BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM

KHOA CÔNG NGHỆ THÔNG TIN

MÔN HỌC: MẠNG MÁY TÍNH NÂNG CAO

BÁO CÁO CUỐI KỲ

Lớp học phần: ADNT330580_01

Sinh Viên Thực hiện:

1. Nguyễn Lưu Gia Bảo, MSSV: 22162005

2. Nguyễn Thắng Lợi, MSSV: 22162023

Thành Phố Hồ Chí Minh, Tháng 12/2024

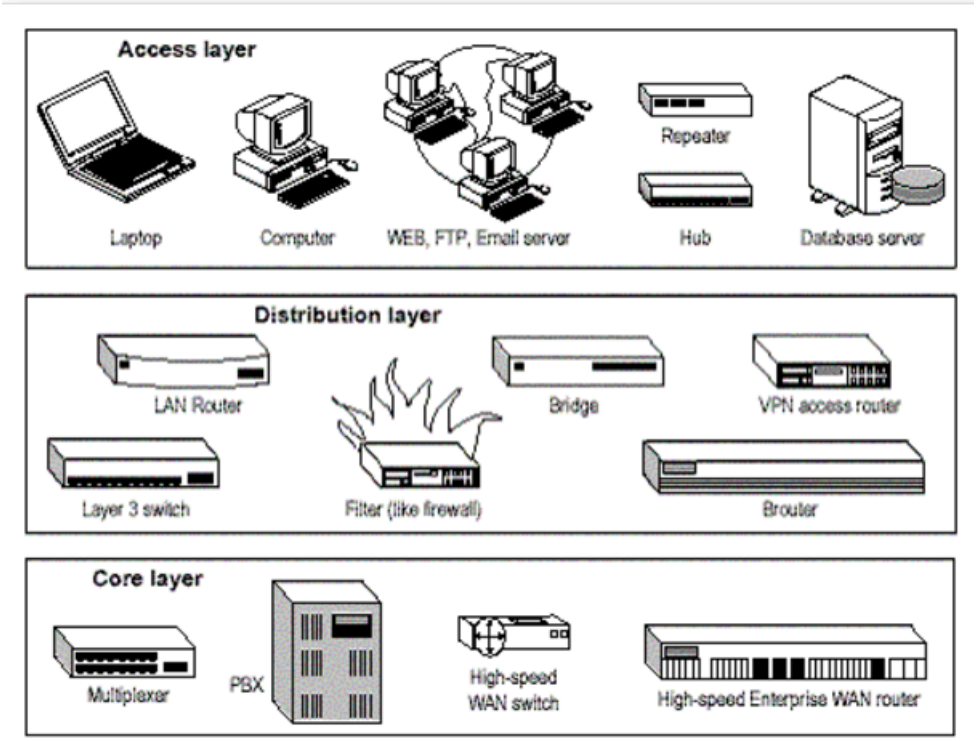
MỤC LỤC

PHẦN I. CÁC CÂU HỎI LÝ THUYẾT

1. Thiết kế mạng theo mô hình phân lớp

Thiết kế mạng theo mô hình phân lớp là phương pháp tổ chức hệ thống mạng thành các lớp (layers), ý tưởng xiên suốt của mô hình là tập trung vào việc nhóm các thiết bị thành các khối chức năng gọi là các lớp đối toàn bộ hệ thống mạng.

Mô hình mạng phân lớp gồm 3 lớp access, distribute, core cho các mạng doanh nghiệp. Mô hình này giúp đơn giản hóa việc xây dựng một hệ thống mạng, đảm bảo các tiêu trí về độ tin cậy, khả năng mở rộng, dễ bảo trì, quản lý và tiết kiệm chi phí. Tùy thuộc thiết bị thuộc khối nào mà nó đảm nhiệm các chức năng phù hợp.



1.1 Các lớp chính trong mô hình phân lớp

a) Core layer

Layer này chịu trách nhiệm chuyển các packet sao cho nhanh và tin cậy nhất có thể. Core layer được biết đến như backbone hay foundation network bởi lẽ toàn bộ các layer khác đều hoạt động dựa trên nó. Mục đích của nó là tăng khả năng vận truyển các packet, giảm độ trễ. Khi triển khai layer này cần chú ý lựa chọn các thiết bị thỏa mãn các yếu tố sau:

- Độ trễ thấp: Layer này chỉ đảm nhiệm chức năng forward chứ không thao tác với packet nên xử lý càng nhanh càng tốt.
- Tốc độ xử lý và truyền dữ liệu cao :Tốc độ là yêu cầu quan trọng của layer này bởi lẽ nó phải chịu tải của tất cả các phân đoạn nhỏ của các layer phía dưới.
- Khả năng tin cậy cao: Layer này cần xây dựng nhiêu đường truyền dữ liệu dự phòng để đảm bảo có backup khi lỗi xảy ra.

Một số thiết bị có thể sử dụng trong layer này bao gồm:

- Cisco switches : 7000, 7200, 7500, and 12000 (for WAN use)
- Catalyst switches : 6000, 5000, and 4000 (for LAN use)
- T-1 and E-1 lines, Frame relay connections, ATM networks, Switched Multimegabit Data Service (SMDS)

b) Distribution layer

Distribution layer chịu trách nhiệm định tuyến. Layer này cũng chịu trách nhiệm áp dụng các policy-based cho các kết nối trong mạng. Cụ thể bao gồm:

- Định tuyến giữa các VLAN.
- Packet filtering (firewalling): Xử lý, thao tác với các packet dự trên thông tin nguồn và đích để tạo borders network.
- QoS: Với các router hoặc Switch layer3 thì layer này có thể đọc các packet để thực hiện policy áp dụng quyền ưu tiên của mỗi packet.
- Điểm kết hợp các Access switches.
- Appliction gateway: Layer này cho phép ta tạo các protocol gateways cho các kiến trúc mạng khác nhau.

- Layer này cũng thực hiện queue và cung cấp khả năng thao tác với traffic của mạng.

Tại layer này ta có thể điều kiển các luồng dữ liệu tới và ra khỏi mạng. Cũng có thể tạo, giới hạn các broadcard domains, virtual LANs. Nếu cần có thể thực hiện các công việc quản trị. Các dòng router có thể sử dụng ở layer này bao gồm: 2600, 4000 và 4500.

c) Access layer

Cho phép các user sử dụng các dịch vụ mà Distribution, Core switch cung cấp. Trong layer này ta có thể mở rộng các collision domain bằng việc sử dụng các repeater, hub. Với access layer ta có thể.

- Thực hiện filter theo MAC (port security).
- Tạo ra các collision domain để giảm xung đột tăng hiệu xuất mạng.
- Share bandwidth: Chia sẻ kết nối mạng giữa các mạng khác nhau.
- Xử lý switch bandwidth: chuyển data từ một mạng tới mạng khác để cân bằng tải.

1.2 Ưu điểm của mô hình phân lớp

a) *Hiệu suất cao:* Ta có thể dễ dàng thiết kế một hệ thống mạng với tốc độ cao bởi mỗi layer sẽ chỉ thực hiện một số chức năng nhất định giảm thiểu tắc nghẽn vì phải xử lý qúa nhiều chức năng cùng lúc tại cùng vị trí.

b) *Tăng khả năng quản lý và troubleshoot khi có sự cố xảy ra:* Mô hình phân cấp cũng giup việc quản lý và xử lý lỗi trở nên dễ dàng. Ví dụ trong tình huống ta gặp các vấn đề về policy chỉ cần kiểm tra lại phân đoạn distribute mà không cần thiết phải kiểm tra các phần khác.

c) *Dễ dàng trong việc quản lý các policy:* Vì các policy chỉ đặt tại distribute layer ta chỉ cần duy nhất tạo, xóa và sửa đổi tại đây.

d) *Khả năng mở rộng cao:* Việc phân nhỏ tạo ra các vùng tự trị khiến cho việc mở rộng trở nên dễ dàng khi có yêu cầu cao hơn.

e) *Dự đoán hành vi:* Khi quản trị hoặc lên kế hoạch xây dựng một mạng. Mô hình cho phép ta biết điều gì xảy ra khi một tải trọng đặt lên nó.

1.3 Ví dụ về việc thiết kế mạng theo mô hình phân lớp

a) Tổng quan bài toán

Một công ty công nghệ có trụ sở chính tại TP.HCM và hai chi nhánh tại Hà Nội và Đà Nẵng cần xây dựng hệ thống mạng theo mô hình phân lớp để:

- Kết nối giữa các văn phòng.
- Đảm bảo tính bảo mật, hiệu suất cao.
- Dễ dàng mở rộng khi doanh nghiệp phát triển.

b) Thiết kế mạng theo mô hình phân lớp

Lớp Truy cập (Access Layer)

Cấu hình

- Mỗi tầng văn phòng có các switch kết nối tất cả thiết bị đầu cuối qua cổng Ethernet.
- Hệ thống Wi-Fi hỗ trợ kết nối không dây với SSID riêng cho khách hàng và nhân viên.
- Triển khai VLAN để phân tách lưu lượng:
    - VLAN 10: Lưu lượng của nhân viên.
    - VLAN 20: Lưu lượng của khách.

Ví dụ cụ thể tại trụ sở chính TP.HCM:

- Tầng 1: Một switch 24-port kết nối các máy tính lễ tân, IP Phone.
- Tầng 2-5: Mỗi tầng có một switch 48-port kết nối nhân viên, mỗi tầng đều được cấp một Access Point phát Wi-Fi.

Lớp Phân phối (Distribution Layer)

Cấu hình

- Sử dụng hai switch Layer 3 (L3) tại trụ sở chính để:
    - Thực hiện định tuyến nội bộ giữa VLAN.
    - Đảm bảo kết nối giữa các VLAN khác nhau (VD: VLAN 10 và VLAN 20).
- Tường lửa được triển khai ở lớp này để kiểm soát lưu lượng truy cập từ mạng nội bộ ra Internet.

Ví dụ cụ thể:

- Một nhân viên kết nối qua VLAN 10 muốn truy cập Internet:
    - Lưu lượng sẽ đi qua lớp truy cập, sau đó được chuyển tiếp lên lớp phân phối, nơi các ACL kiểm tra và định tuyến hợp lệ.
- Trong mạng nội bộ, lưu lượng giữa các VLAN được kiểm soát bởi chính sách tường lửa ở lớp này.

Lớp Lõi (Core Layer)

Cấu hình

- Sử dụng các router lõi để kết nối trụ sở chính với hai chi nhánh qua kênh VPN MPLS.
- Băng thông tối thiểu: 1 Gbps cho các kết nối giữa trụ sở chính và chi nhánh.

Ví dụ cụ thể

- Router tại trụ sở chính TP.HCM sẽ thực hiện định tuyến lưu lượng đến router tại chi nhánh Hà Nội và Đà Nẵng.
- Dữ liệu từ máy chủ tại trung tâm dữ liệu TP.HCM sẽ được truyền tải qua VPN an toàn đến các chi nhánh.

c) Lợi ích từ thiết kế

- Hiệu suất cao: Lớp lõi chịu trách nhiệm chính trong việc truyền tải lưu lượng lớn, giảm tải cho lớp phân phối và truy cập. Ví dụ: Nhân viên ở Hà Nội có thể truy cập máy chủ ERP tại TP.HCM mà không gặp độ trễ cao.
- Tính bảo mật: Tường lửa và ACL ngăn chặn các truy cập trái phép. VLAN giúp tách biệt lưu lượng của nhân viên và khách.
- Dễ dàng mở rộng: Nếu công ty mở thêm chi nhánh, chỉ cần thêm router và cấu hình VPN kết nối đến lớp lõi.
- Quản lý hiệu quả: Mỗi lớp đảm nhận một vai trò cụ thể, giúp quản trị viên dễ dàng theo dõi và khắc phục sự cố.

2. Triển khai ứng dụng trên môi trường Cloud

2.1 Giới thiệu về điện toán đám mây (Cloud Computing)

Điện toán đám mây cung cấp tài nguyên tính toán như máy chủ, lưu trữ, cơ sở dữ liệu và phần mềm qua internet ("đám mây") trên cơ sở trả phí theo nhu cầu. Điều này cho phép các doanh nghiệp triển khai và mở rộng ứng dụng một cách linh hoạt và tiết kiệm chi phí.

2.2 Mô hình dịch vụ Cloud

a) IaaS (Infrastructure as a Service): Cung cấp cơ sở hạ tầng IT như máy chủ, lưu trữ và mạng. Ví dụ: Amazon EC2, Microsoft Azure Virtual Machines.

b) PaaS (Platform as a Service): Cung cấp nền tảng để phát triển, kiểm thử và triển khai ứng dụng. Ví dụ: Google App Engine, Heroku.

c) SaaS (Software as a Service): Cung cấp phần mềm qua internet. Ví dụ: Salesforce, Office 365.

2.3 Lợi ích của triển khai ứng dụng trên Cloud

a) Tính linh hoạt và mở rộng: Tài nguyên có thể được mở rộng hoặc thu hẹp dựa trên nhu cầu từ thực tế.

b) Tiết kiệm chi phí đầu tư ban đầu: Không cần đầu tư vào cơ sở hạ tầng vật lý.

c) Khả năng tiếp cận toàn cầu: Dịch vụ và ứng dụng có thể được truy cập từ bất kỳ đâu.

2.4 Ví dụ minh họa về việc triển khai ứng dụng trên Cloud

a) Tổng quan bài toán

Một trung tâm đào tạo lập trình muốn triển khai ứng dụng quản lý học viên trực tuyến trên Cloud. Ứng dụng cần:

- Quản lý thông tin học viên, lịch học, điểm số.
- Hỗ trợ truy cập đồng thời từ nhiều giảng viên và học viên.
- Đảm bảo tính sẵn sàng cao, dễ dàng mở rộng khi có thêm học viên.

b) Chi tiết triển khai ứng dụng

Phân tích yêu cầu

- Lưu trữ dữ liệu: Ứng dụng cần lưu trữ dữ liệu học viên, khóa học, điểm số.
- Khả năng mở rộng: Phục vụ từ 100 đến 10,000 người dùng tùy từng thời điểm.
- Bảo mật: Đảm bảo dữ liệu nhạy cảm (như điểm số) được mã hóa và bảo vệ.
- Ngân sách: Tối ưu chi phí với mô hình trả phí theo nhu cầu sử dụng.

Lựa chọn dịch vụ Cloud

- Nền tảng: AWS (Amazon Web Services) được chọn vì cung cấp dịch vụ linh hoạt và mạnh mẽ.
- Dịch vụ cụ thể:
- Compute: AWS EC2 để chạy ứng dụng.
- Lưu trữ dữ liệu: AWS RDS (Relational Database Service) với MySQL làm hệ quản trị.
- Lưu trữ tĩnh: Sử dụng Amazon S3 để lưu trữ tài liệu học tập và hình ảnh.
- Mạng: AWS CloudFront làm CDN để phân phối nội dung nhanh chóng.
- Giám sát: AWS CloudWatch để theo dõi hiệu suất và cảnh báo sự cố.

Thiết kế kiến trúc ứng dụng

- Kiến trúc Microservices: Ứng dụng được chia thành các dịch vụ nhỏ độc lập
    - Service 1: Quản lý học viên (Student Management).

    - Service 2: Quản lý khóa học (Course Management).
    - Service 3: Quản lý lịch học và điểm số (Schedule & Grading).
- Load Balancer: Sử dụng AWS Elastic Load Balancer để phân phối lưu lượng giữa các máy chủ EC2.
- Database: Dữ liệu được lưu trong RDS với cấu hình Multi-AZ để đảm bảo tính sẵn sàng cao.
- API Gateway: AWS API Gateway để quản lý các API REST, cho phép giao tiếp giữa client và server.

Triển khai ứng dụng

- Tạo môi trường:
    - Tạo các máy ảo EC2 để triển khai dịch vụ backend.
    - Cài đặt Docker trên các EC2 instance để chạy các container ứng dụng.
- Cài đặt cơ sở dữ liệu:
    - Triển khai MySQL trên AWS RDS.
    - Cấu hình Multi-AZ để đảm bảo phục hồi nhanh khi gặp sự cố.
- Lưu trữ nội dung tĩnh:
    - Tải tài liệu học tập, hình ảnh lên Amazon S3.
    - Cấu hình quyền truy cập để đảm bảo chỉ người dùng được phép mới có thể tải xuống.
- Tích hợp mạng:
    - Sử dụng AWS VPC để cô lập mạng riêng, ngăn chặn truy cập trái phép từ internet.
    - Kết nối VPC với Internet Gateway để cung cấp truy cập công khai đến dịch vụ ứng dụng.
- Cấu hình CDN:
    - Sử dụng AWS CloudFront để phân phối nhanh tài liệu học tập từ S3 đến học viên ở nhiều khu vực.

- Giám sát:
    - Thiết lập AWS CloudWatch để giám sát CPU, RAM, và lưu lượng mạng của các EC2 instances.
    - Tạo cảnh báo khi tài nguyên vượt ngưỡng, ví dụ: CPU vượt 80%.
- Quy trình bảo trì
    - Tự động mở rộng: AWS Auto Scaling tự động thêm hoặc giảm số lượng EC2 instances dựa trên lưu lượng truy cập.
    - Backup: Sử dụng AWS Backup để sao lưu RDS hàng ngày.
    - Cập nhật: Thực hiện rolling update trên các container để đảm bảo không gây gián đoạn dịch vụ.

3. Bảo mật hệ thống CNTT theo mô hình phân lớp (defense-in-depth)

3.1 Giới thiệu về mô hình bảo mật phân lớp (Defense-in-Depth)

Defense-in-Depth là một chiến lược bảo mật trong đó nhiều biện pháp bảo vệ được triển khai ở các lớp khác nhau của hệ thống CNTT. Mục tiêu là tạo ra các lớp phòng thủ liên tiếp để giảm thiểu nguy cơ từ các cuộc tấn công và tăng khả năng phát hiện, phản ứng với sự cố.

3.2 Các lớp bảo mật trong mô hình Defense-in-Depth

a) Policies, Procedures, and Awareness

Mô tả: Đây là nền tảng của bất kỳ chương trình bảo mật nào, bao gồm việc thiết lập các chính sách bảo mật, quy trình hoạt động và nâng cao nhận thức về an ninh thông tin trong tổ chức.

Ví dụ:

- Chính sách bảo mật: Xây dựng chính sách về sử dụng mật khẩu mạnh, yêu cầu thay đổi mật khẩu định kỳ và không chia sẻ thông tin đăng nhập.
- Quy trình: Thiết lập quy trình phản ứng khi xảy ra sự cố an ninh, bao gồm việc báo cáo, điều tra và khắc phục.

- Nhận thức: Tổ chức các buổi đào tạo cho nhân viên về nhận biết và phòng tránh các hình thức tấn công như phishing, malware.

b) Physical Security

Mô tả: Bảo vệ cơ sở hạ tầng vật lý khỏi truy cập trái phép, phá hoại hoặc trộm cắp, đảm bảo chỉ những người được ủy quyền mới có thể tiếp cận các khu vực quan trọng.

Ví dụ:

- Sử dụng hệ thống kiểm soát truy cập bằng thẻ từ, mã PIN hoặc sinh trắc học cho phòng máy chủ.
- Lắp đặt camera giám sát, cảm biến chuyển động và hệ thống báo động tại các khu vực nhạy cảm.
- Bố trí bảo vệ hoặc nhân viên an ninh tuần tra 24/7.

c) Perimeter Defense

Mô tả: Bảo vệ ranh giới giữa mạng nội bộ và mạng bên ngoài (như internet), ngăn chặn các mối đe dọa từ bên ngoài xâm nhập vào hệ thống.

Ví dụ:

- Tường lửa (Firewall): Thiết lập quy tắc lọc lưu lượng mạng dựa trên địa chỉ IP, cổng và giao thức.
- Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS): Giám sát lưu lượng mạng để phát hiện và phản ứng với các hoạt động đáng ngờ
- VPN (Virtual Private Network): Mã hóa kết nối từ xa của nhân viên, đảm bảo an toàn khi truy cập mạng nội bộ.

d) Internal Network Security

Mô tả: Bảo vệ mạng nội bộ khỏi các mối đe dọa bên trong và ngăn chặn sự lây lan nếu có sự cố xảy ra.

Ví dụ:

- Phân đoạn mạng (Network Segmentation): Chia mạng thành các vùng nhỏ hơn để giới hạn phạm vi truy cập.
- Kiểm soát truy cập nội bộ: Sử dụng VLAN và ACL (Access Control List) để quản lý quyền truy cập giữa các bộ phận.
- Giám sát mạng nội bộ: Sử dụng công cụ giám sát để phát hiện hoạt động bất thường.

e) Host Security

Mô tả: Bảo vệ máy chủ, máy tính cá nhân và các thiết bị khác khỏi phần mềm độc hại và các tấn công.

Ví dụ:

- Phần mềm chống virus và chống malware: Cài đặt và cập nhật thường xuyên trên tất cả các thiết bị.
- Quản lý bản vá (Patch Management): Đảm bảo hệ điều hành và phần mềm được cập nhật với các bản vá bảo mật mới nhất.
- Cấu hình bảo mật: Vô hiệu hóa các dịch vụ và cổng không cần thiết, thiết lập chính sách khóa màn hình tự động.

f) Application Security

Mô tả: Bảo vệ ứng dụng khỏi các lỗ hổng bảo mật và tấn công, đảm bảo chúng có thể hoạt động an toàn và tin cậy.

Ví dụ:

- Kiểm tra bảo mật ứng dụng: Thực hiện kiểm thử xâm nhập và đánh giá lỗ hổng trước khi triển khai.
- Biện pháp bảo mật trong phát triển: Áp dụng các phương pháp lập trình an toàn, kiểm tra mã nguồn (code review).
- Bảo vệ giao tiếp ứng dụng: Sử dụng giao thức HTTPS, mã hóa dữ liệu và xác thực người dùng.

g) Data Security

Mô tả: Bảo vệ dữ liệu khỏi truy cập trái phép, mất mát hoặc hủy hoại, đảm bảo tính bảo mật, toàn vẹn và khả dụng của thông tin.

Ví dụ:

- Mã hóa dữ liệu: Mã hóa dữ liệu khi lưu trữ (at rest) và khi truyền tải (in transit).
- Quản lý quyền truy cập dữ liệu: Sử dụng cơ chế kiểm soát truy cập dựa trên vai trò (RBAC), chỉ cấp quyền cần thiết cho người dùng.
- Sao lưu và khôi phục dữ liệu: Thực hiện sao lưu định kỳ và có kế hoạch khôi phục sau thảm họa (Disaster Recovery Plan).

3.3 Lợi ích của mô hình Defense-in-Depth

a) *Bảo vệ toàn diện:* Mỗi lớp bảo mật cung cấp một mức độ bảo vệ riêng, tạo ra một hệ thống phòng thủ đa tầng khó bị xuyên thủng.

b) *Giảm thiểu rủi ro:* Nếu một lớp bị xâm phạm, các lớp khác vẫn tiếp tục bảo vệ, giảm thiểu tác động của cuộc tấn công.

c) *Phát hiện và phản ứng nhanh chóng:* Nhiều lớp giám sát giúp phát hiện sớm các hoạt động đáng ngờ và phản ứng kịp thời.

d) *Tuân thủ quy định:* Hỗ trợ tổ chức đáp ứng các yêu cầu tuân thủ về bảo mật thông tin và dữ liệu, như GDPR, PCI DSS.

3.4 Ví dụ về việc bảo mật hệ thống theo mô hình phân lớp

Giả sử một ngân hàng triển khai chiến lược bảo mật theo mô hình Defense-in-Depth:

a) Policies, Procedures, and Awareness:

- Ban hành chính sách bảo mật nghiêm ngặt về giao dịch tài chính.
- Tổ chức đào tạo định kỳ cho nhân viên về nhận biết tấn công phishing và social engineering.

b) Physical Security:

- Trung tâm dữ liệu được bảo vệ bằng hệ thống kiểm soát truy cập sinh trắc học và có bảo vệ 24/7.

- Lắp đặt camera giám sát và hệ thống báo cháy tự động.

c) Perimeter Defense:

- Sử dụng tường lửa thế hệ mới (Next-Generation Firewall) để lọc lưu lượng mạng nâng cao.
- Triển khai IDS/IPS để giám sát và ngăn chặn các tấn công từ bên ngoài.

d) Internal Network Security:

- Phân đoạn mạng giữa các bộ phận như kế toán, nhân sự, và dịch vụ khách hàng.
- Sử dụng hệ thống giám sát mạng nội bộ để phát hiện hoạt động bất thường.

e) Host Security:

- Máy tính nhân viên được cài đặt phần mềm chống virus và được cập nhật tự động.
- Áp dụng chính sách cấu hình bảo mật chuẩn cho tất cả máy chủ và máy trạm.

f) Application Security:

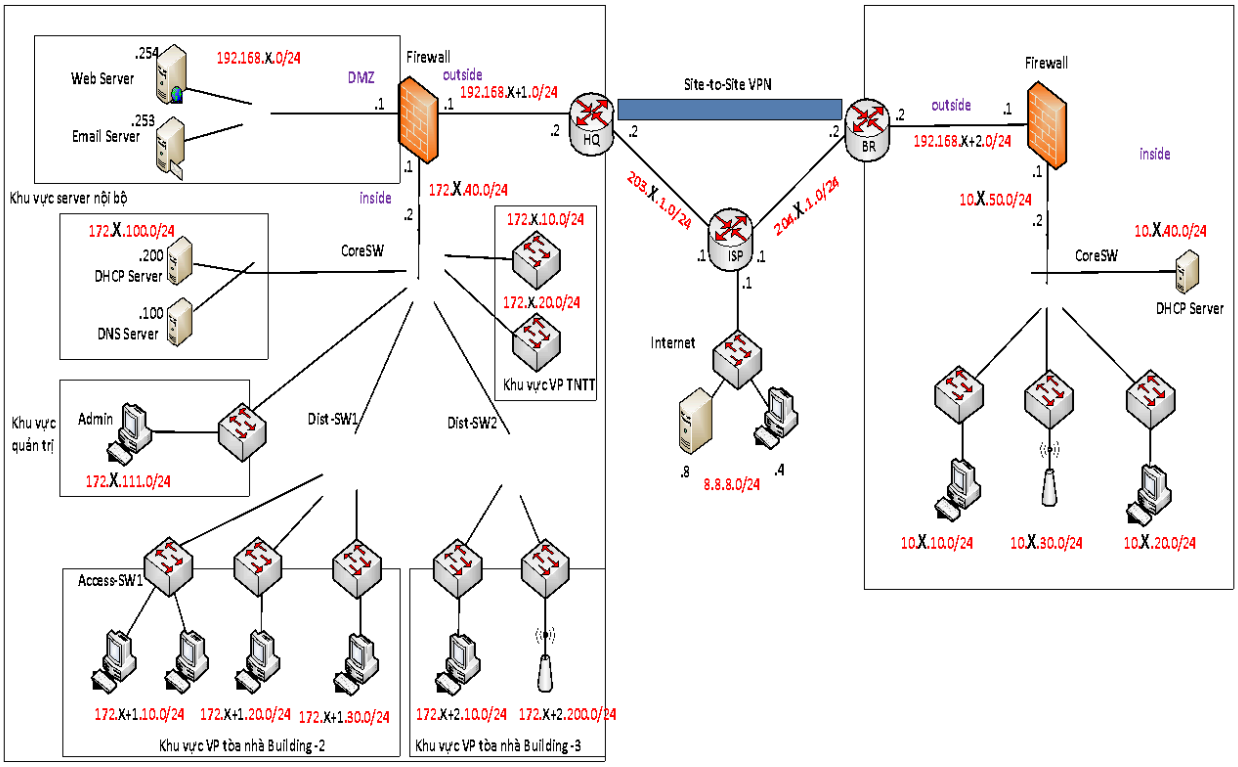
- Ứng dụng ngân hàng trực tuyến được kiểm tra bảo mật định kỳ, bao gồm kiểm thử xâm nhập.
- Sử dụng xác thực hai yếu tố (2FA) cho khách hàng khi đăng nhập.

g) Data Security:

- Dữ liệu giao dịch và thông tin khách hàng được mã hóa bằng các thuật toán mạnh.
- Thiết lập quyền truy cập dữ liệu nghiêm ngặt, chỉ những nhân viên có thẩm quyền mới có thể truy cập thông tin nhạy cảm.
- Thực hiện sao lưu dữ liệu hàng ngày và lưu trữ tại một địa điểm an toàn khác.

PHẦN II. THIẾT KẾ SƠ ĐỒ MẠNG

1. Mô tả vấn đề của bài toán



Bài toán yêu cầu xây dựng và cấu hình một hệ thống mạng hoàn chỉnh cho doanh nghiệp bao gồm Hội sở (HQ) và Chi nhánh (Branch), với mục tiêu đáp ứng các yêu cầu về hạ tầng, dịch vụ và bảo mật. Cần triển khai cấu hình địa chỉ IP, VLAN, VTP, Trunk và EtherChannel để đảm bảo kết nối giữa các thiết bị như Core Switch, Distribution Switch, và Access Switch. Định tuyến mạng (tĩnh hoặc động) phải được cấu hình để liên kết các khu vực mạng, trong khi NAT Overloading và Static NAT phải được thiết lập để cung cấp dịch vụ Web và Email ra ngoài Internet. Hệ thống cũng yêu cầu bảo mật nâng cao, bao gồm hardening, Port Security, SSH, DHCP Snooping, và các ACL để kiểm soát quyền truy cập giữa các VLAN và khu vực quản trị. Các cấu hình tường lửa cần được thiết lập

để kiểm soát luồng dữ liệu và đảm bảo các máy VLAN20 chỉ được sử dụng một số dịch vụ cụ thể, trong khi các máy khác có quyền truy cập toàn diện hơn. Mạng WiFi tại Hội sở cần sử dụng Radius Server để xác thực người dùng. Cuối cùng, bài toán yêu cầu kết nối HQ và Branch thông qua VPN Site-to-Site (IPSec VPN) để đảm bảo sử dụng chung tài nguyên nội bộ, tất cả đều cần được trình bày trong một báo cáo chi tiết với các mục tiêu, cấu hình và kết quả kiểm tra rõ ràng.

2. Topology

Topology của bài toán được xây dựng theo cấu trúc phân lớp với các thành phần chính sau:

2.1 Hội sở (HQ)

- Core Switch (CoreSW): Đặt tại Building 1 (tòa nhà trung tâm) và kết nối với tất cả các Distribution Switch.
- Distribution Switch:
    - Dist-SW1: Đặt tại Building 2, kết nối với các Access Switch để phục vụ 3 phòng ban.
    - Dist-SW2: Đặt tại Building 3, kết nối với các Access Switch để phục vụ 2 phòng ban.
- Access Switch: Kết nối trực tiếp với các máy tính thuộc các phòng ban.
- Server khu vực nội bộ: Gồm DHCP Server và DNS Server phục vụ các dịch vụ mạng nội bộ.
- Server cung cấp dịch vụ ra Internet: Web Server và Email Server được công khai qua địa chỉ IP tĩnh.
- Khu vực quản trị: Gồm máy tính của quản trị viên, có quyền cấu hình từ xa các thiết bị mạng qua Telnet/SSH.
- Firewall tại HQ: Bảo vệ hệ thống mạng nội bộ khỏi các mối đe dọa bên ngoài.
- Kết nối WiFi: Radius Server tại khu vực quản trị để chứng thực người dùng WiFi.

2.2 Chi nhánh (Branch)

- Distribution và Access Switch: Phục vụ kết nối mạng cho 3 phòng ban tại chi nhánh.
- DHCP Server: Cung cấp địa chỉ IP động cho các máy tính trong mạng tại chi nhánh.
- Firewall tại Branch: Bảo vệ hệ thống mạng nội bộ tại chi nhánh.
- Kết nối tới HQ: Chi nhánh sử dụng kết nối VPN Site-to-Site (IPSec VPN) để truy cập các dịch vụ nội bộ tại HQ.

2.3 Kết nối tổng thể

- Kết nối nội bộ tại HQ:
    - Sử dụng VLAN để phân chia mạng theo từng phòng ban.
    - EtherChannel được sử dụng để tăng băng thông và đảm bảo tính sẵn sàng cao giữa CoreSW và Distribution Switch, cũng như giữa Distribution Switch và Access Switch.
- Kết nối giữa HQ và Branch: VPN Site-to-Site được thiết lập để đảm bảo truy cập bảo mật giữa hai mạng.

 Topology này được thiết kế để tối ưu hóa hiệu suất, đảm bảo tính linh hoạt khi mở rộng, và đáp ứng các yêu cầu bảo mật của doanh nghiệp.

3. Mục tiêu

3.1. Đảm bảo tính kết nối và hiệu suất cao của hệ thống mạng:

- Thiết lập một hạ tầng mạng hoàn chỉnh, kết nối hiệu quả giữa các tòa nhà tại Hội sở (HQ) và Chi nhánh (Branch).
- Sử dụng các công nghệ như VLAN, VTP, Trunk, và EtherChannel để tối ưu hóa băng thông và tăng cường tính sẵn sàng.

- Cấu hình định tuyến mạng để đảm bảo các khu vực trong hệ thống có thể giao tiếp với nhau một cách liền mạch.

3.2. Cung cấp các dịch vụ mạng nội bộ và Internet:

- Cấu hình DHCP và DNS Server để hỗ trợ việc cấp phát địa chỉ IP động và phân giải tên miền trong hệ thống mạng nội bộ.
- Cung cấp dịch vụ Web và Email cho người dùng bên ngoài thông qua NAT tĩnh với các địa chỉ IP công khai cụ thể.
- Đảm bảo người dùng trong mạng có thể truy cập Internet với NAT Overloading.

3.3. Đảm bảo tính bảo mật cho hệ thống:

- Áp dụng các biện pháp bảo mật như Port Security, DHCP Snooping, và ACL để kiểm soát truy cập và ngăn chặn các mối đe dọa tiềm tàng trong nội bộ mạng.
- Cấu hình Firewall tại HQ và Branch để quản lý luồng dữ liệu ra/vào hệ thống, chỉ cho phép các dịch vụ và giao thức cần thiết.
- Giới hạn quyền truy cập SSH vào các thiết bị mạng chỉ từ khu vực quản trị.

3.4. Đảm bảo khả năng quản lý và mở rộng:

- Cấu hình hệ thống quản trị mạng cho phép quản trị viên dễ dàng quản lý từ xa thông qua Telnet/SSH.
- Thiết kế mạng linh hoạt, dễ dàng bổ sung hoặc thay đổi số lượng phòng ban, thiết bị, hoặc dịch vụ khi cần thiết.

3.5. Kết nối HQ và Branch:

- Triển khai VPN Site-to-Site (IPSec VPN) để đảm bảo kết nối an toàn giữa Hội sở và Chi nhánh, cho phép sử dụng các dịch vụ nội bộ của HQ từ Branch.

3.6. Tích hợp WiFi bảo mật tại Hội sở:

- Cung cấp kết nối WiFi với Radius Server để chứng thực người dùng, đảm bảo tính an toàn và quản lý dễ dàng thông qua tài khoản được định nghĩa.

3.7. Hỗ trợ nhu cầu sử dụng trong tương lai:

- Thiết kế mạng theo hướng mở, hỗ trợ doanh nghiệp mở rộng hoặc thay đổi mô hình hoạt động mà không làm gián đoạn hệ thống.

