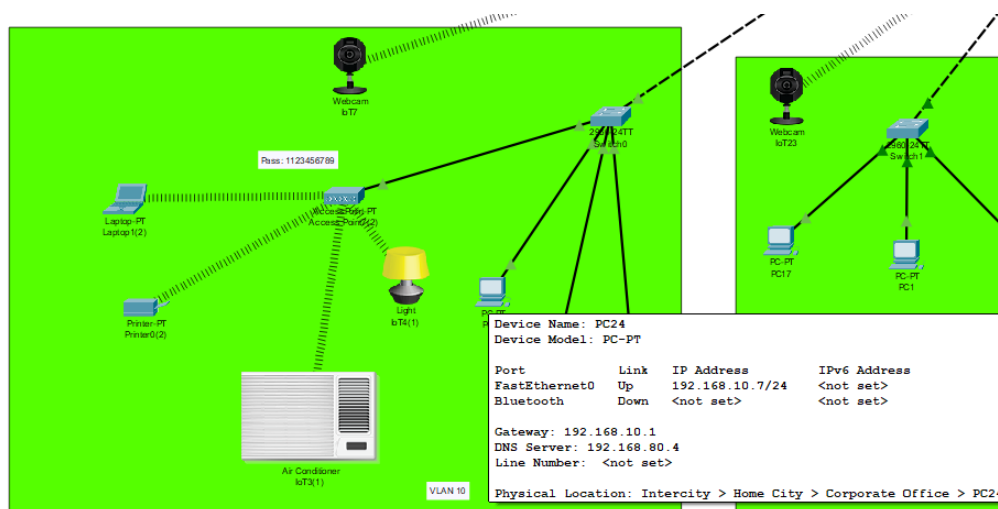


Hình 17: Network Map

## 5 STEP 5

### 5.1 Connect between PCs in the same VLAN

Ta có địa chỉ IP của PC24



Hình 18: PC24's ip

Kết quả của lệnh *ping* và *tracert*:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.7

Pinging 192.168.10.7 with 32 bytes of data:

Reply from 192.168.10.7: bytes=32 time=14ms TTL=128
Reply from 192.168.10.7: bytes=32 time=13ms TTL=128
Reply from 192.168.10.7: bytes=32 time=10ms TTL=128
Reply from 192.168.10.7: bytes=32 time=12ms TTL=128

Ping statistics for 192.168.10.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 14ms, Average = 12ms

C:\>tracert 192.168.10.7

Tracing route to 192.168.10.7 over a maximum of 30 hops:

  1  10 ms   5 ms   18 ms   192.168.10.7

Trace complete.

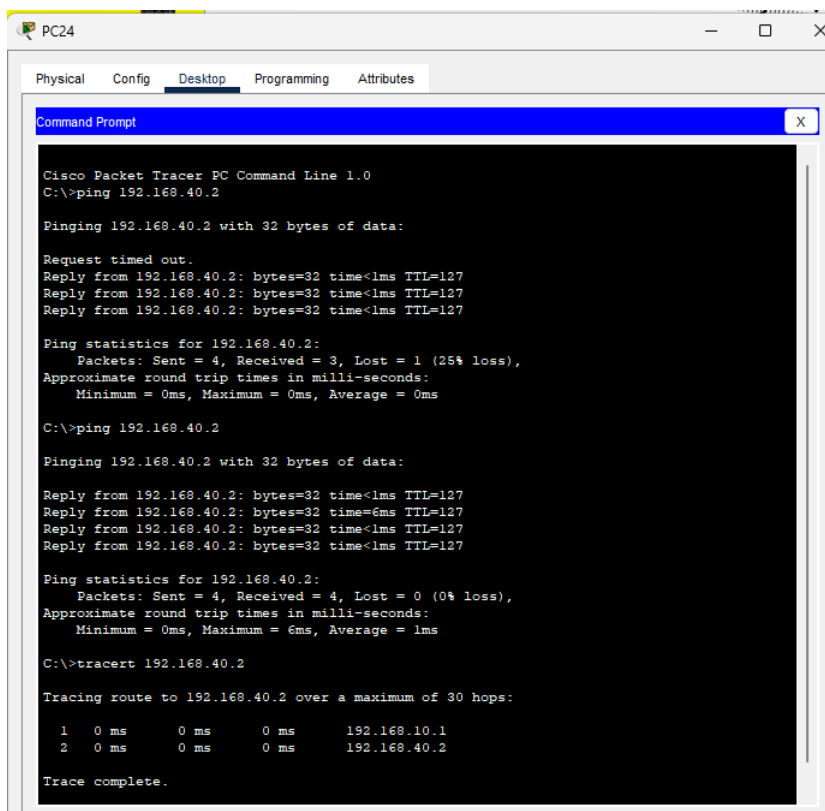
C:\>

```

Hình 19: Result

### 5.2 Connect PCs between VLANs

Ta *ping* từ PC24 ở VLAN 10 có địa chỉ như hình 18 sang PC ở VLAN 40 có địa chỉ IP là 192.168.40.2:  
Kết quả sau 2 lần chạy lệnh *ping* và 1 lần chạy lệnh *tracert*:



