

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



## Mạng máy tính (CO3093)

### Báo cáo bài tập lớn 2

# Thiết kế, mô phỏng hạ tầng mạng cho một công ty lớn

Giảng viên lý thuyết: Phạm Trần Vũ

Giảng viên thực hành: Vũ Thành Tài

Sinh viên: Dinh Công Minh 2212027

Trương Quang Nghĩa 2212243

Phạm Lê Huy 2252260

Trần Thế Đại Phát 2212537

THÀNH PHỐ HỒ CHÍ MINH, THÁNG MUÒI HAI 2024



## Danh sách thành viên & Phân chia công việc

STT	Họ và tên	MSSV	Công việc	Đóng góp
1	Dinh Công Minh	2212027	Thiết kế và hiện thực hệ thống	100%
2	Trương Quang Nghĩa	2212243	Thiết kế và hiện thực hệ thống	100%
3	Phạm Lê Huy	2252260	Làm báo cáo	100%
4	Trần Thế Đại Phát	2212537	Làm bài thuyết trình	100%



## Mục lục

<b>1 Tổng quan</b>	<b>5</b>
1.1 Mô tả . . . . .	5
1.2 Yêu cầu . . . . .	5
<b>2 Phân tích và thiết kế hệ thống mạng</b>	<b>7</b>
2.1 Phân tích kiến trúc của các tầng . . . . .	7
2.2 Thiết kế mạng . . . . .	9
2.2.1 Loại kết nối . . . . .	9
2.2.2 Giải pháp an ninh mạng . . . . .	16
2.2.3 Hệ thống giám sát và thiết bị ngoại vi . . . . .	16
2.2.4 VPN . . . . .	18
2.2.5 VLAN . . . . .	19
2.3 Kết nối mạng . . . . .	21
2.3.1 Tổng quan về lưu lượng . . . . .	21
2.3.2 Tính toán thông lượng và băng thông . . . . .	22
2.3.3 Các tùy chọn nhà cung cấp dịch vụ Internet . . . . .	23
2.3.4 Các tùy chọn đường dây thuê (Leased Lines) . . . . .	24
2.4 Bảng tổng kết chi phí . . . . .	25
<b>3 Thiết kế sơ đồ mạng sử dụng Cisco Packet Tracer</b>	<b>25</b>
3.1 Tổng quan . . . . .	25
3.2 Tính kết nối liên thông (Interconnectivity) . . . . .	27
3.2.1 Mạng WAN . . . . .	27
3.2.2 Kết nối giữa các phòng ban . . . . .	28
3.2.3 Kết nối giữa các thiết bị trong cùng một phòng ban . . . . .	31
3.2.4 Kết nối giữa các mạng LAN và Internet . . . . .	32
3.3 Phân đoạn VLAN . . . . .	32
3.4 Mạng bên ngoài . . . . .	35
3.4.1 Vùng DMZ . . . . .	35
3.4.2 Kết nối người làm việc từ xa . . . . .	36
3.4.3 Site-to-Site VPN . . . . .	39
<b>4 Mô phỏng hệ thống mạng</b>	<b>39</b>
4.1 Kết nối giữa các máy tính trong cùng VLAN . . . . .	39
4.2 Kết nối các PC giữa các VLAN . . . . .	41



---

4.2.1	Kết nối một PC từ phòng vận hành & pháp lý với một PC trong phòng ngân hàng . . . . .	41
4.2.2	Kết nối một PC từ một phòng ban HCM đến một máy chủ . . . . .	41
4.3	Kết nối các PC giữa trụ sở chính và các chi nhánh . . . . .	42
4.3.1	Kết nối PC từ HCM đến một PC ở Hà Nội . . . . .	42
4.3.2	Kết nối PC ở Hà Nội với máy chủ Mail ở HCM . . . . .	44
4.4	Kết nối đến các máy chủ trong DMZ . . . . .	45
4.5	Không có kết nối từ thiết bị của khách hàng đến các PC trong mạng LAN . . . . .	47
4.5.1	Không thể kết nối từ Laptop của khách hàng đến PC ở tầng 2 . . . . .	47
4.5.2	Không thể kết nối từ Laptop của khách hàng đến máy chủ . . . . .	47
4.6	Kết nối đến Internet đến một máy chủ Web . . . . .	48
4.6.1	Kết nối từ PC HCM Tầng 2 đến địa chỉ 8.8.8.8 ở Internet . . . . .	48
4.6.2	Kết nối từ PC tại Hà Nội đến máy chủ Web bằng trình duyệt Web qua HTTP . . . . .	51
4.6.3	Kết nối từ máy khách tại trụ sở Hồ Chí Minh đến máy chủ ở Internet . . . . .	53
4.7	Bảo mật . . . . .	53
4.8	Hệ thống ngăn chặn xâm nhập (IPS) . . . . .	54
<b>5</b>	<b>Dánh giá hệ thống mạng</b>	<b>56</b>
5.1	Dánh giá bảo mật . . . . .	56
5.2	Dánh giá khả năng mở rộng . . . . .	56
5.3	Các vấn đề chưa giải quyết . . . . .	56
5.4	Định hướng thiết kế trong tương lai . . . . .	56



# 1 Tổng quan

## 1.1 Mô tả

CCC (Computer & Construction Concept) được yêu cầu thiết kế mạng máy tính để triển khai tại Trụ sở chính (tại TP HCM) và hai chi nhánh (Đà Nẵng và Hà Nội) của ngân hàng BB đang được xây dựng. Nhóm sinh viên được giao nhiệm vụ thiết kế và triển khai hệ thống mạng cho các tòa nhà này. Nhóm cần đề xuất giải pháp nhằm hiện thực hóa một hệ thống mạng hiệu quả, hỗ trợ giám sát và quản lý tòa nhà, đồng thời tối ưu hóa chi phí năng lượng.

## 1.2 Yêu cầu

Các đặc điểm chính trong hạ tầng mạng của ngân hàng bao gồm:

### 1. Trụ sở chính:

- Cơ sở hạ tầng:
  - Tòa nhà trụ sở chính gồm 7 tầng, tầng một được trang bị một phòng CNTT và trung tâm cáp mạng (sử dụng thanh đấu mạng (patch panel) để tập hợp dây).
  - Quy mô trung bình: 120 máy trạm, 5 máy chủ, 12 thiết bị mạng (hoặc có thể nhiều hơn với các thiết bị chuyên về bảo mật).
  - Sử dụng công nghệ mới cho cơ sở hạ tầng mạng bao gồm kết nối có dây và không dây, cáp quang (GPON), GigaEthernet 1GbE/10GbE. Mạng được tổ chức theo cấu trúc VLAN cho các phòng ban khác nhau.
- Mạng WAN:
  - Mạng con của trụ sở chính kết nối với mạng con của hai chi nhánh thông qua 2 kênh thuê riêng (áp dụng SD-WAN hoặc MPLS) và 2 xDSL để truy cập Internet, tích hợp cơ chế cân bằng tải (load balancing).
  - Tất cả lưu lượng truy cập Internet đi qua mạng con của trụ sở chính.
- Phần mềm: Sử dụng kết hợp giữa phần mềm có bản quyền và mã nguồn mở, bao gồm ứng dụng văn phòng, ứng dụng client-server, đa phương tiện, và cơ sở dữ liệu.
- Yêu cầu:
  - Bảo mật cao (tường lửa, IPS/IDS, phát hiện phishing).



- Có tính khả dụng cao (High Availability), hệ thống phải hoạt động ổn định khi có sự cố.
- Dễ dàng bảo dưỡng và nâng cấp hệ thống.
- Cấu hình đề xuất:
  - VPN site-to-site và kết nối từ xa (teleworker) đến LAN của Công ty.
  - Hệ thống camera giám sát cho toàn Công ty.

## 2. Chi nhánh:

- Cở sở hạ tầng:
  - Mỗi tòa nhà gồm 2 tầng, tầng một được trang bị 1 phòng CNTT và 1 trung tâm cáp mạng.
  - Quy mô nhỏ: 30 máy trạm, 3 máy chủ, 5 thiết bị mạng hoặc hơn.
- Mạng WAN:
  - Thực hiện kết nối giữa trụ sở chính và chi nhánh qua liên kết WAN, sử dụng các công nghệ như SD-WAN hoặc MPLS, tùy thuộc vào chi phí của giải pháp.
  - Đề xuất các tùy chọn với chi phí phù hợp.
  - Phân tích ưu điểm và nhược điểm của giải pháp đã chọn.

Ngoài ra, các khung giờ cao điểm khi mà lưu lượng truy cập chiếm hơn 80% tải hệ thống xảy ra vào các khung giờ: 9h-11h và 15h-16h. Sự phân bổ về truy cập dữ liệu tới Trụ sở chính và các chi nhánh có thể được phân bổ như sau:

- Máy chủ dành cho cập nhật phần mềm, truy cập web, và truy cập cơ sở dữ liệu. Giải sử tổng lượng tải xuống cho từng các máy chủ là như nhau, ước tính: 1000 MB/ngày. Tải lên: 2000 MB/ngày.
- Mỗi máy trạm phục vụ duyệt web, tải tài liệu, và giao dịch khách hàng. Tải xuống: 500 MB/ngày. Tải lên: 100 MB/ngày.
- Các thiết bị kết nối WiFi của khách hàng tải xuống khoảng 500 MB/ngày.

Bên cạnh đó, hệ thống mạng của BB Bank dự kiến sẽ có tốc độ tăng trưởng 20% trong vòng 5 năm (bao gồm số lượng người dùng, tải hệ thống mạng, mở rộng chi nhánh, ...).



## 2 Phân tích và thiết kế hệ thống mạng

### 2.1 Phân tích kiến trúc của các tầng

#### Tổng quan

Thiết kế mạng cần đáp ứng đầy đủ yêu cầu hệ thống với nhiều phương án được đề xuất, kèm theo ưu điểm, nhược điểm và chi phí. Do đó, nhóm chia hệ thống thành các phần nhỏ hơn và tập trung phân tích từng phần.

1. Khảo sát và thiết kế bố trí mạng cho công ty, sau đó đề xuất các sơ đồ mạng.
2. Phân tích thiết bị và sơ đồ mạng ở cấp độ tổng quát.
3. Tính toán lưu lượng dữ liệu và khuyến nghị các gói dịch vụ phù hợp từ nhà cung cấp dịch vụ Internet (ISP).
4. Thiết kế và mô phỏng sơ đồ mạng cụ thể từ danh sách được đề xuất.

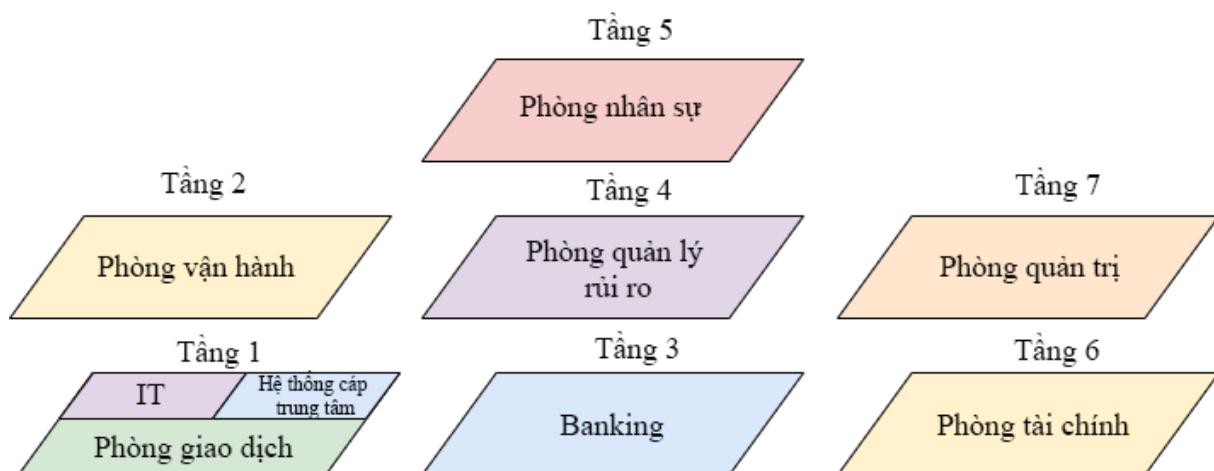
**Khảo sát kiến trúc** Các thông tin cần được ghi nhận trong cuộc khảo sát các văn phòng tại tòa nhà bao gồm:

- Vị trí của tòa nhà:
  - Khu vực lắp đặt thiết bị mạng, thiết bị bảo mật và các thiết bị ngoại vi.
  - Các chướng ngại vật và yếu tố gây nhiễu (điện tòa nhà, từ trường môi trường,...) có thể ảnh hưởng đến tín hiệu mạng.
- Yêu cầu cụ thể theo từng phòng ban:
  - Số lượng người dự kiến trong mỗi phòng.
  - Chức năng và các yêu cầu bảo mật của từng phòng.

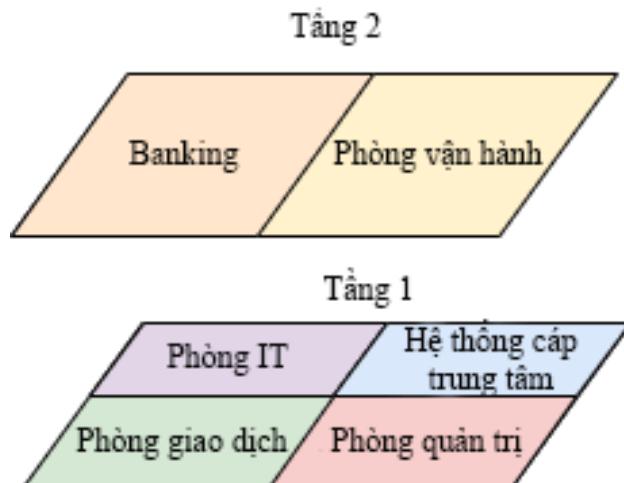
**Phân tích bố trí** Dựa trên nghiên cứu thực tế tại các văn phòng của ngân hàng BB, nhóm thu thập được thông tin về các phòng ban tại trụ sở chính, 2 chi nhánh, và bố trí vật lý của 3 văn phòng như sau:



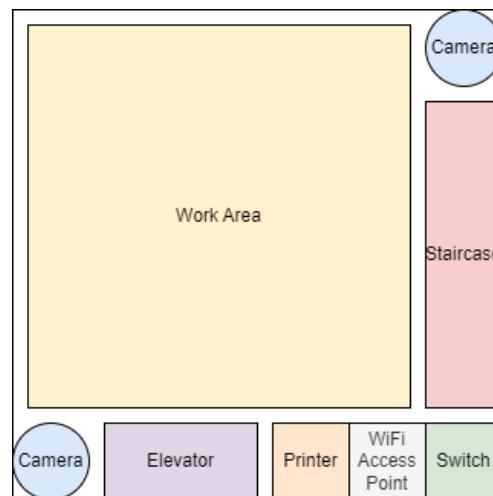
Chi nhánh	Tên phòng ban	Số máy trạm
Trụ sở chính	Banking	20
	Vận hành	20
	Quản lý rủi ro	20
	Tài chính	20
	Nhân sự	20
	IT	10
	Quản trị viên	10
Chi nhánh	Banking	10
	Vận hành	10
	IT	5
	Quản trị viên	5



Hình 2.1: Bố trí tòa Trụ sở chính



Hình 2.2: Bố trí tòa nhà chi nhánh



Hình 2.3: Sơ đồ bố trí cài đặt cho một phòng làm việc.

## 2.2 Thiết kế mạng

### 2.2.1 Loại kết nối

Nhóm xem xét hai tùy chọn đầu tiên để lựa chọn, đó là loại kết nối của các máy trạm. Đầu tiên, cần mua một bộ định tuyến (router) Cisco ISR4331/K9 cho trụ sở chính (HQ) và mỗi chi nhánh, cùng với 4 bộ chuyển mạch Ethernet (Cisco 4-Port Gigabit Ethernet Switch NIM NIM-ES2-4).

Ngoài ra, một công ty sử dụng mạng có dây cần có các điểm truy cập Wi-Fi để phục vụ khách hàng và kết nối các thiết bị ngoại vi.



Đối với kết nối có dây, công nghệ mới nhất và ổn định nhất hiện nay là Ethernet-Cat8. Ưu điểm của nó là cung cấp tốc độ lên đến 40Gbps và giảm nhiễu, nhưng nhược điểm chính là dây cáp kém linh hoạt. Chúng ta vẫn cần 11 bộ chuyển mạch (Cisco 24 Port Catalyst 2960 WS-C2960-24TC-L) và 11 điểm truy cập Wi-Fi nhẹ (TPLink Archer C54) cho 7 tầng của trụ sở chính và 2 tầng của mỗi chi nhánh.

Đối với kết nối không dây, có thể chọn 11 điểm truy cập công nghệ Wi-Fi 6E (Cisco CW9162I-MR 802.11ax Wi-Fi 6E 2x2:2 Access Point). Ưu điểm của tùy chọn này là không bị giới hạn bởi số lượng cổng Ethernet, nhưng nhược điểm là có thể bị nhiễu do nhiều máy trạm cùng truy cập Internet.