4. Kịch bản

4.1. Kịch bản cho cấu hình cơ bản

- **Kết nối giữa các thiết bị mạng:**
  - Dùng EtherChannel để tăng băng thông và đảm bảo tính sẵn sàng giữa CoreSW, DistSW và AccessSW.
  - Cấu hình Trunk trên các cổng EtherChannel để truyền dữ liệu VLAN.
  - Sử dụng VTP để đồng bộ thông tin VLAN giữa các switch.
- **Thiết lập VLAN và phân chia địa chỉ IP:**
  - Tạo VLAN 10, 20, 30, 100, 111 và gán cho từng khu vực mạng như phòng ban, khu vực quản trị và server nội bộ.
  - Cấp IP tĩnh cho các server nội bộ (DHCP, DNS) và cấu hình gateway tại các switch layer 3.
  - Bật tính năng DHCP Relay để cấp phát IP động cho các máy trạm thuộc các VLAN khác nhau.
- **Định tuyến mạng nội bộ:**
  - Sử dụng RIP version 2 để định tuyến giữa các VLAN.
  - Tạo các giao diện VLAN với IP gateway tại CoreSW và DistSW.
- **Khu vực DMZ và Firewall:**
  - Phân chia các vùng mạng Inside, DMZ và Outside.
  - Cấu hình default route trên Router để định tuyến lưu lượng ra Internet.

- Thiết lập ACL tạm thời để cho phép tất cả lưu lượng mạng trong quá trình kiểm tra.

4.2. Kịch bản cấu hình bảo mật

- **Hardening trên AccessSW1:**
  - Tắt tất cả các cổng không sử dụng.
  - Giới hạn số lượng thiết bị được phép kết nối vào từng cổng với Port Security.
- **Truy cập quản trị từ xa:**
  - Cấu hình SSH trên CoreSW, DistSW và AccessSW1 để quản trị từ xa bằng tài khoản bảo mật.
- **Access Control List (ACL):**
  - Cấm các máy thuộc VLAN 10 truy cập khu vực quản trị (VLAN 111).
  - Chỉ cho phép các máy từ VLAN 111 truy cập SSH vào các thiết bị mạng.
- **Firewall tại Hội sở:**
  - Cấu hình để các máy VLAN 20 chỉ được phép truy cập Internet qua dịch vụ PING và FTP.
  - Các máy thuộc VLAN khác được truy cập toàn bộ dịch vụ.
- **Firewall tại Chi nhánh:**
  - Cho phép tất cả các dịch vụ ra Internet mà không hạn chế.

4.3 Kịch bản cấu hình dịch vụ

- Dịch vụ NAT:
  - Static NAT: Cấu hình địa chỉ công khai cho Web Server và Email Server (4.4.4.4 và 5.5.5.5).
  - NAT Overloading (PAT): Cho phép các máy nội bộ truy cập Internet mà không cần IP công khai.
- Web Server và Email Server:

- Cấu hình DNS để phân giải tên miền nội bộ.
- Thử nghiệm truy cập dịch vụ từ cả mạng nội bộ và mạng ngoài Internet.

- Wi-Fi sử dụng Radius Server:
  - Thiết lập Radius Server tại khu vực quản trị để xác thực người dùng WiFi bằng WPA2-Enterprise.
  - Tạo SSID và tài khoản Radius để xác thực.

4.4. Kịch bản kết nối HQ và Branch

- Sử dụng IPSec VPN để mã hóa và kết nối giữa mạng nội bộ HQ và Branch.
- Cấu hình ISAKMP và IPSec với mã hóa 3DES, xác thực MD5 và khóa pre-share.
- Thử nghiệm kết nối VPN và xác nhận gói tin đã được mã hóa thành công.

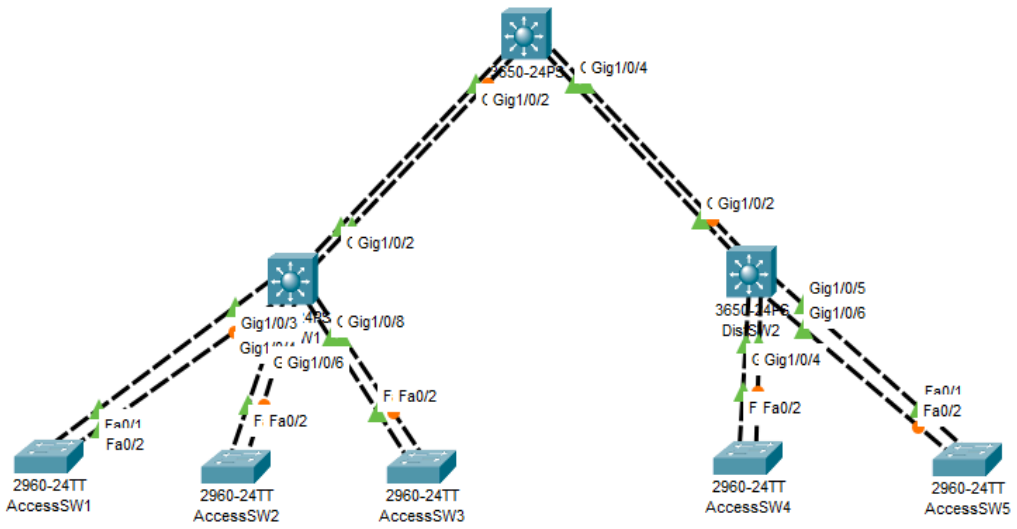
5. Thực hiện và kiểm tra kết quả

5.1 Cấu hình cơ bản

a) Cấu hình EtherChannel, VLAN, VTP, Trunk

Trước tiên ta sẽ dùng một switch layer 3 mẫu 3650-24PS, đặt tên là CoreSW.

Kết nối CoreSW với các Dist-SW, và từ Dist-SW kết nối tới các Access-SW thông qua EtherChannel:



- Kết nối CoreSW với 2 DistSW thông qua EtherChannel:

```
CoreSW(config)#int range gl/0/1, gl/0/2
CoreSW(config-if-range)#channel
CoreSW(config-if-range)#channel-
CoreSW(config-if-range)#channel-g
CoreSW(config-if-range)#channel-group 1 mode ac
CoreSW(config-if-range)#channel-group 1 mode active
CoreSW(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

CoreSW(config-if-range)#int range gl/0/3, gl/0/4
CoreSW(config-if-range)#channel-group 2 mode active
CoreSW(config-if-range)#
Creating a port-channel interface Port-channel 2

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up
```

- Tại 2 DistSW đều được cấu hình tương tự do đều chúng đều giống cổng kết nối:

```
DistSW1(config)#int range gl/0/1, gl/0/2
DistSW1(config-if-range)#channel-g
DistSW1(config-if-range)#channel-group 1 mo
DistSW1(config-if-range)#channel-group 1 mode ac
DistSW1(config-if-range)#channel-group 1 mode active
DistSW1(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

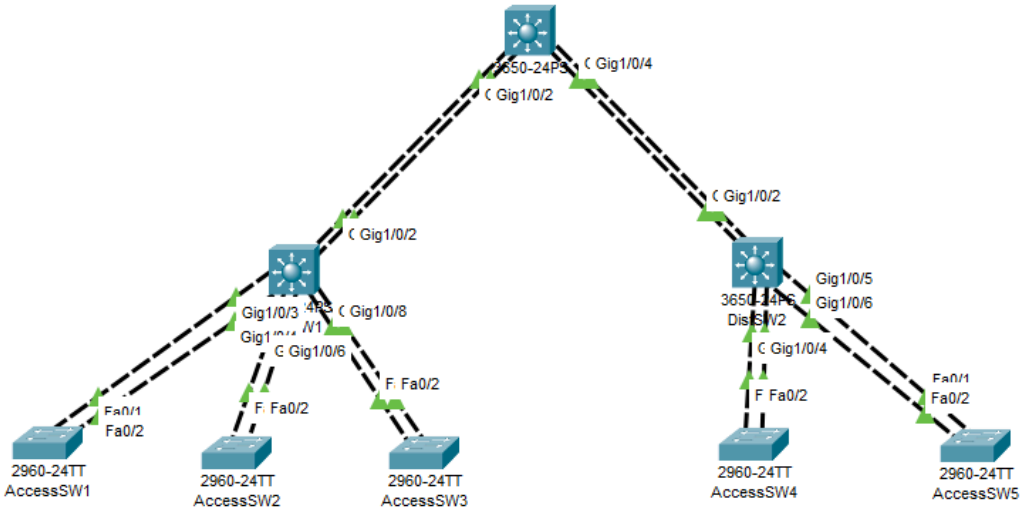
- Tiếp đó là giữa các DistSW và AccessSW. Tại 2 DistSW thì cũng giống nhau, chỉ khác là tại DistSW2 chỉ cần tạo đến port-channel 3 là đủ:

```
DistSW1(config-if-range)#
DistSW1(config-if-range)#int range g1/0/3, g1/0/4
DistSW1(config-if-range)#channel-group 2 mode active
DistSW1(config-if-range)#
Creating a port-channel interface Port-channel 2

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up

DistSW1(config-if-range)#int range g1/0/5, g1/0/6
DistSW1(config-if-range)#channel-group 3 mode active
DistSW1(config-if-range)#
Creating a port-channel interface Port-channel 3

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up

DistSW1(config-if-range)#int range g1/0/7, g1/0/8
DistSW1(config-if-range)#channel-group 4 mode active
```

- Tại các AccessSW thì giống nhau do đều dùng cổng Fa0/1, Fa0/2 để kết nối tới DistSW:

```
AccessSW1>en
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int range f0/1, f0/2
AccessSW1(config-if-range)#channel-g
AccessSW1(config-if-range)#channel-group 1 mode ac
AccessSW1(config-if-range)#channel-group 1 mode active
AccessSW1(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

=> *Như vậy là các kết nối giữa các switch đều trở thành EtherChannel.*



Tiến hành cấu hình cho các cổng EtherChannel là cổng trunk:

```
CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#int pol
CoreSW(config-if)#swi
CoreSW(config-if)#switchport mode trunk

CoreSW(config-if)#int po2
CoreSW(config-if)#switchport mode trunk
```

```
DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#int pol
DistSW1(config-if)#swi
DistSW1(config-if)#switchport mode trunk

DistSW1(config-if)#int po2
DistSW1(config-if)#switchport mode trunk

DistSW1(config-if)#int po3
DistSW1(config-if)#switchport mode trunk

DistSW1(config-if)#int po4
DistSW1(config-if)#switchport mode trunk
```

```
DistSW2>en
DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#int pol
DistSW2(config-if)#swi
DistSW2(config-if)#switchport mode trunk

DistSW2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking Port-channel1 on
VLAN0001. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking Port-channel1 on VLAN0001. Port consistency
restored.


DistSW2(config-if)#int po2
DistSW2(config-if)#switchport mode trunk

DistSW2(config-if)#int po3
DistSW2(config-if)#switchport mode trunk
```

```
AccessSW1>en
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int pol
AccessSW1(config-if)#swi
AccessSW1(config-if)#switchport mode tru
AccessSW1(config-if)#switchport mode trunk
```

Ta có thể tạo VTP để quản lý VLAN trong một mạng lớn bằng cách đồng bộ hóa thông tin VLAN giữa các switch. Đặt VTP domain tên là CoreSW-VTP:

```
CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#vtp domain CoreSW-VTP
Changing VTP domain name from NULL to CoreSW-VTP
CoreSW(config)#vtp mode server
Device mode already VTP SERVER.
```

- Tại các switch khác đều cho gia nhập CoreSW-VTP:

```
DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#vtp domain CoreSW-VTP
Domain name already set to CoreSW-VTP.
```

```
AccessSW1>en
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#vtp do
AccessSW1(config)#vtp domain CoreSW-VTP
Domain name already set to CoreSW-VTP.
```

- Tại CoreSW tạo lần lượt VLAN 10, 20, 30, 100, 111, 200:

```
CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#vlan 10
CoreSW(config-vlan)#vlan 20
CoreSW(config-vlan)#vlan 30
CoreSW(config-vlan)#vlan 100
CoreSW(config-vlan)#vlan 111
CoreSW(config-vlan)#vlan 200
```

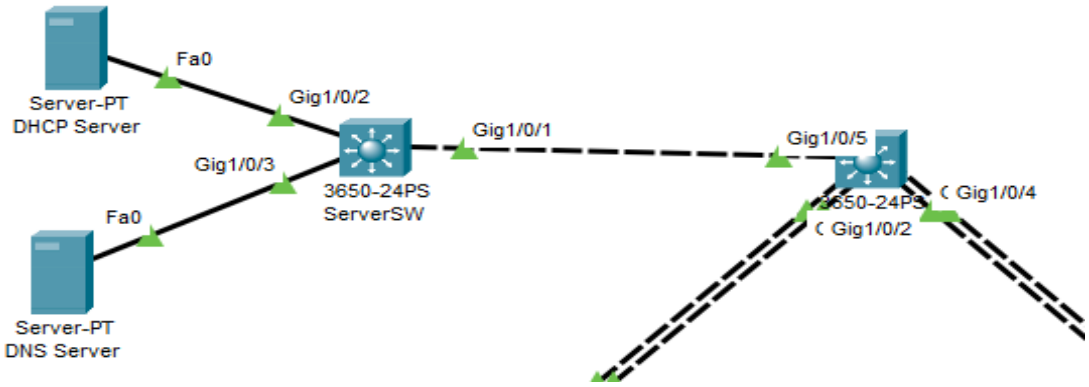
- Sau đó kiểm tra tại các switch khác (không tạo tại các switch này):

```
DistSW1#show vlan br
DistSW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/9, Gig1/0/10, Gig1/0/11, Gig1/0/12
                                                Gig1/0/13, Gig1/0/14, Gig1/0/15,
Gig1/0/16
                                                Gig1/0/17, Gig1/0/18, Gig1/0/19,
Gig1/0/20
                                                Gig1/0/21, Gig1/0/22, Gig1/0/23,
Gig1/0/24
                                                Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
100  VLAN0100                         active
111  VLAN0111                         active
200  VLAN0200                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

AccessSW1#show vlan br
AccessSW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
100  VLAN0100                         active
111  VLAN0111                         active
200  VLAN0200                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
AccessSW1#show vlan br
AccessSW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
100  VLAN0100                         active
111  VLAN0111                         active
200  VLAN0200                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

=> Có thể thấy VLAN đã được đồng bộ qua các switch thông qua VTP. Như vậy là VTP đã được thiết lập thành công

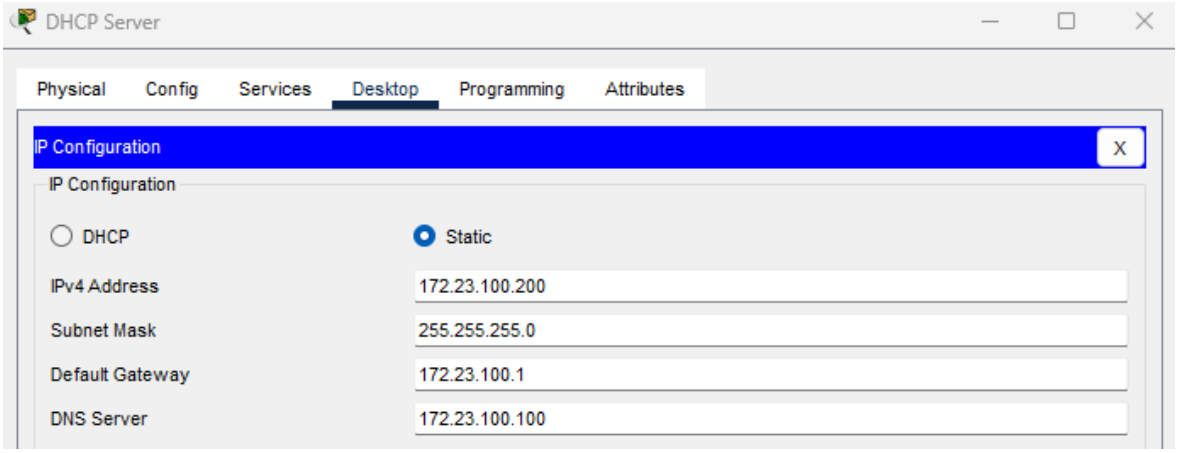
Tiếp đến là cấu hình khu vực server nội bộ thông qua ServerSW. Ở đây sẽ có DHCP Server và DNS Server.

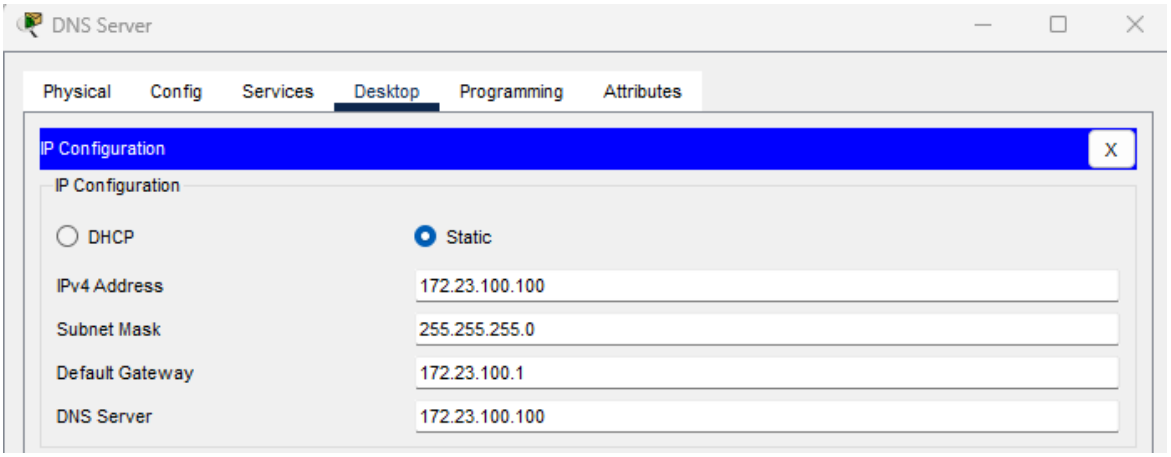


- Cho ServerSW tham gia VTP:

```
ServerSW(config)#int gl/0/1
ServerSW(config-if)#sw
ServerSW(config-if)#switchport mode tru
ServerSW(config-if)#switchport mode trunk

ServerSW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

ServerSW(config-if)#vtp domain CoreSW-VTP
Changing VTP domain name from NULL to CoreSW-VTP
```

- Cho cả 2 server tham gia vào VLAN 100 và với IP là 172.23.100.200 và 172.23.100.100 (IP tĩnh) với gateway là 172.23.100.1 từ ServerSW.





```
ServerSW(config)#int gl/0/2
ServerSW(config-if)#sw
ServerSW(config-if)#switchport ac
ServerSW(config-if)#switchport access vlan 100
ServerSW(config-if)#int gl/0/3
ServerSW(config-if)#swi
ServerSW(config-if)#switchport ac
ServerSW(config-if)#switchport access vlan 100
```

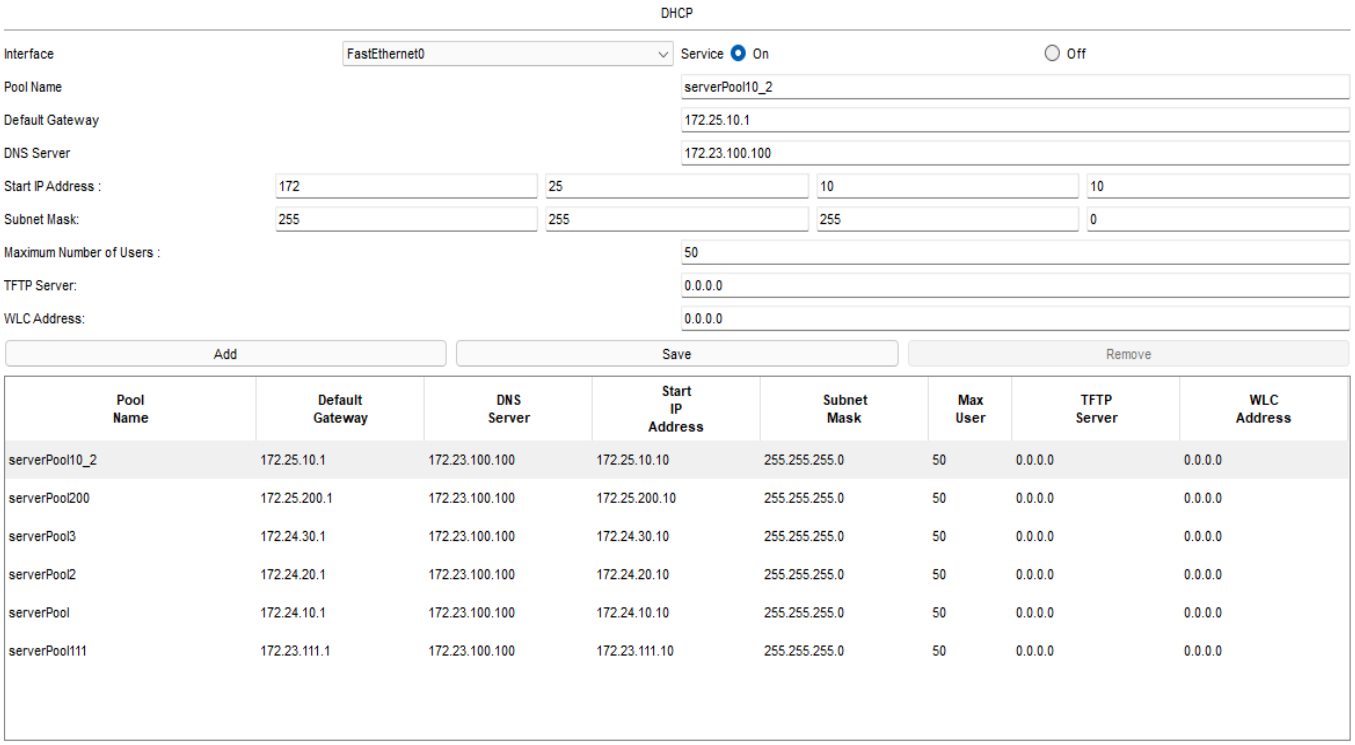
- Tại ServerSW sẽ cấu hình interface cho VLAN và bật chế độ IP routing để định tuyến mạng và VLAN:

```
ServerSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ServerSW(config)#ip routing
ServerSW(config)#int vlan 100
ServerSW(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

ServerSW(config-if)#ip address 172.23.100.1 255.255.255.0
```

- Sau đó thiết lập cho DHCP Server để cấp phát IP cho các VLAN tại các switch:

```
ServerSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ServerSW(config)#ip routing
ServerSW(config)#int vlan 100
ServerSW(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

ServerSW(config-if)#ip address 172.23.100.1 255.255.255.0
```

- Sau đó thiết lập cho DHCP Server để cấp phát IP cho các VLAN tại các switch:



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool10_2	172.25.10.1	172.23.100.100	172.25.10.10	255.255.255.0	50	0.0.0.0	0.0.0.0
serverPool200	172.25.200.1	172.23.100.100	172.25.200.10	255.255.255.0	50	0.0.0.0	0.0.0.0
serverPool3	172.24.30.1	172.23.100.100	172.24.30.10	255.255.255.0	50	0.0.0.0	0.0.0.0
serverPool2	172.24.20.1	172.23.100.100	172.24.20.10	255.255.255.0	50	0.0.0.0	0.0.0.0
serverPool	172.24.10.1	172.23.100.100	172.24.10.10	255.255.255.0	50	0.0.0.0	0.0.0.0
serverPool111	172.23.111.1	172.23.100.100	172.23.111.10	255.255.255.0	50	0.0.0.0	0.0.0.0

Tiến hành bật tính năng routing tại các switch layer 3 khác và tạo thêm VLAN 11 tại CoreSW cho 172.25.10.0/24:

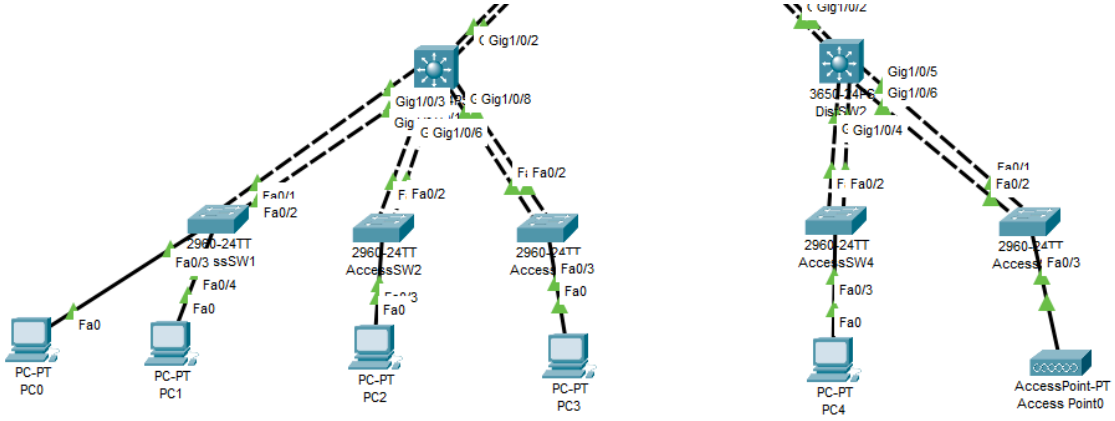
```
CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#ip routing


DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#ip routing


DistSW2>en
DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#ip routing


CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#vlan 11
CoreSW(config-vlan)#ex
```

- Cho các DistSW tạo interface cho VLAN và đặt IP làm default gateway :

```
DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#ip routing
DistSW1(config)#ex
DistSW1#
%SYS-5-CONFIG_I: Configured from console by console

DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#int vlan 10
DistSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

DistSW1(config-if)#ip address 172.24.10.1 255.255.255.0
DistSW1(config-if)#int vlan 20
DistSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

DistSW1(config-if)#ip address 172.24.20.1 255.255.255.0
DistSW1(config-if)#int vlan 30
DistSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

DistSW1(config-if)#ip address 172.24.30.1 255.255.255.0


DistSW2>en
DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#int vlan 200
DistSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up


DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#int vlan 11
DistSW2(config-if)#ip address 172.25.10.1 255.255.255.0
```

- Tiến hành lắp các thiết bị vào các AccessSW:

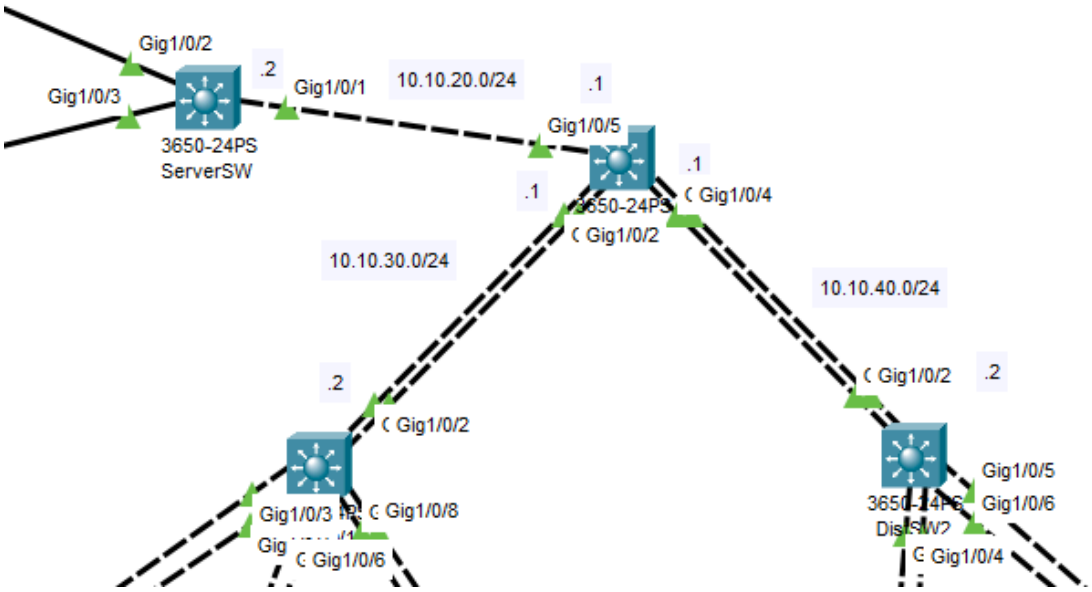
```
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#int vlan 10
DistSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

DistSW1(config-if)#ip address 172.24.10.1 255.255.255.0
DistSW1(config-if)#int vlan 20
DistSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

DistSW1(config-if)#ip address 172.24.20.1 255.255.255.0
DistSW1(config-if)#int vlan 30
DistSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

DistSW1(config-if)#ip address 172.24.30.1 255.255.255.0
```



- Sau đó cho các interface kết nối với các thiết bị đó tham gia vào các VLAN tương ứng như đề bài:

```
AccessSW1>en
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int f0/3
AccessSW1(config-if)#swi
AccessSW1(config-if)#switchport access vlan 10
AccessSW1(config-if)#int f0/4
AccessSW1(config-if)#switchport access vlan 10

AccessSW2>en
AccessSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW2(config)#int f0/3
AccessSW2(config-if)#sw
AccessSW2(config-if)#switchport acc
AccessSW2(config-if)#switchport access vlan 20


AccessSW3>en
AccessSW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW3(config)#int f0/3
AccessSW3(config-if)#switchp
AccessSW3(config-if)#switchport access vlan 30


AccessSW4>en
AccessSW4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW4(config)#int f0/3
AccessSW4(config-if)#sw
AccessSW4(config-if)#switchport ac
AccessSW4(config-if)#switchport access vlan 11


AccessSW5>en
AccessSW5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW5(config)#int f0/3
AccessSW5(config-if)#swi
AccessSW5(config-if)#switchport ac
AccessSW5(config-if)#switchport access vlan 200
```

Để mạng giữa các switch có thể giao tiếp được với nhau, ta phải cấu hình mạng trung gian như sau:



- Với mỗi cổng kết nối giữa các switch sẽ ở chế độ router:

```
CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#int gl/0/5
CoreSW(config-if)#no switchport
CoreSW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up

CoreSW(config-if)#ip address 10.10.20.1 255.255.255.0
CoreSW(config-if)#int po1
CoreSW(config-if)#no switchport
CoreSW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

CoreSW(config-if)#ip address 10.10.30.1 255.255.255.0
CoreSW(config-if)#int po2
CoreSW(config-if)#no switchport
CoreSW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up

CoreSW(config-if)#ip address 10.10.40.1 255.255.255.0
```

```
ServerSW>en
ServerSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ServerSW(config)#int g1/0/1
ServerSW(config-if)#no switchport
ServerSW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

ServerSW(config-if)#ip address 10.10.20.2 255.255.255.0


DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#int po1
DistSW1(config-if)#no switchport
DistSW1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

DistSW1(config-if)#ip address 10.10.30.2 255.255.255.0



DistSW2>en
DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#int po1
DistSW2(config-if)#no switchport
DistSW2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

DistSW2(config-if)#ip address 10.10.40.2 255.255.255.0
```

- Do mặc định các IP này được gán vào VLAN 1 mà nó mặc định down nên cần phải bật VLAN 1 ở mỗi switch lên (đều cấu hình như dưới đây ở các switch):

```
CoreSW#
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#int vlan 1
CoreSW(config-if)#no shut

CoreSW(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

b) Cấu hình định tuyến cho mạng nội bộ (RIP version 2)

Thiết lập định tuyến RIP version 2 tại mỗi switch để các mạng có thể giao tiếp được với nhau bằng việc khai báo các mạng mà tại switch đó kết nối đến.

```
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#router rip
CoreSW(config-router)#version 2
CoreSW(config-router)#network 10.10.20.0
CoreSW(config-router)#network 10.10.30.0
CoreSW(config-router)#network 10.10.40.0
CoreSW(config-router)#no au
CoreSW(config-router)#no auto-summary
```

```
ServerSW(config)#
ServerSW(config)#router rip
ServerSW(config-router)#version 2
ServerSW(config-router)#network 10.10.20.0
ServerSW(config-router)#network 172.23.100.0
ServerSW(config-router)#no au
ServerSW(config-router)#no auto-summary
```

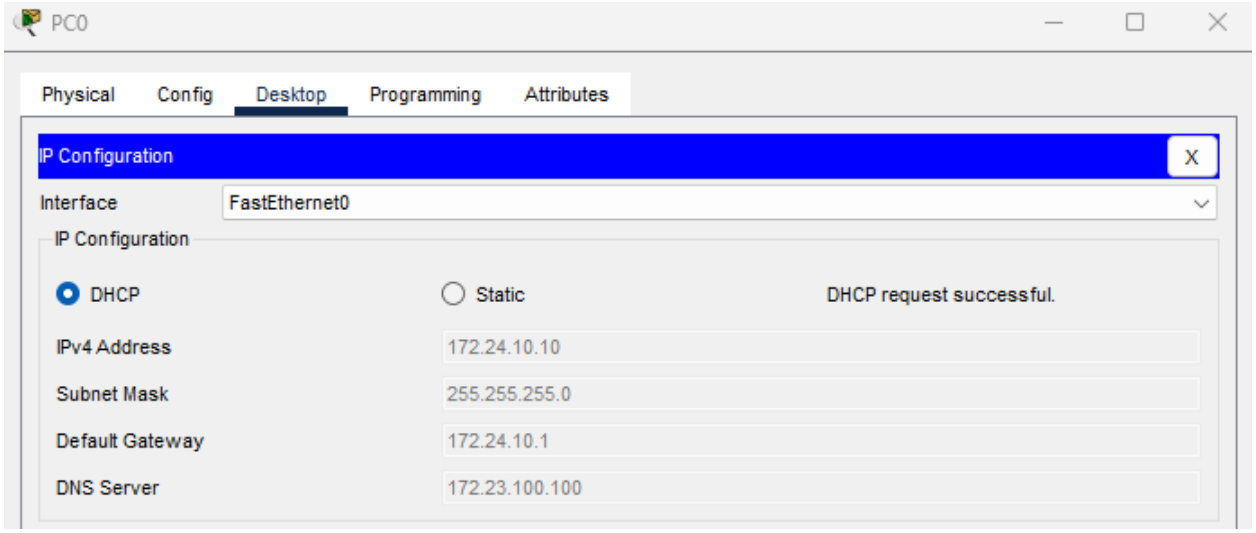
```
DistSW1(config-if)#ip address 10.10.30.2 255.255.255.0
DistSW1(config-if)#
DistSW1(config-if)#ex
DistSW1(config)#
DistSW1(config)#router rip
DistSW1(config-router)#version 2
DistSW1(config-router)#network 10.10.30.0
DistSW1(config-router)#network 172.24.10.0
DistSW1(config-router)#network 172.24.20.0
DistSW1(config-router)#network 172.24.30.0
DistSW1(config-router)#no au
DistSW1(config-router)#no auto-summary
```

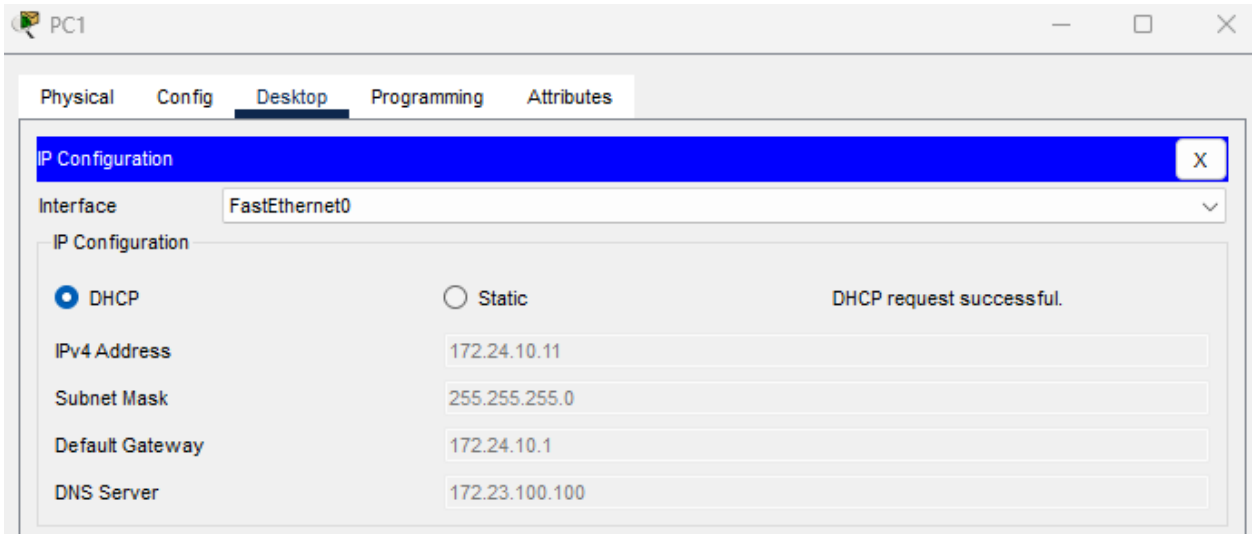
```
DistSW2(config-if)#ip address 10.10.40.2 255.255.255.0
DistSW2(config-if)#ex
DistSW2(config)#
DistSW2(config)#router rip
DistSW2(config-router)#version 2
DistSW2(config-router)#network 10.10.40.0
DistSW2(config-router)#network 172.25.10.0
DistSW2(config-router)#network 172.25.200.0
DistSW2(config-router)#no au
DistSW2(config-router)#no auto-summary
```

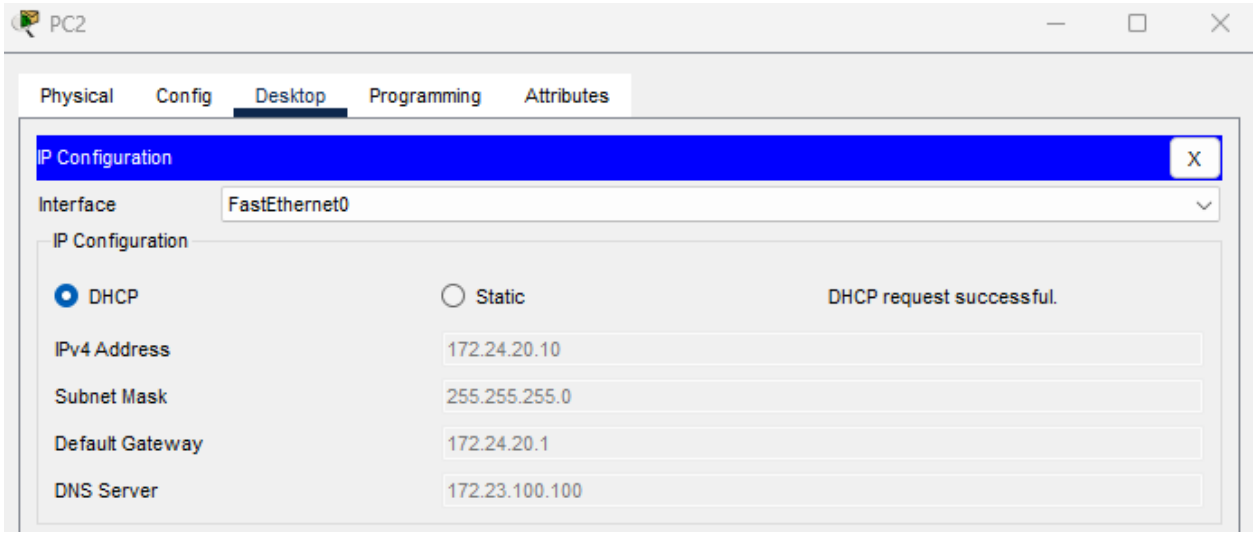
Để có thể nhận IP từ DHCP Server, cần phải thiết lập DHCP Relay. Khi DHCP server nằm trên một VLAN khác hoặc ngoài hệ thống mạng của VLAN, ta cần cấu hình tính năng DHCP Relay tại các DistSW.

