

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



COMPUTER NETWORKING

Assignment

NETWORK DESIGN AND SIMULATION

Giáo viên hướng dẫn: La Quốc Nhựt Huân
Sinh viên: Trần Phước Nhật - 2210615
Trần Uy - 2213669
Nguyễn Đăng Cường - 2210432
Võ Nguyễn Đức Phát - 2213965

HO CHI MINH CITY, NOVEMBER 2024



Contents

1 Phân tích cấu trúc mạng	4
1.1 Trụ sở chính:	4
1.2 Chi nhánh:	4
1.3 Yêu cầu về hệ thống mạng:	4
1.4 Lưu lượng dữ liệu và tải công việc của hệ thống mạng:	4
1.5 Phân tích bối cảnh	5
2 Thiết kế mạng	7
2.1 Danh sách thiết bị	7
2.2 Virtual Private Network	12
2.3 Network Connection	13
2.4 Throughput and Bandwidth	15
3 Thiết kế sơ đồ mạng bằng Packet Tracer	16
3.1 Kết nối liên thông	16
3.1.1 Wide Area Network (WAN) Connectivity	16
3.1.2 Kết nối giữa trụ sở và các chi nhánh	18
3.1.3 Kết nối giữa các thiết bị	19
3.1.4 Kết nối giữa mạng LAN và Internet	19
3.1.5 Mạng ngoài	21
3.1.6 Kết nối từ xa cho nhân viên (Teleworker Connection)	22
4 Mô phỏng Hệ thống Mạng	25
4.1 Kết nối giữa các PC trong cùng một VLAN	25
4.1.1 Kết nối PC được kết nối Ethernet và Laptop được kết nối với Wifi bên trong Phòng Ngân hàng	26
4.2 Kết nối thiết bị giữa các VLAN	27
4.2.1 Kết nối thiết bị từ phòng Vận hành & Pháp lý đến máy tính trong phòng Ngân hàng	27
4.2.2 Kết nối PC từ HCM đến máy chủ	28
4.2.3 Kết nối thiết bị từ HCM đến thiết bị ở Hà Nội	29
4.2.4 Kết nối thiết bị ở Hà Nội với Mail Server ở HCM	30
4.2.5 Kết nối tới máy chủ trong DMZ	31
4.3 Không có kết nối từ thiết bị của khách hàng đến thiết bị trên mạng LAN	32
4.3.1 Không thể kết nối từ Laptop của khách hàng đến PC trên Tầng 2	32
4.3.2 Không thể kết nối từ Laptop của khách hàng đến máy chủ	33
4.4 Kết nối Internet tới Web Server	33
4.4.1 Kết nối từ PC HCM Tầng 2_4 đến 8.8.8.8	33
4.4.2 Kết nối từ PC1 (Hà Nội) đến Web Server bằng trình duyệt Web qua HTTP	34



4.5	Bảo mật	35
4.5.1	Firewall	37
5	Đánh giá Mạng	39
5.1	Dánh giá Bảo mật	39
5.2	Dánh giá khả năng mở rộng	39
5.3	Những vấn đề chưa giải quyết	39
5.4	Hướng đi trong tương lai	39



Danh sách thành viên & Phân chia công việc

No.	Họ và tên	MSSV	Công việc	Phần trăm hoàn thành
1	Trần Phước Nhật	2213669	- Scheduler - Memory Management: Paging-based, Physical Memory	100%
2	Trần Uy	2213846	- TLB - Memory Management: Paging-based, Physical Memory	100%
3	Võ Nguyễn Đức Phát	2212540	- Cơ sở lý thuyết - Viết báo cáo - Làm slide	100%
5	Nguyễn Đăng Cường	2210432	- Memory Management: Virtual Memory, Physical Memory	100%



1 Phân tích cấu trúc mạng

1.1 Trụ sở chính:

- Trụ sở chính tại TP. Hồ Chí Minh bao gồm một tòa nhà với 7 tầng, mỗi tầng dành cho các phòng ban khác nhau.
- Tầng 1 được trang bị một phòng IT và một Cabling Central Local sử dụng patch panel để tập trung hệ thống dây mạng.
- Quy mô trung bình: 120 máy trạm, 5 máy chủ, và ít nhất 12 thiết bị mạng (có thể bao gồm các thiết bị chuyên dụng về bảo mật).

1.2 Chi nhánh:

- Mỗi chi nhánh tại Đà Nẵng và Hà Nội bao gồm một tòa nhà 2 tầng.
- Tầng 1 được trang bị một phòng IT và một Cabling Central Local.
- Quy mô nhỏ: 30 máy trạm, 3 máy chủ, và ít nhất 5 thiết bị mạng.

1.3 Yêu cầu về hệ thống mạng:

- Sử dụng các công nghệ mới cho cơ sở hạ tầng mạng.
- Đảm bảo an ninh cao, độ sẵn sàng cao, hệ thống bền bỉ khi xảy ra sự cố, và dễ dàng nâng cấp.
- Cấu hình VPN cho kết nối site-to-site và cho nhân viên làm việc từ xa kết nối với mạng LAN của công ty.
- Hệ thống camera giám sát cho công ty.
- Kết nối giữa trụ sở chính và các chi nhánh thông qua 2 đường truyền thuê riêng (leased lines) để kết nối WAN.
- Toàn bộ lưu lượng truy cập Internet phải đi qua mạng con của trụ sở chính, sử dụng 2 đường xDSL với cơ chế cân bằng tải (load-balancing).

1.4 Lưu lượng dữ liệu và tải công việc của hệ thống mạng:

Hệ thống mạng của công ty dự kiến hoạt động ở mức cao, đạt khoảng 80% công suất vào giờ cao điểm từ 9h-11h và 15h-16h hàng ngày.

- Máy chủ phục vụ các tác vụ cập nhật phần mềm, truy cập web, truy cập cơ sở dữ liệu,...
Ước tính tải xuống tổng cộng khoảng 1000 MB/ngày và tải lên khoảng 2000 MB/ngày cho mỗi máy chủ.

- Mỗi máy trạm dùng cho việc duyệt web, tải tài liệu và thực hiện các giao dịch với khách hàng,... Ước tính tải xuống tổng cộng khoảng 500 MB/ngày và tải lên khoảng 100 MB/ngày.
- Các thiết bị kết nối WiFi từ khách hàng truy cập tải dữ liệu khoảng 500 MB/ngày.
- Hệ thống có lưu lượng cao nhất vào khung giờ 9h-11h sáng và 15h-16h, với 80% lưu lượng tập trung vào các khung giờ này.

Hệ thống ước tính có tốc độ tăng trưởng 20% trong vòng 5 năm (về số lượng người dùng, tải mạng, mở rộng chi nhánh,...).

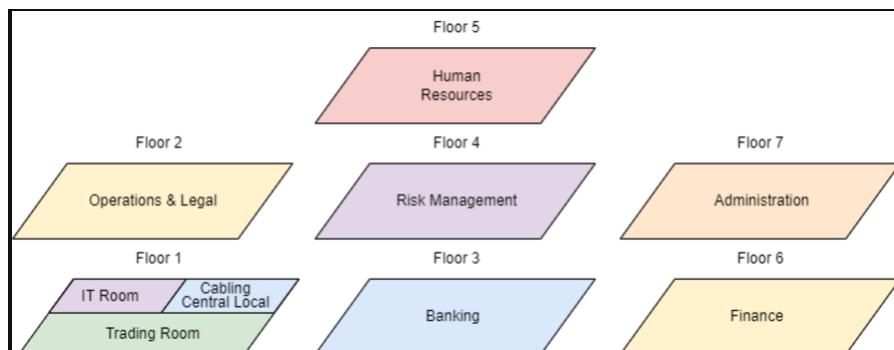
1.5 Phân tích bối cảnh

Với hệ thống của chúng ta, trụ sở chính có 7 tầng, có 2 chi nhánh, mỗi chi nhánh có 2 tầng, ta có thể giả định bối cảnh cho hệ thống như sau:

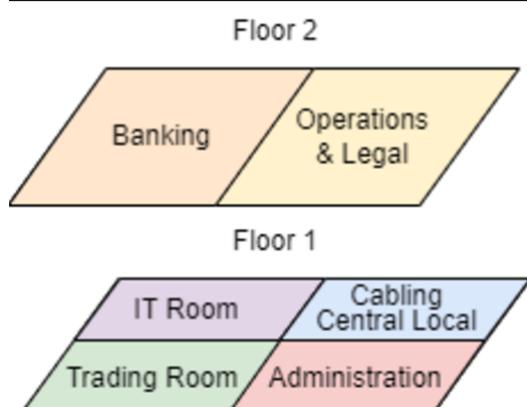
Chi nhánh	Tên phòng ban	Số lượng máy trạm
Trụ sở chính	Ngân hàng	20
Trụ sở chính	Vận hành & Pháp lý	20
Trụ sở chính	Quản lý rủi ro	20
Trụ sở chính	Tài chính	20
Trụ sở chính	Nhân sự	20
Trụ sở chính	IT	10
Trụ sở chính	Hành chính	10
Chi nhánh	Ngân hàng	10
Chi nhánh	Vận hành & Pháp lý	10
Chi nhánh	IT	5
Chi nhánh	Hành chính	5

Bảng 1: Danh sách chi nhánh, phòng ban và số lượng máy trạm

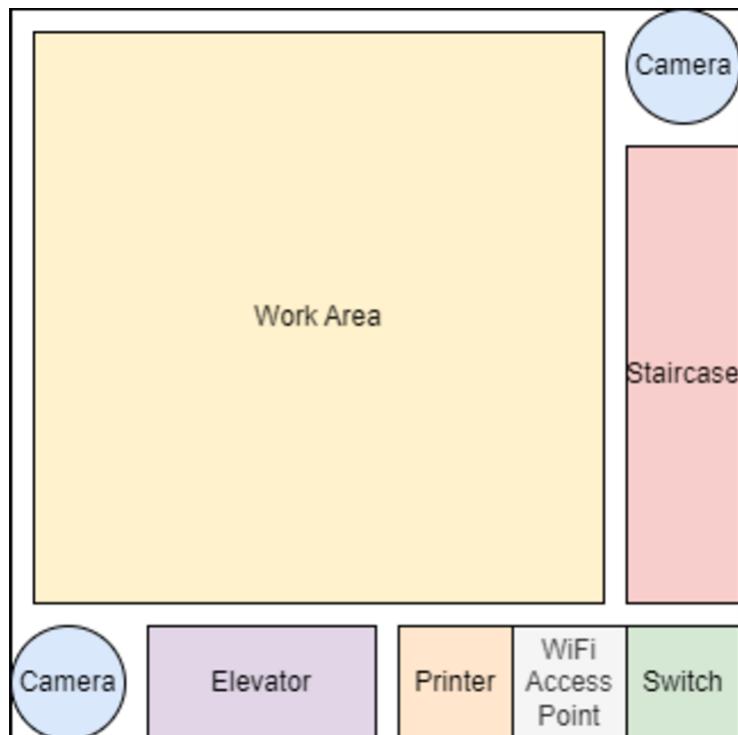
Mô tả cấu trúc



Hình 1: Bố trí tòa nhà trụ sở chính



Hình 2: Bố trí tòa nhà chi nhánh



Hình 3: Bố trí lắp đặt cho một căn phòng

2 Thiết kế mạng

Một trong những yếu tố đầu tiên cần quyết định là lựa chọn loại kết nối cho các máy trạm. Trước hết, công ty cần trang bị một bộ định tuyến (Cisco ISR4331/K9) cho trụ sở chính và mỗi chi nhánh, đi kèm với 4 switch Ethernet (Cisco 4-Port Gigabit Ethernet Switch NIM NIM-ES2-4).

Đồng thời, nếu sử dụng mạng dây, công ty vẫn cần bổ sung các điểm truy cập Wi-Fi để phục vụ nhu cầu kết nối của khách hàng và thiết bị ngoại vi.

