

Trường Đại học Bách khoa
Khoa Khoa học và Kỹ thuật máy tính



MẠNG MÁY TÍNH (CO3093)

Báo cáo Bài tập lớn 2
Network design and simulation for a critical large
company

Sinh viên thực hiện:

Trần Anh Khoa	2211644
Nguyễn Quốc Thắng	2213205
Lê Quang Lợi	2113976
Phạm Quốc Toàn	2213539

Giảng viên hướng dẫn: Vũ Thành Tài

Hồ Chí Minh Ngày 4 Tháng 12 Năm 2024

Mục lục

1 Giới thiệu	4
2 Yêu cầu hệ thống mạng	4
2.1 Trụ sở chính (Thành phố Hồ Chí Minh)	4
2.2 Chi nhánh Đà Nẵng và Hà Nội	4
2.3 Yêu cầu chung	4
3 Phân tích và thiết kế mạng	5
3.1 Phân tích bố trí vật lý	5
3.2 Thiết kế mạng	6
3.3 Bảo mật mạng	10
3.4 Thiết kế hệ thống mạng	12
3.4.1 Kết nối mạng LAN và WAN	12
3.4.2 Phân đoạn VLAN	12
3.4.3 VPN và bảo mật	13
3.4.4 Tính toán thông lượng và băng thông	13
4 Thiết kế bản đồ mạng bằng Packet Tracer	14
4.1 Tổng quan	14
4.2 Mô tả hệ thống mạng	14
4.3 Kết nối liên mạng (Interconnectivity)	15
4.3.1 Kết nối mạng diện rộng (WAN)	15
4.3.2 Chi tiết thiết kế	16
4.3.3 Kết nối giữa các phòng ban	16
4.3.4 Kết nối giữa các thiết bị trong cùng phòng ban	19
4.3.5 Kết nối giữa LAN và Internet	20
4.3.6 VLAN Segmentation	21
4.3.7 Bảo mật	23
5 Kiểm tra kết nối mạng bằng Packet Tracer	28
5.1 Kết nối giữa các PC trong cùng một VLAN	28
5.1.1 PC và PC	28
5.1.2 Laptop và PC	29
5.2 Kết nối giữa các PC khác VLAN	30
5.2.1 PC và PC	30
5.2.2 PC đến Server	31
5.2.3 Laptop đến Server	32
5.2.4 Laptop và PC	33
5.3 Kết nối giữa các PC ở trụ sở chính và chi nhánh	34
5.3.1 PC và PC	34
5.3.2 PC đến Server	35
5.3.3 Laptop và PC	36
5.4 Kết nối đến Server ở DMZ	37
5.4.1 PC đến Server	37
5.5 Kết nối Internet đến Server Web	38
5.5.1 PC Ping và Traceroute đến Web Server	38
5.5.2 PC kết nối đến Server Web bằng trình duyệt	39

5.6	Bảo mật	40
6	Những điểm còn hạn chế và các hướng phát triển, cải thiện trong tương lai	42
6.1	Những vấn đề còn tồn tại	42
6.1.1	Phụ thuộc vào các thiết bị trung tâm	42
6.1.2	Khả năng mở rộng còn hạn chế	42
6.1.3	Vấn đề bảo mật	42
6.2	Hướng cải thiện trong tương lai	43
6.2.1	Đảm bảo tính dự phòng và ổn định	43
6.2.2	Tăng cường bảo mật	43
6.2.3	Cải thiện khả năng mở rộng	43
6.2.4	Hỗ trợ các công nghệ mới	43
6.3	Kết luận	43

Phân công công việc

Tên sinh viên	Phân công công việc	Hoàn thành
Phạm Quốc Toàn	Wireless Network, Internet Access, and Load Balancing, Thuyết trình, Hỗ trợ làm report	100%
Nguyễn Quốc Thắng	HQ Core Network & VLAN Configuration, Làm Report	100%
Trần Anh Khoa	HQ Security, IPS & Firewall Configuration, Demo, Thuyết trình, Làm Report	100%
Lê Quang Lợi	Branch 1 and 2 Network Setup, Hỗ trợ làm report	100%

Bảng 1: Phân công công việc và mức độ hoàn thành

1 Giới thiệu

Công ty BB Bank, với quy mô lớn và yêu cầu cao về tính ổn định, bảo mật, và hiệu suất, đã đặt ra bài toán thiết kế một hệ thống mạng đáp ứng nhu cầu vận hành và phát triển trong tương lai. Dự án của nhóm nhằm thực hiện các nhiệm vụ:

- **Phân tích yêu cầu** và thiết kế hệ thống mạng hoàn chỉnh cho BB Bank.
- **Mô phỏng kết nối mạng** giữa trụ sở chính tại TP.HCM và các chi nhánh ở Đà Nẵng và Hà Nội.
- **Đánh giá hiệu năng mạng** dựa trên các bài kiểm tra thực tế.

2 Yêu cầu hệ thống mạng

2.1 Trụ sở chính (Thành phố Hồ Chí Minh)

- Trụ sở chính bao gồm 7 tầng, tầng đầu tiên bao gồm phòng IT và trung tâm kết nối.
- Bao gồm: **120 máy trạm, 5 máy chủ, và 12 thiết bị mạng (hoặc hơn nếu tính thêm các thiết bị an ninh)**.
- Sử dụng công nghệ mới cho hạ tầng mạng bao gồm cả kết nối có dây và không dây, cáp quang (GPON), và GigaEthernet 1GbE/10GbE. Mạng được xây dựng một cách hệ thống theo cấu trúc VLAN cho mỗi phòng ban.
- Trụ sở chính kết nối tới 2 chi nhánh bằng 2 đường dây thuê riêng để kết nối WAN (có thể dùng SD-WAN, MPLS) và 2 xDSL để kết nối tới Internet với 1 cơ chế cân bằng tải. Tất cả kết nối tới Internet phải đi qua mạng con của Trụ sở chính.
- Công ty sử dụng cả công nghệ đã mua và công nghệ mã nguồn mở.
- Yêu cầu phải có bảo mật cao (tường lửa, IPS/IDS), phải có tính khả dụng cao, phải dễ dàng xử lý khi có vấn đề xảy ra và phải thuận tiện cho việc nâng cấp hệ thống.
- Có cấu hình VPN cho kết nối giữa các bên và cho nhân viên làm việc từ xa.
- Phải có hệ thống camera an ninh.

2.2 Chi nhánh Đà Nẵng và Hà Nội

- Mỗi chi nhánh cho 2 tầng. Tầng đầu tiên bao gồm phòng IT và trung tâm kết nối.
- **30 máy trạm, 3 máy chủ, và 5 thiết bị mạng (hoặc hơn nếu tính thêm các thiết bị an ninh)** tại mỗi chi nhánh.

2.3 Yêu cầu chung

Hệ thống thường có yêu cầu về tải cao tại các khung giờ cao điểm là: 9 - 11 giờ và 15 - 16 giờ. Cụ thể như sau:

- **Trụ sở chính:** yêu cầu máy chủ để cập nhật phần mềm, truy cập mạng, truy cập cơ sở dữ liệu, ... Tổng ước tính tải xuống khoảng 1000 MB/ngày và tải lên khoảng 2000 MB/ngày.
- **Các chi nhánh:** mỗi chi nhánh yêu cầu lướt web, tải tài liệu, giao dịch với khách hàng ... Tổng ước tính tải xuống khoảng 500 MB/ngày và tải lên khoảng 100 MB/ngày.

- Yêu cầu kết nối WiFi cho thiết bị của khách hàng để tải xuống khoảng 500 MB/ngày. Công ty được dự đoán sẽ tăng trưởng khoảng 20% trong 5 năm tới (về số lượng khách hàng, tải truy cập mạng, việc mở rộng chi nhánh, ...)

3 Phân tích và thiết kế mạng

3.1 Phân tích bố trí vật lý

Bản thiết kế phải đáp ứng được những yêu cầu về mạng. Do có nhiều lựa chọn với những mặt lợi và hại và chi phí khác nhau nên nhóm chúng em chia hệ thống ra thành các phần nhỏ và phân tích từng phần.

Chúng em sẽ bắt đầu khảo sát và thiết kế bố trí mạng cho công ty, sau đó sẽ tổng hợp các lựa chọn cho mạng. Tiếp theo là sẽ phân tích từng thiết bị và lựa chọn. Sau đó chúng em sẽ tốc độ đầu - cuối (Throughput) và đưa ra lựa chọn phù hợp cho ISP. Cuối cùng, nhóm chúng em sẽ thiết kế và giả lập bố trí mạng.

Khảo sát tại địa điểm cần thiết kế mạng của công ty cần tập trung vào các điểm sau:

- **Cách bố trí hiện tại của tòa nhà:** quan sát các vật cản và những thứ có thể ảnh hưởng tới kết nối mạng (ví dụ: hệ thống điện, từ trường tại khu vực, ...)
- **Cách bố trí hiện tại của từng phòng ban:** quan sát và dự đoán số người trong 1 phòng ban. Bên cạnh đó cần tìm hiểu về chức năng của từng phòng ban để đề xuất hệ thống an ninh phù hợp.

Dựa theo yêu cầu, nhóm chúng em giả sử kết quả khảo sát của trụ sở chính và các chi nhánh như sau:

Trụ sở chính:

- **Tầng 1:** 10 máy trạm, 5 máy chủ
- **Tầng 2:** 20 máy trạm
- **Tầng 3:** 20 máy trạm
- **Tầng 4:** 20 máy trạm
- **Tầng 5:** 20 máy trạm
- **Tầng 6:** 20 máy trạm
- **Tầng 7:** 10 máy trạm

Chi nhánh:

- **Tầng 1:** 15 máy trạm, 3 máy chủ
- **Tầng 2:** 15 máy trạm

3.2 Thiết kế mạng

Đầu tiên, cần trang bị một bộ định tuyến (Cisco ISR4321/K9) cho trụ sở chính và mỗi chi nhánh. Cùng với đó, cần có một card giao diện mạng (Cisco NIM-ES2-8) để hỗ trợ kết nối. Ngoài ra, ngay cả khi sử dụng mạng có dây, công ty vẫn cần các điểm truy cập Wi-Fi để hỗ trợ kết nối cho khách hàng và các thiết bị ngoại vi.

Kết nối có dây

- **Công nghệ sử dụng:** Ethernet-Cat8, hiện là công nghệ mới và ổn định nhất trên thị trường.
- **Ưu điểm:** Cung cấp tốc độ lên tới 40Gbps, giảm thiểu nhiễu từ môi trường.
- **Nhược điểm:** Cáp Ethernet-Cat8 kém linh hoạt, khó lắp đặt trong môi trường cần thay đổi thường xuyên.
- **Thiết bị cần thiết:**
 - 11 bộ chuyển mạch (Cisco Catalyst 2960-L Series WS-C2960L-24TS-LL) để kết nối các máy trạm với mạng nội bộ tại các tầng của trụ sở chính và chi nhánh.
 - 11 điểm truy cập Wi-Fi nhẹ (TPLink Archer A6) để đảm bảo kết nối không dây tại 7 tầng của trụ sở chính và 2 tầng tại mỗi chi nhánh.

Kết nối không dây

- **Công nghệ sử dụng:** Wi-Fi 6 (Cisco Catalyst 9115AX Series).
- **Ưu điểm:** Không bị giới hạn bởi số lượng cổng Ethernet, dễ dàng triển khai trong các môi trường linh hoạt.
- **Nhược điểm:** Có thể gặp nhiều khi nhiều máy trạm cùng lúc truy cập mạng.
- **Thiết bị cần thiết:** 11 điểm truy cập Wi-Fi Cisco Catalyst 9115AX Series để đáp ứng nhu cầu kết nối cho các tầng của trụ sở chính và các chi nhánh.

Phân tích chi phí và thông số thiết bị

Router: Cisco ISR4321/K9

- **Chi phí:** 23,000,000 VND
- **Thông số kỹ thuật:**
 - **Tổng băng thông:** 50 Mbps đến 100 Mbps
 - **Cổng RJ45:** 2
 - **Cổng SFP:** 2
 - **Khe cắm module NIM:** 2, khe SM-X: 1
 - **Bộ nhớ RAM:** 4 GB (mặc định), 16 GB (tối đa)
 - **Flash:** 4 GB (mặc định), 16 GB (tối đa)
 - **Kích thước:** 44.5 x 345 x 294 mm
 - **Trọng lượng:** 5.5 kg



Hình 1: Router Cisco ISR4321/K9

Card giao diện mạng: Cisco NIM-ES2-8

- **Chi phí:** 12,000,000 VND
- **Thông số kỹ thuật:**
 - **Số cổng:** 8 cổng Gigabit Ethernet
 - **Tiêu chuẩn:** IEEE 802.3, 802.1q, 802.1X
 - **Tính năng quản lý:** SNMP, Telnet, TFTP, Embedded RMON
 - **Kích thước:** 0.8 x 3.5 x 4.9 in.
 - **Trọng lượng:** 85 g



Hình 2: Card giao diện mạng Cisco NIM-ES2-8

Switch: Cisco Catalyst 2960-L Series WS-C2960L-24TS-LL

- **Chi phí:** 14,500,000 VND mỗi thiết bị
- **Thông số kỹ thuật:**

- **Số cổng:** 24 cổng Ethernet Gigabit, 2 cổng uplink SFP
- **Băng thông chuyển tiếp:** 18 Gbps
- **Tốc độ chuyển tiếp:** 10.7 Mpps
- **RAM:** 512 MB
- **Flash:** 256 MB
- **Kích thước:** 4.4 x 45 x 24.2 cm
- **Trọng lượng:** 6.4 kg



Hình 3: Switch Cisco Catalyst 2960-L Series WS-C2960L-24TS-LL

Cáp mạng: UGREEN Cat8 Ethernet Cable

- **Chi phí:** 400,000 VND mỗi dây (10 mét)
- **Thông số kỹ thuật:**
 - **Tốc độ truyền tải:** 40 Gbps
 - **Băng thông:** 2000 MHz
 - **Chất liệu:** Lõi đồng nguyên chất, dây bện 48 sợi
 - **Chống nhiễu:** 4 lớp



Hình 4: Cáp mạng UGREEN Cat8 Ethernet Cable

Điểm truy cập Wi-Fi: TP-Link Archer A6

- **Chi phí:** 500,000 VND mỗi thiết bị
- **Thông số kỹ thuật:**
 - **Tiêu chuẩn Wi-Fi:** Wi-Fi 5
 - **Tốc độ:** 867 Mbps (5 GHz), 300 Mbps (2.4 GHz)
 - **Cổng Ethernet:** 1 WAN, 4 LAN (10/100 Mbps)
 - **Hỗ trợ MU-MIMO:** 2x2



Hình 5: Điểm truy cập Wi-Fi TP-Link Archer A6

Điểm truy cập Wi-Fi: Cisco Catalyst 9115AX Series

- **Chi phí:** 23,000,000 VND mỗi thiết bị
- **Thông số kỹ thuật:**
 - **Tiêu chuẩn Wi-Fi:** Wi-Fi 6
 - **MU-MIMO:** 4x4
 - **Băng tần:** 2.4 GHz, 5 GHz
 - **Tốc độ PHY tối đa:** 5 Gbps
 - **Kích thước:** 250 x 250 x 45 mm
 - **Trọng lượng:** 1.2 kg



Hình 6: Điểm truy cập WiFi Cisco Catalyst 9115AX Series

3.3 Bảo mật mạng

Chúng em sử dụng kiến trúc DMZ (Demilitarized Zone) để đảm bảo an toàn mạng. DMZ sẽ bao gồm một tường lửa và các máy chủ được sử dụng để xử lý các tương tác từ khách hàng hoặc các kết nối ra ngoài.

Tường lửa: Cisco ASA5506-SEC-BUN-K9

- **Chi phí:** 25,000,000 VND
- **Thông số kỹ thuật:**
 - **Băng thông kiểm tra trạng thái tối đa:** 750 Mbps
 - **Băng thông ứng dụng (AVC):** 250 Mbps
 - **Phiên kết nối đồng thời:** 20,000 (50,000 với giấy phép mở rộng)
 - **Kết nối mới mỗi giây:** 5,000
 - **Ứng dụng được hỗ trợ:** 3,000+
 - **Danh mục URL:** 80+
 - **VPN 3DES/AES:** 100 Mbps
 - **Phần mềm tích hợp:** Cisco SEC-K9 License



Hình 7: Tường lửa Cisco ASA5506-SEC-BUN-K9

Hệ thống giám sát: Camera DS-2GN5750-HH

- **Chi phí:** 4,335,000 VND mỗi chiếc
- **Thông số kỹ thuật:**
 - **Độ phân giải:** 4 MP
 - **Công nghệ nén:** H.265+
 - **Chống nước và bụi:** Chuẩn IP67
 - **Hình ảnh màu sắc 24/7:** Có
 - **Phát hiện người và phương tiện:** Có



Hình 8: Camera DS-2GN5750-HH

3.4 Thiết kế hệ thống mạng

3.4.1 Kết nối mạng LAN và WAN

- **Mạng WAN:** Sử dụng giao thức định tuyến OSPF Area 0 để kết nối trụ sở chính với các chi nhánh.
- **Mạng LAN:** Cấu trúc sao, mỗi tầng sử dụng switch riêng kết nối về core switch tại trung tâm.

3.4.2 Phân đoạn VLAN

VLAN ở trụ sở chính và 2 chi nhánh được chia để tách biệt mạng cho từng phòng ban tương ứng với mỗi tầng, đồng thời quản lý thiết bị khách hàng được cài đặt để tăng tính bảo mật.

- **Trụ sở chính ở Thành phố Hồ Chí Minh:**

- VLAN 10: Phòng CNTT
- VLAN 20: Phòng Pháp lý
- VLAN 30: Phòng ngân hàng
- VLAN 40: Phòng quản lý rủi ro
- VLAN 50: Phòng nhân sự
- VLAN 60: Phòng tài chính
- VLAN 70: Phòng quản trị

VLAN	Tầng	Địa chỉ mạng	Default Gateway	Địa chỉ khả dụng
VLAN10	1	192.168.10.0/24	192.168.10.1	192.168.10.2 - 192.168.10.254
VLAN20	2	192.168.20.0/24	192.168.20.1	192.168.20.2 - 192.168.20.254
VLAN30	3	192.168.30.0/24	192.168.30.1	192.168.30.2 - 192.168.30.254
VLAN40	4	192.168.40.0/24	192.168.40.1	192.168.40.2 - 192.168.40.254
VLAN50	5	192.168.50.0/24	192.168.50.1	192.168.50.2 - 192.168.50.254
VLAN60	6	192.168.60.0/24	192.168.60.1	192.168.60.2 - 192.168.60.254
VLAN70	7	192.168.70.0/24	192.168.70.1	192.168.70.2 - 192.168.70.254

Bảng 2: Sơ đồ Vlan trụ sở chính

- **2 chi nhánh ở Đà Nẵng, Hà Nội:**

- VLAN 10: Phòng CNTT
- VLAN 20: Phòng ngân hàng

VLAN	Tầng	Địa chỉ mạng	Default Gateway	Địa chỉ khả dụng
VLAN10	1	10.0.10.0/24	10.0.10.1	10.0.10.2 - 10.0.10.254
VLAN20	2	10.0.20.0/24	10.0.20.1	10.0.20.2 - 10.0.20.254

Bảng 3: Sơ đồ Vlan chi nhánh Đà Nẵng

VLAN	Tầng	Địa chỉ mạng	Default Gateway	Địa chỉ khả dụng
VLAN10	1	172.16.10.0/24	172.16.10.1	172.16.10.2 - 172.16.10.254
VLAN20	2	172.16.20.0/24	172.16.20.1	172.16.20.2 - 172.16.20.254

Bảng 4: Sơ đồ Vlan chi nhánh Hà Nội

3.4.3 VPN và bảo mật

- VPN site-to-site:** Sử dụng giao thức IPSec để mã hóa và bảo vệ dữ liệu.
- VPN cho nhân viên từ xa:** Sử dụng Cisco AnyConnect Secure Mobility Client.
- DMZ:** Thiết lập khu vực trung gian bảo vệ các máy chủ công khai khỏi mạng nội bộ.

3.4.4 Tính toán thông lượng và băng thông

Trụ sở chính

- Máy chủ:** Tổng dung lượng 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 dung lượng 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 50 khách hàng mỗi ngày
 - Tải xuống: $500 \times 50 = 25000$ MB/ngày.
 - Tải lên: 0MB/ngày.