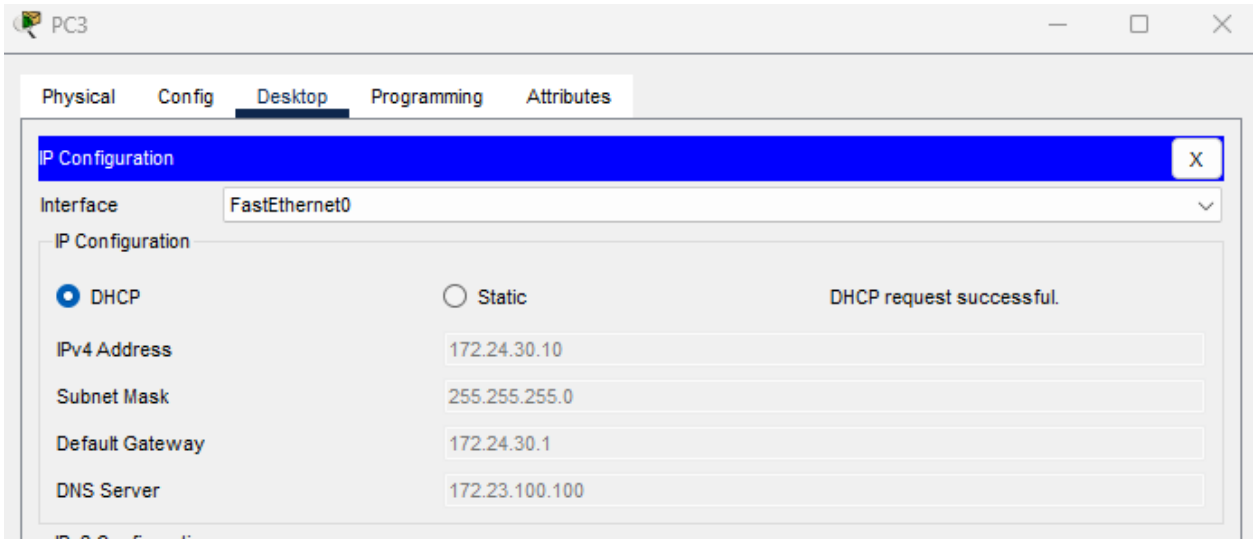
```
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#int vlan 10
DistSW1(config-if)#ip he
DistSW1(config-if)#ip help
DistSW1(config-if)#ip helper-address 172.23.100.200
DistSW1(config-if)#int vlan 20
DistSW1(config-if)#ip helper-address 172.23.100.200
DistSW1(config-if)#int vlan 30
DistSW1(config-if)#ip helper-address 172.23.100.200


DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#int vlan 11
DistSW2(config-if)#ip helper
DistSW2(config-if)#ip helper-address 172.23.100.200
DistSW2(config-if)#int vlan 200
DistSW2(config-if)#ip helper-address 172.23.100.200
```

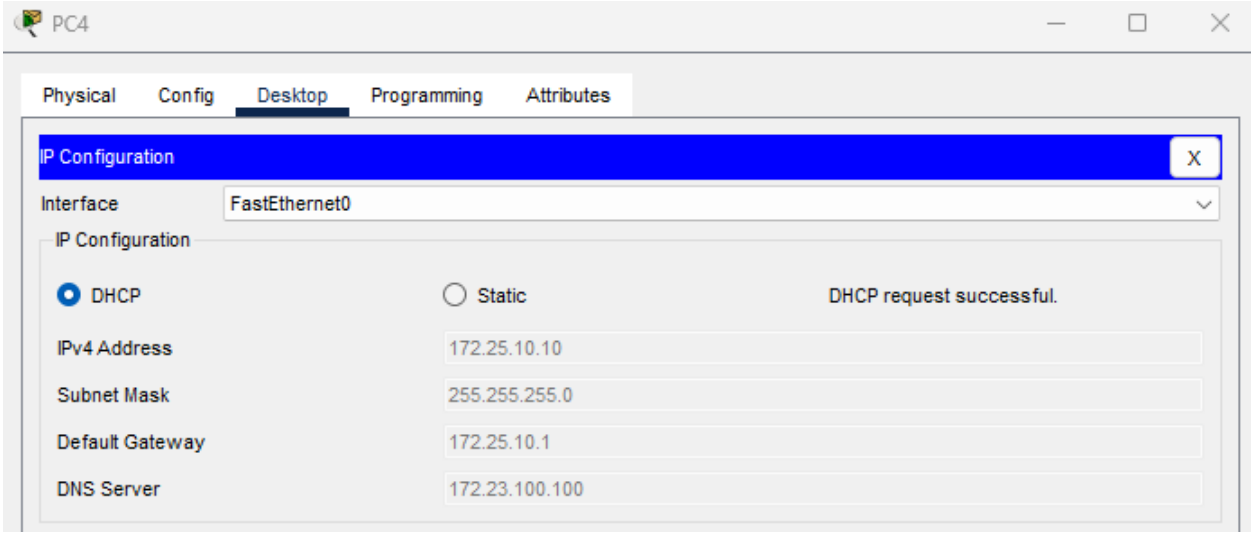
Sau đó thì nhận IP được cấp phát từ DHCP tại các PC thử:



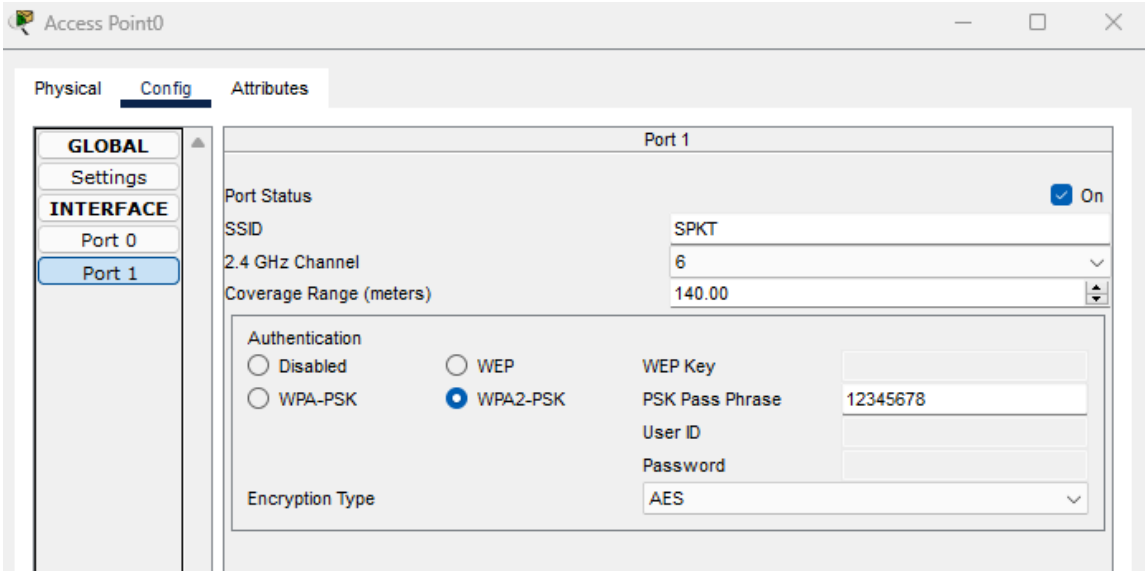

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.24.10.11
Subnet Mask
255.255.255.0
Default Gateway
172.24.10.1
DNS Server
172.23.100.100


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.24.20.10
Subnet Mask
255.255.255.0
Default Gateway
172.24.20.1
DNS Server
172.23.100.100

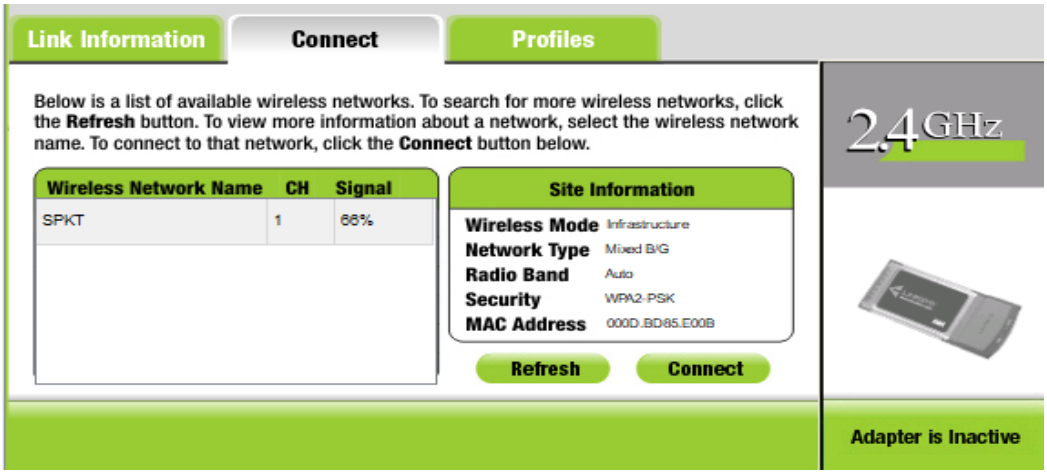

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.24.30.10
Subnet Mask
255.255.255.0
Default Gateway
172.24.30.1
DNS Server
172.23.100.100

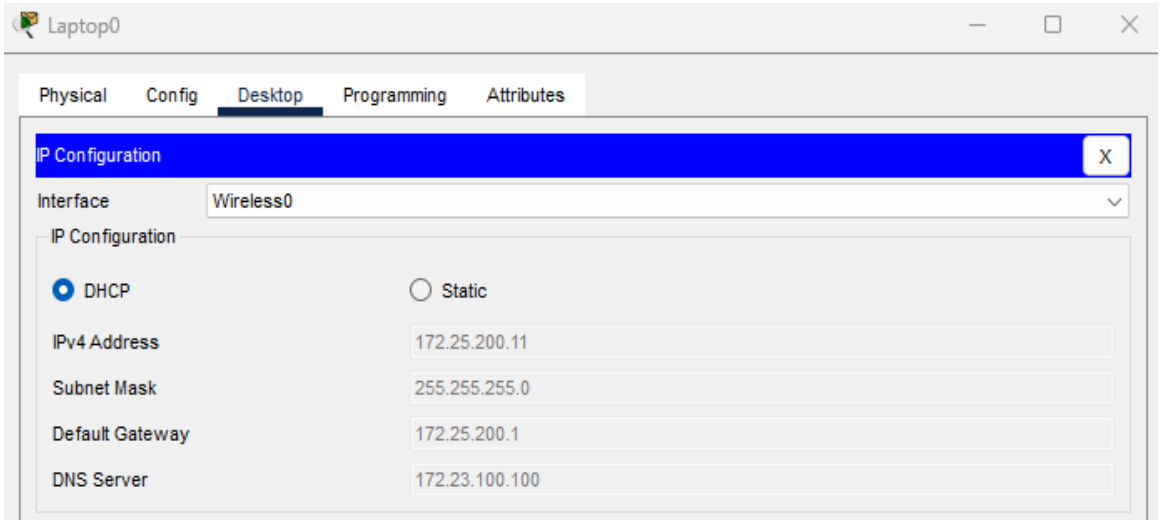


Đối với Access Point ta sẽ thiết lập với SSID là SPKT và mật khẩu là 12345678

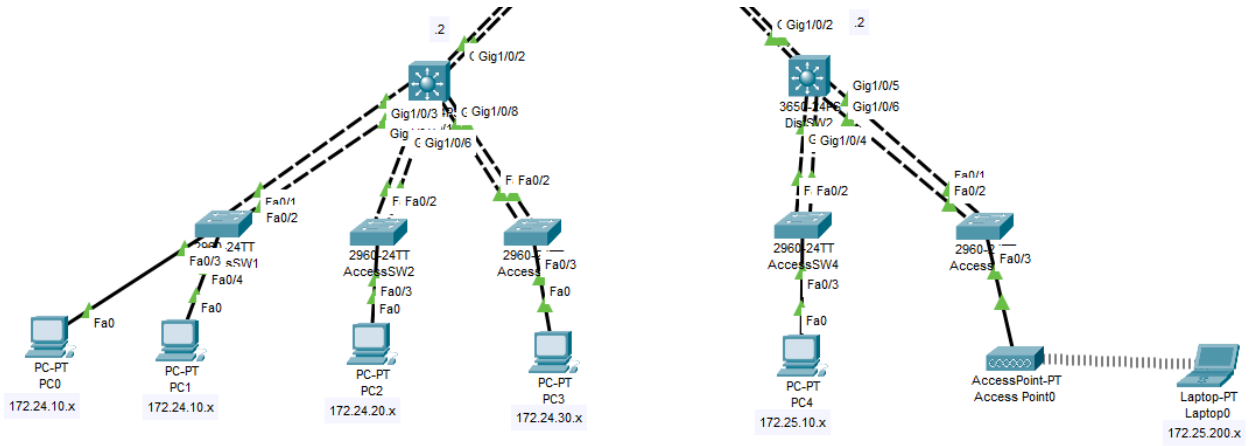


Sau đó để một laptop kết nối vào và nó được cấp phát IP từ DHCP Server thành công:

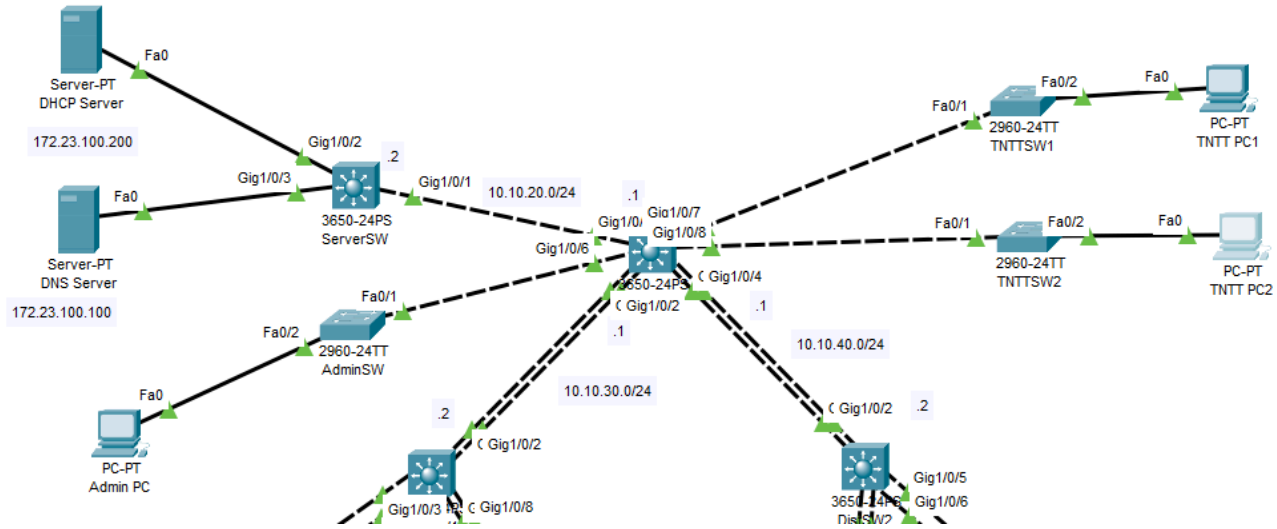




=> Và như vậy đến thời điểm hiện tại ta thu được:



Tiếp đến sẽ cấu hình khu vực quản trị với IP 172.23.111.0/24 thuộc VLAN 111 của CoreSW, và khu vực VPTNTT với IP 172.23.10.0/24 và 172.23.20.0/24 thuộc VLAN 12 và 22 tại CoreSW (Tạo thêm).



```
CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#vlan 12
CoreSW(config-vlan)#vlan 22
CoreSW(config-vlan)#ex
CoreSW(config)#int vlan 111
CoreSW(config-if)#
%LINK-5-CHANGED: Interface Vlan111, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan111, changed state to up

CoreSW(config-if)#ip address 172.23.111.1 255.255.255.0
CoreSW(config-if)#int vlan 12
CoreSW(config-if)#
%LINK-5-CHANGED: Interface Vlan12, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan12, changed state to up

CoreSW(config-if)#ip address 172.23.10.1 255.255.255.0
CoreSW(config-if)#int vlan 22
CoreSW(config-if)#
%LINK-5-CHANGED: Interface Vlan22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan22, changed state to up

CoreSW(config-if)#ip address 172.23.20.1 255.255.255.0


CoreSW(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/7, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to up
```

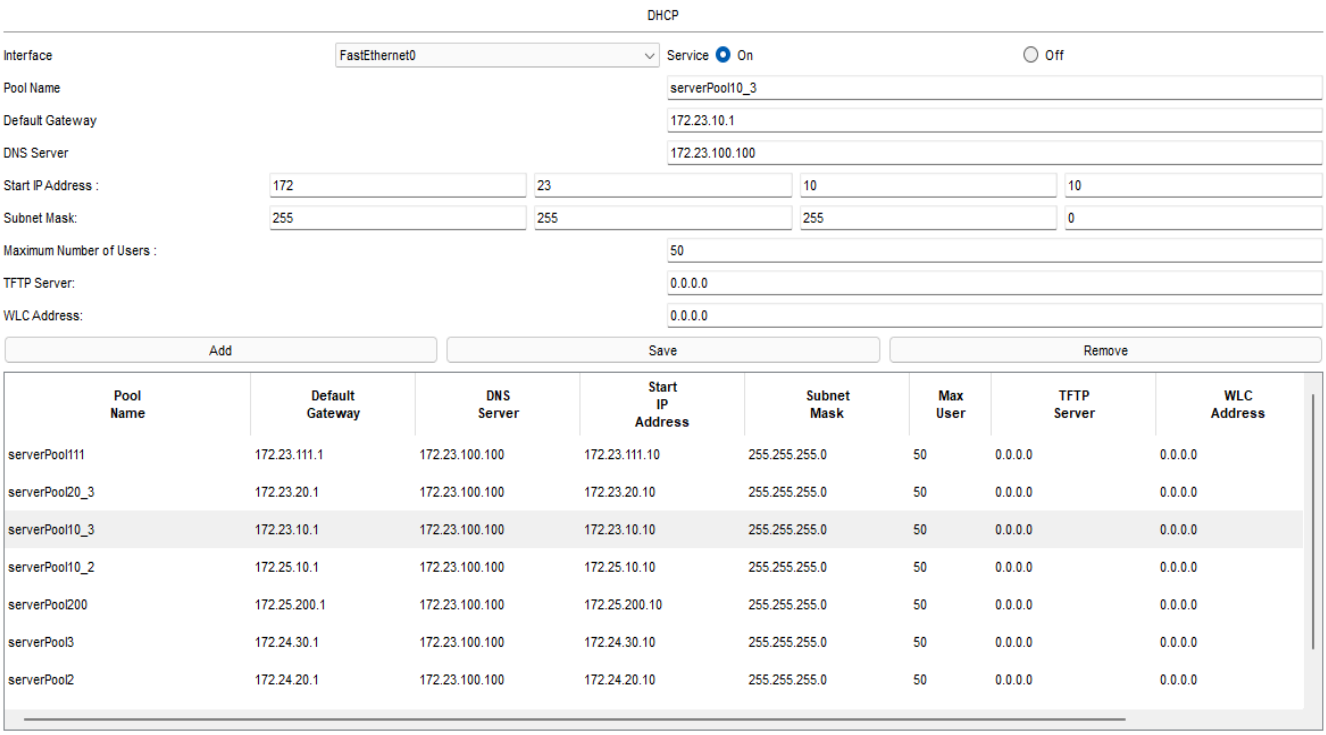
- Thêm những vùng mạng này vào định tuyến RIP của CoreSW:

```
CoreSW(config)#router rip
CoreSW(config-router)#network 172.23.10.0
CoreSW(config-router)#network 172.23.20.0
CoreSW(config-router)#network 172.23.111.0
CoreSW(config-router)#ex
```

- Sau đó cho các switch AdminSW, TNTTSW tham gia vào các VLAN này:

```
AdminSW>en
AdminSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AdminSW(config)#vtp domain CoreSW-VTP
Changing VTP domain name from NULL to CoreSW-VTP
AdminSW(config)#int f0/1
AdminSW(config-if)#swi
AdminSW(config-if)#switchport mode trunk

AdminSW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

AdminSW(config-if)#int f0/2
AdminSW(config-if)#sw
AdminSW(config-if)#switchport access vlan 111


TNTTSW1>en
TNTTSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TNTTSW1(config)#int f0/1
TNTTSW1(config-if)#sw
TNTTSW1(config-if)#switchport mode trunk
TNTTSW1(config-if)#ex
TNTTSW1(config)#vtp domain CoreSW-VTP
Changing VTP domain name from NULL to CoreSW-VTP
TNTTSW1(config)#int f0/2
TNTTSW1(config-if)#switchpor
TNTTSW1(config-if)#switchport ac
TNTTSW1(config-if)#switchport access vlan 12


TNTTSW2>en
TNTTSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TNTTSW2(config)#int f0/1
TNTTSW2(config-if)#sw
TNTTSW2(config-if)#switchport mode trunk
TNTTSW2(config-if)#ex
TNTTSW2(config)#vtp domain CoreSW-VTP
Domain name already set to CoreSW-VTP.
TNTTSW2(config)#int f0/2
TNTTSW2(config-if)#sw
TNTTSW2(config-if)#switchport access vlan 22
```

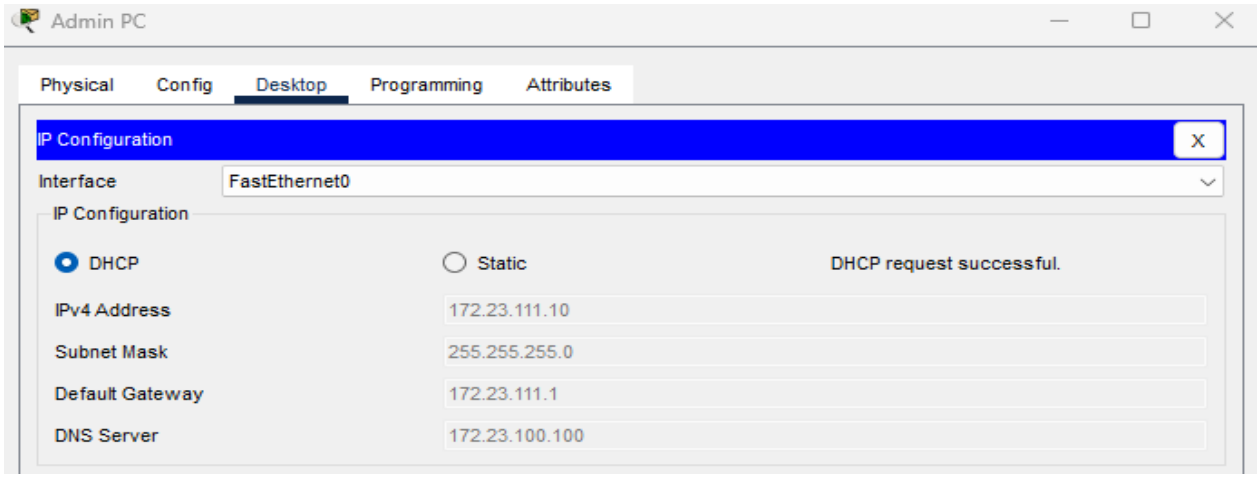
- Cập nhật thêm những vùng mạng trên vào DHCP Pool cho DHCP Server:

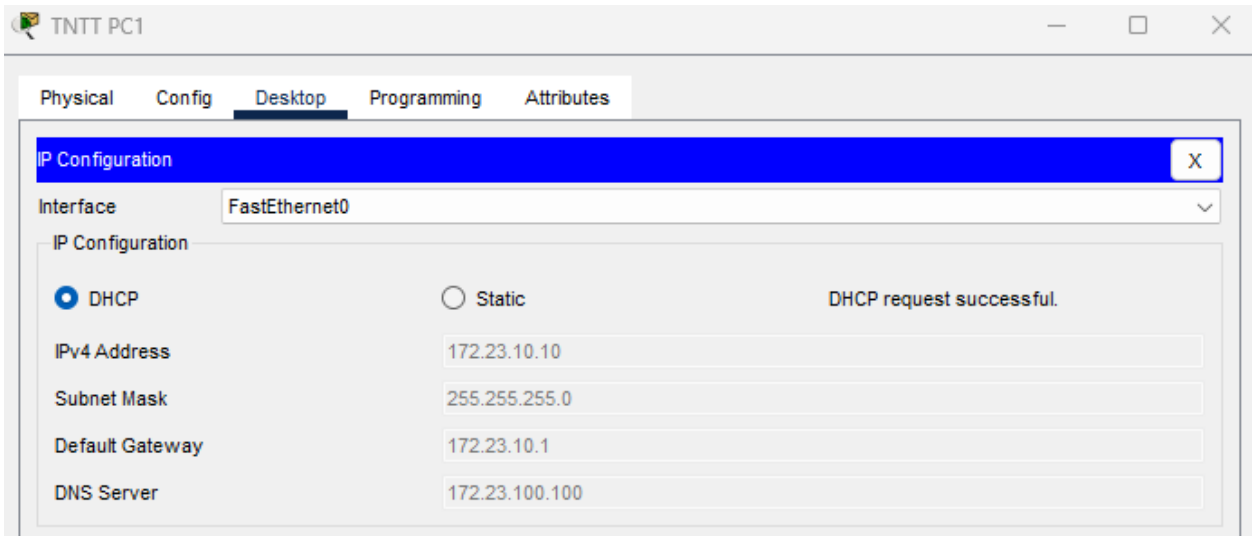


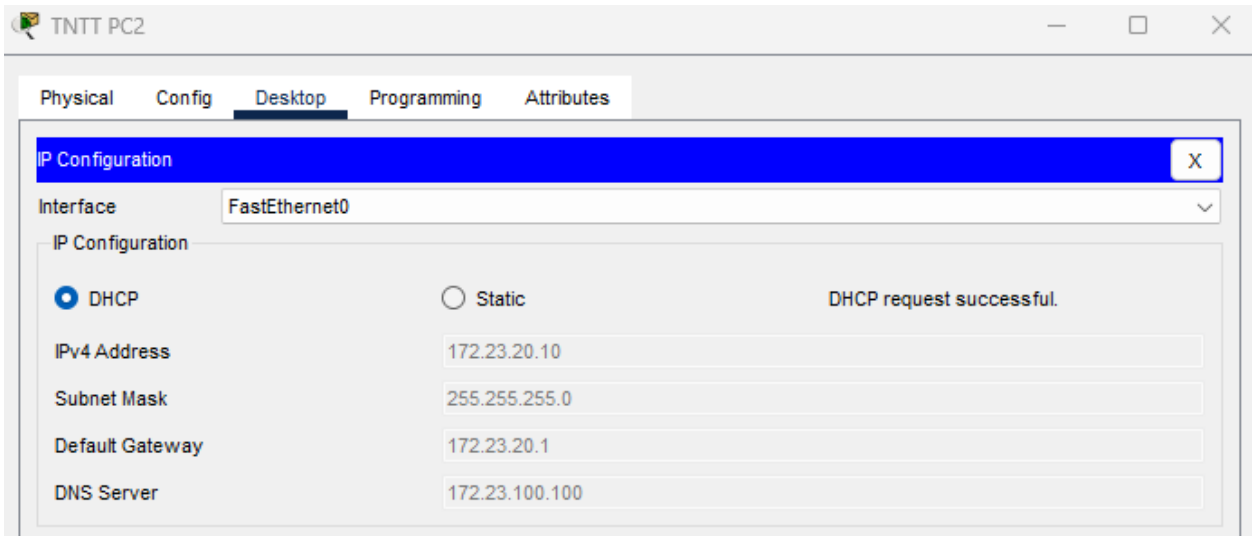
- Sau đó cấu hình CoreSW làm DHCP Relay Agent cho những vùng mạng này

```
CoreSW(config-if-range)#ex
CoreSW(config)#int vlan 12
CoreSW(config-if)#ip helper-a
CoreSW(config-if)#ip helper-address 172.23.100.200
CoreSW(config-if)#int vlan 22
CoreSW(config-if)#ip helper-address 172.23.100.200
CoreSW(config-if)#int vlan 111
CoreSW(config-if)#ip helper-address 172.23.100.200
```

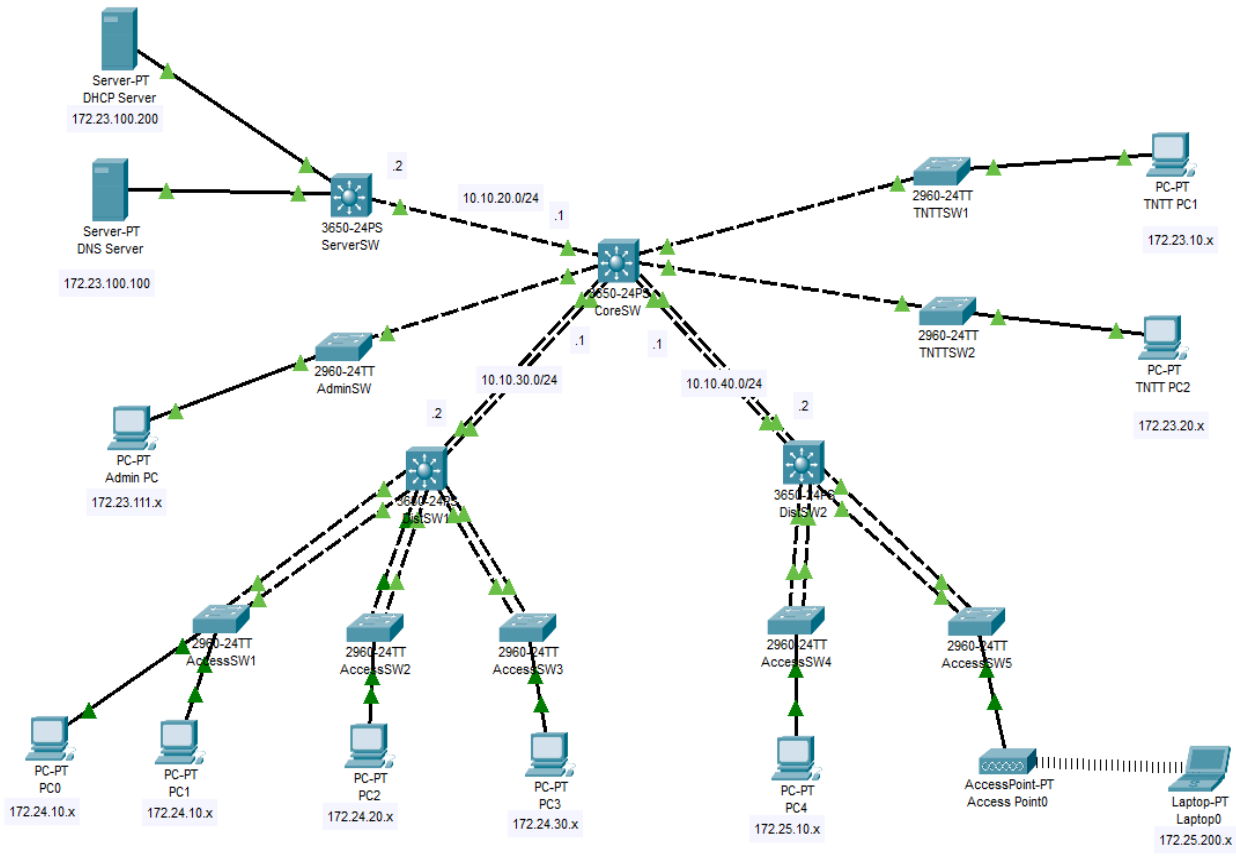
- Thử nhận IP từ DHCP Server từ các máy tính


Admin PC
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.23.111.10
Subnet Mask
255.255.255.0
Default Gateway
172.23.111.1
DNS Server
172.23.100.100

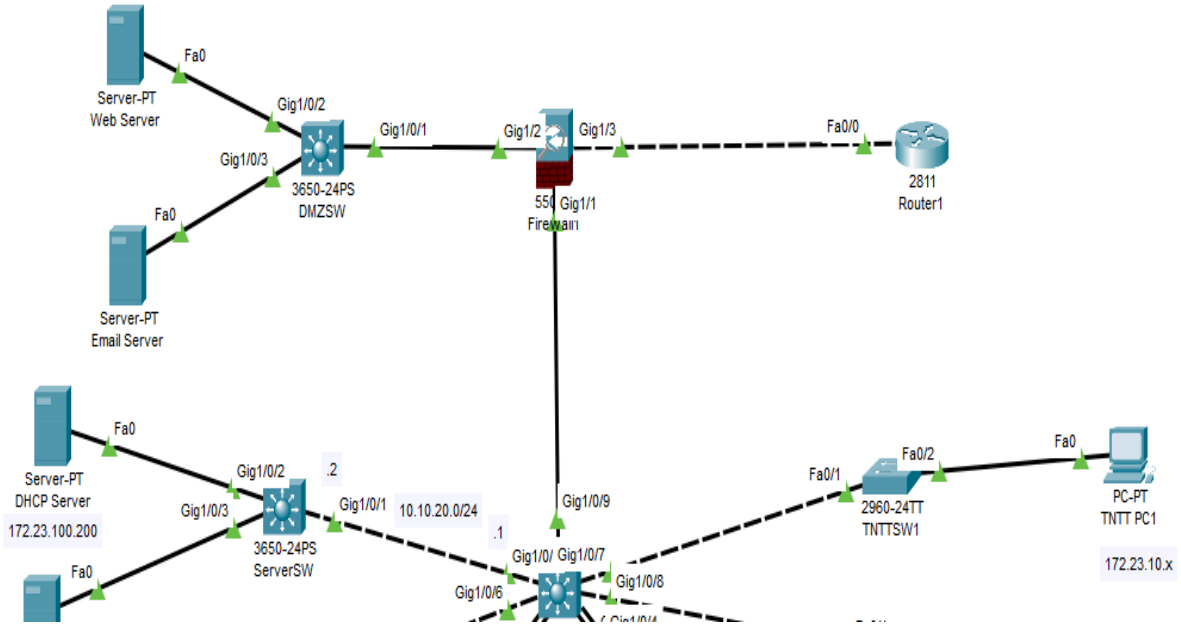

TNTT PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.23.10.10
Subnet Mask
255.255.255.0
Default Gateway
172.23.10.1
DNS Server
172.23.100.100


TNTT PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.23.20.10
Subnet Mask
255.255.255.0
Default Gateway
172.23.20.1
DNS Server
172.23.100.100

=> Như vậy là đã cấu hình thành công mạng nội bộ. Hiện tại sơ đồ mạng của ta thu được như sau:



Tiếp theo là cấu hình cho vùng mạng DMZ, Firewall và Router để đi ra ngoài mạng. Ta sẽ cho vùng mạng tại CoreSW vùng Inside, vùng mạng của các server sẽ là vùng DMZ (vùng mạng trung gian đóng vai trò như một khu vực "đệm" giữa mạng nội bộ (LAN) và mạng bên ngoài), và cuối cùng là vùng mạng tại Router1 để đi ra ngoài internet sẽ là vùng mạng Outside.Ta sẽ đặt IP cũng như nameif và security-level tại các interface của Firewall.