```
PC24
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.40.2: bytes=32 time<1ms TTL=127
Reply from 192.168.40.2: bytes=32 time=6ms TTL=127
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>tracert 192.168.40.2

Tracing route to 192.168.40.2 over a maximum of 30 hops:

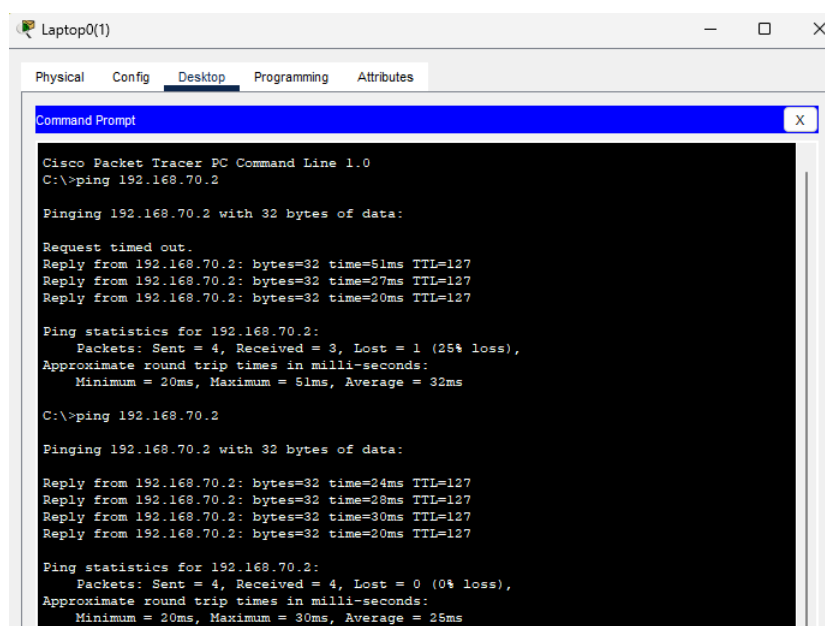
  0  0 ms    0 ms    0 ms   192.168.10.1
  1  0 ms    0 ms    0 ms   192.168.40.2
  2  0 ms    0 ms    0 ms   192.168.40.2

Trace complete.
```

Hình 20: VLAN 10 to VLAN 40

Ta *ping* từ Laptop ở VLAN 30 có địa chỉ 192.168.30.3 sang Laptop ở VLAN 70 có địa chỉ IP là 192.168.70.2:

Kết quả sau 2 lần chạy lệnh *ping*:



```
Laptop0(1)
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.70.2

Pinging 192.168.70.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.70.2: bytes=32 time=51ms TTL=127
Reply from 192.168.70.2: bytes=32 time=27ms TTL=127
Reply from 192.168.70.2: bytes=32 time=20ms TTL=127

Ping statistics for 192.168.70.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 51ms, Average = 32ms

C:\>ping 192.168.70.2

Pinging 192.168.70.2 with 32 bytes of data:

Reply from 192.168.70.2: bytes=32 time=24ms TTL=127
Reply from 192.168.70.2: bytes=32 time=28ms TTL=127
Reply from 192.168.70.2: bytes=32 time=30ms TTL=127
Reply from 192.168.70.2: bytes=32 time=20ms TTL=127

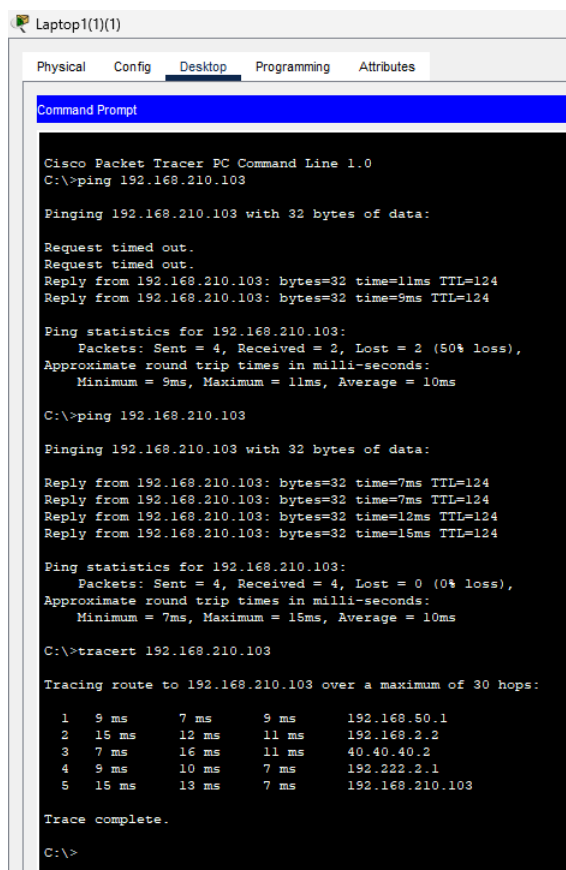
Ping statistics for 192.168.70.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 30ms, Average = 25ms
```

Hình 21: VLAN 30 to VLAN 70

### 5.3 Connect PCs between Headquarters and branches

Ta *ping* từ Laptop ở VLAN 50 có địa chỉ 192.168.30.5 ở Headquarter sang PC ở VLAN 210 có địa chỉ IP là 192.168.210.103 ở Hà Nội Branch:

Kết quả sau 2 lần chạy lệnh *ping* và 1 lần chạy lệnh *tracert*:



```
Laptop1(1)(1)
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.210.103

Pinging 192.168.210.103 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.210.103: bytes=32 time=11ms TTL=124
Reply from 192.168.210.103: bytes=32 time=9ms TTL=124

Ping statistics for 192.168.210.103:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 11ms, Average = 10ms

C:\>ping 192.168.210.103

Pinging 192.168.210.103 with 32 bytes of data:

Reply from 192.168.210.103: bytes=32 time=7ms TTL=124
Reply from 192.168.210.103: bytes=32 time=7ms TTL=124
Reply from 192.168.210.103: bytes=32 time=12ms TTL=124
Reply from 192.168.210.103: bytes=32 time=15ms TTL=124

Ping statistics for 192.168.210.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 15ms, Average = 10ms

C:\>tracert 192.168.210.103

Tracing route to 192.168.210.103 over a maximum of 30 hops:

  0  9 ms    7 ms    9 ms    192.168.50.1
  1  15 ms   12 ms   11 ms   192.168.2.2
  2  7 ms    16 ms   11 ms   40.40.40.2
  3  9 ms    10 ms    7 ms   192.222.2.1
  4  15 ms   13 ms    7 ms   192.168.210.103

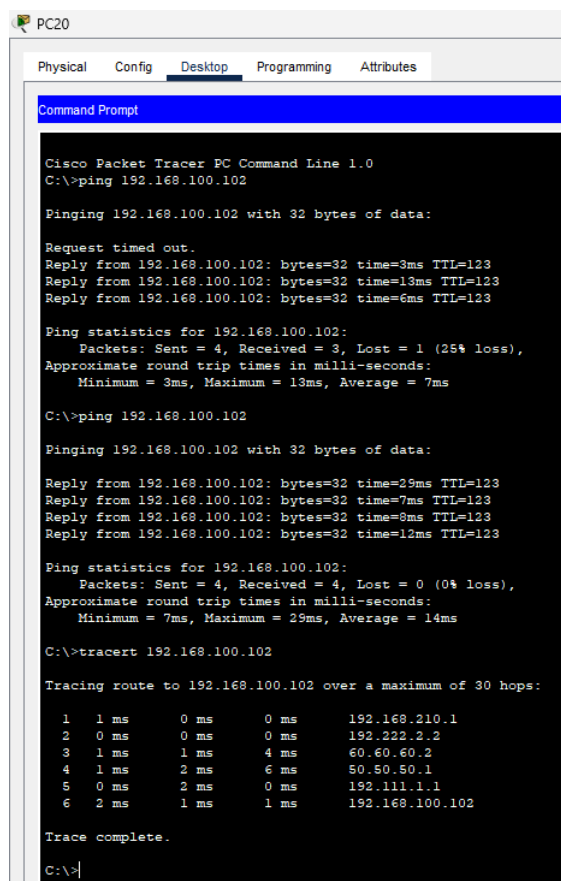
Trace complete.

C:\>
```

Hình 22: Headquarter to Hà Nội Branch

Ta *ping* từ PC ở VLAN 210 có địa chỉ 192.168.210.102 ở Hà Nội Branch sang Server ở VLAN 100 có địa chỉ IP là 192.168.100.102 ở Đà Nẵng Branch:

Kết quả sau 2 lần chạy lệnh *ping* và 1 lần chạy lệnh *tracert*:



```
PC20
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.102

Pinging 192.168.100.102 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.102: bytes=32 time=3ms TTL=123
Reply from 192.168.100.102: bytes=32 time=13ms TTL=123
Reply from 192.168.100.102: bytes=32 time=6ms TTL=123

Ping statistics for 192.168.100.102:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 13ms, Average = 7ms

C:\>ping 192.168.100.102

Pinging 192.168.100.102 with 32 bytes of data:

Reply from 192.168.100.102: bytes=32 time=29ms TTL=123
Reply from 192.168.100.102: bytes=32 time=7ms TTL=123
Reply from 192.168.100.102: bytes=32 time=8ms TTL=123
Reply from 192.168.100.102: bytes=32 time=12ms TTL=123

Ping statistics for 192.168.100.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 29ms, Average = 14ms

C:\>tracert 192.168.100.102

Tracing route to 192.168.100.102 over a maximum of 30 hops:

  0  1 ms    0 ms    0 ms    192.168.210.1
  1  0 ms    0 ms    0 ms    192.222.2.2
  2  1 ms    1 ms    4 ms    60.60.60.2
  3  1 ms    2 ms    6 ms    50.50.50.1
  4  0 ms    2 ms    0 ms    192.111.1.1
  5  2 ms    1 ms    1 ms    192.168.100.102

Trace complete.

C:\>
```

Hình 23: Hà Nội Branch to Đà Nẵng Branch

Ta *ping* từ PC ở VLAN 110 có địa chỉ 192.168.110.101 ở Đà Nẵng Branch sang PC ở VLAN 20 có địa chỉ IP là 192.168.20.3 ở Headquarter:

Kết quả sau 2 lần chạy lệnh *ping* và 1 lần chạy lệnh *tracert*:

```

PC7(1)(1)(1)
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.20.3: bytes=32 time=6ms TTL=124
Reply from 192.168.20.3: bytes=32 time=2ms TTL=124

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 6ms, Average = 4ms

C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=11ms TTL=124
Reply from 192.168.20.3: bytes=32 time=3ms TTL=124
Reply from 192.168.20.3: bytes=32 time=2ms TTL=124
Reply from 192.168.20.3: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 4ms

C:\>tracert 192.168.20.3

Tracing route to 192.168.20.3 over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.110.1
  1  0 ms  0 ms  0 ms  192.111.1.2
  2  3 ms  4 ms  2 ms  10.10.10.1
  3  4 ms  2 ms  2 ms  192.168.2.1
  4  2 ms  1 ms  10 ms  192.168.20.3

Trace complete.