Chi nhánh

- Máy chủ:** Tổng dung lượng tải lên và tải xuống của 3 máy chủ
 - Tải xuống: $1000 \times 3 = 3000$ MB/ngày.
 - $2000 \times 3 = 6000$ MB/ngày.
- Máy trạm:** Tổng dung lượng 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 30 máy khách mỗi ngày
 - Tải xuống: $500 \times 30 = 15000$ MB/ngày.
 - Tải lên: 0MB/ngày.

Trong 3 giờ cao điểm từ 9h-11h sáng và 3h-4h chiều, 80% lưu lượng dữ liệu tập trung vào thời gian này. Chúng ta cũng cần thêm 20% để dự phòng cho việc sử dụng và số lượng thiết bị tăng trong tương lai.

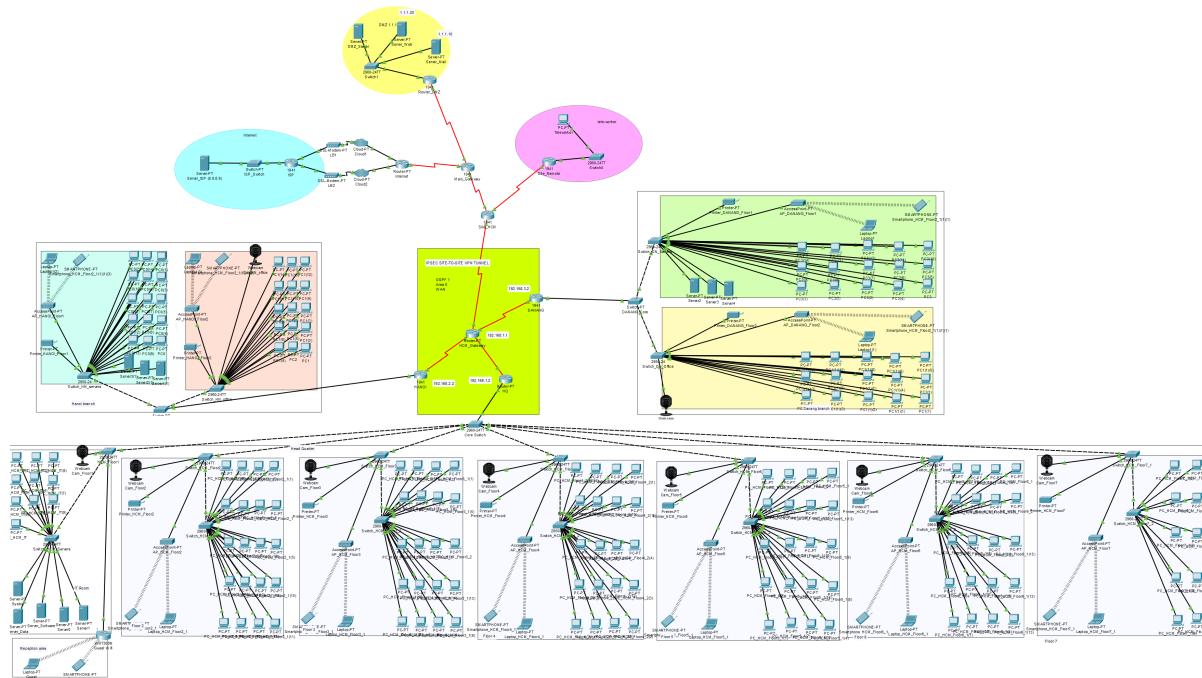
- Giờ cao điểm (80% tải):**
 - Tải xuống: 133.12 Mbps.
 - Tải lên: 34.13 Mbps.

- **ISP phù hợp:** VNPT, FPT, hoặc Viettel với băng thông tối thiểu 134 Mbps tải xuống và 35 Mbps tải lên.

4 Thiết kế bản đồ mạng bằng Packet Tracer

4.1 Tổng quan

Hình bên dưới trình bày bản thiết kế đầy đủ của mô hình mạng được triển khai trên Packet Tracer.



Hình 9

4.2 Mô tả hệ thống mạng

Bản thiết kế mạng bao gồm các thành phần chính sau:

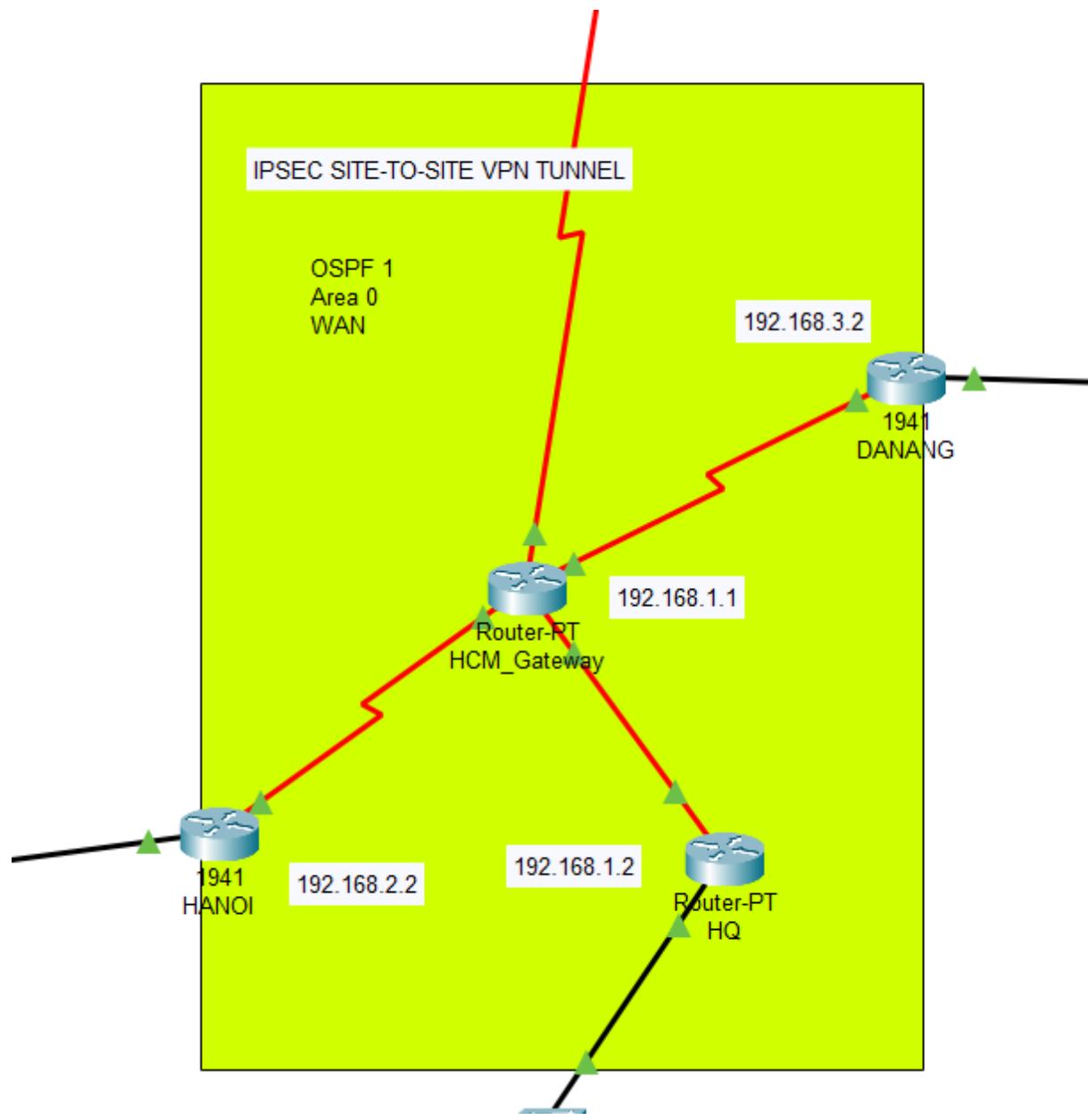
- **Khu vực nội bộ (Internal Area)**
 - **Chi nhánh Trụ sở chính:**
 - * Bao gồm 7 tầng, mỗi tầng chứa các phòng ban khác nhau, với nhiều máy trạm (workstations).
 - * Gateway router được đặt giữa các chi nhánh, cùng với một số máy chủ (Servers) và các thiết bị trung gian.
 - **Chi nhánh Đà Nẵng và Hà Nội:**
 - * Mỗi chi nhánh có quy mô thiết bị nhỏ hơn so với trụ sở chính, bao gồm các máy trạm và máy chủ cục bộ.
- **Khu vực bên ngoài (External Area):**
 - Thiết kế mạng cũng bao gồm các khu vực nằm ngoài các chi nhánh, cụ thể là:

- * **DMZ (Demilitarized Zone):** Khu vực bảo mật trung gian giữa mạng nội bộ và Internet.
- * **Internet:** Kết nối với mạng toàn cầu.
- * **Teleworker:** Kết nối dành cho nhân viên làm việc từ xa.

4.3 Kết nối liên mạng (Interconnectivity)

4.3.1 Kết nối mạng diện rộng (WAN)

Hình dưới minh họa cấu trúc kết nối mạng diện rộng (WAN) của ngân hàng BB Bank với ba chi nhánh, sử dụng giao thức định tuyến OSPF (Open Shortest Path First) trong cấu hình Area 0.



Hình 10

4.3.2 Chi tiết thiết kế

- **OSPF Area 0 (Backbone Area):**

- Các router trong khu vực này là một phần của Area 0, khu vực backbone trong môi trường mạng OSPF.
- Các địa điểm khác (ví dụ: các chi nhánh và khu vực bên ngoài) trong mạng phải kết nối với Area 0, đảm bảo việc truyền tải tuyến (route propagation) OSPF và khả năng giao tiếp hiệu quả giữa các khu vực.

- **Router-PT HCM Gateway:**

- Hoạt động như một gateway cho trụ sở chính và là router trung tâm kết nối tất cả các router chi nhánh.
- Là điểm kết nối với các mạng khác, như Internet, khu vực DMZ. Trong sơ đồ, các chi nhánh Đà Nẵng và Hà Nội kết nối với mạng bên ngoài hoặc Internet thông qua liên kết này (hiển thị bên trái sơ đồ).
- Gateway này kết nối với các router chính của mỗi chi nhánh thông qua đường truyền thuê riêng, đảm bảo kết nối quan trọng và tải trọng.

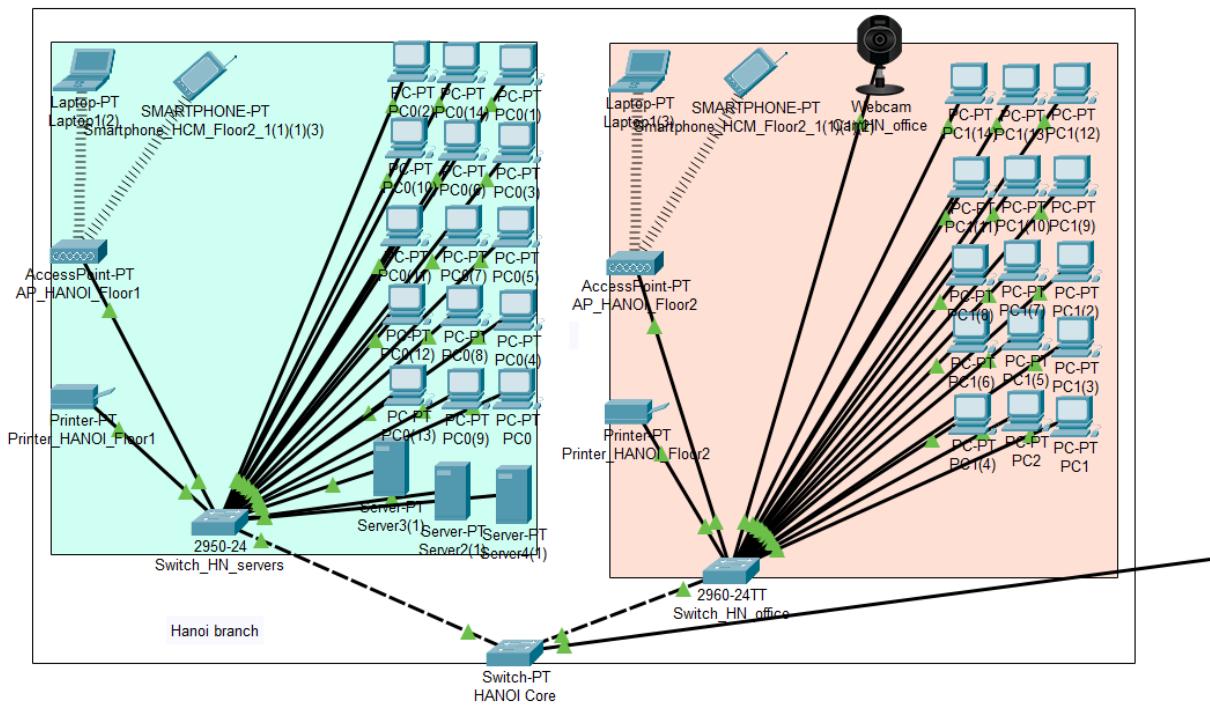
- **Router-PT HQ/HANOI/DANANG:**

- Là các router chính cho mỗi chi nhánh, đóng vai trò cầu nối giữa mạng nội bộ và các trang web bên ngoài.
- Mỗi router kết nối với mạng nội bộ của chi nhánh qua cáp đồng thẳng (Copper Straight-Through).

4.3.3 Kết nối giữa các phòng ban

Nằm giữa các router chính và các thiết bị đầu cuối trong mạng nội bộ của tất cả các chi nhánh là ba **Core Switch**. Các thiết kế chi nhánh cụ thể như sau:

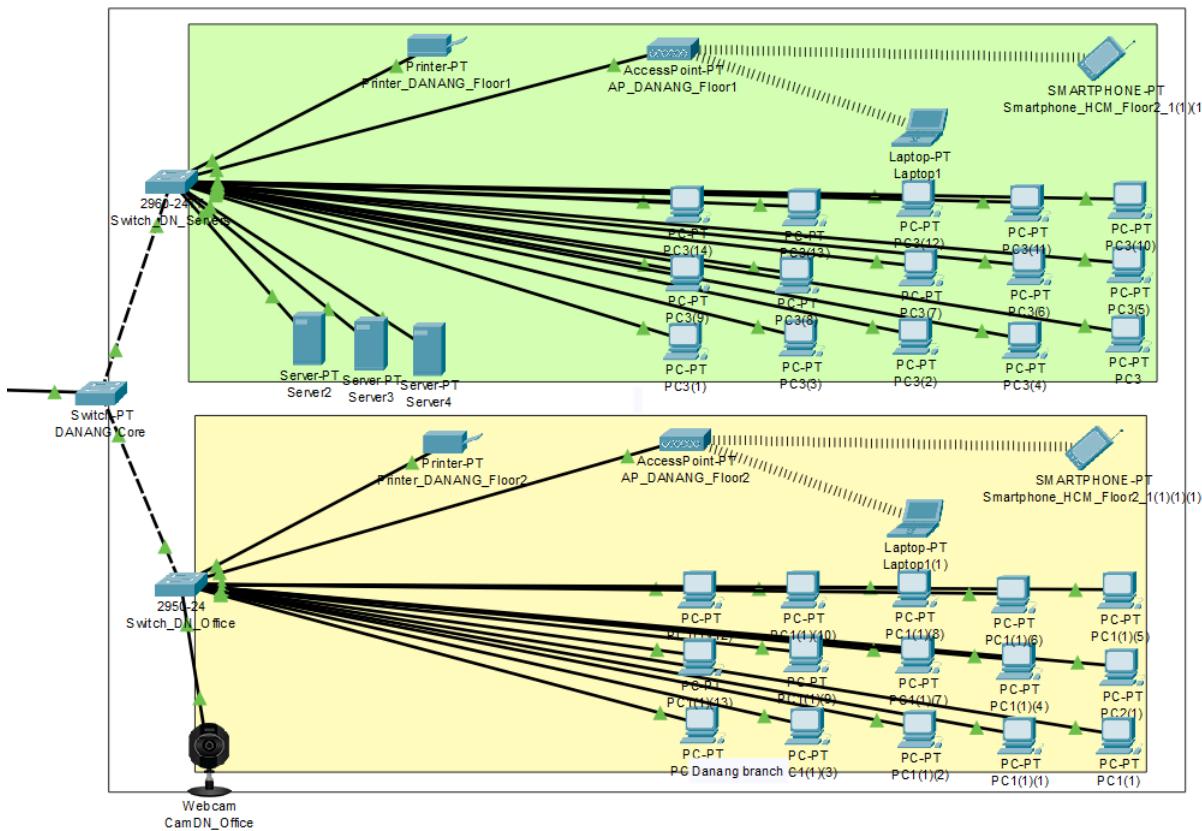
Hình dưới mô tả thiết kế mạng của chi nhánh Hà Nội.



Hình 11: Chi nhánh Hà Nội

- **Switch-PT HANOI Core:** Kết nối với các switch tầng và thiết bị mạng.
- **Switch 2950-24TT:** Kết nối với hai máy trạm (PC0, PC1) và một webcam giám sát (Camera N1).
- **Server-PT (Server1, Server4):** Đóng vai trò xử lý và lưu trữ dữ liệu.

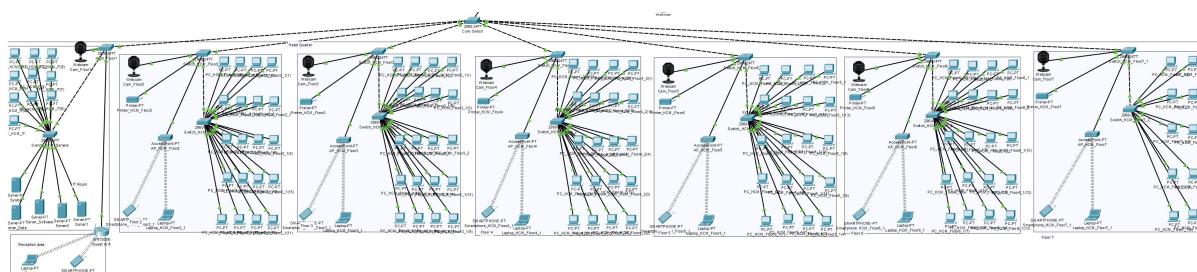
Hình này mô tả thiết kế mạng của chi nhánh Đà Nẵng.



Hình 12: Chi nhánh Đà Nẵng

- **Switch-PT DANANG Core:** Điều phối kết nối giữa các thiết bị.
- **Switch 2960-24TT:** Kết nối với hai máy trạm (PC0, PC1) và một webcam giám sát (Camera N1).
- **Server-PT (Server2, Server3, Server4):** Quản lý lưu trữ và hoạt động mạng cục bộ.

Hình này mô tả thiết kế mạng của chi nhánh Hồ Chí Minh.