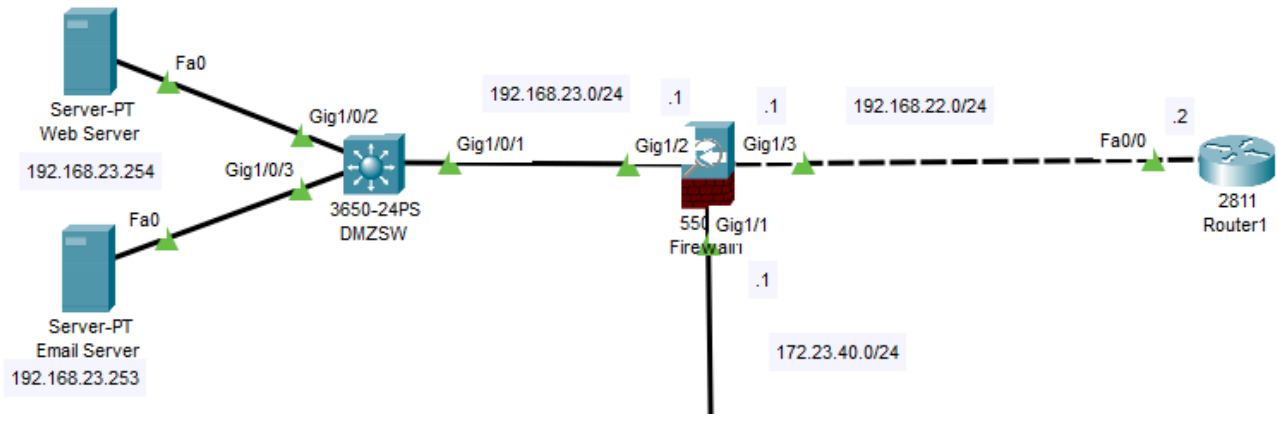



```
Firewalll#conf t
Firewalll(config)#int gl/1
Firewalll(config-if)#ip address 172.23.40.1 255.255.255.0
Firewalll(config-if)#no shut
Firewalll(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
Firewalll(config-if)#int gl/2
Firewalll(config-if)#ip address 192.168.23.1 255.255.255.0
Firewalll(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
Firewalll(config-if)#secu
Firewalll(config-if)#security-level 50
Firewalll(config-if)#no shut

Firewalll(config-if)#int gl/3
Firewalll(config-if)#ip address 192.168.22.1 255.255.255.0
Firewalll(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
Firewalll(config-if)#no shut

%LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to down
```

Với các security-level: 100 đối với inside, 50 đối với dmz và 0 đối với outside. Firewall mặc định sẽ cho phép lưu lượng đi từ security-level cao hơn sang thấp hơn mà không cần ACL. Lưu lượng từ thấp hơn sang cao hơn bị chặn trừ khi có ACL rõ ràng. Sau đó cấu hình tại các vùng mạng xung quanh tương ứng.

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#int f0/0
Router1(config-if)#ip address 192.168.22.2 255.255.255.0
Router1(config-if)#no shut


CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#int gl/0/9
CoreSW(config-if)#no swi
CoreSW(config-if)#no switchport
CoreSW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/9, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/9, changed state to up

CoreSW(config-if)#ip ad
CoreSW(config-if)#ip address 172.23.40.2 255.255.255.0
CoreSW(config-if)#no shut
```

=> Kết quả thu được như dưới đây:



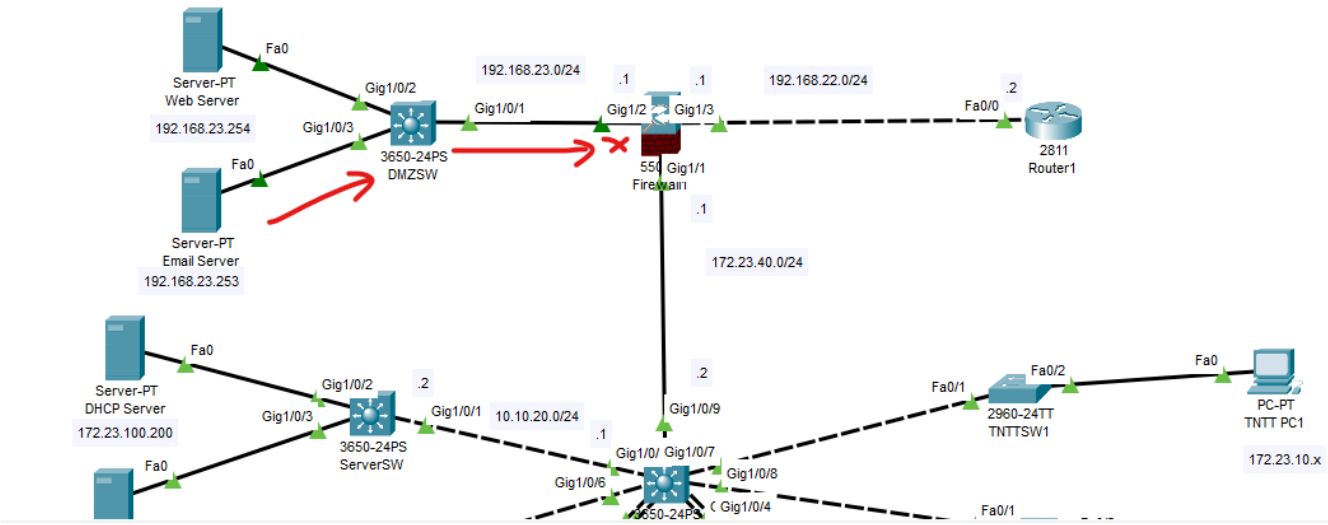
Tiếp đó là cấu hình định tuyến RIP cho Firewall cho các mạng được kết nối với Firewall. Đối với vùng OUTSIDE sẽ làm default route để cho các mạng không có trong bảng định tuyến sẽ đi ra ngoài internet.

```
Firewalll#conf t
Firewalll(config)#router rip
Firewalll(config-router)#version 2
Firewalll(config-router)#network 192.168.23.0
Firewalll(config-router)#network 192.168.22.0
Firewalll(config-router)#network 172.23.40.0
Firewalll(config-router)#no au
Firewalll(config-router)#no auto-summary


Firewalll(config)#route outside 0.0.0.0 0.0.0.0 192.168.22.2
Firewalll(config)#
```

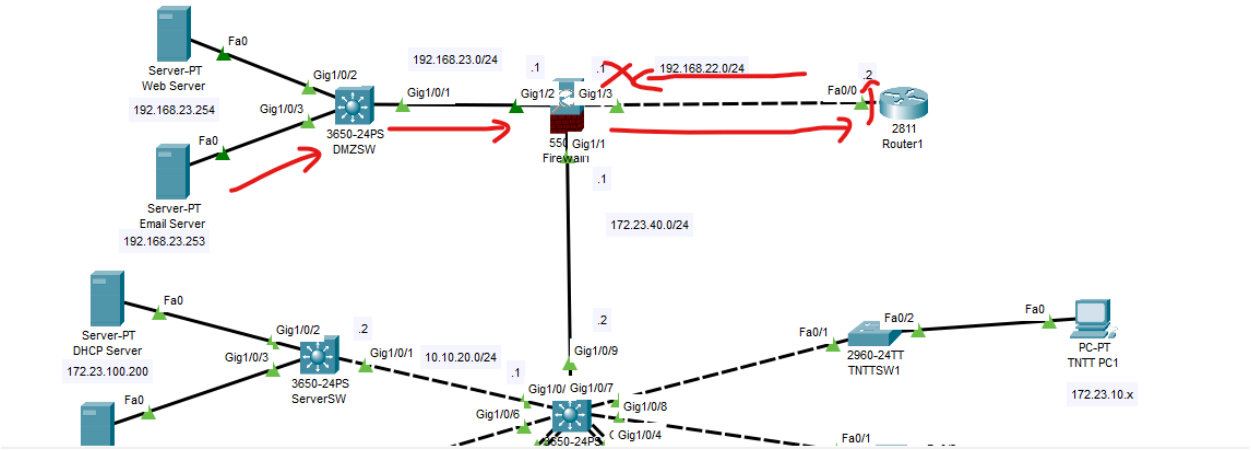
Tại Router1 sẽ cấu hình định tuyến RIP với vùng mạng 192.168.22.0/24, vùng mạng sẽ kết nối với ISP sẽ không được định tuyến.

```
Router1>en
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 192.168.22.0
Router1(config-router)#no au
Router1(config-router)#no auto-summary
```

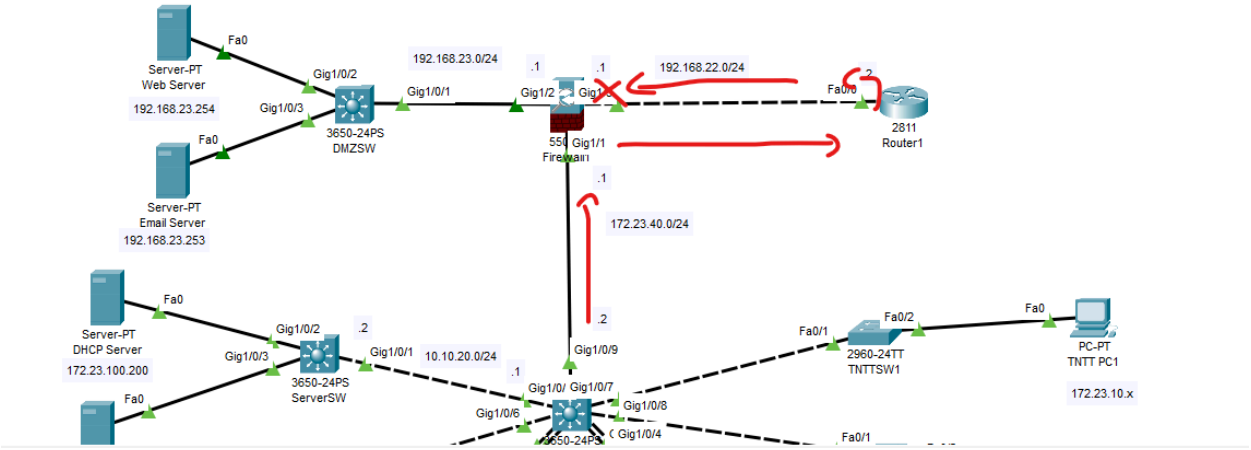
Tuy nhiên hiện tại thì vùng mạng DMZ và INSIDE không thể giao tiếp với nhau, vì các gói tin sẽ đi từ vùng có security-level cao xuống thấp được những ngược lại thì không được. Vùng DMZ có security-level là 50 còn INSIDE là 100, nên khi gói tin đi tới Firewall sẽ bị chặn lại:



Tương tự với vùng mạng từ DMZ ra OUTSIDE, do OUTSIDE có security-level thấp hơn nên khi gói tin phản hồi tới Firewall thì cũng bị chặn lại:



Vùng INSIDE ra OUTSIDE cũng tương tự vậy:



=> Vì vậy ta sẽ phải cấu hình ACL cho Firewall để cho các gói tin có thể đi qua (Tất cả các giao thức). Phần cấu hình bảo mật sẽ được cấu hình sau.

Tạm thời ta sẽ cho tất cả gói tin đi qua để dễ kiểm tra.

```
Firewalll#conf t
Firewalll(config)#access-li
Firewalll(config)#access-list PERMIT_ALL ex
Firewalll(config)#access-list PERMIT_ALL extended permit ip any any
```

Với access-lists trên sẽ cho phép tất cả lưu lượng giữa bất kỳ nguồn và bất kỳ đích (tất cả giao thức), sau đó gán vào access-group

```
Firewalll(config)#access-gr
Firewalll(config)#access-group PERMIT_ALL out int inside
Firewalll(config)#access-group PERMIT_ALL out int dmz
```

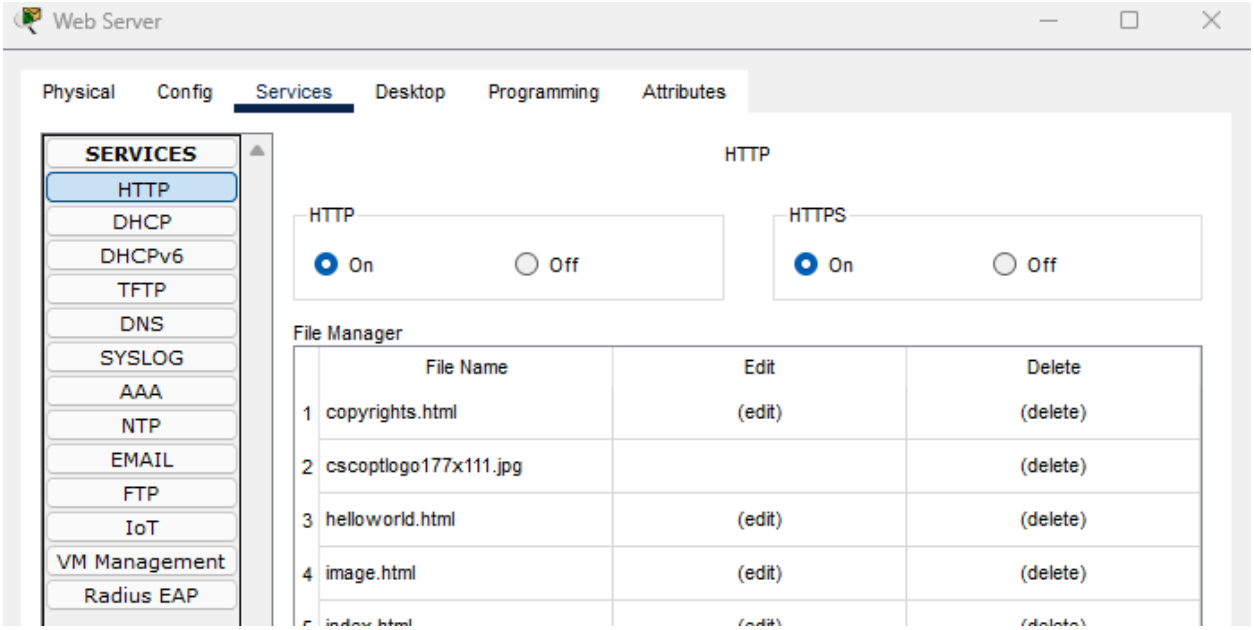
Với các lệnh trên sẽ áp dụng ACL cho lưu lượng đi ra interface INSIDE và DMZ, nghĩa là sẽ không còn bị ràng buộc security-level từ thấp không đi sang cao nữa. Bây giờ sẽ dùng máy tính từ mạng 172.24.10.0/24 (Từ vùng INSIDE) ping ra thử vùng DMZ và OUTSIDE:

```
C:\>ping 192.168.23.254

Pinging 192.168.23.254 with 32 bytes of data:

Reply from 192.168.23.254: bytes=32 time<1ms TTL=125
Reply from 192.168.23.254: bytes=32 time<1ms TTL=125
Reply from 192.168.23.254: bytes=32 time=16ms TTL=125
Reply from 192.168.23.254: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.23.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>ping 192.168.22.2

Pinging 192.168.22.2 with 32 bytes of data:

Reply from 192.168.22.2: bytes=32 time<1ms TTL=252
Reply from 192.168.22.2: bytes=32 time=10ms TTL=252
Reply from 192.168.22.2: bytes=32 time=10ms TTL=252
Reply from 192.168.22.2: bytes=32 time=10ms TTL=252

Ping statistics for 192.168.22.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 7ms
```

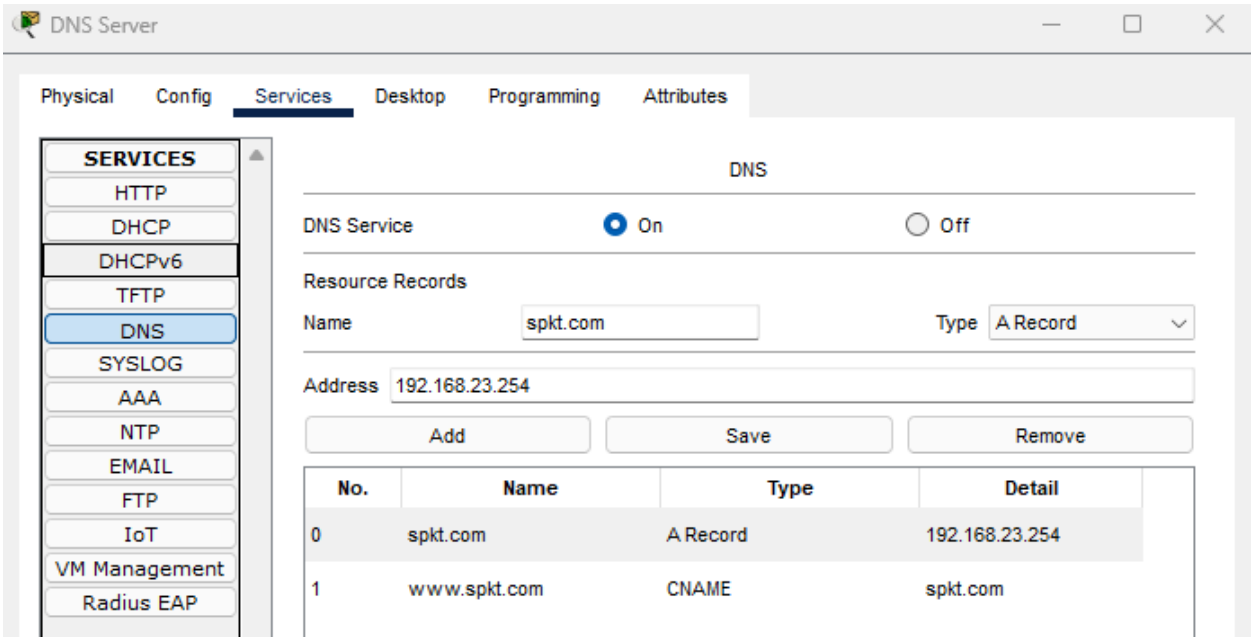
=> Như vậy là đã cấu hình thành công.

c) Cấu hình Web Server và Email Server

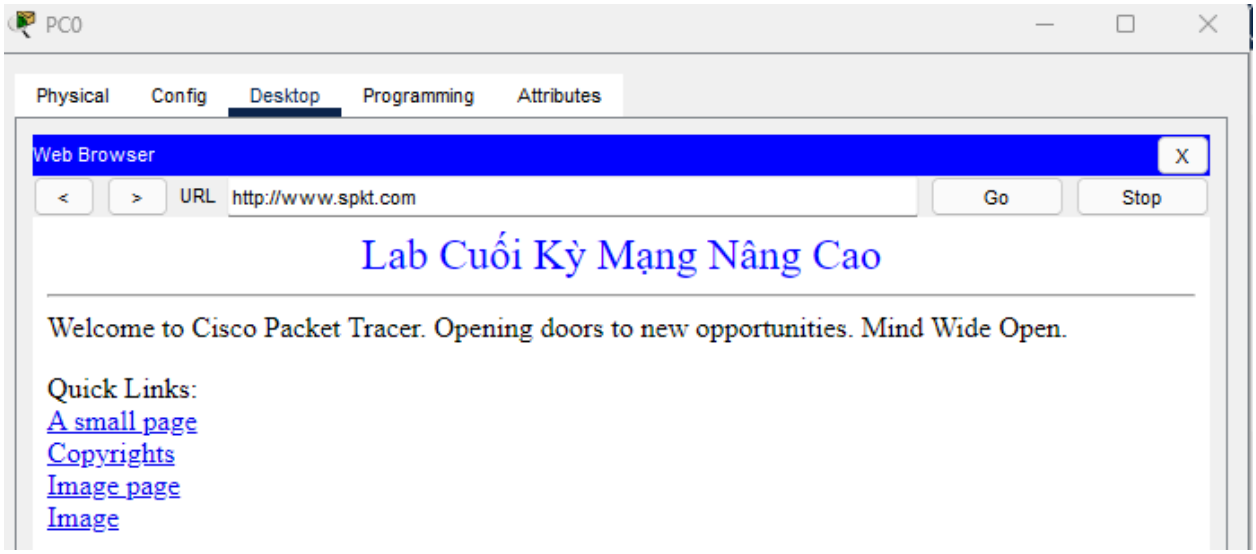
Đầu tiên tiến hành bật dịch vụ HTTP tại Web Server:



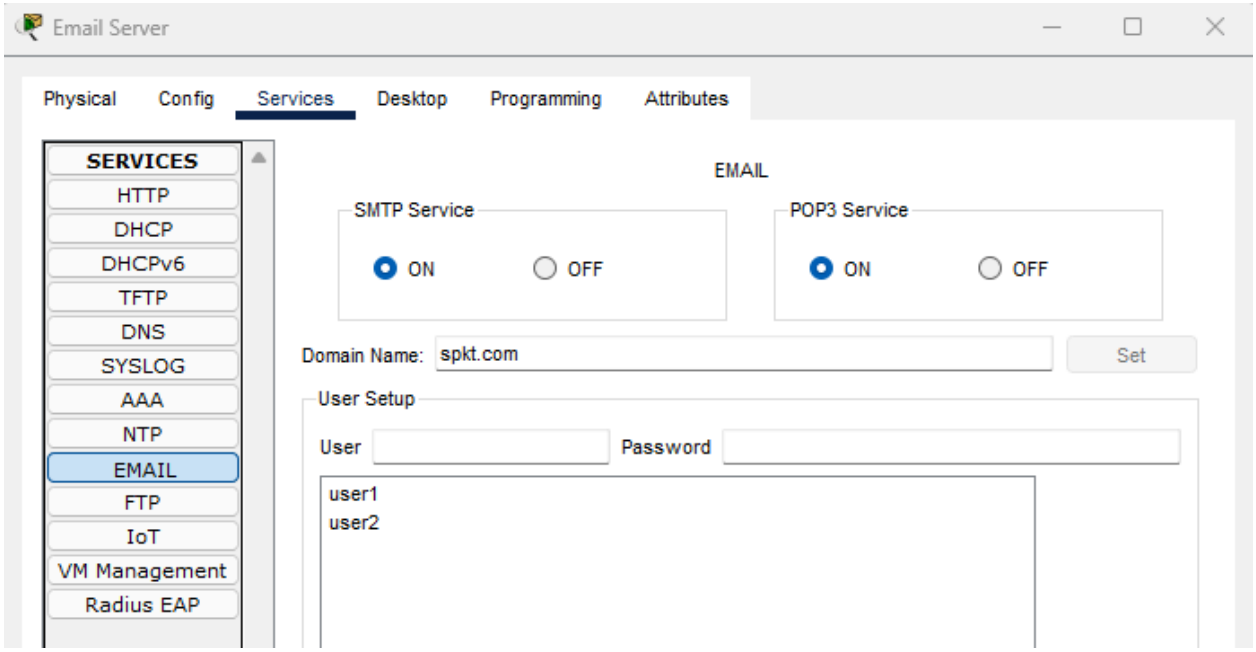
Tại DNS Server sẽ thêm vào A Record và CNAME để thành tên miền spkt.com và www.spkt.com:

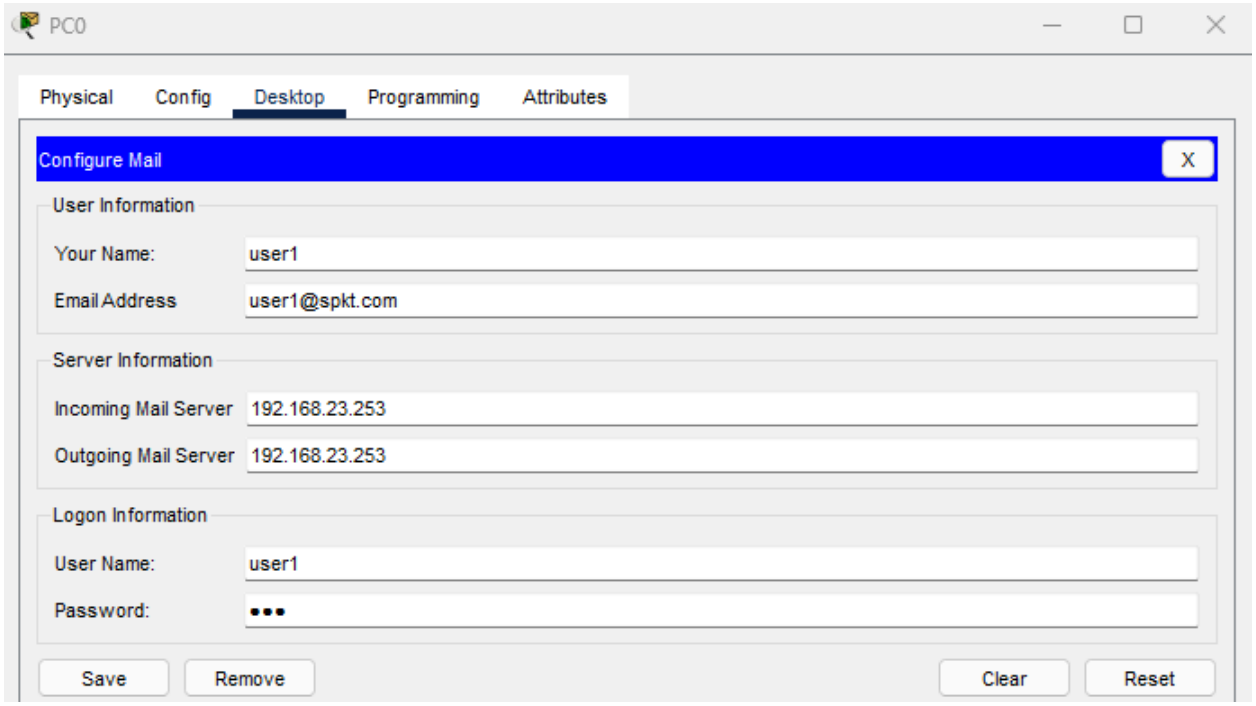


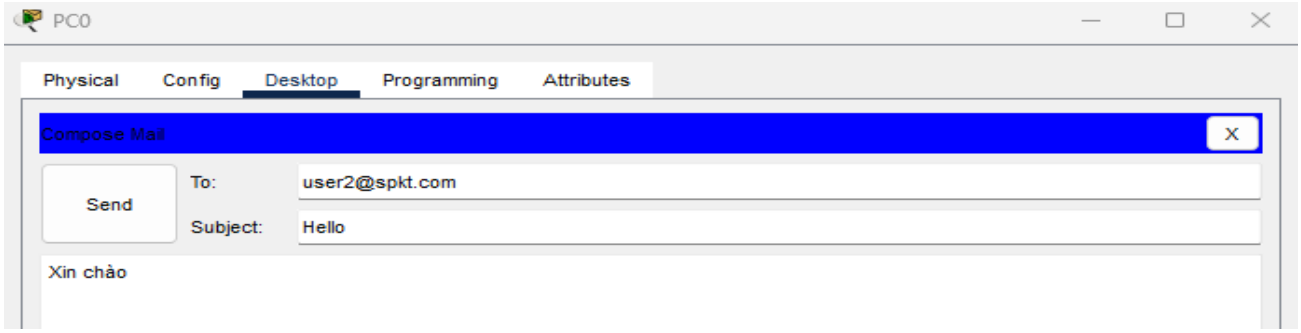
Thử truy cập từ client:

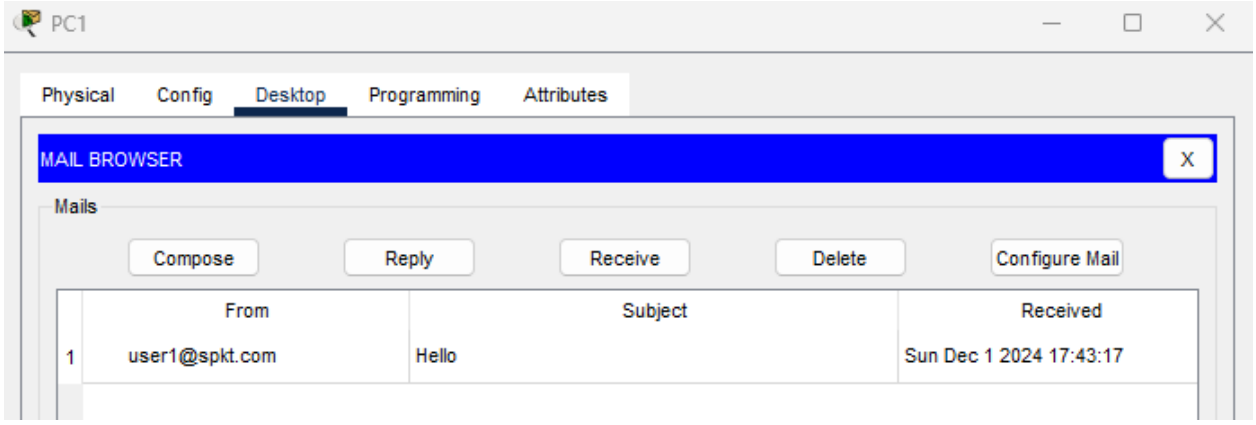


Với Email Server thì sẽ thiết lập tên miền cũng là spkt.com và tạo 2 user và thử nghiệm kết quả bằng cách gửi mail qua lại:



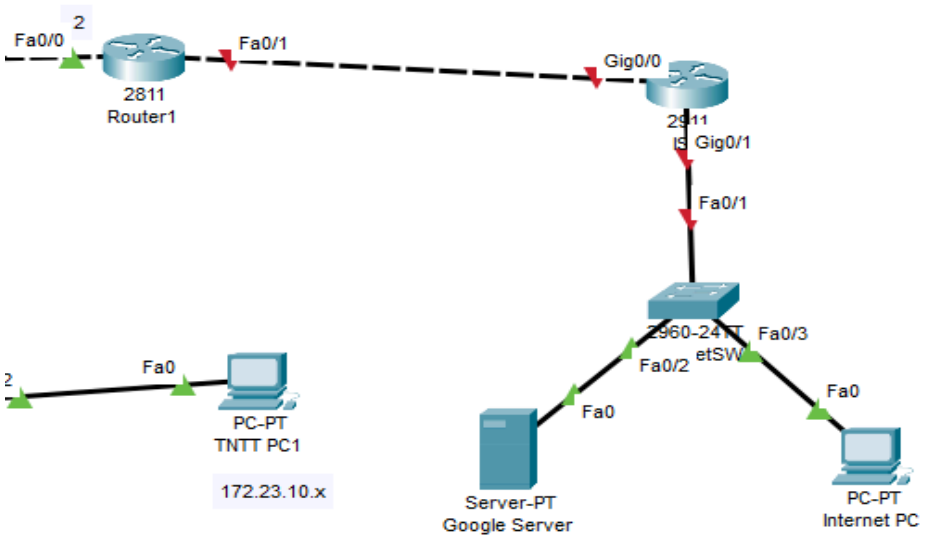

PC0
Physical
Config
Desktop
Programming
Attributes
Configure Mail
X
User Information
Your Name:
user1
Email Address
user1@spkt.com
Server Information
Incoming Mail Server
192.168.23.253
Outgoing Mail Server
192.168.23.253
Logon Information
User Name:
user1
Password:
Save
Remove
Clear
Reset


PC0
Physical
Config
Desktop
Programming
Attributes
Compose Mail
X
Send
To:
user2@spkt.com
Subject:
Hello
Xin chào


PC1
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
X
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
user1@spkt.com
Hello
Sun Dec 1 2024 17:43:17

d) Cấu hình static NAT và PAT (static NAT cho phép người dùng bên ngoài internet truy cập vào Web Server và Email Server)

Trước tiên sẽ thiết lập ISP để giả lập mạng bên ngoài internet:



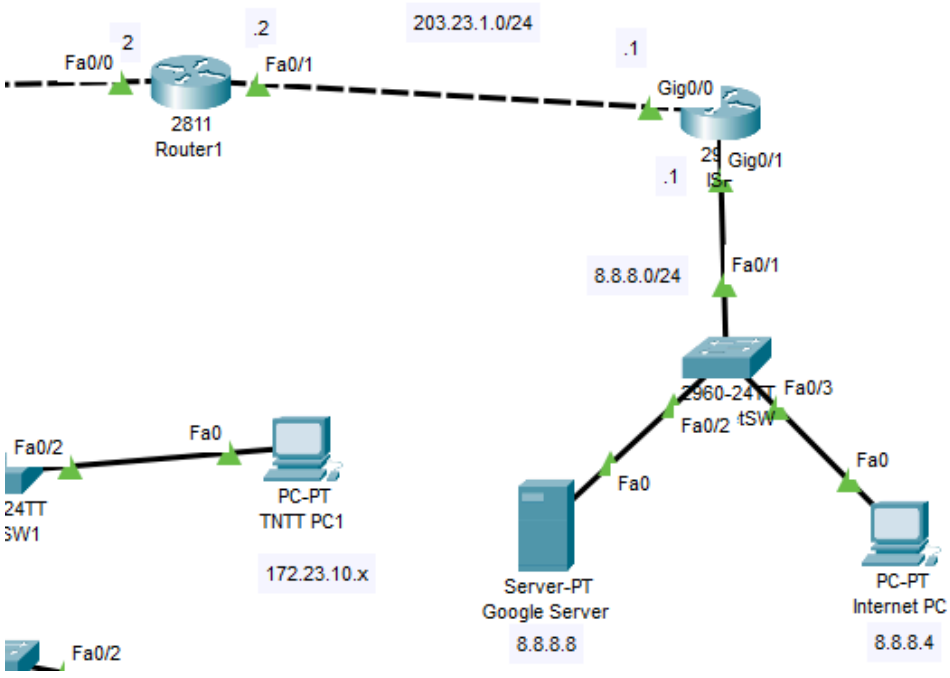

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#int g0/0
ISP(config-if)#ip address 203.23.1.1 255.255.255.0
ISP(config-if)#no shut

ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

ISP(config-if)#int g0/1
ISP(config-if)#ip address 8.8.8.1 255.255.255.0
ISP(config-if)#no shut

ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Tại Router1 cũng thiết lập IP public đi ra ngoài ISP và đồng thời thiết lập default route để cho các gói tin không có trong bảng định tuyến sẽ đi ra ngoài internet:

```
Router1>en
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#int f0/1
Router1(config-if)#ip address 203.23.1.2 255.255.255.0
Router1(config-if)#no shut

Router1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router1(config-if)#ex
Router1(config)#ip route 0.0.0.0 0.0.0.0 f0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
```

Đồng thời cũng đặt default route cho mạng internet để từ ngoài internet có thể truy cập Web Server và Email Server của Router1 (giả lập). Sau đó đặt IP cho các máy bên ngoài internet và ta được:

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
```



Tiền hành thiết lập NAT inside và outside cho Router1:

```
Router1>en
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#int f0/0
Router1(config-if)#ip nat inside
Router1(config-if)#int f0/1
Router1(config-if)#ip nat outside
```

Ở đây ta sẽ cấu hình NAT cho Web Server và Email Server để cung cấp các dịch vụ Web, Email để người dùng ở ngoài Internet có thể sử dụng được. Để cấu hình như vậy thì sẽ phải dùng static NAT tại Router1. Với IP public của Web Server (local IP 192.168.23.254) là 4.4.4.4 và Email Server (local IP 192.168.23.253) là 5.5.5.5:

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#ip nat inside sou
Router1(config)#ip nat inside source static 192.168.23.254 4.4.4.4
Router1(config)#ip nat inside source static 192.168.23.253 5.5.5.5
```

- Sau đó thử dùng Web Server ping ra 8.8.8.8:

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.
Reply from 8.8.8.8: bytes=32 time<1ms TTL=125
Reply from 8.8.8.8: bytes=32 time<1ms TTL=125
Reply from 8.8.8.8: bytes=32 time<1ms TTL=125

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Kiểm tra bảng NAT:

```
Router1#show ip na
Router1#show ip nat tr
Router1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 4.4.4.4:5         192.168.23.254:5   8.8.8.8:5          8.8.8.8:5
icmp 4.4.4.4:6         192.168.23.254:6   8.8.8.8:6          8.8.8.8:6
icmp 4.4.4.4:7         192.168.23.254:7   8.8.8.8:7          8.8.8.8:7
icmp 4.4.4.4:8         192.168.23.254:8   8.8.8.8:8          8.8.8.8:8
---  4.4.4.4           192.168.23.254     ---                ---
---  5.5.5.5           192.168.23.253     ---                ---
```

- Truy cập 4.4.4.4 từ máy bên ngoài Internet (8.8.8.4).

=> Như vậy là đã thiết lập static NAT cho các máy bên ngoài internet có thể truy cập vào Web Server và Email Server thành công.

Tiếp đến là cấu hình NAT Overloading (PAT) cho các máy bên trong mạng nội bộ ra ngoài internet (từ bên ngoài sẽ không truy cập vào được, chỉ từ trong ra ngoài và nhận về gói tin do không có public IP cho từng thiết bị).Để làm như vậy ta sẽ tạo access-list cho các vùng mạng endpoint bên trong (172.23.0.0/16, 172.24.0.0/16, 172.25.0.0/16).

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#access-list 10 permit 172.23.0.0 0.0.255.255
Router1(config)#access-list 11 permit 172.24.0.0 0.0.255.255
Router1(config)#access-list 12 permit 172.25.0.0 0.0.255.255
```

Sau đó áp dụng các access-list trên vào NAT inside overload và thiết lập default route tại các switch layer 3 để dẫn ra bên ngoài internet đối với các mạng không có trong bảng định tuyến tại các switch đó.