- **Đối với mạng dây**, công nghệ Ethernet-Cat8 hiện được xem là tiên tiến và đáng tin cậy nhất. Công nghệ này mang lại tốc độ lên đến 40Gbps và khả năng giảm nhiễu tốt. Tuy nhiên,劣势 là dây cáp kẽm linh hoạt. Để đáp ứng nhu cầu mạng dây, cần triển khai 11 switch (Cisco 24 Port Catalyst 2960 WS-C2960-24TC-L) và 11 điểm truy cập Wi-Fi gọn nhẹ (TPLink Archer C54) nhằm bao phủ toàn bộ 7 tầng của trụ sở chính và 2 tầng tại mỗi chi nhánh.
- **Đối với mạng không dây**, công ty có thể lựa chọn 11 điểm truy cập sử dụng công nghệ Wi-Fi 6E (Cisco CW9162I-MR 802.11ax Wi-Fi 6E 2x2:2 Access Point). Giải pháp này có ưu điểm lớn là không bị giới hạn bởi số lượng cổng Ethernet. Tuy nhiên, nó có thể gặp vấn đề nhiễu tín hiệu khi nhiều máy trạm cùng lúc truy cập Internet.

2.1 Danh sách thiết bị

Dưới đây là mô tả chi tiết các thiết bị được sử dụng trong hệ thống mạng

Router: Cisco ISR4331/K9



- Thông lượng tổng hợp: 100 Mbps đến 300 Mbps
- Tổng số cổng WAN hoặc LAN tích hợp 10/100/1000: 3
- Cổng dựa trên RJ45: 2

- Cổng dựa trên SFP: 2
- Khe cắm mô-đun dịch vụ nâng cao (SM-X): 1
- Khe cắm mô-đun giao diện mạng (NIM): 2
- Bộ nhớ: 4 GB (mặc định) / 16 GB (tối đa)
- Bộ nhớ Flash: 4 GB (mặc định) / 16 GB (tối đa)

Network Interface Card: Cisco 4-Port Gigabit Ethernet Switch NIM NIM-ES2-4



- Tiêu chuẩn: IEEE 802.3, 802.1q, 802.1X, RFC 2284, RFC 1213, và các tiêu chuẩn khác
- Hỗ trợ SNMP và Telnet, cổng SPAN để giám sát, hỗ trợ TFTP để nâng cấp phần mềm
- Cổng: 10BASE-T, 100BASE-TX, 1000BASE-TX
- Cáp: Đầu nối RJ-45, cáp UTP
- Hỗ trợ phần mềm Cisco IOS-XE Software Release 3.15
- Dáp ứng các tiêu chuẩn của router Cisco dòng 4000 Series

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

thietbimang**cisco**.vn



- Tiêu chuẩn gắn rack: Gắn rack 1U (Rack-mountable 1U)
- Tính năng: LAN Base
- Giao diện uplink: 2 (SFP hoặc 1000BASE-T)
- Cổng: 24 cổng Ethernet 10/100
- Băng thông chuyển tiếp: 16 Gbps
- Tốc độ chuyển tiếp: 6.5 Mpps
- RAM 128 MB và có bộ nhớ Flash 64 MB

Baseus Cat8 40-Gigabit RJ45 Network Cable



- Tốc độ truyềnl: 40 Gbps
- Băng thông: 2000 MHz
- Chống nhiễu: 4 lớp
- Lõi dây: Dây đồng nguyên chất 30 AWG
- Vỏ cáp: 48 sợi bện

Access Point: TP-Link Archer C54



- Wi-Fi:
 - Tiêu chuẩn: Wi-Fi 5
 - Tốc độ: 867 Mbps (băng tần 5 GHz), 300 Mbps (băng tần 2.4 GHz)
 - Phạm vi phủ sóng: Căn hộ 3 phòng ngủ, 4 anten
 - Khả năng kết nối: Trung bình
 - Băng tần kép: Có
- Phần cứng có cổng Ethernet 1 cổng WAN, 4 cổng LAN (10/100 Mbps)
- Mã hóa Wi-Fi: WPA, WPA2
- Bảo mật mạng: Tường lửa SPI, Kiểm soát truy cập
- Mạng khách: 1 mạng 5 GHz, 1 mạng 2.4 GHz

Access Point: Cisco CW9162I-MR 802.11ax Wi-Fi 6E 2x2:2 Access Point



- MU-MIMO: 2x2 (6 GHz truyền/nhận, 2.4 GHz và 5 GHz chỉ truyền)
- Hỗ trợ: OFDMA, TWT, BSS coloring, MRC, beamforming chuẩn 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: Tối đa 3.9 Gbps
- Có ăng-ten tích hợp
- Cổng Ethernet: 1× Multigigabit Ethernet 100M/1000M/2.5G, RJ-45
- Cổng quản lý: RJ-45, USB 2.0 (4.5W)
- Bộ nhớ hệ thống DRAM 2048 MB và Flash 1024 MB

Firewall: Cisco ASA5506-SEC-BUN-K9



- Băng thông: Kiểm soát ứng dụng (AVC) - 250 Mbps
- Băng thông: Kiểm soát ứng dụng (AVC) và IPS - 125 Mbps
- Số phiên kết nối đồng thời tối đa: 20,000 (50,000 với giấy phép)
- Số kết nối mới mỗi giây tối đa: 5,000
- Ứng dụng hỗ trợ: Hơn 3,000
- Danh mục URL: Hơn 80
- URL đã phân loại: Hơn 280 triệu
- Băng thông kiểm tra trạng thái (tối đa): 750 Mbps
- Băng thông kiểm tra trạng thái (đa giao thức): 300 Mbps
- Băng thông VPN 3DES/AES: 100 Mbps
- Số người dùng/nút: Không giới hạn

Software: Cisco SEC-K9 License

- Hỗ trợ VPN cho các kết nối từ xa an toàn.
- Mã hóa nâng cao cho bảo mật dữ liệu.
- Tính năng tường lửa tích hợp.
- Hệ thống phòng ngừa xâm nhập (IPS) cho bảo vệ mạng.
- Lọc nội dung.

Thêm vào đó có thêm các hệ thống camera được gọi ý như DS-2GN5750-HH,...



2.2 Virtual Private Network

Lựa chọn cấu hình VPN Site-to-Site với các yêu cầu sau:

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

Với những yêu cầu này, phù hợp nhất sẽ chọn **Cisco Meraki MX Series** vì nó cung cấp các tính năng SD-WAN và bảo mật tích hợp. Được quản lý trên đám mây, giúp đơn giản hóa việc thiết lập VPN phức tạp.

Cấu hình VPN cho nhân viên làm việc từ xa (Teleworker VPN)

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

Với yêu cầu đó, giải pháp phù hợp là **Cisco AnyConnect Secure Mobility Client** vì cung cấp khả năng tuân thủ điểm cuối thông nhất, bảo mật truy cập mạng mạnh mẽ, bảo vệ web và roaming, khả năng hiển thị mạng, hỗ trợ thiết bị di động và các tùy chọn VPN nâng cao cho kết nối từ xa an toàn và linh hoạt.

Virtual Local Area Network

- VLAN sẽ được triển khai trên toàn bộ mạng của BB Bank để phân đoạn mạng thành các phần nhỏ hơn, dễ quản lý. Việc phân đoạn này giúp cải thiện hiệu suất, tăng cường bảo mật và đơn giản hóa quản lý mạng. VLAN phân tách hiệu quả lưu lượng mạng của các phòng ban khác nhau, đảm bảo hiệu quả hoạt động và bảo mật dữ liệu.
- Mỗi phòng ban trong BB Bank (ví dụ: Kế toán, Nhân sự, Dịch vụ khách hàng) sẽ có một VLAN riêng. Cách tiếp cận này đảm bảo rằng lưu lượng và tài nguyên liên quan đến mỗi phòng ban được phân tách, từ đó giảm lưu lượng không cần thiết và tăng cường bảo mật.



- Kích thước của mỗi VLAN sẽ dựa trên số lượng nhân sự, mà chúng ta chỉ có thể ước lượng giới hạn tối đa, và chức năng của từng phòng ban.

Tên VLAN	Kích thước VLAN	Subnet
Tầng 1	256	192.168.10.1/24
Vận hành & Pháp lý	256	192.168.20.1/24
Ngân hàng	256	192.168.30.1/24
Quản lý rủi ro	256	192.168.40.1/24
Nhân sự	256	192.168.50.1/24
Tài chính	256	192.168.60.1/24
Hành chính	256	192.168.70.1/24

Bảng 2: Kế hoạch IP VPN

Ngoại trừ Tầng 1, nơi có sự kết hợp giữa máy tính CNTT, máy chủ và thiết bị của khách hàng, mỗi tầng sẽ chứa một phòng ban khác nhau và được phân đoạn với một VLAN riêng biệt.

2.3 Network Connection

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

- Băng thông: là tốc độ tối đa của việc truyền tải dữ liệu qua một mạng, thường được đo bằng Megabit trên giây (Mbps), cho biết khả năng lưu lượng thông tin.
- Throughput (tốc độ thực): là lượng dữ liệu thực tế được truyền tải thành công qua một kênh giao tiếp trong một khoảng thời gian nhất định, phản ánh hiệu quả thực tế của việc truyền tải dữ liệu.

Tổng quan Lưu lượng

Dòng dữ liệu và khối lượng công việc của hệ thống tại trụ sở chính có thể 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 của khách hàng: Với ước tính có 50 khách hàng mỗi ngày, ta có

- Tải xuống: $500 \times 50 = 25000$ MB/ngày.
- Tải lên: 0 MB/ngày.

Như vậy trụ sở chính có tổng tải xuống là 90000 MB/ngày và tải lên là 22000 MB/ngày. Một khác, dòng 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.

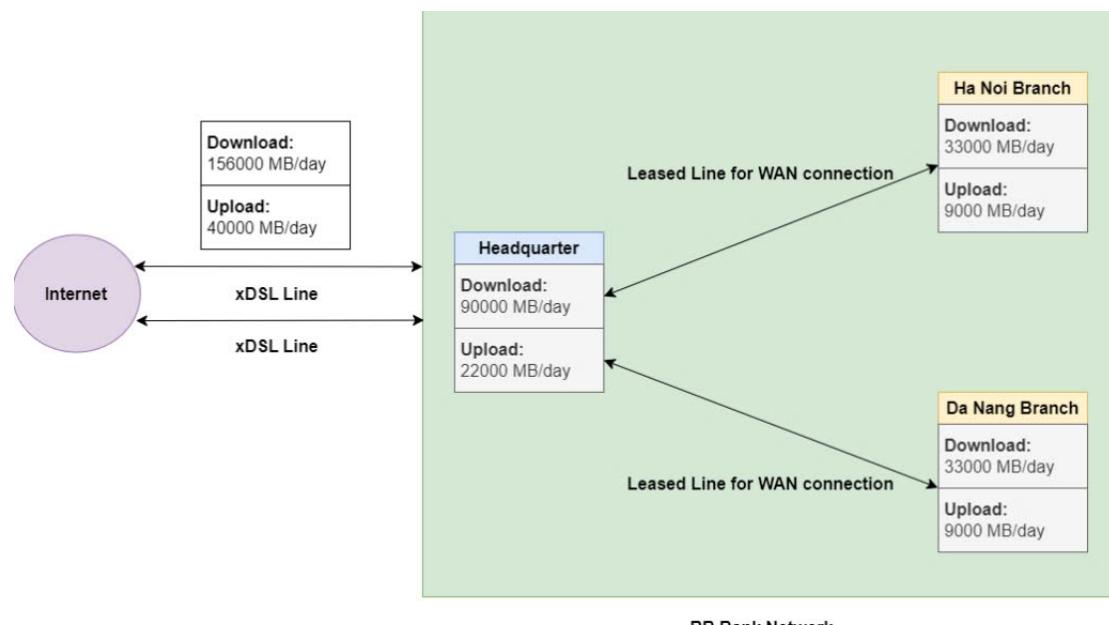
Máy trạm: Tổng tải lên và tải xuống của 30 máy trạm

- Tải xuống: $500 \times 30 = 15000$ MB/ngày.
- Tải lên: $100 \times 30 = 3000$ MB/ngày.

Thiết bị của khách hàng: Với ước tính có 30 khách hàng mỗi ngày, ta có

- Tải xuống: $500 \times 30 = 15000$ MB/ngày.
- Tải lên: 0 MB/ngày.

Như vậy tại chi nhánh có tổng tải xuống là 33000 MB/ngày và tải lên là 9000 MB/ngày.