Mỗi thiết bị với thông số kỹ thuật và chi phí điển hình như sau:

1. Router Cisco ISR4331/K9



Hình 2.4: Router: Cisco ISR4331/K9

- Chi phí: 25,000,000 VND
- Thông lượng tổng hợp: 100 Mbps đến 300 Mbps
- Tổng số cổng WAN hoặc LAN 10/100/1000 tích hợp: 3
- Cổng RJ45: 2
- Cổng SFP: 2
- Khe cắm mô-đun dịch vụ nâng cao (SM-X): 1
- Khe cắm mô-đun giao diện mạng (NIM): 2
- Khe cắm ISC tích hợp: 1
- Bộ nhớ: 4 GB (mặc định) / 16 GB (tối đa)

- Bộ nhớ Flash: 4 GB (mặc định) / 16 GB (tối đa)
- Tùy chọn nguồn: Nguồn nội bộ: AC và PoE
- Chiều cao rack: 1 RU
- Kích thước: 44.45 x 438.15 x 438.15 mm
- Trọng lượng đóng gói: 12.96 Kg

2. Card mạng: Cisco 4-Port Gigabit Ethernet Switch NIM NIM-ES2-4



Hình 2.5: Card mạng Cisco 4-Port Gigabit Ethernet Switch NIM NIM-ES2-4

- Chi phí: 10,000,000 VND
- Hình dạng: Mô-đun NIM đơn rộng
- Kích thước: 0.8 x 3.1 x 4.8 in.
- Trọng lượng: 79g (0.17 lb)
- Tiêu chuẩn: IEEE 802.3, 802.1q, 802.1X, RFC 2284, RFC 1213, v.v
- Khả năng quản lý:
  - Hỗ trợ SNMP và Telnet
  - Tích hợp agent RMON
  - Cổng SPAN cho giám sát
  - TFTP để nâng cấp phần mềm
  - Đèn LED hiển thị trạng thái
- Kết nối:



- Cổng: 10BASE-T, 100BASE-TX, 1000BASE-TX
- Cáp: Kết nối RJ-45, cáp UTP
- Yêu cầu nguồn điện:
  - Nguồn nội bộ với tùy chọn PoE
  - Hỗ trợ nguồn DC trên một số mẫu
- Hỗ trợ phần mềm: Cisco IOS-XE Software Release 3.15
- Môi trường:
  - Nhiệt độ hoạt động: 32° đến 104°F
  - Độ ẩm hoạt động: 10 đến 90
  - Độ cao: Lên đến 15,000 ft
  - Tuân thủ quy định:
  - Đạt tiêu chuẩn của các router dòng Cisco 4000

### 3. Switch: Cisco 24 Port Catalyst 2960 WS-C2960-24TC-L



Hình 2.6: Cisco 24 Port Catalyst 2960 WS-C2960-24TC-L

- Chi phí: 15,000,000 VND
- Tiêu chuẩn gắn rack: Có thẻ gắn rack 1U
- Bộ tính năng: LAN Base
- Cổng uplink: 2 (SFP hoặc 1000BASE-T)
- Số cổng: 24 x Cổng Ethernet 10/100



- Hiệu suất:
  - Băng thông chuyển tiếp: 16 Gbps
  - Tốc độ chuyển tiếp: 6.5 Mpps
- Bộ nhớ:
  - RAM: 128 MB
  - Bộ nhớ flash: 64 MB
- Kích thước: 4.4 cm x 45.0 cm x 24.2 cm
- Trọng lượng: 7.73 Kg

#### 4. Cáp Ethernet-Cat8



Hình 2.7: Cáp Ethernet-Cat8

- Chi phí: 400,000 VND/cáp dài 10 mét
- Tốc độ truyền tải: 40 Gbps
- Băng thông: 2000 MHz
- Chống nhiễu: 4 lớp bảo vệ
- Lõi dây: Đồng nguyên chất 30 AWG
- Vỏ cáp: Dây bện 48 sợi

#### 5. Điểm truy cập: TP-Link Archer C54



Hình 2.8: TPLink Archer C54

- Chi phí: 400,000 VND
- WiFi
  - Chuẩn: Wi-Fi 5
  - Tốc độ: 867 Mbps (5 GHz), 300 Mbps (2.4 GHz)
  - Phạm vi phủ sóng: Căn hộ 3 phòng ngủ, 4× ăng-ten
  - Khả năng: Trung bình
  - Băng tần kép: Có
  - MU-MIMO: 2×2
- Phần cứng: Cổng Ethernet: 1× WAN, 4× LAN (10/100 Mbps)
- Bảo mật: Mã hóa Wi-Fi: WPA, WPA2
- Phần mềm:
  - Bảo mật mạng: Tường lửa SPI, Kiểm soát truy cập
  - Mạng khách: 1× 5 GHz, 1× 2.4 GHz

## 6. Điểm truy cập Wi-Fi 6E: Cisco CW9162I-MR



Hình 2.9: Cisco CW9162I-MR

- Chi phí: 25,000,000 VND
- Thông số kỹ thuật
  - Mã sản phẩm: CW9162I-MR
  - Phần mềm: Chuẩn 802.11ax
  - MU-MIMO: 2x2 (6 GHz up/down, 2.4 GHz và 5 GHz down)
  - Tính năng: OFDMA, TWT, BSS coloring, MRC, Beamforming 802.11ax
  - Kênh: 20/40/80/160 MHz (6 GHz), 20/40/80 MHz (5 GHz), 20 MHz (2.4 GHz)
  - Tốc độ dữ liệu PHY: Lên đến 3.9 Gbps
  - Gộp gói dữ liệu: A-MPDU, A-MSDU
  - Hỗ trợ: DFS, CSD, WPA3
- Ảng-ten tích hợp:
  - Tần số 2.4 GHz: 4 dBi, hướng đa chiều
  - Tần số 5 GHz: 5 dBi, hướng đa chiều
  - Tần số 6 GHz: 5 dBi, hướng đa chiều
- Interface:
  - Cổng Ethernet: 1 × 100M/1000M/2.5G Multigigabit, RJ-45
  - Cổng quản lý: RJ-45, USB 2.0 (4.5W)
- Đèn báo hiệu
  - LED trạng thái:



- \* Bộ tải khởi động
- \* Kết nối
- \* Trạng thái hoạt động
- \* Cảnh báo, lỗi
- Kích thước và trọng lượng
  - Kích thước: 7.8 x 7.8 x 1.7 in. (200 x 200 x 44.45 mm)
  - Trọng lượng: 2.05 lb. (0.93 kg)
- Bộ nhớ hệ thống
  - DRAM: 2048 MB
  - Flash: 1024 MB

### 2.2.2 Giải pháp an ninh mạng

Giải pháp bảo mật có thể được đề xuất theo kiến trúc DMZ. Một DMZ sẽ bao gồm một Firewall và các máy chủ xử lý tương tác từ phía khách hàng hoặc đi ra ngoài. Phần mềm: Giấy phép Cisco SEC-K9

- Giá: 27,258,507 VND
- Mục đích: Tăng cường bảo mật trên các bộ định tuyến và switch của Cisco.
- Tính năng chính:
  - Hỗ trợ VPN cho kết nối từ xa an toàn.
  - Mã hóa nâng cao để bảo mật dữ liệu.
  - Tích hợp khả năng tường lửa.
  - Hệ thống ngăn chặn xâm nhập (IPS) để bảo vệ mạng.
  - Tùy chọn lọc nội dung.

### 2.2.3 Hệ thống giám sát và thiết bị ngoại vi

Một lựa chọn khác cho BB Bank là thiết kế hệ thống giám sát và thiết bị ngoại vi dựa trên khung công nghệ Internet of Things (IoT) hoặc để từng thiết bị độc lập xử lý các chức năng khác nhau.

**Lựa chọn thiết bị độc lập** Nếu chọn tùy chọn thứ hai, hệ thống có thể được thiết kế sao cho hệ thống giám sát truyền dữ liệu đến phòng IT thông qua điểm truy cập WiFi

hoặc router gần nhất. Các thiết bị ngoại vi như thiết bị giám sát cháy và còi báo động cho khu vực lưu trữ tiền sẽ hoạt động độc lập.

- **Ưu điểm:** Các thiết bị hoạt động độc lập, không có điểm lỗi duy nhất và chi phí thấp hơn so với tùy chọn IoT.
- **Nhược điểm:** BB Bank sẽ có khả năng kiểm soát hệ thống thấp hơn.

**Hệ thống IoT** Hệ thống IoT có thể được thiết kế phù hợp với bố trí vật lý của 3 địa điểm của BB Bank, kết nối trực tiếp với VLAN của phòng IT. Hệ thống này sẽ kiểm soát các thiết bị ngoại vi và hệ thống giám sát, được quản lý bởi phòng IT.

- **Ưu điểm:** Giúp BB Bank kiểm soát tốt hơn không gian làm việc, cải thiện hiệu suất tổng thể của hệ thống.
- **Nhược điểm:**
  - Chi phí cao hơn so với tùy chọn trước.
  - Yêu cầu đội ngũ IT có chuyên môn để duy trì hệ thống.
  - Có điểm lỗi duy nhất.

**Đè xuât hệ thống giám sát:** Camera: DS-2GN5750-HH



Hình 2.10: DS-2GN5750-HH

- Giá: 4.335.000 VNĐ
- Tính năng nổi bật:



- Hình ảnh chất lượng cao với độ phân giải 4 MP.
- Hiệu suất ánh sáng yếu xuất sắc.
- Công nghệ nén H.265+ hiệu quả.
- Chống nước và bụi (IP67).
- Hình ảnh màu sắc 24/7.
- Hỗ trợ phát hiện người và phương tiện.

#### Số lượng camera tại trụ sở chính:

Tầng	Số lượng camera
1	3
2-7	2 mỗi tầng

#### Số lượng camera tại các chi nhánh:

Tầng	Số lượng camera
1	2
2	1

#### 2.2.4 VPN

##### Cấu hình VPN Site-to-Site

###### 1. Yêu cầu cấu hình VPN Site-to-Site:

- Kết nối trụ sở chính với các chi nhánh khu vực bằng VPN Site-to-Site sử dụng giao thức IPSec để đảm bảo giao tiếp an toàn và mã hóa giữa các địa điểm.
- Mỗi chi nhánh sẽ có một cổng VPN riêng kết nối với máy chủ VPN trung tâm tại trụ sở chính. Cấu hình này cho phép chia sẻ tài nguyên liền mạch và duy trì tính nhất quán trong bảo mật.
- VPN sẽ được cấu hình hỗ trợ các giao thức định tuyến động như OSPF hoặc BGP để quản lý lưu lượng mạng hiệu quả.

###### 2. Giải pháp lựa chọn: Cisco Meraki MX Series

- Tính năng: Tích hợp SD-WAN và các tính năng bảo mật, quản lý qua đám mây giúp đơn giản hóa các thiết lập VPN phức tạp.



- Chi phí: Từ 14.500.000 VND cho mẫu rẻ nhất (MX67).

### Cấu hình VPN Teleworker

#### 1. Yêu cầu cấu hình VPN Teleworker:

- Nhân viên làm việc từ xa sẽ được cung cấp phần mềm VPN client để cài đặt trên thiết bị làm việc của họ. Phần mềm này sẽ tạo kết nối an toàn tới mạng LAN của BB Bank.
- VPN Teleworker sẽ sử dụng mã hóa SSL/TLS, mang lại sự cân bằng giữa bảo mật cao và tính dễ sử dụng mà không cần thêm phần cứng.
- Xác thực đa yếu tố (MFA) sẽ được triển khai để tăng cường bảo mật, đảm bảo chỉ những người được ủy quyền mới có thể truy cập mạng của ngân hàng từ xa.

#### 2. Giải pháp lựa chọn: Cisco AnyConnect Secure Mobility Client

- Tính năng: Đảm bảo tuân thủ điểm cuối, bảo mật truy cập mạng mạnh mẽ, bảo vệ khi duyệt web và di chuyển, hiển thị mạng, hỗ trợ thiết bị di động, và các tùy chọn VPN nâng cao để kết nối linh hoạt và an toàn từ xa.
- Chi phí: 100.943.200 VND cho giấy phép eDelivery với 100 kết nối đồng thời.

### 2.2.5 VLAN

VLAN sẽ được triển khai trên toàn bộ mạng của BB Bank để chia nhỏ mạng thành các phần dễ quản lý hơn. Sự phân đoạn này giúp cải thiện hiệu suất, tăng cường bảo mật và đơn giản hóa quản lý mạng.

VLAN hiệu quả trong việc tách biệt lưu lượng của các bộ phận khác nhau, đảm bảo hiệu quả hoạt động và bảo mật dữ liệu.

Mỗi bộ phận trong BB Bank (ví dụ: Kế toán, Nhân sự, Dịch vụ khách hàng) sẽ có VLAN riêng. Phương pháp này đảm bảo rằng lưu lượng và tài nguyên liên quan đến từng bộ phận được cách ly, từ đó giảm lưu lượng không cần thiết và tăng cường bảo mật.

Kích thước của từng VLAN được xác định dựa trên số lượng nhân sự (ước tính giới hạn trên) và chức năng của từng bộ phận.

**Bảng kế hoạch IP VLAN:**



Tên VLAN	Kích thước VLAN	Subnet
Phòng thông tin	254	192.168.10.0/24
Phòng Vận Hành & Pháp lý	254	192.168.20.0/24
Banking	254	192.168.30.0/24
Quản lý rủi ro	254	192.168.40.0/24
Nhân sự	254	192.168.50.0/24
Tài chính	254	192.168.60.0/24
Hành chính	254	192.168.70.0/24

Bảng kế hoạch IP VLAN chi nhánh Hà Nội:

Tên VLAN	Kích thước VLAN	Subnet
Banking	254	172.16.20.0/24
Phòng thông tin	254	172.16.10.0/24

Bảng kế hoạch IP VLAN chi nhánh Đà Nẵng:

Tên VLAN	Kích thước VLAN	Subnet
Banking	254	10.0.20.0/24
Phòng thông tin	254	10.0.10.0/24

### Chi tiết phân đoạn VLAN

- Tầng 1: Chứa các máy tính IT, máy chủ và thiết bị khách hàng, hỗn hợp nhiều chức năng.
- Các tầng khác: Mỗi tầng là nơi làm việc của một bộ phận khác nhau và được phân đoạn với VLAN riêng biệt.

Việc này giúp:

- Tách biệt rõ ràng giữa các lưu lượng mạng.
- Đảm bảo quyền riêng tư dữ liệu và tăng cường bảo mật.
- Tối ưu hóa hiệu quả hoạt động và quản lý tài nguyên mạng.



## 2.3 Kết nối mạng

Về mặt kết nối mạng, chúng ta cần tính toán thông lượng yêu cầu và băng thông dự kiến để đảm bảo việc truyền dữ liệu diễn ra mượt mà và hiệu suất tối ưu cho các thiết bị và hệ thống được kết nối.

- **Băng thông:** Là tốc độ tối đa mà dữ liệu có thể được truyền qua mạng, thường được đo bằng Megabit mỗi giây (Mbps), phản ánh khả năng lưu thông thông tin.
- **Thông lượng:** Là lượng dữ liệu thực tế được truyền thành công qua một kênh truyền thông trong một khoảng thời gian nhất định, phản ánh hiệu quả thực tế của việc truyền dữ liệu.

### 2.3.1 Tổng quan về lưu lượng

Dòng dữ liệu và khối lượng công việc của hệ thống tại trụ sở chính được phân loại như sau:

- **Máy chủ:** Tổng tải lên và tải xuống của 5 máy chủ:
  - Tải xuống:  $1000 \times 5 = 5000$  MB/ngày
  - Tải lên:  $2000 \times 5 = 10000$  MB/ngày
- **Máy trạm:** Tổng tải lên và tải xuống của 120 máy trạm:
  - Tải xuống:  $500 \times 120 = 60000$  MB/ngày
  - Tải lên:  $100 \times 120 = 12000$  MB/ngày
- **Thiết bị khách hàng:** Với ước tính 50 khách hàng mỗi ngày:
  - Tải xuống:  $500 \times 50 = 25000$  MB/ngày
  - Tải lên: 0 MB/ngày

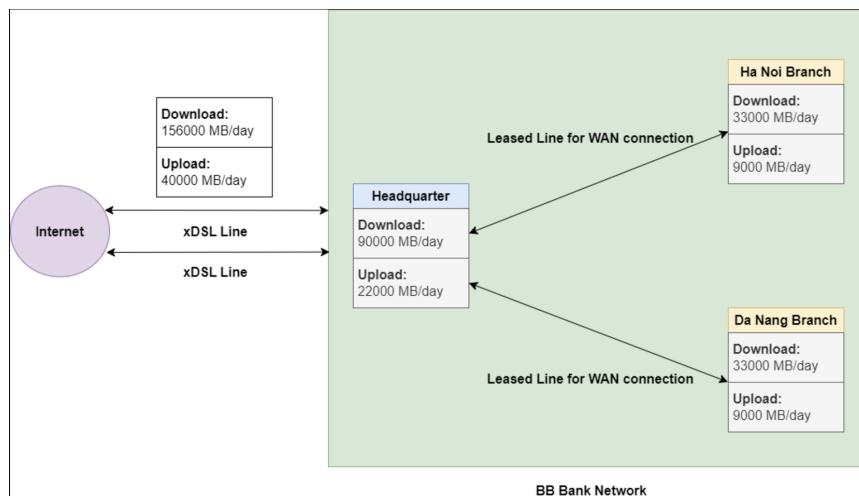
Tóm lại, DHQ = 90000 MB/ngày and UHQ = 22000 MB/ngày. Mặt khác, lưu lượng dữ liệu và khối lượng công việc của hệ thống tại mỗi chi nhánh có thể được phân loại như sau:

- **Máy chủ:** Tổng tải lên và tải xuống của 3 máy chủ:
  - Tải xuống:  $1000 \times 3 = 3000$  MB/ngày
  - Tải lên:  $2000 \times 3 = 6000$  MB/ngày

- Máy trạm: Tổng tải lên và tải xuống của 30 máy trạm:
  - Tải xuống:  $500 \times 30 = 15000 \text{ MB/ngày}$
  - Tải lên:  $100 \times 30 = 3000 \text{ MB/ngày}$
- Thiết bị khách hàng: Với ước tính 30 khách hàng mỗi ngày:
  - Tải xuống:  $500 \times 50 = 15000 \text{ MB/ngày}$
  - Tải lên: 0 MB/ngày

Tóm lại, DB = 33000 MB/ngày và UB = 9000 MB/ngày.

Vậy tổng lượng tải xuống cho một ngày là  $90000 + 33000 + 33000 = 156000 \text{ (MB/ngày)}$  và tổng lượng tải lên cho một ngày là  $22000 + 9000 + 9000 = 40000 \text{ (MB/ngày)}$



Hình 2.11: Tổng quan về Network Dataflow của BB Bank ở thời điểm hiện tại

### 2.3.2 Tính toán thông lượng và băng thông

Với 80% lưu lượng dữ liệu tập trung vào các giờ cao điểm từ 9 giờ sáng đến 11 giờ sáng và 3 giờ chiều đến 4 giờ chiều, chúng ta có thể tính toán thông lượng trung bình trong 3 giờ cao điểm này. Ngoài ra, cần dự phòng thêm 20% (tăng 1.2) để đáp ứng nhu cầu tăng trưởng trong tương lai 5 năm đến cho cả việc sử dụng thiết bị và số lượng thiết bị trên mạng của ngân hàng. Lưu lượng dữ liệu cần sử lý trong giờ cao điểm là:

- Tải xuống:

$$\frac{156000 \times 0.8 \times 1.2 \times 8}{3 \times 60 \times 60} = 110.93 \text{ Mbps}$$



- Tải lên:

$$\frac{40000 \times 0.8 \times 1.2 \times 8}{3 \times 60 \times 60} = 28.44 \text{ Mbps}$$

Vì lưu lượng dữ liệu trong giờ cao điểm xác định thông lượng trung bình, nhà cung cấp dịch vụ Internet (ISP) cần cung cấp băng thông lớn hơn 111 Mbps tải xuống và 29 Mbps tải lên để đảm bảo hoạt động kinh doanh diễn ra ổn định.

### 2.3.3 Các tùy chọn nhà cung cấp dịch vụ Internet

Một số tùy chọn ISP có thể được xem xét:

#### **VNPT: FIBERVIP6**

Lựa chọn này đặc biệt hữu ích vì băng thông đáp ứng yêu cầu đã tính toán ở trên. WAN tĩnh hỗ trợ ngân hàng BB với địa chỉ IP cố định và không thay đổi, đặc biệt hữu ích khi ngân hàng sử dụng máy chủ DNS riêng.