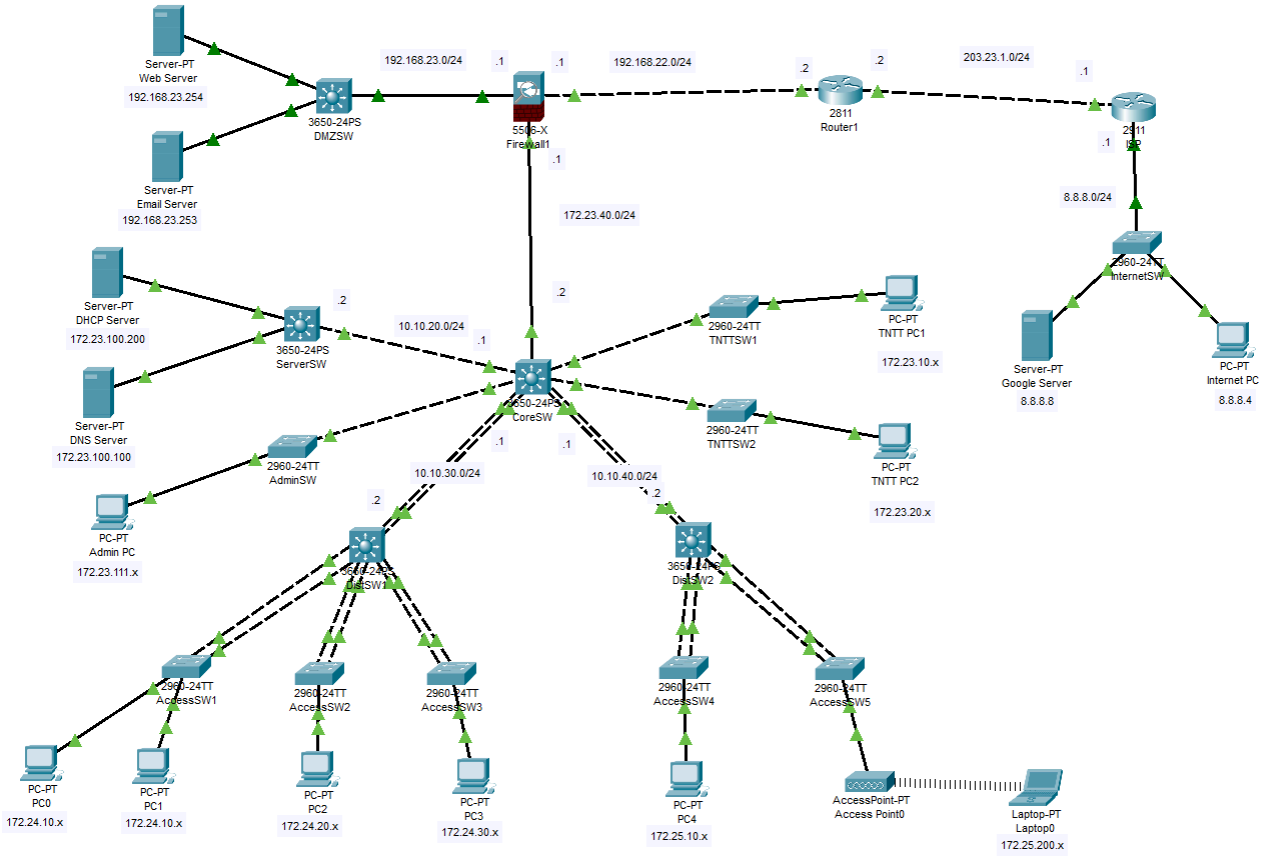
```
Router1(config)#ip nat in
Router1(config)#ip nat inside so
Router1(config)#ip nat inside source li
Router1(config)#ip nat inside source list 10 i
Router1(config)#ip nat inside source list 10 interface f0/1 o
Router1(config)#ip nat inside source list 10 interface f0/1 overload
Router1(config)#ip nat inside source list 11 interface f0/1 overload
Router1(config)#ip nat inside source list 12 interface f0/1 overload


DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#ip route 0.0.0.0 0.0.0.0 10.10.30.1


DistSW2>en
DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#ip route 0.0.0.0 0.0.0.0 10.10.40.1


ServerSW>en
ServerSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ServerSW(config)#ip route 0.0.0.0 0.0.0.0 10.10.20.1


CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#ip route 0.0.0.0 0.0.0.0 172.23.40.1
```

Dùng các máy trong mạng nội bộ ping ra bên ngoài (8.8.8.8) rồi kiểm tra bảng NAT:

```
Router1#show ip nat
Router1#show ip nat tr
Router1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.23.1.2:1024   172.23.20.10:1     8.8.8.8:1          8.8.8.8:1024
icmp 203.23.1.2:1025   172.23.20.10:2     8.8.8.8:2          8.8.8.8:1025
icmp 203.23.1.2:1026   172.23.20.10:3     8.8.8.8:3          8.8.8.8:1026
icmp 203.23.1.2:1027   172.23.20.10:4     8.8.8.8:4          8.8.8.8:1027
icmp 203.23.1.2:18     172.24.10.11:18    8.8.8.8:18         8.8.8.8:18
icmp 203.23.1.2:19     172.24.10.11:19    8.8.8.8:19         8.8.8.8:19
icmp 203.23.1.2:1      172.23.100.100:1   8.8.8.8:1          8.8.8.8:1
icmp 203.23.1.2:20     172.24.10.11:20    8.8.8.8:20         8.8.8.8:20
icmp 203.23.1.2:2      172.23.100.100:2   8.8.8.8:2          8.8.8.8:2
icmp 203.23.1.2:3      172.23.100.100:3   8.8.8.8:3          8.8.8.8:3
icmp 203.23.1.2:4      172.23.100.100:4   8.8.8.8:4          8.8.8.8:4
---  4.4.4.4           192.168.23.254     ---                ---
---  5.5.5.5           192.168.23.253     ---                ---
tcp 4.4.4.4:80         192.168.23.254:80  8.8.8.4:1025       8.8.8.4:1025
```

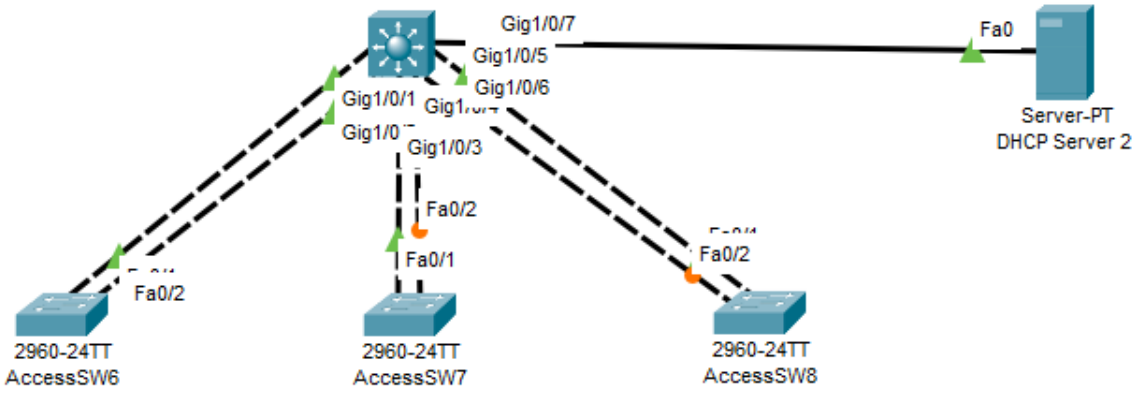
=> Như vậy là đã thiết lập NAT Overload (PAT) thành công.

=> Kết quả thu được đến hiện tại như sau:



e) Cấu hình cho phần mạng LAN bên phải

Cấu hình tại đây cũng giống như sơ đồ mạng ở trên nên sẽ không đi vào quá chi tiết. Trước tiên ta có sơ đồ (CoreSW2):



- Cấu hình port-channel và trunk cho các thiết bị:

```
CoreSW2(config-if-range)#int range gl/0/3, gl/0/4
CoreSW2(config-if-range)#channel-group 2 mode active
CoreSW2(config-if-range)#
Creating a port-channel interface Port-channel 2


CoreSW2(config-if-range)#int range gl/0/5, gl/0/6
CoreSW2(config-if-range)#channel-group 3 mode active
CoreSW2(config-if-range)#
Creating a port-channel interface Port-channel 3


CoreSW2(config-if-range)#int range gl/0/5, gl/0/6
CoreSW2(config-if-range)#channel-group 3 mode active
CoreSW2(config-if-range)#
Creating a port-channel interface Port-channel 3


CoreSW2(config-if-range)#ex
CoreSW2(config)#int po1
CoreSW2(config-if)#sw
CoreSW2(config-if)#switchport mode trunk
CoreSW2(config-if)#int po2
CoreSW2(config-if)#switchport mode trunk
CoreSW2(config-if)#int po3
CoreSW2(config-if)#switchport mode trunk
```

- Tại các AccessSW đều làm như nhau:

```
AccessSW6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW6(config)#int range f0/1, f0/2
AccessSW6(config-if-range)#channel-group 1 mode active
AccessSW6(config-if-range)#
Creating a port-channel interface Port-channel 1


AccessSW6(config-if-range)#int po1
AccessSW6(config-if)#switchpo
AccessSW6(config-if)#switchport mode trunk
```

- Tạo VTP Domain tại CoreSW2 và cho các AccessSW gia nhập:

```
CoreSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW2(config)#vtp domain CoreSW2-VTP
Changing VTP domain name from NULL to CoreSW2-VTP


AccessSW6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW6(config)#vtp domain CoreSW2-VTP
Domain name already set to CoreSW2-VTP.
```

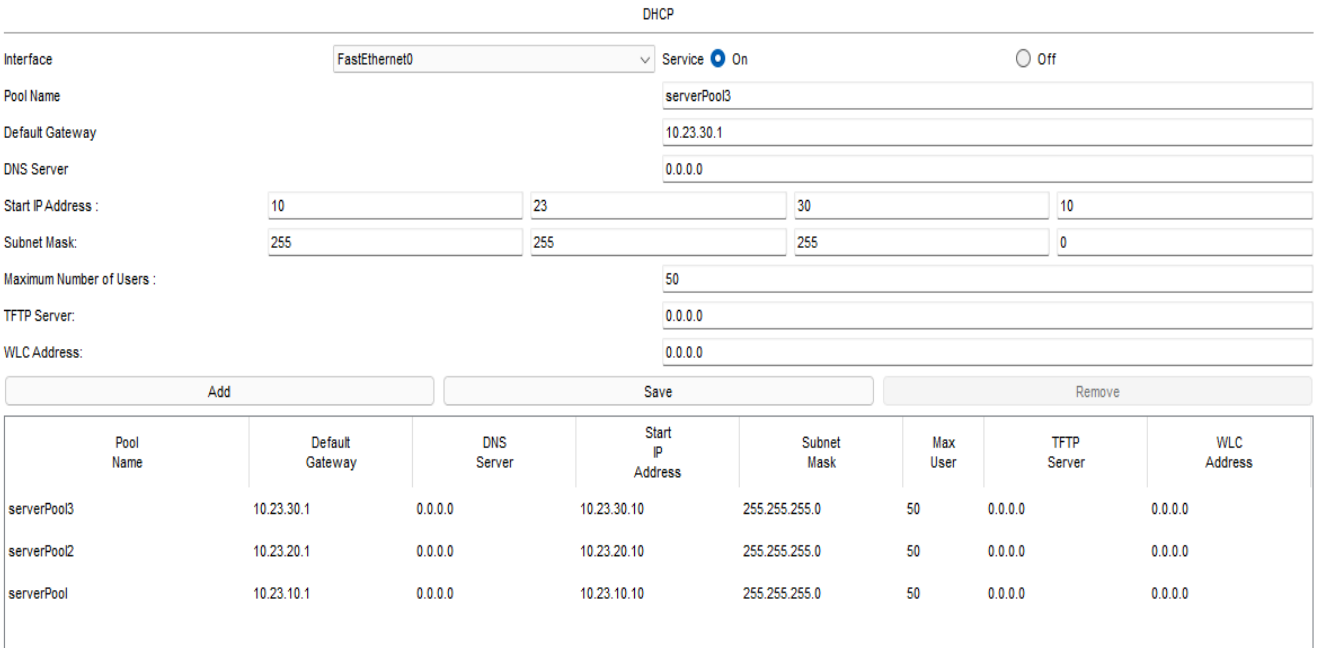
- Tạo các VLAN 10, 20, 30 và đặt IP cho interface VLAN:

```
CoreSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW2(config)#vlan 10
CoreSW2(config-vlan)#vlan 20
CoreSW2(config-vlan)#vlan 30
CoreSW2(config-vlan)#int vlan 10
CoreSW2(config-if)#ip address 10.23.10.1 255.255.255.0
CoreSW2(config-if)#no shut
CoreSW2(config-if)#int vlan 20
CoreSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

CoreSW2(config-if)#ip address 10.23.20.1 255.255.255.0
CoreSW2(config-if)#no shut
CoreSW2(config-if)#int vlan 30
CoreSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

CoreSW2(config-if)#ip address 10.23.30.1 255.255.255.0
CoreSW2(config-if)#no shut
```

- Đặt IP cho vùng mạng phía DHCP Server 2 và bật chế độ ip routing:

```
CoreSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW2(config)#int gl/0/7
CoreSW2(config-if)#no swi
CoreSW2(config-if)#no switchport
CoreSW2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/7, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/7, changed state to up

CoreSW2(config-if)#ip address 10.23.40.1 255.255.255.0
CoreSW2(config-if)#no shut
CoreSW2(config-if)#ex
CoreSW2(config)#ip routing
```

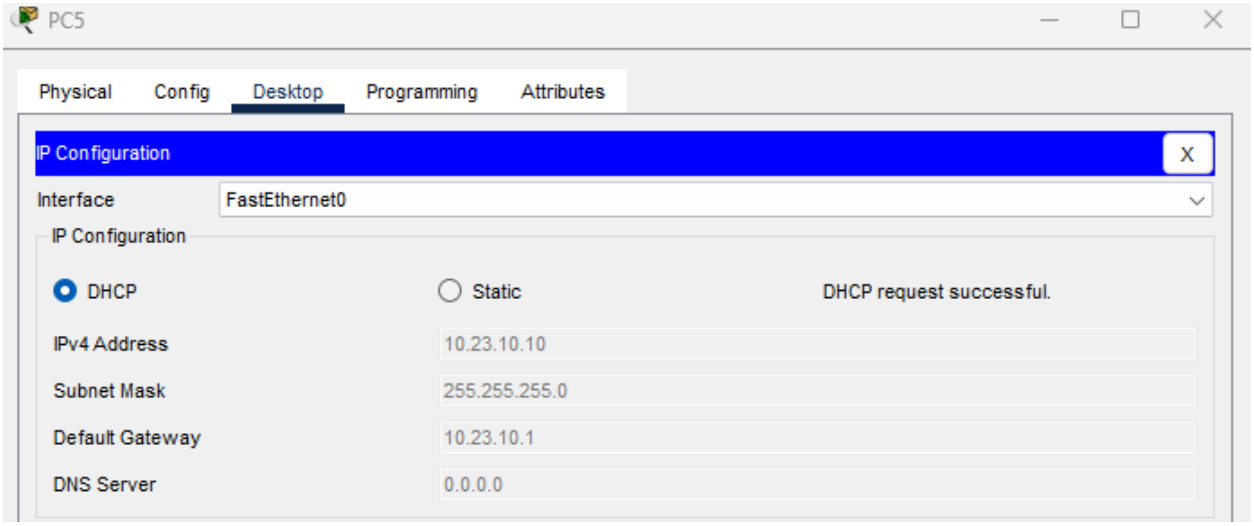
- Sau đó đặt IP cho server và thiết lập dịch vụ DHCP. Ta cho CoreSW2 làm DHCP Relay Agent:




```
CoreSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW2(config)#int vlan 10
CoreSW2(config-if)#ip helper-a
CoreSW2(config-if)#ip helper-address 10.23.40.100
CoreSW2(config-if)#int vlan 20
CoreSW2(config-if)#ip helper-address 10.23.40.100
CoreSW2(config-if)#int vlan 30
CoreSW2(config-if)#ip helper-address 10.23.40.100
```

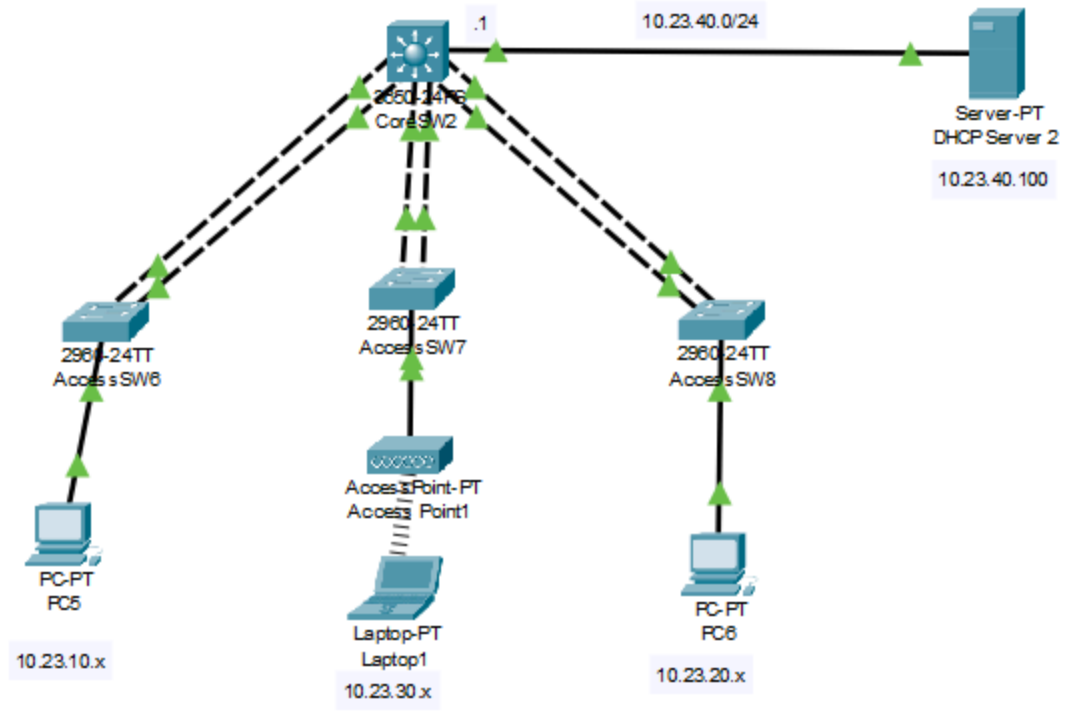
- Cho cổng kết nối máy tính của AccessSW tham gia vào VLAN tương ứng.

```
AccessSW6#
AccessSW6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW6(config)#int f0/3
AccessSW6(config-if)#swi
AccessSW6(config-if)#switchport access vlan 10


AccessSW7>en
AccessSW7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW7(config)#int f0/3
AccessSW7(config-if)#swi
AccessSW7(config-if)#switchport access vlan 30


AccessSW8>en
AccessSW8#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW8(config)#int f0/3
AccessSW8(config-if)#swi
AccessSW8(config-if)#switchport access vlan 20
```

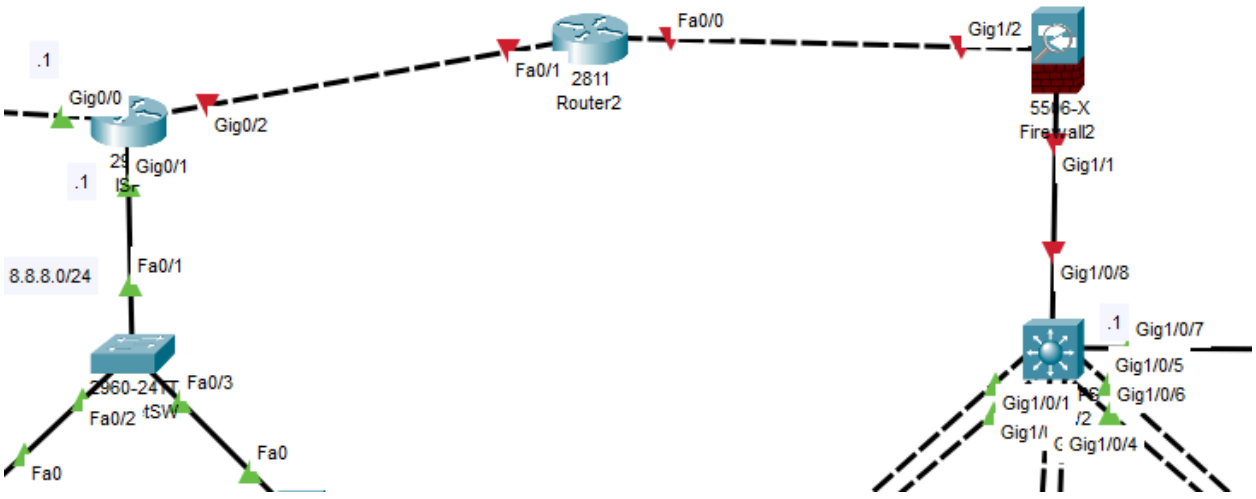


=> Các máy được cấp IP DHCP thành công.

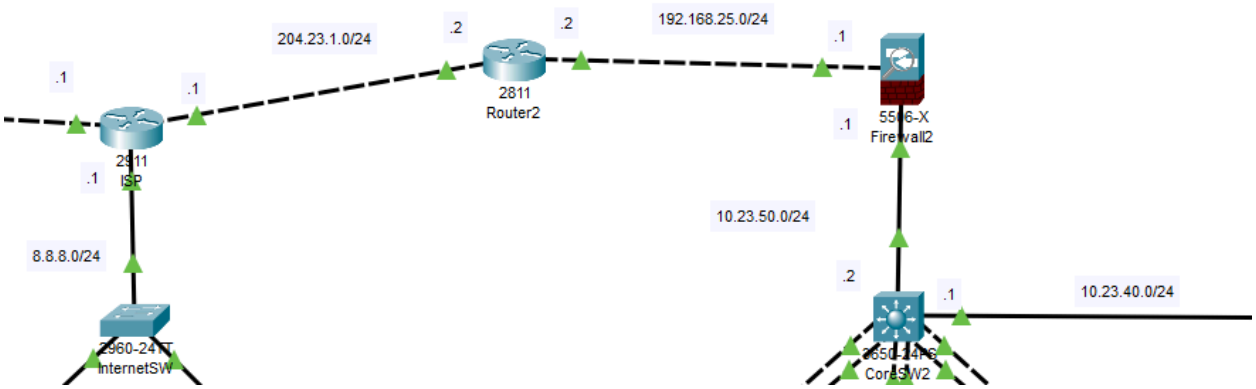
=> Kết quả thu được như sau:



Tiếp theo là thiết lập Firewall để kết nối đến Router2 để NAT ra bên ngoài internet.



```
Firewall2#conf t
Firewall2(config)#int gl/1
Firewall2(config-if)#ip address 10.23.50.1 255.255.255.0
Firewall2(config-if)#no shut

Firewall2(config-if)#
Firewall2(config-if)#int gl/2
Firewall2(config-if)#ip address 192.168.25.1 255.255.255.0
Firewall2(config-if)#no shut


CoreSW2(config-if)#ex
CoreSW2(config)#int gl/0/8
CoreSW2(config-if)#no sw
CoreSW2(config-if)#no switchport
CoreSW2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to up

CoreSW2(config-if)#ip address 10.23.50.2 255.255.255.0
CoreSW2(config-if)#no shut


Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#int f0/0
Router2(config-if)#ip address 192.168.25.2 255.255.255.0
Router2(config-if)#no shut

Router2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router2(config-if)#int f0/1
Router2(config-if)#ip address 204.23.1.2 255.255.255.0
Router2(config-if)#no shut

Router2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up


ISP>en
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#int g0/2
ISP(config-if)#ip address 204.23.1.1 255.255.255.0
ISP(config-if)#no shut

ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
```



Tiến thành thiết lập định tuyến RIP cho từng thiết bị và default route, trừ mạng 204.23.1.0/24 của Router2 vì phần này sẽ dùng NAT:

```
CoreSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW2(config)#router rip
CoreSW2(config-router)#version 2
CoreSW2(config-router)#network 10.23.10.0
CoreSW2(config-router)#network 10.23.20.0
CoreSW2(config-router)#network 10.23.30.0
CoreSW2(config-router)#network 10.23.40.0
CoreSW2(config-router)#network 10.23.50.0
CoreSW2(config-router)#no au
CoreSW2(config-router)#no auto-summary
CoreSW2(config-router)#ex
CoreSW2(config)#ip route 0.0.0.0 0.0.0.0 10.23.50.1


Firewall2#conf t
Firewall2(config)#router rip
Firewall2(config-router)#version 2
Firewall2(config-router)#network 10.23.50.0
Firewall2(config-router)#network 192.168.25.0
Firewall2(config-router)#no au
Firewall2(config-router)#no auto-summary
Firewall2(config-router)#ex


Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#router rip
Router2(config-router)#version 2
Router2(config-router)#network 192.168.25.0
Router2(config-router)#no au
Router2(config-router)#no auto-summary
Router2(config-router)#ip route 0.0.0.0 0.0.0.0 204.23.1.1
```

Thiết lập vùng mạng INSIDE và OUTSIDE cho Firewall2, INSIDE sẽ là vùng mạng có CoreSW, OUTSIDE là vùng mạng có Router2:

```
Firewall2#conf t
Firewall2(config)#int gl/1
Firewall2(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
Firewall2(config-if)#int gl/2
Firewall2(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
Firewall2(config-if)#ex
Firewall2(config)#route outside 0.0.0.0 0.0.0.0 192.168.25.2
```

Đặt access-list để lưu lượng mạng có thể đi về lại vùng INSIDE:

```
Firewall2#conf t
Firewall2(config)#access-l
Firewall2(config)#access-list PERMIT_ALL ex
Firewall2(config)#access-list PERMIT_ALL extended permit ip any any


Firewall2(config)#access-group PERMIT_ALL out in
Firewall2(config)#access-group PERMIT_ALL out interface inside
```

Cuối cùng là thiết lập NAT Overloading (PAT). Do LAN này không có vùng DMZ nên sẽ không cần NAT tĩnh để internet có thể giao tiếp với những server. Vì vậy sẽ chỉ dùng PAT. Thiết lập cũng tương tự như đã làm với LAN trước đó.

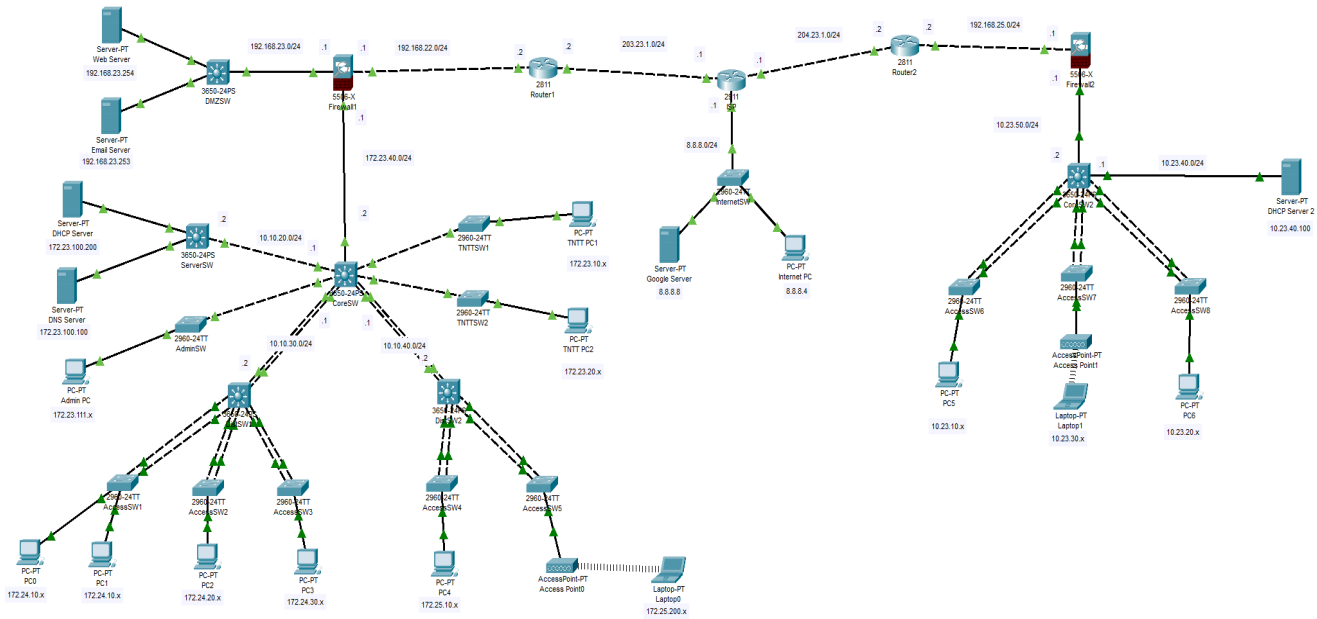
```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#int f0/0
Router2(config-if)#ip nat inside
Router2(config-if)#int f0/1
Router2(config-if)#ip nat outside
Router2(config-if)#ex
Router2(config)#access-l
Router2(config)#access-list 10 permit 10.23.0.0 0.0.255.255
Router2(config)#ip nat in
Router2(config)#ip nat inside sour
Router2(config)#ip nat inside source li
Router2(config)#ip nat inside source list 10 in
Router2(config)#ip nat inside source list 10 interface f0/1 overload
```

Sau đó thử ping từ các máy trong LAN ra ngoài internet rồi kiểm tra bảng NAT.

```
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<1ms TTL=124
Reply from 8.8.8.8: bytes=32 time<1ms TTL=124
Reply from 8.8.8.8: bytes=32 time<1ms TTL=124
Reply from 8.8.8.8: bytes=32 time=1ms 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 = 0ms, Maximum = 1ms, Average = 0ms
```

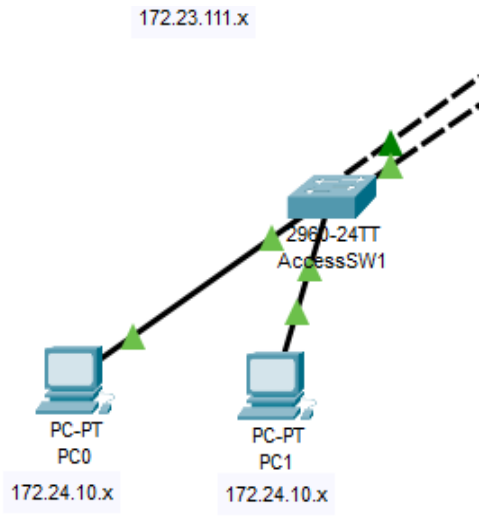
```
Router2#show ip nat tra
Router2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 204.23.1.2:1024   10.23.40.100:13    8.8.8.8:13         8.8.8.8:1024
icmp 204.23.1.2:1025   10.23.40.100:14    8.8.8.8:14         8.8.8.8:1025
icmp 204.23.1.2:1026   10.23.40.100:15    8.8.8.8:15         8.8.8.8:1026
icmp 204.23.1.2:1027   10.23.40.100:16    8.8.8.8:16         8.8.8.8:1027
icmp 204.23.1.2:13     10.23.10.10:13     8.8.8.8:13         8.8.8.8:13
icmp 204.23.1.2:14     10.23.10.10:14     8.8.8.8:14         8.8.8.8:14
icmp 204.23.1.2:15     10.23.10.10:15     8.8.8.8:15         8.8.8.8:15
icmp 204.23.1.2:16     10.23.10.10:16     8.8.8.8:16         8.8.8.8:16
icmp 204.23.1.2:1      10.23.30.10:1      8.8.8.8:1          8.8.8.8:1
icmp 204.23.1.2:2      10.23.30.10:2      8.8.8.8:2          8.8.8.8:2
icmp 204.23.1.2:3      10.23.30.10:3      8.8.8.8:3          8.8.8.8:3
icmp 204.23.1.2:4      10.23.30.10:4      8.8.8.8:4          8.8.8.8:4
```

=> Như vậy là đã thiết lập hoàn thành các cấu hình cơ bản.