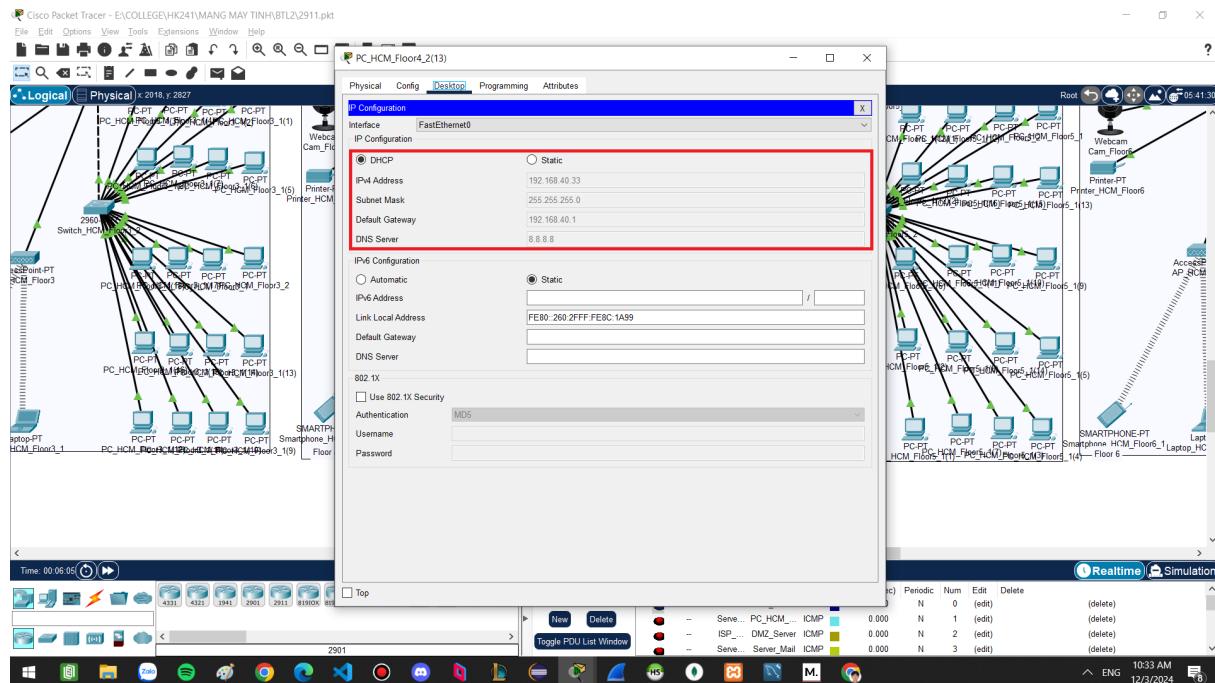
Hình 13: Trụ sở chính Thành phố Hồ Chí Minh

Trong kiến trúc này, Core Switch đóng vai trò trung tâm cho mạng của mỗi chi nhánh. Nó chịu trách nhiệm định tuyến và chuyển đổi lưu lượng mạng để đảm bảo kết nối liên tục qua các phòng ban và dịch vụ.

- Mỗi tầng hoặc phòng ban trong chi nhánh có switch truy cập riêng, kết nối về Core Switch trung tâm để tạo ra **mạng hình sao (Star Topology)**.
- **VLANs:**

- Trải dài trên nhiều switch bằng các liên kết trunk.
- Các liên kết trunk truyền tải lưu lượng từ tất cả VLANs giữa các switch, cho phép các thiết bị trên các VLAN khác nhau (ví dụ: máy trạm từ các tầng/phòng ban khác nhau) giao tiếp qua thiết bị lớp 3.

Hình này mô tả cách các thiết bị sử dụng DHCP để nhận địa chỉ IP.



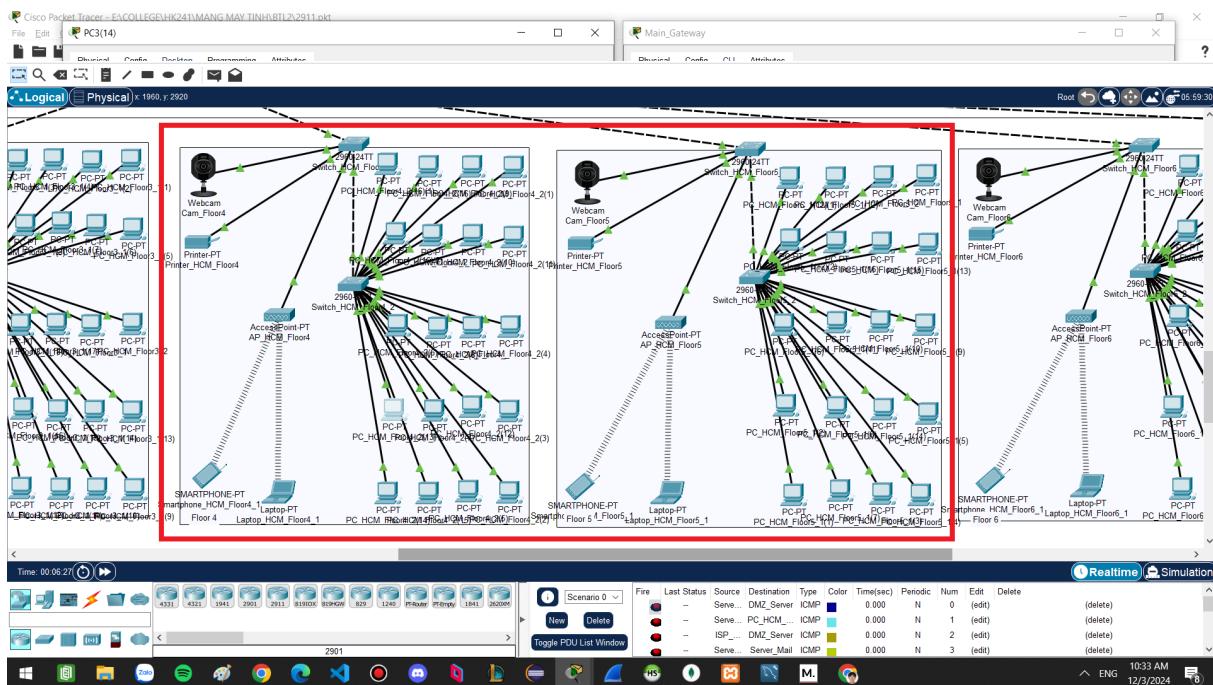
Hình 14

Cáu hình được thiết lập để cho phép từng thiết bị nhận địa chỉ IP thông qua DHCP. Ví dụ:

- Thiết bị thuộc VLAN 40 (trong hình là tầng 4) nhận địa chỉ IP là 192.168.40.33 cùng subnet mask và gateway tương ứng.
- Một số thiết bị như **IP Camera** và **Server** được cấp địa chỉ IP cố định để đảm bảo truy cập ổn định.

4.3.4 Kết nối giữa các thiết bị trong cùng phòng ban

Hình này minh họa cách các thiết bị đầu cuối được kết nối với switch theo tầng.



Hình 15

Trong thiết kế, các thiết bị đầu cuối trên mỗi tầng hoặc trong cùng một phòng ban được kết nối với **switch theo tầng**. Điều này cho phép các thiết bị giao tiếp trực tiếp với nhau.

- **Switch tầng (Floor-Level Switch):**

- Kết nối các thiết bị như PC, Laptop, máy in, smartphone và camera giám sát.
- Tạo liên kết trực tiếp giữa các thiết bị nội bộ trên cùng tầng.

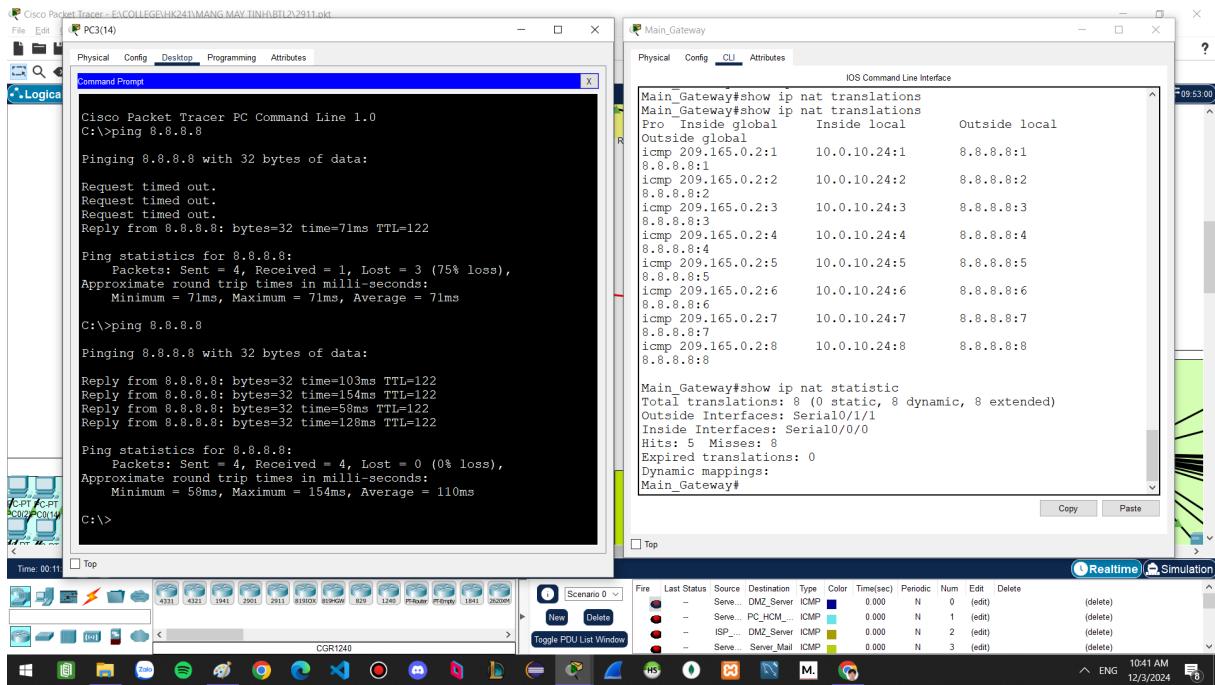
- **Thiết bị đầu cuối:**

- PC, Laptop, smartphone, webcam, và máy in đảm bảo các chức năng văn phòng cơ bản.
- Các điểm truy cập (Access Point) cung cấp mạng không dây cho smartphone và Laptop.

4.3.5 Kết nối giữa LAN và Internet

Trong thiết kế này, các địa chỉ IP nội bộ đã được dịch sang **địa chỉ IP công cộng**. Ví dụ:

- **PC 14** trên tầng 2 của chi nhánh Đà Nẵng có địa chỉ IP 10.0.10.24.
- Địa chỉ này được dịch sang địa chỉ IP công cộng 209.165.0.2 (địa chỉ IP toàn cầu trên giao diện bên ngoài Serial0/1/1 của Gateway chính).



Hình 16

4.3.6 VLAN Segmentation

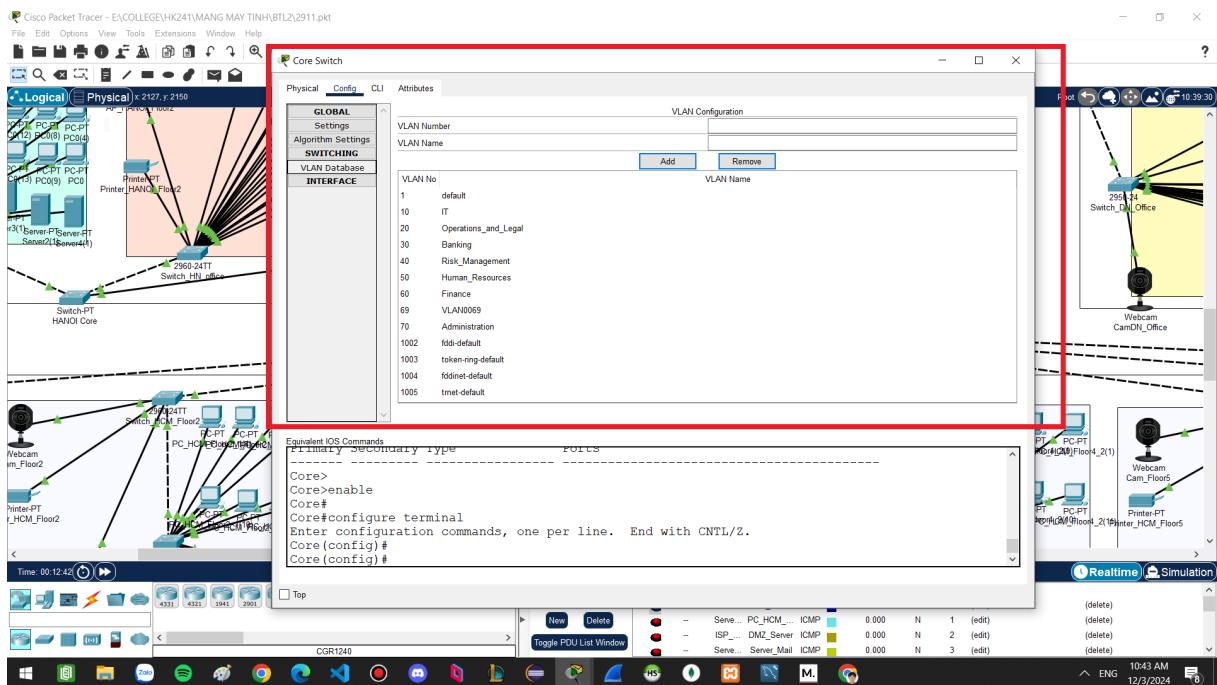
Mục này tập trung giải thích cấu hình VLAN tại chi nhánh HCM, vì đây là chi nhánh phức tạp nhất. Các chi nhánh tại Hà Nội và Đà Nẵng có cấu hình tương tự nhưng quy mô nhỏ hơn.

Phân đoạn VLAN

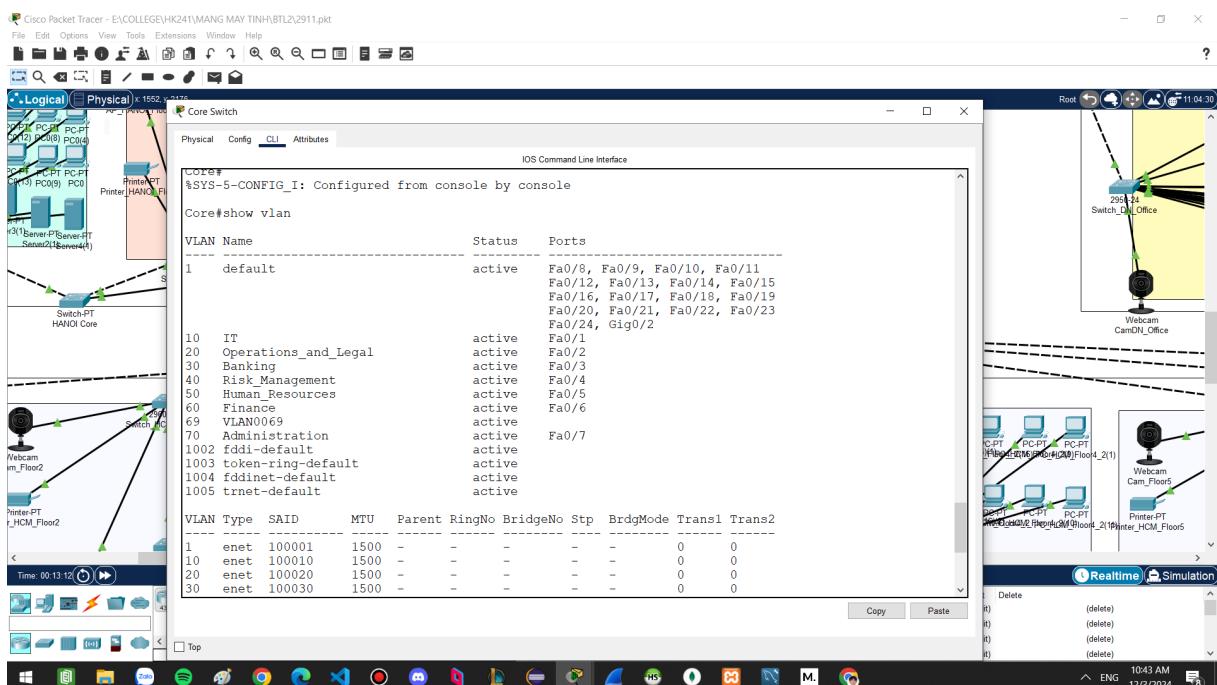
- Mạng được chia logic thành nhiều **VLANs**, cách ly các máy chủ quan trọng, nhóm người dùng, và lưu lượng khách.
- Phân đoạn này giúp tăng cường bảo mật và quản lý lưu lượng mạng.
- Định tuyến liên VLAN (Inter-VLAN Routing)** được xử lý bởi các switch lớp 3 (core switches) để tối ưu hóa luồng dữ liệu.

Cấu hình Core Switch

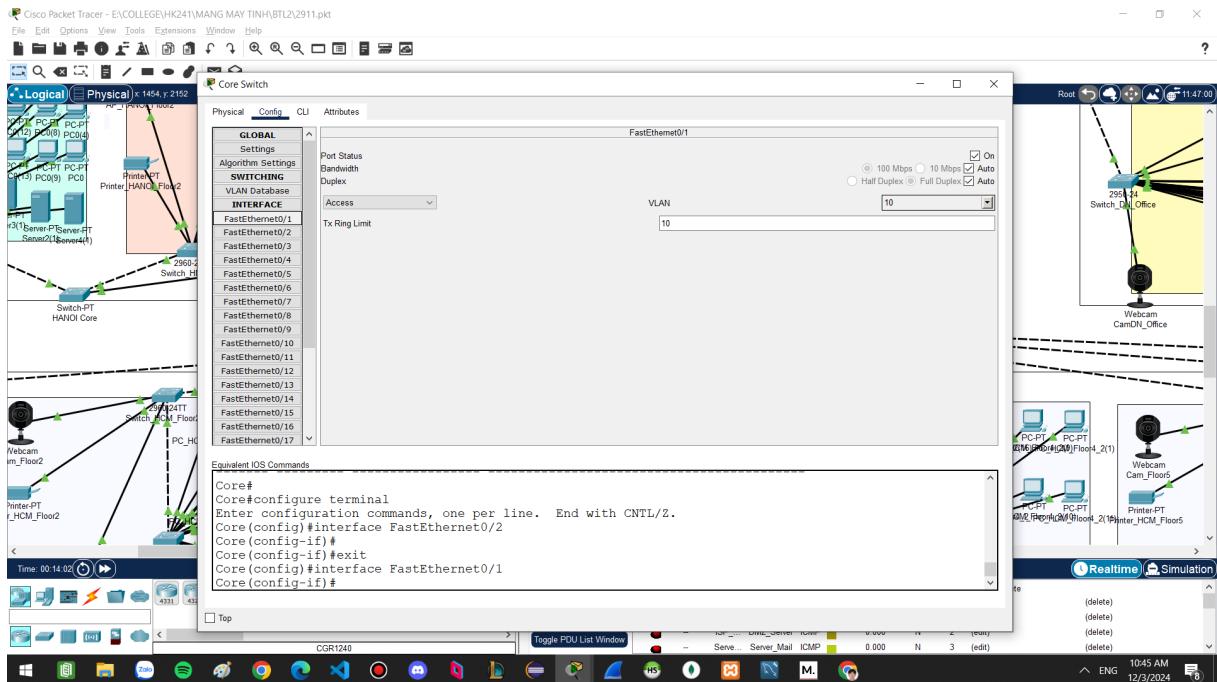
- Core switch được cấu hình để bao gồm các VLAN khác nhau, như đã được mô tả trong thiết kế ở mục 3.4.2.
- Các switch từ từng phòng ban được kết nối với các cổng khác nhau trên core switch.
- Các cổng trên core switch được gán vào các VLAN tương ứng để đảm bảo sự phân đoạn logic trong hệ thống.