Hình 4: Tổng quan về luồng dữ liệu mạng của BB Bank



2.4 Throughput and Bandwidth

Với 80% lưu lượng dữ liệu tập trung vào giờ cao điểm từ 9 giờ sáng đến 11 giờ sáng và từ 3 giờ chiều đến 4 giờ chiều, chúng ta có thể tính toán tốc độ thực trung bình trong 3 giờ cao điểm này. Chúng ta cũng cần tính thêm 20% cho sự phát triển trong tương lai, cả về việc sử dụng thiết bị và số lượng thiết bị trong mạng của Ngân hàng:

$$\text{Tải xuống: } \frac{156000 \times 0.8 \times 1.22 \times 8}{3 \times 60 \times 60} = 133.12 \text{ Mbps}$$

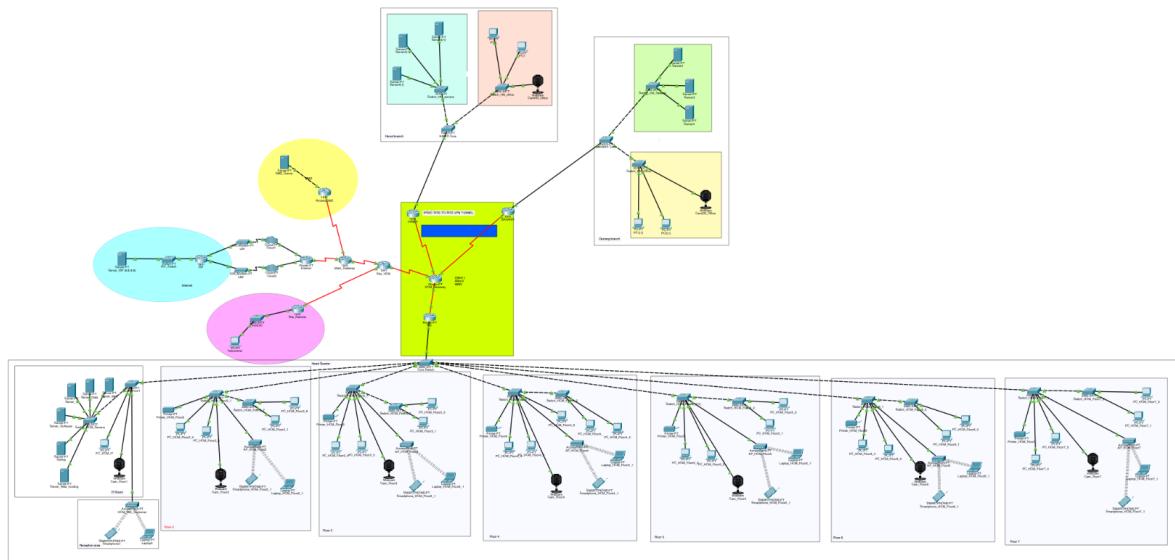
$$\text{Tải lên: } \frac{40000 \times 0.8 \times 1.22 \times 8}{3 \times 60 \times 60} = 34.1333 \text{ Mbps}$$

Vì lưu lượng dữ liệu từ giờ cao điểm xác định tỷ lệ tốc độ thực trung bình, các nhà cung cấp dịch vụ Internet (ISP) cần cung cấp băng thông lớn hơn 134 Mbps cho tải xuống và 35 Mbps cho tải lên để đảm bảo hoạt động của doanh nghiệp. Một số lựa chọn cho nhà cung cấp dịch vụ Internet (ISP) phù hợp như VNPT-FIBERVIP6, FPT-SUPER250, Viettel-F200N. Những ISP này đều có đặc điểm chung như:

- Cung cấp kết nối Static WAN (Wide Area Network):
- Cung cấp băng thông trong nước ổn định. Các mức băng thông này đều nằm trong phạm vi yêu cầu cho việc kết nối giữa các chi nhánh và trụ sở chính của ngân hàng.
- Đáp ứng yêu cầu tải dữ liệu nội bộ nhanh chóng, đặc biệt khi cần xử lý các giao dịch ngân hàng hoặc truy xuất cơ sở dữ liệu

Về đường thuê bao có thể được đề nghị như của VNPT, Viettel...

3 Thiết kế sơ đồ mạng bằng Packet Tracer



Hình 5: Tổng quan về thiết kế mạng BBBank trong Packet Tracer

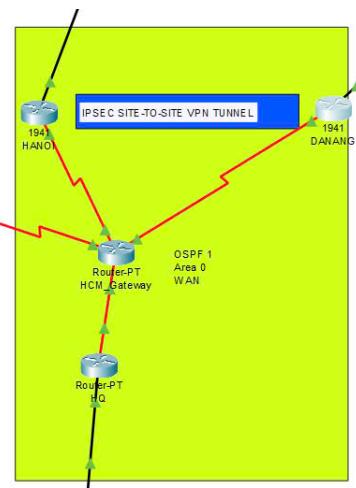
Nhìn chung, sơ đồ mạng này bao gồm một số thành phần của hệ thống mạng:

- Chi nhánh trụ sở chính: Gồm bảy tầng, mỗi tầng là nơi làm việc của các phòng ban khác nhau, với nhiều máy trạm, cổng Router kết nối giữa tất cả các chi nhánh, cùng với các máy chủ và thiết bị trung gian.
- Chi nhánh Đà Nẵng và Hà Nội: Mỗi chi nhánh này có một tập hợp các thiết bị nhỏ hơn so với chi nhánh trụ sở chính, bao gồm các máy trạm và các máy chủ nội bộ của từng chi nhánh.
- Khu vực ngoài: Thiết kế cũng bao gồm một số khu vực mạng bên ngoài các chi nhánh, như khu vực DMZ, "Internet" và kết nối từ các nhân viên làm việc từ xa (Teleworker).

3.1 Kết nối liên thông

3.1.1 Wide Area Network (WAN) Connectivity

Sơ đồ trên mô tả kết nối Mạng Diện Rộng (WAN) của 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 thông qua thuật toán trạng thái liên kết.



Hình 6: OSPF 1 Area 0 WAN

OSPF Area 0 (Khu vực xương sống):

- Các router trong phần này là một phần của Area 0, khu vực xương sống của môi trường mạng OSPF.
- Các địa điểm khác (ví dụ: chi nhánh và khu vực bên ngoài) trong mạng phải kết nối với Area 0, khiến nó trở thành trung tâm của việc phát tán lộ trình OSPF và đảm bảo tất cả các khu vực có thể giao tiếp hiệu quả.

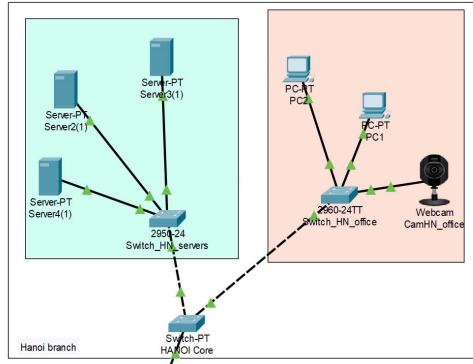
Router-PT HCM Gateway:

- Đóng vai trò là cổng kết nối cho Trụ sở và là router lõi kết nối tất cả các router chi nhánh.
- Đóng vai trò là điểm kết nối tới 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 vào mạng bên ngoài hoặc Internet (được mô tả bên trái sơ đồ này) thông qua liên kết này.
- Cổng kết nối với các router chính của từng chi nhánh sử dụng các đường thuê riêng để đảm bảo các kết nối và tải trọng quan trọng.

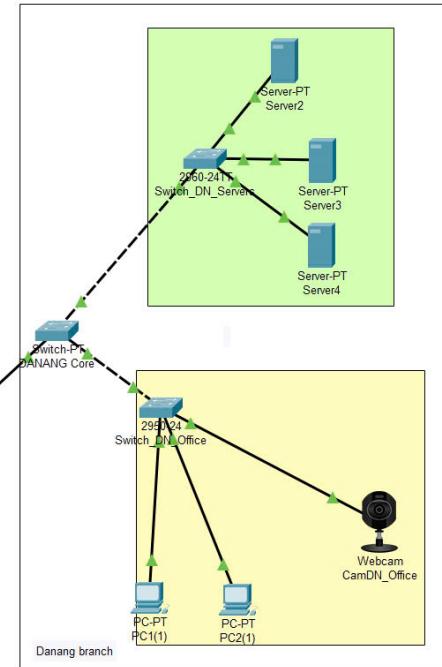
Router-PT HQ/HANOI/DANANG:

- Các router chính cho mỗi chi nhánh, kết nối mạng nội bộ và mạng bên ngoài.
- Mỗi router kết nối với mạng nội bộ của chi nhánh sử dụng cáp đồng thẳng (Copper Straight-Through).

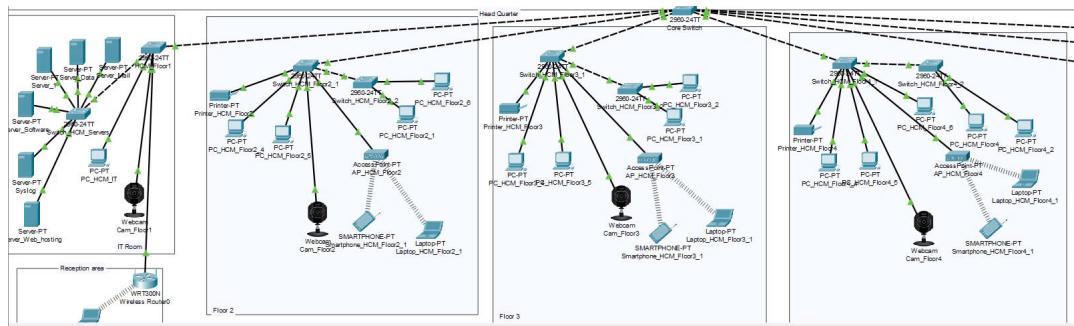
3.1.2 Kết nối giữa trung tâm và các chi nhánh



Hình 7: Hanoi Site Design



Hình 8: Danang Site Design

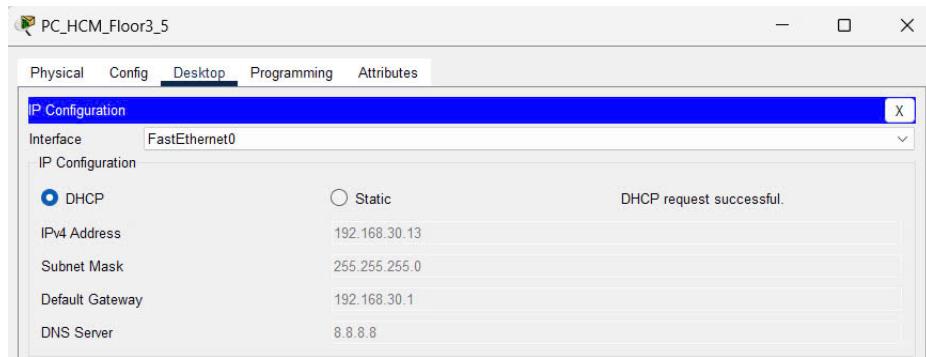


Hình 9: Ho Chi Minh Core Switch

Trong kiến trúc này, core switch đóng vai trò là trung tâm cho mạng của mỗi chi nhánh. Nó có nhiệm vụ định tuyến và chuyển mạch lưu lượng mạng một cách hiệu quả, đảm bảo kết nối liên tục giữa các phòng ban và dịch vụ của công ty.

Mỗi tầng hoặc phòng ban trong các chi nhánh sẽ có một access switch riêng biệt, kết nối với core switch trung tâm. Điều này tạo thành một topology hình sao, nén tất cả lưu lượng mạng được quản lý tập trung.

Các **VLAN** trải rộng qua nhiều switch thông qua các trunk links. Các trunk links này mang lưu lượng từ tất cả các VLAN mặc định giữa các switch, cho phép các thiết bị trên các VLAN khác nhau (ví dụ như các máy tính tại các tầng/phòng ban khác nhau) có thể giao tiếp với nhau qua thiết bị lớp 3.

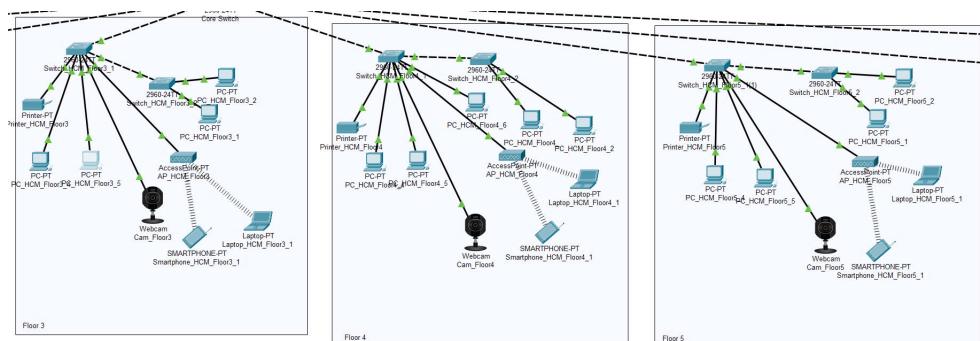


Hình 10: Các thiết bị đầu cuối sử dụng DHCP để nhận địa chỉ IP

Một cấu hình được thiết lập để cho phép mỗi thiết bị nhận địa chỉ IP thông qua DHCP. Ví dụ, thiết bị dưới đây ở tầng 3 (thuộc VLAN 30) sẽ nhận địa chỉ IP như mong đợi trong phạm vi subnet của nó. Một số thiết bị khác như camera IP và máy chủ sẽ được gán một địa chỉ IP cố định để đảm bảo việc truy cập liên tục.