- Chi phí: 1.000.000 VND/tháng (không bao gồm chi phí lắp đặt).
- Cấu hình:
  - 1 IPv4 WAN tĩnh.
  - 1 Subnet/56 IPv6 LAN tĩnh.
- Tốc độ trong nước: 200 Mbps.

#### **FPT: SUPER250**

Đây là một tùy chọn khả thi khác cho ngân hàng BB. Mặc dù không cung cấp 1 Subnet/56 IPv6 LAN tĩnh, nhưng tốc độ quốc tế cao với chi phí gần như tương đương là một lợi thế.

- Chi phí: 1.045.000 VND/tháng (chi phí lắp đặt: 100.000 VND).
- Cấu hình: 1 IPv4 WAN tĩnh.
- Tốc độ trong nước: 250 Mbps.
- Tốc độ quốc tế: Lên đến 10.8 Mbps.

#### **Viettel: F200N**

Đây cũng là một lựa chọn tốt. Tuy nhiên, tốc độ quốc tế của Viettel thấp hơn so với FPT.

- Chi phí: 1.100.000 VND/tháng (không bao gồm chi phí lắp đặt).



- Cấu hình: 1 IPv4 WAN tĩnh.
- Tốc độ trong nước: 200 Mbps.
- Tốc độ quốc tế: 2 Mbps.

#### 2.3.4 Các tùy chọn đường dây thuê (Leased Lines)

Một số tùy chọn đường dây thuê có thể được liệt kê như sau:

##### VNPT

Chi phí hàng tháng rất cao, VNPT cung cấp băng thông 34 Mbps, phù hợp cho kết nối giữa chi nhánh và trụ sở chính.

- Chi phí: 51.120.000 VND/tháng, chi phí lắp đặt 30.000.000 VND cho mỗi đường dây.
- Băng thông: 34 Mbps.

##### Viettel

Chi phí lắp đặt cao hơn nhưng có chi phí hàng tháng thấp hơn, tùy chọn này rõ ràng là sự lựa chọn tốt hơn cho ngân hàng BVBANK.

- Chi phí: 41.498.000 VND/tháng, chi phí lắp đặt 40.000.000 VND cho mỗi đường dây.
- Băng thông: 34 Mbps.



## 2.4 Bảng tổng kết chi phí

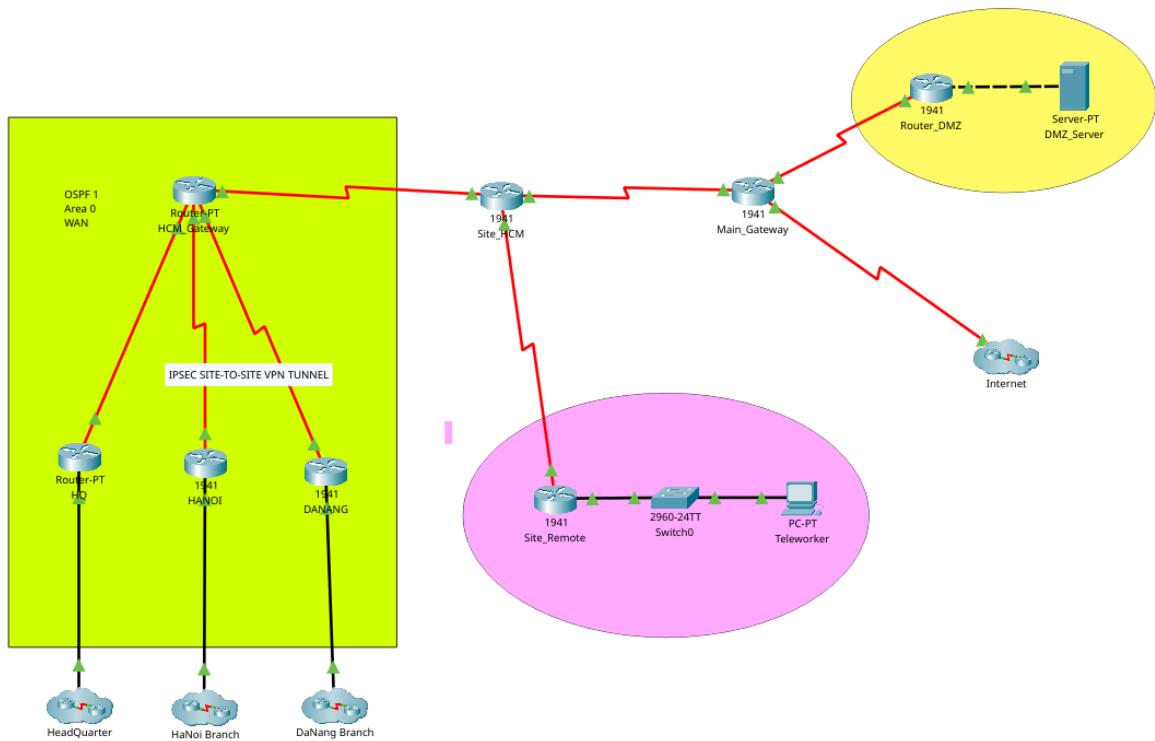
Danh mục	Tên thiết bị	Số lượng	Giá mỗi đơn vị (VND)	Tổng chi phí (VND)
Router	Cisco ISR4331/K9 (Trụ sở + 2 Chi nhánh)	3	25,000,000	75,000,000
Card mạng	Cisco 4-Port Gigabit Ethernet Switch	4	10,000,000	40,000,000
Switch	Cisco 24 Port Catalyst 2960	11	15,000,000	165,000,000
Cáp mạng	Baseus Cat8 10m Cable	Nhiều	400,000	4,000,000
Điểm truy cập (có dây)	TPLink Archer C54	11	400,000	4,400,000
Điểm truy cập (không dây)	Cisco CW9162I-MR Wi-Fi 6E	11	25,000,000	275,000,000
Bảo mật mạng	Cisco SEC-K9 License	1	27,258,507	27,258,507
Camera giám sát	DS-2GN5750-HH	21	4,335,000	91,035,000
Giải pháp VPN	Cisco Meraki MX Series	3	14,500,000	43,500,000
VPN từ xa	Cisco AnyConnect License (100 kết nối)	1	100,943,200	100,943,200
<b>Tổng chi phí đầu tư ban đầu</b>				<b>826,136,707</b>
Chi phí ISP hàng tháng	Viettel F200N	1	1,100,000	1,100,000/tháng
Đường truyền thuê bao	Viettel	1	41,498,000	41,498,000/tháng
<b>Chi phí vận hành hàng tháng</b>				<b>42,598,000/tháng</b>

Bảng 2.1: Bảng chi phí đầu tư và vận hành mạng

## 3 Thiết kế sơ đồ mạng sử dụng Cisco Packet Tracer

### 3.1 Tổng quan

Dưới đây là cái nhìn tổng quan về việc triển khai trong Packet Tracer.



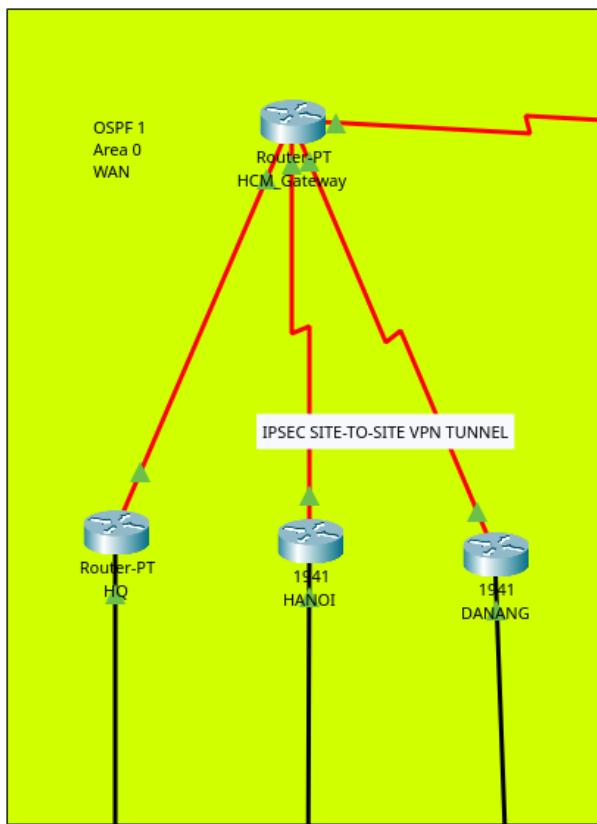
Hình 3.1: Tổng quan về thiết kế mạng BBBank trong Packet Tracer

Sơ đồ mạng bao gồm một số thành phần của hệ thống mạng:

- Chi nhánh trụ sở chính: Bao gồm bảy tầng, mỗi tầng chứa các phòng ban khác nhau với nhiều máy trạm, cổng Router kết nối giữa các chi nhánh, cũng như một số máy chủ và thiết bị trung gian.
- Chi nhánh Đà Nẵng và Hà Nội: Mỗi chi nhánh có một tập hợp thiết bị nhỏ hơn so với chi nhánh trụ sở chính, bao gồm các máy trạm và máy chủ địa phương của chúng.
- Khu vực ngoài: Thiết kế cũng bao gồm một số khu vực từ mạng ngoài các chi nhánh, bao gồm khu vực DMZ, "Internet", và kết nối từ Teleworker.

### 3.2 Tính kết nối liên thông (Interconnectivity)

#### 3.2.1 Mạng WAN



Hình 3.2: OSPF 1 Vùng 0 WAN

Sơ đồ trên mô tả kết nối Mạng Khu Vực Rộng (WAN) cho BB Bank với ba chi nhánh, sử dụng OSPF (Open Shortest Path First) làm giao thức định tuyến với cấu hình Area 0. OSPF là một giao thức định tuyến được sử dụng trong các mạng lớn để phân phối thông tin định tuyến IP bằng thuật toán trạng thái liên kết.

- OSPF Area 0 (Khu Vực Lõi):

- Các router trong khu vực này là một phần của Area 0, khu vực lõi trong môi trường mạng OSPF.
- Các địa điểm khác (ví dụ: chi nhánh và các khu vực ngoài) trong mạng phải kết nối với Area 0, làm cho nó trở thành trung tâm trong việc lan truyền các tuyến đường OSPF và đảm bảo tất cả các khu vực có thể giao tiếp hiệu quả với nhau.

- Router-PT HCM Gateway:

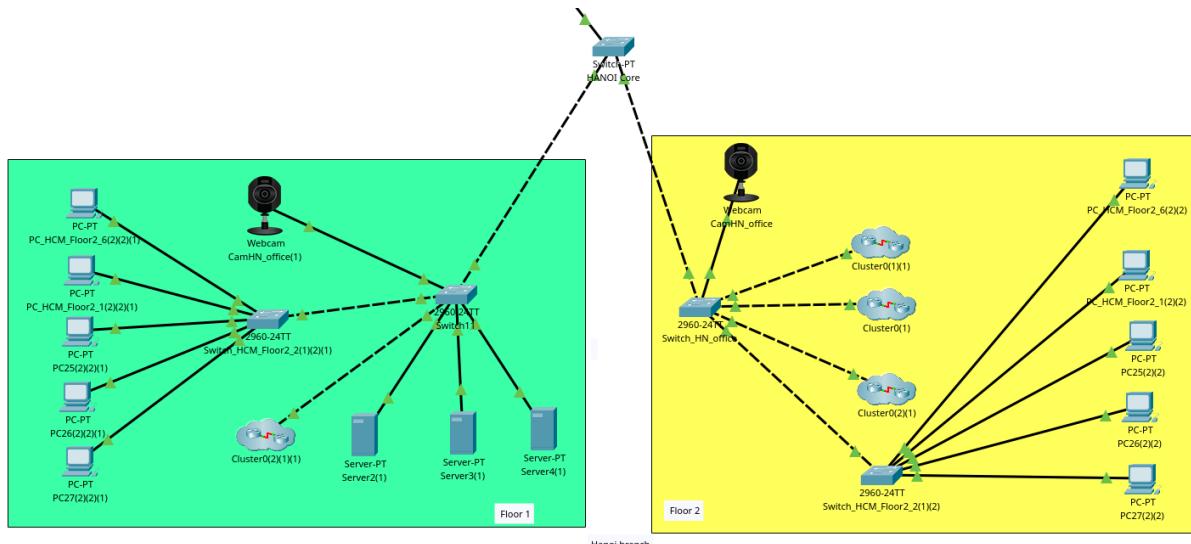
- Dóng vai trò là cổng kết nối cho Trụ sở chính (Headquarter) và là router cốt lõi kết nối tất cả các router chi nhánh.
- Là điểm kết nối đến các mạng khác, chẳng hạn như Internet và khu vực DMZ. Nói cách khác, các chi nhánh Đà Nẵng và Hà Nội sẽ truy cập phần còn lại của mạng ngoài hoặc Internet (được mô tả ở bên trái sơ đồ này) thông qua liên kết này.
- Cổng kết nối với các router chính của mỗi chi nhánh sử dụng các đường dây thuê riêng biệt để đảm bảo kết nối và tải quan trọng.

- Router-PT HQ/HANOI/DANANG:

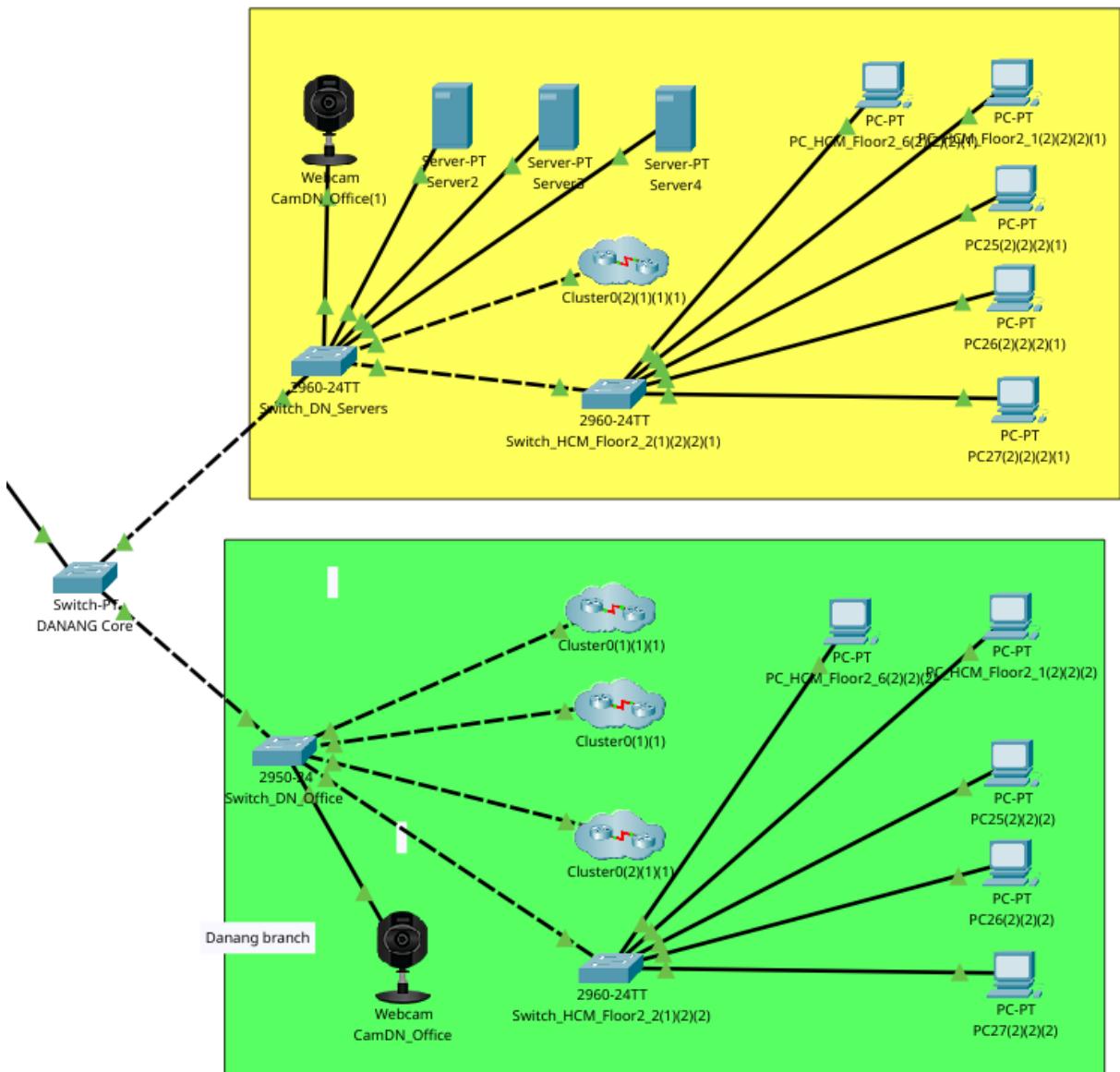
- Là các router chính cho mỗi chi nhánh, cầu nối mạng giữa các khu vực nội bộ và bên ngoài.
- Mỗi router kết nối với mạng nội bộ của chi nhánh bằng Copper Straight-Through.

