

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA



BÁO CÁO BÀI TẬP LỚN
TRUYỀN SỐ LIỆU VÀ MẠNG

Đề tài:

CẤU HÌNH THIẾT BỊ BẰNG PHẦN MỀM MÔ PHỎNG MẠNG:

CẤU HÌNH MẠNG LAN/WAN

Configure Devices Using Network Simulation Software:

Configuring LAN/WAN Network

LỚP L05 - NHÓM 04 - HK242

GVHD: VÕ TUẤN KIỆT

Thành viên trong nhóm:

MSSV	Họ và tên	Đánh giá
2213758	Văn Đắc Phong Trực	
2212832	Hà Phước Việt Quốc	
2211735	Thái Trung Kiên	

Thành phố Hồ Chí Minh, ngày .. tháng .. năm 2025

MỤC LỤC

1. Mở đầu	4
1.1. Giới thiệu đề tài.....	4
1.2. Mục tiêu nghiên cứu	4
1.3. Phạm vi nghiên cứu	5
2. Cơ sở lý thuyết.....	7
2.1. Khái niệm mạng LAN	7
2.1.1. Định nghĩa của mạng LAN (Local Area Network)	7
2.1.2. Phạm vi và cấu trúc của mạng LAN.....	7
2.1.3. Dynamic Host Configuration Protocol.....	9
2.2. Khái niệm mạng WAN	10
2.2.1. Định nghĩa của mạng WAN	10
2.2.2. Đặc điểm của mạng WAN	11
2.2.3. Phạm vi và cấu trúc của mạng WAN	11
2.3. So sánh mạng LAN và WAN	12
2.4. Các định nghĩa trong một hệ thống mạng.....	13
2.4.1. TCP/IP	13
2.4.2. Subnet Mask	15
2.4.3. Gateway	17
2.4.3.1. Khái niệm Gateway	17
2.4.3.2. Cách hoạt động của Gateway	17
2.4.3.3. Chức năng của Gateway.....	18
2.4.3.4. Lợi ích của Gateway	19
2.4.4. DNS.....	19
Khái niệm về DNS:	19
2.5. Các thiết bị mạng cơ bản	20
2.5.1. Router	20
2.5.2. Switch	22

2.6. Các giao thức định tuyến trong kết nối mạng LAN/WAN	23
2.6.1. Giao thức RIP	23
2.6.2. Giải thuật OSPF	24
2.6.3. Giải thuật EIGRP.....	26
2.7. Phần mềm mô phỏng mạng	28
3. Thực hiện mô phỏng trên phần mềm.....	30
3.1. Chuẩn bị môi trường mô phỏng.....	30
3.2. Thiết kế mô hình mạng	31
3.2.1. Xây dựng topology mạng LAN đơn giản	31
3.2.2. Mở rộng sang mạng WAN.....	36
3.3. Kết quả mô phỏng cấu hình thiết bị mạng.....	45
3.3.1. Cấu hình cho các thiết bị trong mạng LAN.....	45
3.3.2. Cấu hình định tuyến (routing) cho mạng WAN.....	47
3.4. Kiểm tra và đánh giá	52
3.5. Mô phỏng hệ thống mạng thực tế.....	53
4. Nhận xét	56
4.1. Ưu điểm của phương pháp mô phỏng so với thực tế.....	56
4.2. Hạn chế gặp phải trong quá trình cấu hình.	57
4.3. Đề xuất cải tiến mô hình mạng.....	57
5. Kết luận và hướng phát triển.....	58
5.1. Kết luận.....	58
5.2. Hướng phát triển	60
5.2.1. Mở rộng mô hình với các giao thức phức tạp hơn (như VLAN, VPN)..	60
5.2.2. Ứng dụng vào các kịch bản thực tế (doanh nghiệp, trường học).	60
6. Tài liệu tham khảo	62

1. Mở đầu

1.1. Giới thiệu đề tài

Trong thời đại công nghệ thông tin phát triển mạnh mẽ như hiện nay, mạng máy tính đã trở thành một phần không thể thiếu trong đời sống, học tập và công việc. Đặc biệt, mạng LAN (Local Area Network) và WAN (Wide Area Network) đóng vai trò quan trọng trong việc kết nối các thiết bị, chia sẻ tài nguyên và đảm bảo hiệu quả hoạt động của các hệ thống mạng hiện đại. Mạng LAN cung cấp khả năng kết nối nhanh chóng trong phạm vi nhỏ như văn phòng, trường học, trong khi mạng WAN mở rộng phạm vi kết nối trên các khu vực địa lý rộng lớn, hỗ trợ liên kết toàn cầu. Sự phát triển của hai loại mạng này không chỉ nâng cao hiệu suất làm việc mà còn đặt nền tảng cho các ứng dụng công nghệ tiên tiến như điện toán đám mây, Internet vạn vật (IoT) hay trí tuệ nhân tạo.

Bên cạnh đó, việc thiết kế và cấu hình mạng ngày càng trở nên phức tạp, đòi hỏi sự chính xác và hiệu quả cao. Đây là lúc phần mềm mô phỏng mạng phát huy vai trò quan trọng. Các công cụ mô phỏng như Cisco Packet Tracer, GNS3 hay NS-3 cho phép người dùng thử nghiệm, phân tích và tối ưu hóa cấu hình mạng trong môi trường ảo trước khi triển khai thực tế. Nhờ vậy, chúng giúp giảm thiểu rủi ro, tiết kiệm chi phí và thời gian, đồng thời cung cấp một nền tảng học tập trực quan cho sinh viên và chuyên gia trong lĩnh vực mạng.

Lý do chọn đề tài này xuất phát từ tính thực tiễn và tiềm năng ứng dụng rộng rãi của nó. Trong bối cảnh nhu cầu về mạng máy tính ngày càng tăng, việc hiểu rõ tầm quan trọng của mạng LAN/WAN cũng như cách sử dụng phần mềm mô phỏng để thiết kế và quản lý mạng không chỉ hỗ trợ hiệu quả trong học tập mà còn mang lại giá trị thực tiễn trong công việc, đặc biệt là đối với các ngành liên quan đến công nghệ thông tin và viễn thông. Đề tài này không chỉ mang tính học thuật mà còn đáp ứng nhu cầu thực tế của xã hội hiện đại.

1.2. Mục tiêu nghiên cứu

Nghiên cứu này được thực hiện với hai mục tiêu chính, nhằm khai thác sâu hơn về vai trò và ứng dụng của phần mềm mô phỏng trong việc thiết kế, cấu hình và quản lý các hệ thống mạng LAN (Local Area Network) và WAN (Wide Area Network), từ đó cung cấp một cái nhìn toàn diện về hiệu quả của các công cụ này trong môi trường hiện đại.

Mục tiêu đầu tiên là tìm hiểu và làm quen với cách sử dụng phần mềm mô phỏng mạng, chẳng hạn như Cisco Packet Tracer, GNS3 hoặc các công cụ tương tự, để thực hiện cấu hình các hệ thống mạng LAN và WAN trong một môi trường ảo. Quá trình này bao gồm việc nghiên cứu cách thiết lập các thành phần cơ bản của mạng như switch, router, máy chủ và máy trạm, cũng như cách gán địa chỉ IP, thiết lập các giao thức định tuyến (như RIP, OSPF hoặc BGP), và áp dụng các chính sách bảo mật cần thiết. Việc tìm hiểu này không chỉ dừng lại ở lý thuyết mà còn đi sâu vào thực hành, giúp người nghiên cứu hiểu rõ cách các công cụ mô phỏng tái hiện hoạt động của mạng thực tế, từ đó hỗ trợ quá trình thiết kế mạng một cách chính xác và hiệu quả. Đặc biệt, mục tiêu này còn hướng đến việc khám phá các tính năng nâng cao của phần mềm, chẳng hạn như mô phỏng lưu lượng mạng, kiểm tra khả năng chịu tải hoặc xử lý các sự cố mạng phổ biến.

Mục tiêu thứ hai là xây dựng một mô hình mạng mẫu cụ thể, kết hợp cả mạng LAN và WAN, để mô phỏng hoạt động của hệ thống trong các kịch bản thực tế. Mô hình này sẽ được thiết kế dựa trên các yêu cầu cụ thể, chẳng hạn như kết nối một mạng nội bộ (LAN) trong một văn phòng với một mạng diện rộng (WAN) liên kết các chi nhánh ở các địa điểm khác nhau. Sau khi hoàn thiện, nghiên cứu sẽ tiến hành phân tích hiệu quả hoạt động của mô hình thông qua việc đánh giá các yếu tố quan trọng như tốc độ truyền dữ liệu, độ trễ của mạng, khả năng xử lý lưu lượng lớn, tính ổn định khi gặp sự cố, và khả năng mở rộng khi cần bổ sung thêm thiết bị hoặc người dùng. Quá trình phân tích không chỉ dừng lại ở việc thu thập số liệu mà còn bao gồm việc so sánh các kết quả với tiêu chuẩn thực tế, từ đó rút ra những ưu điểm nổi bật cũng như những hạn chế còn tồn tại trong mô hình. Dựa trên kết quả này, nghiên cứu sẽ đề xuất các phương án tối ưu hóa hoặc cải tiến, chẳng hạn như điều chỉnh cấu hình, nâng cấp thiết bị hoặc thay đổi giao thức, nhằm nâng cao hiệu suất tổng thể của hệ thống mạng.

Thông qua việc thực hiện hai mục tiêu trên, nghiên cứu không chỉ mang lại giá trị học thuật bằng cách làm rõ cách thức hoạt động của phần mềm mô phỏng mạng, mà còn cung cấp những kỹ năng thực tiễn cần thiết để áp dụng vào công việc thực tế. Kết quả của nghiên cứu có thể được sử dụng như một tài liệu tham khảo hữu ích cho sinh viên, kỹ sư mạng hoặc những người quan tâm đến lĩnh vực công nghệ thông tin, đặc biệt trong bối cảnh nhu cầu về các hệ thống mạng hiệu quả và đáng tin cậy ngày càng gia tăng trong xã hội hiện đại.

1.3. Phạm vi nghiên cứu

Nghiên cứu này giới hạn phạm vi tập trung vào các khía cạnh cơ bản nhưng thiết yếu trong việc thiết kế và cấu hình mạng LAN (Local Area Network) và WAN (Wide Area Network) thông qua việc sử dụng phần mềm mô phỏng. Cụ thể, nghiên cứu sẽ chỉ tập trung vào việc cấu hình các thiết bị mạng cơ bản, bao gồm router, switch và PC, vốn là những thành phần chủ chốt trong hầu hết các hệ thống mạng hiện nay. Router sẽ được sử dụng để định tuyến lưu lượng giữa các mạng khác nhau, switch đảm nhận vai trò kết nối các thiết bị trong cùng một mạng LAN, còn PC đại diện cho các thiết bị đầu cuối như máy trạm hoặc máy khách. Việc giới hạn ở các thiết bị này nhằm đảm bảo nghiên cứu đi sâu vào các nguyên tắc cơ bản của mạng mà không bị phân tán bởi các thiết bị hoặc công nghệ phức tạp hơn như firewall, server chuyên dụng hay các thiết bị không dây.

Về công cụ, nghiên cứu chọn sử dụng phần mềm mô phỏng mạng phổ biến là Cisco Packet Tracer. Đây là một phần mềm được đánh giá cao nhờ giao diện thân thiện, tính năng đa dạng và khả năng mô phỏng chính xác các hoạt động của mạng thực tế. Cisco Packet Tracer cho phép người dùng thiết kế, cấu hình và kiểm tra các mô hình mạng mà không cần đến phần cứng vật lý, đồng thời hỗ trợ nhiều giao thức và thiết bị mạng phổ biến. Việc lựa chọn công cụ này không chỉ đảm bảo tính khả thi trong quá trình thực hiện mà còn phù hợp với mục tiêu học tập và ứng dụng thực tiễn, đặc biệt đối với những người mới bắt đầu tìm hiểu về mạng máy tính.

Phạm vi mô phỏng của nghiên cứu sẽ tập trung vào việc xây dựng và phân tích các mô hình mạng LAN/WAN cơ bản, phản ánh các ứng dụng thực tế thường gặp. Cụ thể, mô hình mạng LAN sẽ được thiết kế để mô phỏng một mạng nội bộ, chẳng hạn như mạng trong một văn phòng nhỏ hoặc một lớp học, với các thiết bị được kết nối qua switch và sử dụng địa chỉ IP tĩnh hoặc động. Trong khi đó, mô hình WAN sẽ mở rộng để kết nối nhiều mạng LAN ở các vị trí địa lý khác nhau thông qua router, mô phỏng các tình huống như liên kết giữa các chi nhánh của một công ty. Các kịch bản mô phỏng sẽ được xây dựng sao cho gần gũi với thực tế, ví dụ như truyền tải dữ liệu giữa các máy tính, kiểm tra kết nối qua lệnh ping hoặc thiết lập giao thức định tuyến đơn giản như RIP. Nghiên cứu không đi sâu vào các hệ thống mạng phức tạp như mạng doanh nghiệp quy mô lớn hoặc mạng không dây, nhằm giữ cho phạm vi phù hợp với mục tiêu và nguồn lực hiện có.

Tóm lại, phạm vi nghiên cứu được giới hạn ở việc cấu hình các thiết bị cơ bản (router, switch, PC), sử dụng Cisco Packet Tracer làm công cụ chính, và tập trung vào mô phỏng các mạng LAN/WAN cơ bản để phản ánh các ứng dụng thực

tế. Sự giới hạn này giúp đảm bảo tính tập trung, khả thi và phù hợp với mục tiêu tìm hiểu cũng như ứng dụng của đề tài.

2. Cơ sở lý thuyết

2.1. Khái niệm mạng LAN

2.1.1. Định nghĩa của mạng LAN (Local Area Network)

Mạng cục bộ là một hệ thống mạng máy tính cục bộ, cho phép các thiết bị như máy tính, máy in và các thiết bị khác kết nối và giao tiếp với nhau trong một phạm vi địa lý giới hạn, như trong một văn phòng, tòa nhà hoặc trường học. Kết nối trong mạng LAN thường được thiết lập thông qua cáp mạng hoặc kết nối không dây (Wi-Fi), giúp các thiết bị chia sẻ dữ liệu và tài nguyên một cách hiệu quả.

2.1.2. Phạm vi và cấu trúc của mạng LAN

Mạng LAN thường được triển khai trong các khu vực nhỏ như văn phòng, nhà riêng, trường học hoặc doanh nghiệp, với phạm vi không vượt quá 100 mét. Trong phạm vi này, các thiết bị có thể kết nối và giao tiếp với nhau để chia sẻ tài nguyên và thông tin.

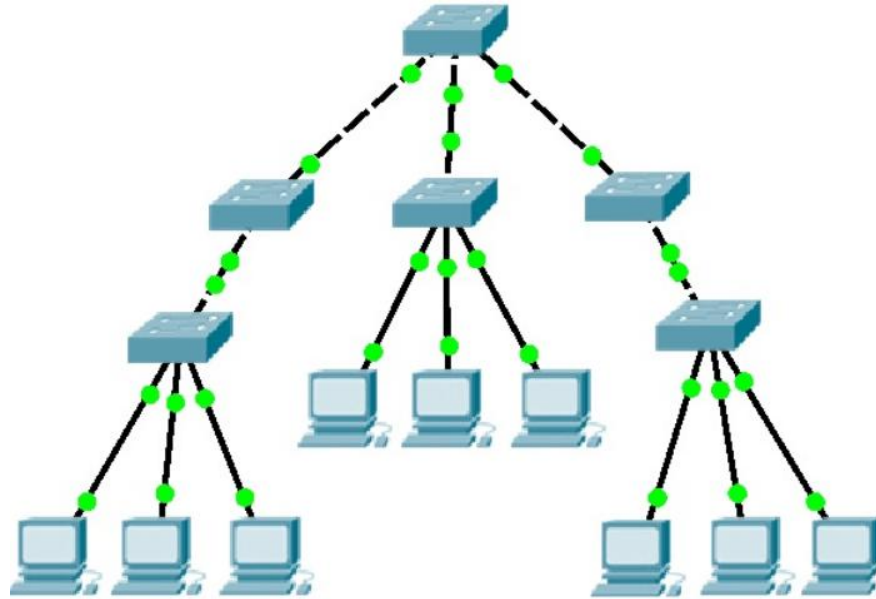
Các kiểu cấu trúc của mạng LAN:

Mạng hình sao, thường có một trung tâm điều phối gồm 1 switch hay hub, các thiết bị như PC, máy in,... được kết nối độc lập tới trung tâm. Ưu điểm là dễ quản lý, mở rộng linh hoạt, lỗi ở một thiết bị không ảnh hưởng mạng. Hạn chế khi trung tâm hỏng thì toàn mạng ngưng hoạt động và khoảng cách kết nối bị giới hạn (~100m).