3.1.3 Kết nối giữa các thiết bị

Các thiết bị đầu cuối ở mỗi tầng sẽ kết nối với một switch tầng. Điều này cho phép các thiết bị trong phòng có thể kết nối với nhau.



Hình 11: Các switch cấp tầng

3.1.4 Kết nối giữa mạng LAN và Internet

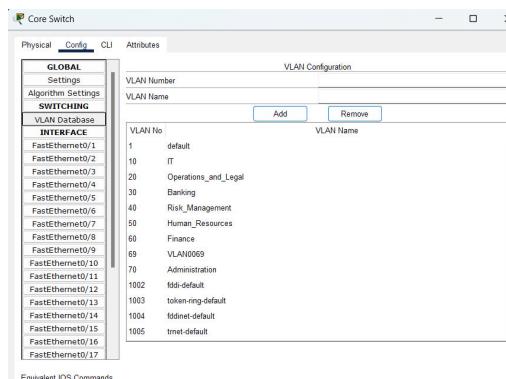
Ở hình 12 ta có thể thấy rằng các địa chỉ IP nội bộ đã được chuyển đổi thành các địa chỉ IP công cộng. Ví dụ, trong hình, địa chỉ IP của PC2 ở tầng 2 của chi nhánh Đà Nẵng, được chuyển từ

172.16.20.11 thành 209.165.0.2 (địa chỉ IP toàn cầu trên giao diện ngoài Serial0/1/1 của Main Gateway).

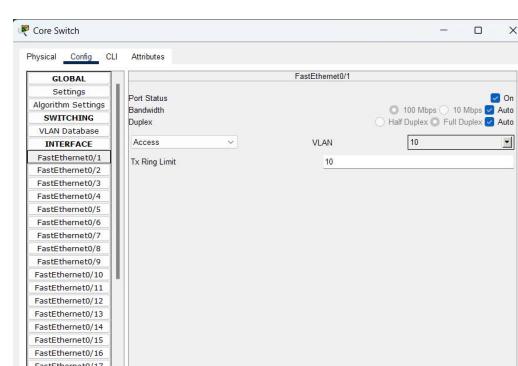
Phân Đoạn VLAN

Mạng được phân chia một cách logic thành nhiều VLANs, tách biệt các máy chủ quan trọng, nhóm người dùng, và lưu lượng khách mời. Việc phân đoạn này giúp nâng cao bảo mật và quản lý lưu lượng mạng, với việc định tuyến giữa các VLAN được xử lý bởi các switch lớp 3 (các "core switches" đã đề cập ở phần trên) để tối ưu hóa luồng lưu lượng mạng.

Hình 12: NAT



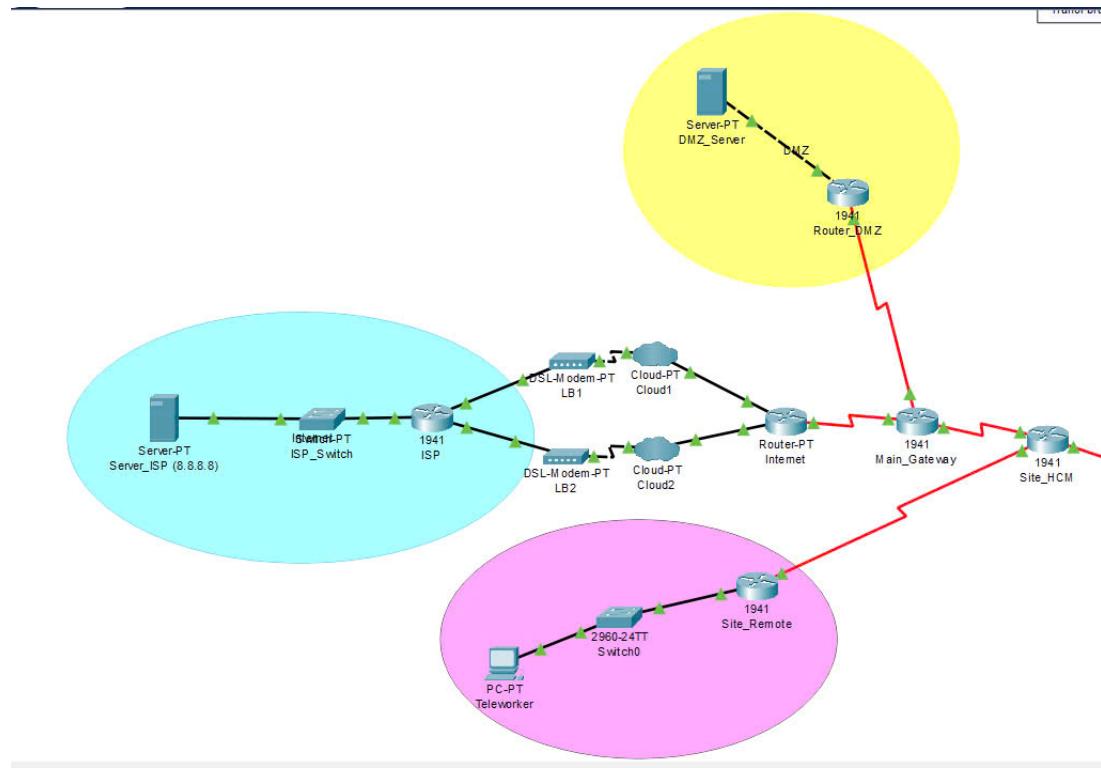
Hình 13: Core Switch VLAN Database



Hình 14: Core Switch Interfaces

Các switch của từng phòng ban khác nhau được kết nối với các cổng khác nhau trên core switch, và chúng được cấu hình để được gán vào các VLAN khác nhau theo mô tả đã được đưa ra.

3.1.5 Mạng ngoài



Hình 15: Thành phần mạng ngoài

Sơ đồ trên trình bày một mạng phức hợp bao gồm các thành phần để truy cập Internet, một DMZ dành cho các dịch vụ có thể truy cập công khai, và kết nối với các trang web từ xa dành cho nhân viên làm việc từ xa.

Demilitarized Zone (DMZ)

Trong các mạng máy tính, DMZ (Demilitarized Zone) là một mạng con vật lý hoặc logic được sử dụng để tách biệt mạng cục bộ (LAN) với các mạng không tin cậy khác – thường là Internet công cộng. DMZ cũng được gọi là mạng chu vi hoặc mạng con được sàng lọc.

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

DMZ networks thường được sử dụng để:

- Cách ly và bảo vệ các hệ thống tiềm ẩn mục tiêu khỏi mạng nội bộ.
- Giảm thiểu và kiểm soát quyền truy cập của người dùng bên ngoài vào các hệ thống đó.



- Lưu trữ tài nguyên công ty để một số tài nguyên này có thể được truy cập bởi người dùng bên ngoài được ủy quyền.

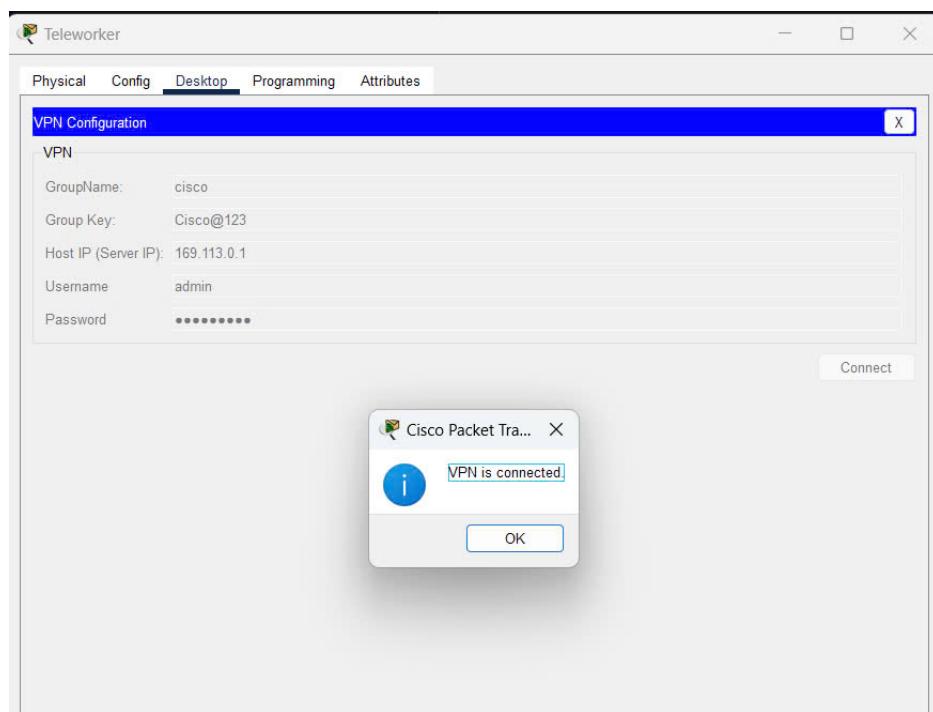
3.1.6 Kết nối từ xa cho nhân viên (Teleworker Connection)

Với VPN (Virtual Private Network), lưu lượng mạng giữa các văn phòng của tổ chức sẽ được truyền qua Internet công cộng thay vì thông qua một mạng vật lý độc lập. Tuy nhiên, để đảm bảo tính bảo mật, dữ liệu liên văn phòng sẽ được mã hóa trước khi đi vào Internet công cộng. Trong hệ thống này, tổ chức gồm có một trụ sở chính, 2 chi nhánh và một nhân viên làm việc từ xa thường truy cập Internet từ nhà.

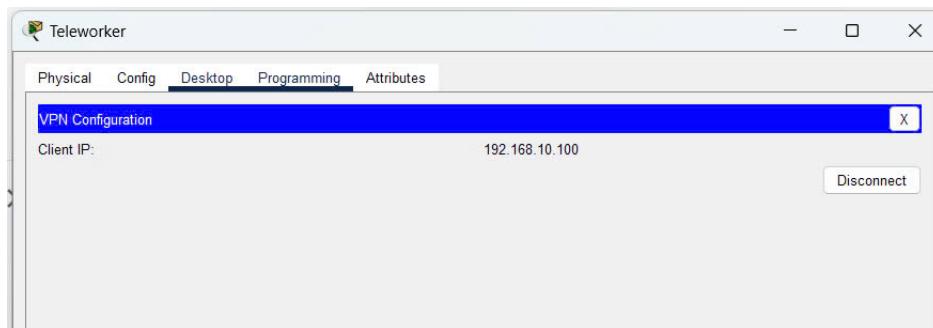
- Khi 2 thiết bị trong trụ sở chính gửi các gói tin IP cho nhau hoặc khi các thiết bị trong cùng chi nhánh liên lạc, chúng sử dụng IPv4 thông thường (không cần dịch vụ IPsec).
- Tuy nhiên, nếu thiết bị ở hai địa điểm khác nhau trong tổ chức cần giao tiếp qua Internet công cộng, lưu lượng sẽ được mã hóa trước khi truyền qua Internet.