### 3.2.2 Kết nối giữa các phòng ban

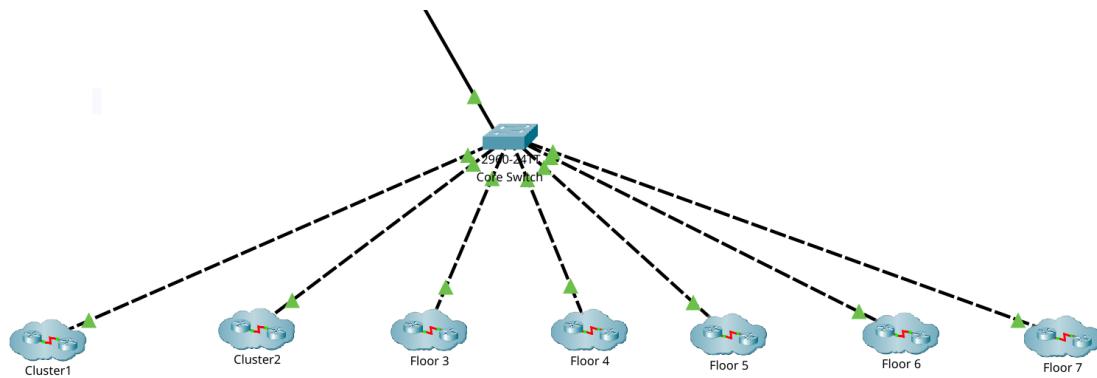
Ở giữa các router chính và các thiết bị mạng nội bộ trong các chi nhánh là ba Core Switch tại tất cả các chi nhánh:



Hình 3.3: Thiết kế site Hà Nội



Hình 3.4: Thiết kế site Đà Nẵng

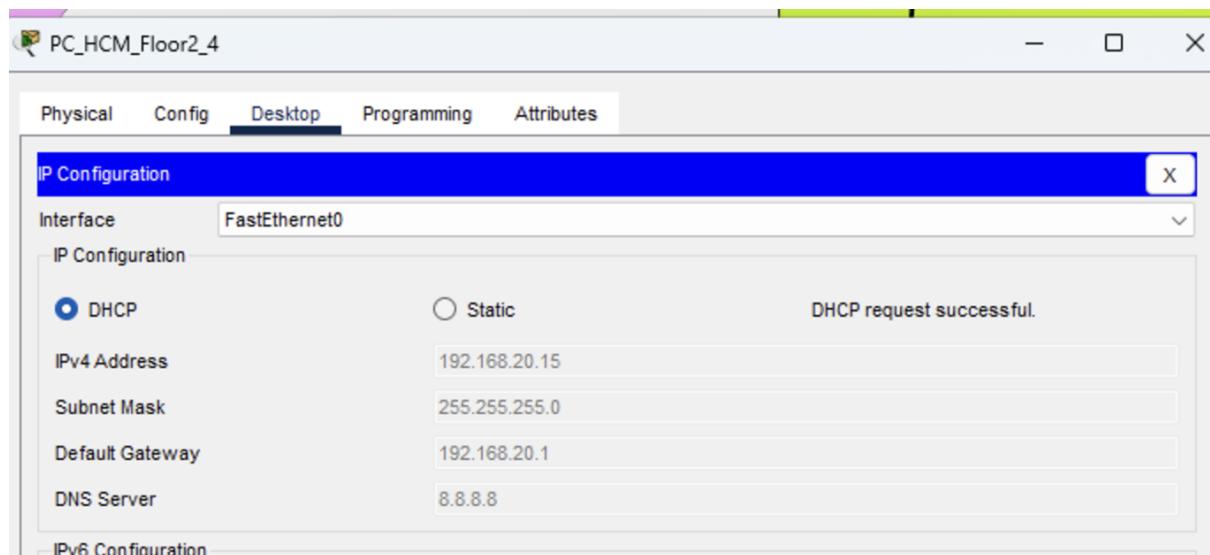


Hình 3.5: Thiết kế site Thành phố Hồ Chí Minh

Trong kiến trúc này, Core Switch đóng vai trò là trung tâm cho mạng của mỗi chi nhánh. Nó chịu trách nhiệm định tuyến và chuyển mạch lưu lượng mạng một cách hiệu quả để đảm bảo kết nối liền mạch giữa các phòng ban và dịch vụ của công ty.

Mỗi tầng hoặc phòng ban trong các chi nhánh có một Access Switch riêng, kết nối lại với Core Switch trung tâm, tạo thành một star topology giúp quản lý lưu lượng mạng một cách tập trung.

Các VLANs trải rộng trên nhiều switch sử dụng các trunk links. Các trunk links mang lưu lượng của tất cả các VLAN mặc định giữa các switch, cho phép các thiết bị trên các VLAN khác nhau (trong trường hợp này là các máy trạm ở các tầng/phòng ban khác nhau) có thể giao tiếp với nhau thông qua thiết bị Layer 3.



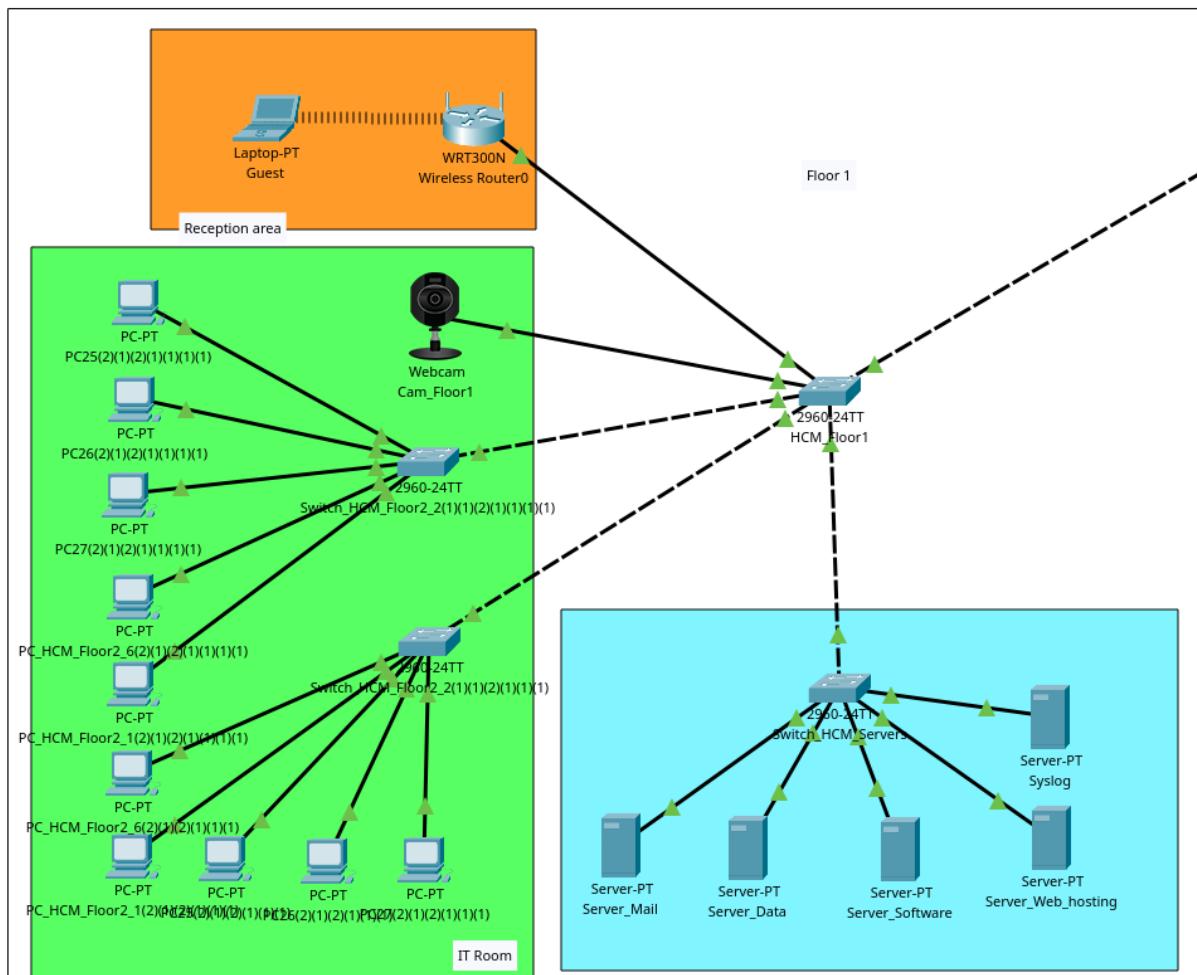
Hình 3.6: Thiết bị cuối sử dụng DHCP để lấy IP

Một cấu hình đã được thiết lập để cho phép mỗi thiết bị nhận địa chỉ IP qua DHCP. Ví dụ, thiết bị dưới đây ở tầng hai (thuộc VLAN 20) nhận địa chỉ IP mong muốn trong phạm vi submask của nó.

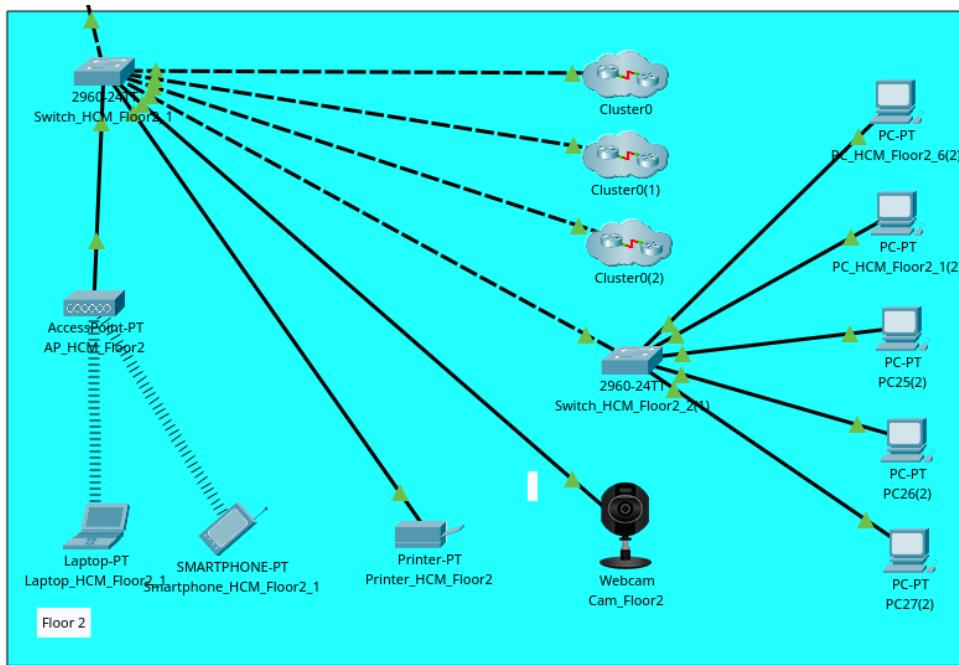
Một số thiết bị khác như IP Camera và Server được cấp địa chỉ IP tĩnh để đảm bảo việc truy cập ổn định và nhất quán.

### 3.2.3 Kết nối giữa các thiết bị trong cùng một phòng ban

Các thiết bị cuối (end devices) ở mỗi tầng/phòng ban được kết nối với switch cấp tầng (floor-level switch), cho phép chúng có thể kết nối và giao tiếp với nhau.



Hình 3.7: Floor-level switch cho tầng 1



Hình 3.8: Floor-level switch cho tầng 2

### 3.2.4 Kết nối giữa các mạng LAN và Internet

Như bạn có thể thấy, các địa chỉ IP nội bộ đã được chuyển đổi thành các địa chỉ IP công cộng. Ví dụ, trong hình ảnh, địa chỉ IP của PC2 ở tầng hai của chi nhánh Đà Nẵng, được chuyển đổi từ 172.16.20.11 thành 209.165.0.2 (địa chỉ IP toàn cầu trên giao diện ngoài Serial 0/1/1 của Main Gateway).

## 3.3 Phân đoạn VLAN

Phần dưới đây sẽ giải thích về cấu hình tại chi nhánh HCM, vì đây là chi nhánh phức tạp nhất, trong khi đó các chi nhánh ở Hà Nội và Đà Nẵng có cấu hình tương tự nhưng quy mô nhỏ hơn.

Mạng được chia logic thành nhiều VLANs, tách biệt các máy chủ quan trọng, nhóm người dùng và lưu lượng khách. Việc phân đoạn này giúp tăng cường bảo mật và quản lý lưu lượng, với việc định tuyến giữa các VLANs được thực hiện bởi các Switch Layer 3 (các core switch đã được đề cập ở phần trên) để tối ưu hóa lưu lượng mạng.



```

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::20A:41FF:FE4C:CD8
IPv6 Address.....: :::
IPv4 Address.....: 172.16.10.15
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
                           172.16.10.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
                           0.0.0.0

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=73ms TTL=122
Reply from 8.8.8.8: bytes=32 time=51ms TTL=122
Reply from 8.8.8.8: bytes=32 time=51ms TTL=122
Reply from 8.8.8.8: bytes=32 time=74ms TTL=122

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 51ms, Maximum = 74ms, Average = 62ms

Main_Gateway>
Main_Gateway>
Main_Gateway>
Main_Gateway>
Main_Gateway>
Main_Gateway#show ip nat statistics
Total translations: 3 (0 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/1/1
Inside Interfaces: Serial0/0/0
Hits: 5 Misses: 8
Expired translations: 5
Dynamic mappings:
Main_Gateway#show ip nat translations
Main_Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.0.2:13    172.16.10.15:13  8.8.8.8:13        8.8.8.8:13
icmp 209.165.0.2:14    172.16.10.15:14  8.8.8.8:14        8.8.8.8:14
icmp 209.165.0.2:15    172.16.10.15:15  8.8.8.8:15        8.8.8.8:15
icmp 209.165.0.2:16    172.16.10.15:16  8.8.8.8:16        8.8.8.8:16
Main_Gateway#

```

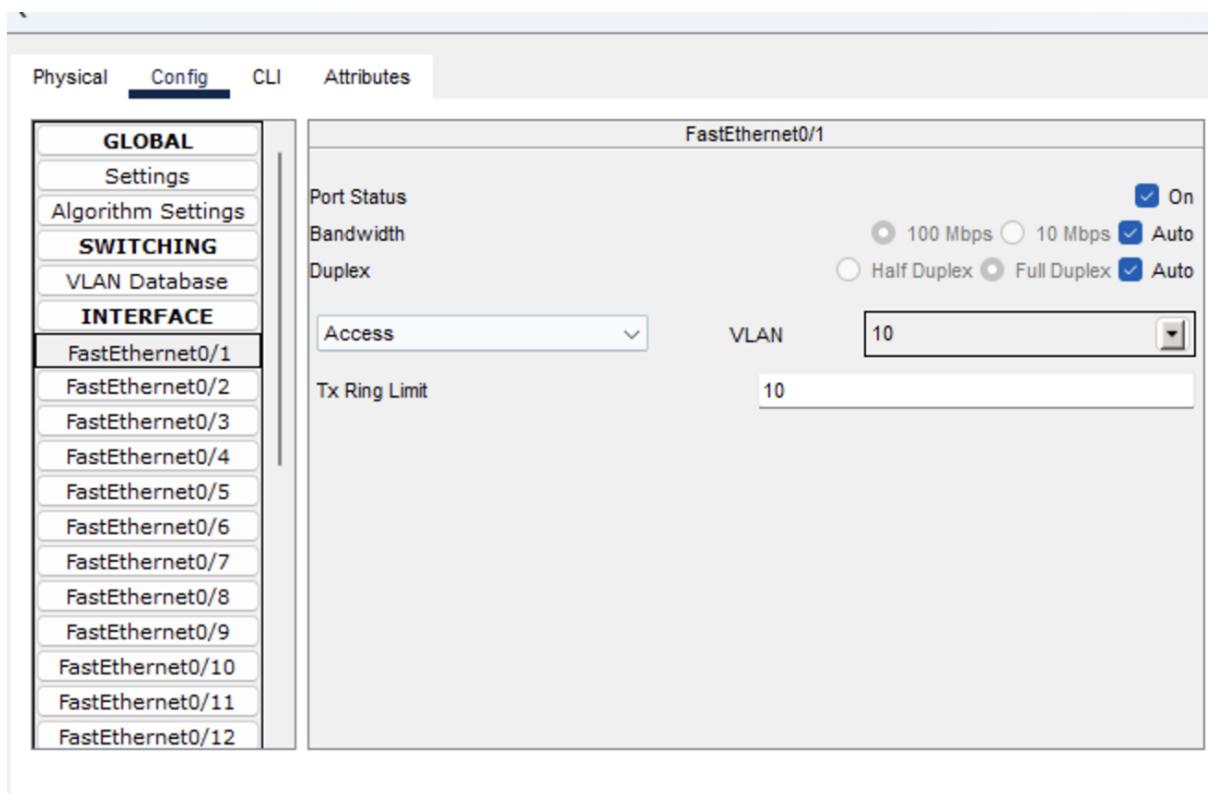
Copy

Hình 3.9: NAT

GLOBAL		VLAN Configuration	
Settings		VLAN Number	
Algorithm Settings		VLAN Name	
SWITCHING		Add	Remove
<b>VLAN Database</b>			
<b>INTERFACE</b>			
FastEthernet0/1		VLAN No	VLAN Name
FastEthernet0/2		1	default
FastEthernet0/3		10	IT
FastEthernet0/4		20	Operations_and_Legal
FastEthernet0/5		30	Banking
FastEthernet0/6		40	Risk_Management
FastEthernet0/7		50	Human_Resources
FastEthernet0/8		60	Finance
FastEthernet0/9		69	VLAN0069
FastEthernet0/10		70	Administration
FastEthernet0/11			
FastEthernet0/12			

Hình 3.10: Cơ sở dữ liệu Core Switch VLAN

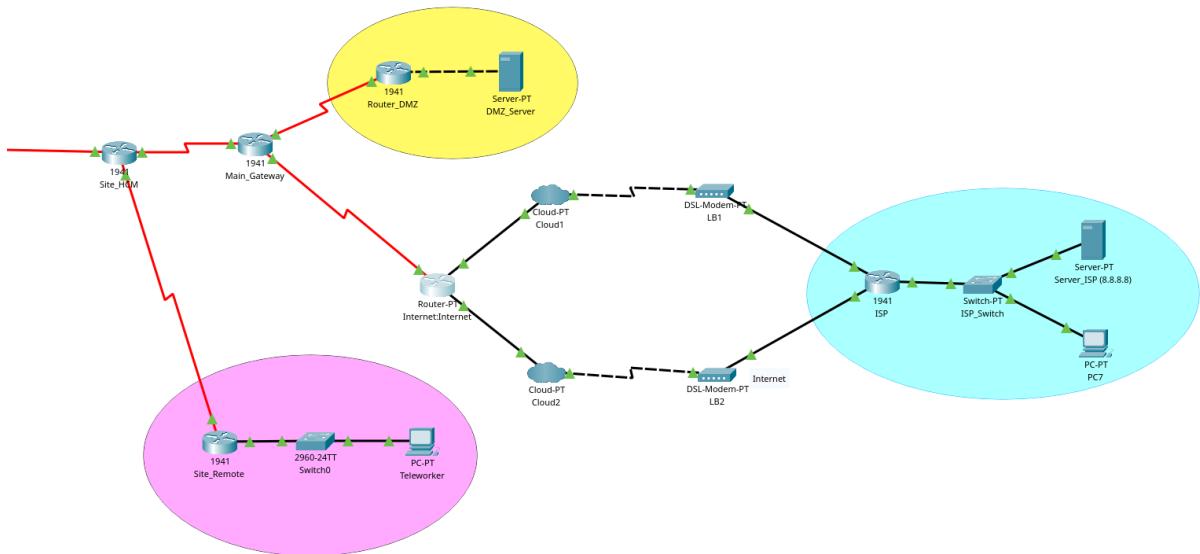
Core Switch được cấu hình để bao gồm các cấu hình VLAN khác nhau, như đã trình bày trong thiết kế ở phần 2.2.5.



Hình 3.11: Core Switch Interfaces

Các switch khác nhau từ mỗi phòng ban được kết nối với các cổng khác nhau trên core switches và được cấu hình để được cấp các VLAN khác nhau, như đã trình bày trong cuộc đàm thoại ở trên.