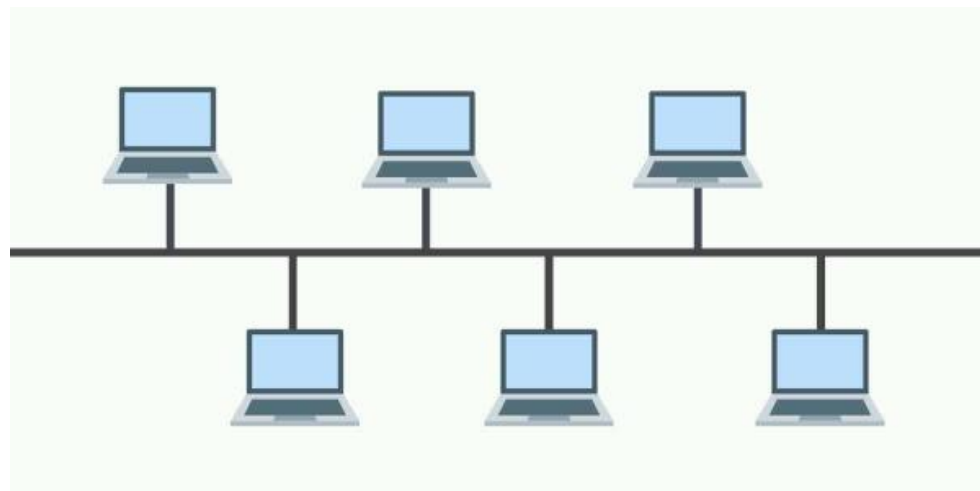
Hình 1: Mô hình mạng hình sao (Stars)

(Tree Topology) Mạng cây hay còn gọi là mạng phân cấp: là sự kết hợp của mạng hình sao mở rộng, giúp xây dựng hệ thống mạng rộng lớn và có tổ chức. Thích hợp cho trường học, doanh nghiệp lớn, hoặc các hệ thống nhiều tầng/phòng ban. Dễ phân quyền, quản lý lưu lượng mạng, triển khai theo từng nhánh.



Hình 2: Cấu trúc mạng hình cây

Mạng hình tuyến: Các thiết bị nối trên một trục dây cáp chính. Ưu điểm là tiết kiệm dây, dễ lắp đặt, Nhược điểm dễ nghẽn dữ liệu, khó phát hiện lỗi, sửa chữa ảnh hưởng toàn mạng.



Hình 3: Cấu trúc mạng bus

Mạng dạng lưới, mỗi thiết bị kết nối với tất cả thiết bị khác, dạng này có Rất ổn định, độ tin cậy cao và được sử dụng trong những ứng dụng quan trọng như an ninh, quốc phòng, nhà máy điện.

2.1.3. Dynamic Host Configuration Protocol

Đối với môi trường lớn có nhiều thiết bị kết nối, việc cấu hình địa chỉ IP bằng tay là điều không thể. Vì thế ta sử dụng DHCP, một giao thức mạng được sử dụng để tự động cấu hình địa chỉ IP cho những thiết bị kết nối vào mạng. Khi một thiết bị mới kết nối vào mạng, DHCP cho phép máy chủ DHCP tự động cấu hình những thông số cần thiết cho thiết bị, bao gồm địa chỉ IP, subnet mask, default gateway và những máy chủ DNS. Quá trình này giúp cho việc quản lý địa chỉ IP trên mạng trở nên dễ dàng và hiệu quả hơn, đồng thời giảm thiểu lỗi do cấu hình địa chỉ IP sai hoặc trùng lặp trên mạng. DHCP là một giao thức mạng phổ biến được sử dụng trong hầu hết mạng LAN (Local Area Network) và WAN (Wide Area Network).



Hình 4: Giao thức DHCP

Cách hoạt động DHCP (Dynamic Host Configuration Protocol) là giao thức tự động cấp phát địa chỉ IP cho các thiết bị trong mạng. Quá trình hoạt động của DHCP bao gồm 4 bước chính:

DHCP Discover: Thiết bị mới kết nối vào mạng sẽ gửi một yêu cầu broadcast để tìm kiếm DHCP server (thường là router).

DHCP Offer: DHCP server nhận yêu cầu và gửi lại một đề xuất gồm địa chỉ IP và các thông tin cấu hình như gateway, DNS server.

DHCP Request: Thiết bị nhận được offer sẽ gửi yêu cầu xác nhận để sử dụng địa chỉ IP được cấp phát.

DHCP Acknowledgement: DHCP server gửi một thông báo xác nhận và cấp phát địa chỉ IP cho thiết bị.

Tầm quan trọng của DHCP:

DHCP (Dynamic Host Configuration Protocol) là một giao thức mạng quan trọng, giúp tự động cấp phát địa chỉ IP cho các thiết bị trên mạng mà không cần phải cấu hình thủ công. Điều này làm đơn giản hóa quá trình thiết lập mạng, giảm thiểu các sai sót do cấu hình sai và tiết kiệm thời gian cho người quản trị mạng. Ngoài việc cấp phát địa chỉ IP, DHCP còn cung cấp các thông tin cấu hình mạng khác như địa chỉ máy chủ DNS, địa chỉ gateway mặc định và các thông tin mạng khác. Việc cấu hình thủ công những thông tin này cho từng thiết bị trong mạng sẽ rất phức tạp, đặc biệt là trong các mạng có quy mô lớn.

Hơn nữa, DHCP giúp việc quản lý các thiết bị trong mạng trở nên dễ dàng hơn. Quản trị viên mạng có thể theo dõi và quản lý các địa chỉ IP đã cấp phát cho thiết bị. Nếu một thiết bị không còn sử dụng trong một khoảng thời gian dài, địa chỉ IP của nó có thể được thu hồi và cấp lại cho thiết bị khác, giúp tối ưu hóa tài nguyên mạng. Vì vậy, DHCP là một phần không thể thiếu trong các mạng lớn và phức tạp, đóng vai trò quan trọng trong việc duy trì sự ổn định và hiệu quả hoạt động của mạng.

2.2. Khái niệm mạng WAN

2.2.1. Định nghĩa của mạng WAN

Mạng WAN (Wide Area Network) là một hệ thống mạng diện rộng kết nối nhiều mạng LAN hoặc các thiết bị ở khoảng cách lớn, có thể là giữa các thành phố, quốc gia hoặc thậm chí toàn cầu. Mạng WAN giúp truyền tải dữ liệu qua các khoảng cách xa bằng cách sử dụng các công nghệ như cáp quang, vệ tinh hoặc mạng di động.

Nhiều WAN kết nối với nhau tạo thành mạng GAN. Nếu kết nối WAN không tồn tại, các tổ chức sẽ bị cô lập trong các khu vực hạn chế hoặc các khu vực địa lý

cụ thể. Mạng LAN sẽ cho phép các tổ chức làm việc trong tòa nhà của họ, nhưng sự phát triển ra các khu vực bên ngoài - các thành phố khác nhau hoặc thậm chí các quốc gia khác nhau - sẽ không thể thực hiện được vì cơ sở hạ tầng liên quan sẽ có chi phí cao đối với hầu hết các tổ chức.

Khi các tổ chức phát triển và trở nên quốc tế, mạng WAN cho phép họ giao tiếp giữa các chi nhánh, chia sẻ thông tin và duy trì kết nối. Khi nhân viên đi công tác, mạng WAN cho phép họ truy cập thông tin họ cần để thực hiện công việc của mình. Mạng WAN cũng giúp các tổ chức chia sẻ thông tin với khách hàng, cũng như các tổ chức đối tác, chẳng hạn như khách hàng B2B hoặc khách hàng.

2.2.2. Đặc điểm của mạng WAN

Phạm vi rộng: Có thể phủ sóng từ vài km đến hàng ngàn km, vì vậy nó có thể kết nối các văn phòng của một công ty lại với nhau.

Tốc độ truyền dữ liệu: Thường thấp hơn so với mạng LAN do khoảng cách xa và ảnh hưởng của hạ tầng viễn thông, khi đường truyền càng xa cũng ảnh hưởng nhiều đến chất lượng của data, nếu tốc độ cao sẽ có nhiều bit error, vì vậy người ta giới hạn tốc độ truyền dữ liệu ở một mức cho phép.

Công nghệ kết nối: Sử dụng các đường truyền như cáp quang, vệ tinh, mạng di động (3G, 4G, 5G) hoặc đường truyền thuê riêng (*leased line*).

Chi phí cao: Do yêu cầu về hạ tầng và bảo trì phức tạp, khi hạ tầng dễ bị hư do thiên tai bão lũ, chi phí bảo trì ở mức rất cao.

Bảo mật: Cần các biện pháp mã hóa và bảo mật cao hơn do dữ liệu truyền qua nhiều hệ thống mạng trung gian.

2.2.3. Phạm vi và cấu trúc của mạng WAN

Phạm vi kết nối mạng WAN:

- + Kết nối các văn phòng của một doanh nghiệp có khoảng cách lớn vài km.
- + Kết nối các văn phòng của một doanh nghiệp trên toàn thế giới.
- + Có thể kết nối đến tất cả các vùng mà internet cáp quang không phủ cập bằng các phương pháp tiên tiến như Starlink của công ty SpaceX.

+ Kết nối các tàu thuyền, hàng không, hàng hải lại với nhau, phù hợp cho việc điều khiển hoạt động tránh xảy ra va chạm và an toàn tham gia giao thông

2.3. So sánh mạng LAN và WAN

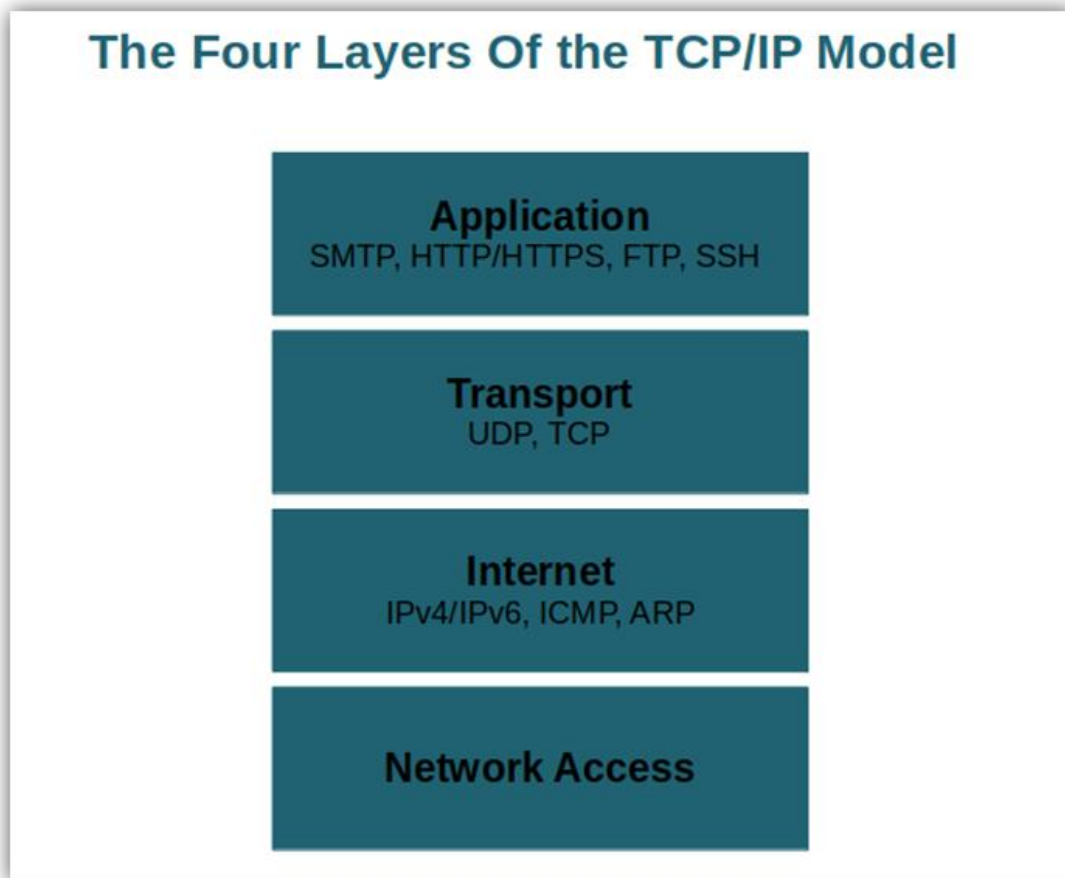
Tiêu chí	LAN	WAN
Phạm vi	Phạm vi tương đối nhỏ, chủ yếu trong một tòa nhà, hay một khuôn viên của trường học hay công ty.	Phạm vi tương đối lớn, có thể sự kết nối của khu vực lại với nhau cũng như kết nối toàn cầu lại với nhau.
Khoảng cách	Vài mét đến 1 km	Từ 1 km đến hàng ngàn km
Tốc độ	100Mbps đến 10Gbps	1 Mbs đến 1 Gbs, phụ thuộc vào hạ tầng.
Độ trễ	Rất thấp, hầu như không tồn tại độ trễ	Độ trễ cao, có thể đến 100ms, tùy vào độ dài của đường truyền mạng
Băng thông	Băng thông lớn và ổn định	Băng thông bị giới hạn ở mức nhất định
Công nghệ kết nối	Ethernet, cáp đồng, cáp quang, Wifi	Cáp quang biển, MPLS, Leased Line, VPN, vệ tinh.
Chi phí	Chi phí triển khai tương đối thấp, vì ngày nay hệ thống mạng cục bộ hầu hết đã trở nên đại trà.	Chi phí cao, cần những thiết bị phức tạp để kết nối các đầu đuôi lại với nhau, vệ tinh, cáp quang xuyên biển. Chi phí sửa chữa rất tốn kém
Quản lý	Do một tổ chức kiểm soát	Nhiều nhà mạng tham gia kiểm soát mạng.
Bảo mật	Bảo mật cao hơn, do không chia sẻ dữ liệu ra bên ngoài	Có lượng truy cập từ nhiều nơi, có thể bị tấn công và đánh cắp dữ liệu.

2.4. Các định nghĩa trong một hệ thống mạng

2.4.1. TCP/IP

Để hai thiết bị bất kì giao tiếp với nhau thì chúng ta phải dùng một loại ngôn ngữ chung để chúng hiểu nhau, đối với các thiết bị mạng hay cụ thể là máy tính làm sao nó có thể hiểu đâu là độ dài dữ liệu, đâu là dữ liệu thực chất, đâu là địa chỉ của máy nhận, đâu là điện chỉ của máy thu, do đó TCP/IP ra đời để giải quyết các vấn đề trên, một giao thức mà rất quan trọng trong công việc về mạng. *TCP (Transmission Control Protocol)/ IP (Internet Protocol)* là hai giao thức cốt lõi của bộ giao thức TCP/IP, nền tảng của mọi kết nối Internet và mạng máy tính hiện đại.

Để cho phép các máy tính giao tiếp với nhau TCP/IP sử dụng mô hình truyền thông nhiều lớp khác nhau, khi qua mỗi lớp dữ liệu được bao bọc thêm nhiều thông tin, đảm bảo quá trình truyền dữ liệu chính xác hơn.



Hình 5: Các lớp (layer) trong TCP/IP model

Lớp 1: Application Layer:

Lớp ứng dụng là tầng cao nhất trong mô hình TCP/IP. Đây là lớp mà người dùng trực tiếp tương tác khi gửi và nhận dữ liệu. Nó cũng chịu trách nhiệm tạo ra

dữ liệu và yêu cầu kết nối. Trong ví dụ về việc gửi email xin nghỉ phép cho sếp, hệ thống email của bạn chính là một phần của lớp ứng dụng. Một số giao thức quan trọng trong lớp này bao gồm:

- + Giao thức truyền thư đơn giản (SMTP - Simple Mail Transfer Protocol): Dùng để gửi email. Đây là giao thức bạn đã sử dụng khi gửi email cho sếp.