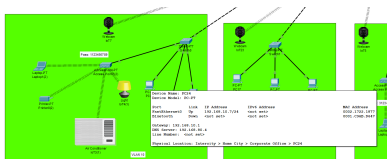
C:\>

```

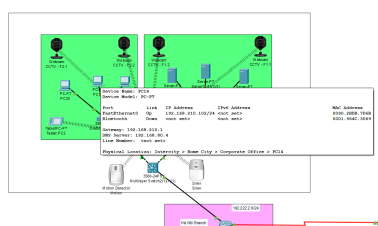
Hình 24: Đà Nẵng Branch to Headquarter

## 5.4 Connect to server in the DMZ

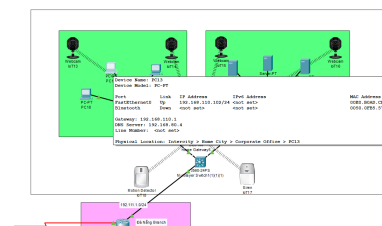
Nhóm sẽ kiểm tra bằng 3 PC ở 3 nơi lần lượt là trụ sở, chi nhánh Hà Nội và chi nhánh Đà Nẵng. Thông tin của từng máy như sau:



Hình 25: Máy tính ở trụ sở



Hình 26: Máy tính ở chi nhánh Hà Nội



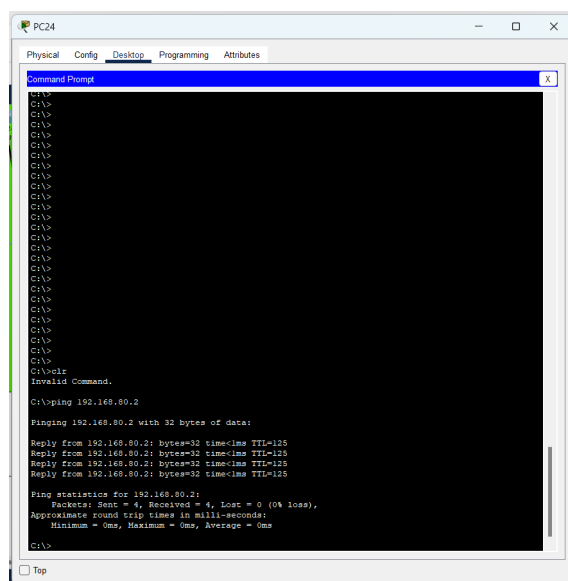
Hình 27: Máy tính ở chi nhánh Đà Nẵng



Nhóm sẽ tiến hành kiểm tra bằng cách ping và chạy các service cho các máy bất kỳ:

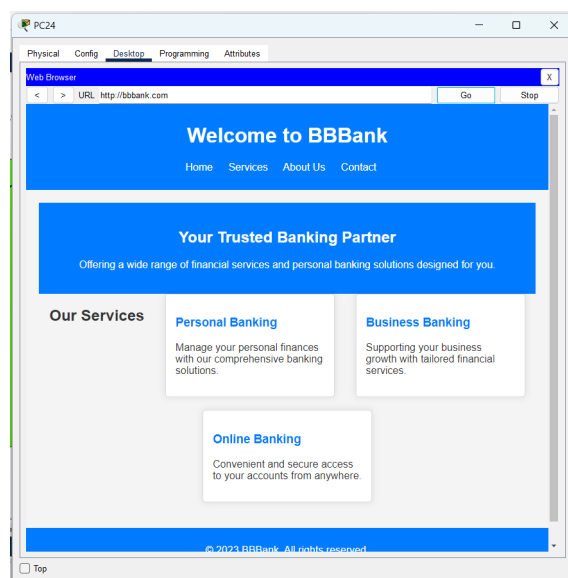
Đối với máy ở trụ sở:

Nhóm ping máy đến IP của web server là 192.168.80.2:



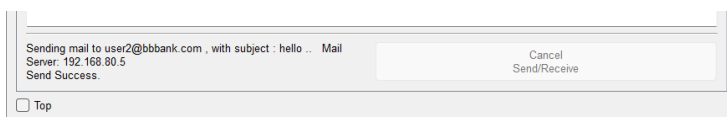
Hình 28: ping từ máy trụ sở đến vùng DMZ

Tiếp theo nhóm truy cập tên miền **bbbank.com** cho máy ở trụ sở:

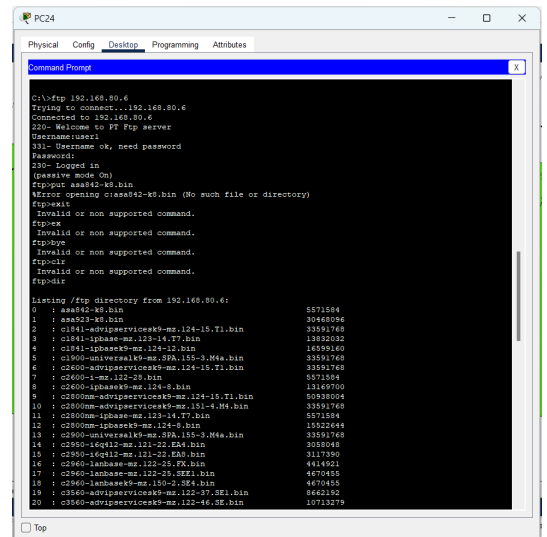


Hình 29: ping từ máy trụ sở đến vùng DMZ

Các dịch vụ tương ứng khác (Email và FTP):

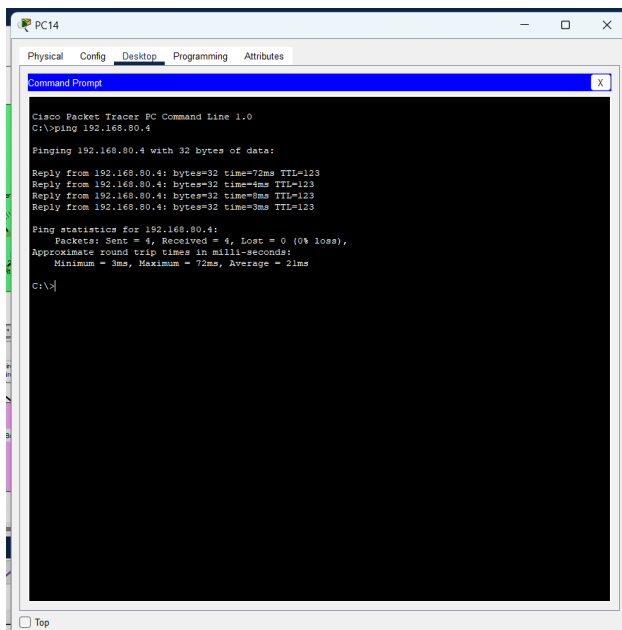


Hình 30: Dịch vụ Email

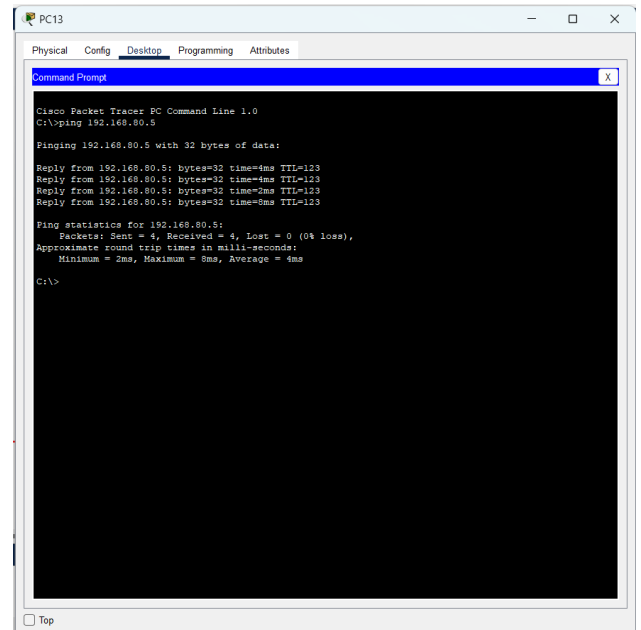


Hình 31: Dịch vụ FTP

Để đảm bảo dịch vụ từ DMZ không bị gián đoạn khi kết nối với các chi nhánh, nhóm cũng tiến hành ping để kiểm tra kết nối giữa DMZ và trụ sở:



Hình 32: ping từ chi nhánh Hà Nội



Hình 33: ping từ chi nhánh Đà Nẵng

Trong hình trên, máy từ Hà Nội đang ping đến DNS server và máy từ Đà Nẵng đang ping đến Web server.

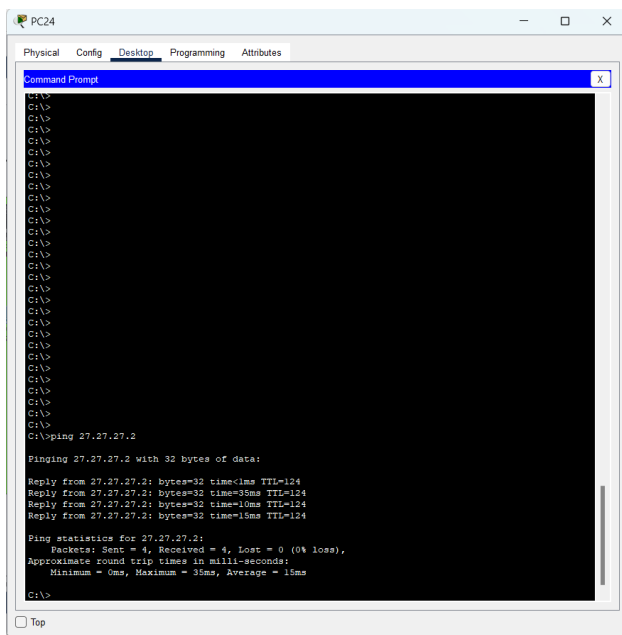
### 5.5 No connections from Customers' devices to PCs on the LAN

Nhóm thiết kế trên tường lửa như sau:

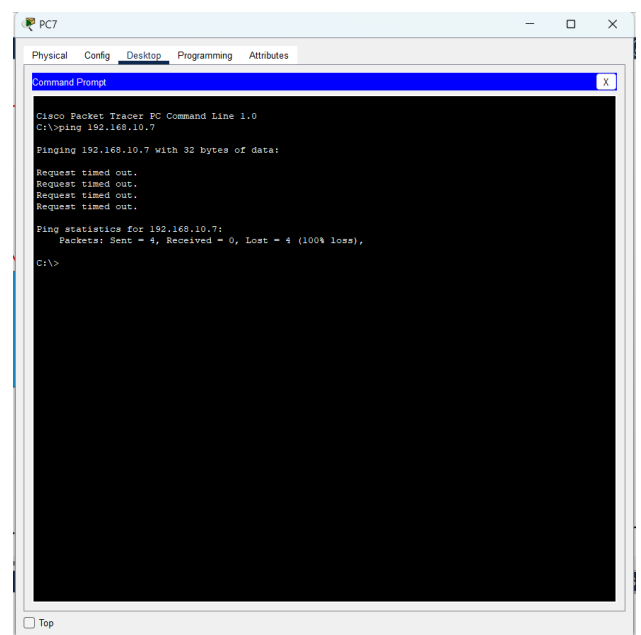
- Tạo luật (rule) cụ thể cho 1 subnet thuộc vùng nội bộ và cho ping ra máy customer ở vùng ngoại.
- Tuy nhiên, máy ở ngoài không được phép kết nối với máy nội bộ, tín hiệu có nguồn gốc từ máy ngoài gửi tới sẽ bị tường lửa chặn.

Mô tả tình huống: Máy ở vùng ngoài có IP thuộc dải địa chỉ 27.27.27.0 gửi vào máy nội bộ có dải địa chỉ là 192.168.10.0:

Kết quả kỳ vọng: Máy nội bộ có thể ping thành công máy ngoài nhưng ping đến từ máy ngoài không được phép đi vào vùng nội bộ (bị tường lửa chặn).



**Hình 34:** ping từ nội bộ ra ngoài



**Hình 35:** ping từ ngoài vào nội bộ

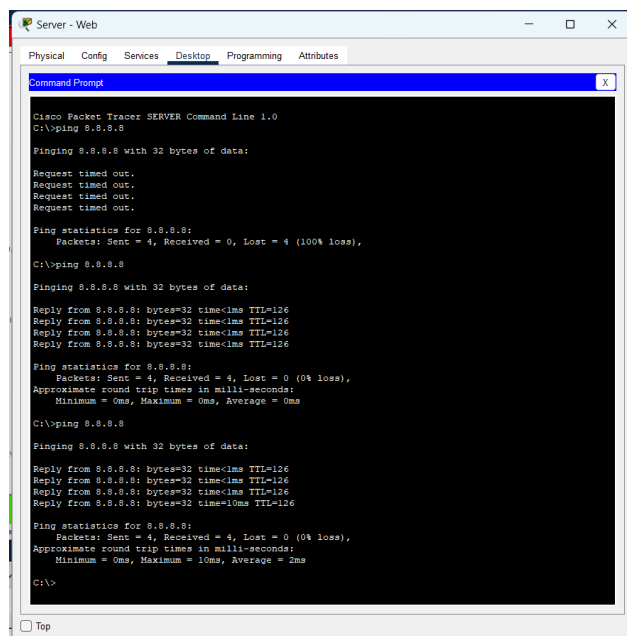
Như trong ảnh, có thể thấy khi ping từ máy nội bộ thì kết quả là thành công nhưng khi ping từ máy vùng ngoài vào thì tường lửa không cho phép tín hiệu đi qua nên ping máy ngoài hiện **Request time out**.