### 3.4 Mạng bên ngoài



Hình 3.12: Các thành phần mạng ngoại bộ

Sơ đồ trên trình bày một mạng đa chiều với các thành phần cho việc truy cập Internet, một DMZ cho các dịch vụ công khai có thể truy cập và kết nối từ xa cho người làm việc từ xa, tất cả đều được kết nối qua bộ định tuyến Main Gateway kết nối với khu vực WAN như đã giải thích ở phần 3.2.1

#### 3.4.1 Vùng DMZ

Trong mạng máy tính, DMZ, hay Demilitarized Zone, là một subnet vật lý hoặc logic tách biệt mạng LAN nội bộ khỏi các mạng không đáng tin cậy – thường là Internet công cộng. DMZ cũng được gọi là các mạng ngoài biên hoặc các subnet được lọc.

Các máy chủ và tài nguyên trong DMZ có thể truy cập từ Internet, nhưng phần còn lại của mạng LAN nội bộ vẫn không thể truy cập. Cách tiếp cận này cung cấp một lớp bảo mật bổ sung cho mạng LAN vì nó hạn chế khả năng của kẻ tấn công khi muốn truy cập trực tiếp vào các máy chủ và dữ liệu nội bộ từ Internet.

Các mạng DMZ thường được sử dụng cho các mục đích sau:

- Tách biệt và giữ các hệ thống tiềm năng có thể bị tấn công tách khỏi mạng nội bộ;
- Giảm thiểu và kiểm soát việc truy cập vào các hệ thống này từ người dùng bên ngoài;



- Lưu trữ các tài nguyên của công ty để cung cấp một số tài nguyên cho người dùng bên ngoài được ủy quyền.

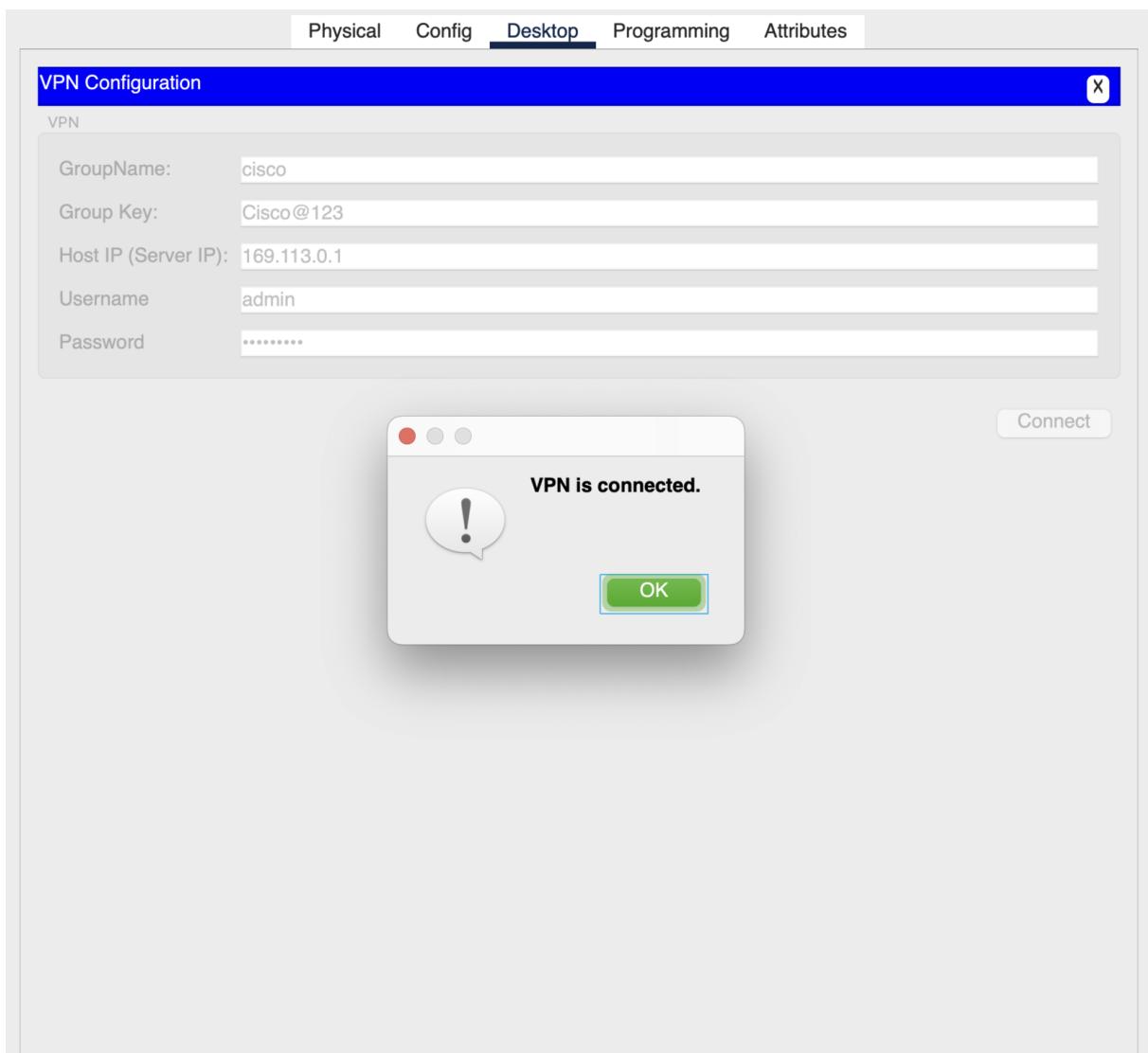
### 3.4.2 Kết nối người làm việc từ xa

Với một VPN, lưu lượng giao tiếp giữa các văn phòng của tổ chức được gửi qua Internet công cộng thay vì qua một mạng độc lập về mặt vật lý. Tuy nhiên, để đảm bảo tính bảo mật, lưu lượng giao tiếp giữa các văn phòng sẽ được mã hóa trước khi đi vào Internet công cộng.

Ở đây, tổ chức bao gồm một trụ sở chính, 2 chi nhánh, và một người làm việc từ xa thường truy cập Internet từ nhà của họ. Trong mạng VPN này, mỗi khi hai máy chủ trong trụ sở chính gửi các datagram IP cho nhau hoặc khi hai máy chủ trong chi nhánh muốn giao tiếp, chúng sử dụng IPv4 truyền thông (tức là không sử dụng dịch vụ IPsec). Tuy nhiên, khi hai máy chủ của tổ chức giao tiếp qua một con đường đi qua Internet công cộng, lưu lượng giao tiếp sẽ được mã hóa trước khi vào Internet.

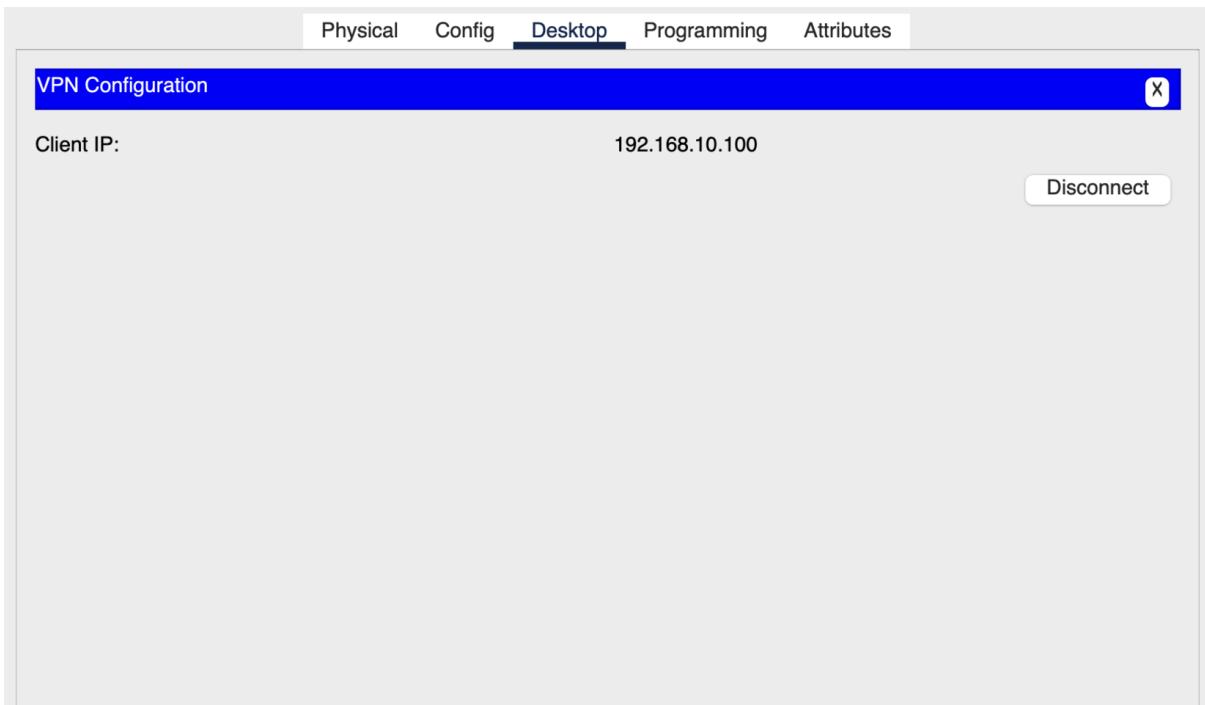
Cấu hình VPN là:

- Group Name: cisco
- Group Key: Cisco@123
- Host IP (Server IP): 169.113.0.1
- Username: admin
- Password: Admin@123



Hình 3.13: Người làm việc từ xa cô gắng kết nối vào VPN

Người làm việc từ xa đã truy cập thành công vào VPN:



Hình 3.14: Người làm việc từ xa truy cập VPN thành công

Bây giờ, người làm việc từ xa có thể truy cập vào máy chủ web tại Trụ sở chính.

```
site_HCM#show crypto ipsec sa
interface: Serial0/0/1
Crypto map tag: MAP1, local addr 169.113.0.1

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.100/255.255.255.255/0/0)
current_peer 9.9.9.9 port 500
PERMIT, flags=(origin_is_acl,)
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 169.113.0.1, remote crypto endpt.:9.9.9.9
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
current outbound spi: 0x920CF6A9(2450323113)

inbound esp sas:
spi: 0x314FD837(827316279)
transform: esp-3des esp-md5-hmac ,
in use settings ={tunnel, }
conn id: 2009, flow_id: FPGA:1, crypto map: MAP1
sa timing: remaining key lifetime (k/sec): (4525504/1452)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:
inbound pcp sas:
outbound esp sas:
--More--
```

```
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=55ms TTL=124
Reply from 8.8.8.8: bytes=32 time=64ms TTL=124
Reply from 8.8.8.8: bytes=32 time=55ms TTL=124
Reply from 8.8.8.8: bytes=32 time=56ms TTL=124

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 64ms, Average = 57ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....:: FE80::201:97FF:FE04:BED7
IPv6 Address.....:: ::
IPV4 Address.....:: 9.9.9.9
Subnet Mask.....:: 255.255.255.0
Default Gateway.....:: 9.9.9.1

Bluetooth Connection:

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....:: ::
IPv6 Address.....:: ::
IPV4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: 0.0.0.0
Tunnel Interface IP Address.....:: 192.168.10.100
```

Hình 3.15: Teleworker có thể ping máy chủ web ở HQ

### 3.4.3 Site-to-Site VPN

Sau khi kết nối giữa 1 PC tại Hà Nội và 1 PC tại Đà Nẵng được thiết lập, tunnel VPN được đặt ở chế độ Active, vì vậy thông tin VPN site-to-site sẽ được hiển thị trên cả hai bộ định tuyến.

```
DANANG>
DANANG>en
DANANG>show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 192.168.3.2
    protected vrf: (none)
    local ident (addr/mask/prot/port): (10.0.0.0/255.255.0.0/0/0)
    remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
    current_peer 192.168.2.2 port 500
        PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

    local crypto endpt.: 192.168.3.2, remote crypto endpt.:192.168.2.2
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
    current outbound spi: 0xD46F03A0(3564045216)

    inbound esp sas:
        spi: 0x60EA7FA9(1625980841)
            transform: esp-aes esp-sha-hmac ,
            in use settings ={Tunnel, }
            conn id: 2006, flow_id: FPGA:1, crypto map: VPN-MAP
            sa timing: remaining key lifetime (k/sec): (4525504/3569)
            IV size: 16 bytes
            replay detection support: N
            Status: ACTIVE

    inbound ah sas:
    inbound pcp sas:

--More--
```

Cisco Packet Tracer PC Command Line 1.0  
C:\>ping 172.16.20.14

Pinging 172.16.20.14 with 32 bytes of data:

Request timed out.  
Request timed out.  
Reply from 172.16.20.14: bytes=32 time=17ms TTL=126  
Reply from 172.16.20.14: bytes=32 time=2ms TTL=126

Ping statistics for 172.16.20.14:  
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 17ms, Average = 9ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:D3FF:FE55:E415
IPv6 Address.....: ::  
IPv4 Address.....: 10.0.20.21
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :: 10.0.20.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::  
IPv6 Address.....: ::  
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :: 0.0.0.0

Hình 3.16: Gói tin liên lạc giữa hai chi nhánh đã được mã hóa

## 4 Mô phỏng hệ thống mạng

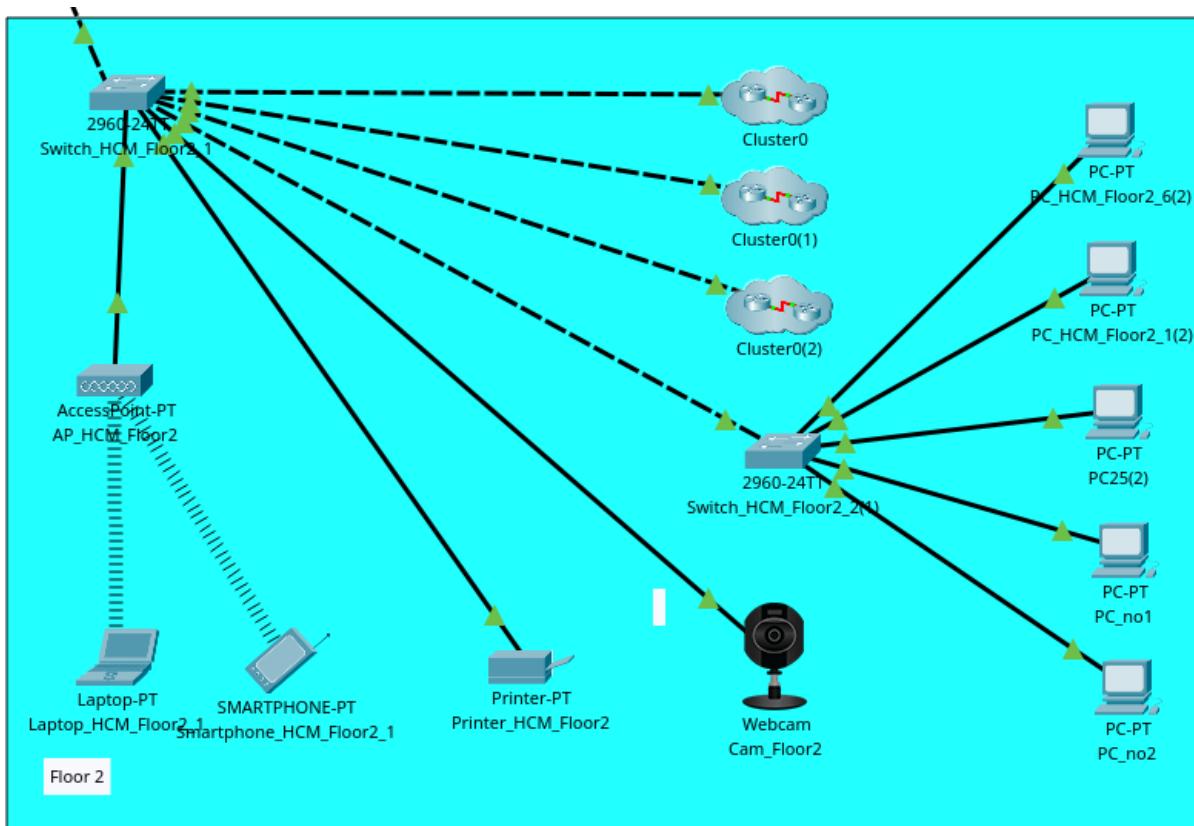
Nhiều bài kiểm tra được thực hiện để xác nhận kết nối theo yêu cầu. Lưu ý rằng các địa chỉ IP từ các máy tính trong một số bài kiểm tra dưới đây có thể thay đổi từ bài kiểm tra này sang bài kiểm tra khác do DHCP.

Chúng ta sẽ sử dụng bài kiểm tra PING để kiểm tra kết nối và lệnh TRACERT để xác nhận các tuyến đường trong một số bài kiểm tra như kết nối Internet.

### 4.1 Kết nối giữa các máy tính trong cùng VLAN

#### Kết nối hai máy tính trong phòng ban vận hành & pháp lý

Một bài kiểm tra ping được thực hiện giữa PC HCM PC\_no2 (192.168.20.12) và PC\_no2 (192.168.20.13).



Hình 4.1: PC\_no1 và PC\_no2

The screenshot shows two windows from Cisco Packet Tracer. The left window is titled 'PC\_no1' and the right window is titled 'PC\_no2'. Both windows have tabs for Physical, Config, Desktop, Programming, and Attributes, with the Desktop tab selected. Each window has a Command Prompt interface at the top and a terminal window below it displaying ping results.