- + Giao thức truyền siêu văn bản/phiên bản bảo mật (HTTP/HTTPS - Hypertext Transfer Protocol/Secure):

- + Cả hai đều được sử dụng để truy cập web. HTTPS (phiên bản bảo mật hơn của HTTP nhờ mã hóa) là giao thức bạn đang dùng để đọc bài viết này. Đây là những giao thức bạn sử dụng mỗi khi lướt internet.

- + Giao thức truyền tệp (FTP - File Transfer Protocol): Dùng để truyền tệp từ hệ thống này sang hệ thống khác. Bạn sẽ sử dụng giao thức này nếu muốn tải nội dung lên website của mình.

- + Secure Shell (SSH): Tương tự như Telnet nhưng bảo mật hơn. Quản trị viên hệ thống thường dùng SSH để truy cập an toàn vào máy tính từ một mạng không an toàn.

Lớp 2: The Transport Layer:

Lớp Vận chuyển thiết lập một kết nối dữ liệu tin cậy và không lỗi giữa ứng dụng/thiết bị và điểm đích. Lớp này chia nhỏ dữ liệu thành các gói tin nhỏ hơn và đánh số chúng theo thứ tự. Nó xác định:

- + Lượng dữ liệu cần được gửi,
- + Đích đến của dữ liệu, và
- + Tốc độ truyền dữ liệu (kiểm soát luồng).

Ngoài ra, lớp này còn nhận được xác nhận rằng bên nhận đã nhận được các gói tin.

Các giao thức được sử dụng trong lớp này bao gồm:

- + Giao thức UDP (User Datagram Protocol): Được sử dụng để cung cấp dịch vụ không kết nối và truyền dữ liệu từ đầu đến cuối. Nó phát hiện lỗi truyền dẫn nhưng không chỉ rõ chúng.

- + Giao thức TCP (Transmission Control Protocol): Được sử dụng để đảm bảo truyền tải gói tin một cách tin cậy. Nó cũng thiết lập kết nối mạng giữa nguồn và đích.

Lớp 3: Internet

Lớp Internet (còn gọi là lớp IP hoặc lớp mạng - không nên nhầm với lớp truy cập mạng sẽ được đề cập sau) chịu trách nhiệm gửi các gói tin và đảm bảo dữ liệu được truyền đi một cách chính xác nhất. Nó hoạt động giống như người điều phối

giao thông, kiểm soát luồng và tốc độ truyền dữ liệu. Ngoài ra, lớp này cung cấp các chức năng và phương thức để truyền các chuỗi dữ liệu.

Các giao thức chính trong lớp Internet:

- + Giao thức IPv4 và IPv6 (Internet Protocol versions 4 & 6): Được sử dụng để định tuyến dữ liệu trên mạng. Chịu trách nhiệm giao các gói tin từ máy nguồn đến máy đích bằng cách xác định địa chỉ IP trong gói tin.

- + Giao thức ICMP (Internet Control Message Protocol): Cung cấp thông báo cho các máy chủ khi có sự cố mạng (ví dụ: mất kết nối, quá tải).

- + Giao thức ARP (Address Resolution Protocol): Dùng để tìm địa chỉ phần cứng (MAC Address) của một máy tính khi đã biết địa chỉ IP của nó.

Lớp 4: Network Access

Lớp *Truy cập Mạng* (còn được gọi là lớp liên kết dữ liệu hoặc lớp vật lý) là tầng cuối cùng trong hệ thống phân cấp mô hình TCP/IP. Nó tương ứng với lớp liên kết dữ liệu và lớp vật lý trong mô hình OSI (mô hình kết nối hệ thống mở). Lớp này có các chức năng chính:

- + Thêm địa chỉ MAC đích vào các khung dữ liệu (data frames)

- + Truyền dữ liệu giữa các ứng dụng hoặc thiết bị qua mạng

Ngoài ra, lớp này còn xử lý cơ sở hạ tầng vật lý cho phép các thiết bị giao tiếp qua Internet, bao gồm:

- + Cáp Ethernet

- + Mạng không dây (Wi-Fi)

- + Card giao diện mạng (NIC)

- + Trình điều khiển (drivers) và các thành phần khác

2.4.2. Subnet Mask

Subnet Mask, hiểu đơn giản là các mạng con, thường được biểu thị dưới dạng một dãy số thập phân chia bởi dấu chấm (ví dụ: 255.255.255.0), là một thành phần quan trọng trong địa chỉ IP (Internet Protocol). Nó được sử dụng để xác định phần nào của địa chỉ IP đại diện cho mạng (network) và phần nào đại diện cho máy tính cá nhân hoặc thiết bị (host) trên mạng đó.

Subnet Mask hoạt động dựa trên nguyên tắc phân biệt giữa địa chỉ mạng và địa chỉ máy tính trong một địa chỉ IP. Trong một Subnet Mask, phần của địa chỉ IP được biểu diễn bởi các bit 1 (thường là phần đầu của dãy số) chỉ ra phần địa chỉ mạng, trong khi các bit 0 chỉ ra phần địa chỉ máy tính hoặc host. Ví dụ, với Subnet Mask 255.255.255.0, ba nhóm số đầu tiên (255.255.255) xác định mạng, và nhóm cuối cùng (0) xác định máy tính cụ thể trong mạng đó.

Có năm lớp chính được xác định trong hệ thống địa chỉ IP phiên bản 4 (IPv4) - lớp A, B, C, D, và E. Mỗi lớp có đặc điểm và phạm vi địa chỉ riêng biệt, phù hợp với các mục đích sử dụng khác nhau. Dưới đây là hướng dẫn về cách tính và xác định lớp của một địa chỉ IP dựa trên những bit đầu tiên của nó.

+ Lớp A: Nếu bit đầu tiên của địa chỉ IP là 0, địa chỉ đó thuộc lớp A. Phạm vi của lớp A là từ 0.0.0.0 đến 127.255.255.255. Điều này cho phép mạng lớp A hỗ trợ một số lượng lớn các hosts.

+ Lớp B: Nếu hai bit đầu tiên là 10, địa chỉ đó thuộc lớp B. Phạm vi của lớp B là từ 128.0.0.0 đến 191.255.255.255, hỗ trợ một số lượng vừa phải các mạng và hosts.

+ Lớp C: Địa chỉ IP thuộc lớp C nếu ba bit đầu tiên là 110. Phạm vi của lớp C là từ 192.0.0.0 đến 223.255.255.255, chủ yếu dùng cho các mạng nhỏ với ít hosts hơn.

+ Lớp D: Lớp D, với bốn bit đầu là 1110, phạm vi từ 224.0.0.0 đến 239.255.255.255, được dùng cho mục đích đa phương tiện và nhóm đa điểm (multicast).

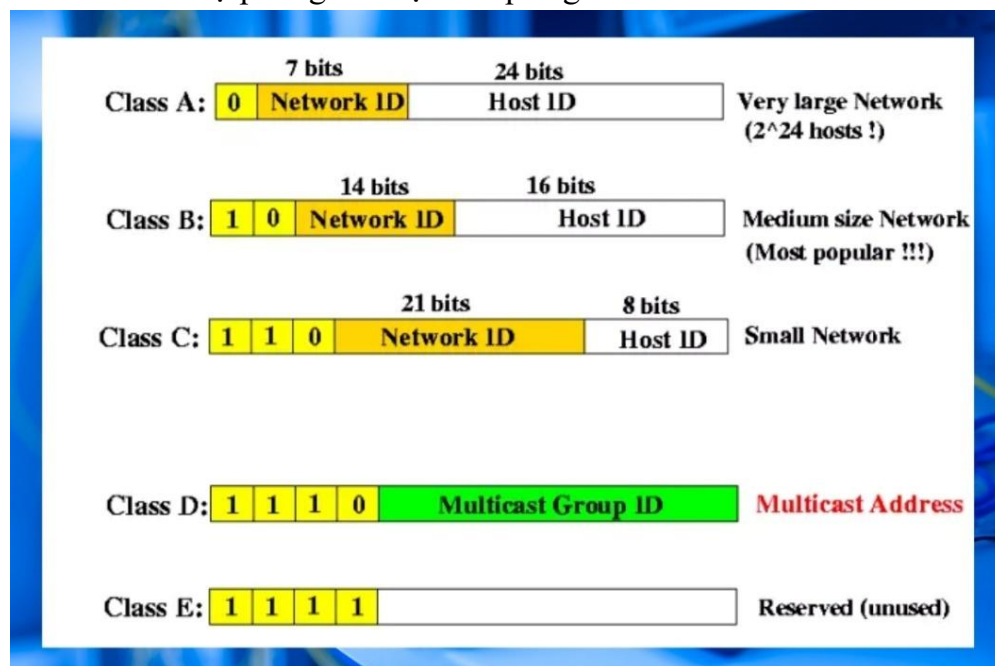
+ Lớp E: Còn lại là lớp E, từ 240.0.0.0 đến 255.255.255.255, dành riêng cho mục đích thử nghiệm và nghiên cứu.

Điều đặc biệt trong sử dụng Subnet mask:

Nếu tất cả các bit của subnet:

= 0: Dự phòng cho địa chỉ mạng (Thường không sử dụng)

= 1: Dự phòng cho địa chỉ quảng bá.



Hình 6: Các class trong hệ thống địa chỉ IP

Lý do sử dụng subnet mask:

Thứ nhất, giảm lãng phí địa chỉ IP: Chia mạng lớn thành các mạng con nhỏ hơn giúp phân phối địa chỉ IP một cách hiệu quả, giảm lãng phí và tối ưu hóa việc sử dụng chúng. Bên cạnh đó còn tăng cường bảo mật và kiểm soát mạng nhờ vào việc phân chia mạng và kiểm soát lưu lượng tốt hơn giữa các phần khác nhau của mạng. Ngoài ra, các sự cố như lỗi mạng hoặc virus có thể được cô lập dễ dàng hơn trong từng mạng con, giúp ngăn chặn sự lan truyền trên toàn mạng.

Thứ hai, tối ưu hóa hiệu suất mạng: Mỗi mạng con có lưu lượng broadcast riêng, giúp giảm bớt tổng lượng lưu lượng broadcast trong toàn mạng, nâng cao hiệu suất.

Thứ ba, quản lý mạng linh hoạt hơn: Chia mạng thành các mạng con giúp quản trị mạng linh hoạt hơn trong việc quản lý và phân phối địa chỉ IP. Khi cần mở rộng mạng, việc đã có sẵn các mạng con giúp quá trình này trở nên thuận tiện và linh hoạt hơn.

Thứ tư, tạo điều kiện cho các mạng đặc biệt: Trong một số trường hợp, việc chia mạng thành các mạng con là cần thiết để hỗ trợ các mô hình mạng phức tạp, như mạng với nhiều chi nhánh.

2.4.3. Gateway

2.4.3.1. Khái niệm Gateway

Gateway là bộ chuyển đổi giao thức, được sử dụng để nối kết hai mạng với các giao thức khác nhau. Trước khi dữ liệu được định tuyến, nó sẽ đi qua Gateway. Khi hai mạng muốn tương tác, Gateway xử lý đầu vào và đầu ra của mạng, tạo điều kiện tương thích giữa hai giao thức, hỗ trợ việc giao tiếp giữa chúng.

Nói một cách đơn giản, Gateway là điểm giao tiếp giữa hai mạng khác nhau, có khả năng phân phối lưu lượng mạng, định tuyến gói tin và thực hiện các chức năng bảo mật như tường lửa. Gateway có thể triển khai dưới dạng phần cứng hoặc phần mềm, và có thể áp dụng trong nhiều bối cảnh khác nhau, từ mạng doanh nghiệp đến mạng gia đình.

2.4.3.2. Cách hoạt động của Gateway

Gateway, hoạt động như sự kết hợp giữa modem và router, đóng vai trò quan trọng trong quản lý dữ liệu trên mạng hiện tại. Nó không chỉ chuyển hướng dữ liệu nội bộ mà còn xử lý các thông tin từ mạng ngoại vi, tạo nên một liên kết liền mạch giữa các thiết bị và mạng truy cập. Hoạt động của

gateway dựa trên việc chuyển tiếp dữ liệu giữa các mạng thông qua các giao thức và phương tiện truyền thông đa dạng. Khi một thiết bị truy cập mạng yêu cầu truy cập Internet, thông điệp sẽ được gửi đến gateway của mạng.

Công gateway lưu trữ thông tin về đường dẫn nội bộ và mạng bổ sung. Một cách đơn giản để hiểu là gateway tạo điều kiện tương thích giữa các giao thức, hoạt động như một trình chuyển đổi giao thức trên tất cả các tầng của mô hình hệ thống mở kết nối.

Gateway xử lý thông điệp bằng cách kiểm tra địa chỉ đích để xác định liệu thông điệp cần được chuyển đến mạng cục bộ hay mạng ngoại vi (Internet), tiếp theo thông điệp được chuyển tiếp đến đích tương ứng. Khi thông điệp đến gateway đích, nó được xử lý để gửi lại thông tin yêu cầu đến thiết bị truy cập mạng gốc.

Bên cạnh đó, gateway cũng có khả năng thực hiện các chức năng bảo mật như tường lửa, quản lý truy cập và theo dõi lưu lượng mạng. Ngoài ra, nó cũng có khả năng định tuyến gói tin qua các mạng khác nhau bằng cách sử dụng các giao thức định tuyến như *RIP (Routing Information Protocol)* và *OSPF (Open Shortest Path First)*.

2.4.3.3. Chức năng của Gateway

Gateway đóng một vai trò quan trọng trong việc tạo điều kiện cho giao tiếp giữa các mạng sử dụng các giao thức khác nhau. Dưới đây là một số chức năng quan trọng mà Gateway thực hiện:

- + Kết nối mạng: Gateway là một thiết bị kết nối hai hoặc nhiều mạng khác nhau, cho phép các thiết bị trong các mạng khác nhau liên kết và truyền thông tin với nhau.

- + Định tuyến gói tin: Gateway có khả năng định tuyến gói tin giữa các mạng khác nhau bằng cách sử dụng các giao thức định tuyến như *RIP (Routing Information Protocol)* và *OSPF (Open Shortest Path First)*.

- + Tường lửa: Thực hiện các chức năng bảo mật như tường lửa, bảo vệ mạng khỏi các mối đe dọa từ Internet và các mạng bên ngoài.

+ Giám sát mạng: Giám sát lưu lượng mạng và xử lý vấn đề liên quan đến mạng, hỗ trợ quản trị viên mạng trong việc phát hiện và giải quyết các vấn đề kịp thời.

+ Cải thiện hiệu suất mạng: Tối ưu hóa lưu lượng mạng và cải thiện hiệu suất bằng cách tăng tốc độ truyền dữ liệu và giảm độ trễ.

+ Kết nối các mạng khác nhau: Kết nối các loại mạng khác nhau như mạng LAN, mạng WLAN, mạng MAN, mạng WAN và Internet.

+ Chuyển đổi giao thức: Chuyển đổi giữa các giao thức khác nhau, giúp thiết bị trong các mạng khác nhau có thể trao đổi thông tin.

+ Cân bằng tải: Cân bằng tải giữa các mạng khác nhau, tối ưu hóa sự phân phối tài nguyên và tăng cường hiệu suất mạng.

2.4.3.4. Lợi ích của Gateway

Ngoài tìm hiểu Gateway là gì, bạn cũng nên biết rằng Gateway mang lại nhiều ưu điểm cho hoạt động bảo mật mạng và điều hướng lưu lượng mạng. Dưới đây là một số lợi ích của Gateway:

+ Tăng cường bảo mật mạng: Đóng vai trò như một tường lửa, bảo vệ mạng khỏi các mối đe dọa từ bên ngoài, ngăn chặn cuộc tấn công và các hoạt động xâm nhập.

+ Điều khiển lưu lượng mạng: Giám sát, điều khiển và quản lý lưu lượng truy cập, giúp giảm độ trễ và tăng tốc độ truyền dữ liệu.