Cấu hình VPN:

- Tên nhóm (Group Name): cisco
- Khóa nhóm (Group Key): Cisco@123
- IP máy chủ (Host IP): 169.113.0.1
- Tên người dùng (Username): admin
- Mật khẩu (Password): Admin@123



Hình 16: Người làm việc từ xa truy cập VPN



Hình 17: Nhân viên làm việc từ xa truy cập VPN thành công



```
C:\>ipconfig

FastEthernet0 Connection:(default port)
  Connection-specific DNS Suffix...:
  Link-local IPv6 Address.....: FE80::201:97FF:FE04:BED7
  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.....: ::1
  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

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=66ms TTL=124
Reply from 8.8.8.8: bytes=32 time=76ms TTL=124
Reply from 8.8.8.8: bytes=32 time=70ms TTL=124
Reply from 8.8.8.8: bytes=32 time=83ms 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 = 66ms, Maximum = 83ms, Average = 73ms
C:\>
```

Hình 18: Người làm việc từ xa có thể ping máy chủ web ở HQ

Site-to-Site VPN

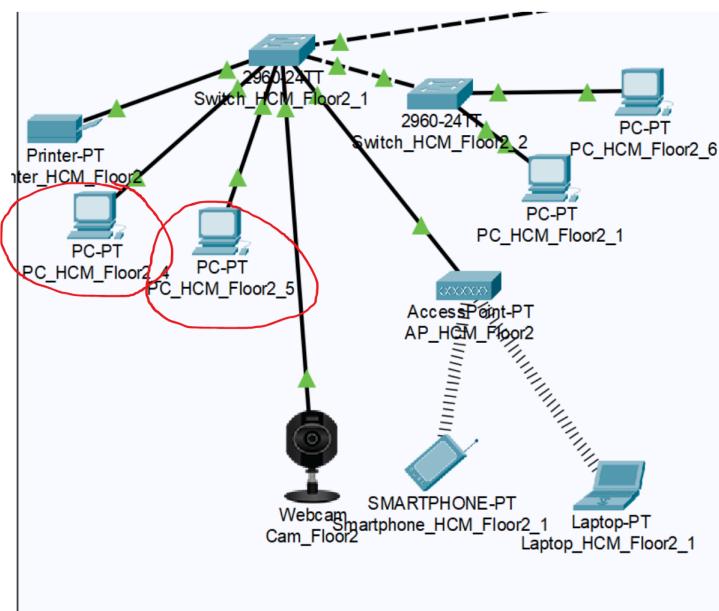
- Khi kết nối VPN giữa một PC ở Hà Nội và một PC ở Đà Nẵng được thiết lập, đường hầm VPN sẽ chuyển sang chế độ Active.
- Thông tin của VPN sẽ được hiển thị trên cả hai bộ định tuyến của hai địa điểm.

4 Mô phỏng Hệ thống Mạng

Có các kiểm tra được thực hiện để xác nhận kết nối theo yêu cầu. Lưu ý rằng các địa chỉ IP của các PC trong trường hợp có thể thay đổi từ bài kiểm tra này sang bài kiểm tra khác do DHCP. Chúng ta sẽ sử dụng lệnh **PING** để kiểm tra kết nối và lệnh **TRACERT** để xác nhận các tuyến đường trong một số bài kiểm tra, chẳng hạn như kiểm tra kết nối Internet.

4.1 Kết nối giữa các PC trong cùng một VLAN

Giả sử ta kết nối giữa hai PC trong Bộ phận Vận hành & Pháp lý



Hình 19: PC HCM Floor2_4 and PC HCM Floor2_5

```

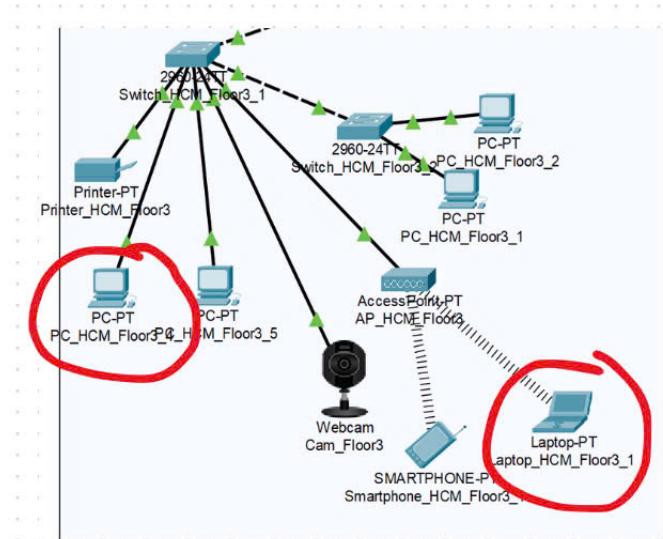
PC_HCM_Floor2_4
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address...: FE80::230:FE2FF:FE4D:92A6
IPv4 Address....: 192.168.20.13
Subnet Mask.....: 255.255.255.0
Default Gateway...: 192.168.20.1
Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address...: ::1
IPv4 Address....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway...: 0.0.0.0
C:\>ping 192.168.20.14
Pinging 192.168.20.14 with 32 bytes of data:
Reply from 192.168.20.14: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.20.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

PC_HCM_Floor2_5
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address...: FE80::230:A0FF:FE1:152A
IPv4 Address....: 192.168.20.14
Subnet Mask.....: 255.255.255.0
Default Gateway...: 192.168.20.1
Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address...: ::1
IPv4 Address....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway...: 0.0.0.0
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 = 0ms, Average = 0ms
C:\>

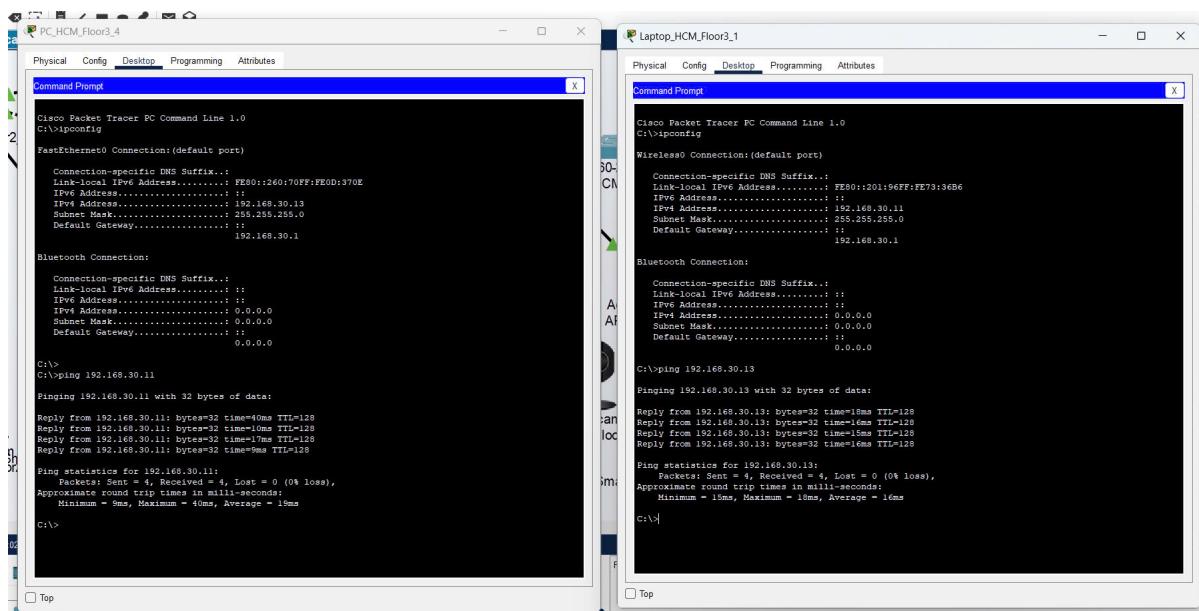
```

Hình 20: Kết nối giữa PC2_4 và PC2_5

4.1.1 Kết nối PC được kết nối Ethernet và Laptop được kết nối với Wifi bên trong Phòng Ngân hàng



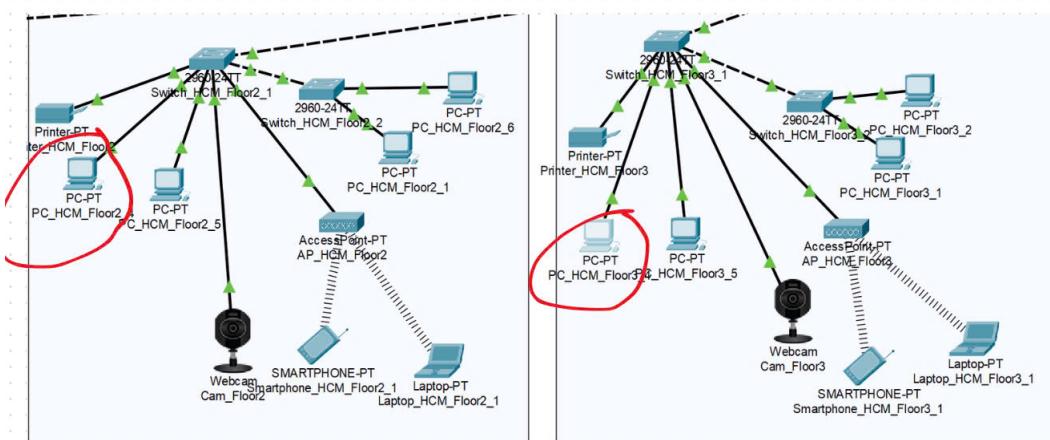
Hình 21: PC HCM Floor3_4 and Laptop HCM Floor3_1



Hình 22: Kết nối PC HCM Tầng 3_4 và Laptop HCM Tầng 3_1

4.2 Kết nối thiết bị giữa các VLAN

4.2.1 Kết nối thiết bị từ phòng Vận hành & Pháp lý đến máy tính trong phòng Ngân hàng



Hình 23: PC HCM Tầng 2_4 và Laptop HCM Tầng 3_4

```

PC_HCM_Floor2_4
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.30.13:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ipconfig
FastEthernet0 Connection:(default port)
    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....:: FE80::230:FF:FE4D:92A6
    IPv4 Address.....: 192.168.20.13
    IPv4 Address.....: 192.168.20.13
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: :: 192.168.20.1
Bluetooth Connection:
    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....:: ::
    IPv4 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0
C:\>ping 192.168.30.13
Pinging 192.168.30.13 with 32 bytes of data:
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.30.13:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

```



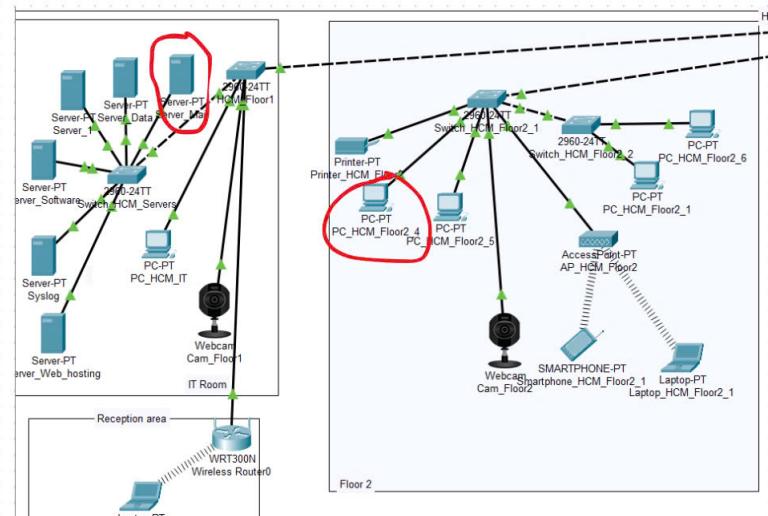
```

PC_HCM_Floor3_4
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.20.13: bytes=32 time<1ms TTL=127
Reply from 192.168.20.13: bytes=32 time<1ms TTL=127
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 = 7ms, Average = 1ms
C:\>ipconfig
FastEthernet0 Connection:(default port)
    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....:: FE80::260:70FF:FE0D:370E
    IPv4 Address.....: 192.168.30.13
    IPv4 Address.....: 192.168.30.13
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: :: 192.168.30.1
Bluetooth Connection:
    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....:: ::
    IPv4 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0
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=127
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:\>