**PC\_no1 Terminal Output:**

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.13

Pinging 192.168.20.13 with 32 bytes of data:

Reply from 192.168.20.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

**PC\_no2 Terminal Output:**

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.12

Pinging 192.168.20.12 with 32 bytes of data:

Reply from 192.168.20.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

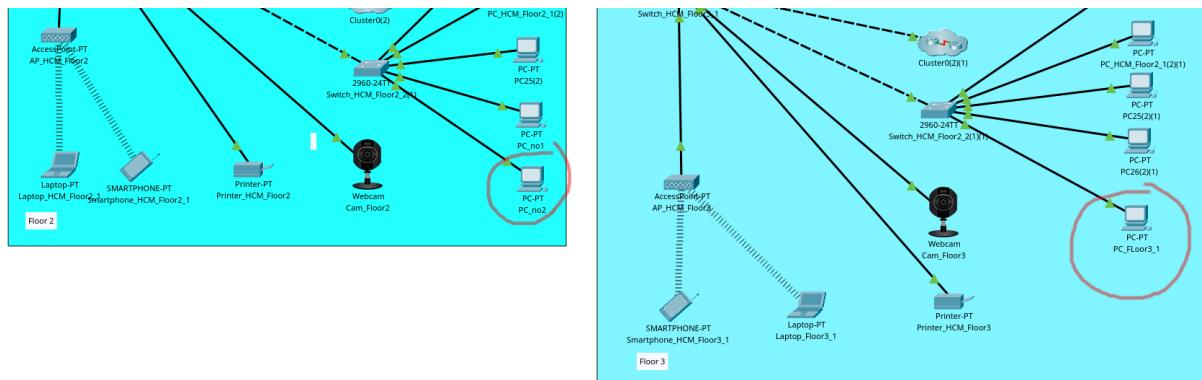
Hình 4.2: Kết quả Ping của 2 PC\_no1 và PC\_no2



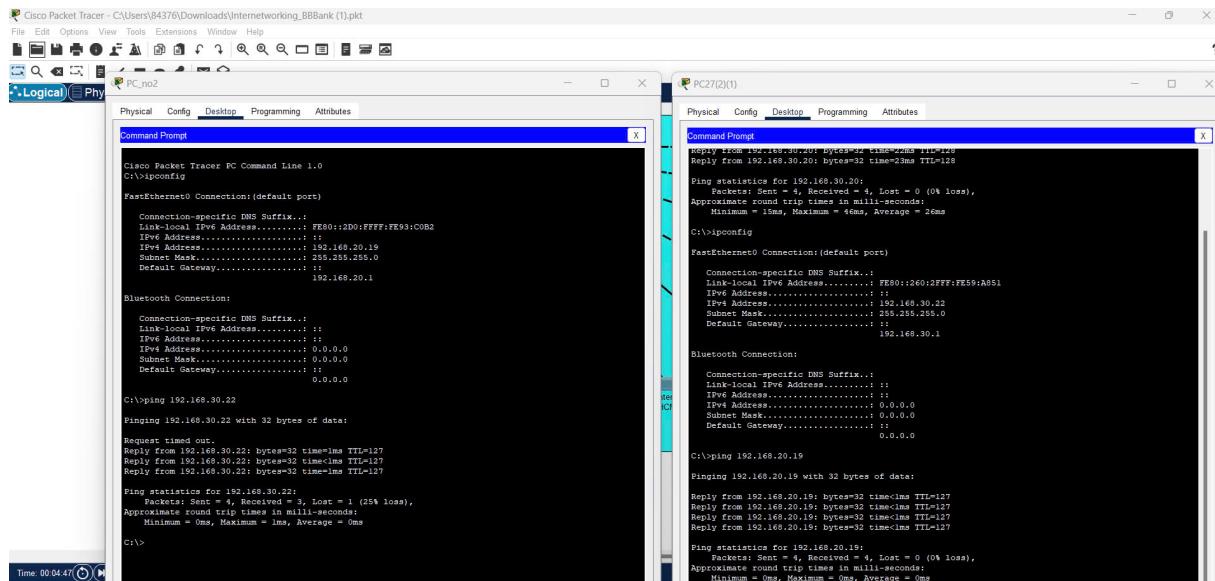
## 4.2 Kết nối các PC giữa các VLAN

### 4.2.1 Kết nối một PC từ phòng vận hành & pháp lý với một PC trong phòng ngân hàng

Một bài kiểm tra ping được thực hiện giữa PC HCM Tầng 2 4 (192.168.20.19) và PC HCM Tầng 3 4 (192.168.30.22).



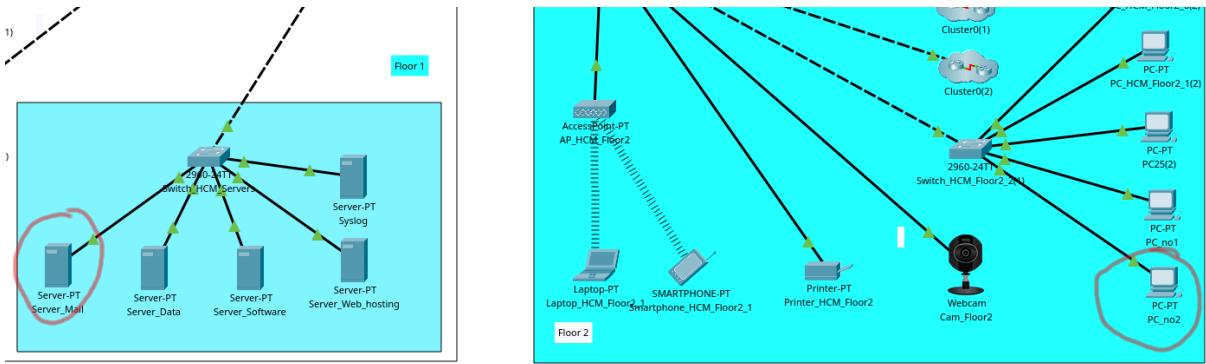
Hình 4.3: PC HCM Tầng 2 và PC HCM Tầng 3



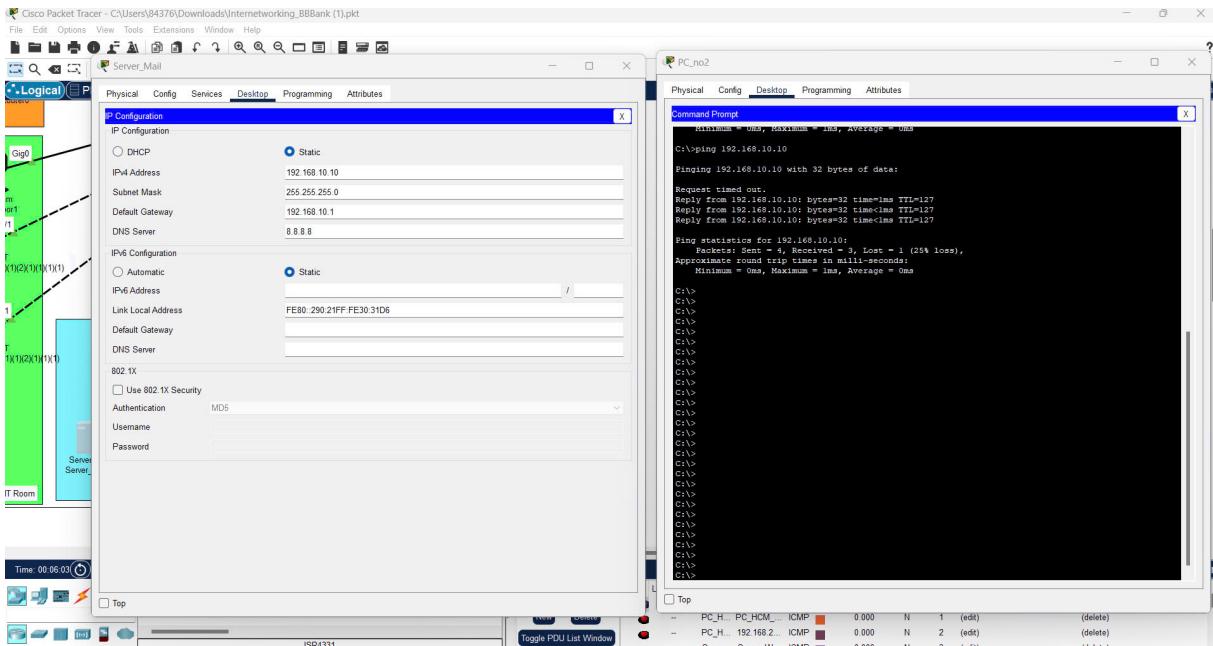
Hình 4.4: Kết quả ping giữa PC HCM Tầng 2 và PC HCM Tầng 3

### 4.2.2 Kết nối một PC từ một phòng ban HCM đến một máy chủ

Một bài kiểm tra ping được thực hiện giữa PC HCM tầng 2 (192.168.20.15) và máy chủ Mail (192.168.10.30).



Hình 4.5: PC HCM tầng 2 và máy chủ Mail

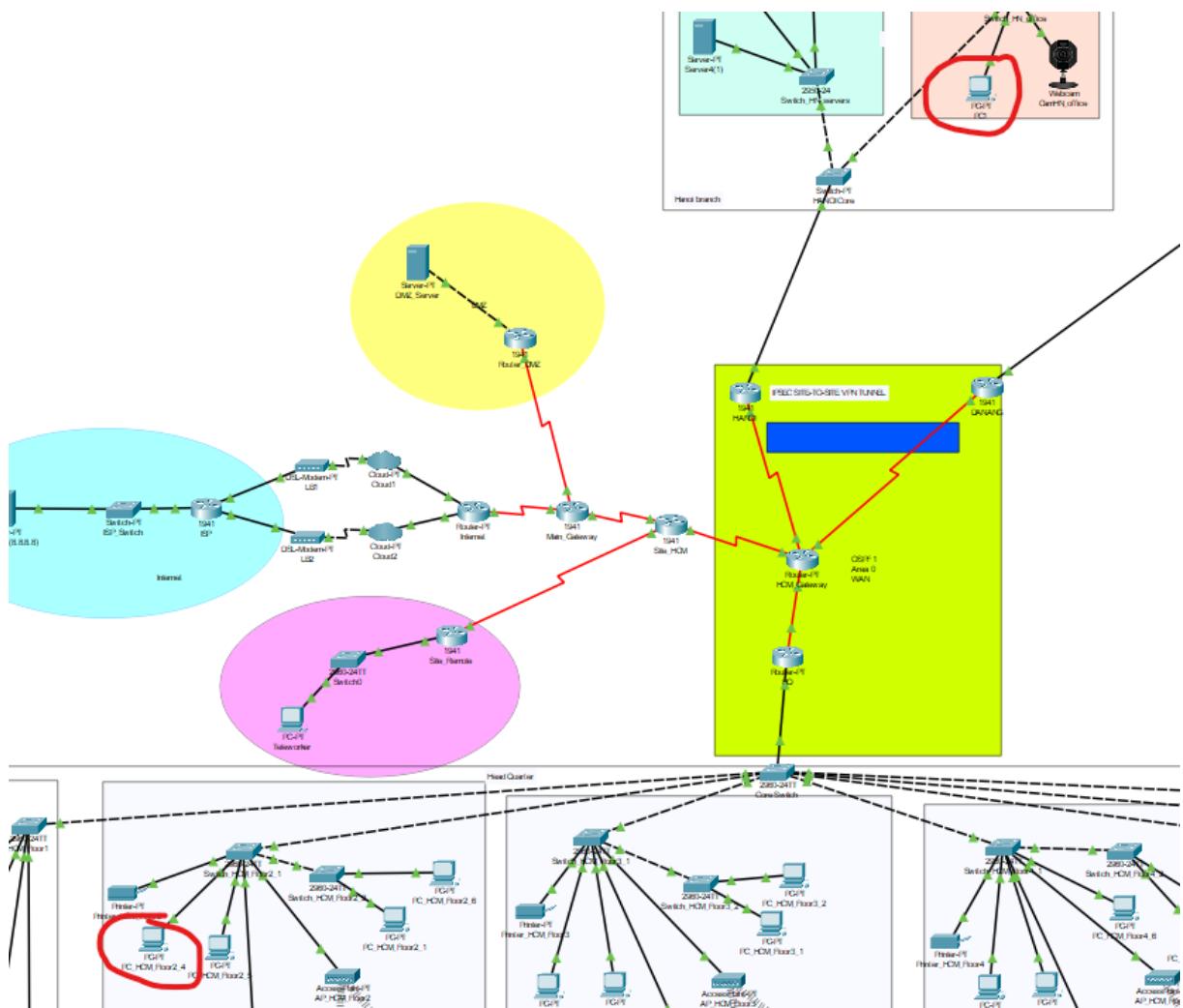


Hình 4.6: Kết quả ping từ PC HCM tầng 2 đến máy chủ Mail

### 4.3 Kết nối các PC giữa trụ sở chính và các chi nhánh

#### 4.3.1 Kết nối PC từ HCM đến một PC ở Hà Nội

Để xác minh kết nối của các PC giữa Trụ sở chính và các chi nhánh, chúng tôi thực hiện ping một PC ở chi nhánh HÀ NỘI (172.16.20.11) từ một PC ở HCM (192.168.20.11).



Hình 4.7: PC HCM Tầng 2\_4 và PC1 (HÀ NỘI).  
Mô hình được sử dụng chỉ để mô tả vị trí vật lý của hai thiết bị đầu cuối này.  
(Đây không phải là thiết kế cuối cùng của hệ thống).



The screenshot shows two Command Prompt windows side-by-side. The left window is titled 'PC27(2)(2)' and the right is 'PC\_no2'. Both windows have tabs for Physical, Config, Desktop, Programming, and Attributes, with Command Prompt selected.

**PC27(2)(2) Command Prompt:**

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

FastEthernet0 Connection:(default port)
  Connection-specific DNS Suffix.:: 
  Link-local IPv6 Address.....:: FE80::201:96FF:FE75:9077
  IPv4 Address. ....: 10.0.20.15
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: :: 10.0.20.1

Bluetooth Connection:
  Connection-specific DNS Suffix.:: 
  Link-local IPv6 Address.....:: :: 
  IPv4 Address. ....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway.....: :: 0.0.0.0

C:\>xping 192.168.20.19
Pinging 192.168.20.19 with 32 bytes of data:

Reply from 192.168.20.19: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.20.19:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>
```

**PC\_no2 Command Prompt:**

```
192.168.20.1

Bluetooth Connection:
  Connection-specific DNS Suffix.:: 
  Link-local IPv6 Address.....:: :: 
  IPv4 Address. ....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway.....: :: 0.0.0.0

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.9.20.15
Pinging 10.9.20.15 with 32 bytes of data:
Request timed out.
Request timed out.

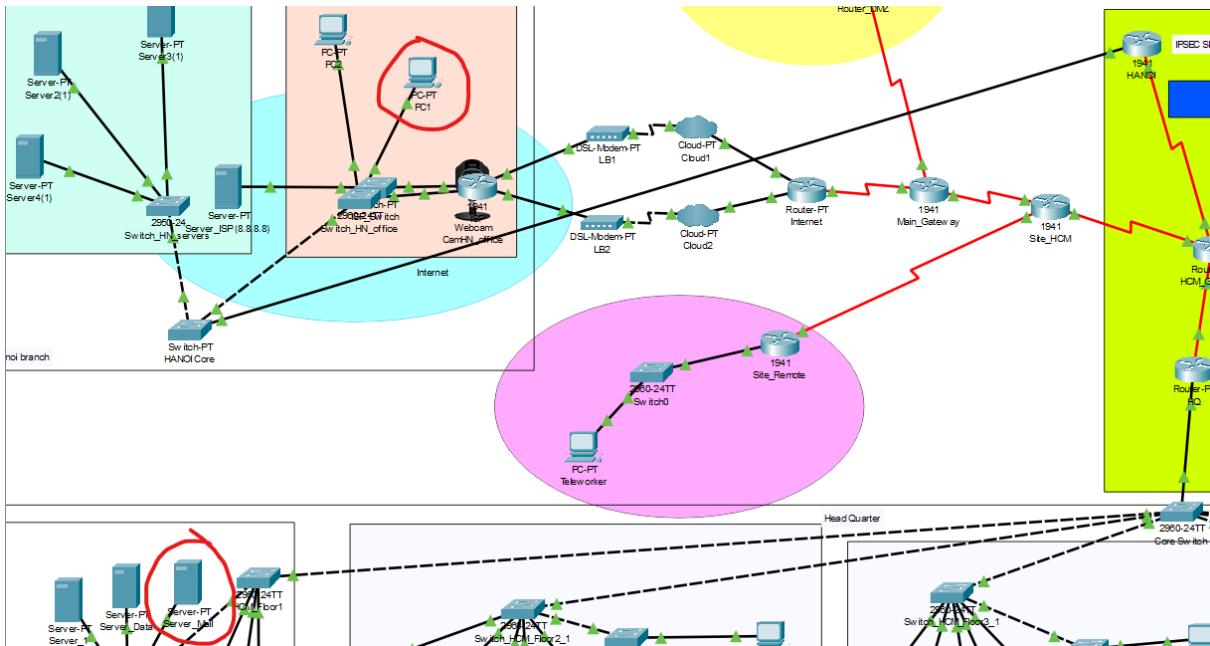
Ping statistics for 10.9.20.15:
  Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\>ping 10.0.20.15
Pinging 10.0.20.15 with 32 bytes of data:
Request timed out.
Reply from 10.0.20.15: bytes=32 time=2ms TTL=125
Reply from 10.0.20.15: bytes=32 time=6ms TTL=125
Reply from 10.0.20.15: bytes=32 time=2ms TTL=125