+ Tối ưu hóa hiệu suất mạng: Tối ưu hóa mạng bằng cách cân bằng tải giữa các mạng, tăng tốc độ truyền dữ liệu và giảm độ trễ.

+ Cung cấp kết nối Internet: Đóng vai trò quan trọng trong mạng Internet, cho phép các thiết bị trong mạng truy cập vào các dịch vụ Internet như email, truy cập trang web, truyền thông đa phương tiện và các phần mềm trực tuyến khác.

+ Tích hợp các giao thức mạng khác nhau: Gateway kết nối các mạng sử dụng các giao thức khác nhau, giúp thiết bị trong các mạng khác nhau trao đổi thông tin và tương tác với nhau.

2.4.4. DNS

Khái niệm về DNS:

DNS (Domain Name System) là hệ thống phân giải tên miền cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên internet. Khi người dùng nhập địa chỉ trang web trên trình duyệt, DNS sẽ tìm địa chỉ IP của máy chủ chứa trang web và trả về kết quả hiển thị tương ứng của trang web cần tìm. Do đó, thay vì phải ghi nhớ địa chỉ IP phức tạp, người dùng có thể dễ dàng truy cập các trang web thông qua tên miền. Ngoài ra, DNS cũng giúp tăng tính linh hoạt và quản lý hiệu quả hơn cho hệ thống mạng, cung cấp tính bảo mật và tăng tốc độ truy cập internet.

Chức năng của DNS:

DNS là hệ thống quản lý (Management System) và chuyển đổi tên miền thành địa chỉ IP tương ứng. Cụ thể, DNS thực hiện các nhiệm vụ sau:

- + Chuyển đổi tên miền thành địa chỉ IP: DNS giúp chuyển đổi tên miền dễ đọc (ví dụ: `www.example.com`) thành địa chỉ IP (ví dụ: `192.168.1.1`) để thiết bị có thể xác định được vị trí chính xác của máy chủ trên mạng.

- + Quản lý các bản ghi DNS: DNS lưu trữ thông tin trong các bản ghi DNS, bao gồm các loại bản ghi như A (địa chỉ IPv4), AAAA (địa chỉ IPv6), CNAME (tên miền chấp nhận mệnh đề), MX (máy chủ thư điện tử) và nhiều loại khác.

- + Phân giải ngược: DNS cũng có khả năng phân giải ngược, chuyển đổi địa chỉ IP thành tên miền. Tuy nhiên, chức năng này ít được sử dụng hơn so với chuyển đổi tên miền thành địa chỉ IP.

Nhờ vào DNS, người dùng có thể truy cập các trang web và dịch vụ trực tuyến mà không cần ghi nhớ các địa chỉ IP phức tạp.

2.5. Các thiết bị mạng cơ bản

2.5.1. Router

Khái niệm về Router: Bộ định tuyến kết nối máy tính và các thiết bị khác với Internet. Bộ định tuyến hoạt động như một bộ điều phối, chọn tuyến đường tốt nhất để thông tin của bạn di chuyển. Nó kết nối doanh nghiệp của bạn với thế giới, bảo vệ thông tin khỏi các mối đe dọa bảo mật và thậm chí có thể quyết định máy tính nào được ưu tiên hơn những máy tính khác.

Các loại router có trên thị trường:

+ *Wired Router*: Là thiết bị định tuyến chỉ hỗ trợ kết nối có dây (qua cáp Ethernet). Nhận dữ liệu từ modem (qua cáp quang/ADSL) và phân phối đến các thiết bị khác thông qua cổng LAN (RJ45).

+ *Wireless Routers*: Là thiết bị định tuyến hỗ trợ cả kết nối có dây lẫn không dây (Wi-Fi). Tích hợp access point để phát sóng Wi-Fi, cho phép điện thoại, laptop kết nối không dây.

Sự cần thiết của Router:

Bộ định tuyến giúp bạn kết nối nhiều thiết bị với Internet và kết nối các thiết bị với nhau. Ngoài ra, bạn có thể sử dụng bộ định tuyến để tạo mạng cục bộ của thiết bị. Các mạng cục bộ này rất hữu ích nếu bạn muốn chia sẻ tệp giữa các thiết bị hoặc cho phép nhân viên chia sẻ các công cụ phần mềm.

Nếu bạn không có bộ định tuyến, dữ liệu của doanh nghiệp bạn sẽ không được chuyển đến đúng nơi. Ví dụ: nếu bạn muốn in một tài liệu, bạn cần một bộ định tuyến để giúp đưa tài liệu đó đến máy in – không phải đến máy tính hoặc máy quét khác.

Cách Router hoạt động:

Hãy nghĩ về bộ định tuyến như một bộ điều khiển không lưu và các gói dữ liệu như máy bay hướng đến các sân bay (hoặc mạng lưới) khác nhau. Cũng giống như mỗi máy bay có một điểm đến duy nhất và đi theo một tuyến đường duy nhất, mỗi gói cần được hướng dẫn đến đích của nó một cách hiệu quả nhất có thể. Tương tự như cách kiểm soát viên không lưu đảm bảo rằng máy bay đến đích mà không bị lạc hoặc bị gián đoạn lớn trên đường đi, bộ định tuyến giúp hướng các gói dữ liệu đến địa chỉ IP đích của chúng.

Để định hướng các gói một cách hiệu quả, một bộ định tuyến sử dụng bảng định tuyến nội bộ - một danh sách các đường dẫn đến các điểm đến mạng khác nhau. Bộ định tuyến đọc tiêu đề của gói để xác định nơi nó đang đi, sau đó tham khảo bảng định tuyến để tìm ra đường dẫn hiệu quả nhất đến đích đó. Sau đó, nó chuyển tiếp gói đến mạng tiếp theo trong đường dẫn.

Sự khác nhau giữa Router và Modem:

Mặc dù một số nhà cung cấp dịch vụ Internet (ISP) có thể kết hợp bộ định tuyến và modem trong một thiết bị duy nhất, nhưng chúng không giống nhau. Mỗi người đóng một vai trò khác nhau nhưng không kém phần quan trọng trong việc kết nối mạng với nhau và với Internet.

Bộ định tuyến hình thành mạng và quản lý luồng dữ liệu trong và giữa các mạng đó, trong khi modem kết nối các mạng đó với Internet. Modem tạo kết nối với

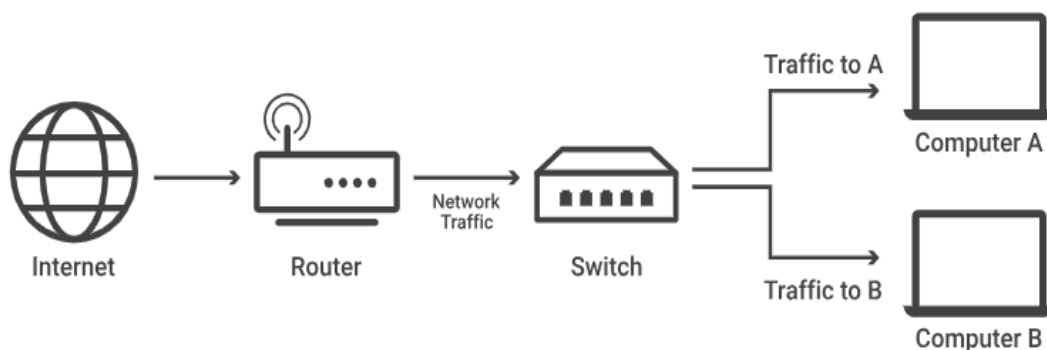
Internet bằng cách chuyển đổi tín hiệu từ ISP thành tín hiệu kỹ thuật số có thể được giải thích bởi bất kỳ thiết bị được kết nối nào. Một thiết bị duy nhất có thể cắm vào modem để kết nối với Internet; ngoài ra, bộ định tuyến có thể giúp phân phối tín hiệu này đến nhiều thiết bị trong một mạng đã thiết lập, cho phép tất cả chúng kết nối Internet đồng thời.

Nếu có bộ định tuyến, nhưng không có modem, ta sẽ có thể tạo mạng LAN và gửi dữ liệu giữa các thiết bị trên mạng đó. Tuy nhiên, ta sẽ không thể kết nối mạng đó với Internet. Mặt khác, nếu có modem, nhưng không có bộ định tuyến, ta sẽ có thể kết nối một thiết bị duy nhất với Internet (ví dụ: máy tính xách tay làm việc), nhưng không thể phân phối kết nối Internet đó cho nhiều thiết bị (máy tính xách tay và điện thoại thông minh của). Trong khi đó, nếu có một bộ định tuyến và một modem. Sử dụng cả hai thiết bị, ta có thể tạo mạng LAN với máy tính để bàn, máy tính bảng và điện thoại thông minh của mình và kết nối tất cả chúng với Internet cùng một lúc.

2.5.2. Switch

Khái niệm về Switch:

Bộ switch kết nối các thiết bị trong mạng (thường là mạng cục bộ, hoặc LAN) và chuyển tiếp các gói dữ liệu đến và đi từ các thiết bị đó. Không giống như Router, switch chỉ gửi dữ liệu vào thiết bị duy nhất mà nó được thiết kế (có thể là một bộ chuyển mạch khác, Router hoặc một máy tính của người dùng), không phải đến mạng của nhiều thiết bị.



Hình 7: Mô tả cấu trúc cơ bản của hệ thống mạng

Sự khác biệt giữa Router và Switch:

Bộ Router chọn đường dẫn cho các gói dữ liệu để băng qua mạng và đến đích của chúng. Bộ định tuyến thực hiện điều này bằng cách kết nối với các mạng khác nhau và chuyển tiếp dữ liệu từ mạng này sang mạng khác - bao gồm mạng LAN, mạng diện rộng (WAN) hoặc hệ thống tự trị, là những mạng lớn tạo nên Internet.

Trong thực tế, điều này có nghĩa là Router là cần thiết cho kết nối Internet, trong khi bộ chuyển mạch chỉ được sử dụng cho các thiết bị kết nối với nhau. Gia đình và văn phòng nhỏ cần bộ định tuyến để truy cập Internet, nhưng hầu hết không cần bộ Switch, trừ khi chúng yêu cầu một lượng lớn cổng Ethernet. Tuy nhiên, các văn phòng lớn, mạng và trung tâm dữ liệu với hàng chục hoặc hàng trăm máy tính thường yêu cầu switch, để sử dụng mạng ổn định hơn.

2.6. Các giao thức định tuyến trong kết nối mạng LAN/WAN

2.6.1. Giao thức RIP

Khái niệm:

Routing Information Protocol (RIP) là một giao thức định tuyến vectơ khoảng cách được sử dụng để xác định đường dẫn tốt nhất cho dữ liệu truyền qua mạng. RIP hoạt động ở lớp mạng (Lớp 3) của mô hình OSI và chủ yếu được sử dụng trong các mạng nhỏ hơn do tính đơn giản và dễ thực hiện.

RIP có hai phiên bản: RIPv1 và RIPv2. RIPv1 là phiên bản gốc và sử dụng địa chỉ phân loại, có nghĩa là nó không hỗ trợ mặt nạ mạng con có độ dài thay đổi (VLSM) hoặc CIDR. RIPv2 là một phần mở rộng của RIPv1 và hỗ trợ cập nhật địa chỉ, xác thực và đa hướng không lớp.

RIP phần lớn đã được thay thế bằng các giao thức định tuyến tiên tiến hơn, chẳng hạn như OSPF và EIGRP, do những hạn chế về khả năng mở rộng, hội tụ chậm và kém hiệu quả trong việc xử lý các mạng lớn. Tuy nhiên, nó vẫn được sử dụng trong một số mạng nhỏ và làm nền tảng để tìm hiểu về các giao thức định tuyến.

Giao thức RIP hoạt động thế nào:

Routing Information Protocol (RIP) là một giao thức định tuyến vectơ khoảng cách được sử dụng trong mạng Giao thức Internet (IP), chủ yếu để định tuyến trong Hệ thống tự trị (AS). Chức năng chính của nó là xác định tuyến đường tốt nhất cho các gói dữ liệu di chuyển giữa các nút trong mạng. RIP sử dụng thuật toán Bellman-Ford và số bước nhảy làm thước đo để xác định tuyến đường tốt nhất. Đây là cách hoạt động của RIP:

1. *Khởi tạo*: Khi một bộ định tuyến khởi động hoặc RIP được bật, nó sẽ khởi tạo bảng định tuyến của nó với thông tin về các mạng được kết nối trực tiếp.
2. *Route Advertisement*: Mỗi bộ định tuyến hỗ trợ RIP định kỳ gửi toàn bộ bảng định tuyến của nó đến các hàng xóm của nó, thường là 30 giây một lần. Quảng cáo này chứa thông tin về các mạng mà bộ định tuyến biết và số bước nhảy liên quan của chúng.
3. *Route Learning*: Khi một bộ định tuyến nhận được một quảng cáo định tuyến từ một người lân cận, nó sẽ so sánh các tuyến được quảng cáo với bảng định tuyến của riêng nó. Nếu nó tìm thấy một tuyến đường mới hoặc một tuyến đường tốt hơn (với số bước nhảy thấp hơn) đến một mạng cụ thể, nó sẽ cập nhật bảng định tuyến của nó cho phù hợp.
4. *Split Horizon*: Để ngăn chặn các vòng lặp định tuyến, RIP sử dụng một kỹ thuật gọi là Split Horizon. Điều đó có nghĩa là một bộ định tuyến không quảng cáo một tuyến đường trở lại giao diện mà từ đó nó được học.
5. *Lão hóa tuyến đường và thời gian chờ*: RIP thực hiện lão hóa tuyến đường và thời gian chờ để xóa các tuyến cũ khỏi bảng định tuyến. Nếu một bộ định tuyến không nhận được bản cập nhật cho một tuyến đường cụ thể trong một thời gian nhất định (thường là 180 giây), nó sẽ đánh dấu tuyến đường đó là không hợp lệ. Sau một khoảng thời gian giữ bổ sung (thường là 120 giây), tuyến đường sẽ bị xóa khỏi bảng định tuyến.
6. *Cập nhật được kích hoạt*: Khi bộ định tuyến phát hiện ra sự thay đổi trong cấu trúc liên kết mạng (ví dụ: lỗi liên kết), nó sẽ ngay lập tức gửi bản cập nhật được kích hoạt đến các hàng xóm của nó, thông báo cho họ về sự thay đổi. Điều này giúp truyền bá thông tin cập nhật nhanh hơn trên toàn mạng.
7. *Số bước nhảy tối đa*: RIP có số bước nhảy tối đa là 15. Nếu một tuyến có số bước nhảy từ 16 trở lên, nó được coi là không thể truy cập được, ngăn các vòng lặp định tuyến kéo dài vô thời hạn.

Điều đáng chú ý là RIP có một số hạn chế, chẳng hạn như thời gian hội tụ chậm, sử dụng băng thông không hiệu quả và chỉ số số bước nhảy đơn giản không tính đến các yếu tố như tốc độ liên kết hoặc độ tin cậy. Do đó, các giao thức định tuyến tiên tiến hơn như OSPF và EIGRP đã thay thế phần lớn RIP trong các mạng hiện đại.