## 5.6 Connect to the Internet to a Web Server

Nhóm đặt ở vùng ngoài thêm 1 server tượng trưng cho Internet với tên là Google.com. Nhóm sẽ tiến hành cấu hình tường lửa để cho phép kết nối dịch vụ web (địa chỉ IP là 192.168.80.2) từ vùng DMZ ra đến Internet (với địa chỉ IP là 8.8.8.8).

Kết quả kỳ vọng: Tường lửa cho phép server web ping được Internet từ server google.com nhưng ngăn chặn internet ping ngược lại web server.

Kết quả cho thấy, sau 3 lần ping thì web ping thành công internet còn internet sau 3 lần ping đều **Request time out** do đã bị tường lửa chặn tín hiệu.



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

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

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=126ms TTL=126
Reply from 8.8.8.8: bytes=32 time=126ms TTL=126
Reply from 8.8.8.8: bytes=32 time=126ms TTL=126
Reply from 8.8.8.8: bytes=32 time=126ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 8.8.8.8

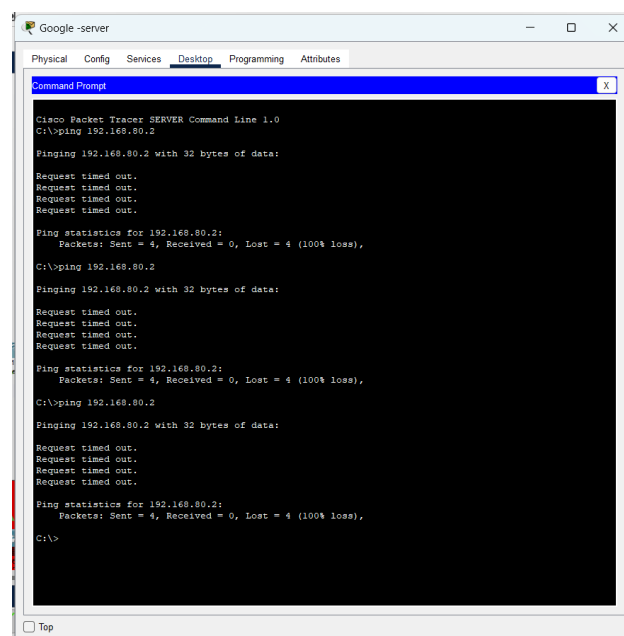
Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=126ms TTL=126
Reply from 8.8.8.8: bytes=32 time=126ms TTL=126
Reply from 8.8.8.8: bytes=32 time=126ms TTL=126
Reply from 8.8.8.8: bytes=32 time=105ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 105ms, Average = 2ms

C:\>
```