Hình 17



Hình 18

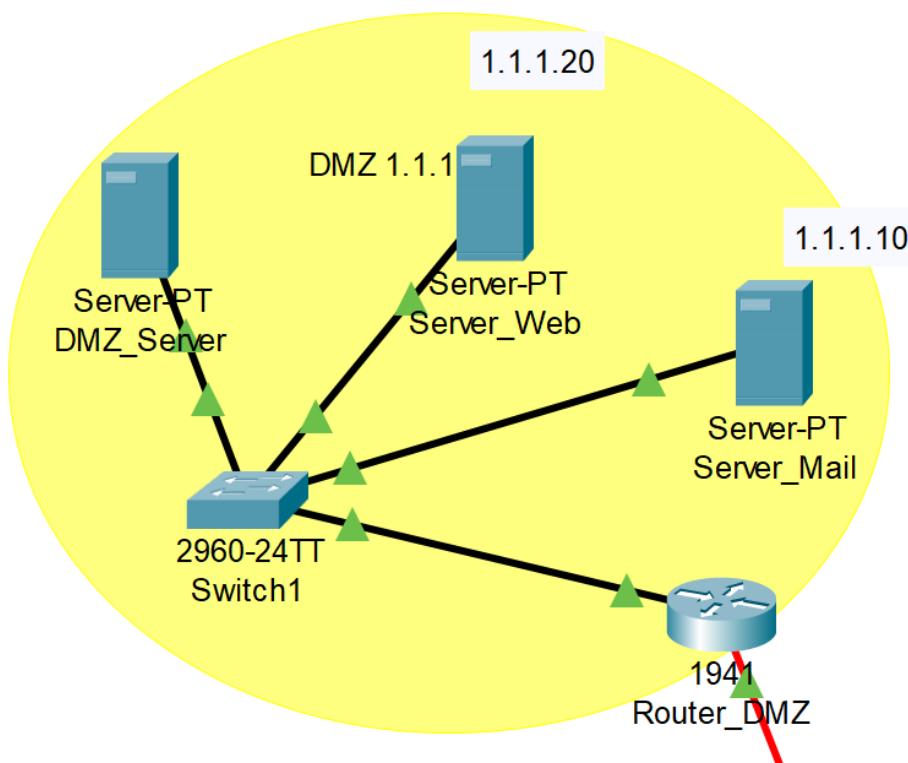


Hình 19

4.3.7 Bảo mật

Hệ thống mạng nhóm em được chia thành 3 vùng chính: **Internal (Mạng nội bộ)**, **DMZ (Demilitarized Zone)**, và **External (Internet)**. Việc phân chia này nhằm mục đích kiểm soát truy cập, đảm bảo an toàn cho tài nguyên nội bộ, và cung cấp dịch vụ công khai một cách an toàn thông qua các cơ chế bảo mật sau:

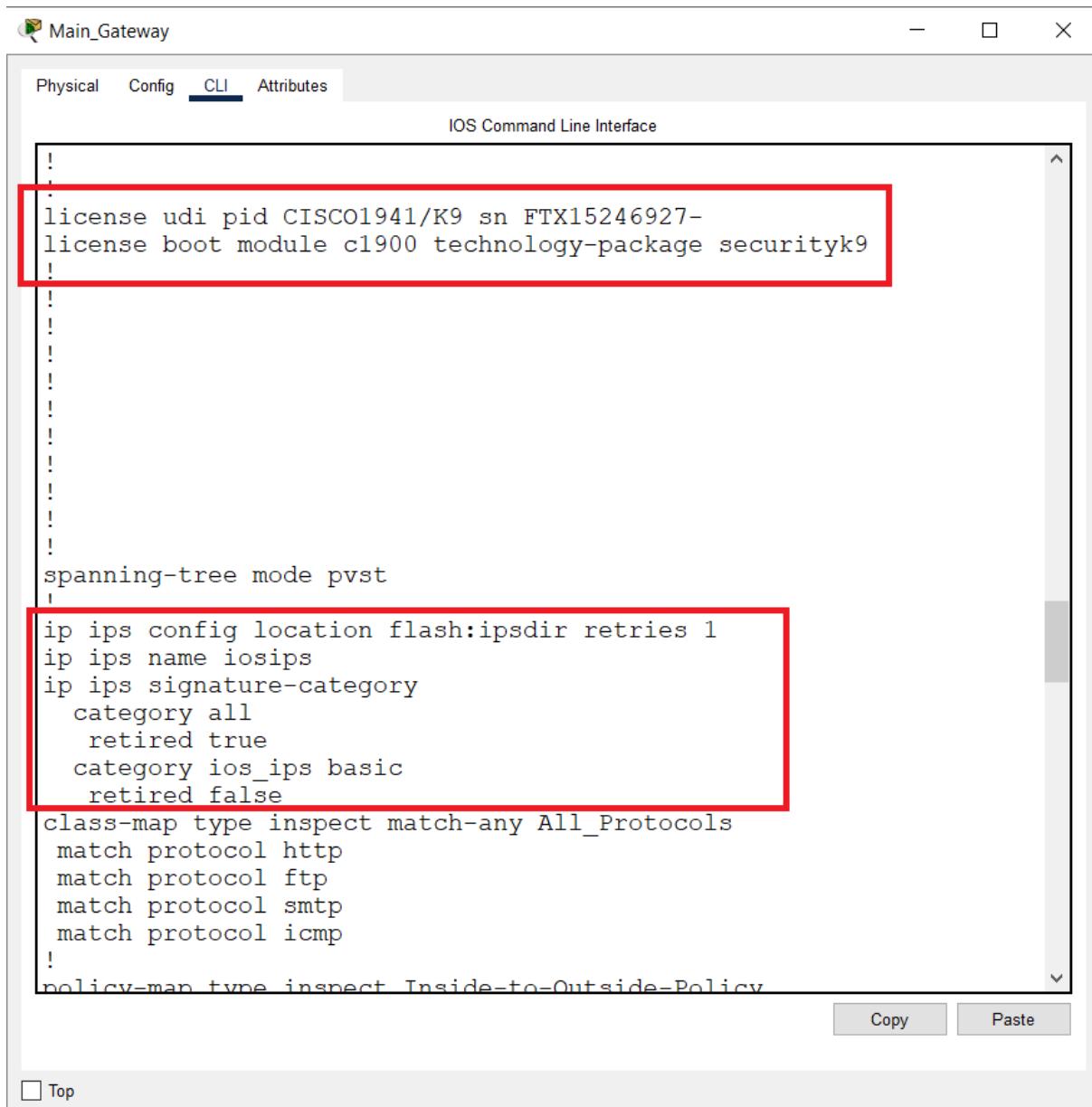
- **DMZ (Demilitarized Zone)**
 - DMZ là vùng mạng cách ly, nơi đặt các server công khai như **Web Server** và **Mail Server**.
 - DMZ được tách biệt với mạng nội bộ và Internet thông qua **Firewall** trên router Main Gateway.
 - Các server trong DMZ sử dụng địa chỉ IP riêng và chỉ có thể giao tiếp với Internet qua các quy tắc được định nghĩa rõ ràng bên trong router Main Gateway



Hình 20: DMZ (Demilitarized Zone)

- Firewall
 - Router Main Gateway được cấu hình như một **Zone-Based Firewall (ZBF)** để kiểm soát lưu lượng giữa các vùng:
 - * **Inside (Internal)**: Bảo vệ tài nguyên nội bộ.
 - * **DMZ**: Cách ly các server công khai.
 - * **Outside (Internet)**: Quản lý truy cập từ bên ngoài.
- IPS (Intrusion Prevention System)
 - **IPS (Intrusion Prevention System)** được kích hoạt trên router Main Gateway để phát hiện và chặn các hành vi bất thường hoặc tấn công mạng.
 - IPS hoạt động trên giao diện kết nối giữa Internal và External, giám sát các gói tin đến và đi:
 - * Chặn các cuộc tấn công dựa trên chữ ký (*signature*). Ở đây nhóm sử dụng gói chữ ký cơ bản sau khi kích hoạt gói Security K9. Các kết nối bị chặn sẽ được ghi nhận và Syslog Server có tích hợp trong Router.
 - * Ngăn chặn các hành vi nguy hiểm, như **ICMP Flood** hoặc **Port Scanning**.
- ACL (Access Control List)
 - **Access Control List (ACL)** được áp dụng để kiểm soát chi tiết lưu lượng truy cập:
 - * **Chặn** các giao thức không cần thiết từ Internet vào Internal.
 - * **Cho phép** các dịch vụ như HTTP, HTTPS, SMTP từ Internet vào DMZ.

- * **Hạn chế ICMP** (ping) để tránh tấn công quét mạng.
- Chính sách bảo mật trong Zone-Based Firewall
 - Các **policy-map** được cấu hình trong router Main Gateway để kiểm tra lưu lượng giữa các vùng
- Các hình dưới đây là cấu hình bảo mật của Router Main Gateway, bao gồm các kết nối đến Internal, DMZ, và External



The screenshot shows the Cisco IOS CLI interface for a router named 'Main_Gateway'. The 'CLI' tab is selected. The configuration text is as follows:

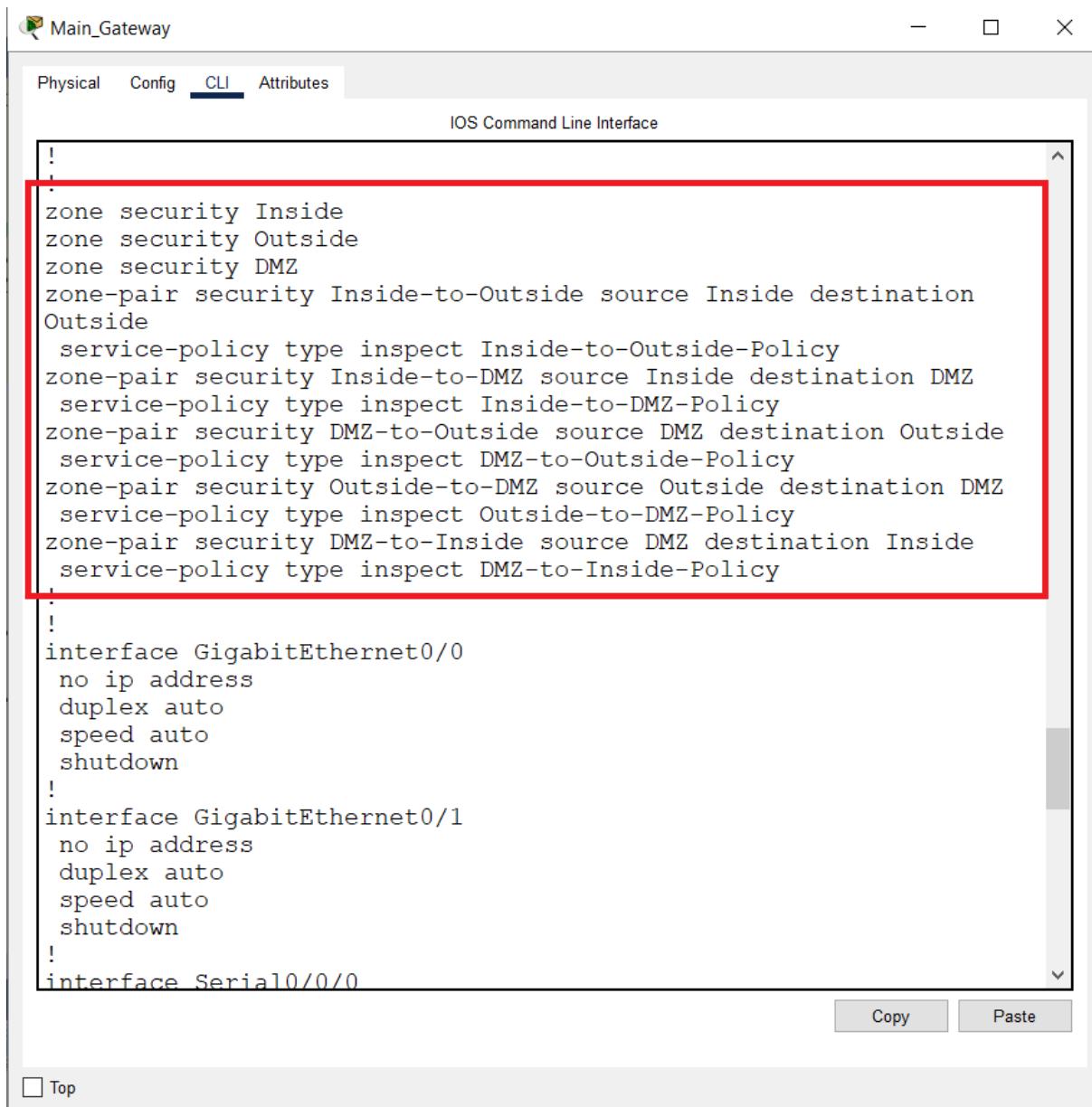
```
!
license udi pid CISCO1941/K9 sn FTX15246927-
license boot module c1900 technology-package securityk9
!
spanning-tree mode pvst
!
ip ips config location flash:ipsdir retries 1
ip ips name iosips
ip ips signature-category
  category all
    retired true
  category ios_ips basic
    retired false
class-map type inspect match-any All_Proocols
  match protocol http
  match protocol ftp
  match protocol smtp
  match protocol icmp
!
policy-map type inspect Inside-to-Outside-Policy
```

Two specific sections of the configuration are highlighted with red boxes:

- The first red box highlights the 'ip ips' configuration block, which includes the command 'ip ips name iosips'.
- The second red box highlights the 'class-map' block, which includes the 'match protocol icmp' line.

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons, and a 'Top' button.

Hình 21: IPS được kích hoạt

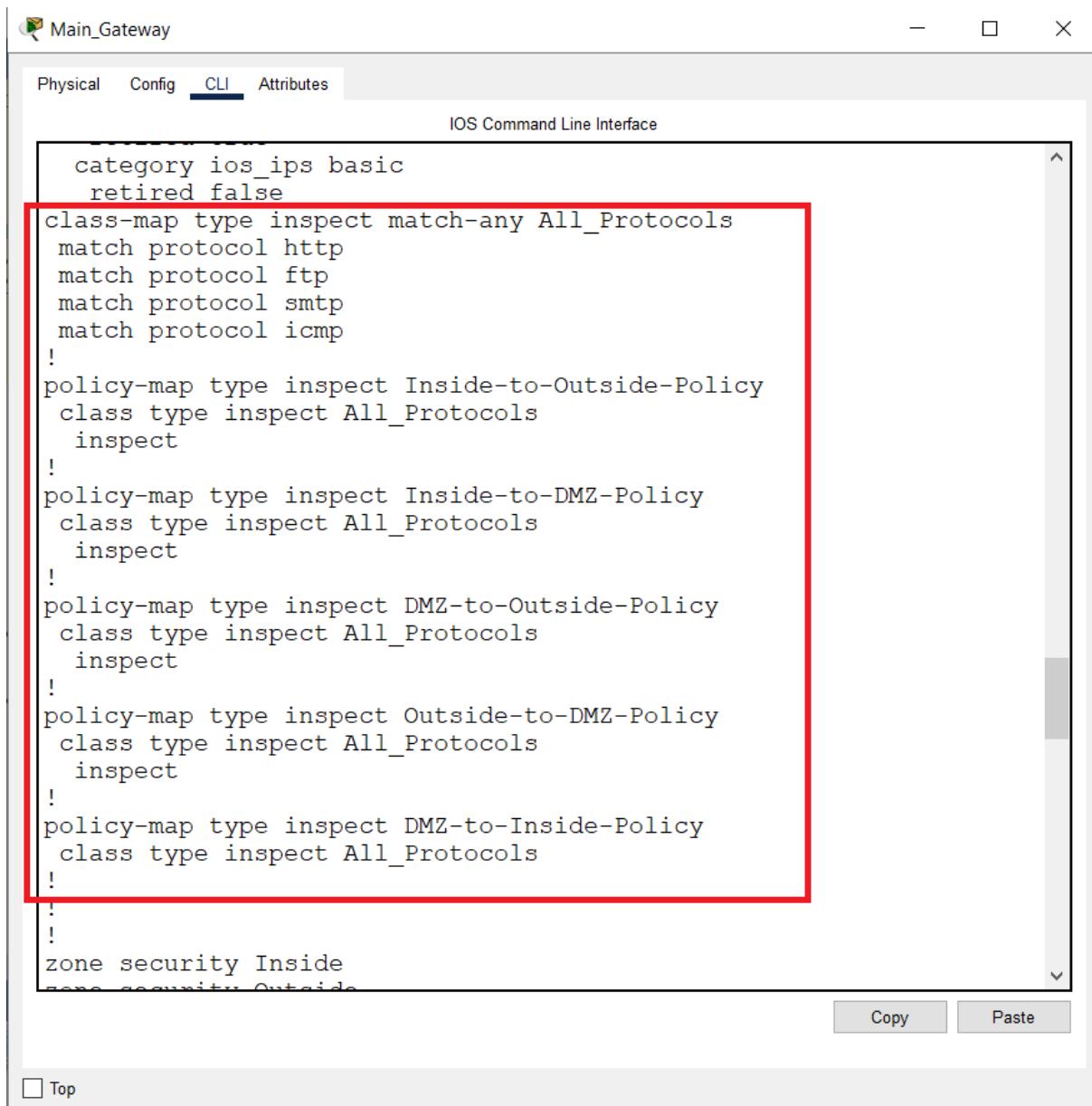


! zone security Inside zone security Outside zone security DMZ zone-pair security Inside-to-Outside source Inside destination Outside service-policy type inspect Inside-to-Outside-Policy zone-pair security Inside-to-DMZ source Inside destination DMZ service-policy type inspect Inside-to-DMZ-Policy zone-pair security DMZ-to-Outside source DMZ destination Outside service-policy type inspect DMZ-to-Outside-Policy zone-pair security Outside-to-DMZ source Outside destination DMZ service-policy type inspect Outside-to-DMZ-Policy zone-pair security DMZ-to-Inside source DMZ destination Inside service-policy type inspect DMZ-to-Inside-Policy ! interface GigabitEthernet0/0 no ip address duplex auto speed auto shutdown ! interface GigabitEthernet0/1 no ip address duplex auto speed auto shutdown ! interface Serial0/0/0

Top

Copy Paste

Hình 22: Các Zone được tạo

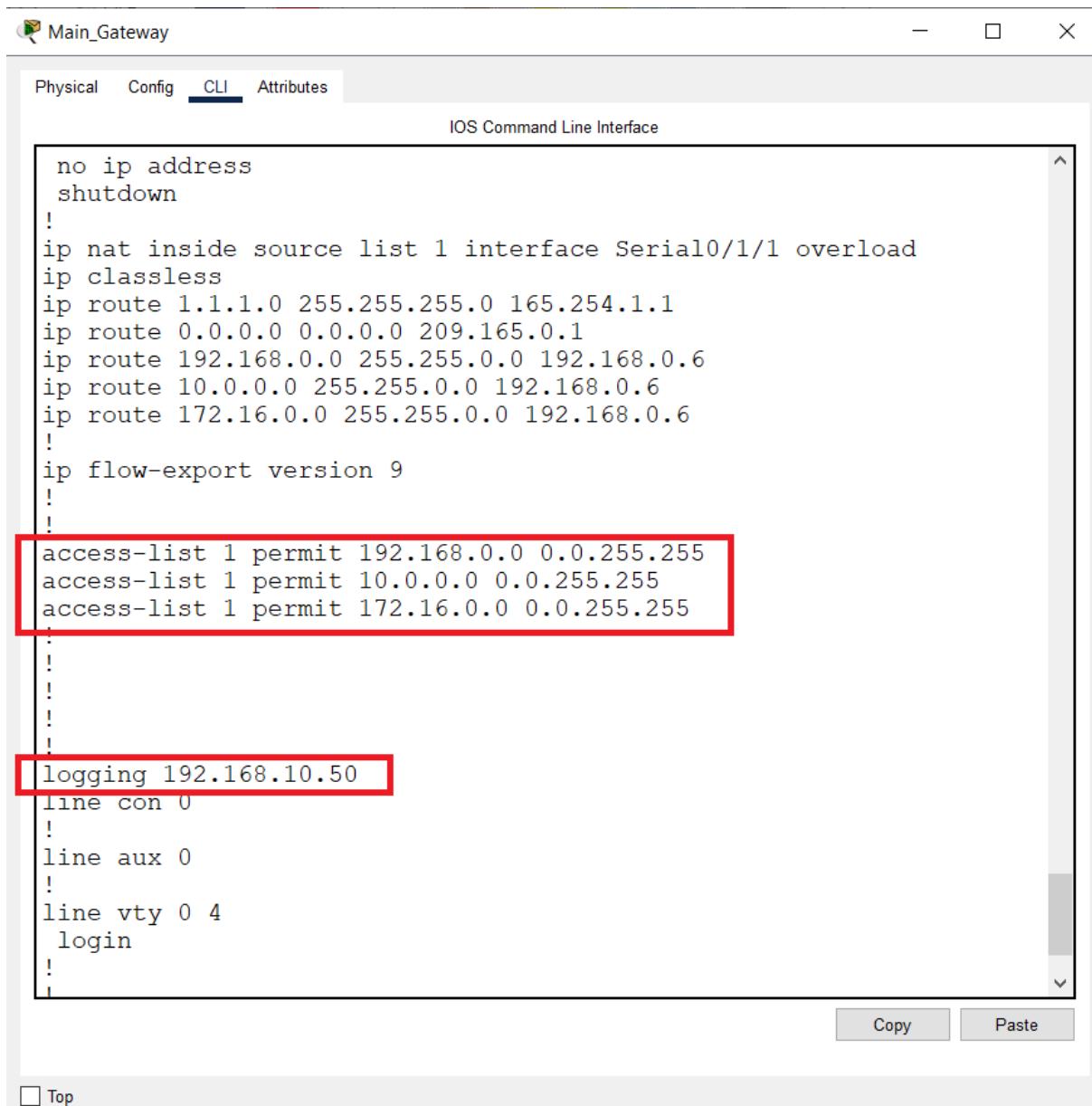


The screenshot shows the Cisco IOS Command Line Interface (CLI) for a device named 'Main_Gateway'. The 'CLI' tab is selected in the top navigation bar. The configuration text is as follows:

```
category ios_ip basic
  retired false
class-map type inspect match-any All_Protocols
  match protocol http
  match protocol ftp
  match protocol smtp
  match protocol icmp
!
policy-map type inspect Inside-to-Outside-Policy
  class type inspect All_Protocols
    inspect
!
policy-map type inspect Inside-to-DMZ-Policy
  class type inspect All_Protocols
    inspect
!
policy-map type inspect DMZ-to-Outside-Policy
  class type inspect All_Protocols
    inspect
!
policy-map type inspect Outside-to-DMZ-Policy
  class type inspect All_Protocols
    inspect
!
policy-map type inspect DMZ-to-Inside-Policy
  class type inspect All_Protocols
!
!
zone security Inside
zone security Outside
```

Below the configuration text, there are 'Copy' and 'Paste' buttons. At the bottom left, there is a 'Top' button.