2.6.2. Giải thuật OSPF

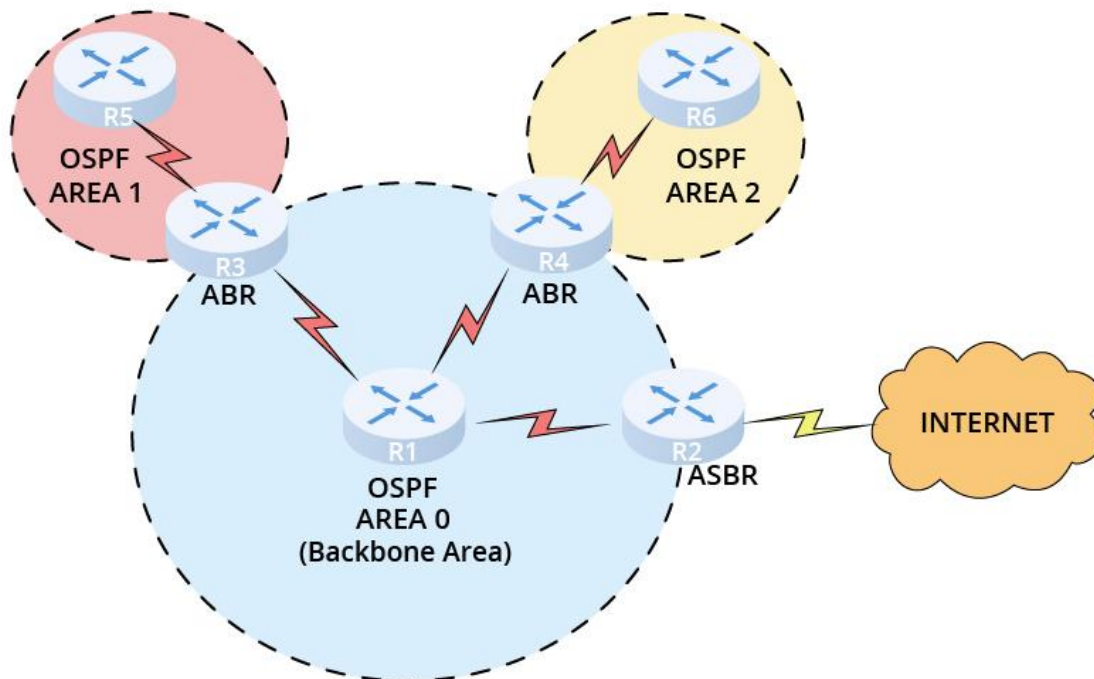
Khái niệm:

OSPF, viết tắt của *Open Shortest Path First*, là một giao thức định tuyến động thường được sử dụng trong các mạng IP quy mô lớn. Nó hoạt động bằng cách xác định đường dẫn ngắn nhất để định tuyến các gói dữ liệu giữa các bộ định tuyến. OSPF tính toán đường dẫn này dựa trên các chỉ số khác nhau như băng thông liên kết, độ trễ và chi phí.

Về cốt lõi, OSPF là một giao thức định tuyến được xây dựng cho các mạng Giao thức Internet (IP). Nó hoạt động trong một Hệ thống tự trị (AS) - một tập hợp các mạng IP và bộ định tuyến dưới sự kiểm soát của một thực thể trình bày một chính sách định tuyến chung đến Internet.

Cách hoạt động của OSPF:

OSPF (Open Shortest Path First) hoạt động dựa trên một quy trình được xác định rõ ràng liên quan đến việc phổ biến thông tin định tuyến trong mạng và tính toán các đường dẫn định tuyến tối ưu. Hoạt động của OSPF có thể được chia thành các giai đoạn riêng biệt, như chi tiết dưới đây:



Hình 8: Mô tả giao thức định tuyến OSPF

1. *LSAs (Link-State Advertisements)*: Bộ định tuyến chia sẻ thông tin về các kết nối trực tiếp của chúng trong các tin nhắn được gọi là LSA. Điều này bao gồm thông tin về những người hàng xóm được kết nối và chi phí tiếp cận họ.

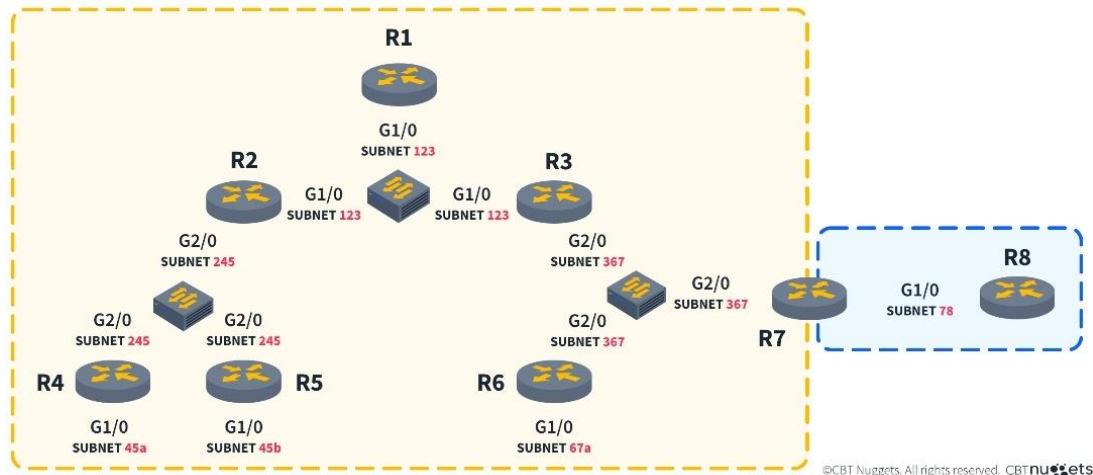
2. *Flooding of LSAs*: Mỗi bộ định tuyến OSPF gửi LSA của mình đến các bộ định tuyến khác trong cùng một khu vực. Sau đó, các bộ định tuyến cập nhật Cơ sở dữ liệu trạng thái liên kết (LSDB) của chúng với thông tin nhận được, đảm bảo tất cả các bộ định tuyến có chế độ xem nhất quán về cấu trúc liên kết mạng.
3. *Topology Map*: Sử dụng LSDB, mỗi bộ định tuyến xây dựng một bản đồ cấu trúc liên kết của mạng, cho thấy cách tất cả các bộ định tuyến và mạng được kết nối với nhau.
4. *Shortest Path Tree*: Mỗi bộ định tuyến áp dụng thuật toán của Dijkstra vào bản đồ cấu trúc liên kết của nó để tính toán đường dẫn ngắn nhất đến mọi nút khác trong mạng, tạo thành một cây đường dẫn ngắn nhất.
5. *Routing Table*: Kết quả của tính toán cây đường dẫn ngắn nhất được sử dụng để điền vào bảng định tuyến. Bảng này giúp bộ định tuyến chuyển tiếp các gói dữ liệu đến dọc theo các đường dẫn tốt nhất đến đích của chúng.
6. *OSPF Areas*: Để quản lý các mạng lớn, OSPF chia mạng thành các khu vực giúp giảm độ phức tạp của định tuyến. Khu vực đường trục (Khu vực 0) kết nối với các khu vực khác và giúp định tuyến giao thông giữa chúng.
7. *Router Types*: OSPF sử dụng các loại bộ định tuyến khác nhau như bộ định tuyến nội bộ (bên trong một khu vực), bộ định tuyến biên khu vực (ABR) (kết nối hai hoặc nhiều khu vực) và bộ định tuyến ranh giới hệ thống tự trị (ASBR) (kết nối với các miền hoặc mạng định tuyến khác nhau).
8. *Convergence*: OSPF phản ứng với những thay đổi của mạng bằng cách nhanh chóng truyền thông tin tuyến đường mới và tính toán lại đường dẫn, đảm bảo tất cả các bộ định tuyến biết về trạng thái hiện tại của mạng.
9. *Hello Protocol*: Bộ định tuyến OSPF định kỳ gửi các gói Hello đến các hàng xóm của chúng để thiết lập và duy trì các mối quan hệ lân cận. Quá trình này cũng giúp phát hiện lỗi mạng.

2.6.3. Giải thuật EIGRP

Khái niệm:

EIGRP được Cisco phát triển vào đầu những năm 90 như một bản nâng cấp cho Giao thức định tuyến công nội bộ (IGRP). IGRP là một giao thức định tuyến vector khoảng cách, một cải tiến trên Giao thức thông tin định tuyến (RIP) cũ hơn.

Một trong những điều làm cho EIGRP khác biệt là nó sử dụng kết hợp các giao thức định tuyến vector khoảng cách và trạng thái liên kết. Về mặt kỹ thuật, điều này làm cho EIGRP trở thành một giao thức vector khoảng cách nâng cao hoặc giao thức lai.



Hình 9: Mô tả cách hoạt động của giao thức EIGRP

Một số tính năng chính của EIGRP mang lại cho nó một số lợi thế so với các giao thức vectơ khoảng cách truyền thống:

- + EIGRP sử dụng thuật toán cập nhật khuếch tán (DUAL) để đạt được thời gian hội tụ nhanh. Thời gian hội tụ là tốc độ của một giao thức định tuyến có thể thích ứng với những thay đổi trong cấu trúc liên kết mạng và tìm đường dẫn tốt nhất cho các gói dữ liệu.

- + EIGRP tiết kiệm băng thông bằng cách chỉ gửi các bản cập nhật một phần, giúp giảm thiểu lượng dữ liệu mà nó phải gửi.

- + Nó hỗ trợ nhiều giao thức lớp mạng: EIGRP xử lý nhiều giao thức khác nhau và có thể định tuyến IP, IPX và AppleTalk.

- + Nó tương thích với IGRP: EIGRP tương thích ngược với IGRP. Tương thích với IPv4 và IPv6: EIGRP có hỗ trợ cho cả mạng IPv4 và IPv6.

Nguyên tắc hoạt động của EIGRP:

EIGRP có một số nguyên tắc cốt lõi cho phép nó hoạt động hiệu quả và có thể mở rộng với các tính năng hội tụ nhanh của nó. Một số nguyên tắc hoạt động này là:

- + *Protocol-dependent modules (PDMs)*: EIGRP sử dụng các PDM riêng biệt cho từng giao thức được định tuyến, cho phép nó hoạt động độc lập hơn và cho phép cấu hình tinh chỉnh hơn.

- + *Diffusing Update Algorithm (DUAL)*: EIGRP sử dụng DUAL để hội tụ nhanh chóng và cho phép nó hoạt động trong cấu trúc liên kết không có vòng lặp.

- + *Reliable Transport Protocol (RTP)*: RTP mang lại cho EIGRP độ tin cậy, cho phép nó phân phối các gói liên tục giữa các bộ định tuyến lân cận.

- + *Neighbor relationships*: EIGRP tạo mối quan hệ hàng xóm bằng cách sử dụng các gói hello để khám phá các bộ định tuyến lân cận.

2.7. Phần mềm mô phỏng mạng

Trong nghiên cứu này, phần mềm mô phỏng mạng được lựa chọn là Cisco Packet Tracer – một công cụ mạnh mẽ và phổ biến do Cisco Systems phát triển. Cisco Packet Tracer được thiết kế nhằm hỗ trợ việc học tập, thiết kế và kiểm tra các hệ thống mạng trong một môi trường ảo, phù hợp cho cả người mới bắt đầu lẫn các chuyên gia trong lĩnh vực công nghệ thông tin. Phần mềm này cung cấp một giao diện trực quan, cho phép người dùng kéo thả các thiết bị mạng như router, switch, PC, và các thiết bị đầu cuối khác để xây dựng mô hình mạng. Bên cạnh đó, nó hỗ trợ cấu hình chi tiết các thiết bị thông qua dòng lệnh hoặc giao diện đồ họa, đồng thời mô phỏng hoạt động của mạng như truyền dữ liệu, định tuyến gói tin và kiểm tra kết nối. Cisco Packet Tracer cũng tích hợp nhiều giao thức mạng phổ biến như TCP/IP, RIP, OSPF, DHCP, và VLAN, giúp người dùng có thể thử nghiệm các kịch bản mạng đa dạng. Với tính năng mô phỏng thời gian thực và khả năng hiển thị luồng dữ liệu trực quan, phần mềm này trở thành một công cụ lý tưởng để nghiên cứu và thực hành cấu hình mạng LAN/WAN cơ bản trong phạm vi đề tài.

Ưu điểm của việc sử dụng phần mềm mô phỏng cấu hình mạng:

Việc sử dụng phần mềm mô phỏng mạng như Cisco Packet Tracer mang lại nhiều ưu điểm vượt trội trong quá trình thiết kế và cấu hình mạng, đặc biệt khi so sánh với việc triển khai trực tiếp trên phần cứng thực tế:

Thứ nhất, phần mềm mô phỏng giúp tiết kiệm chi phí đáng kể. Thay vì phải đầu tư vào các thiết bị mạng đắt tiền như router, switch hay cáp kết nối, người dùng có thể thực hiện mọi thao tác trong môi trường ảo mà không cần đến cơ sở hạ tầng vật lý. Điều này đặc biệt hữu ích trong môi trường học tập hoặc các dự án thử nghiệm quy mô nhỏ.

Thứ hai, phần mềm mô phỏng mang lại sự linh hoạt và an toàn. Người dùng có thể dễ dàng thay đổi cấu hình, thử nghiệm các kịch bản khác nhau hoặc thậm chí mô phỏng các sự cố mạng (như đứt cáp hoặc lỗi định tuyến) mà không lo ảnh hưởng đến hệ thống thực tế. Nếu có sai sót trong quá trình cấu hình, việc khôi phục chỉ đơn giản là khởi động lại mô phỏng, thay vì phải xử lý các vấn đề phức tạp trên phần cứng.

Thứ ba, Cisco Packet Tracer hỗ trợ học tập và thực hành hiệu quả nhờ tính trực quan và khả năng mô phỏng chi tiết. Người dùng có thể quan sát cách các gói

tin di chuyển qua mạng, kiểm tra trạng thái kết nối bằng các lệnh như ping hoặc traceroute, và phân tích hiệu suất mạng trong thời gian thực. Điều này không chỉ giúp củng cố kiến thức lý thuyết mà còn rèn luyện kỹ năng thực tiễn, từ đó nâng cao khả năng thiết kế và quản lý mạng.

Cuối cùng, phần mềm mô phỏng cho phép thử nghiệm các ý tưởng sáng tạo mà không bị giới hạn bởi nguồn lực vật lý. Người dùng có thể xây dựng các mô hình mạng phức tạp, mở rộng quy mô hoặc tích hợp nhiều công nghệ khác nhau để đánh giá hiệu quả trước khi áp dụng vào thực tế. Nhờ những ưu điểm này, Cisco Packet Tracer không chỉ là công cụ hỗ trợ đắc lực trong nghiên cứu này mà còn là một giải pháp phổ biến trong giáo dục và phát triển kỹ năng mạng trên toàn cầu.

Nhược điểm của Cisco Packet Tracer

Bên cạnh những ưu điểm nổi bật, Cisco Packet Tracer cũng tồn tại một số nhược điểm cần được lưu ý:

Thứ nhất, phần mềm này bị giới hạn về tính năng so với các thiết bị mạng thực tế hoặc các công cụ mô phỏng cao cấp hơn như GNS3. Cisco Packet Tracer chủ yếu tập trung vào các giao thức và thiết bị cơ bản, do đó không hỗ trợ đầy đủ các tính năng nâng cao hoặc các thiết bị phần cứng mới nhất của Cisco, cũng như các sản phẩm từ các nhà cung cấp khác. Điều này khiến nó kém phù hợp khi mô phỏng các hệ thống mạng phức tạp hoặc doanh nghiệp quy mô lớn.

Thứ hai, tính chân thực của Cisco Packet Tracer không hoàn toàn tương đồng với thực tế. Vì là một công cụ mô phỏng được đơn giản hóa để phục vụ mục đích học tập, nó không thể tái hiện chính xác các vấn đề phần cứng như độ trễ vật lý, hiệu suất thực tế của thiết bị hay các lỗi phát sinh từ môi trường thực. Điều này có thể dẫn đến sự khác biệt giữa kết quả mô phỏng và triển khai thực tế.

Thứ ba, phần mềm này thiếu khả năng tích hợp với các hệ thống thực. Không giống như một số công cụ khác cho phép kết nối với phần cứng thật hoặc các mạng vật lý, Cisco Packet Tracer chỉ hoạt động trong môi trường ảo khép kín, hạn chế khả năng thử nghiệm trong các tình huống kết hợp giữa mô phỏng và thực tế.

Cuối cùng, việc phụ thuộc quá nhiều vào Cisco Packet Tracer có thể khiến người học hoặc người dùng thiếu kinh nghiệm thực tế với phần cứng vật lý, vốn là một kỹ năng quan trọng trong công việc thực tiễn. Dù vậy, với mục tiêu nghiên cứu

cơ bản và học tập, những nhược điểm này không làm giảm giá trị của phần mềm trong phạm vi đề tài.