Ping statistics for 10.0.20.15:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms
C:\>
```

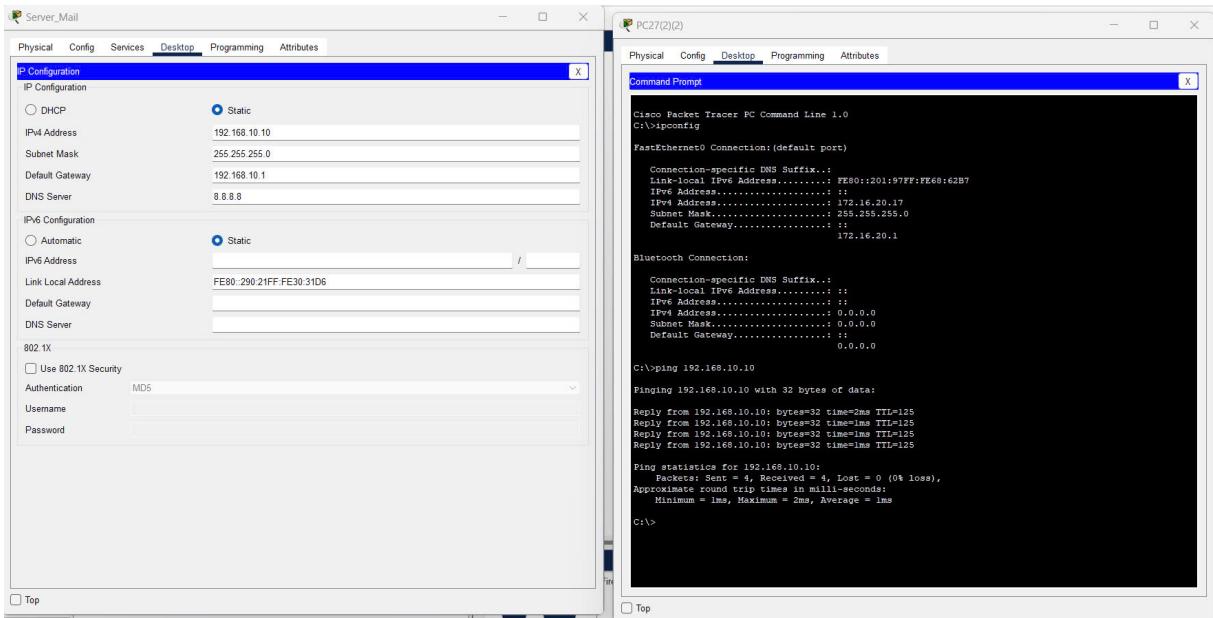
Hình 4.8: Kết quả ping giữa PC HCM Tầng 2 và PC1 (HÀ NỘI)

#### 4.3.2 Kết nối PC ở Hà Nội với máy chủ Mail ở HCM

Nhóm cũng kiểm tra kết nối từ một PC ở Hà Nội (172.16.20.11) để truy cập máy chủ mail (192.168.10.10) ở HCM.



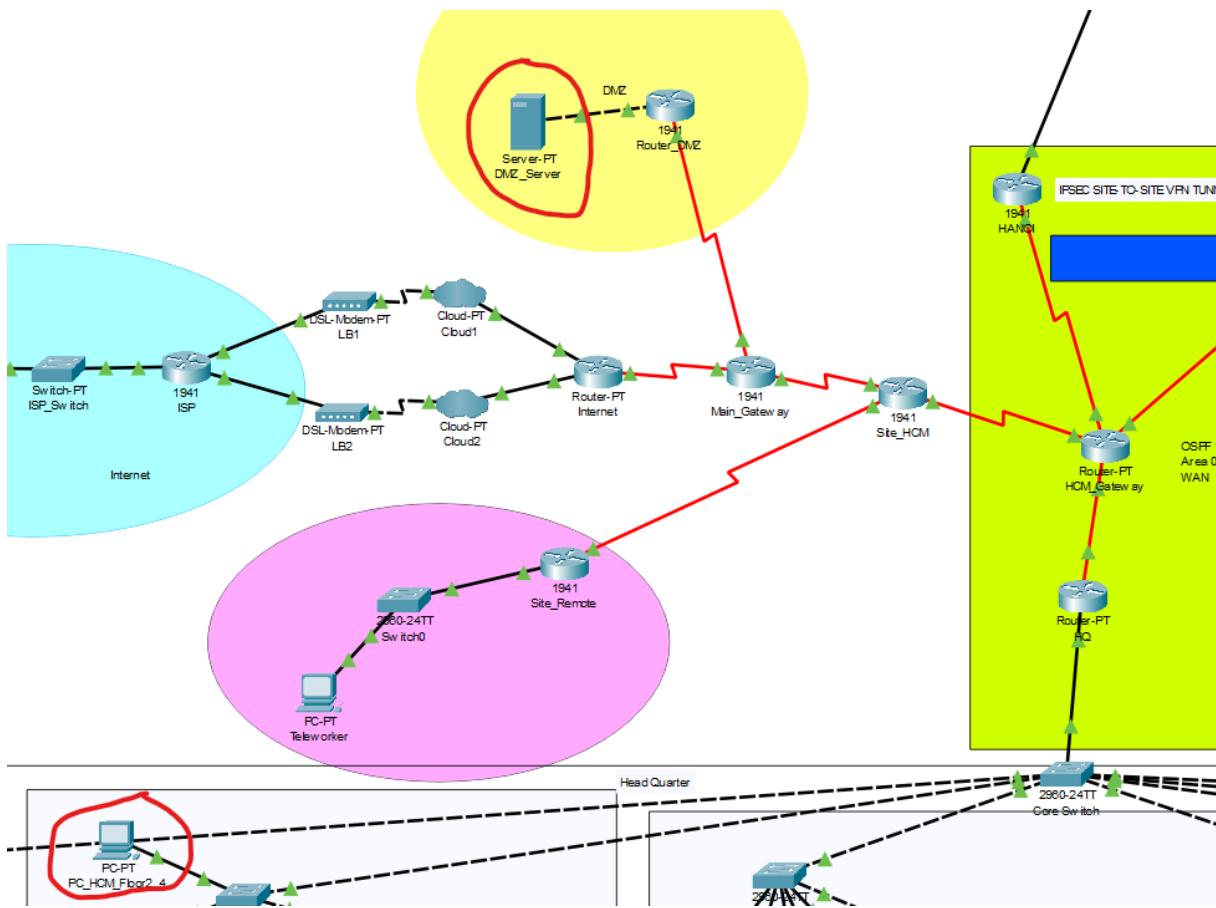
Hình 4.9: PC Hà Nội và máy chủ Mail HCM



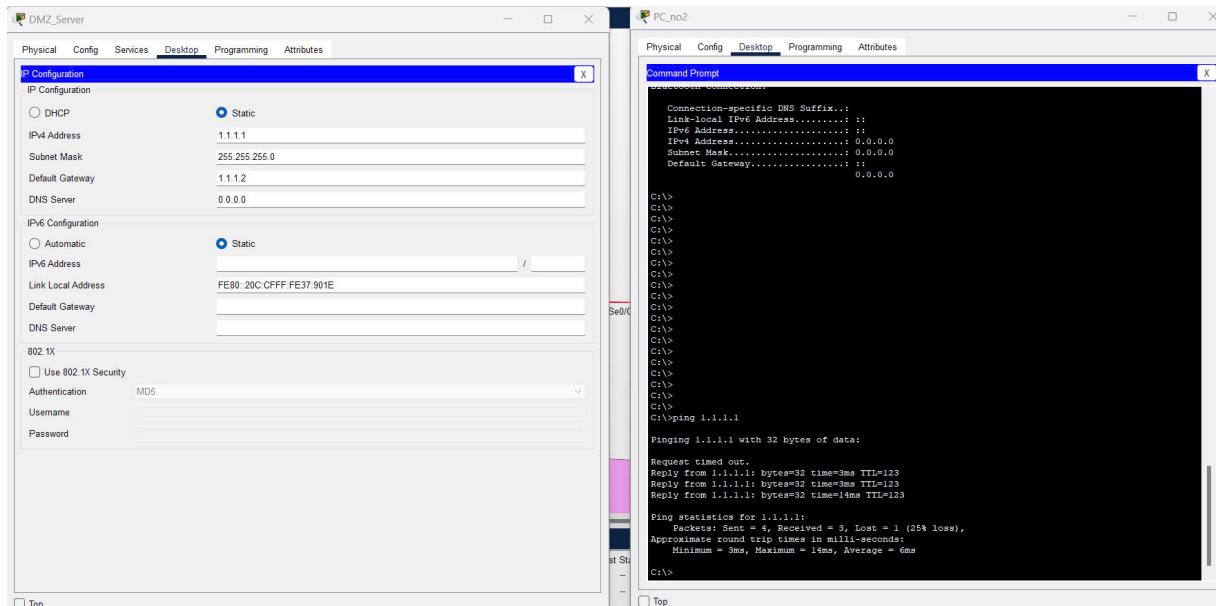
Hình 4.10: Kết quả ping từ PC ở Hà Nội đến máy chủ Mail ở HCM

#### 4.4 Kết nối đến các máy chủ trong DMZ

Một bài kiểm tra ping được thực hiện giữa PC trong chi nhánh HCM và một máy chủ trong DMZ.



Hình 4.11: PC HCM Tầng 2 và Máy chủ DMZ



Hình 4.12: Kết quả ping từ PC HCM Tầng 2 đến Máy chủ DMZ

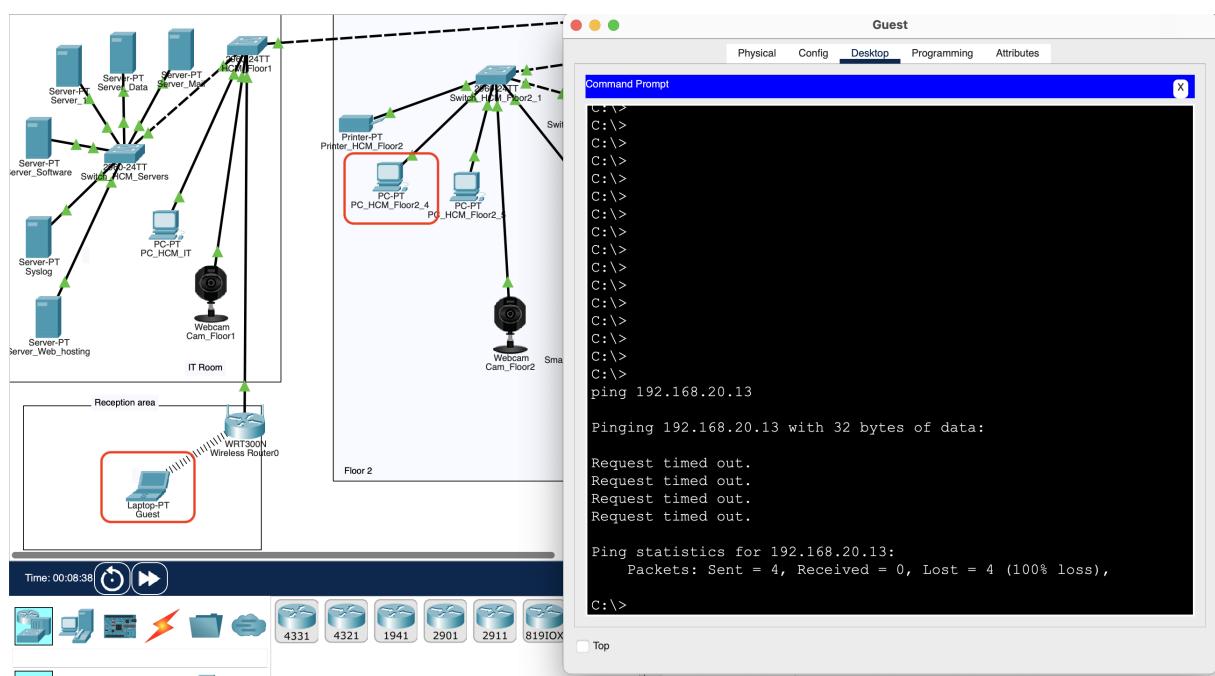


## 4.5 Không có kết nối từ thiết bị của khách hàng đến các PC trong mạng LAN

Các laptop của khách hàng kết nối với WIFI Khách hàng bị chặn truy cập vào phần còn lại của mạng bằng cách sử dụng ACL/Firewall.

### 4.5.1 Không thể kết nối từ Laptop của khách hàng đến PC ở tầng 2

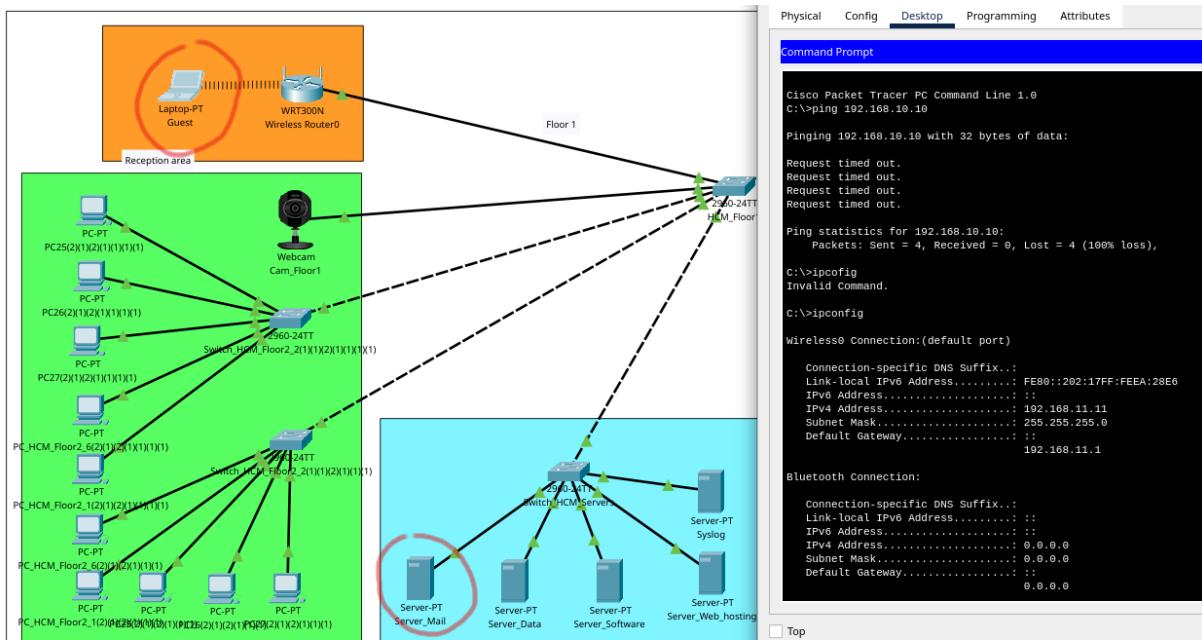
Một bài kiểm tra ping được thực hiện giữa Laptop0 của khách hàng (169.254.42.232) và PC HCM Tầng 2\_4 (192.168.20.13) để xác nhận không có kết nối.



Hình 4.13: Kết quả ping thất bại từ Laptop Khách (của khách hàng) đến PC HCM Tầng 2\_4

### 4.5.2 Không thể kết nối từ Laptop của khách hàng đến máy chủ

Một bài kiểm tra ping được thực hiện giữa Laptop của khách hàng (192.168.11.11) và Máy chủ Mail (192.168.10.10) để xác nhận không có kết nối.

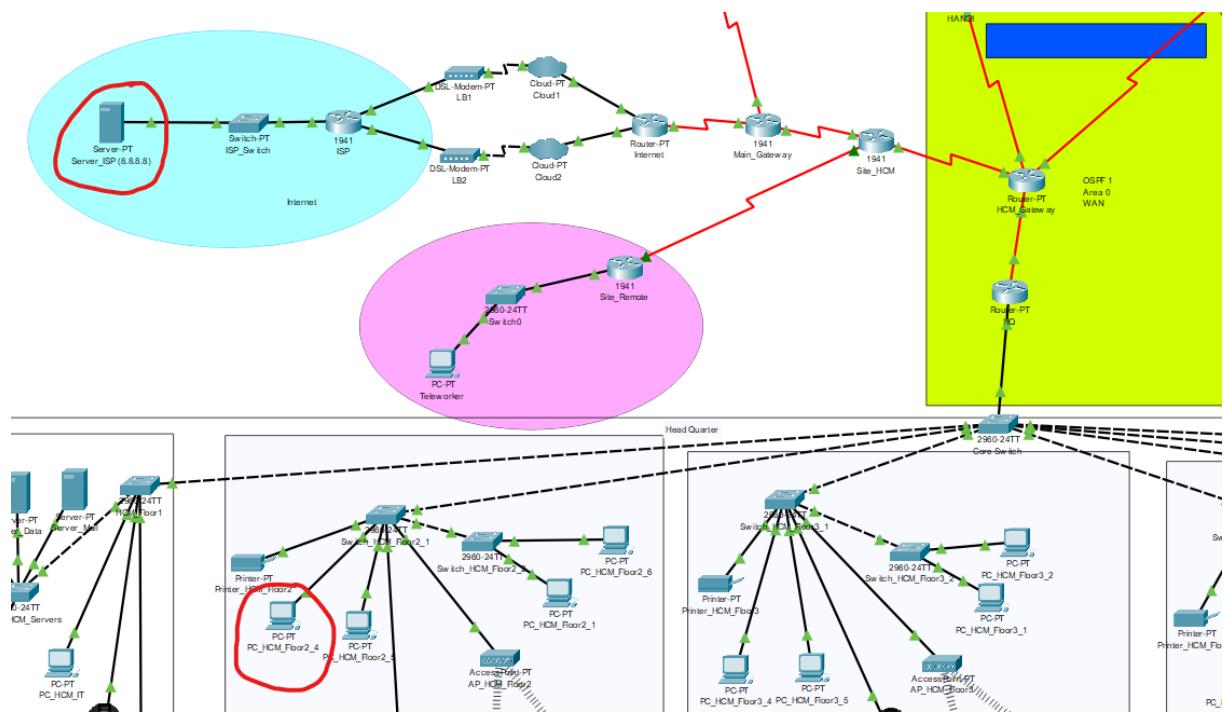


Hình 4.14: Yêu cầu ping thất bại từ Laptop Khách (của khách hàng) và Máy chủ Mail

## 4.6 Kết nối đến Internet đến một máy chủ Web

### 4.6.1 Kết nối từ PC HCM Tầng 2 đến địa chỉ 8.8.8.8 ở Internet

Một bài kiểm tra ping và truy vết được thực hiện từ một PC ở HCM đến máy chủ 8.8.8.8 trên internet để xác nhận kết nối và định tuyến đến internet.



Hình 4.15: PC HCM Tầng 2 và Máy chủ Web trên internet

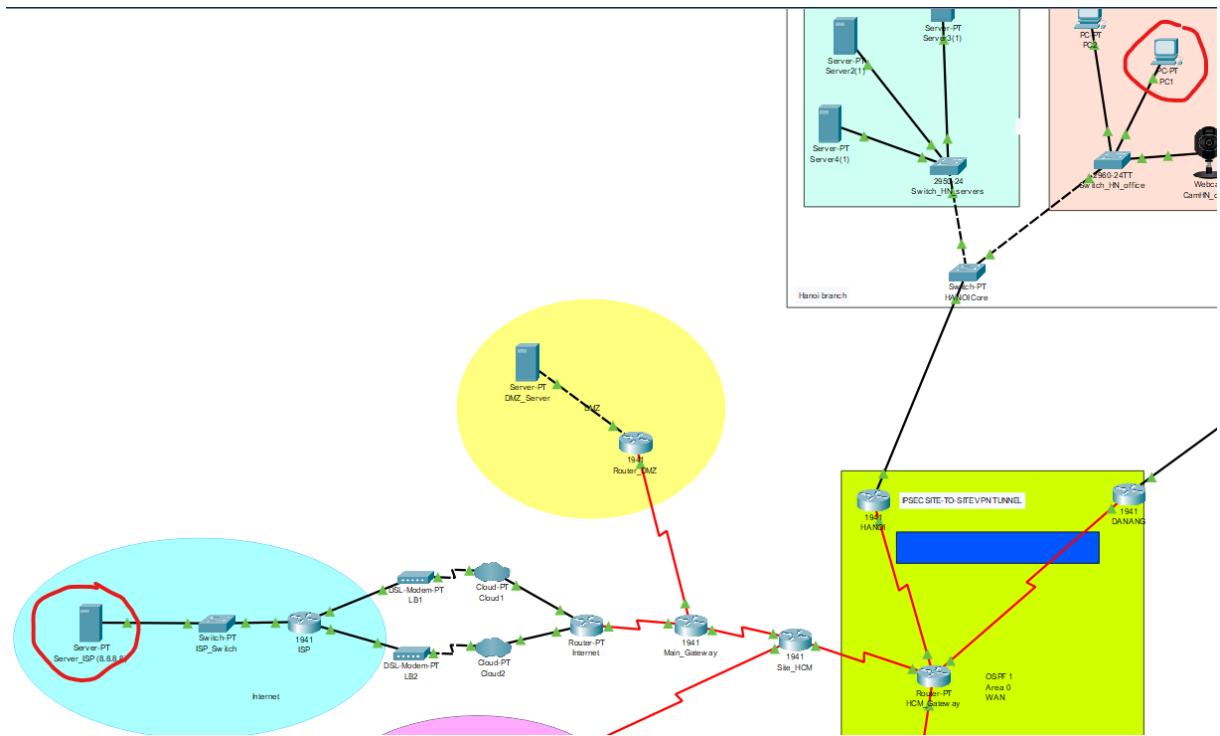


The screenshot shows a Windows Command Prompt window with the title bar 'PC\_HCM\_Floor2\_4'. The window contains the following command-line output:

```
Request timed out.  
Request timed out.  
Request timed out.  
Reply from 8.8.8.8: bytes=32 time=80ms TTL=122  
  
Ping statistics for 8.8.8.8:  
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 80ms, Maximum = 80ms, Average = 80ms  
  
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=85ms TTL=122  
Reply from 8.8.8.8: bytes=32 time=61ms TTL=122  
Reply from 8.8.8.8: bytes=32 time=90ms TTL=122  
Reply from 8.8.8.8: bytes=32 time=57ms TTL=122  
  
Ping statistics for 8.8.8.8:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 57ms, Maximum = 90ms, Average = 73ms  
  
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  1 ms      4 ms      1 ms      192.168.0.2  
 4  13 ms     9 ms      5 ms      192.168.0.5  
 5  *          *          *          Request timed out.  
 6  *          *          *          Request timed out.  
 7  29 ms     32 ms     32 ms      8.8.8.8  
  
Trace complete.  
  