Hình 23: Các Policy được tạo



```
no ip address
shutdown
!
ip nat inside source list 1 interface Serial0/1/1 overload
ip classless
ip route 1.1.1.0 255.255.255.0 165.254.1.1
ip route 0.0.0.0 0.0.0.0 209.165.0.1
ip route 192.168.0.0 255.255.0.0 192.168.0.6
ip route 10.0.0.0 255.255.0.0 192.168.0.6
ip route 172.16.0.0 255.255.0.0 192.168.0.6
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.0.255.255
access-list 1 permit 172.16.0.0 0.0.255.255
!
!
logging 192.168.10.50
line con 0
!
line aux 0
!
line vty 0 4
login
!
```

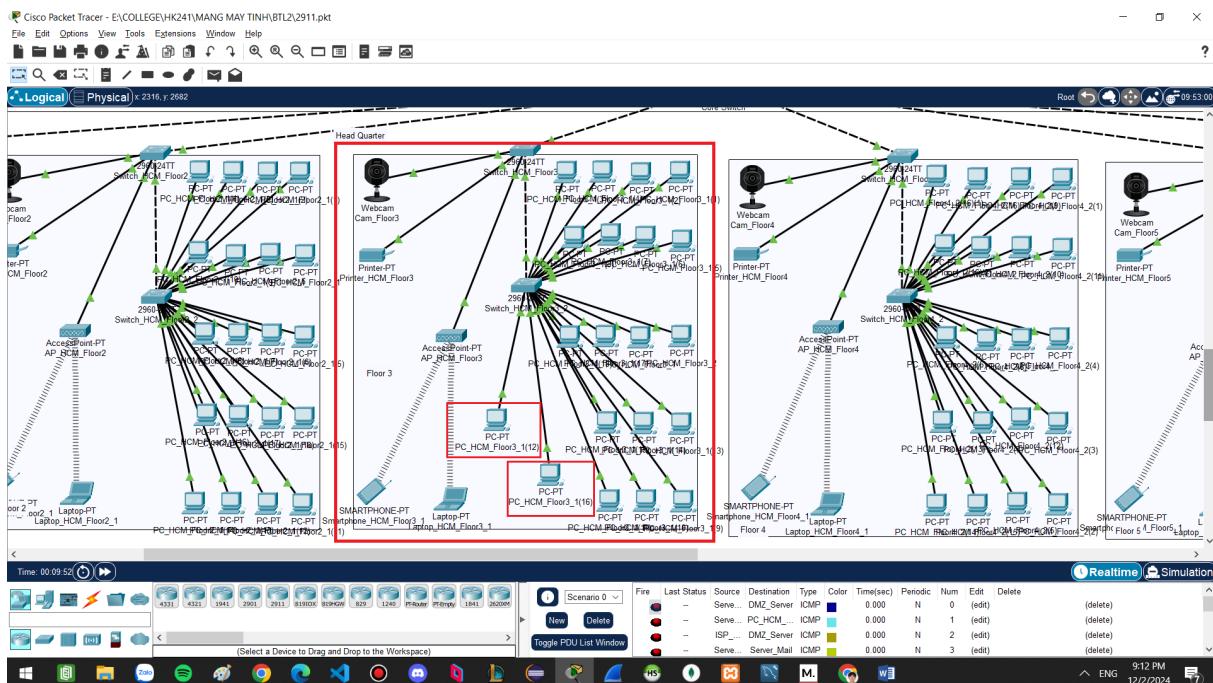
Hình 24: Các ACL được tạo

5 Kiểm tra kết nối mạng bằng Packet Tracer

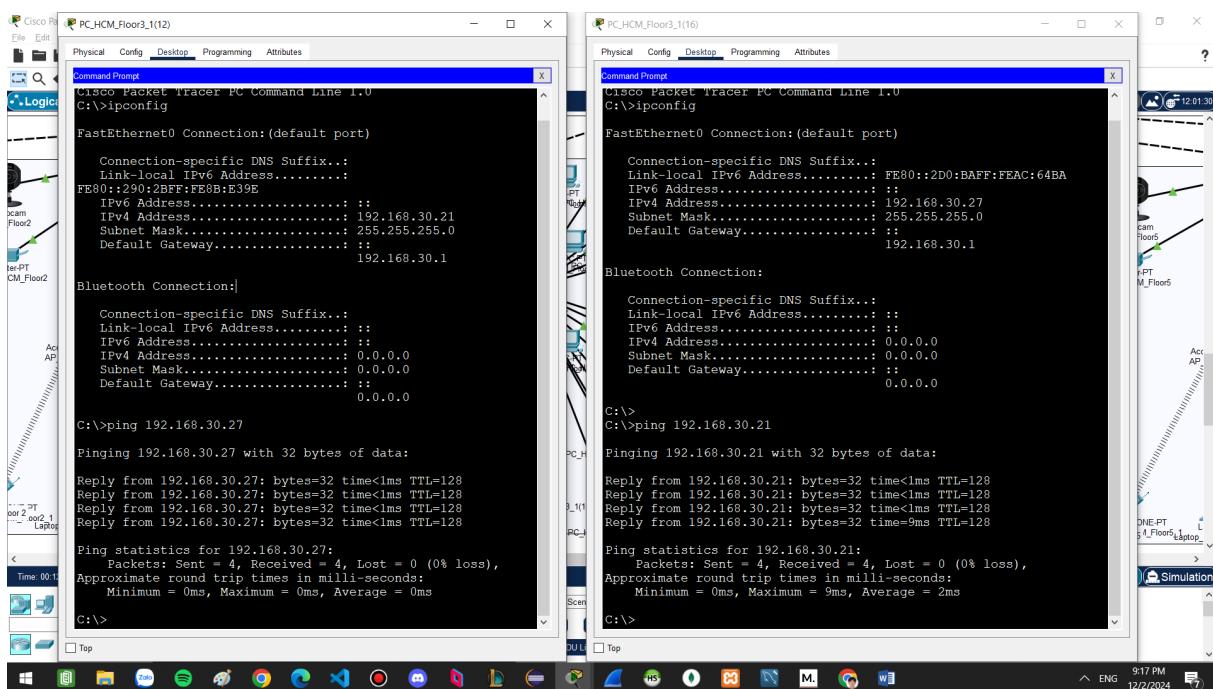
5.1 Kết nối giữa các PC trong cùng một VLAN

5.1.1 PC và PC

Kết nối được kiểm tra bằng lệnh Ping giữa PC_HCM_Floor3_1(12) (192.168.30.21) và PC_HCM_Floor3_1(16) (192.168.30.27)



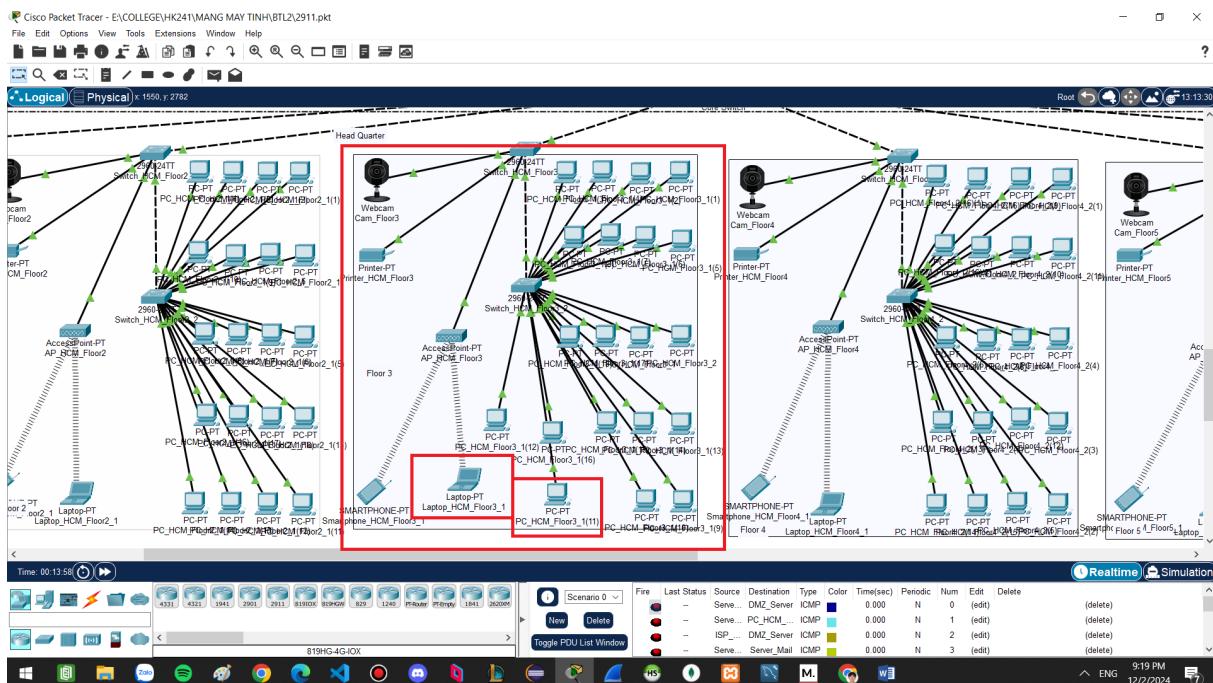
Hình 25



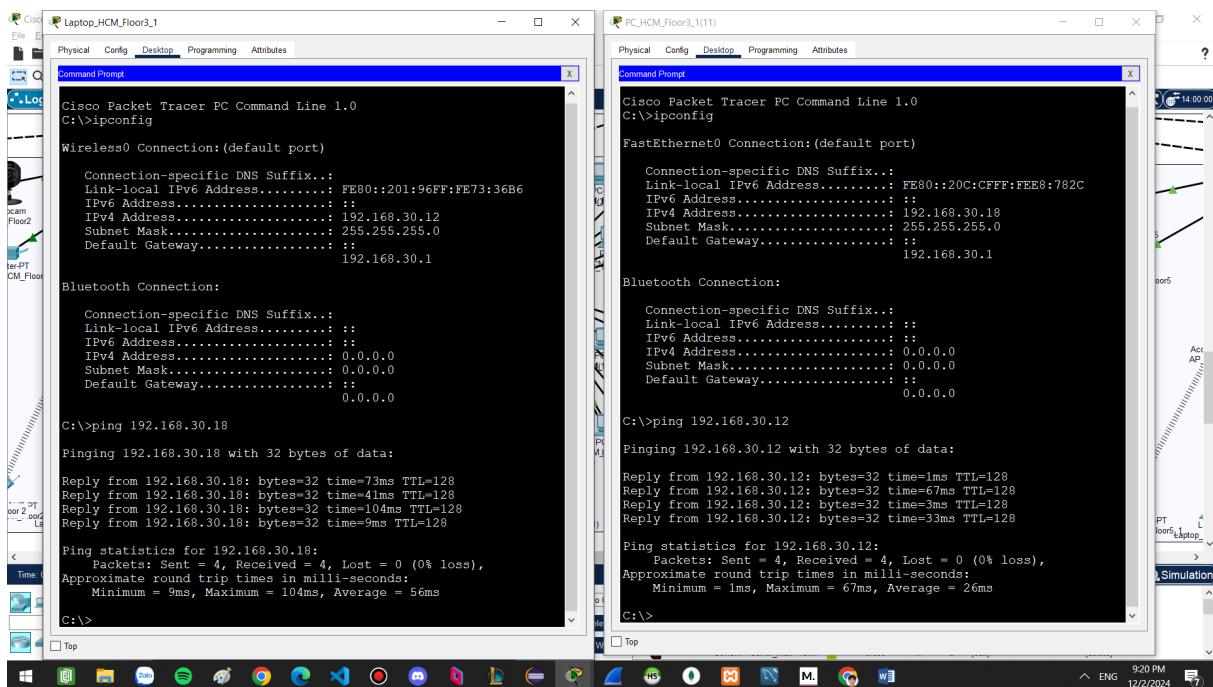
Hình 26

5.1.2 Laptop và PC

Kết nối được kiểm tra bằng lệnh Ping giữa Laptop_HCM_Floor3_1 (192.168.30.12) và PC_HCM_Floor3_1(11) (192.168.30.18)



Hình 27

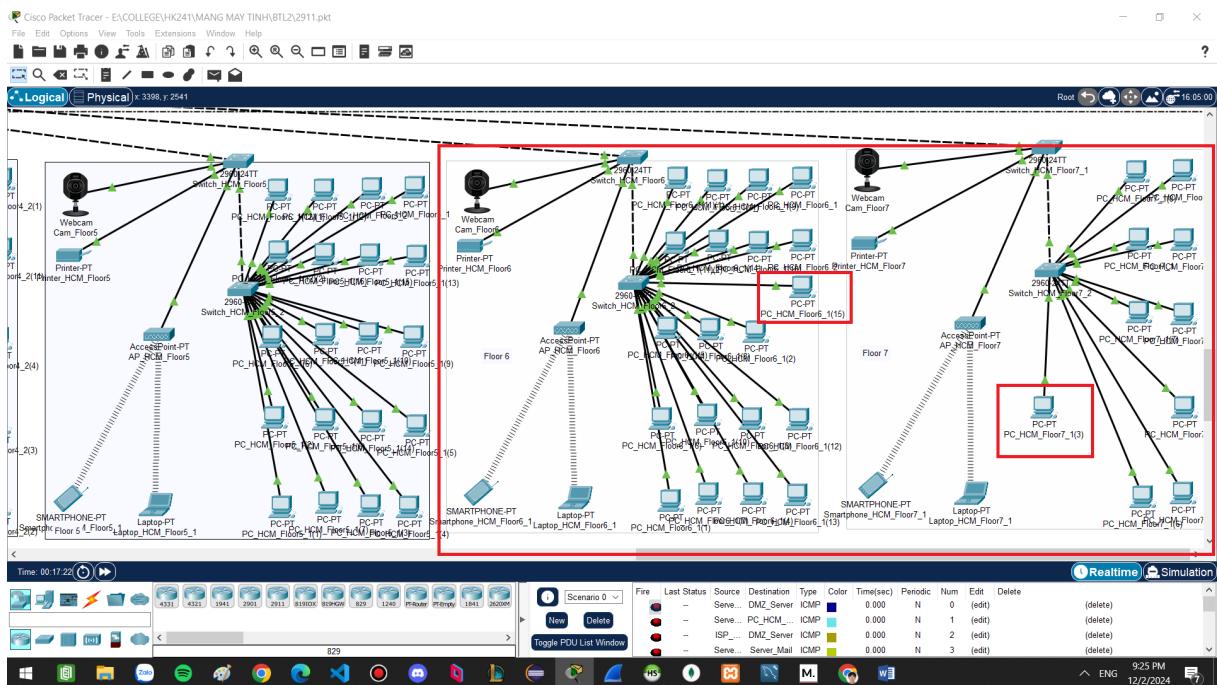


Hình 28

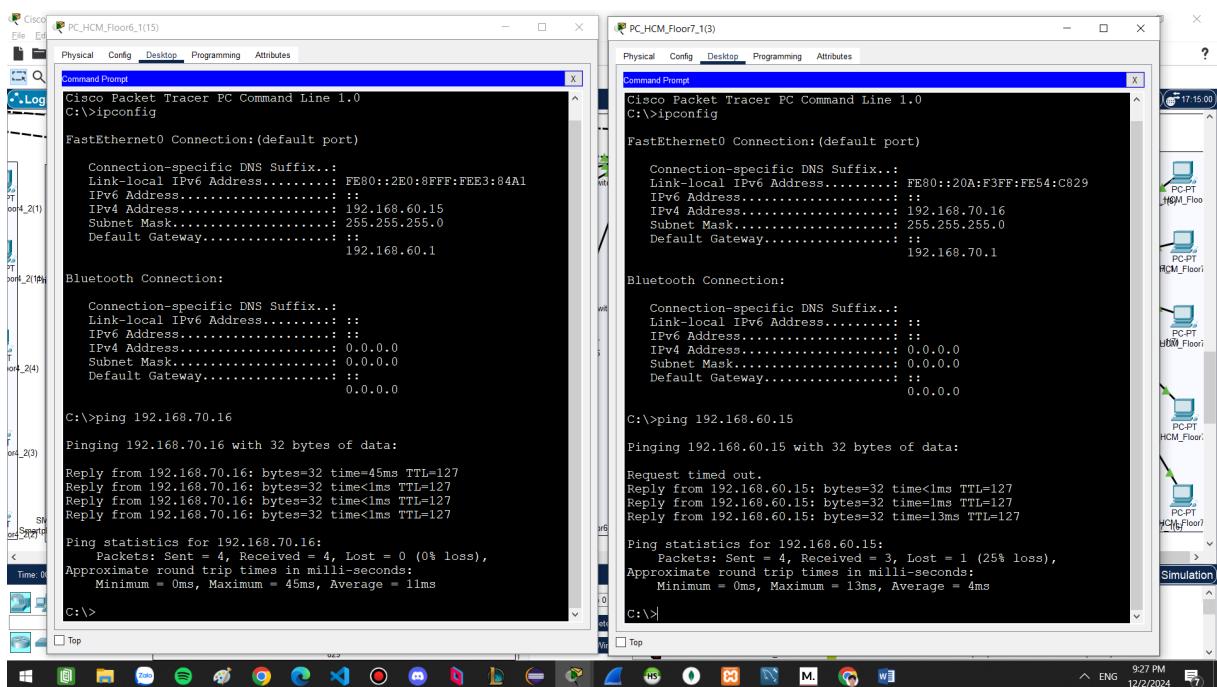
5.2 Kết nối giữa các PC khác VLAN

5.2.1 PC và PC

Kết nối được kiểm tra bằng lệnh Ping giữa PC_HCM_Floor6_1(15) (192.168.60.15) và PC_HCM_Floor7_1(3) (192.168.70.16)