3. Thực hiện mô phỏng trên phần mềm

3.1. Chuẩn bị và cài đặt môi trường mô phỏng

Việc chuẩn bị môi trường mô phỏng mạng là một bước quan trọng để thực hành và nghiên cứu các khái niệm mạng một cách hiệu quả. Quá trình này bao gồm hai giai đoạn chính: cài đặt phần mềm mô phỏng mạng và lựa chọn thiết bị cùng công cụ trong phần mềm:

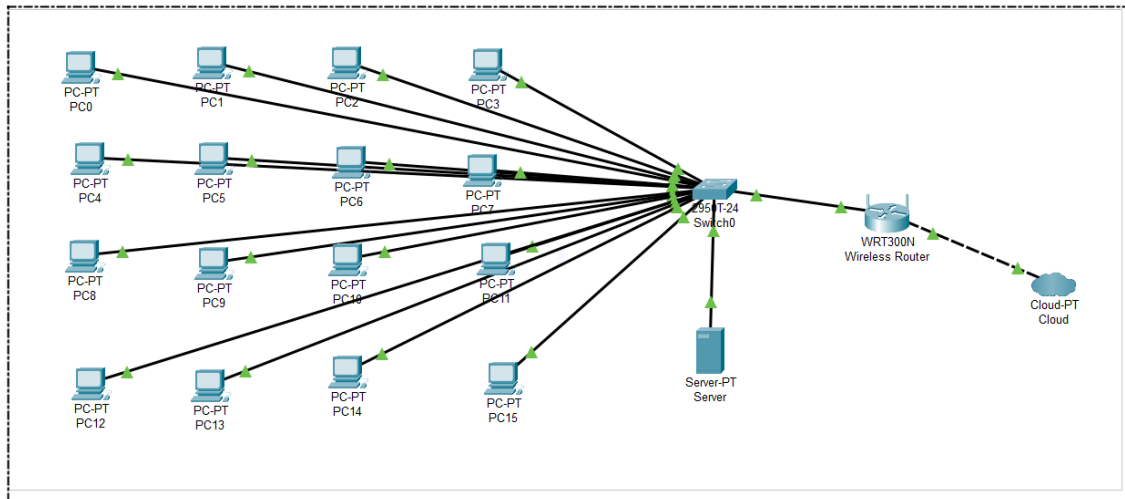
Trước tiên, việc cài đặt phần mềm đòi hỏi người dùng phải chọn một công cụ phù hợp với nhu cầu và cấu hình máy tính. Cisco Packet Tracer là lựa chọn phổ biến cho người mới bắt đầu nhờ tính miễn phí và dễ sử dụng, hỗ trợ mô phỏng mạng cơ bản. Để cài đặt, người dùng chỉ cần truy cập trang chính thức của Cisco, tải phiên bản mới nhất như 8.x, và làm theo hướng dẫn cài đặt trên các hệ điều hành như Windows, macOS hoặc Linux. Trong khi đó, GNS3 lại phù hợp với mô phỏng mạng phức tạp hơn, yêu cầu tích hợp file IOS của thiết bị thực tế như router Cisco và một máy tính có cấu hình tối thiểu 8GB RAM. Người dùng có thể tải GNS3 từ trang chủ gns3.com, cài đặt cùng GNS3 VM để tối ưu hóa tài nguyên. Đối với những ai cần môi trường chuyên sâu và đa dạng thiết bị từ nhiều hãng như Cisco hay Juniper, EVE-NG là lựa chọn tối ưu. Phần mềm này được cài đặt dưới dạng máy ảo trên VMware hoặc VirtualBox, sau đó truy cập qua giao diện web để cấu hình.

Sau khi cài đặt phần mềm, bước tiếp theo là lựa chọn thiết bị và công cụ trong phần mềm để xây dựng mô hình mạng. Với Cisco Packet Tracer, người dùng có thể kéo thả các thiết bị như router (1941, 2911), switch (2950, 2960), hoặc máy tính từ thanh công cụ, sau đó sử dụng tính năng kết nối tự động để nối chúng bằng cáp phù hợp như Ethernet hay Serial. GNS3, ngược lại, yêu cầu cấu hình thủ công hơn: sau khi thêm IOS image vào phần mềm, người dùng kéo thiết bị vào khu vực làm việc và kết nối các cổng như FastEthernet0/0 bằng công cụ cáp ảo. Tương tự, trong EVE-NG, người dùng tải image thiết bị vào hệ thống, thêm chúng vào topology qua giao diện web, và nối các cổng bằng thao tác chuột phải. Mỗi phần mềm có ưu điểm riêng: Packet Tracer đơn giản và nhẹ, phù hợp cho mạng LAN cơ bản; GNS3 và EVE-NG sát thực tế hơn nhờ chạy hệ điều hành thật, lý tưởng cho mạng phức tạp hoặc đa hãng. Việc lựa chọn phụ thuộc vào mục tiêu mô phỏng và tài nguyên máy tính, nhưng dù sử dụng công cụ nào, quá trình này đều giúp người dùng thiết kế topology, cấu hình địa chỉ IP, và kiểm tra hoạt động mạng một cách hiệu quả trong môi trường ảo hóa.

3.2. Thiết kế mô hình mạng

3.2.1. Xây dựng topology mạng LAN đơn giản

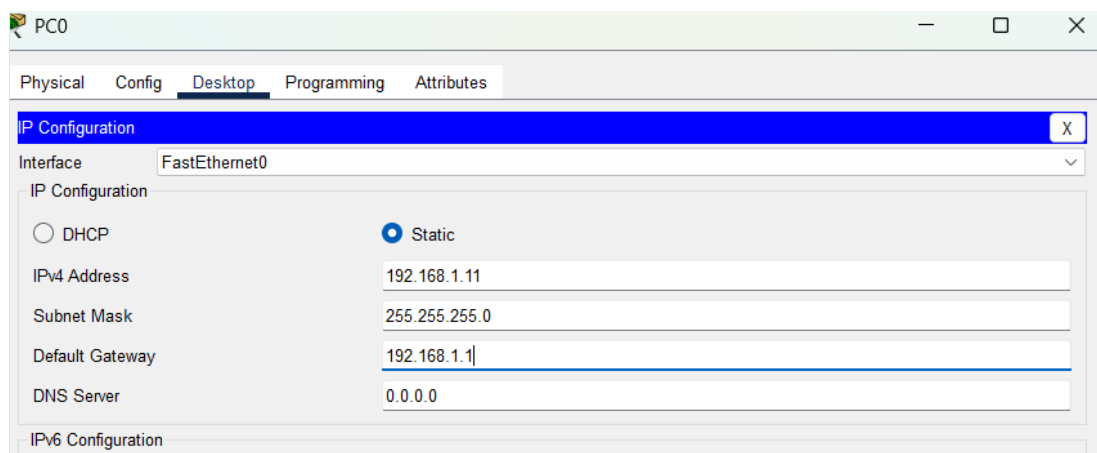
Mô hình mạng LAN được sử dụng để mô phỏng là mô hình sao (Stars). Về mạng hình sao, nó sử dụng gồm có 16 PC, 1 hub, 1 sever và 1 router.



Hình 10:Mô phỏng mạng LAN mô hình sao (Stars) trên CPT

Nguyên lí hoạt động, trong giao tiếp nội bộ các máy tính (PC0 → PC15 và sever) đều kết nối trực tiếp với Switch0 thông qua dây mạng. Switch hoạt động như một thiết bị trung tâm, dùng để gửi dữ liệu đến đúng thiết bị đích, dựa trên địa chỉ *MAC*. Đối với giao tiếp ra bên ngoài, Switch0 kết nối đến Router, nó đóng vai trò phân phối mạng và kết nối với Internet (đại diện ở đây là Cloud-PT). Ở máy chủ nội bộ có thể cung cấp các dịch vụ web, lưu trữ...

Chúng ta cấu hình địa chỉ IP tĩnh cho máy PC0-15 tương ứng với địa chỉ 11-26. Để phân phát IP tự động ta chỉnh toàn bộ máy PC0-15 sang DHCP.

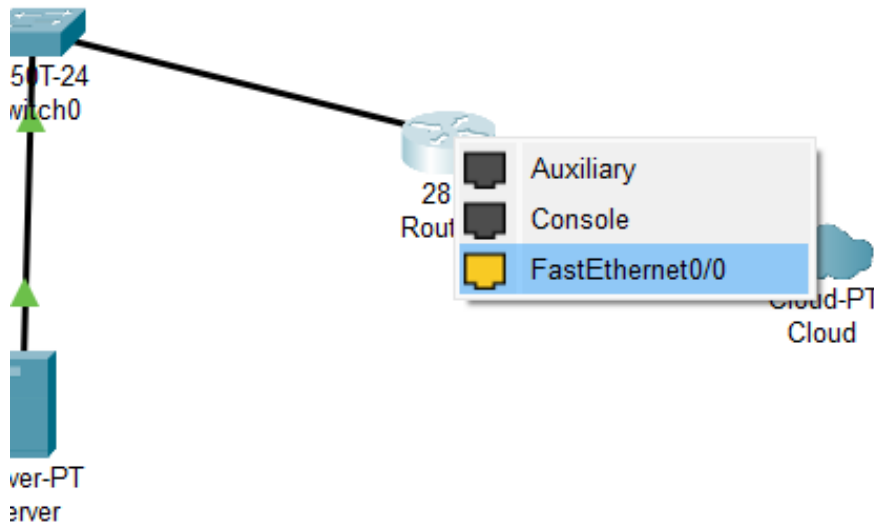


Hình 11: Cấu hình địa chỉ static

Cấu hình DHCP server trên router

Chuyển sang chế độ *CLI* của Router nhập lệnh “enable”, nhập “configure terminal” để vào (config).

Dùng lệnh “interface fastEthernet 0/0” để vào (config if), đặt IP cho cổng này là “ip address 192.168.10.1 255.255.255.0” do ta đã kết nối switch sang router là cổng fastEthernet 0/0, dùng lệnh “no shutdown” để bật cổng FastEthernet0/0, dùng lệnh Exit để thoát (config if)



Hình 12: Kết nối cổng FastEthernet 0/0

Để bật được dịch vụ DHCP của router, ta sử dụng lệnh “service DHCP” và đặt tên cho DHCP qua lệnh “IP dhcp pool MANGLAN”. Lúc này ta đã vào (DHCP-config), sử dụng tiếp lệnh “network 192.168.10.0 255.255.255.0” để có địa chỉ mạng bắt đầu phân phát. Sử dụng “default-router 192.168.10.1” Địa chỉ IP của router được cấp phát làm default gateway.

Sử dụng “ip dhcp excluded-address 192.168.10.1 192.168.10.10” để địa chỉ IP từ 1 đến 10 sẽ không được phân phát qua DHCP điều này ứng dụng cho các thiết bị tĩnh như Router.


```

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inter fastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#Exit
Router(config)#service DHCP
Router(config)#IP dhcp pool MANGLAN
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
Router(config)#

```

Hình 13:Cấu hình DHCP

Kiểm tra có cấu hình thành công chưa, ta có thể chọn PC bất kì để xem địa chỉ IP hoặc xem toàn bộ thiết bị kết nối với mạng LAN qua câu lệnh “show ip dhcp binding”

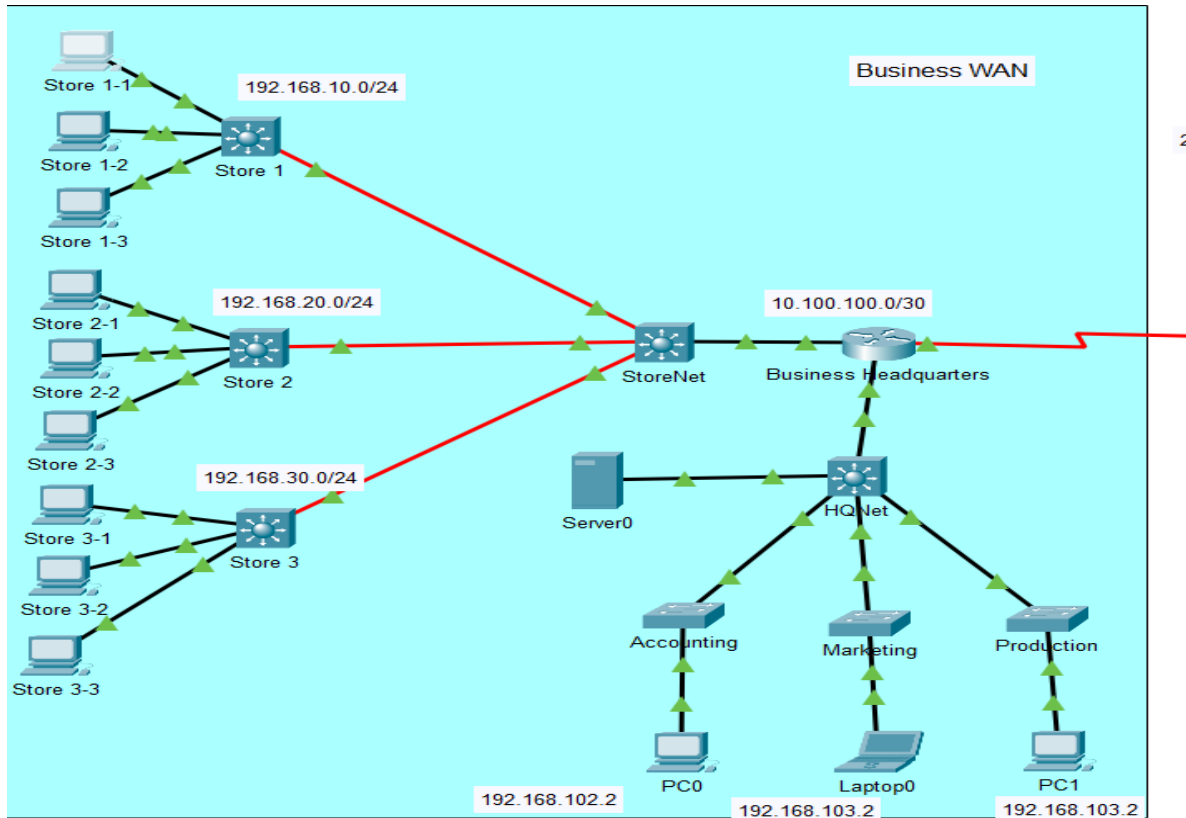
```

Router#show ip dhcp binding
IP address      Client-ID/
                Hardware address
192.168.10.13    0009.7C33.1563    --    Automatic
192.168.10.15    0002.161D.4B77    --    Automatic
192.168.10.16    0009.7C67.B22E    --    Automatic
192.168.10.11    0002.4A3A.657D    --    Automatic
192.168.10.14    00E0.8F39.A7E7    --    Automatic
192.168.10.12    00D0.58A7.232A    --    Automatic
192.168.10.21    00E0.A37B.3EB4    --    Automatic
192.168.10.17    00E0.A313.4CD3    --    Automatic
192.168.10.19    0090.2B9C.C692    --    Automatic
192.168.10.22    000C.CF05.49C3    --    Automatic
192.168.10.25    000D.BD81.03E2    --    Automatic
192.168.10.24    0002.16B6.AC59    --    Automatic
192.168.10.20    0002.4AA0.14A0    --    Automatic
192.168.10.26    00D0.FF8E.24A4    --    Automatic
192.168.10.27    000A.41EA.44DB    --    Automatic
192.168.10.18    000C.8594.C5B2    --    Automatic
192.168.10.23    0030.A3E9.B9B1    --    Automatic
Router#

```

Hình 14: Kết quả hiển thị các địa chỉ IP đã kết nối

Cấu hình mật khẩu cho router mạng Wired LAN



Hình 15: Mô phỏng hệ thống mạng LAN doanh nghiệp

Để cấu hình password cho hệ thống quản lý, ta sẽ cấu hình mật khẩu trên Router Headquarter nhằm quản lý quyền truy cập của các users. Bên cạnh đó ta cũng có thể cấu hình mật khẩu đa level lên các switch nhằm tăng mức độ bảo mật, tuy nhiên điều này sẽ gây khó khăn và phiền phức trong trường hợp ta chỉ quan tâm đến mô phỏng cấu hình mật khẩu đơn giản và tập trung vào các mục tiêu khác như build hoặc giải thuật định tuyến...