C:\>
```

Top

Hình 4.16: Ping và truy vết với tracert từ một PC ở HCM đến Internet



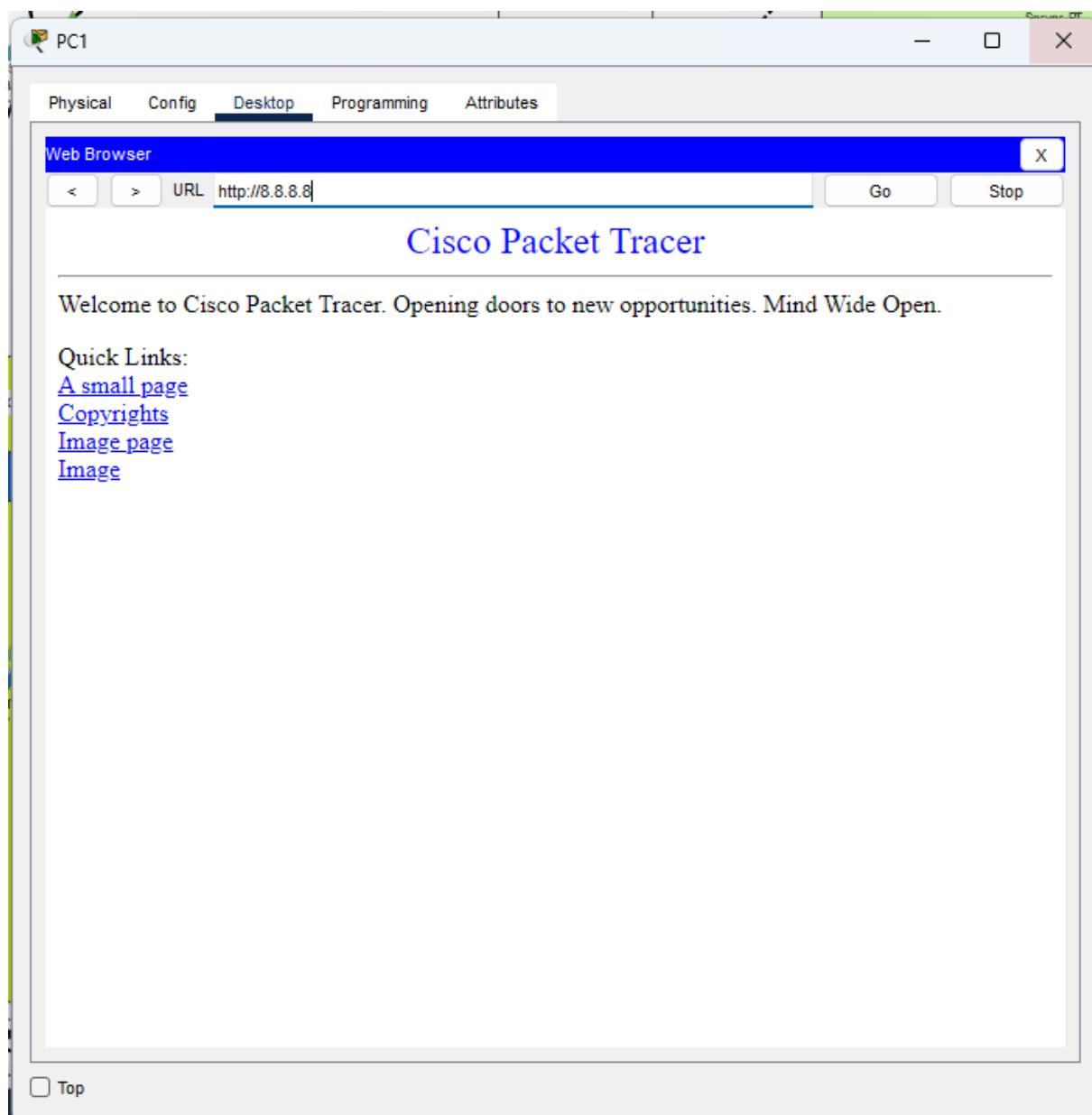
Hình 4.18: PC ở Hà Nội đến máy chủ 8.8.8.8

```
Main_Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/1
Inside Interfaces: Serial0/0/0
Hits: 1 Misses: 4
Expired translations: 4
Dynamic mappings:
Main_Gateway#show ip nat translations
Main_Gateway#show ip nat translations
Pro Inside global     Inside local      Outside local      Outside global
icmp 209.165.0.2:5    192.168.20.18:5   8.8.8.8:5        8.8.8.8:5
icmp 209.165.0.2:6    192.168.20.18:6   8.8.8.8:6        8.8.8.8:6
icmp 209.165.0.2:7    192.168.20.18:7   8.8.8.8:7        8.8.8.8:7
icmp 209.165.0.2:8    192.168.20.18:8   8.8.8.8:8        8.8.8.8:8
```

Hình 4.17: Kết quả của bản NAT khi PC ở chi nhánh Hồ Chí Minh truy cập đến địa chỉ trên Internet

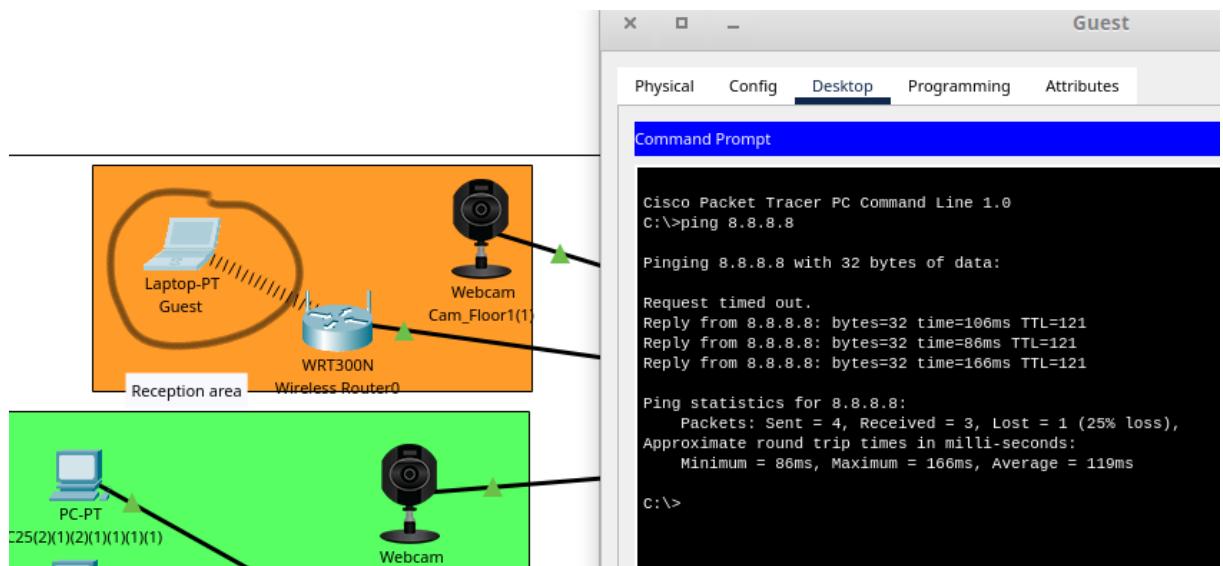
#### 4.6.2 Kết nối từ PC tại Hà Nội đến máy chủ Web bằng trình duyệt Web qua HTTP

Ngoài ra, chúng tôi cũng thử sử dụng trình duyệt web để truy cập máy chủ 8.8.8.8 trên Internet.



Hình 4.19: Truy cập 8.8.8.8 từ một PC ở Hà Nội

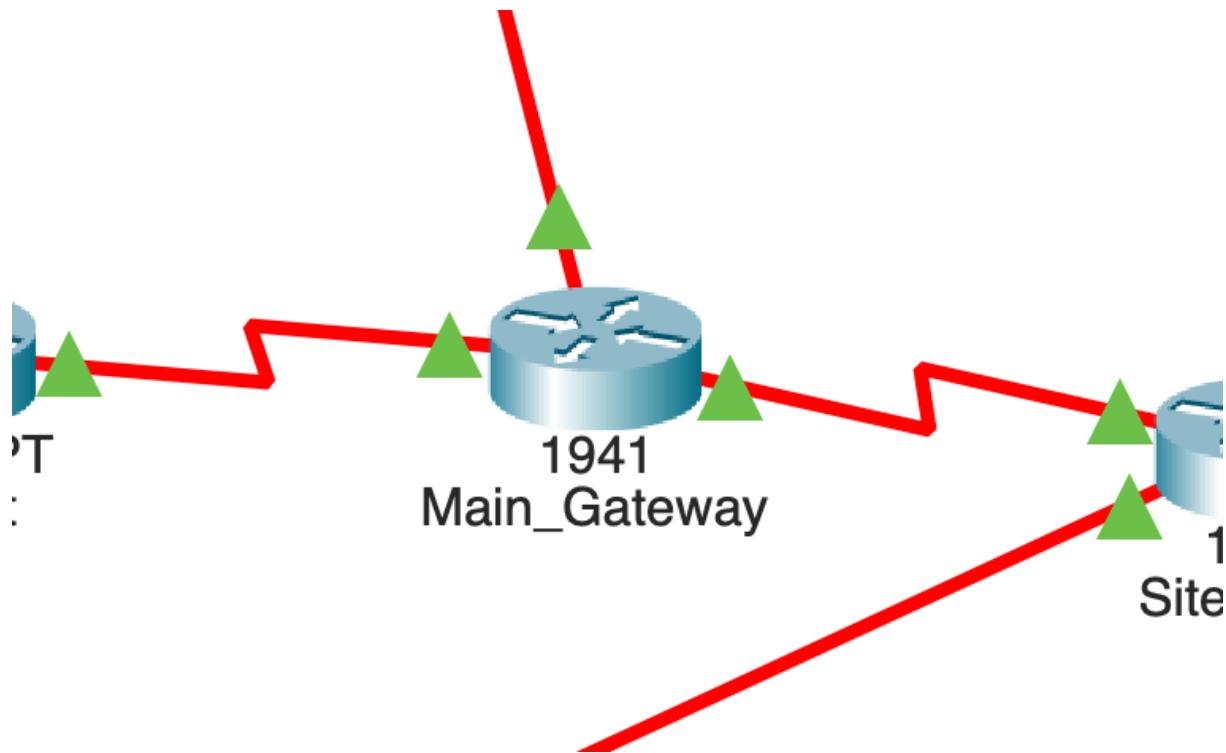
#### 4.6.3 Kết nối từ máy khách tại trụ sở Hồ Chí Minh đến máy chủ ở Internet



Hình 4.20: Máy khách tại HCM và Máy chủ Web trên Internet

### 4.7 Bảo mật

Trong phần này, nhóm đã thêm giấy phép bảo mật K9 cho router

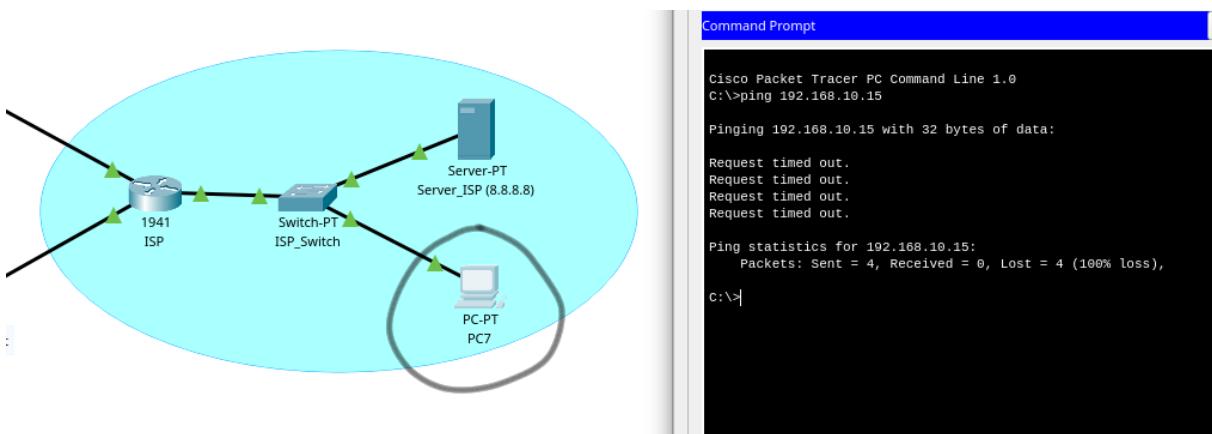


Hình 4.21: Router được trang bị giấy phép bảo mật K9

#### 4.8 Hệ thống ngăn chặn xâm nhập (IPS)

Mạng LAN nội bộ bao gồm Trụ sở chính và 2 chi nhánh gửi lưu lượng truy cập đến DMZ và Internet. DMZ có thể gửi và nhận lưu lượng truy cập từ LAN và Internet. Internet không thể gửi lưu lượng truy cập đến mạng LAN nội bộ. Nó bị chặn bởi Hệ thống Ngăn chặn Xâm nhập (IPS) trong gateway router chính.

Thiết bị bên ngoài mạng Internet thử truy cập đến địa chỉ của thiết bị bên trong mạng nội bộ là **192.168.10.15** (một thiết bị thuộc trụ sở Hồ Chí Minh)



Hình 4.22: Hệ thống ngăn chặn xâm nhập đến thiết bị trong mạng nội bộ

Lưu lượng từ máy chủ ISP bị gateway router chính (Main Gateway) ngăn chặn khi cố gắng gửi các gói tin ICMP đến máy chủ Mail tại trụ sở chính do bị chặn bởi tường lửa và hệ thống phát hiện xâm nhập (IPS), những hệ thống này sẽ gửi SYSLOG đến máy chủ SysLog trong phòng IT.

The interface has a sidebar with a tree view containing: Firewall, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP.

The main area is titled "Syslog" and shows a table with the following columns: Time, HostName, and Message.

Service		<input checked="" type="radio"/> On <input type="radio"/> Off
Time	HostName	Message
1 03.01.1993 12:40:47.636 AM	192.168.0.5	...
2 03.01.1993 12:40:53.620 AM	192.168.0.5	...
3 03.01.1993 12:40:59.633 AM	192.168.0.5	[8.8.8.69 -> 192.168.10.15:0] RiskRating:25

Hình 4.23: Danh sách bị các địa chỉ đã bị hệ thống ngăn chặn

Thông điệp được lưu trữ là: "%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [8.8.8.69 -> 192.168.10.15:0] RiskRating:25".

Với **8.8.8.69** là địa chỉ của thiết bị bên ngoài Internet và **192.168.10.15** là máy tính ở trụ ở Hồ Chí Minh mà ta đã cố truy cập tới.



## 5 Đánh giá hệ thống mạng

### 5.1 Đánh giá bảo mật

Hệ thống của một công ty phải mạnh mẽ và an toàn để bảo vệ các thông tin quan trọng, chiến lược kinh doanh và hợp đồng đối tác. Do đó, hệ thống phải đáp ứng một số yêu cầu bảo mật tối thiểu, như:

- Kiểm soát quyền truy cập của người dùng.
- Ngăn chặn sớm các truy cập trái phép.
- Cảnh báo ngay lập tức khi có các nỗ lực truy cập trái phép.

Tất cả những yêu cầu này đã được hiện thực và được minh họa ở những phần trên.

### 5.2 Đánh giá khả năng mở rộng

Hệ thống nên được thiết kế để dễ dàng mở rộng (thêm thiết bị, cáp mạng, v.v.) nhằm đáp ứng nhu cầu phát triển của ngân hàng, cả ở trụ sở chính và các chi nhánh.

Hiện tại, trụ sở chính có khoảng 120 máy trạm phân bổ trên 7 tầng, mỗi tầng có các phòng ban với 10-30 máy trạm. Theo thiết kế hiện tại, mỗi tầng sử dụng 2 switch 24 cổng (trừ một cổng kết nối với switch chính), cung cấp 47 cổng, cho phép kết nối thêm thiết bị khi số lượng nhân viên tăng lên.

### 5.3 Các vấn đề chưa giải quyết

Các vấn đề chưa giải quyết bao gồm:

- Hệ thống vẫn còn nhiều điểm kết nối tập trung (switch lõi, router lõi), gây gián đoạn toàn hệ thống khi các thiết bị này gặp sự cố.
- Vì chủ yếu dựa trên lý thuyết, thiết kế có thể không hoàn toàn phù hợp với thực tế.
- Chi phí thiết bị mạng Cisco cao, mặc dù có thể giảm chi phí ở một số khu vực.

### 5.4 Định hướng thiết kế trong tương lai

- Tìm các giải pháp thay thế thiết bị Cisco để tiết kiệm chi phí.
- Thiết kế đảm bảo mạng không bị tắc nghẽn, đáp ứng yêu cầu dung lượng tải xuống và tải lên hàng ngày.



- Đánh giá kỹ lưỡng nhu cầu thực tế, chi phí thiết bị và chi phí thiết kế để tạo ra một mạng lưới đáp ứng cả yêu cầu hệ thống và chi phí.
- Triển khai giải pháp an toàn để khi một nút quan trọng (như switch lỗi) gặp sự cố, hệ thống vẫn hoạt động ổn định.