5.2 Cấu hình bảo mật

a) Cấu hình Hardening trên AccessSW1

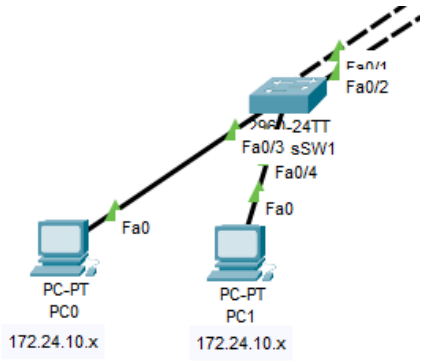


Vì Access-SW1 chỉ cho sử dụng 2 máy tính nên các port không sử dụng phải tắt đi. Do AccessSW1 đang sử dụng 2 cổng để làm port-channel kết nối với CoreSW, 2 cổng để kết nối tới PC0 và PC1. Vì vậy nên ngoài 4 cổng này thì ta sẽ shutdown tất cả các cổng còn lại.

```
AccessSW1$show int st
AccessSW1$show int status
Port      Name               Status       Vlan       Duplex  Speed Type
Po1                          connected    trunk      auto    auto
Fa0/1                        connected    trunk      auto    auto  10/100BaseTX
Fa0/2                        connected    trunk      auto    auto  10/100BaseTX
Fa0/3                        connected    10         auto    auto  10/100BaseTX
Fa0/4                        connected    10         auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
Fa0/22                       notconnect   1          auto    auto  10/100BaseTX
Fa0/23                       notconnect   1          auto    auto  10/100BaseTX
Fa0/24                       notconnect   1          auto    auto  10/100BaseTX
Gig0/1                       notconnect   1          auto    auto  10/100BaseTX
Gig0/2                       notconnect   1          auto    auto  10/100BaseTX
```

```
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int range f0/5-f0/24
AccessSW1(config-if-range)#shut
AccessSW1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down


AccessSW1(config-if-range)#
AccessSW1(config-if-range)#int range g0/1, g0/2
AccessSW1(config-if-range)#shut
AccessSW1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
```

b) Cấu hình tính năng Port Secutity trên AccessSW1



Tại AccessSW1 hiện tại có 2 máy tính đang được kết nối là PC0 và PC1. Ta sẽ cấu hình cho AccessSW1 để người dùng không thể tự ý thay đổi PC0 và PC1 thành thiết bị khác. Trước tiên là điều chỉnh chế độ cổng sang access (mặc định là auto sẽ không dùng được port-security).

```
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int f0/3
AccessSW1(config-if)#switchport mode access
AccessSW1(config-if)#int f0/4
AccessSW1(config-if)#switchport mode access
```

Tiếp theo sẽ thiết lập port-security và cho địa chỉ MAC tối đa mà mỗi cổng được phép học, sau đó sẽ cho cổng đó học địa chỉ MAC của máy tính đang được kết nối vào cổng đó và cuối cùng là cấu hình hành động mà switch sẽ thực hiện khi phát hiện một vi phạm bảo mật trên cổng được cấu hình mà ở đây là sẽ shutdown khi thấy địa chỉ MAC của thiết bị được kết nối không khớp với địa chỉ MAC đã học.

```
AccessSW1>en
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int f0/3
AccessSW1(config-if)#switchport port-security
AccessSW1(config-if)#switchport port-security maximum 1
AccessSW1(config-if)#switchport port-security mac-address 0002.1791.E6EC
AccessSW1(config-if)#switchport port-security violation shutdown
```

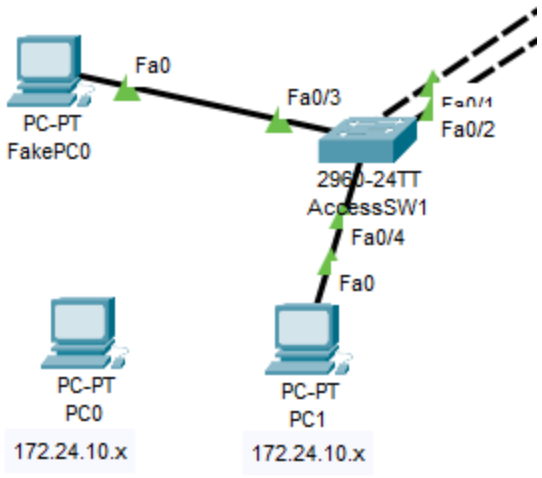
Cấu hình tương tự ở cổng còn lại.

```
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int f0/4
AccessSW1(config-if)#switchport port-security
AccessSW1(config-if)#switchport port-security maximum 1
AccessSW1(config-if)#switchport port-security mac-address 0001.4335.AE81
AccessSW1(config-if)#switchport port-security violation shutdown
```

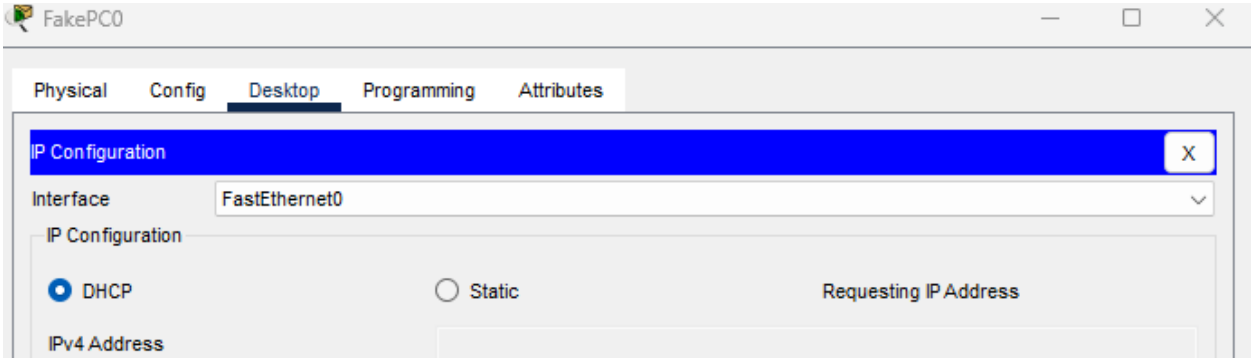
Kiểm tra cấu hình:

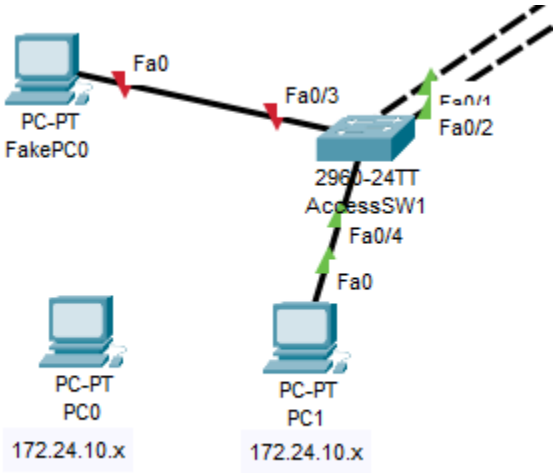
```
AccessSW1>en
AccessSW1#show por
AccessSW1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
-------------------------------------------------------------------------
        Fa0/3        1           1                 0         Shutdown
        Fa0/4        1           1                 0         Shutdown
-------------------------------------------------------------------------
```

Bây giờ sẽ kết nối một máy tính tên FakePC0 vào cổng Fa0/3 để thay thế PC0:

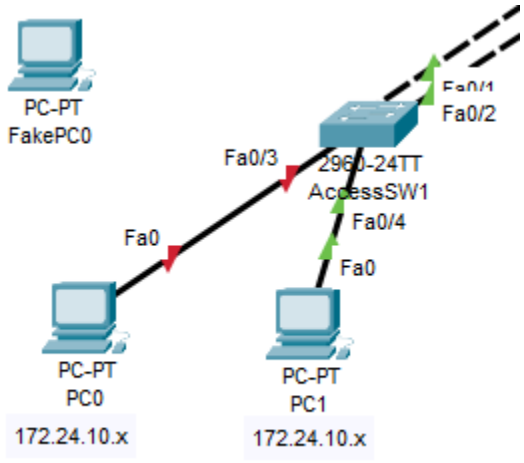


Khi kết nối thì có thể thấy cổng vẫn hoạt động. Tuy nhiên khi vừa thiết lập IP tĩnh hoạt nhận IP từ DHCP Thì FakePC0 sẽ đẩy traffic đến switch, switch sẽ nhận diện được MAC này không hợp lệ và shutdown nó:



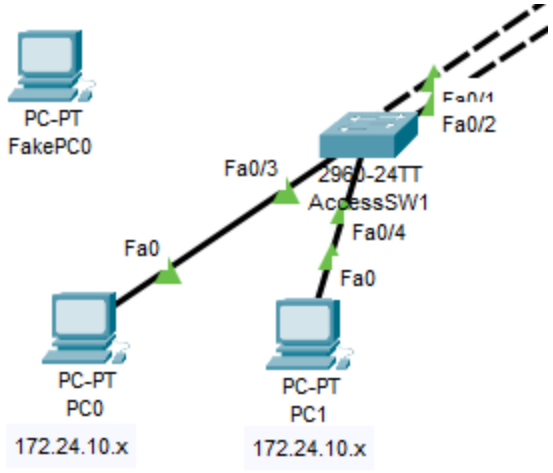


Tuy nhiên, khi chuyển lại sang PC0 kết nối với cổng Fa0/1 của switch (đúng địa chỉ MAC trong port-security), thì cổng này vẫn bị shutdown.



Đó là do giới hạn giả lập của Cisco Packet Tracer nên không thể cấu hình cho nó tự động được. Vì vậy cần phải thiết lập mở lại cổng một cách thủ công bằng lệnh shutdown và sau đó là no shutdown tại cổng Fa0/3.

```
AccessSW1#en
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#int f0/3
AccessSW1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
AccessSW1(config-if)#no shut

AccessSW1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```



Nếu là thiết bị thật, thì ta có thể dùng lệnh **errdisable detect cause all** ở chế độ config để cấu hình chế độ phát hiện nguyên nhân cho tất cả các trường hợp bị vô hiệu hóa (errdisable) trên các cổng của switch. Sau đó dùng lệnh **errdisable recovery cause all** để cấu hình việc tự động phục hồi (recovery) từ trạng thái "errdisable" cho tất cả các nguyên nhân có thể gây ra trạng thái "errdisable" trên các cổng của thiết bị. Cuối cùng là dùng lệnh **errdisable recovery interval 30** để cấu hình thời gian chờ giữa các lần thử lại tự động sau khi một cổng đã bị vô hiệu hóa (errdisabled) được kích hoạt. Khi được cấu hình, switch sẽ chờ một khoảng thời gian xác định trước khi thử lại kích hoạt lại cổng đó. Nghĩa là khi một cổng bị shutdown, switch sẽ cố thử mở lại cổng sau mỗi 30 giây một cách tự động mà không cần phải mở lại cổng một cách thủ công. Tuy nhiên thì tính năng này không có trên Cisco Packet Tracer nên không thể làm được trong giả lập này.

c) Mở truy cập từ xa bằng dịch vụ SSH trên CoreSW, các DistSW và AcessSW1

Trước tiên sẽ cấu hình tại CoreSW. Đầu tiên sẽ đặt domain-name là coresw.com và tạo ra khoá RSA 1024 bit (Từ 768 đến 4096 mới dùng được SSH version 2).

```
CoreSW#
%SYS-5-CONFIG_I: Configured from console by console

CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#ip domain-name coresw.com
CoreSW(config)#crypto key gen
CoreSW(config)#crypto key generate rsa
The name for the keys will be: CoreSW.coresw.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]


CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#ip ssh version 2
```

Sau đó tạo tài khoản SSH admin với chỉ số privilege. Giá trị này từ 0 đến 15. với giá trị 15 nghĩa là có toàn quyền với thiết bị:

```
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#username admin pr
CoreSW(config)#username admin privilege 15 password 123
```

Cuối cùng là bật tính năng SSH trên VTY (Virtual Teletype):

```
CoreSW(config)#line vty 0 4
CoreSW(config-line)#login local
CoreSW(config-line)#transport input ssh
CoreSW(config-line)#exec-timeout 5
```

Với VTY 0 4 thường là các dòng mặc định trên thiết bị Cisco, cho phép tối đa 5 kết nối đồng thời từ xa, chỉ cho phép kết nối qua SSH và yêu cầu người dùng nhập username và password để xác thực khi kết nối. Và timeout kết thúc phiên làm việc là 5 phút. Thử truy cập vào terminal của CoreSW từ máy tính PC bất kỳ:

```
C:\>ssh -l admin 10.10.40.1

Password:



CoreSW#
```

=> Đã thực hiện thành công

Với các thiết bị còn lại ta cũng cấu hình tương tự như vậy:

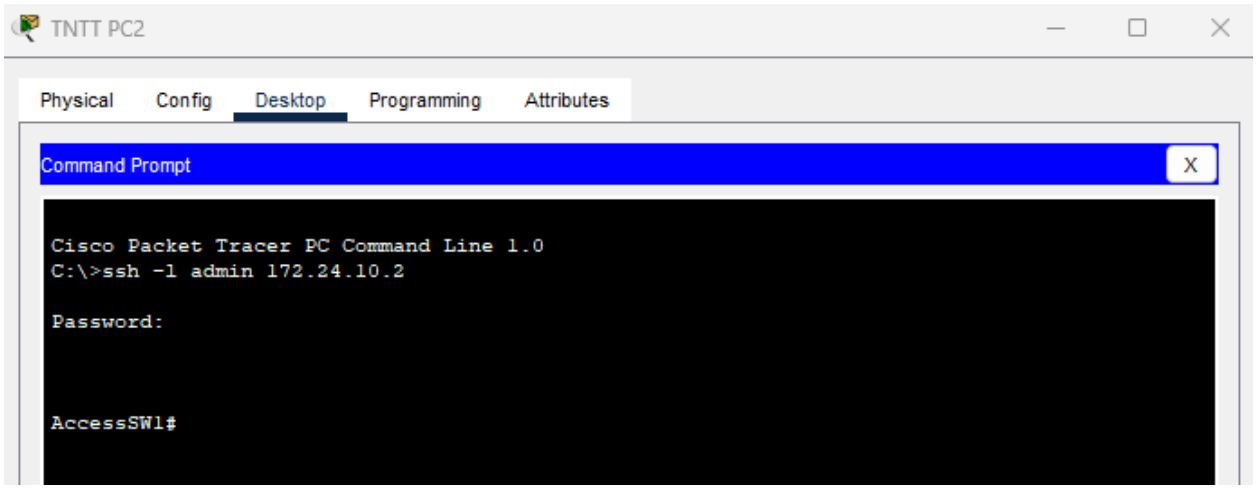
```
DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#ip domain-name distsw1.com
DistSW1(config)#crypto key generate rsa
The name for the keys will be: DistSW1.distsw1.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

DistSW1(config)#ip ssh version 2
*Mar 1 0:47:23.869: %SSH-5-ENABLED: SSH 1.99 has been enabled
DistSW1(config)#username admin privilege 15 password 123
DistSW1(config)#line vty 0 4
DistSW1(config-line)#login local
DistSW1(config-line)#transport input ssh
DistSW1(config-line)#exec-timeout 5


DistSW2>en
DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#ip domain-name distsw2.com
DistSW2(config)#crypto key generate rsa
The name for the keys will be: DistSW2.distsw2.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

DistSW2(config)#ip ssh version 2
*Mar 1 0:49:20.85: %SSH-5-ENABLED: SSH 1.99 has been enabled
DistSW2(config)#username admin privilege 15 password 123
DistSW2(config)#line vty 0 4
DistSW2(config-line)#login local
DistSW2(config-line)#transport input ssh
DistSW2(config-line)#exec-timeout 5
```

```
AccessSW1>en
AccessSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSW1(config)#ip domain-name accessswl.com
AccessSW1(config)#crypto key generate rsa
The name for the keys will be: AccessSW1.accessswl.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

AccessSW1(config)#ip ssh version 2
*Mar 1 0:51:43.702: %SSH-5-ENABLED: SSH 1.99 has been enabled
AccessSW1(config)#username admin privilege 15 password 123
AccessSW1(config)#line vty 0 4
AccessSW1(config-line)#login local
AccessSW1(config-line)#transport input ssh
AccessSW1(config-line)#exec-timeout 5
```

Với AccessSW1 thì cần đặt IP cho VLAN của nó (VLAN 10 giống với các PC kết nối với nó).

```
AccessSW1(config-if)#ip address 172.24.10.2 255.255.255.0
AccessSW1(config-if)#ip default
AccessSW1(config-if)#ip default-g
AccessSW1(config-if)#ip default-gateway 172.24.10.1
```

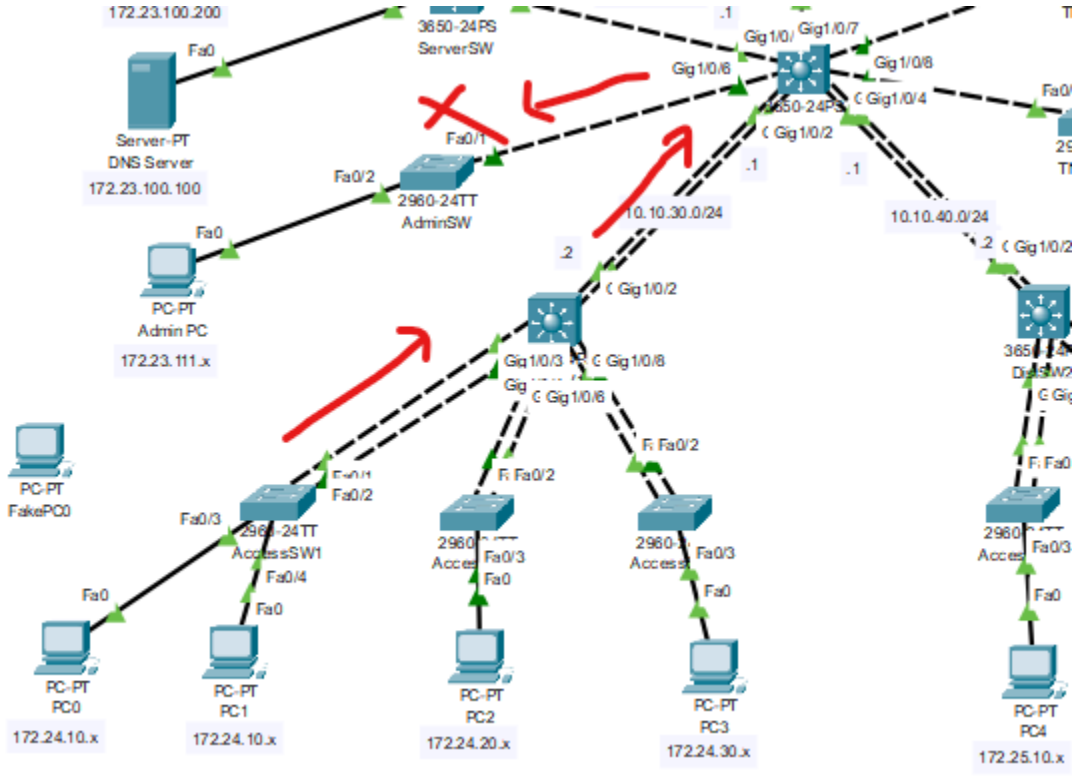
Thử kết nối từ máy TNTT PC2 (172.23.20.x):



=> Như vậy là đã thiết lập SSH thành công.

d) Cấu hình ACL

- Cấu hình để cấm các PC thuộc phòng ban VLAN10 truy cập vào khu vực quản trị (có địa chỉ là 172.32.111.0/24):

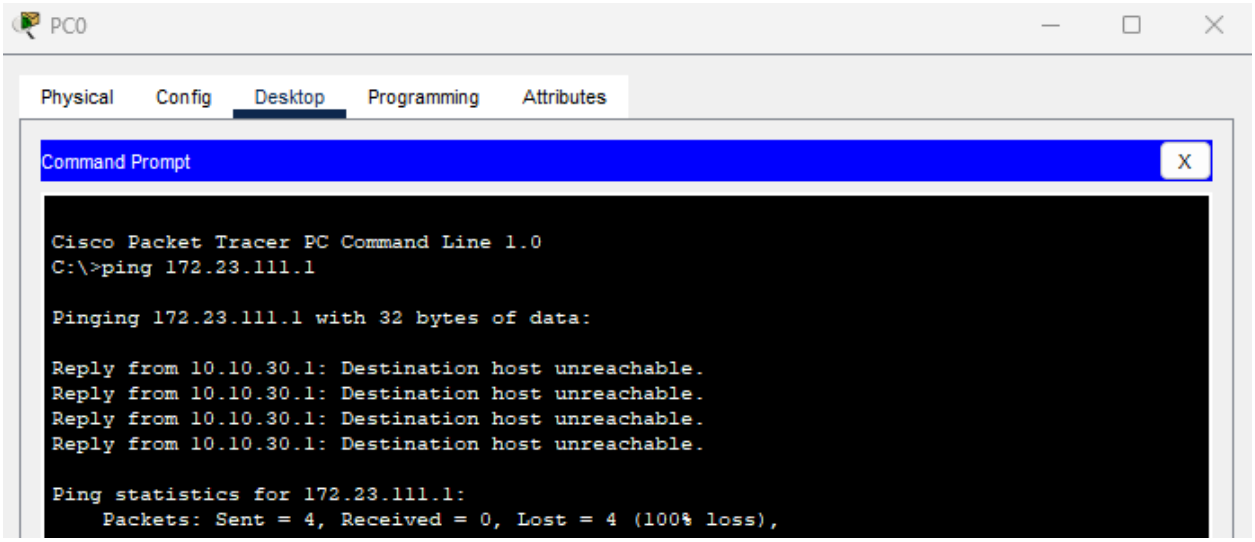


Để cấm các PC thuộc VLAN 10 truy cập vào khu vực quản trị, ta cần phải đặt ACL tại CoreSW để ngăn lưu lượng từ VLAN 10. Do cấm hết lưu lượng (Bao gồm tất cả giao thức) nên ta chỉ đơn giản là deny ip.

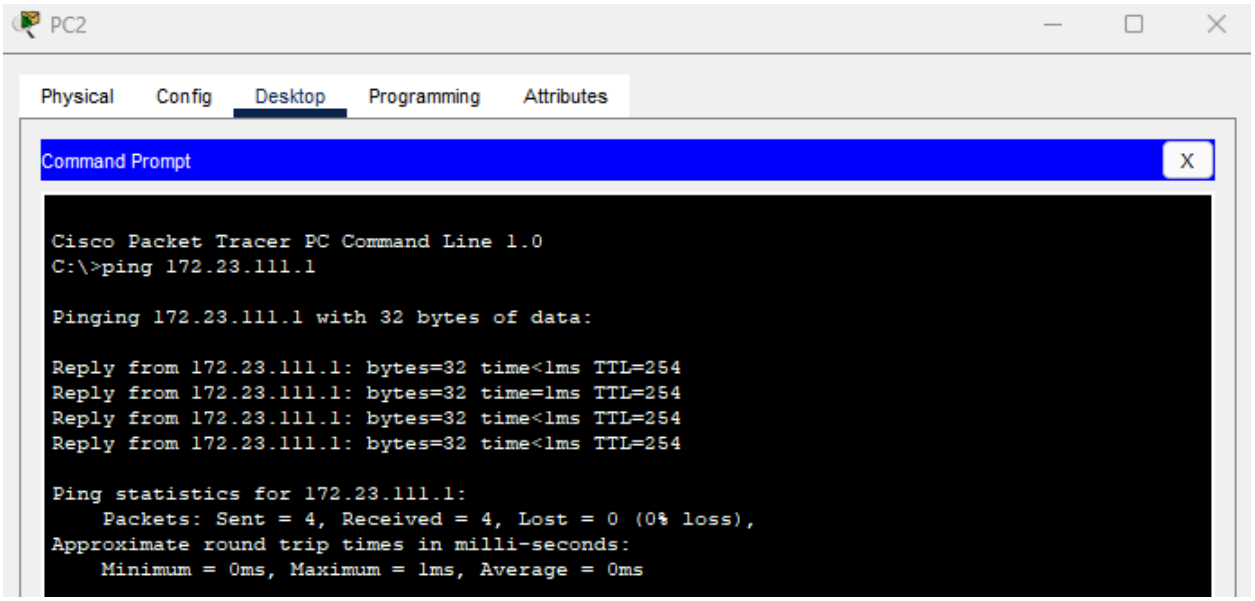
```
CoreSW>en
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#ip access-list extended DENY_VLAN10_TO_ADMIN
CoreSW(config-ext-nacl)#10 deny ip 172.24.10.0 0.0.0.255 172.23.111.0 0.0.0.255
CoreSW(config-ext-nacl)#100 permit ip any any
CoreSW(config-ext-nacl)#int po1
CoreSW(config-if)#ip acc
CoreSW(config-if)#ip access-group DENY_VLAN10_TO_ADMIN in
```

Khi ta gán vào access-group của cổng Po1 thì với access-list trên, khi khớp IP của VLAN 10 (172.24.10.0) mà đi tới IP của VLAN 111 (172.23.111.0) ở hướng đi vào cổng Po1 thì

sẽ bị chặn lại, còn nếu không sẽ xuống rule tiếp theo là cho phép lưu lượng đi qua. Thử ping từ PC0 (172.24.10.x) đến máy Gateway của khu vực Admin (172.23.111.1).



Với PC khác thuộc VLAN20 thì chỉ có PC0 thuộc VLAN 10 là bị chặn lại, các PC thuộc VLAN khác vẫn có thể truy cập vào khu vực quản trị:



- Chỉ cho phép các máy thuộc khu vực quản trị được quyền truy cập từ xa bằng dịch vụ SSH vào các thiết bị

Để làm như vậy, ta sẽ tạo một ACL trên CoreSW:

```
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#ip access-list extended ONLY_ADMIN_SSH
CoreSW(config-ext-nacl)#10 permit tcp 172.23.111.0 0.0.0.255 any eq 22
CoreSW(config-ext-nacl)#20 deny tcp any any eq 22


CoreSW(config-ext-nacl)#30 permit ip any any
CoreSW(config-ext-nacl)#
```

ACL trên sẽ chỉ chấp nhận kết nối SSH (cổng 22) từ mạng của khu vực quản trị (172.23.111.0) đến các SSH server, còn lại thì sẽ cấm kết nối SSH. Với rule cuối (30) sẽ chấp nhận mọi kết nối còn lại nếu đã khớp hết những rule trên. Sau đó gán vào acess-group của các cổng của CoreSW.

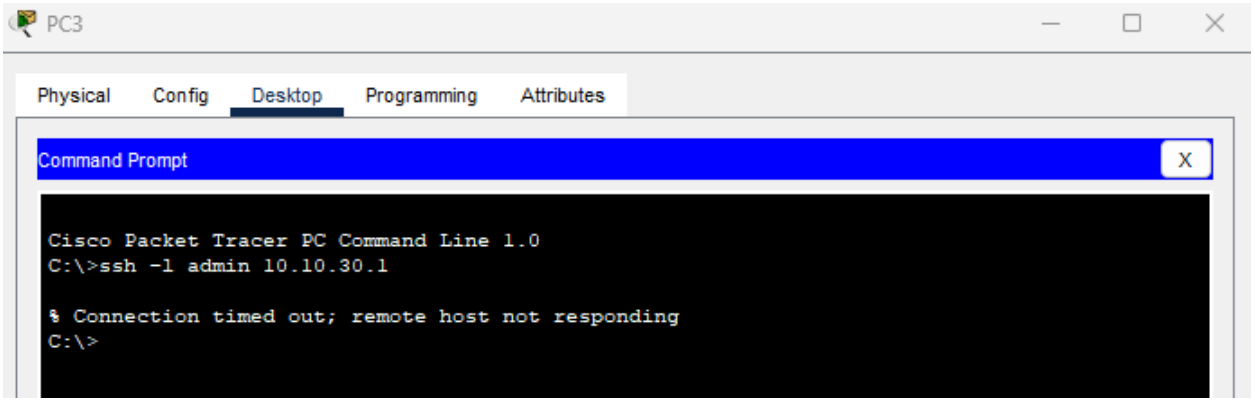
```
CoreSW(config)#int po1
CoreSW(config-if)#ip access-group ONLY_ADMIN_SSH in
CoreSW(config-if)#int po2
CoreSW(config-if)#ip access-group ONLY_ADMIN_SSH in
CoreSW(config-if)#int gl/0/5
CoreSW(config-if)#ip access-group ONLY_ADMIN_SSH in
CoreSW(config-if)#int gl/0/6
CoreSW(config-if)#ip access-group ONLY_ADMIN_SSH in
CoreSW(config-if)#int gl/0/7
CoreSW(config-if)#ip access-group ONLY_ADMIN_SSH in
CoreSW(config-if)#int gl/0/8
CoreSW(config-if)#ip access-group ONLY_ADMIN_SSH in
CoreSW(config-if)#int gl/0/9
CoreSW(config-if)#ip access-group ONLY_ADMIN_SSH in
```

Làm điều tương tự với các DistSW1 và DistSW2:

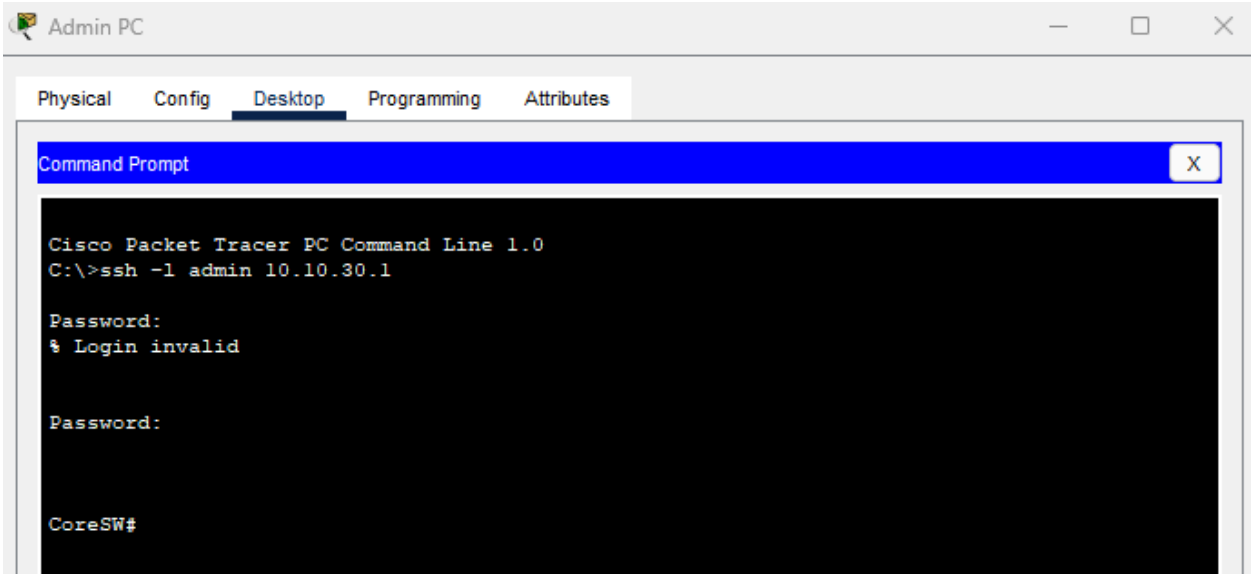
```
DistSW1>en
DistSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW1(config)#ip access-list extended ONLY_ADMIN_SSH
DistSW1(config-ext-nacl)#10 permit tcp 172.23.111.0 0.0.0.255 any eq 22
DistSW1(config-ext-nacl)#20 deny tcp any any eq 22


DistSW1(config-ext-nacl)#30 permit ip any any
DistSW1(config-ext-nacl)#
```

```
DistSW1(config)#int pol
DistSW1(config-if)#ip access-grou
DistSW1(config-if)#ip access-group ONLY_ADMIN_SSH in


DistSW1(config)#int pol
DistSW1(config-if)#ip access-group ONLY_ADMIN_SSH out


DistSW2>en
DistSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DistSW2(config)#ip access-list extended ONLY_ADMIN_SSH
DistSW2(config-ext-nacl)#10 permit tcp 172.23.111.0 0.0.0.255 any eq 22
DistSW2(config-ext-nacl)#20 deny tcp any any eq 22