Đầu tiên ta sẽ truy cập vào CLI của Router, sau đó sẽ tiến hành cấu hình như sau:

```

BussinessRouter>BussinessRouter>en
Password:
BussinessRouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BussinessRouter(config)#enable password 123
BussinessRouter(config)#enable secret 123
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.
BussinessRouter(config)#
BussinessRouter(config)#enable secret 1234
BussinessRouter(config)#username admin
BussinessRouter(config)#username admin secret 123
BussinessRouter(config)#line vt 0 4
BussinessRouter(config-line)#login local
BussinessRouter(config-line)#exit
BussinessRouter(config)#exit
BussinessRouter#
%SYS-5-CONFIG_I: Configured from console by console
BussinessRouter#

```

Hình 16: Cấu hình Telnet line

Trong đó:

- Lệnh *enable password 123* là thiết lập mật khẩu truy cập vào địa chỉ quản lý router.
- Lệnh *enable secret 1234* là thiết lập mật khẩu bí mật để truy cập quyền chỉnh sửa thông tin trên hệ thống router. Với mật khẩu bí mật này, ta có thể dễ quản lý quyền truy cập và chỉ có thể truy cập bởi người quản trị nắm giữ mật khẩu này.
- Với *username* là *admin*, đó cũng là tài khoản mà ta sẽ có thể truy cập vào router mạng này.

Để kiểm tra lại mật khẩu đã được cấu hình thành công hay chưa, ta sẽ truy cập vào một PC bất kỳ trong mạng local, sau đó truy cập Command Prompt và thực hiện:

```

C:\>telnet 10.100.100.1
Trying 10.100.100.1 ...Open

User Access Verification

Username: admin
Password:
BussinessRouter>en

```

Hình 17: Kết quả kiểm tra trên cmd

Lệnh *telnet 10.100.100.100.1* là lệnh thực hiện telnet line, là một phương pháp kết nối liên lạc các thiết bị trong mạng local. Địa chỉ IP được nhấn đến là địa chỉ IP của router mà ta định là administrator.

Password truy cập vào tài khoản *admin* là *123* như đã cài đặt.

```
BussinessRouter>en
```

```
Password:
```

Theo như ta thấy, để có thể truy cập quyền chỉnh sửa cũng như xem được thông tin connect trên Router, ta sẽ phải nhập mật khẩu *secret* là *1234*

```
BussinessRouter#show run
Building configuration...

Current configuration : 1056 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BussinessRouter
!
!
!
enable secret 5 $l$mERr$4dpRATlgxQacPVK0CfNV4/
enable password 123
!
!
!
!
!
!
no ip cef
--More--
```

Hình 18:Hiển thị password

Sau khi đã truy cập được vào Router, ta có thể dùng lệnh *show run* hoặc *show running-config* để xem được thông tin của admin's user account.

3.2.2. Mở rộng sang mạng WAN

Cấu hình địa chỉ IP cho mạng LAN1 và LAN2

Sau khi connect các thiết bị với nhau, ta tiến hành cấu hình thiết bị Router:

Mở CLI, sau đó cấu hình theo các code line lần lượt như hình:

```

R0>en
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#hostname R0
R0(config)#int f 0/0
R0(config-if)#ip add 172.16.10.1 255.255.255.0

```

Hình 19: Định địa chỉ IP cho Router R0

Trong đó:

- Lệnh `int f 0/0` là truy cập quyền vào kết nối FastEthernet 0/0.
- Địa chỉ IP là địa chỉ IP định sẵn cho kết nối mạng LAN thông qua SWITCH với segment cuối khác 0 và 255, SUBNET MASK mặc định là 255.255.255.0 vì không phân vùng subnet.

Sau đó nhấn thêm lệnh: *R0 (config-if) #no shut* để ping vào mạng, nếu trên đường bus hiện mũi tên màu xanh là kết nối thành công.

Làm tương tự với mạng LAN2 với địa chỉ IP tự định sẵn với segment cuối khác 0 và 255, subnet mask tương tự.

Cấu hình địa chỉ IP cho các Router

Để các Router được kết nối với nhau, ta kết nối dây thông qua các cổng Serial Port. Tương tự để cấu hình các thiết bị Router, ta mở CLI

```

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int s 3/0
R1(config-if)#exit
R1(config)#int s 2/0
R1(config-if)#ip add 192.168.10.2 255.255.255.0
R1(config-if)#no shut

```

Hình 20: Định địa chỉ IP cho router R1

Trong đó:

- Lệnh `int s 3/0` là truy cập quyền vào kết nối Serial với Router khác thứ tự là 3/0
- Địa chỉ IP được định vào địa chỉ của Serial Port mà ta đã get into.

```

R1(config-if)#clock rate 56000
R1(config-if)#exit

```

Hình 21: Cấu hình Clock rate để đồng bộ xung với 56000 Hz

Làm tương tự với các Router còn lại trong mạng WAN với cổng Serial Port đã thiết lập (phải trùng với địa chỉ IP Network Address của bus kết nối, chỉ thay đổi Host Address sao cho khác 0 và 255).

Để xem được các giao tiếp đã thiết lập đã kết nối chưa, ta có thể dùng câu lệnh:

R1# show ip interface brief

```

R1#
%SYS-5-CONFIG_I: Configured from console by console
show ip int brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	172.16.10.254	YES	manual	up	up
FastEthernet1/0	unassigned	YES	unset	administratively down	down
Serial2/0	192.168.10.1	YES	manual	down	down
Serial3/0	unassigned	YES	unset	administratively down	down
FastEthernet4/0	unassigned	YES	unset	administratively down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down
Modem6/0	unassigned	YES	unset	administratively down	down
Modem7/0	unassigned	YES	unset	administratively down	down
Modem8/0	unassigned	YES	unset	administratively down	down
Modem9/0	unassigned	YES	unset	administratively down	down

```

R1#exit

```

Hình 22: Các địa chỉ IP được hiển thị đối với từng kết nối

Kết quả như hình trên cho thấy ta đã thiết lập các địa chỉ IP cho các giao tiếp FastEthernet 0/0 (172.16.10.254) và Serial 2/0 (192.168.10.1).

Sau đó, để kiểm tra các kết nối đã thành công chưa, ta có thể test bằng cách ping data đến địa chỉ IP cần kiểm tra:

```

R0(config-if)#exit
R0(config)#exit
R0#
%SYS-5-CONFIG_I: Configured from console by console
R0#ping 172.16.10.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.254, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/8 ms

R0#ping 200.200.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R0#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/7/13 ms

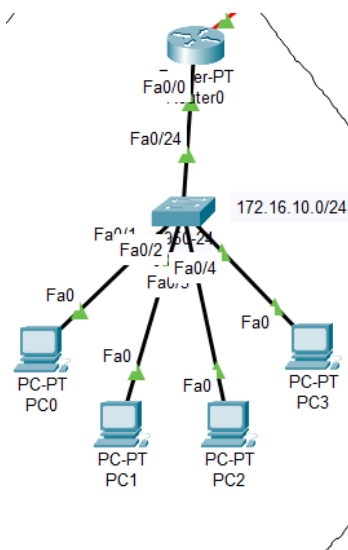
```

Hình 23: Mô phỏng ping data đến địa chỉ IP đã kết nối

Như hình trên, ta thấy địa chỉ IP được ping tới là 172.16.10.254 được thể hiện là *Success rate is 100 percent*, nghĩa là đã kết nối thành công được đến địa chỉ IP đó.

Ngược lại, với địa chỉ IP 200.200.200.1, ta nhận được kết quả *Success rate is 0 percent*, nghĩa là ta chưa thiết lập thành công được kết nối từ thiết bị đang sử dụng gửi đến địa chỉ IP đó.

Cấu hình địa chỉ IP static cho các End-devices



Hình 24: Các kết nối của thiết bị đầu cuối trong mô phỏng

Đối với từng mạng LAN, ta cấu hình địa chỉ IP cho từng thiết bị đầu cuối kết nối vào mạng (PC-Laptop).

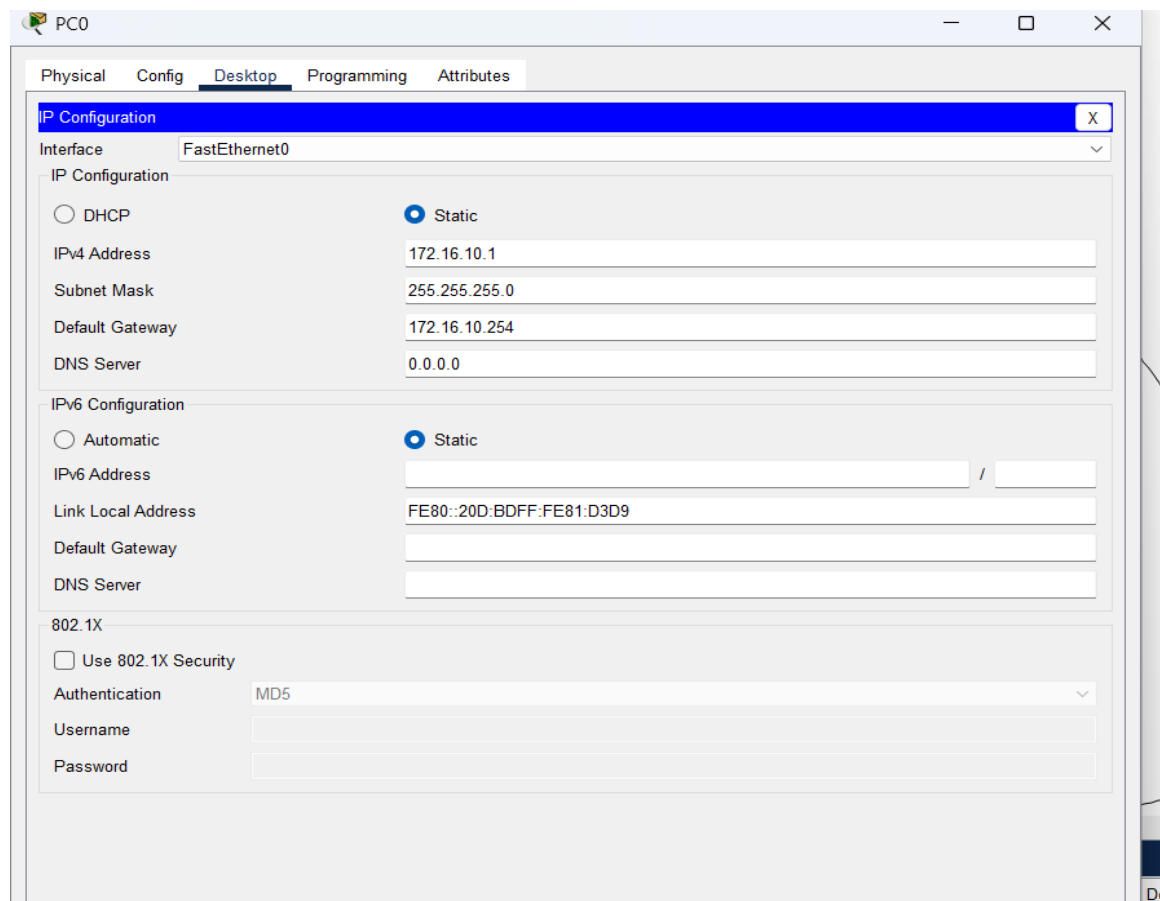
Ta truy cập vào *Desktop PC -> IP configuration*.

Địa chỉ IPv4 là địa chỉ có Network Address là 2 bytes đầu giống với trên địa chỉ của giao tiếp FastEthernet 0/0, byte thứ giống với Host Address, byte cuối cùng là số thứ tự định cho device (Các device có số thứ tự khác nhau, khác 0 và 254).

Subnet Mask được thiết lập theo default class C (256 blocks)







Default Gateway là địa chỉ IP mà PC được kết nối mạng vào, ở đây ta sử dụng địa chỉ IP trên giao tiếp FastEthernet 0/0 của Router0

Sau đó làm tương tự đối với các End-devices còn lại.



Hình 25: Kết quả hiển thị trên Config

Sau khi thiết lập địa chỉ IPv4 cho các devices, ta có thể kiểm tra lại đường truyền bằng cách test gửi thư qua kết nối.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC8	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC0	Router1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	Router0	ICMP		0.000	N	2	(edit)	(delete)

Hình 26: Test gửi sms

Như trên hình ta có thể thấy, đối với địa chỉ mà ta đã liên kết đúng hoặc đã thiết lập đúng thì sẽ có Status là *Successful*. Ngược lại nếu ta thiết lập sai hoặc đường truyền lỗi, ta sẽ thấy thông báo là *Failed*.

Hoặc ta có thể kiểm tra nhanh bằng ping IP destination trên CLI hoặc Commant Promt của PC.

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

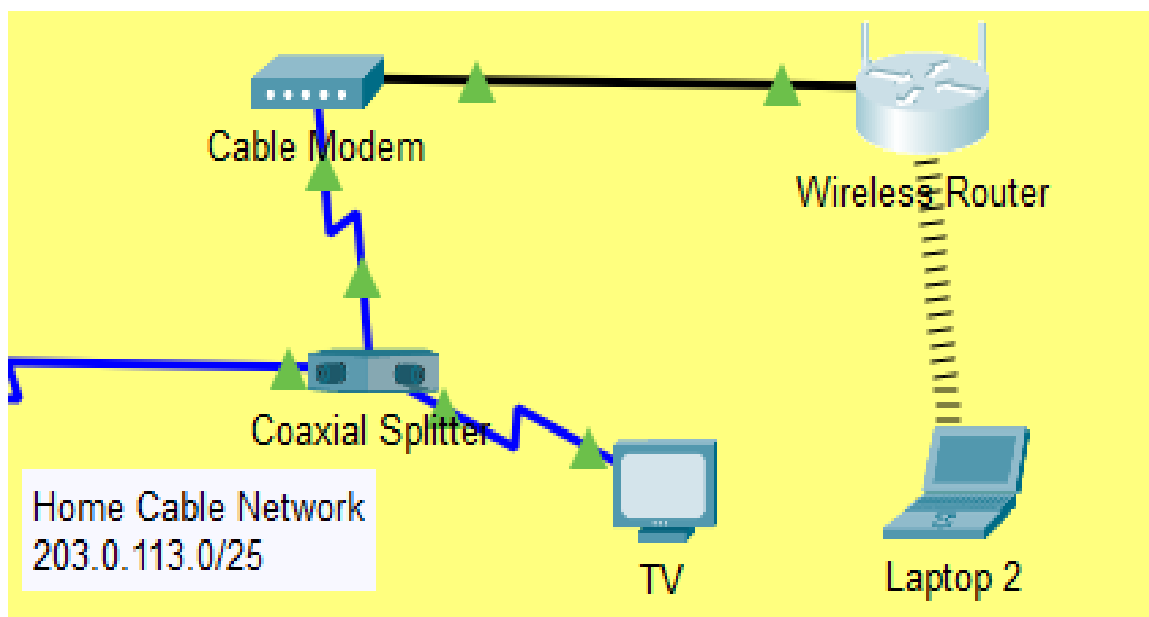
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 200.200.200.1
```

Hình 27: Kiểm tra kết nối trên cmd

Khi ta thấy báo *Lost = 0* nghĩa là đã kết nối và truyền dữ liệu thành công, nếu *Lost=4* thì nghĩa là kết nối đã gặp lỗi.