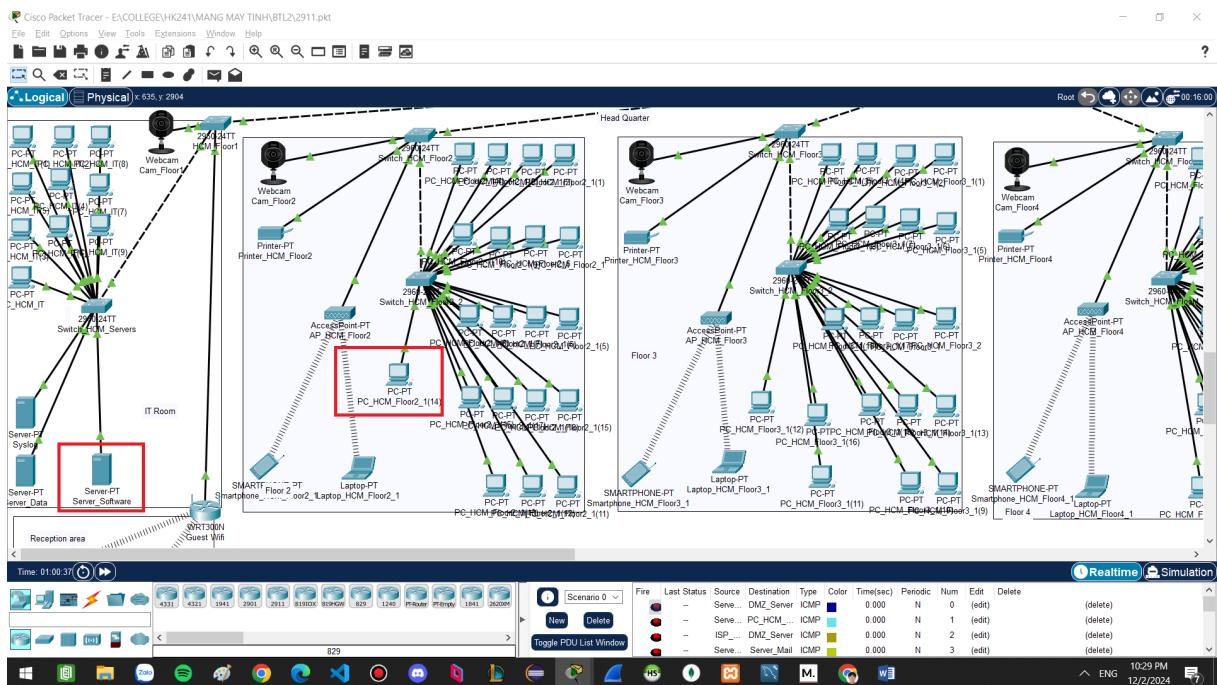
Hình 29



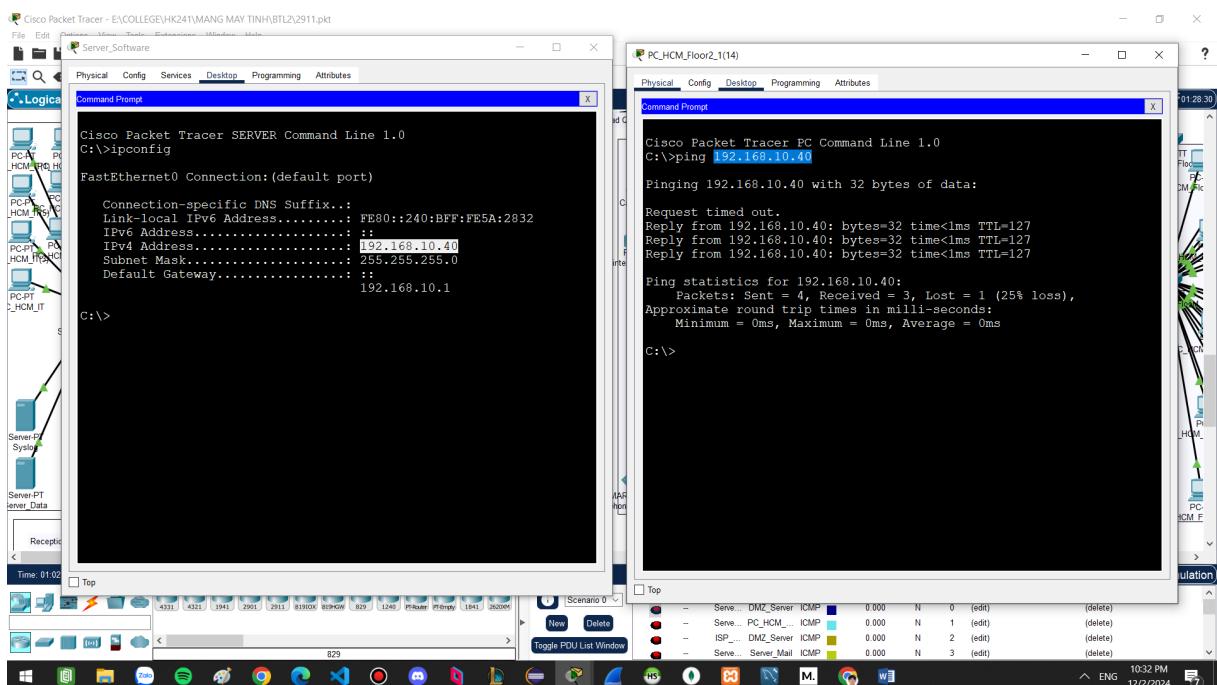
Hình 30

5.2.2 PC đến Server

Kết nối được kiểm tra bằng lệnh Ping giữa PC_HCM_Floor2_1(14) (192.168.20.24) và Server_Software (192.168.10.40)



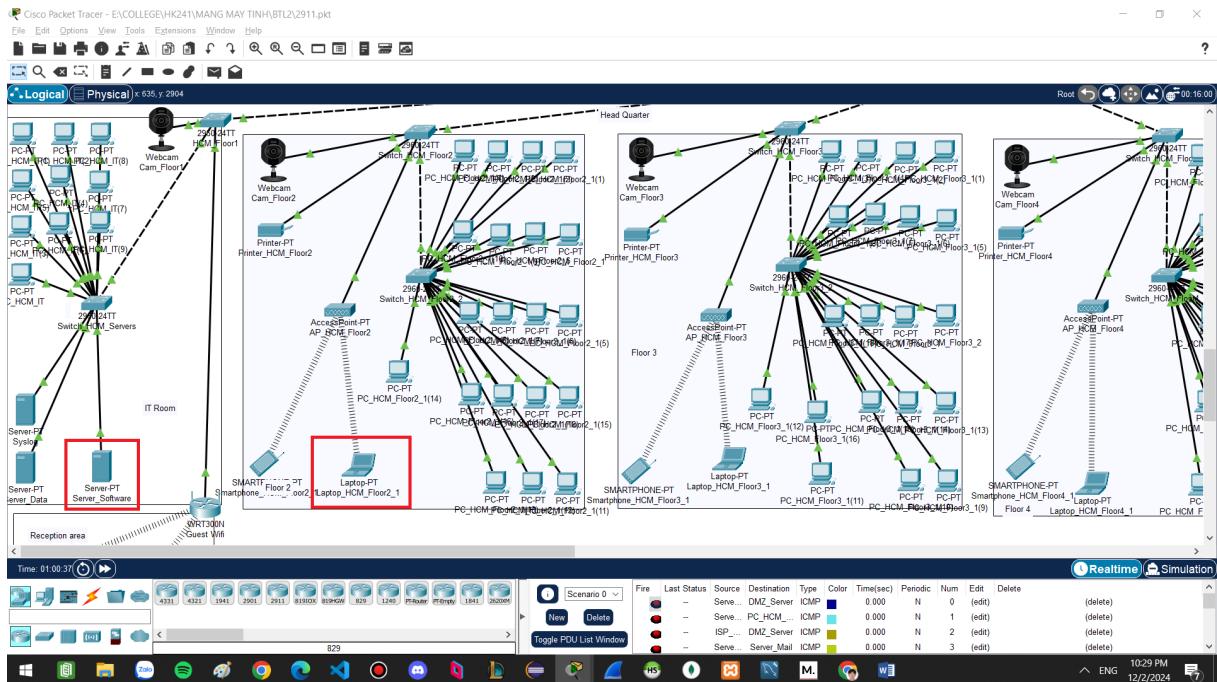
Hình 31



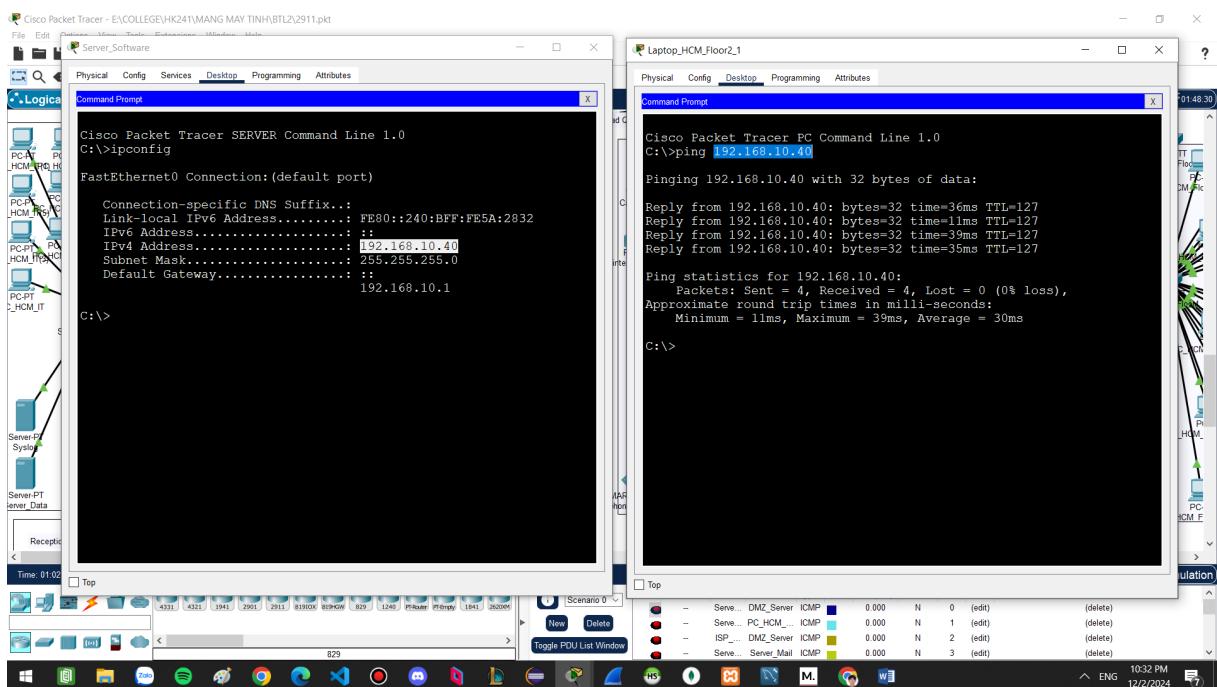
Hình 32

5.2.3 Laptop đến Server

Kết nối được kiểm tra bằng lệnh Ping giữa Laptop_HCM_Floor2_1 (192.168.20.12) và Server_Software (192.168.10.40)



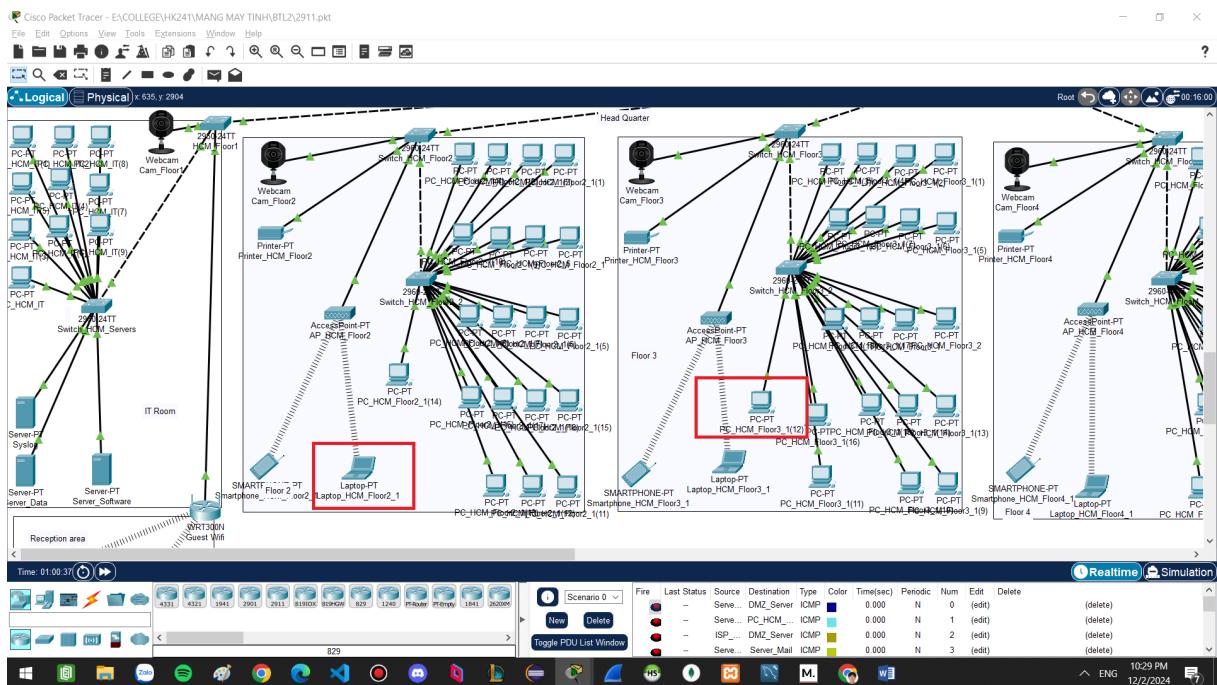
Hình 33



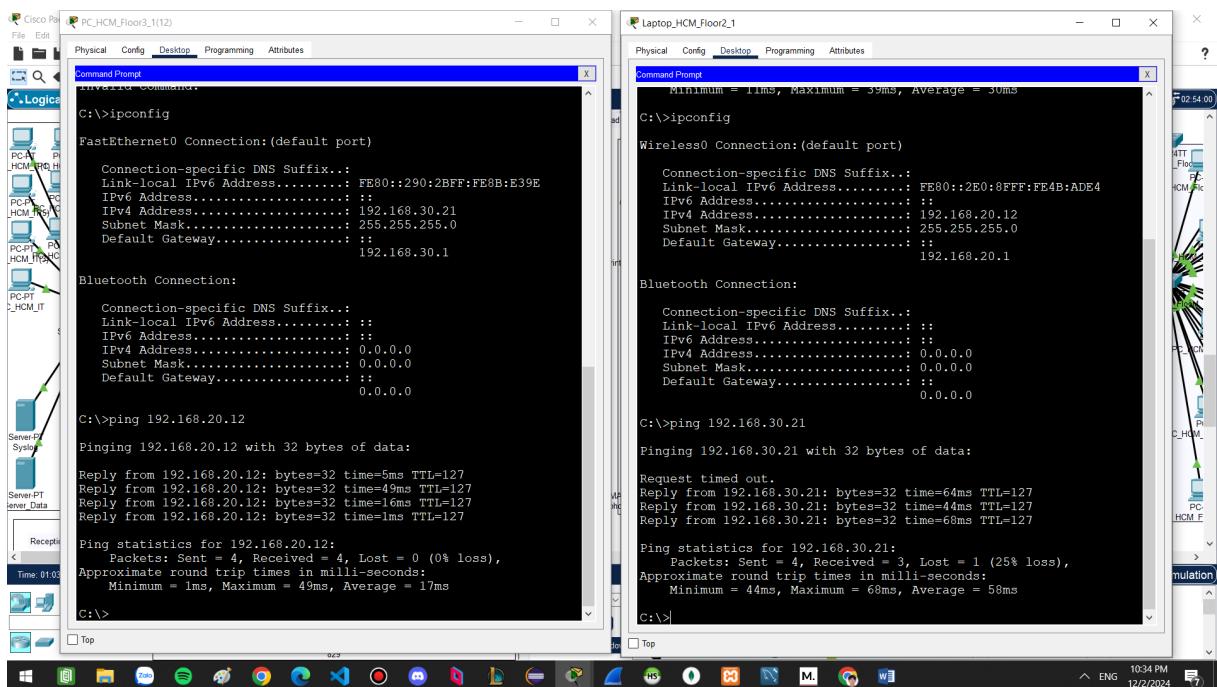
Hình 34

5.2.4 Laptop và PC

Kết nối được kiểm tra bằng lệnh Ping giữa Laptop_HCM_Floor2_1 (192.168.20.12) và PC_HCM_Floor3_1(12) (192.168.30.1)



Hình 35

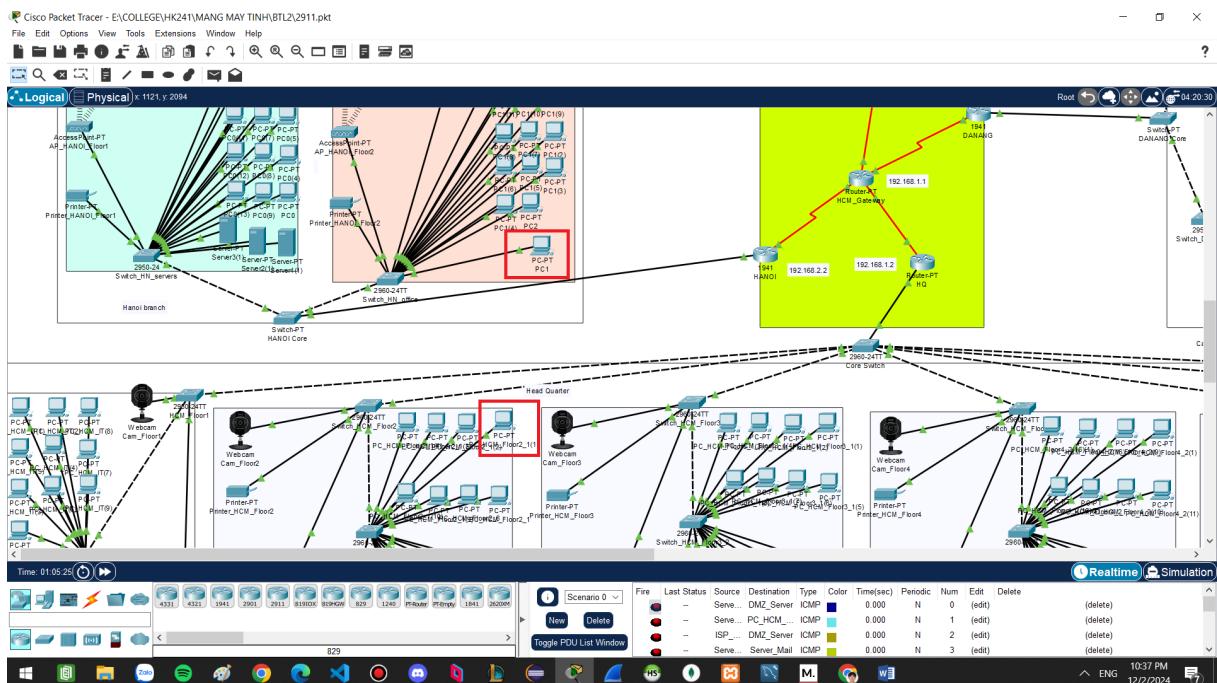


Hình 36

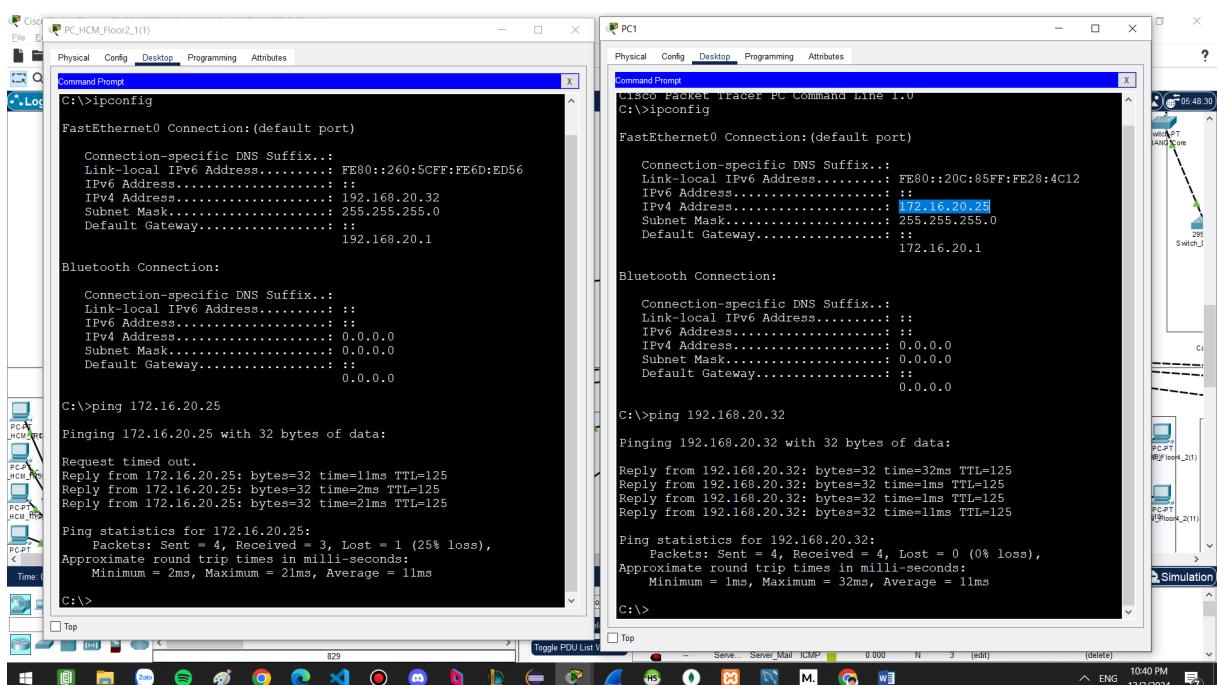
5.3 Kết nối giữa các PC ở trung tâm và chi nhánh