Hình 36: ping từ web server đến internet



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.80.2

Pinging 192.168.80.2 with 32 bytes of data:

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

Ping statistics for 192.168.80.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.80.2

Pinging 192.168.80.2 with 32 bytes of data:

Reply from 192.168.80.2: bytes=32 time=126ms TTL=126
Reply from 192.168.80.2: bytes=32 time=126ms TTL=126
Reply from 192.168.80.2: bytes=32 time=126ms TTL=126
Reply from 192.168.80.2: bytes=32 time=105ms TTL=126

Ping statistics for 192.168.80.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 105ms, Average = 2ms

C:\>
```

Hình 37: ping từ internet đến web server

## 6 STEP 6

### 6.1 Re-evaluate the designed network system

#### Tính Ổn định:

- Thiết kế mạng bao gồm nhiều nhánh và một trung tâm theo mô hình mạng diện rộng.
- Cần xem xét tính dự phòng, có thể sử dụng các giao thức như HSRP (Giao thức Định tuyến Dự phòng Nhanh) hoặc VRRP (Giao thức Dự phòng Định tuyến Ảo) để chuyển tiếp giữa các bộ định tuyến trong trường hợp một bộ định tuyến gặp sự cố.
- Ngoài ra, khi số lượng các workstation tăng lên thì nhóm cũng cần nhắc để chuyển sang cấu hình theo phương thức LACP để đảm bảo việc di chuyển tín hiệu không bị ngưng, trễ khi có nhiều workstation cần làm việc.
- Sự hiện diện của các kết nối đa điểm giữa các nút cho thấy việc tạo ra tính dự phòng nhằm cải thiện tính ổn định.

#### Dễ nâng cấp:

- Nếu mạng được xây dựng theo mô-đun (như được gợi ý bởi sự hiện diện của các phân đoạn mạng riêng biệt), việc nâng cấp có thể được thực hiện từng mô-đun, giảm thiểu thời gian ngừng hoạt động của toàn bộ hệ thống.
- Sử dụng các giao thức và thiết bị có khả năng mở rộng sẽ giúp thuận tiện cho việc nâng cấp trong tương lai mà không cần phải thực hiện thay đổi lớn.

#### Hỗ trợ Phần mềm Đa dạng:

- Thiết kế mạng nên tích hợp các công cụ quản lý và giám sát mạng để giải quyết vấn đề và bảo trì một cách chủ động.
- Hỗ trợ cho các nền tảng phần mềm khác nhau gợi ý việc sử dụng các giao thức và giao diện tiêu chuẩn để đảm bảo tính tương thích và tích hợp với các ứng dụng và dịch vụ khác nhau.

### An toàn và Bảo mật Mạng:

- Nhóm sử dụng tường lửa để ngăn chặn các truy cập trái phép từ miền ngoài tiến vào vùng DMZ và vùng mạng nội bộ. Hiện tại, tường lửa thiết kế cho phép DMZ và mạng nội bộ có thể kết nối với internet ở miền ngoài nhưng ngăn chặn toàn bộ các truy cập ngược từ bên ngoài vào trong nội bộ.
- Cần thực hiện cập nhật thường xuyên và chính sách bảo mật để bảo vệ khỏi các mối đe dọa tiến hóa.
- Phân đoạn (có thể được biểu thị bằng các khu vực được mã màu khác nhau) có thể cô lập lưu lượng và ngăn chặn các vi phạm tiềm ẩn.

### Vấn đề còn lại cho Dự án:

- Tường lửa mới chỉ ở mức cấu hình cơ bản, cho phép mạng nội bộ sử dụng tự do các dịch vụ từ DMZ và ngăn chặn các địa chỉ IP không có trong ACL tiến vào mạng nội bộ (ngoại trừ Internet)

### Hướng phát triển trong tương lai:

- Chuyển dịch sang mô hình SDN (Mạng Định nghĩa Bằng Phần mềm) có thể mang lại sự linh hoạt và kiểm soát cao hơn cũng như tiết kiệm chi phí năng cấp và bảo trì thiết bị.
- Cấu hình lại các vấn đề an ninh liên quan đến tường lửa để có chính sách bảo mật chặt chẽ và an toàn hơn.
- Mở rộng khả năng mạng không dây đồng thời đảm bảo bảo mật mạnh mẽ với WPA3 và các giao thức tiên tiến khác.
- Áp dụng các thiết bị IoT (Internet of Things) và tính toán biên để phân phối xử lý gần nguồn dữ liệu và giảm độ trễ.

### Tài liệu tham khảo

- [1] *Adding an Extended Access List*. [https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa\\_84\\_cli\\_config/acl\\_extended.pdf](https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/acl_extended.pdf).
- [2] *Category: 120 Labs CCNA*. <https://itexamanswers.net/120-labs/page/16>.
- [3] *Cisco IOS VPN Configuration Guide*. [https://www.cisco.com/c/en/us/td/docs/security/vpn\\_modules/6342/vpn\\_cg/6342site3.html](https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html).
- [4] *How to configure wireless network in packet tracer*. <https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-wireless-network-in-packet-tracer.html>.
- [5] *Inter-VLAN Routing*. <https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=4>.
- [6] *IP Routing: OSPF Configuration Guide*. [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html).