```

Hình 24: Kết nối PC HCM Tầng 2_4 và Laptop HCM Tầng 3_4

4.2.2 Kết nối PC từ HCM đến máy chủ



Hình 25: PC HCM Floor2_4 and Server Mail

```

Server_Mail
Physical Config Services Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer SERVER Command Line 1.0.
C:\>ipconfig

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix: .
Link-local IPv4 Address . . . . : FE80::290:21FF:FE30:31D6
IPv4 Address . . . . : 192.168.10.10
Subnet Mask . . . . : 255.255.255.0
Default Gateway . . . . : 192.168.10.1
C:\>

PC_HCM_Floor2_4
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127

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

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127

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

C:\>ping 192.168.10.10

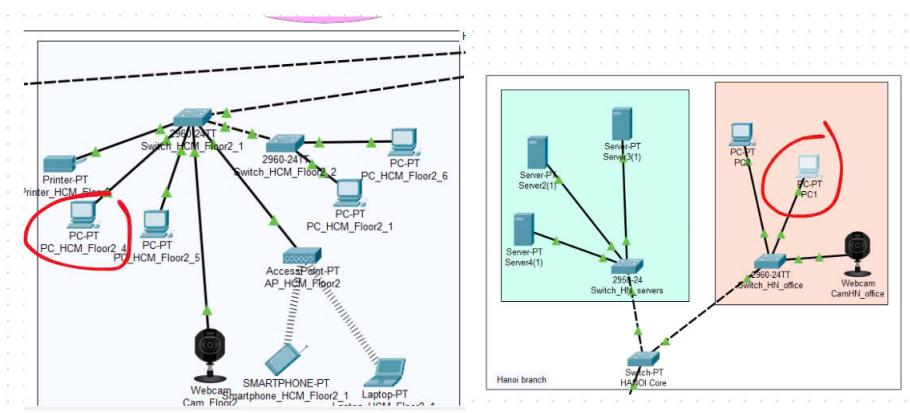
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>2

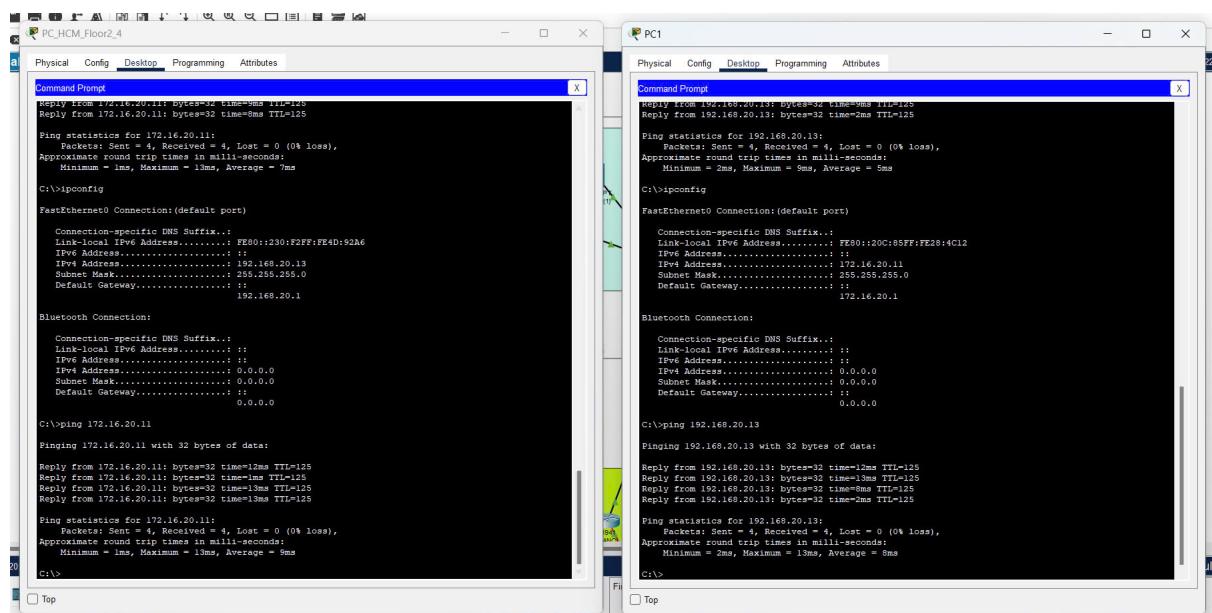
```

Hình 26: Kết nối PC HCM Tầng 2_4 đến Server Mail

4.2.3 Kết nối thiết bị từ HCM đến thiết bị ở Hà Nội

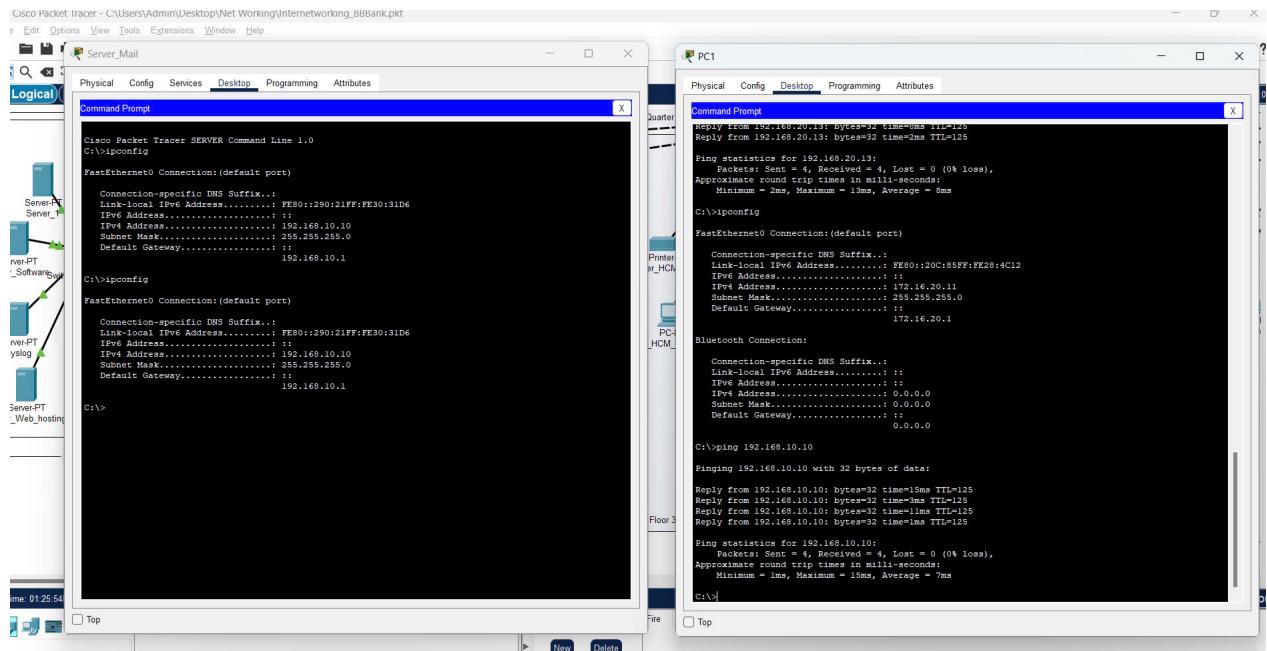


Hình 27: PC HCM Tầng 2_4 và PC1 (Hà Nội)



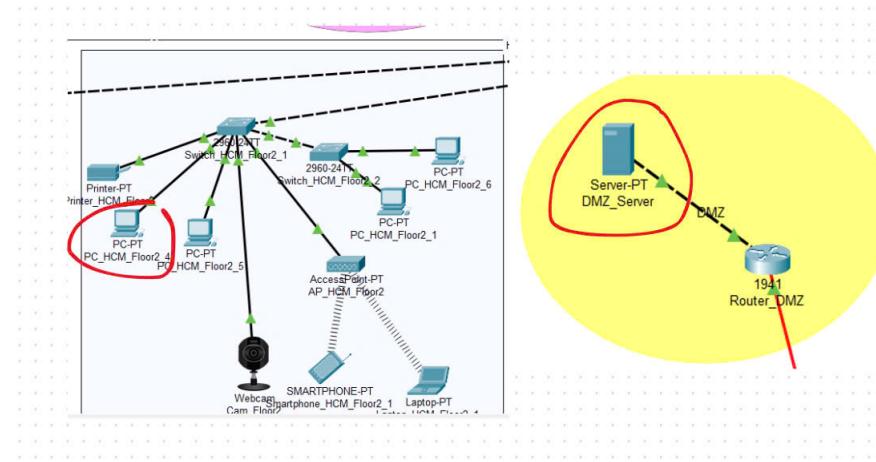
Hình 28: Kết nối PC HCM Tầng 2_4 và PC1 (Hà Nội)

4.2.4 Kết nối thiết bị ở Hà Nội với Mail Server ở HCM

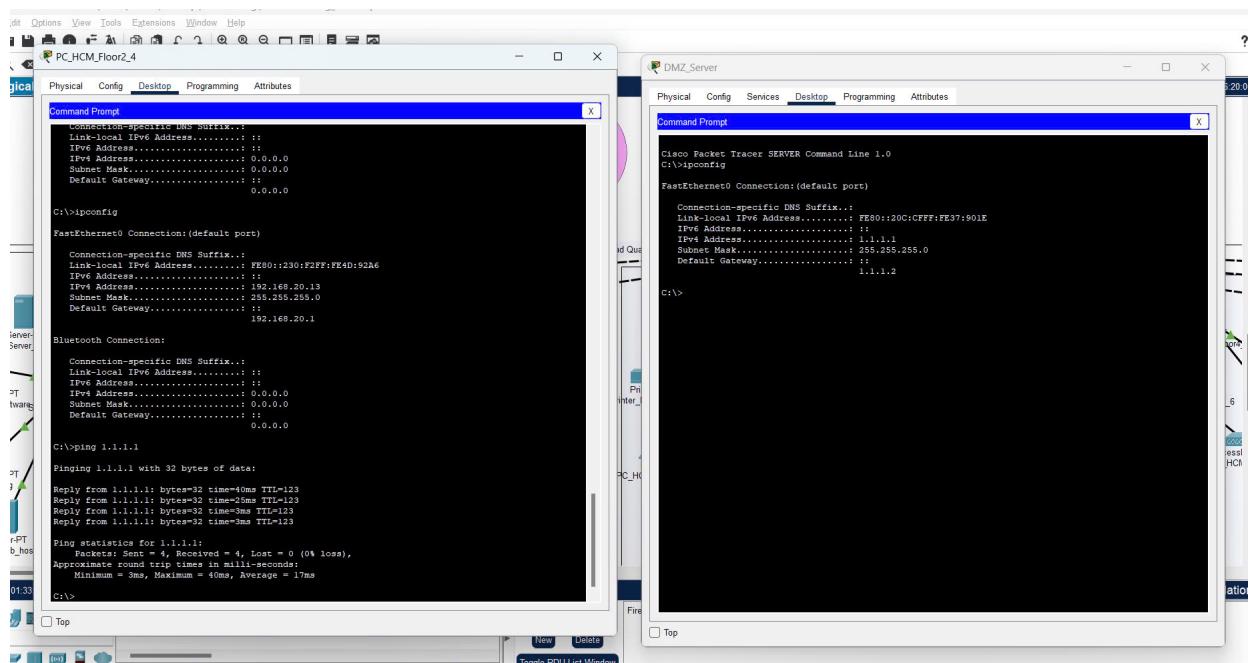


Hình 29: Kết nối PC ở Hà Nội đến Mail Server ở HCM

4.2.5 Kết nối tới máy chủ trong DMZ



Hình 30: PC HCM Tầng 2_4 và DMZ Server)