5.3.1 PC và PC

Kết nối được kiểm tra bằng lệnh Ping giữa PC_HCM_Floor2_1(1) (192.168.20.32) và PC1 (172.16.20.25)



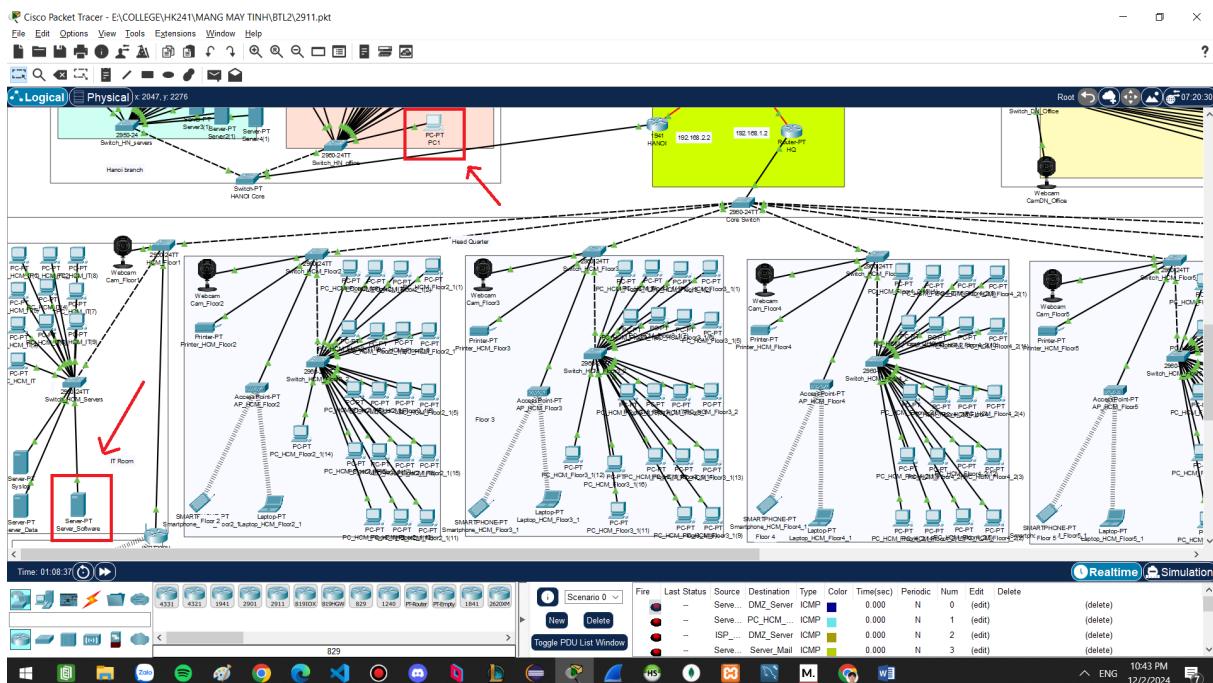
Hình 37



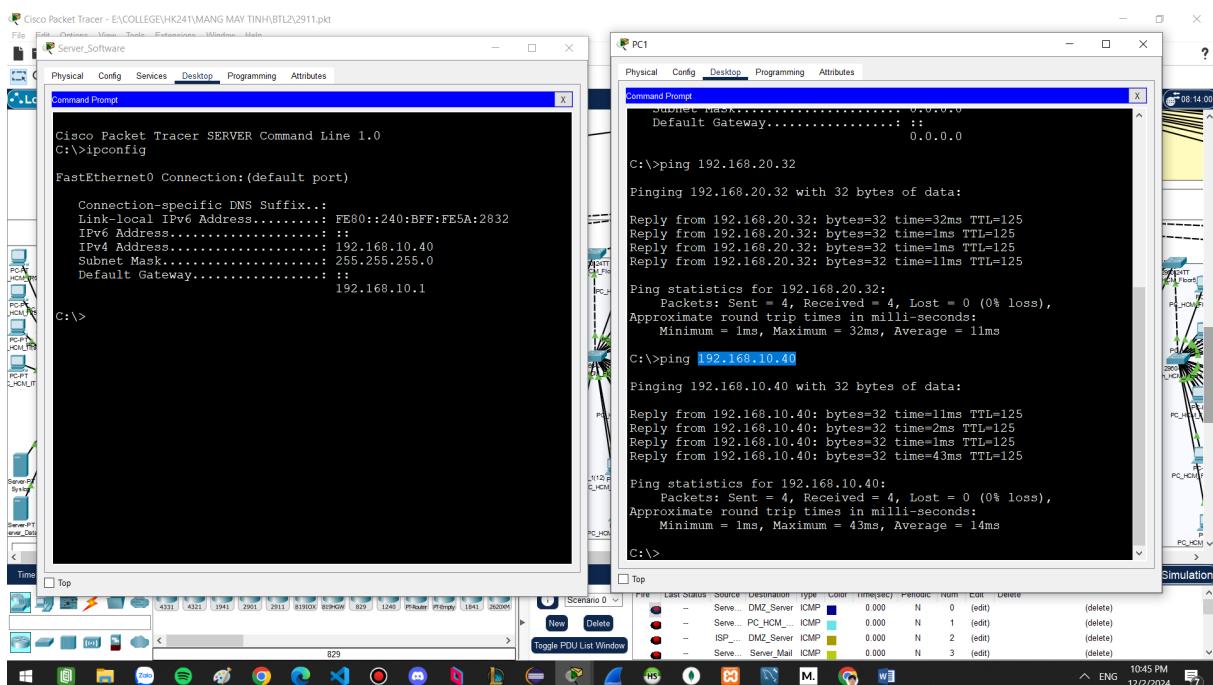
Hình 38

5.3.2 PC đến Server

Kết nối được kiểm tra bằng lệnh Ping giữa PC1 (172.16.20.25) và Server_Sofware (192.168.10.40)



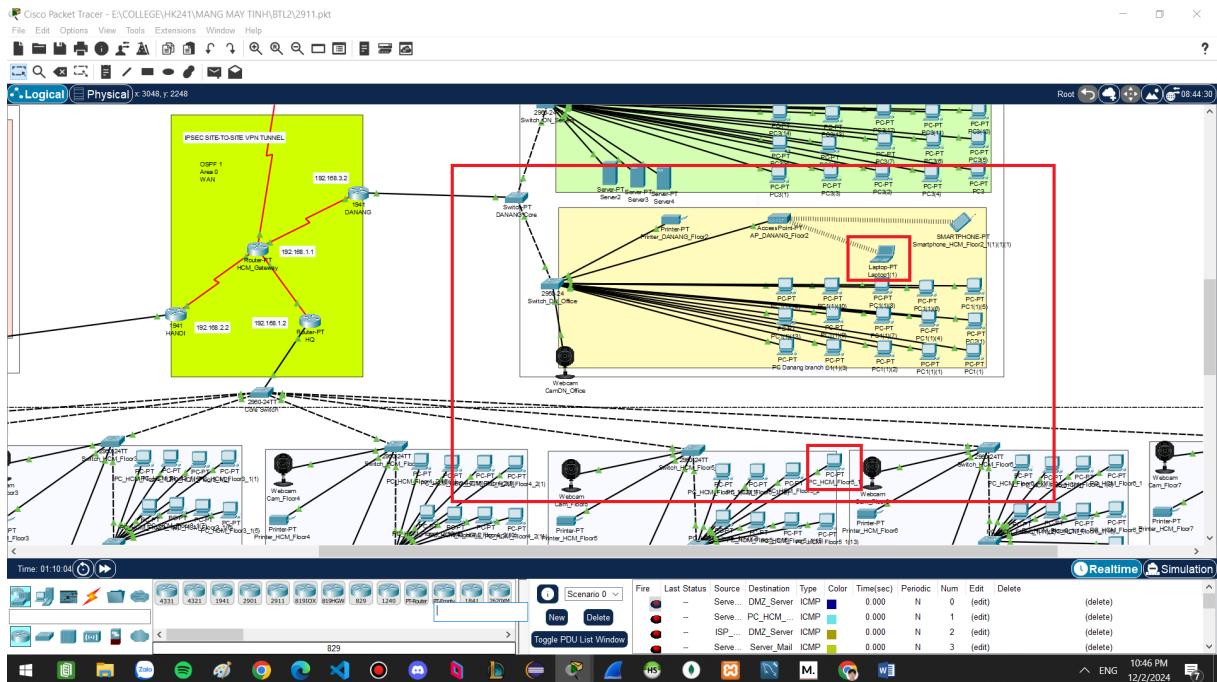
Hình 39



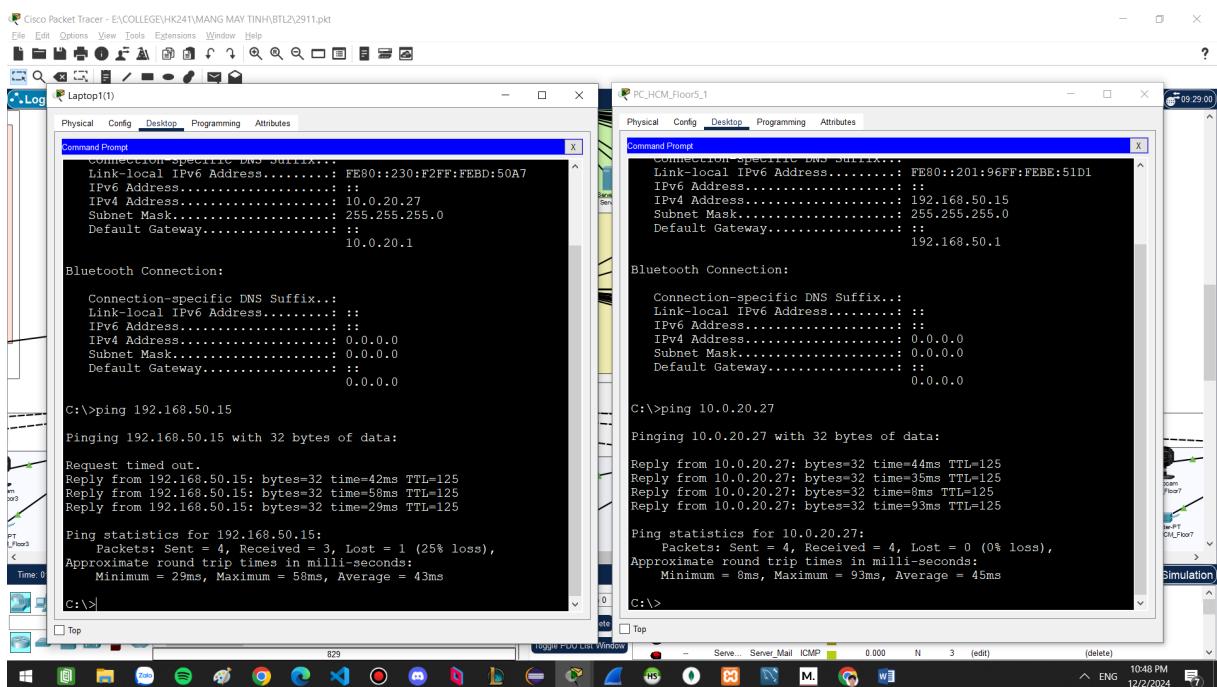
Hình 40

5.3.3 Laptop và PC

Kết nối được kiểm tra bằng lệnh Ping giữa Laptop1(1) (10.0.20.27) và PC_HCM_Floor5_1 (192.168.50.15)



Hình 41

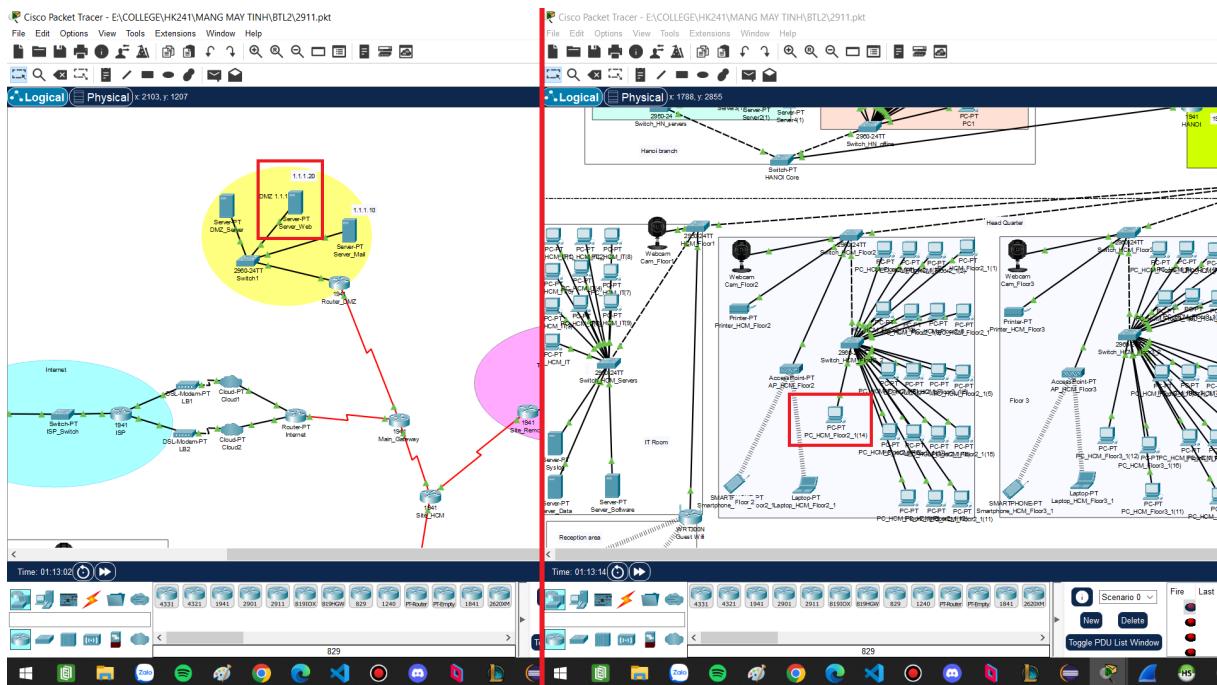


Hình 42

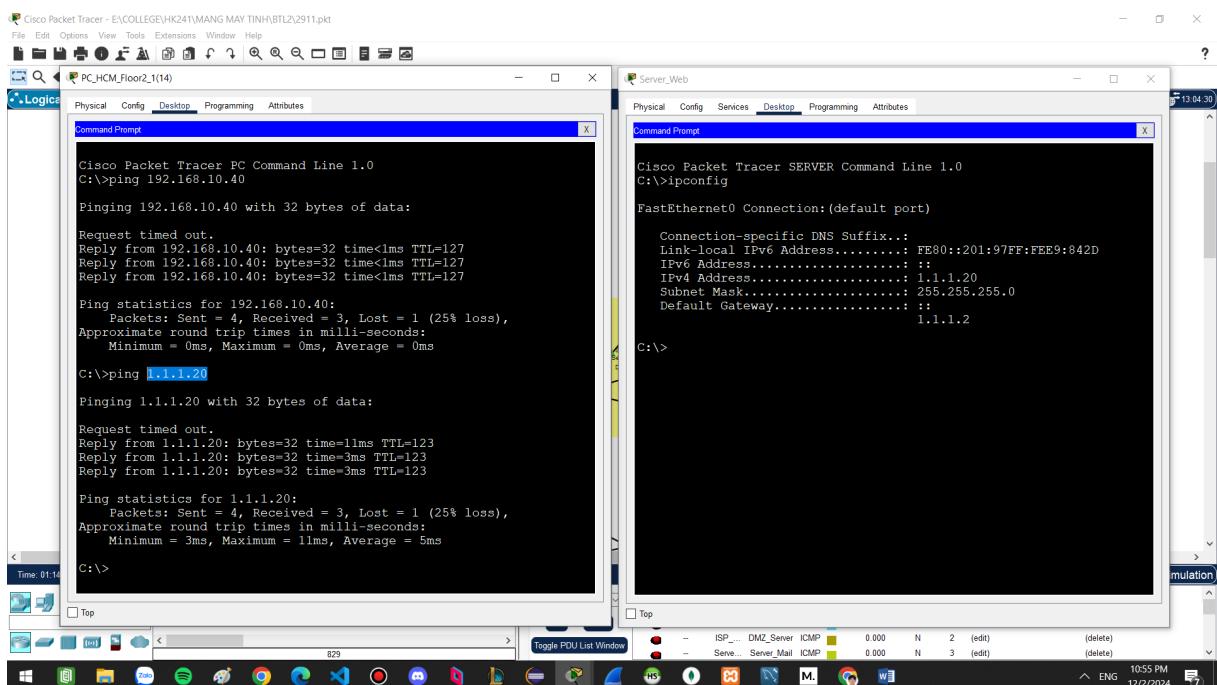
5.4 Kết nối đến Server ở DMZ

5.4.1 PC đến Server

Kết nối được kiểm tra bằng lệnh Ping giữa PC_HCM_Floor2_1(14) (192.168.20.24) và Server_Web (1.1.1.20)



Hình 43

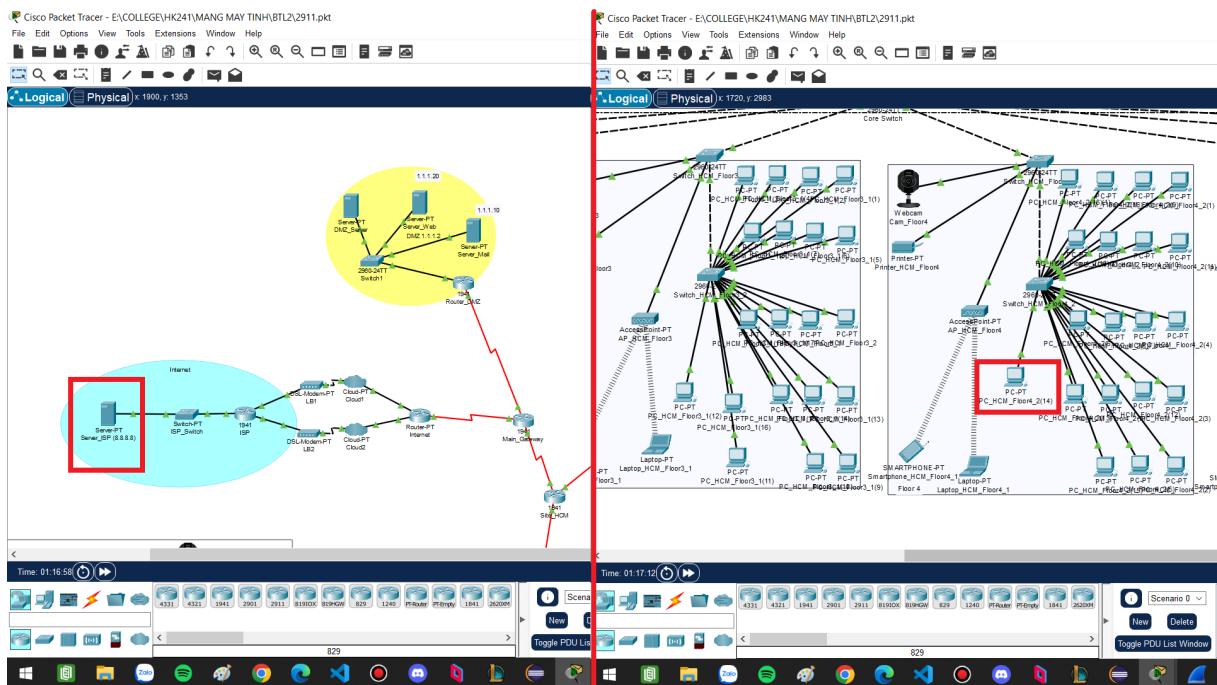


Hình 44

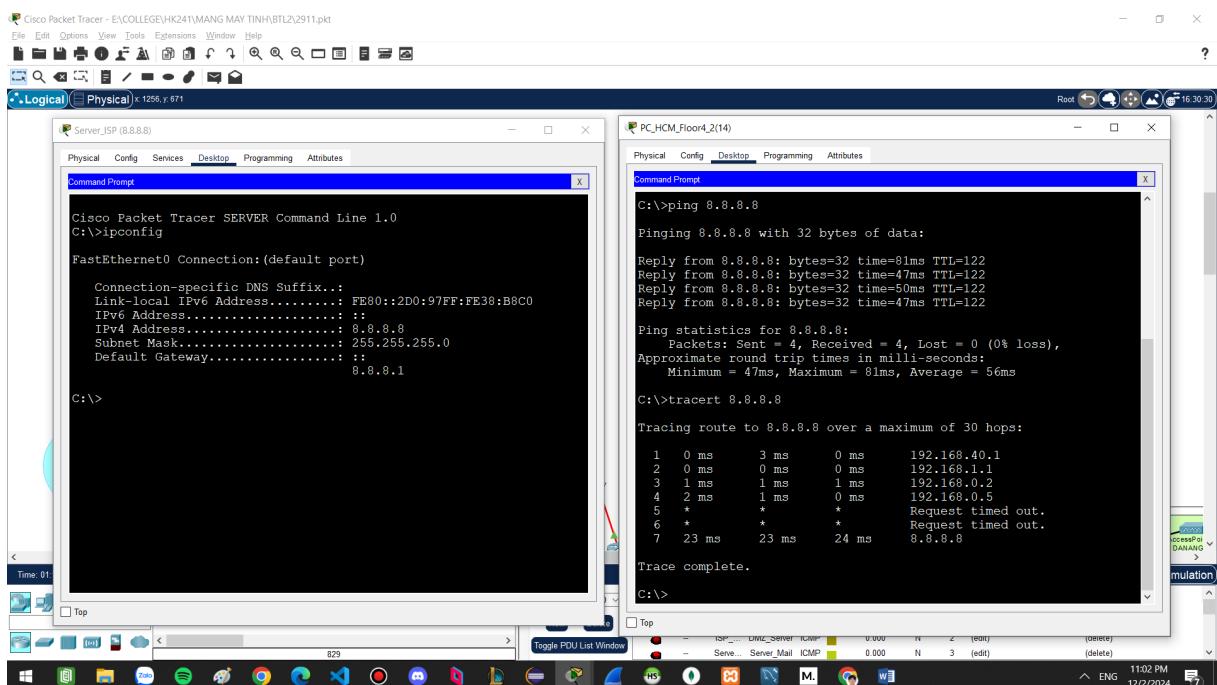
5.5 Kết nối Internet đến Server Web

5.5.1 PC Ping và Traceroute đến Web Server

Kết nối được kiểm tra bằng lệnh Ping và Traceroute từ PC_HCM_Floor2_1(14) (192.168.20.24) đến Server_ISP (8.8.8.8)