DistSW2(config-ext-nacl)#30 permit ip any any
DistSW2(config-ext-nacl)#


DistSW2(config)#int pol
DistSW2(config-if)#ip access-group ONLY_ADMIN_SSH in


DistSW2(config)#int pol
DistSW2(config-if)#ip access-group ONLY_ADMIN_SSH out
```

Tuy nhiên tại các DistSW sẽ có hạn chế là không thể chặn truy cập SSH từ các cổng swich (layer 2), vì vậy nên các máy được kết nối trực tiếp vẫn có thể truy cập vào các switch này. Bây giờ sẽ thử từ PC0 (172.24.30.x) truy cập vào SSH của CoreSW.



Tiếp theo là thử ở máy Admin PC:



=> Như vậy có thể thấy việc chặn truy cập được áp dụng khá tốt ở CoreSW. Còn ở DistSW thì chỉ có thể chặn từ mạng ngoài truy cập vào (Trừ Admin), còn máy trong mạng vẫn có thể truy cập do Layer 2 không thể lọc lưu lượng IP.

e) Cấu hình Firewall ở Hội sở

- Các máy ở VLAN20 chỉ được truy cập ra ngoài bằng dịch vụ PING và dịch vụ FTP

Đầu tiên ta tạo access-list ACL_VLAN20, cho phép lưu lượng ICMP (PING) từ các máy trong VLAN 20 đến bất kỳ địa chỉ IP nào.

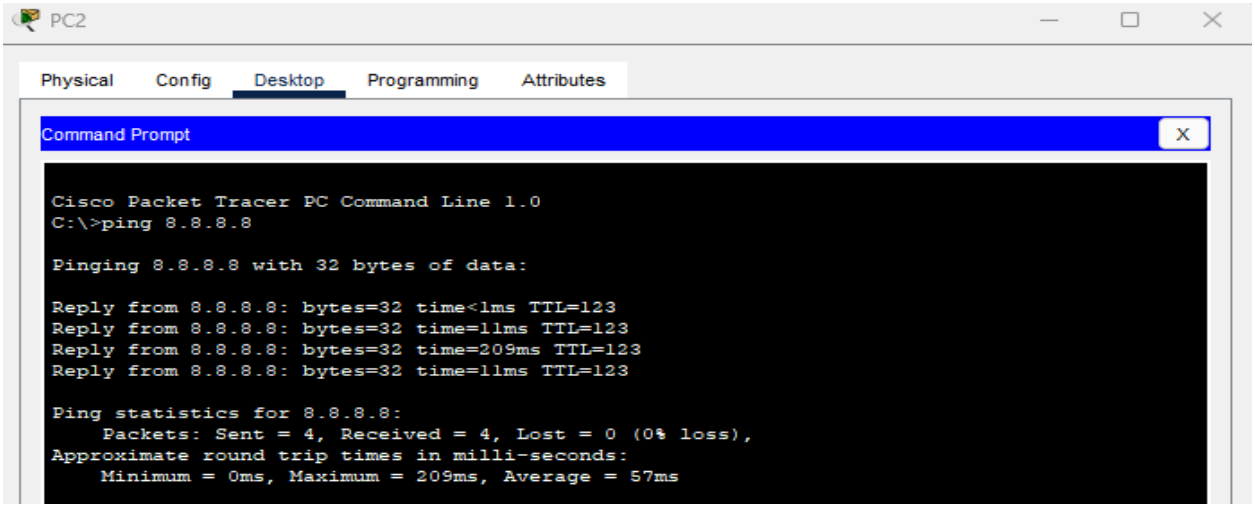
```
Firewalll#conf t
Firewalll(config)#access-list ACL_VLAN20 permit icmp 172.24.20.0 255.255.255.0 any
Firewalll(config)#access-list ACL_VLAN20 permit tcp 172.24.20.0 255.255.255.0 any eq ftp
Firewalll(config)#access-list ACL_VLAN20 deny ip 172.24.20.0 255.255.255.0 any
Firewalll(config)#access-list ACL_VLAN20 permit ip any any
```

Sau đó cho phép lưu lượng TCP từ VLAN 20 đến bất kỳ máy nào trên cổng FTP (TCP port 21). Tiếp theo là chặn tất cả các lưu lượng IP còn lại từ VLAN 20. Cuối cùng là cho phép tất cả các kết nối còn lại (tính chất bảo vệ cuối cùng).

Áp dụng ACL trên đối với lưu lượng đi vào INSIDE:

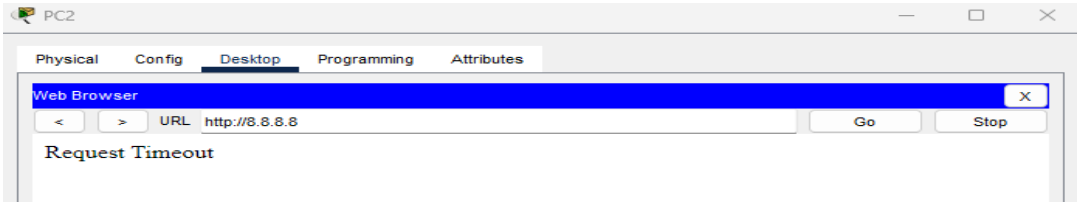
```
Firewalll#conf t
Firewalll(config)#access-group ACL_VLAN20 in interface inside
```

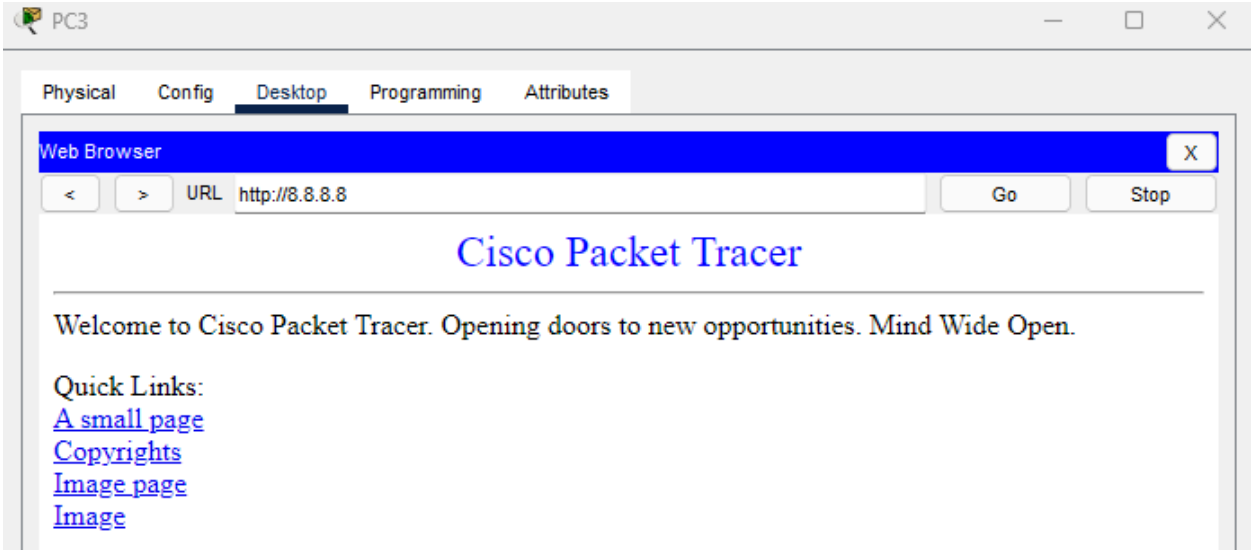
Bây giờ sẽ dùng máy PC2 thuộc VLAN 20 (172.24.20.x) ping ra 8.8.8.8:



=> Có thể thấy là vẫn ping được bình thường

Tuy nhiên khi truy cập HTTP bên ngoài thì sẽ không được, trong khi các máy thuộc VLAN khác lại được:





=> Cấu hình thành công như yêu cầu

- Các máy tính khác trong mạng truy cập được tất cả các dịch vụ bên ngoài Internet

Vì tại phần Cấu hình cơ bản của Firewall1 trước đó đã cấu hình access-group PERMIT_ALL chấp nhận mọi lưu lượng đi ra phía INSIDE và DMZ.

```
Firewalll#conf t
Firewalll(config)#access-li
Firewalll(config)#access-list PERMIT_ALL ex
Firewalll(config)#access-list PERMIT_ALL extended permit ip any any


Firewalll(config)#access-gr
Firewalll(config)#access-group PERMIT_ALL out int inside
Firewalll(config)#access-group PERMIT_ALL out int dmz
```

Vì vậy khi lưu lượng đi ra hướng INSIDE và DMZ sẽ kiểm tra và chấp nhận PERMIT_ALL đầu tiên, sau đó mới đến access-group tiếp theo nên các máy trong mạng INSIDE và DMZ có thể đi ra internet.

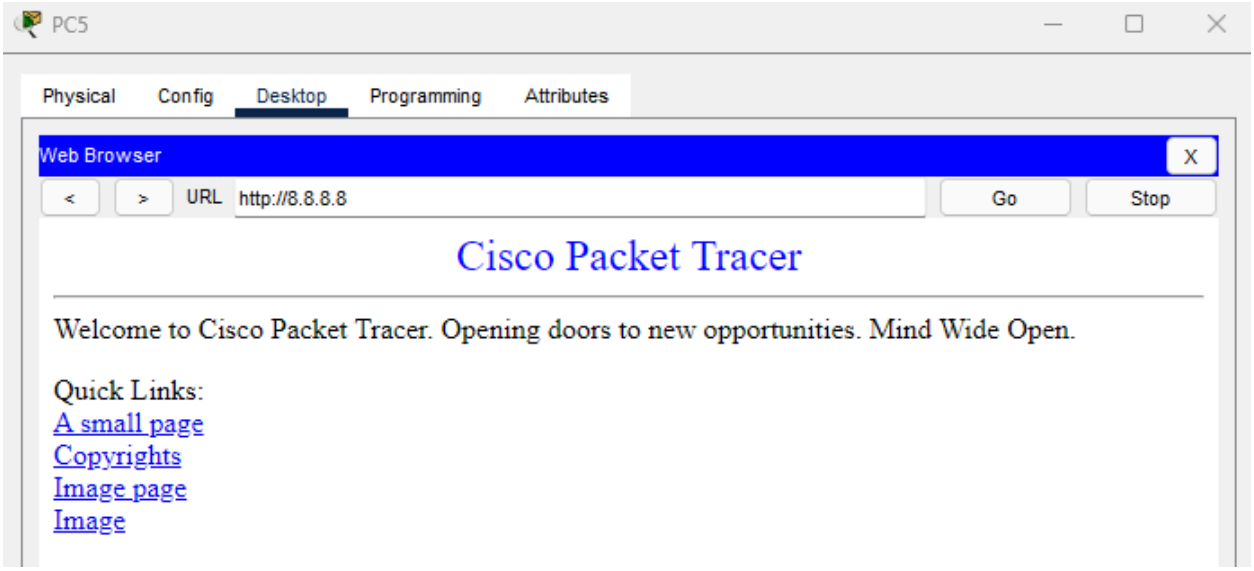
```
route outside 0.0.0.0 0.0.0.0 192.168.22.2 1
!
access-list PERMIT_ALL extended permit ip any any
access-list ACL_VLAN20 extended permit icmp 172.24.20.0 255.255.255.0 any
access-list ACL_VLAN20 extended permit tcp 172.24.20.0 255.255.255.0 any eq ftp
access-list ACL_VLAN20 extended deny ip 172.24.20.0 255.255.255.0 any
access-list ACL_VLAN20 extended permit ip any any
!
!
access-group ACL_VLAN20 out interface inside
access-group PERMIT_ALL out interface dmz
access-group ACL_VLAN20 in interface inside
```

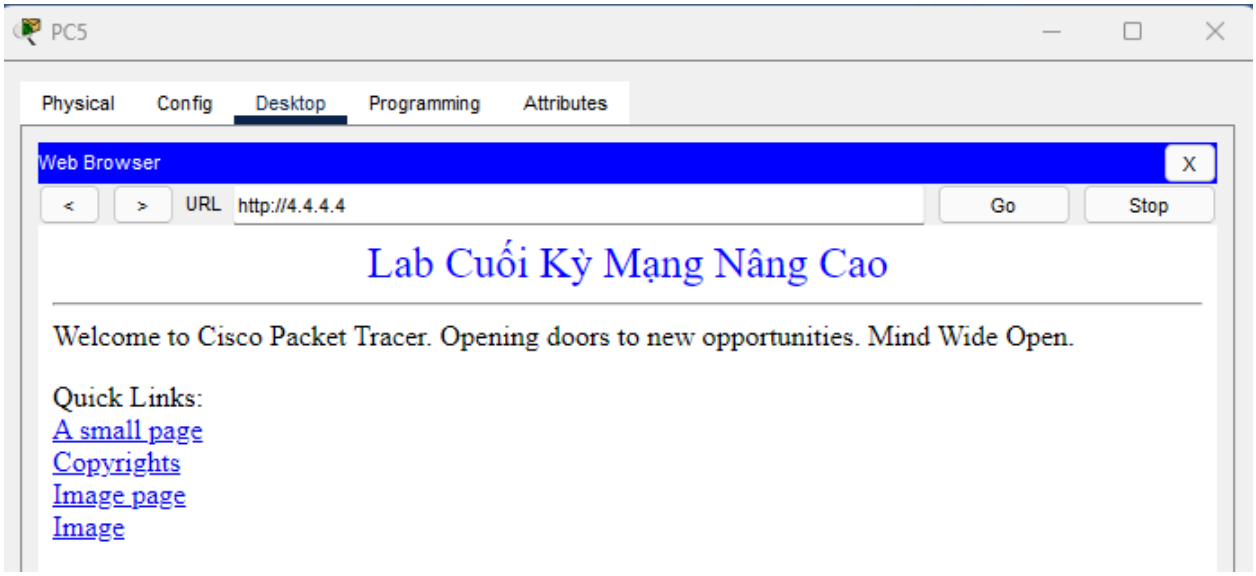
f) Cấu hình Firewall ở Chi nhánh (Cho phép tất cả các dịch vụ ra ngoài Internet)

Cũng tương tự Firewall ở Hội sở, tại phần Cấu hình cơ bản của Firewall2 trước đó đã cấu hình access-group PERMIT_ALL:

```
Firewall2#conf t
Firewall2(config)#access-l
Firewall2(config)#access-list PERMIT_ALL ex
Firewall2(config)#access-list PERMIT_ALL extended permit ip any any

Firewall2(config)#access-group PERMIT_ALL out in
Firewall2(config)#access-group PERMIT_ALL out interface inside
```

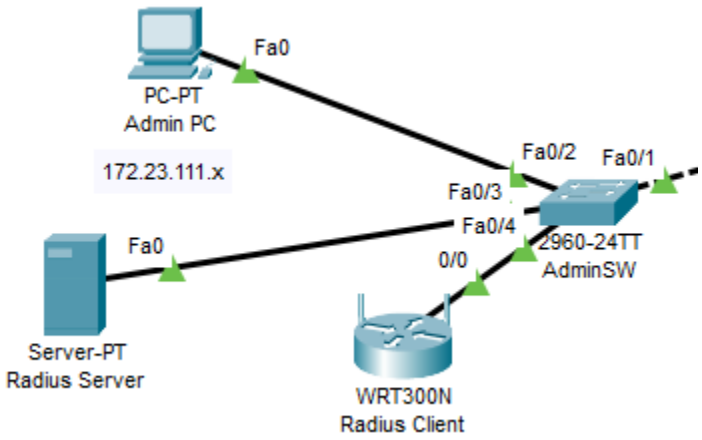
Vì vậy tại Chi nhánh, các máy ở bên trong đều có thể truy cập dịch vụ bên ngoài internet, PC5 (10.23.10.x):





g) Mạng Wi-Fi (Radius Server tại khu vực quản trị)

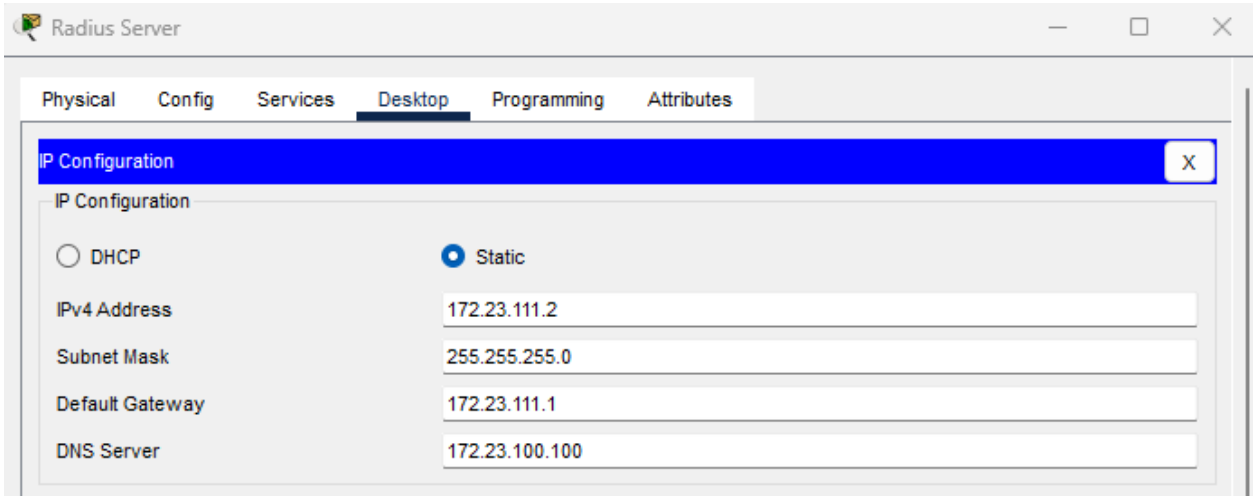
Ta sẽ sử dụng Server làm Radius Server và Access Point (Wireless Router) làm Radius Client.



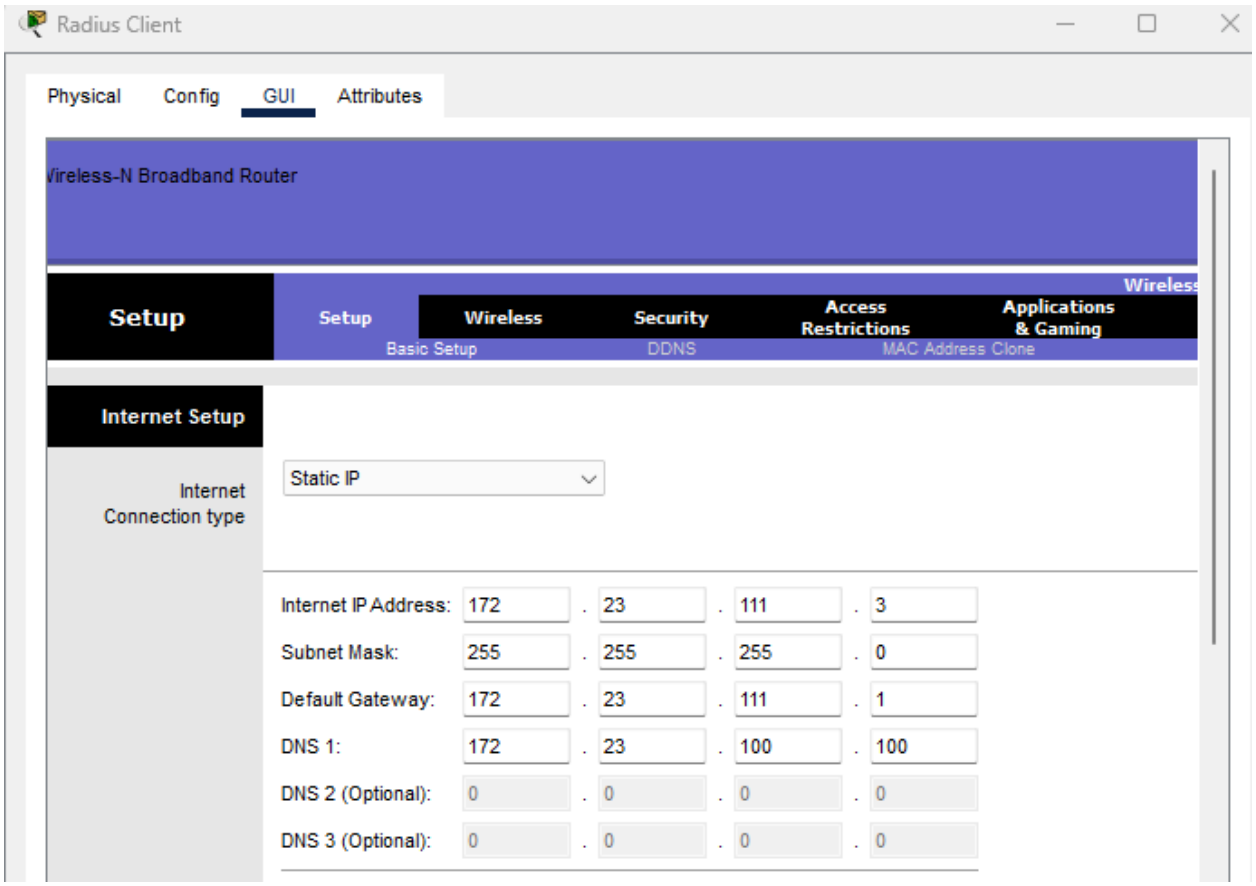
Cho các cổng vừa kết nối với Radius Server và Radius Client tham gia vào VLAN 111 (của mạng 172.23.111.0/24):

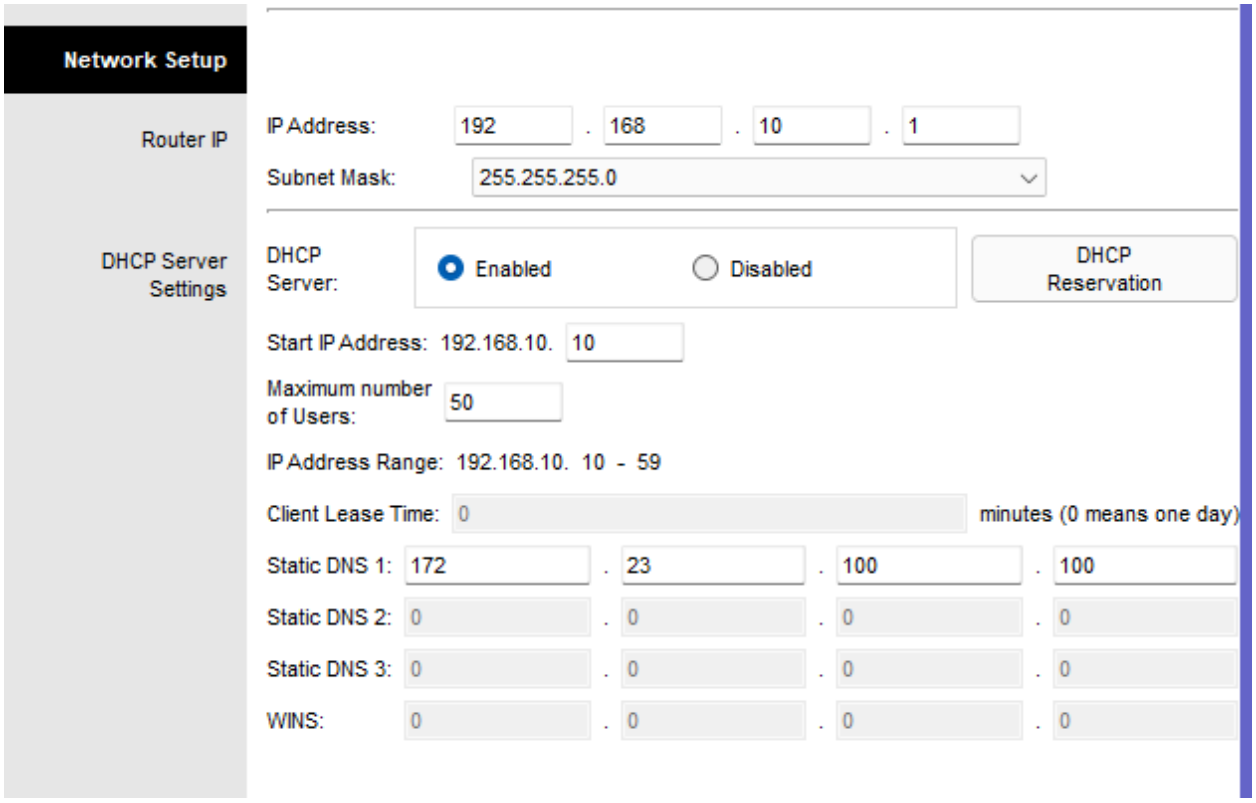
```
AdminSW>en
AdminSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AdminSW(config)#int f0/3
AdminSW(config-if)#swi
AdminSW(config-if)#switchport access vlan 111
AdminSW(config-if)#int f0/4
AdminSW(config-if)#switchport access vlan 111
```

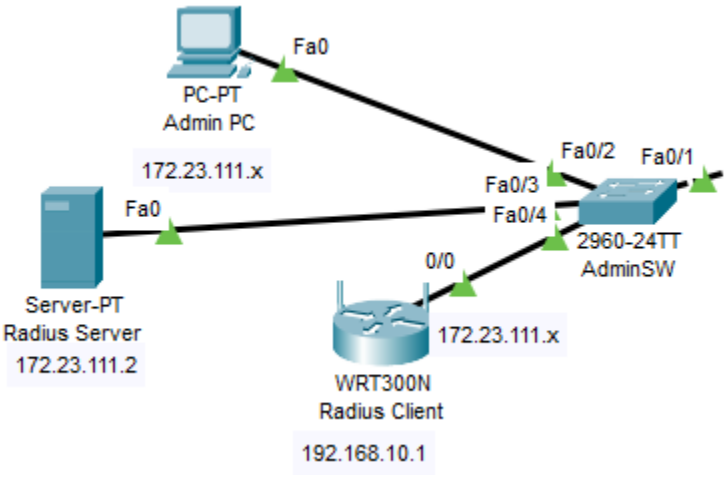
Đặt IP tĩnh cho Radius Client và Radius Server:



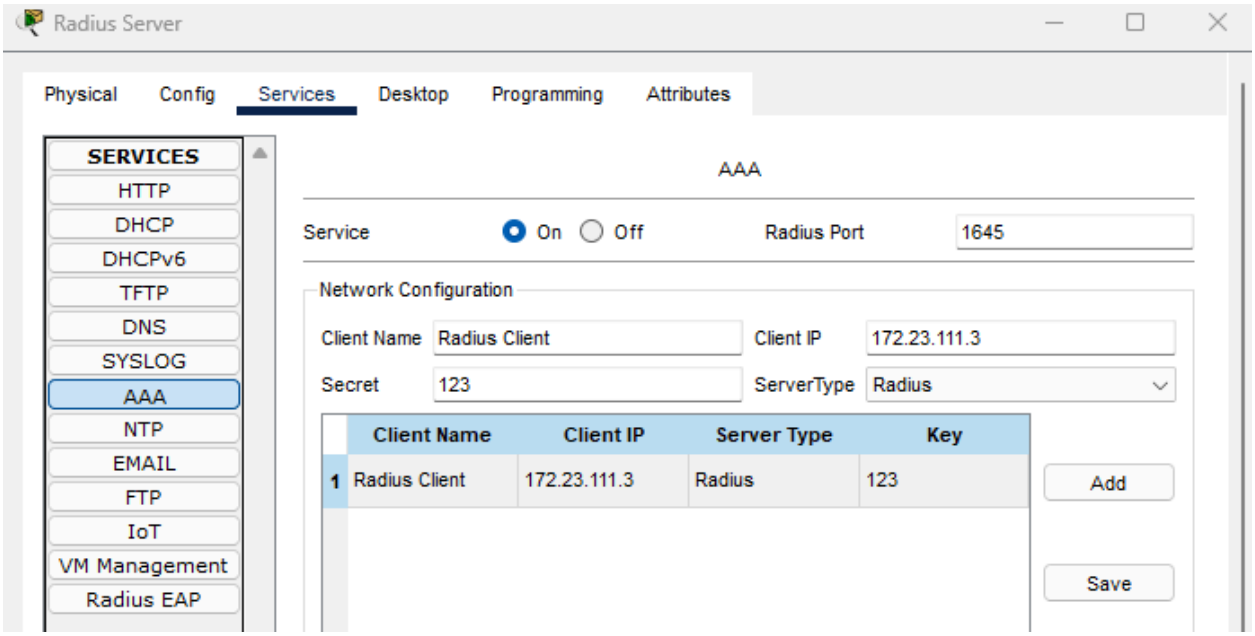
Tại Radius Client, phía kết nối với AdminSW thì sẽ nhận đặt IP ở vùng mạng 172.23.111.0/24, đặt IP tĩnh, còn phía LAN của nó sẽ thiết lập IP là 192.168.10.1 và sẽ cấp DHCP cho những máy kết nối đến :



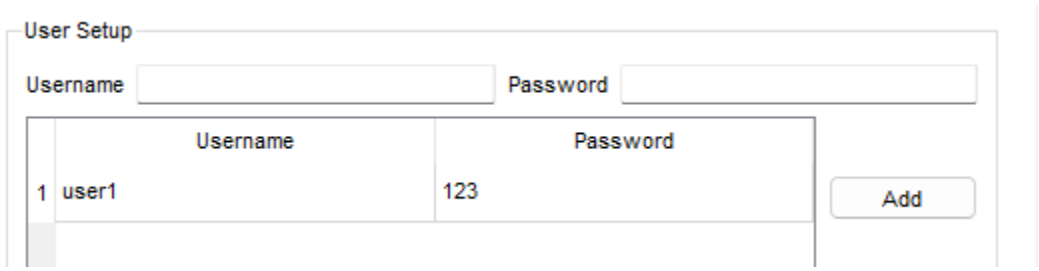




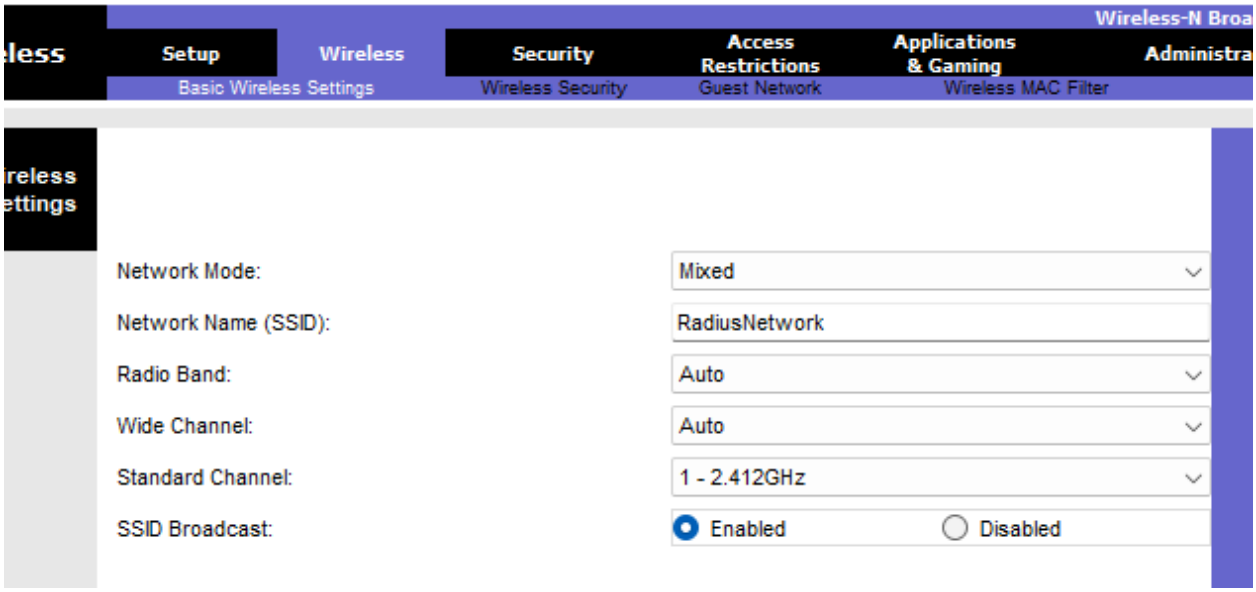
Tại cấu hình AAA của Radius Server sẽ thêm vào IP của Radius Client:

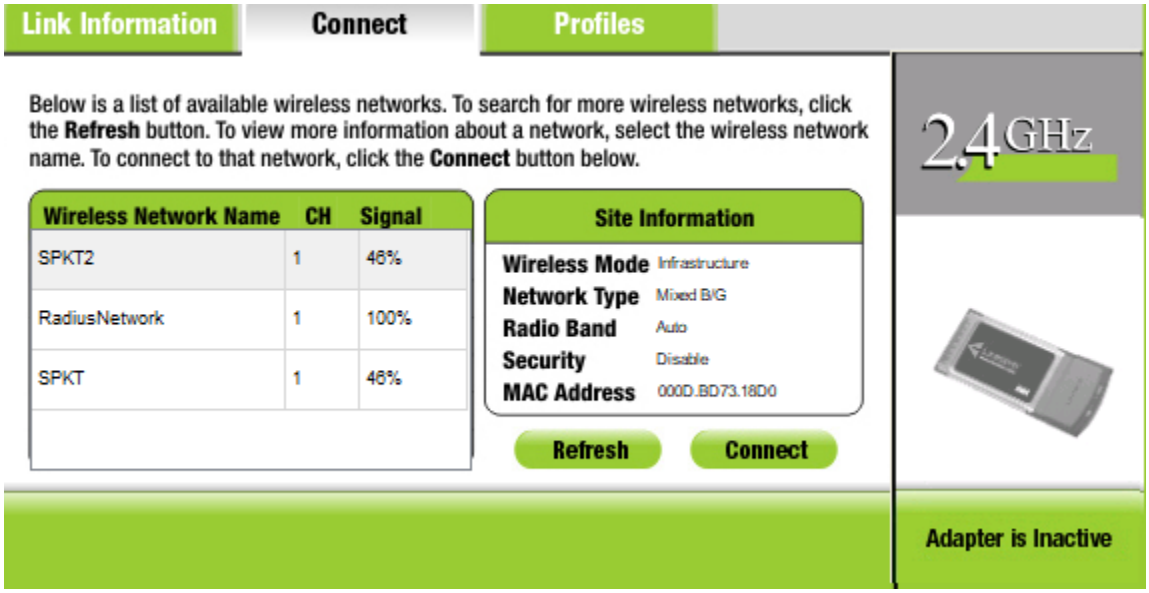


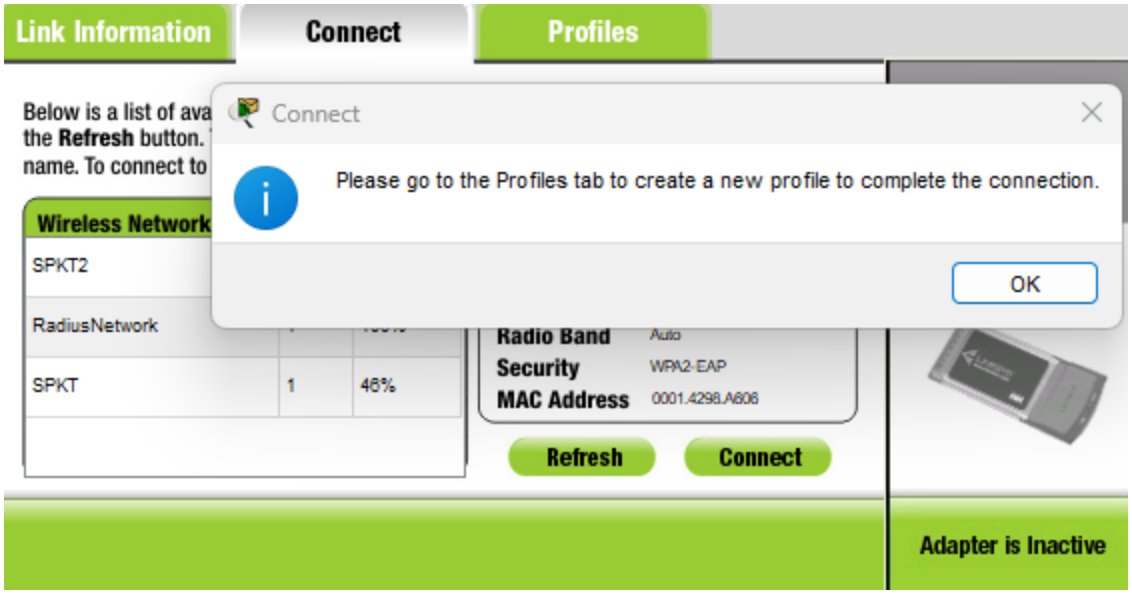
Trong Radius, tài khoản và mật khẩu được sử dụng để xác thực người dùng khi họ cố gắng kết nối vào mạng, tiếp đến ta sẽ thêm tài khoản và mật khẩu ở phía dưới phần Radius Client.



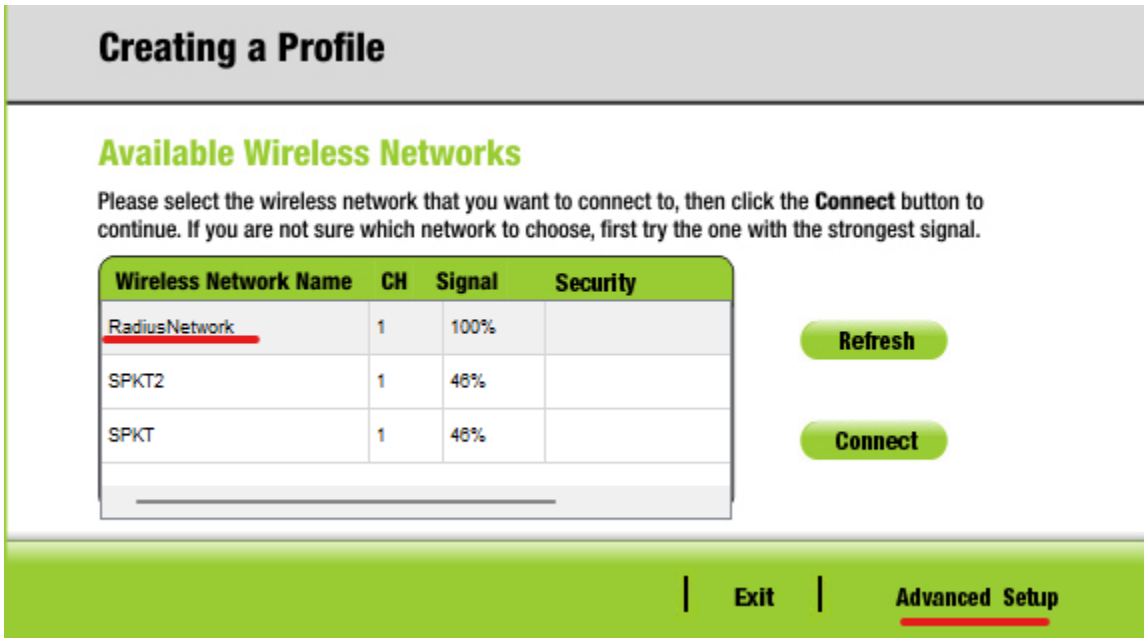
Đặt SSID cho Radius Client là RadiusNetwork, lúc này vào Laptop để kết nối sẽ thấy mạng có SSID là RadiusNetwork:

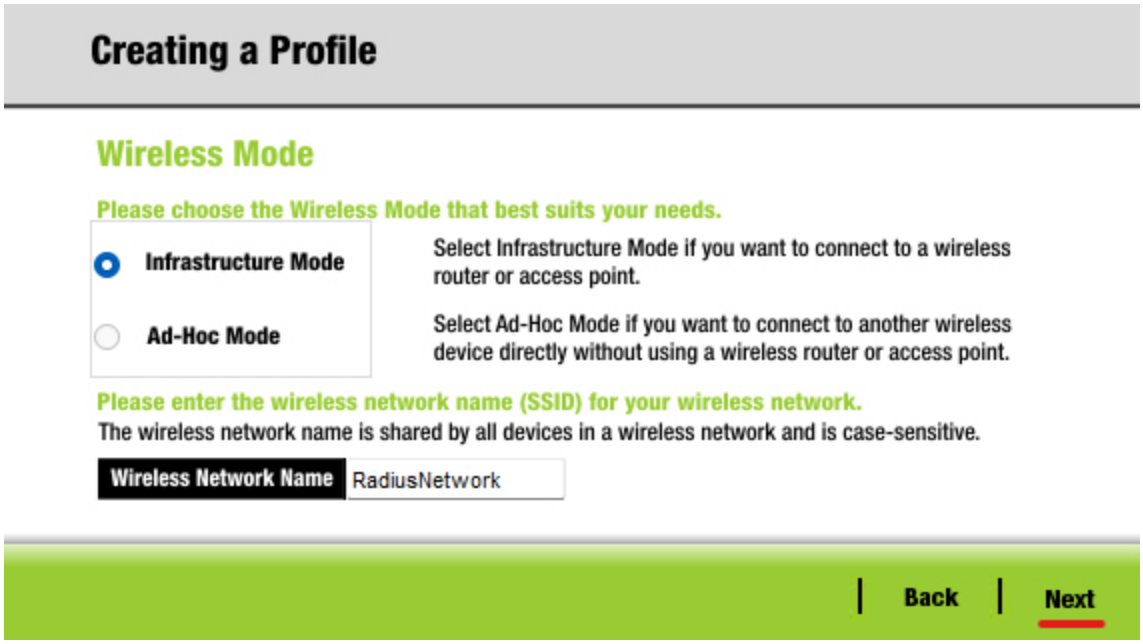

Wireless-N Broa
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administra
Basic Wireless Settings
Wireless Security
Guest Network
Wireless MAC Filter
Network Mode:
Mixed
Network Name (SSID):
RadiusNetwork
Radio Band:
Auto
Wide Channel:
Auto
Standard Channel:
1 - 2.412GHz
SSID Broadcast:
Enabled
Disabled

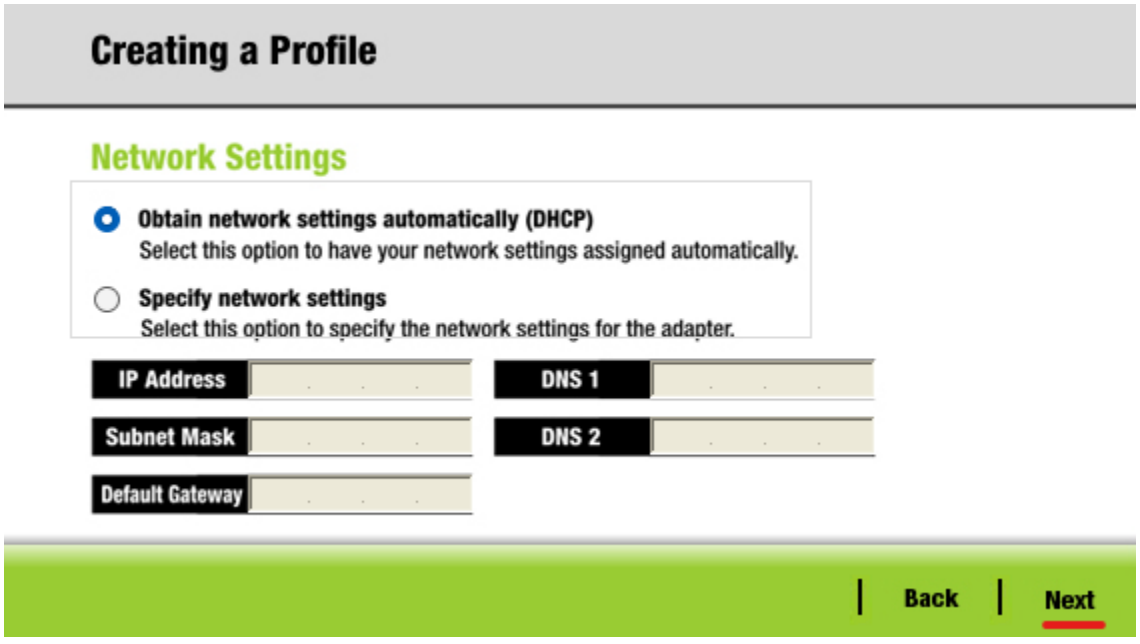

Link Information
Connect
Profiles
Below is a list of available wireless networks. To search for more wireless networks, click the Refresh button. To view more information about a network, select the wireless network name. To connect to that network, click the Connect button below.
Wireless Network Name
CH
Signal
SPKT2
1
46%
RadiusNetwork
1
100%
SPKT
1
46%
Site Information
Wireless Mode
Infrastructure
Network Type
Mixed B/G
Radio Band
Auto
Security
Disable
MAC Address
000D.BD73.18D0
Refresh
Connect
2.4GHz
Adapter is Inactive



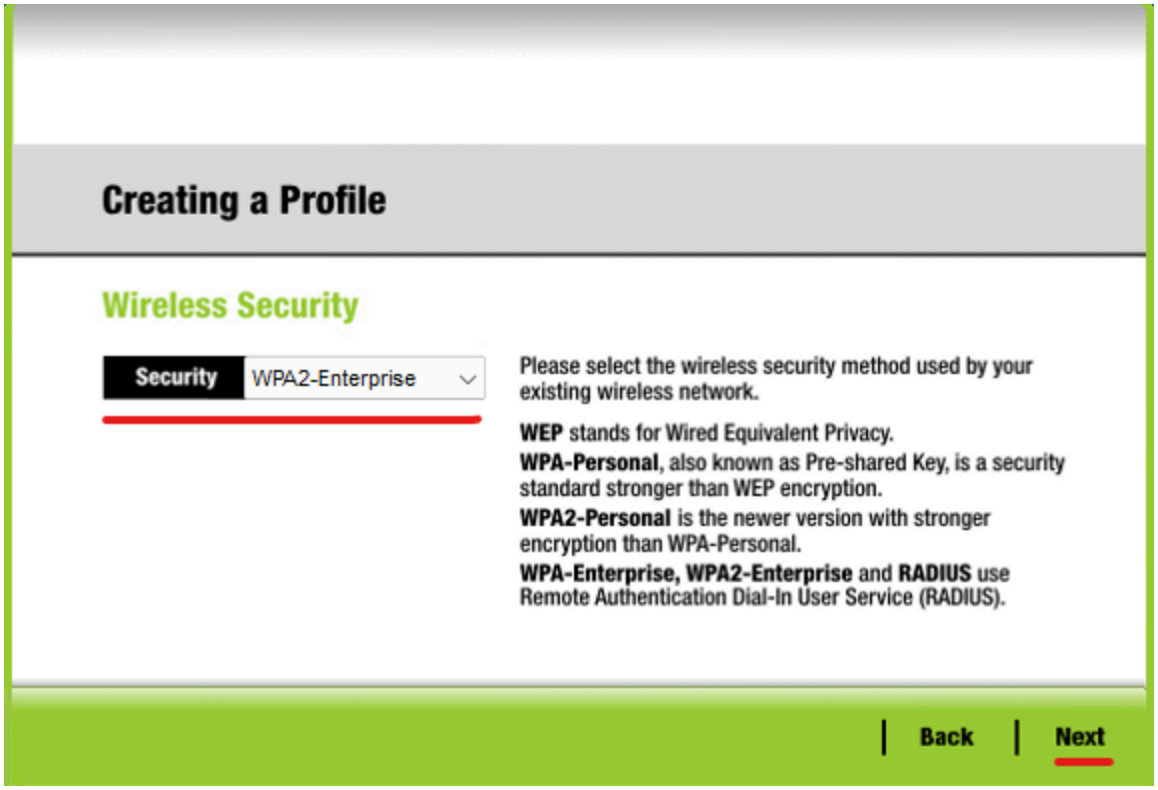
Khi kết nối sẽ hiện thông báo phải tạo Profile, vì vậy cần tạo Profile cho mạng RadiusNetwork:





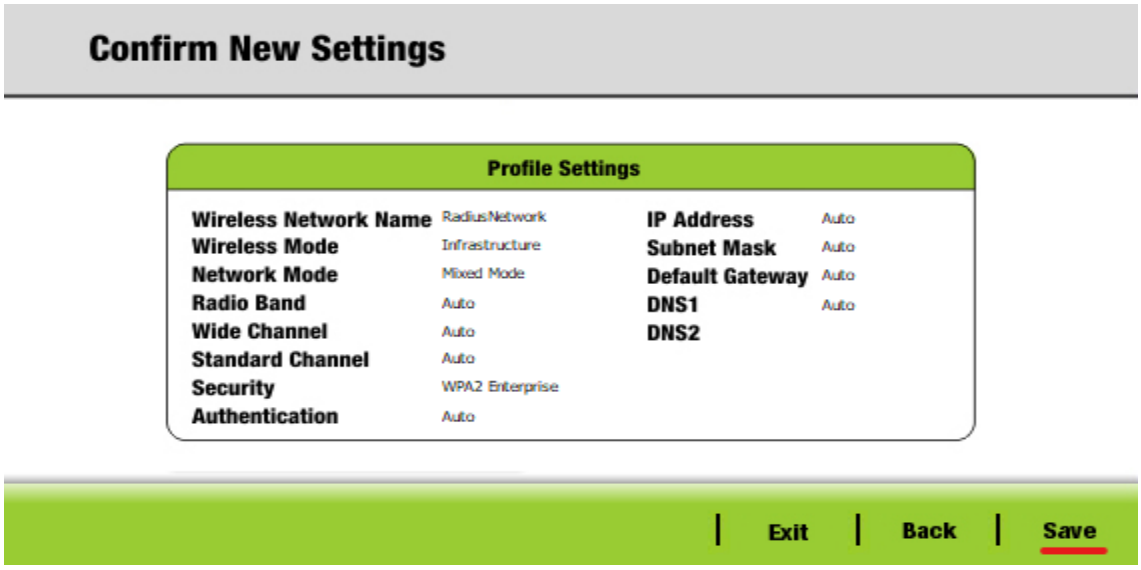


Chọn Wireless Security là WPA2-Enterprise:

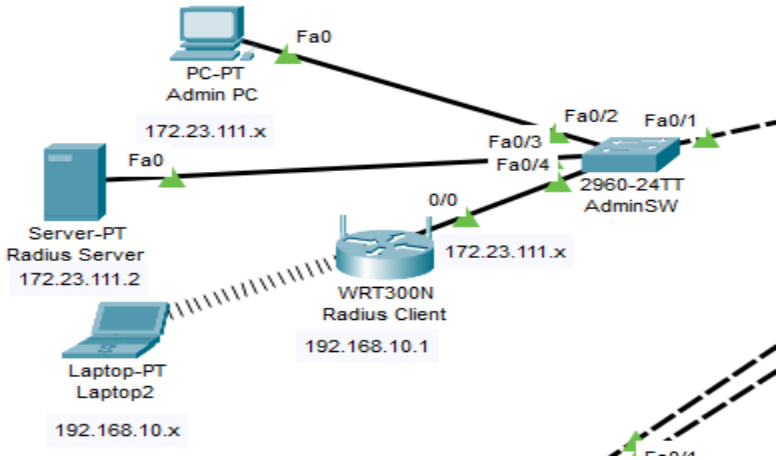


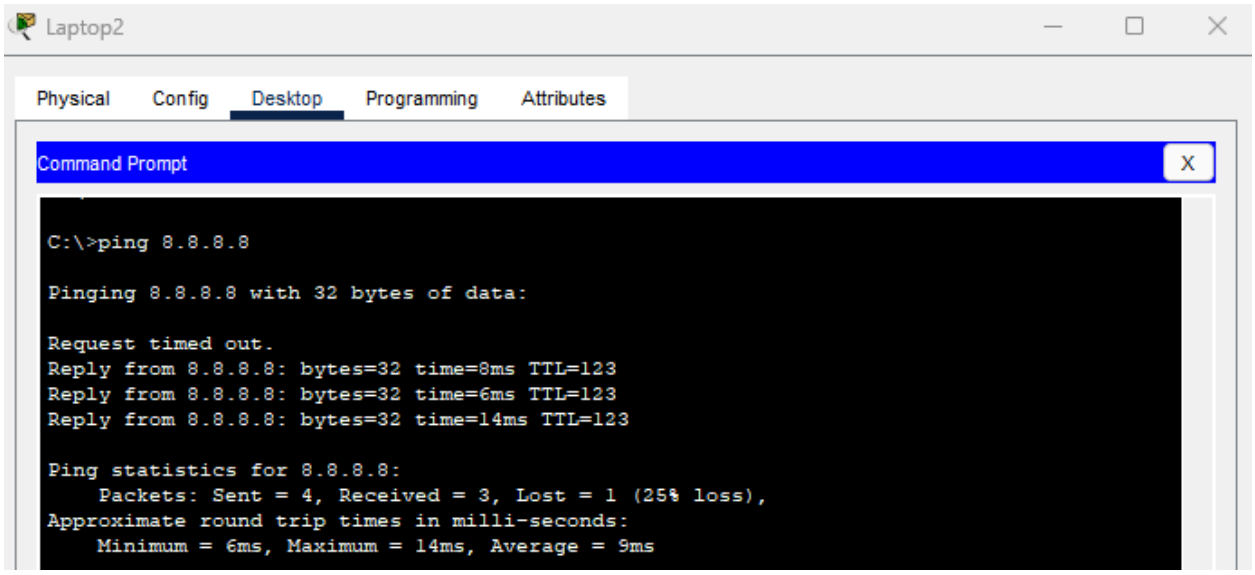
Nhập Login name và password đã tạo khi nãy trên Radius Server:


Creating a Profile
Wireless Security - WPA2 Enterprise
Authentication
PEAP
Please select the authentication method that you use to access your network.
Login Name
user1
Enter the Login Name used for authentication.
Password
Enter the Password used for authentication.
Server Name
Enter the Server Name used for authentication. (Optional)
Certificate
Trust Any
Please select the certificate used for authentication.
Inner Authen.
TOKEN CARD
Please select the inner authentication method used inside the PEAP tunnel.
Back
Next
Wireless-N Notebook Adapter
Wireless Network Monitor v1.11
Model No. WPC300N


Confirm New Settings
Profile Settings
Wireless Network Name
RadiusNetwork
Wireless Mode
Infrastructure
Network Mode
Mixed Mode
Radio Band
Auto
Wide Channel
Auto
Standard Channel
Auto
Security
WPA2 Enterprise
Authentication
Auto
IP Address
Auto
Subnet Mask
Auto
Default Gateway
Auto
DNS1
Auto
DNS2
Exit
Back
Save

=> Kết nối thành công



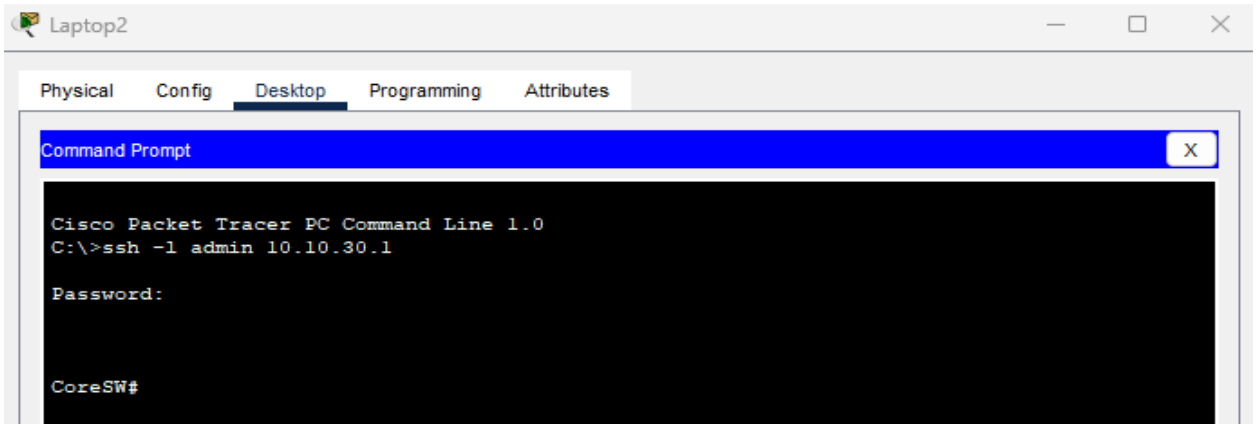


Tuy nhiên lúc này máy ở khu vực quản trị nhưng sẽ không kết nối được đến SSH, vì vậy ta cần bổ sung thêm rule cho access-list đã tạo lúc trước ở các switch:

```
CoreSW#
CoreSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSW(config)#ip access-list extended ONLY_ADMIN_SSH
CoreSW(config-ext-nacl)#15 permit tcp 192.168.10.0 0.0.0.255 any eq 22
```

(Các DistSW tương tự).

```
CoreSW#show ac
CoreSW#show access-lists
Extended IP access list DENY_VLAN10_TO_ADMIN
    10 deny ip 172.24.10.0 0.0.0.255 172.23.111.0 0.0.0.255
    20 permit ip any any
Extended IP access list ONLY_ADMIN_SSH
    10 permit tcp 172.23.111.0 0.0.0.255 any eq 22
    15 permit tcp 192.168.10.0 0.0.0.255 any eq 22
    20 deny tcp any any eq 22
    30 permit ip any any
```



=> Như vậy là đã cấu hình xong Radius Server.

5.3 Cấu hình VPN Site-to-Site (IPSec VPN) để kết nối HQ và Branch

Đầu tiên ta sẽ loại bỏ NAT đã thiết lập cho vùng mạng nội bộ giữa của 2 router ngoài (Router1 là HQ, Router2 là Branch)

```
Router1#show access-lists
Standard IP access list 10
    10 permit 172.23.0.0 0.0.255.255 (12 match(es))
Standard IP access list 11
    10 permit 172.24.0.0 0.0.255.255 (8 match(es))
Standard IP access list 12
    10 permit 172.25.0.0 0.0.255.255 (14 match(es))


Router2#show access-lists
Standard IP access list 10
    10 permit 10.23.0.0 0.0.255.255 (6 match(es))


Router1>en
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#no ip nat inside source list 10 int f0/1 overload
Router1(config)#no ip nat inside source list 11 int f0/1 overload
Router1(config)#no ip nat inside source list 12 int f0/1 overload


Router2>en
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#no ip nat inside source list 10 int f0/1 overload
```

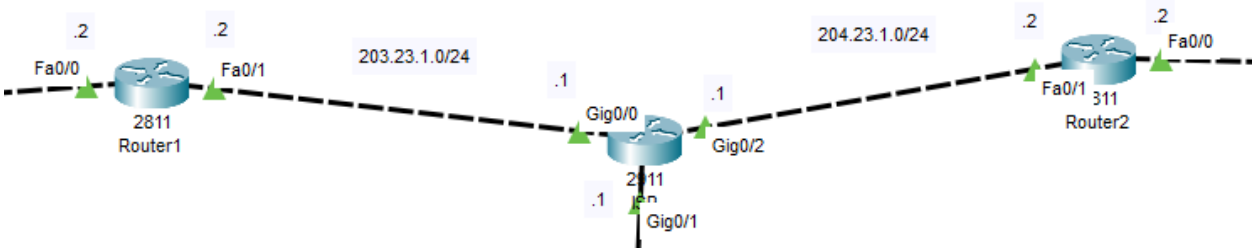
Như vậy là máy trong mạng nội bộ sẽ không giao tiếp ra ngoài internet được nữa.

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

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

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

Ta sẽ tạo VPN để cho phép 2 mạng là 172.0.0.0/8 có thể giao tiếp đến 10.23.0.0/16. Sau đó tạo access-list mới giữa 2 LAN của HQ và Branch từ chối kết nối giữa 2 LAN và áp dụng vào NAT overload.

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#ip access-list extended MYNAT
Router1(config-ext-nacl)#deny ip 172.0.0.0 0.255.255.255 10.23.0.0 0.0.255.255
Router1(config-ext-nacl)#permit ip any any
Router1(config-ext-nacl)#ex
Router1(config)#ip nat inside source list MYNAT int f0/1 overload


Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#ip access-list extended MYNAT
Router2(config-ext-nacl)#deny ip 10.23.0.0 0.0.255.255 172.0.0.0 0.255.255.255
Router2(config-ext-nacl)#permit ip any any
Router2(config-ext-nacl)#ex
Router2(config)#ip nat inside source list MYNAT int f0/1 overload
```

Sau đó tại Router1 cấu chính sách ISAKMP: chính sách số 10 sử dụng xác thực pre-share, mã hóa 3DES, hàm băm MD5, nhóm DH số 2, và thời gian sống 86400 giây. Sau đó, thiết lập khóa ISAKMP là 123456 cho địa chỉ IP 204.23.1.2 (Router2).

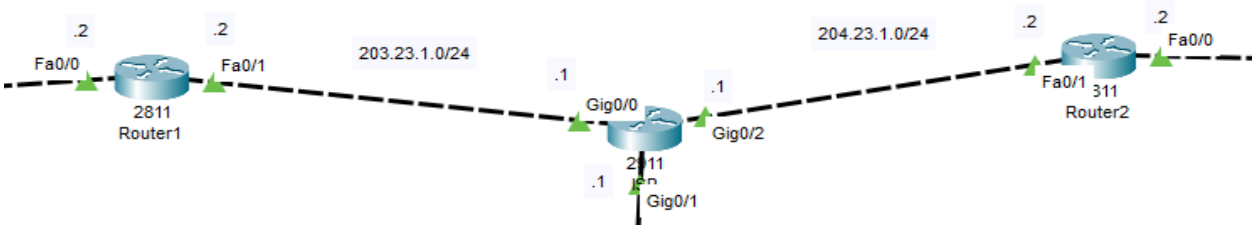


```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#crypto isakmp policy 10
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#encryption 3des
Router1(config-isakmp)#hash md5
Router1(config-isakmp)#group 2
Router1(config-isakmp)#lifetime 86400
Router1(config-isakmp)#exit
Router1(config)#crypto isakmp key 123456 address 204.23.1.2
```

Tiếp đến tập hợp chuyển đổi IPSec MYSET sử dụng mã hóa 3DES và xác thực MD5, tạo ACL số 100 để cho phép lưu lượng giữa mạng nội bộ 172.0.0.0/8 và mạng đích 10.23.0.0/16, thiết lập bản đồ mã hóa IPSec MYMAP với đối tác 204.23.1.2, sử dụng tập chuyển đổi MYSET, và áp dụng điều kiện từ ACL 100. Cuối cùng, bản đồ mã hóa MYMAP được gắn vào giao diện fa0/1 (ra lưu lượng bên ngoài)

```
Router1(config)#ex
Router1#
%SYS-5-CONFIG_I: Configured from console by console

Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#crypto ipsec transform-set MYSET esp-3des esp-md5-hmac
Router1(config)#access-list 100 permit ip 172.0.0.0 0.255.255.255 10.23.0.0 0.0.255.255
Router1(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router1(config-crypto-map)#set peer 204.23.1.2
Router1(config-crypto-map)#set transform-set MYSET
Router1(config-crypto-map)#match address 100
Router1(config-crypto-map)#int f0/1
Router1(config-if)#crypto map MYMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Tại Router2 cũng tương tự, chỉ khác IP đối tác:



```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#crypto isakmp policy 10
Router2(config-isakmp)#authentication pre-share
Router2(config-isakmp)#encryption 3des
Router2(config-isakmp)#hash md5
Router2(config-isakmp)#group 2
Router2(config-isakmp)#lifetime 86400
Router2(config-isakmp)#exit
Router2(config)#crypto isakmp key 123456 address 203.23.1.2
Router2(config)#exit


Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#crypto ipsec transform-set MYSET esp-3des esp-md5-hmac
Router2(config)#access-list 100 permit ip 10.23.0.0 0.0.255.255 172.0.0.0 0.255.255.255
Router2(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router2(config-crypto-map)#set peer 203.23.1.2
Router2(config-crypto-map)#set transform-set MYSET
Router2(config-crypto-map)#match address 100
Router2(config-crypto-map)#int f0/1
Router2(config-if)#crypto map MYMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

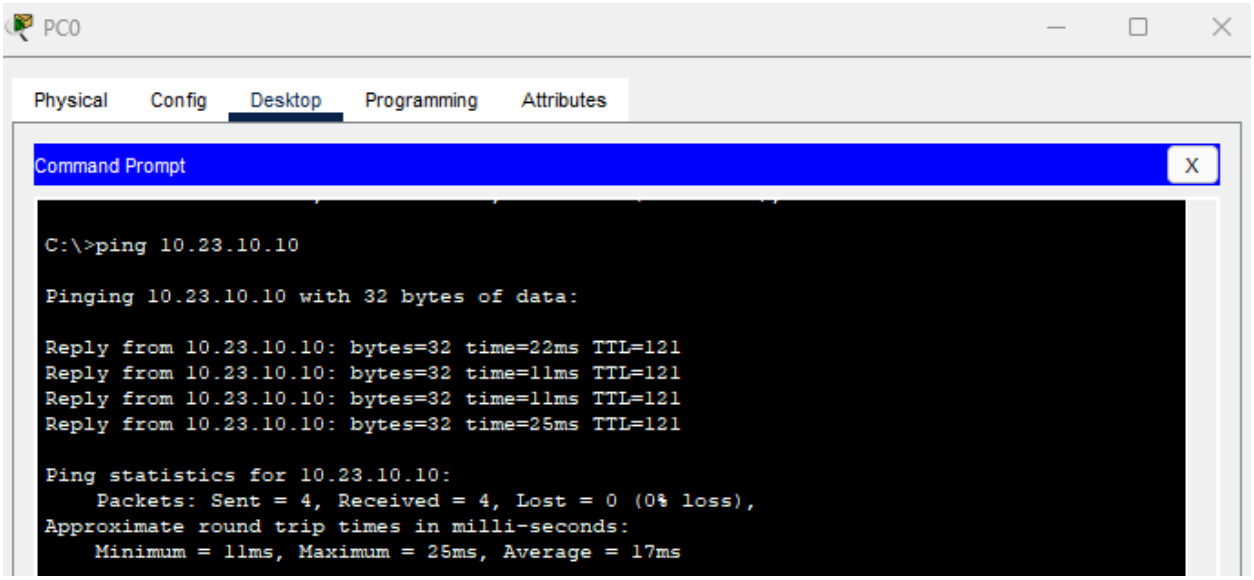
=> Như vậy là đã thiết lập xong

Cuối cùng ta tiến hành kiểm tra cấu hình như sau:

- Tại Router1, với lệnh show crypto ipsec sa thì có thể thấy chưa có gói tin nào đi qua VPN:

```
Router1#show crypto ip
Router1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: MYMAP, local addr 203.23.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
   remote  ident (addr/mask/prot/port): (10.23.0.0/255.255.0.0/0/0)
   current_peer 204.23.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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.: 203.23.1.2, remote crypto endpt.:204.23.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)
```

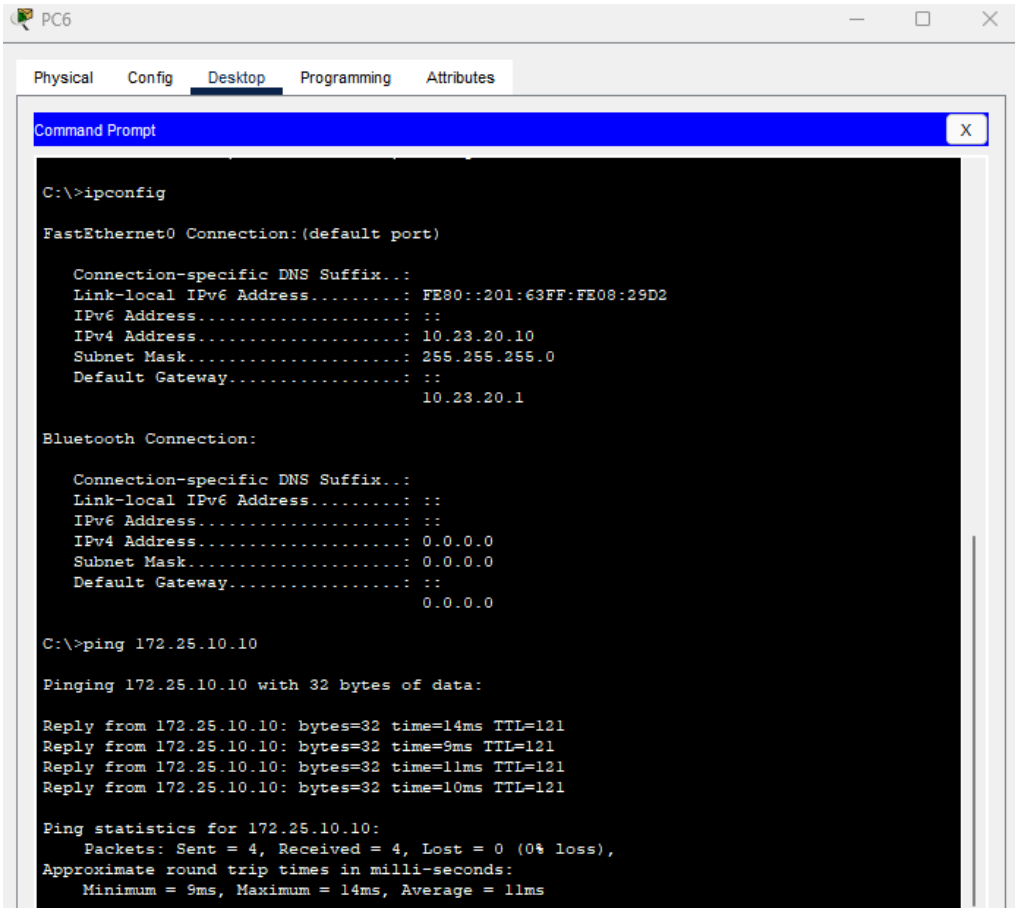
- Sau đó ping từ 172.24.10.10 (PC0 của VLAN 10) qua 10.23.10.10:



- Sau đó kiểm tra lại lệnh show crypto ipsec sa tại Router1:

```
Router1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: MYMAP, local addr 203.23.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
   remote  ident (addr/mask/prot/port): (10.23.0.0/255.255.0.0/0/0)
   current_peer 204.23.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #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 1, #recv errors 0

     local crypto endpt.: 203.23.1.2, remote crypto endpt.:204.23.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0xB3C9BEC7(3016343239)
```

- Ở chiều ngược lại ping từ 10.23.20.10 đến 172.25.10.10:



- Sau đó kiểm tra Router2:

```
Router2#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: MYMAP, local addr 204.23.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.23.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
   current_peer 203.23.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 11, #pkts decrypt: 11, #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.: 204.23.1.2, remote crypto endpt.:203.23.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0xF5DBDFA3(4124827555)

     inbound esp sas:
      spi: 0xB3C9BEC7(3016343239)
```

=> Như vậy là các gói tin kết nối VPN đi qua được mã hoá và giải mã. Cấu hình VPN đã hoàn thành như mong đợi.

6. Kết luận và đề xuất một số giải pháp nâng cao hiệu suất

6.1. Kết luận

Hệ thống mạng đã được thiết kế và triển khai hoàn chỉnh, đáp ứng đầy đủ các yêu cầu về kết nối, dịch vụ, bảo mật, và khả năng quản lý. Việc sử dụng các công nghệ như VLAN, VTP, EtherChannel, NAT, và VPN giúp tối ưu hóa hiệu suất và đảm bảo tính bảo mật. Hệ thống mạng không chỉ đảm bảo kết nối hiệu quả giữa các thành phần tại Hội sở và Chi nhánh, mà còn cung cấp khả năng mở rộng linh hoạt cho tương lai. Các thử nghiệm về dịch vụ, bảo mật và kết nối đều cho kết quả thành công, minh chứng cho sự phù hợp của mô hình mạng được triển khai.

6.2. Đề xuất một số giải pháp nâng cao hiệu suất

Cải thiện thiết bị phần cứng:

- Sử dụng switch và router thế hệ mới với băng thông cao hơn để hỗ trợ lưu lượng mạng lớn hơn.
- Trang bị thiết bị tường lửa chuyên dụng để tăng cường bảo mật và giảm tải cho router.

Áp dụng các giao thức định tuyến tiên tiến:

- Sử dụng giao thức OSPF hoặc EIGRP thay vì RIP để cải thiện tốc độ định tuyến và tối ưu hóa mạng lưới lớn.

Tăng cường băng thông:

- Sử dụng đường truyền tốc độ cao hơn giữa Hội sở và Chi nhánh để giảm độ trễ và tăng khả năng đáp ứng.

- Triển khai Link Aggregation trên các kết nối giữa Core Switch và Distribution Switch.

Tối ưu hóa bảo mật:

- Thực hiện kiểm tra bảo mật định kỳ với các công cụ xâm nhập (penetration testing) để phát hiện và khắc phục lỗ hổng.
- Triển khai hệ thống giám sát mạng tập trung (SIEM - Security Information and Event Management) để phát hiện sớm các mối đe dọa.

Tăng cường khả năng dự phòng:

- Cấu hình dự phòng nóng (Hot Standby Router Protocol - HSRP) hoặc VRRP trên router để đảm bảo tính sẵn sàng cao.
- Xây dựng kịch bản phục hồi thảm họa (Disaster Recovery Plan) để bảo vệ dữ liệu và dịch vụ trong trường hợp sự cố lớn.

Cải thiện chất lượng dịch vụ (QoS):

- Triển khai QoS trên mạng để ưu tiên các ứng dụng quan trọng như VoIP hoặc Video Conference, đảm bảo trải nghiệm người dùng tốt hơn.

Nâng cấp dịch vụ WiFi:

- Sử dụng công nghệ WiFi 6 để cải thiện tốc độ và khả năng xử lý nhiều thiết bị cùng lúc.
- Tích hợp giải pháp quản lý WiFi tập trung để dễ dàng quản trị và mở rộng.

Đào tạo đội ngũ IT:

- Tổ chức các khóa đào tạo định kỳ để nâng cao kỹ năng cho đội ngũ IT, đảm bảo khả năng quản lý và vận hành hiệu quả hệ thống mạng.