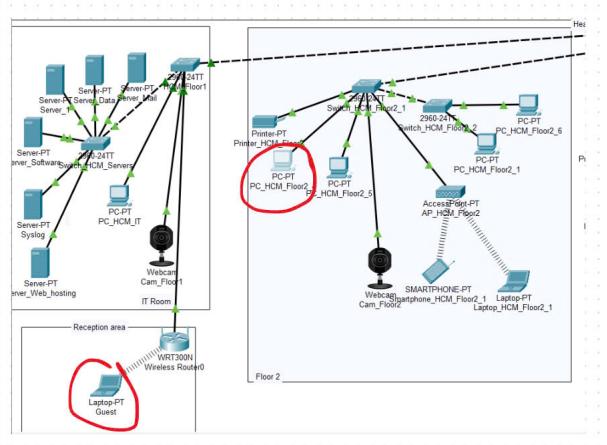


Hình 31: Kết nối PC HCM Tầng 2_4 và DMZ Server

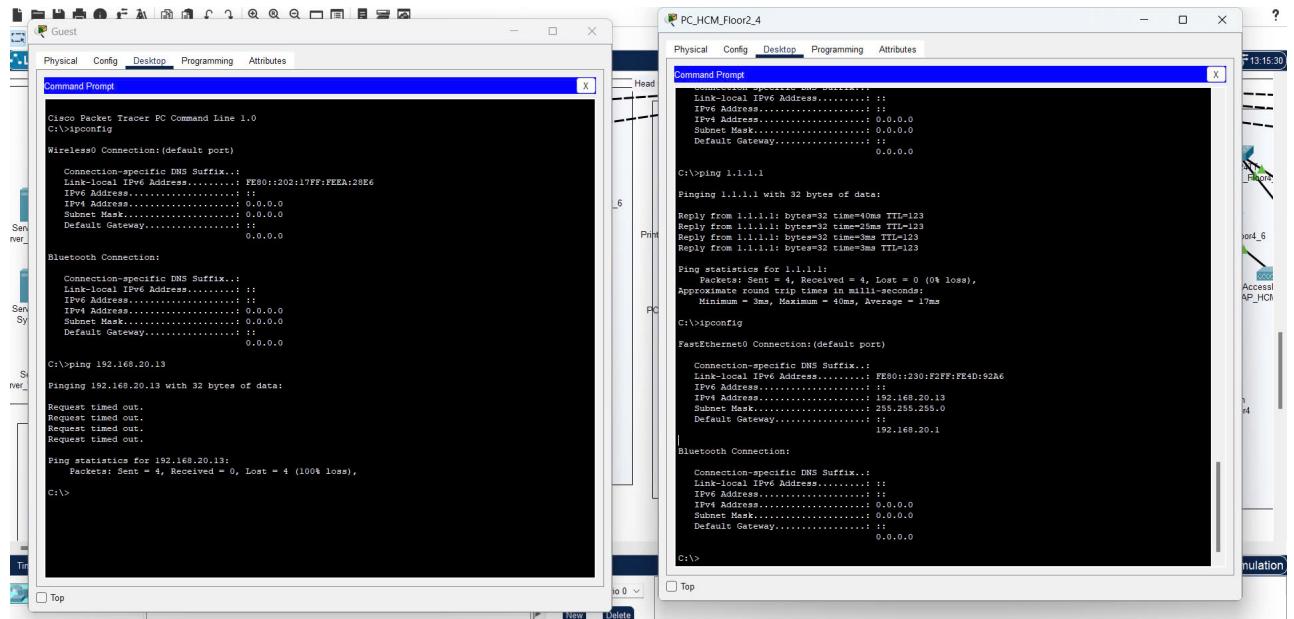
4.3 Không có kết nối từ thiết bị của khách hàng đến thiết bị trên mạng LAN

Các laptop của khách hàng kết nối với WIFI của khách hàng bị chặn không thể truy cập vào phần còn lại của mạng thông qua ACL/Firewall.

4.3.1 Không thể kết nối từ Laptop của khách hàng đến PC trên Tầng 2

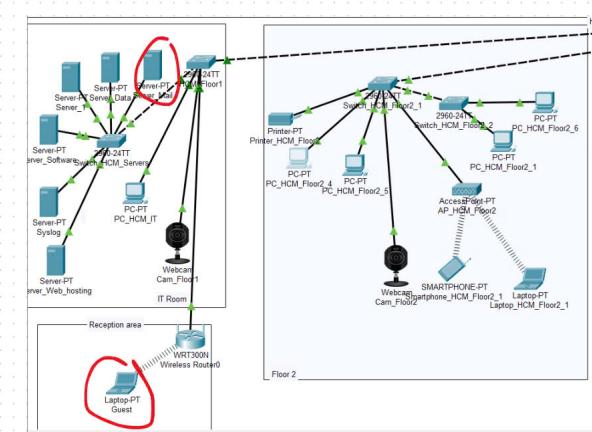


Hình 32: Laptop Guest và PC HCM Floor2_4

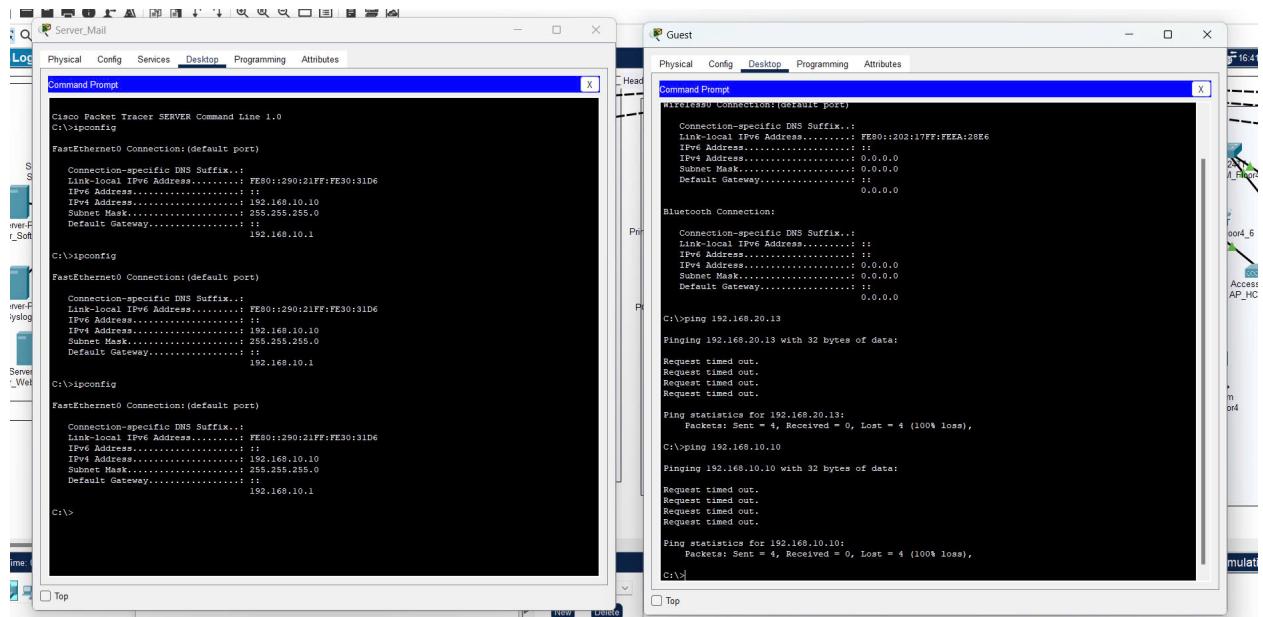


Hình 33: Yêu cầu ping không thành công từ Laptop Guest

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



Hình 34: Laptop Guest và Server Data

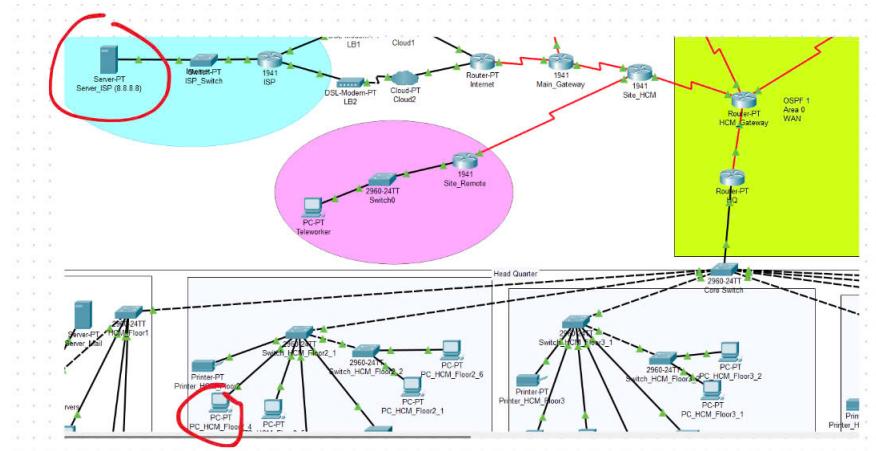


Hình 35: Yêu cầu ping không thành công từ Laptop Guest

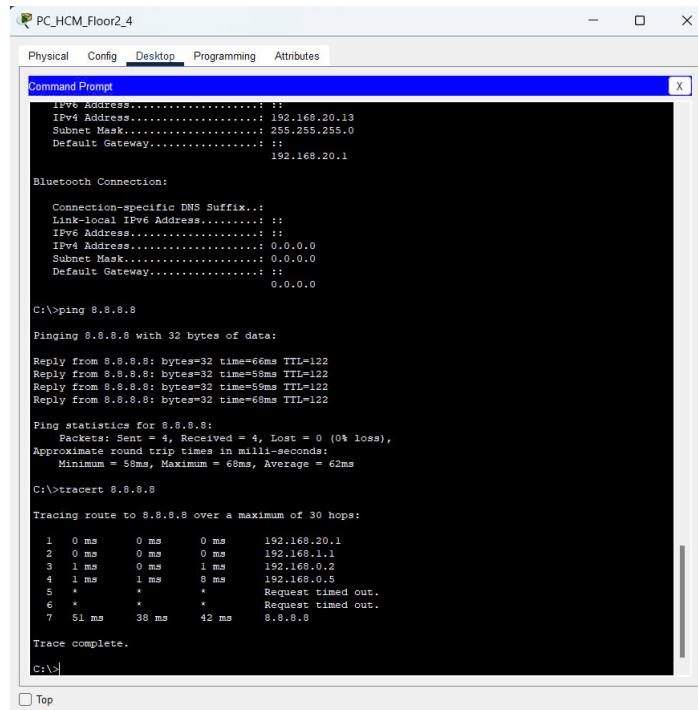
4.4 Kết nối Internet tới Web Server

4.4.1 Kết nối từ PC HCM Tầng 2_4 đến 8.8.8.8

Kiểm tra ping và theo dõi đường dẫn được thực hiện từ PC ở HCM đến máy chủ 8.8.8.8 trên Internet để xác nhận kết nối và định tuyến đến Internet.



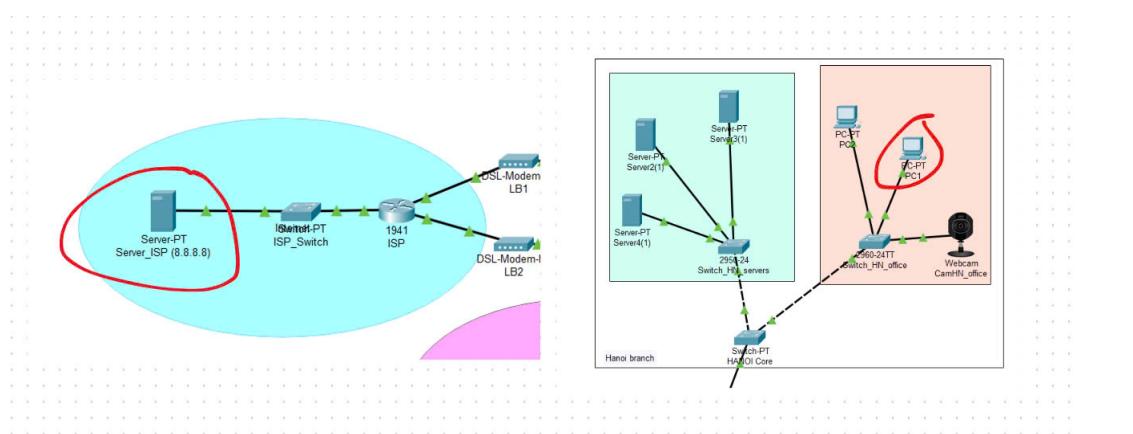
Hình 36: PC HCM Floor2 4 and internet Web Server



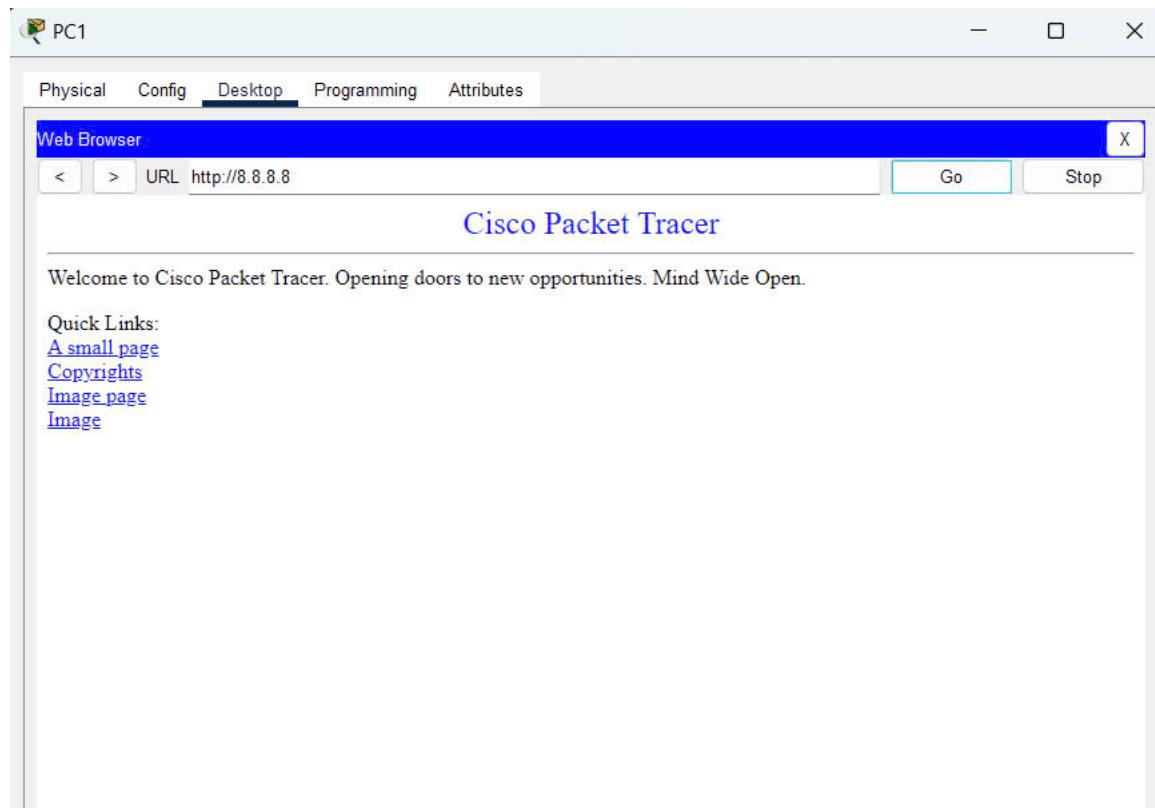
Hình 37: Ping và theo dõi đường dẫn từ PC in HCM đến Internet

4.4.2 Kết nối từ PC1 (Hà Nội) đến Web Server bằng trình duyệt Web qua HTTP

Chúng ta cũng sử dụng trình duyệt web để truy cập máy chủ 8.8.8.8 trên internet.