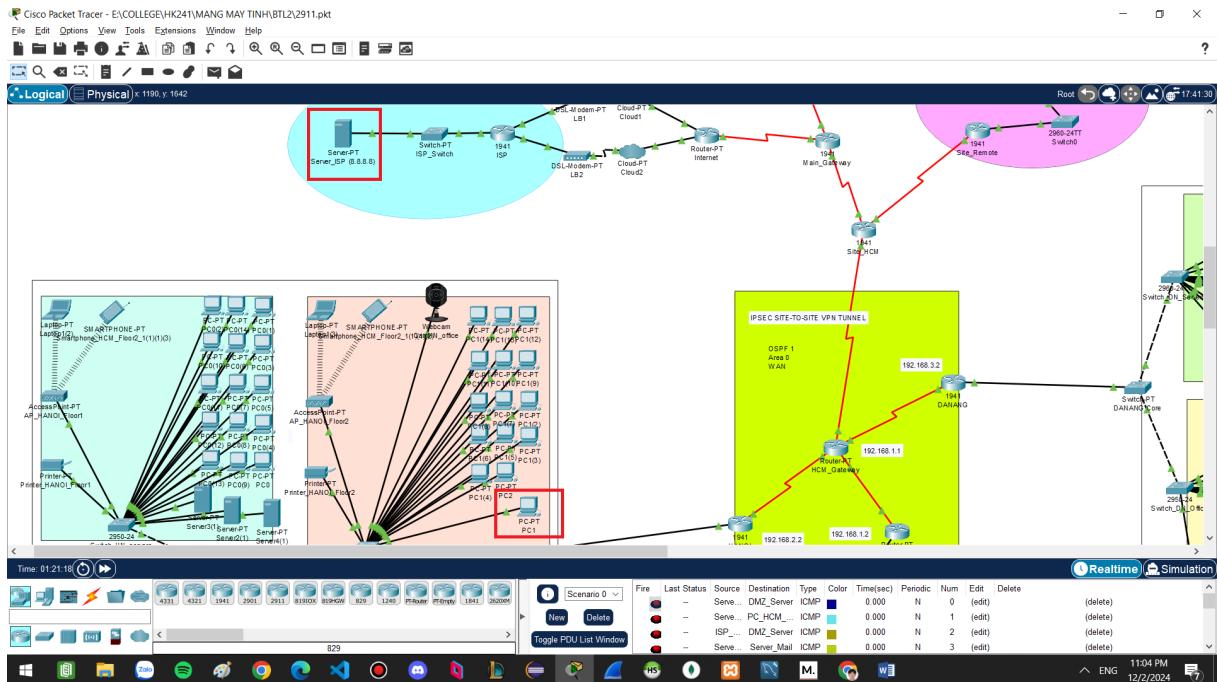
Hình 45



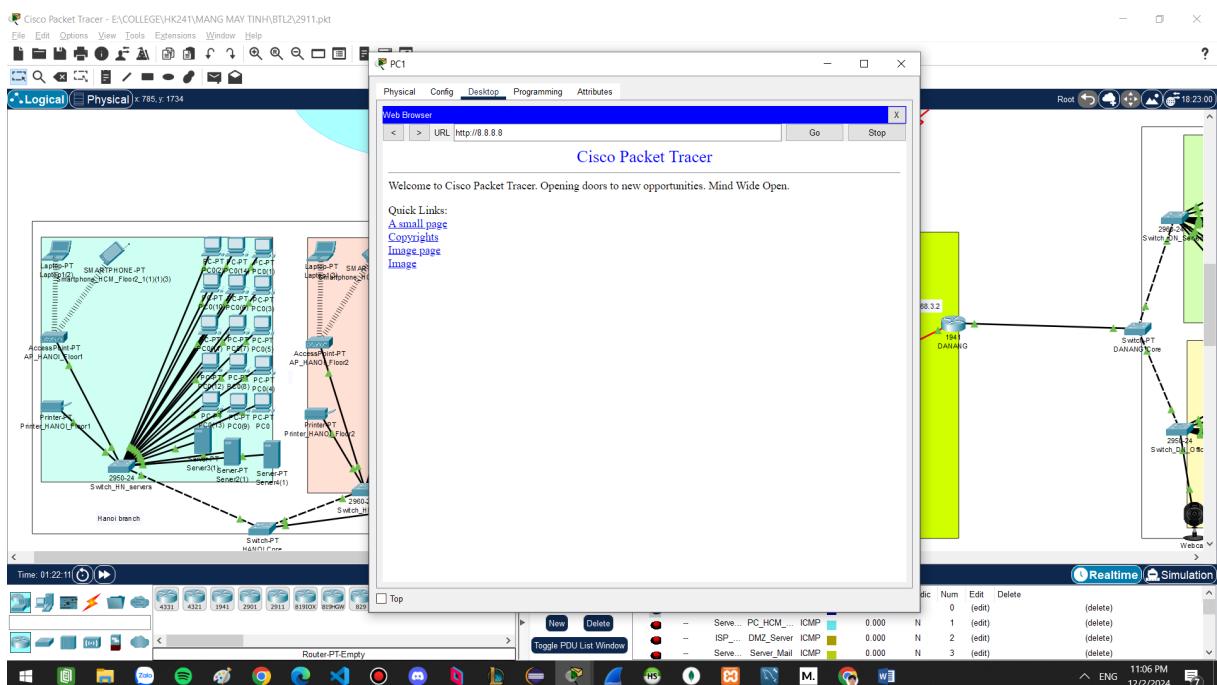
Hình 46

5.5.2 PC kết nối đến Server Web bằng trình duyệt

Kết nối được kiểm tra bằng cách mở trình duyệt của PC1 (172.16.20.25) lên và kết nối đến Server Web qua URL: <http://8.8.8.8>



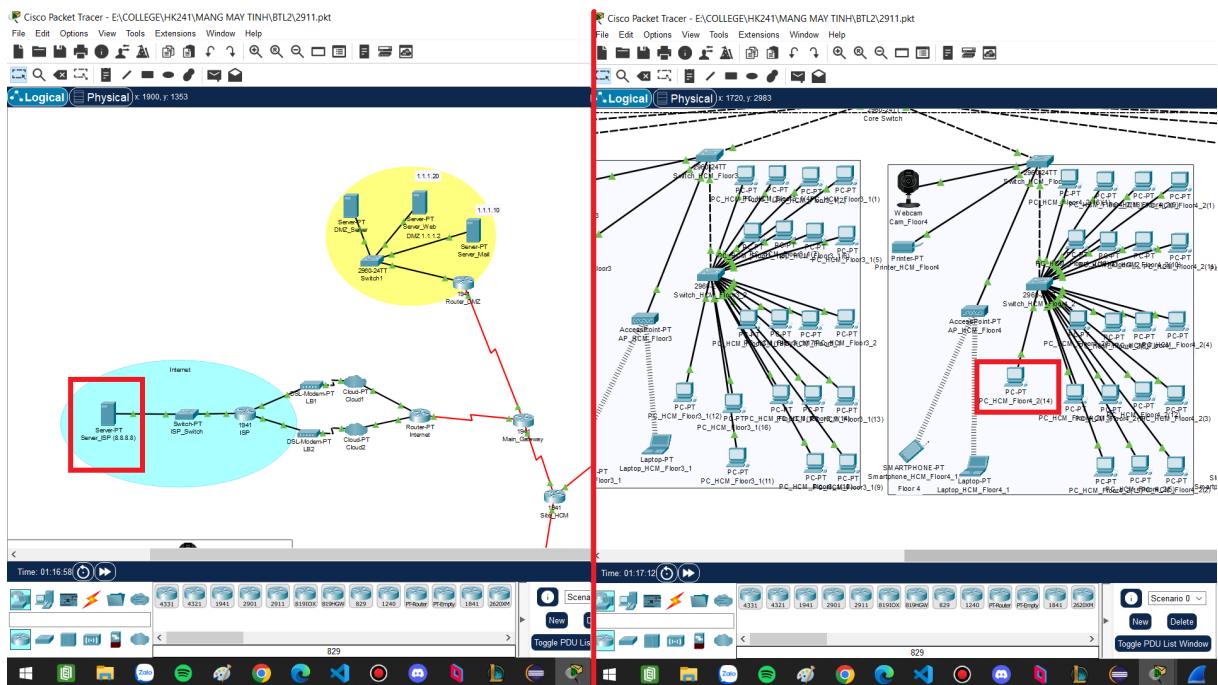
Hình 47



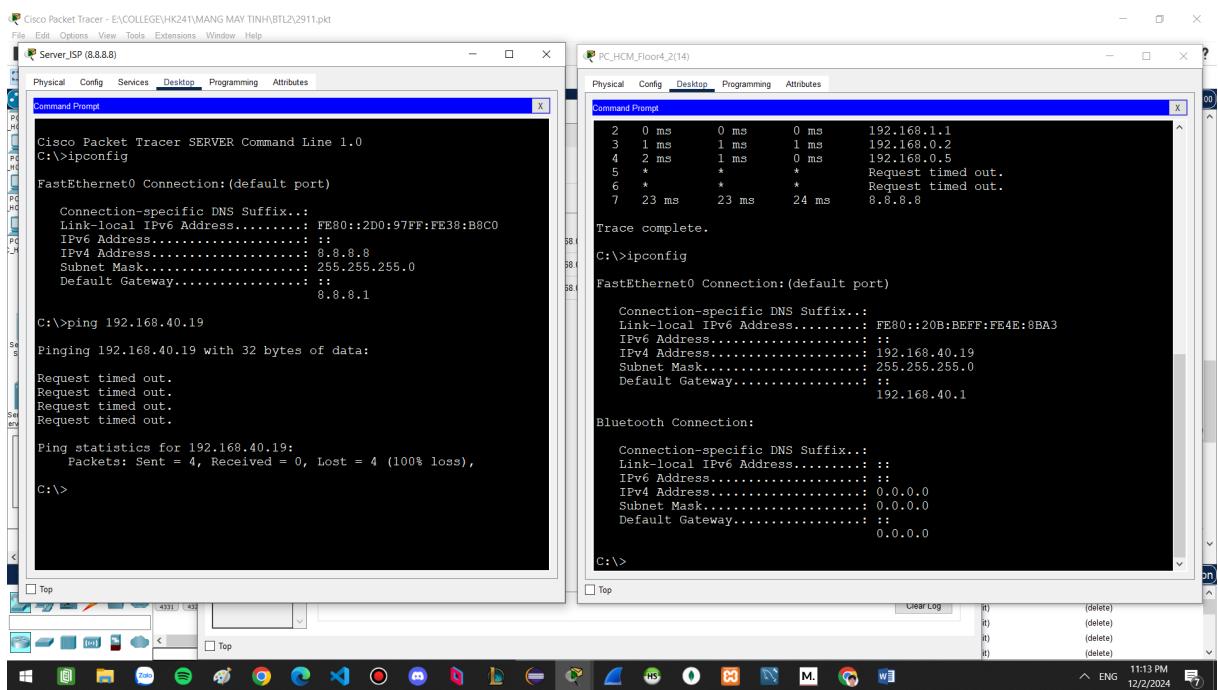
Hình 48

5.6 Bảo mật

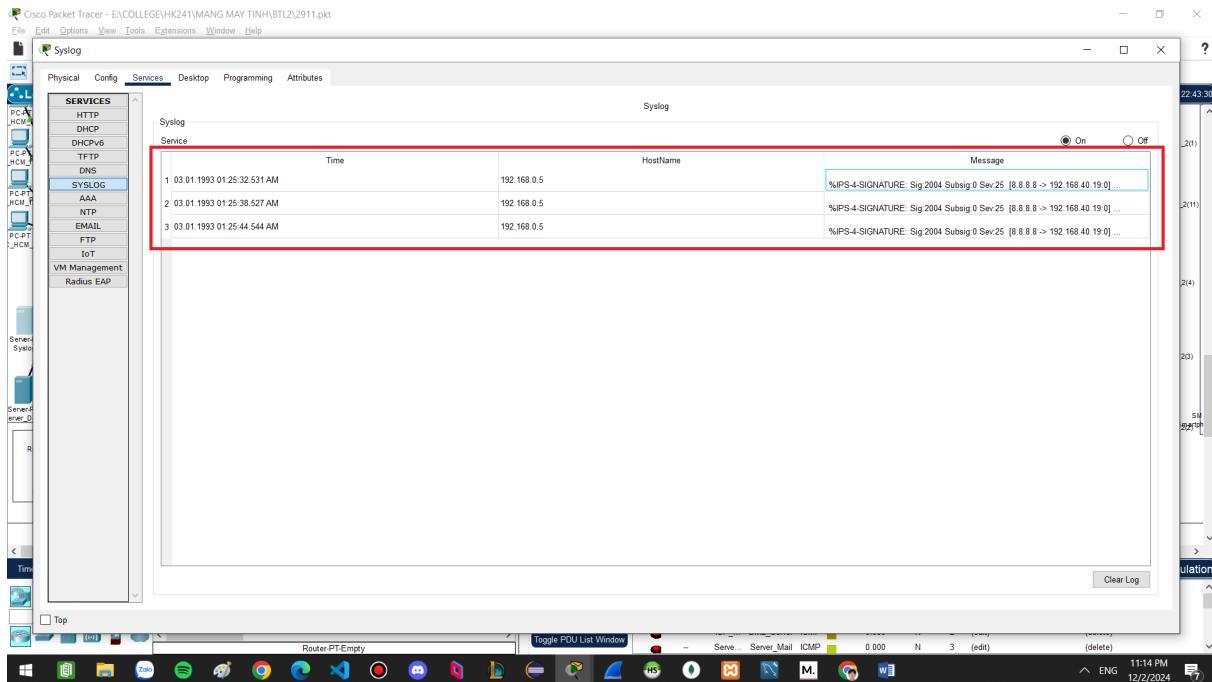
Server ở Internet không thể sử dụng Ping đến một PC ở trụ sở chính TPHCM vì bị chặn kết nối bởi IPS. Kết nối bị chặn đó sẽ được ghi lại trong Syslog của Syslog Server được đặt ở tầng 1 trụ sở chính TPHCM



Hình 49



Hình 50



Hình 51: Syslog

6 Những điểm còn hạn chế và các hướng phát triển, cải thiện trong tương lai

Sau một thời gian sử dụng, hệ thống mạng đã xây dựng cho thấy nhiều ưu điểm nhưng đồng thời cũng bộc lộ một số vấn đề cần khắc phục. Dưới đây là đánh giá chi tiết về các điểm mạnh, những hạn chế còn tồn tại và các hướng cải thiện trong tương lai.

6.1 Những vấn đề còn tồn tại

6.1.1 Phụ thuộc vào các thiết bị trung tâm

Hệ thống hiện tại tập trung vào router chính và switch lõi. Điều này đồng nghĩa với việc, nếu một trong những thiết bị này gặp sự cố, toàn bộ hệ thống có thể bị ảnh hưởng nghiêm trọng. Đây là rủi ro lớn mà hệ thống chưa thực sự giải quyết được.

6.1.2 Khả năng mở rộng còn hạn chế

Cấu trúc mạng hiện tại có thể đáp ứng tốt cho tình hình hiện tại, nhưng nếu số lượng thiết bị và người dùng tăng đột biến, việc mở rộng sẽ gặp khó khăn. Ví dụ, việc bổ sung các VLAN mới hay tái phân bổ địa chỉ IP có thể cần nhiều thời gian và công sức.

6.1.3 Vấn đề bảo mật

Mặc dù đã có firewall và ACL, nhưng khu vực DMZ và Internal vẫn còn một số lỗ hổng bảo mật. Đặc biệt, DMZ chưa kết nối được với Internal một cách toàn diện, dẫn đến hạn chế trong việc cung cấp dịch vụ nội bộ.

6.2 Hướng cải thiện trong tương lai

6.2.1 Đảm bảo tính dự phòng và ổn định

Thêm các thiết bị dự phòng như router backup hoặc triển khai giao thức định tuyến HSRP. Điều này sẽ giúp hệ thống duy trì hoạt động ngay cả khi một thiết bị gặp lỗi.

6.2.2 Tăng cường bảo mật

Cần nâng cấp hệ thống bảo mật hiện tại bằng cách nâng cấp các công cụ như IDS/IPS, tường lửa để phát hiện tấn công sớm. Bên cạnh đó, tăng cường kiểm soát truy cập bằng xác thực đa yếu tố (MFA) sẽ đảm bảo an toàn cho cả người dùng và thiết bị.

6.2.3 Cải thiện khả năng mở rộng

Chuyển đổi sang IPv6 để giải quyết bài toán về địa chỉ IP. Đồng thời, thiết kế lại cấu trúc VLAN để dễ dàng thêm thiết bị mới mà không cần tái cấu hình toàn bộ hệ thống.

6.2.4 Hỗ trợ các công nghệ mới

Chuẩn bị cho việc tích hợp IoT và các giải pháp đám mây để tăng tính linh hoạt. Ngoài ra, việc triển khai SD-WAN cũng là một giải pháp hợp lý để quản lý lưu lượng mạng hiệu quả hơn.

6.3 Kết luận

Hệ thống mạng hiện tại là một nền tảng tương đối tốt, đáp ứng được phần lớn các yêu cầu cơ bản. Tuy nhiên, để duy trì sự ổn định và sẵn sàng cho tương lai, cần phải có những bước cải thiện rõ ràng. Các vấn đề tồn tại cần được giải quyết sớm, và định hướng phát triển cần tập trung vào việc tối ưu hiệu suất, bảo mật và khả năng mở rộng. Điều này không chỉ đảm bảo hệ thống hoạt động ổn định mà còn giúp tổ chức sẵn sàng thích ứng với các thay đổi trong môi trường số hóa.