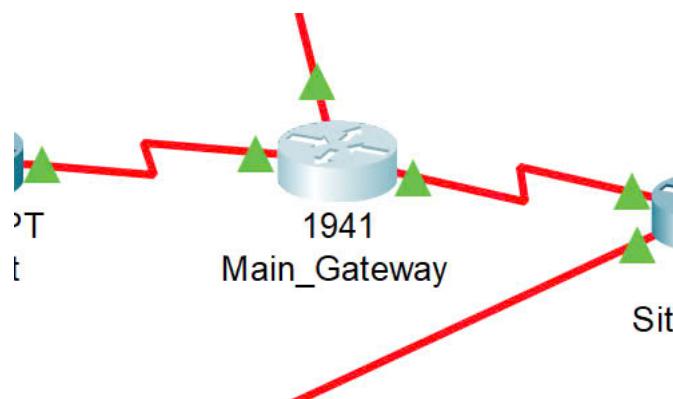
Hình 38: PC in Hanoi to 8.8.8.8 server



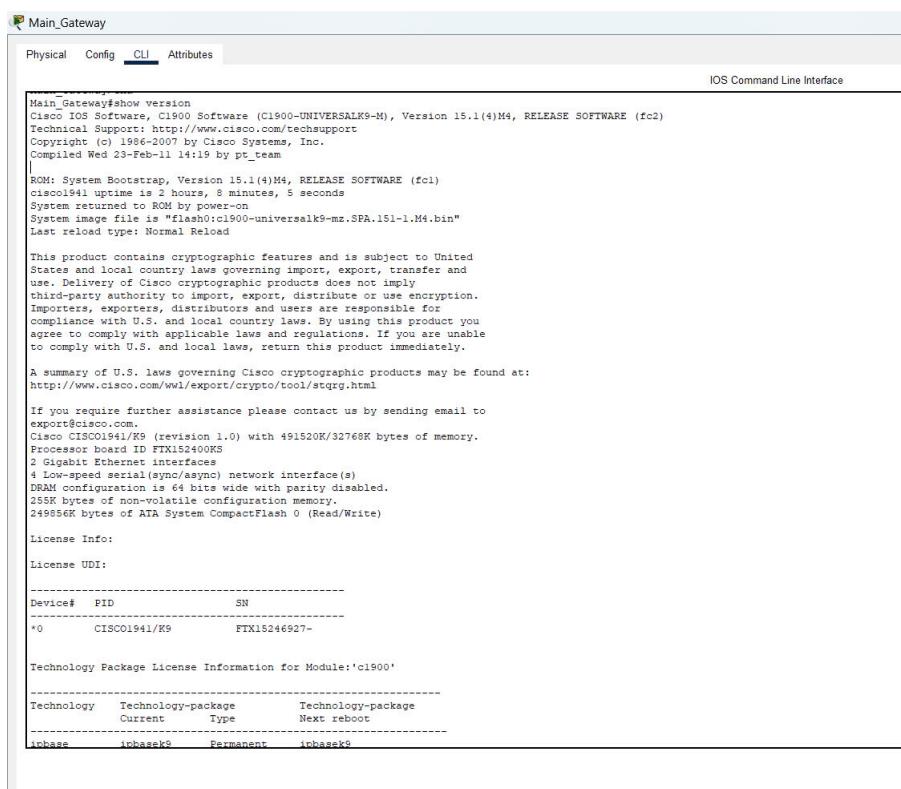
Hình 39: Truy cập 8.8.8.8 từ PC tại Hà Nội

4.5 Bảo mật

Có giấy phép bảo mật có tên K9 cho bộ định tuyến.



Hình 40: Router Main GateWay



Main_Gateway#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed Feb 23 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 2 hours, 5 minutes, 5 seconds
System returned to ROM by power-on
System image file is "flash:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/w处处/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
4 Low-speed serial (sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
256K Bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

Device# PID SN

*0 CISCO1941/K9 FTX15246927-

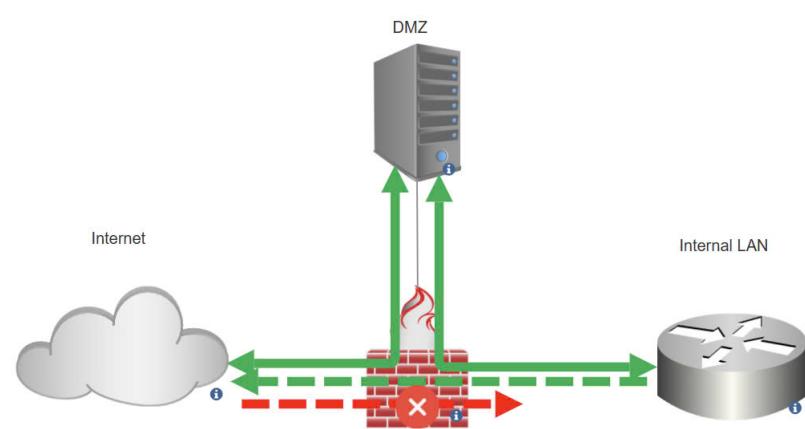
Technology Package License Information for Module:'c1900'

Technology Technology-package Technology-package
Current Type Next reboot

imbase imbasek9 Permanent imbasek9

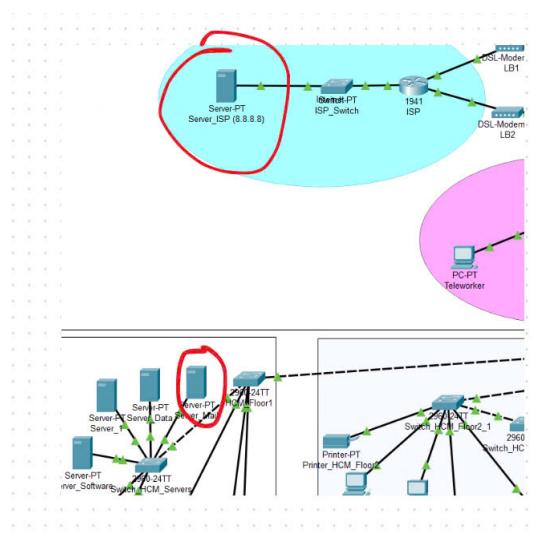
Hình 41: Router được trang bị giấy phép Security K9

4.5.1 Firewall



Hình 42: Firewall

Mạng LAN nội bộ bao gồm Trụ sở chính và 2 chi nhánh, chúng gửi lưu lượng đến DMZ và Internet. DMZ có thể gửi và nhận lưu lượng từ LAN và Internet. Tuy nhiên, Internet không thể gửi lưu lượng đến mạng LAN nội bộ. Lưu lượng này bị chặn bởi tường lửa và Hệ thống Ngăn chặn Xâm nhập (IPS) trong router Main Gateway.



Hình 43: Server ISP và Mail server



The image shows two adjacent windows from the Cisco Packet Tracer SERVER Command Line interface. Both windows have a title bar labeled "Cisco Packet Tracer SERVER Command Line 1.0" and a menu bar with "Physical", "Config", "Services", "Desktop", "Programming", and "Attributes". The left window is titled "Server_Mail" and the right window is titled "Server_ISP (8.8.8.8)". Both windows show command-line output.

Server_Mail Output:

```
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix .:
Link-local IPv4 Address . . . . . : FE80::2D0:97FF:FE30:31D6
  IPv4 Address . . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix .:
Link-local IPv4 Address . . . . . : FE80::2D0:97FF:FE30:31D6
  IPv4 Address . . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix .:
Link-local IPv4 Address . . . . . : FE80::2D0:97FF:FE30:31D6
  IPv4 Address . . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
C:\>
```

Server_ISP Output:

```
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix .:
Link-local IPv4 Address . . . . . : FE80::2D0:97FF:FE30:31D6
  IPv4 Address . . . . . : 8.8.8.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 8.8.8.1
C:\>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.10:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.10:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Hình 44: Hệ thống phòng chống xâm nhập

5 Đánh giá Mạng

5.1 Đánh giá Bảo mật

Hệ thống của công ty cần đảm bảo tính vững chắc và an toàn để bảo vệ các thông tin quan trọng, chiến lược kinh doanh và hợp đồng với đối tác. Do đó, hệ thống phải đáp ứng một số yêu cầu bảo mật cơ bản, bao gồm:

- Kiểm soát quyền truy cập của người dùng.
- Ngăn ngừa sớm các hành vi truy cập trái phép.
- Cung cấp cảnh báo tức thời khi có những nỗ lực truy cập không hợp lệ.

Các yếu tố này đã được triển khai và chứng minh trong phần trước.

5.2 Đánh giá khả năng mở rộng

Hệ thống cần được thiết kế sao cho dễ dàng mở rộng (thêm thiết bị, cáp mạng, v.v.) để đáp ứng nhu cầu phát triển của ngân hàng, không chỉ tại trụ sở chính mà còn ở các chi nhánh. Hiện tại, trụ sở chính có khoảng 120 máy trạm trải rộng trên 7 tầng, mỗi tầng có các phòng ban với 10-30 máy. Theo thiết kế hiện tại, mỗi tầng sử dụng 2 switch 24 cổng (trừ một cổng kết nối với switch chính), cho phép sử dụng tối đa 47 cổng, giúp dễ dàng kết nối thêm thiết bị khi số lượng nhân viên tăng lên.

5.3 Những vấn đề chưa giải quyết

- Hệ thống vẫn còn nhiều điểm kết nối tập trung (các switch và router lõi), dẫn đến nguy cơ gián đoạn toàn bộ hệ thống khi các thiết bị này gặp sự cố.
- Chưa thể xác nhận thiết kế có đáp ứng được nhu cầu băng thông tải xuống và tải lên hàng ngày hay không.
- Thiết kế chủ yếu dựa vào lý thuyết, có thể không hoàn toàn phù hợp với thực tế triển khai.
- Chi phí của các thiết bị mạng Cisco khá cao, mặc dù có thể tiết kiệm ở một số khu vực.

5.4 Hướng đi trong tương lai

- Tìm kiếm các giải pháp thay thế thiết bị Cisco để giảm chi phí.
- Thiết kế để đảm bảo mạng không bị nghẽn và đáp ứng được yêu cầu băng thông của hệ thống trong việc tải xuống và tải lên.
- Dánh giá kỹ các nhu cầu thực tế, chi phí thiết bị và chi phí thiết kế để xây dựng một mạng đáp ứng cả yêu cầu về hệ thống lẫn chi phí.



- Triển khai các biện pháp dự phòng để sự cố ở một nút quan trọng (như switch lõi) không làm gián đoạn toàn bộ hệ thống.



References

- [1] <https://tutorials.ptnetacad.net/>
- [2] <https://www.youtube.com/@gurutechnetworks>