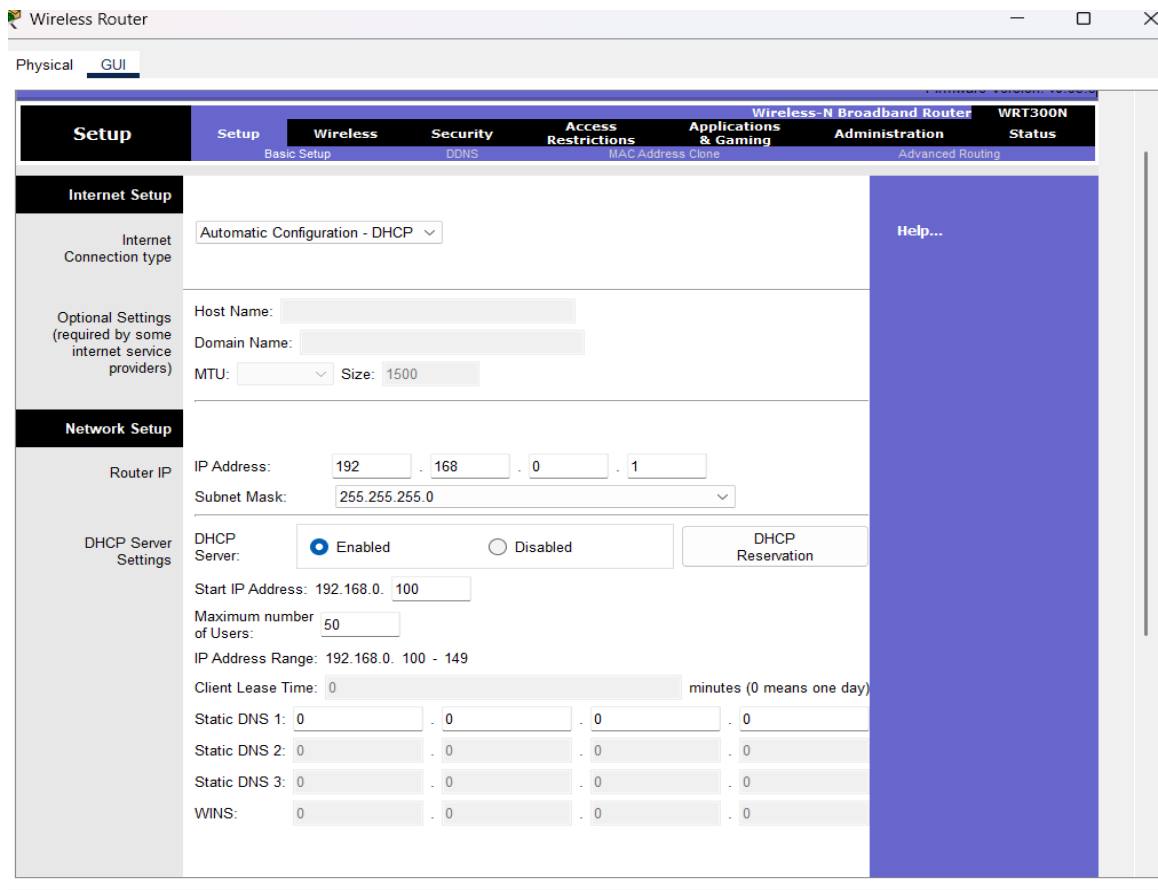
Cấu hình mật khẩu cho router mạng không dây (WLAN)



Hình 28: Mô phỏng mạng home WLAN

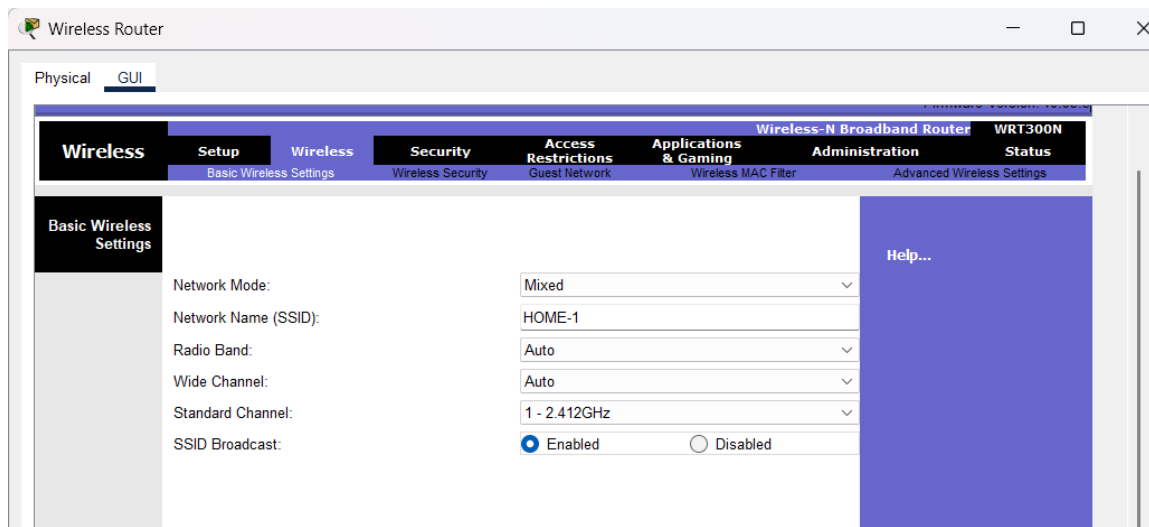
Trong thực tế, ta rất cần cấu hình mật khẩu truy cập cho các mạng WLAN (thông dụng trong thương mại là Wifi) nhằm giới hạn lượng người dùng và tăng tính bảo mật cho người dùng đã truy cập. Vì thế ta cũng sẽ mô phỏng cách cấu hình mật khẩu cho router mạng WLAN.

Đầu tiên truy cập vào Wireless Router -> GUI -> thiết lập các thông tin cơ bản như địa chỉ Internet Connection type (Ở đây ta cấu hình theo định dạng DHCP), Hostname, Domain, IP address và DHCP server.



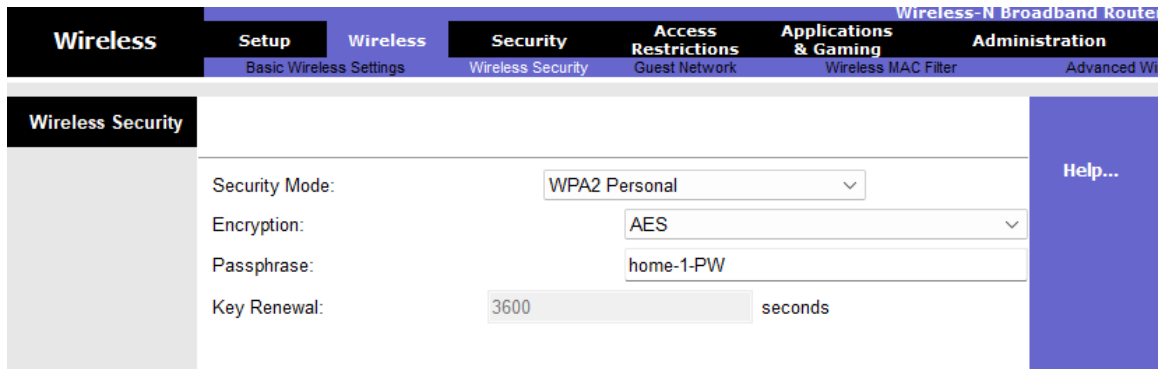
Hình 29: Các cài đặt trên Router GUI

Chuyển qua mục Wireless, ta sẽ cấu hình các mục như Network mode, SSID và Channel, Radio Band. Như hình dưới đây thì ta cấu hình chuẩn kênh có băng tần thông thường là 2.4Ghz



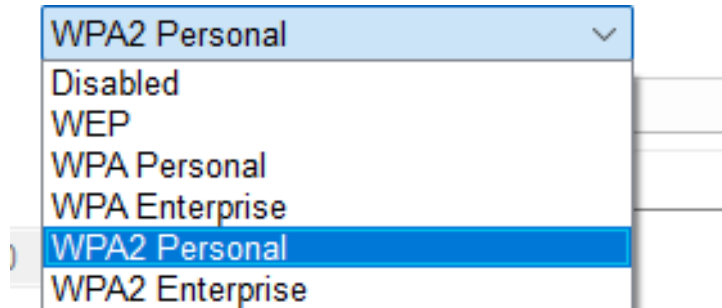
Hình 30: Cấu hình phát sóng mạng

Sau đó chuyển qua Title có tên là Wireless Security, ta sẽ thấy có các mục mà ta cần thiết lập như Security Mode, Phương pháp mã hóa (Encryption), Passphrase và thời gian làm mới quyền truy cập (Key renewal).



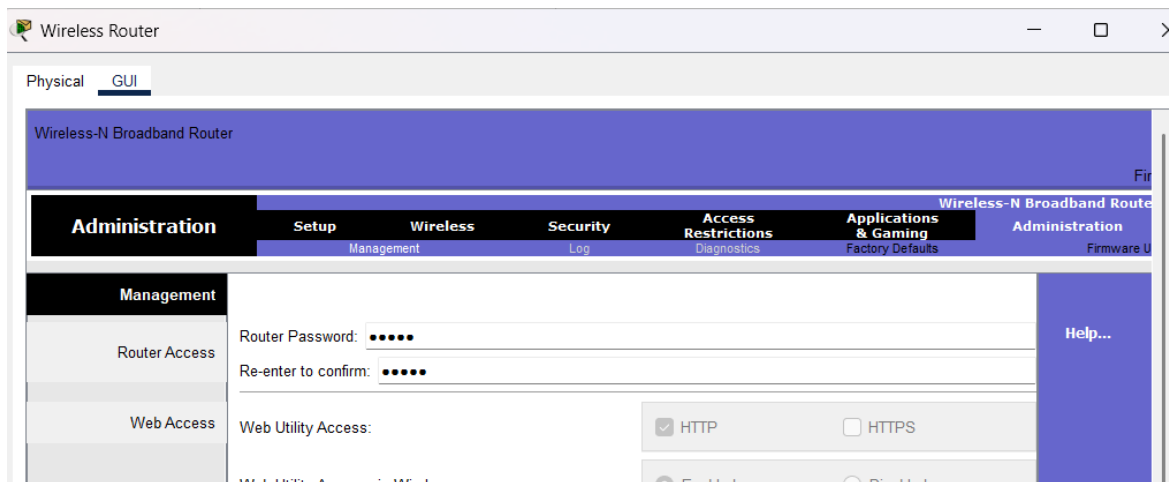
Hình 31: Cấu hình Wireless Security

Tùy vào các router mà ta cài đặt cũng như là server định tuyến mà ta có thể lựa chọn các level cho password. Có nhiều chuẩn cho ta lựa chọn như WEP, WPA, WPA2,... Mỗi tiêu chuẩn có cách mã hóa (Encryption) riêng biệt và sẽ có độ phức tạp khác nhau, điều này nhằm tăng cường bảo vệ quyền truy cập tài khoản kết nối cũng như an toàn thông tin cho user, hạn chế bị hack thông tin truy cập.



Hình 32: Các tiêu chuẩn mã hóa mật khẩu

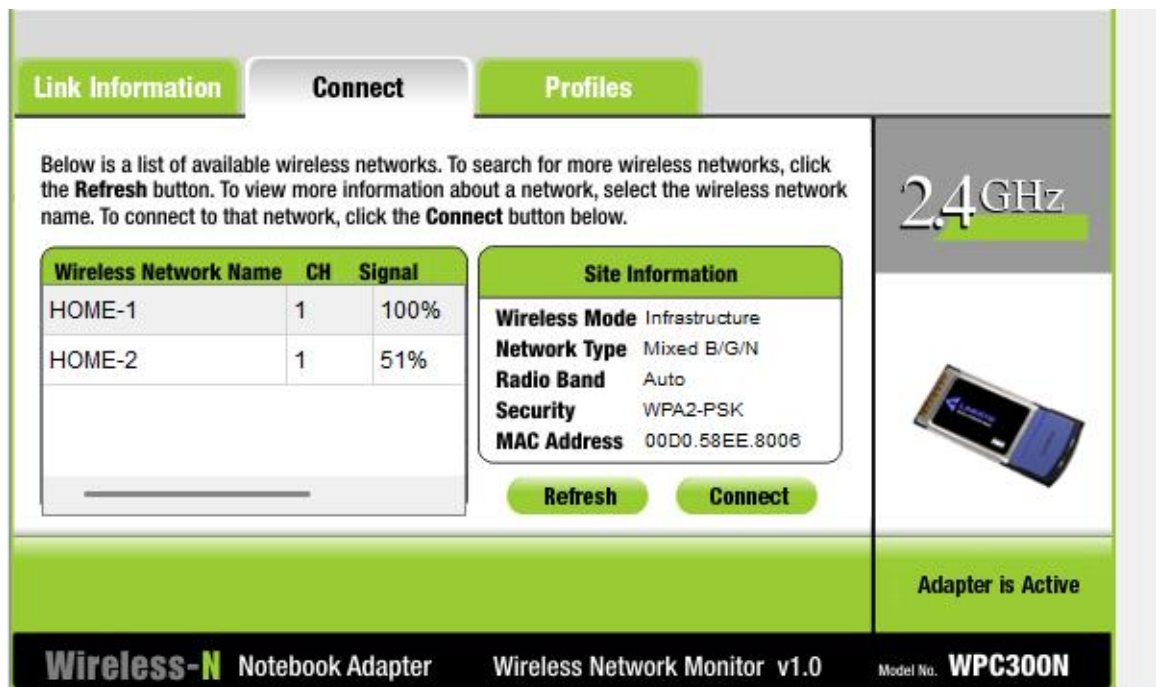
Để thiết lập mật khẩu quản trị viên cho router, ta sẽ chuyển qua mục Administration, sau đó sẽ nhập mật khẩu cần cấu hình vào 2 mục như hình bên dưới. Ở đây ta cấu hình mật khẩu đơn giản là 12345.



Hình 33: Cài đặt mật khẩu admin

Để kiểm tra lại mật khẩu đã cấu hình thành công chưa, ta có thể sử dụng End-devices bất kỳ như PC, Laptop hay Tablet.

Truy cập vào *Desktop -> PC Wireless*. Khi đã tìm thấy tên mạng không dây đã cài đặt -> chọn mạng ta đã thiết lập -> nhập mật khẩu 12345 và kết nối.



Hình 34: Hiện thị các mạng đang phát sóng

3.3. Kết quả mô phỏng cấu hình thiết bị mạng

3.3.1. Cấu hình cho các thiết bị trong mạng LAN.

Kết quả mô phỏng

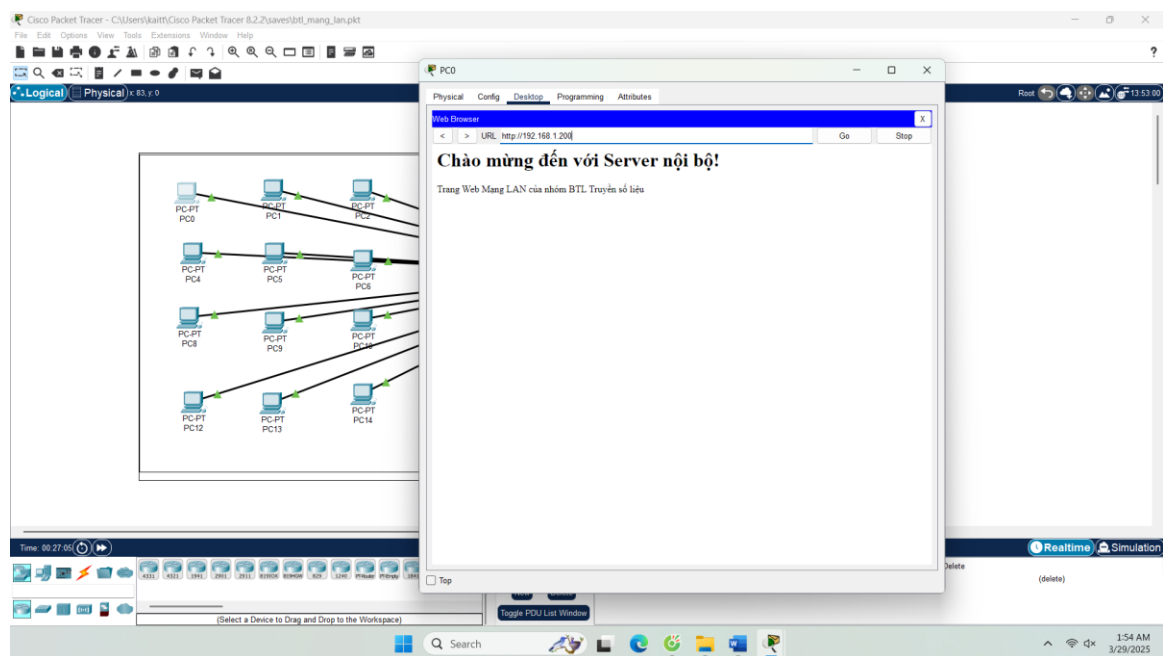
Khi đã cấu hình IP hết ở các thiết bị ta mô phỏng Ping giữa 2 máy, mục đích là để 2 máy có liên lạc với nhau hay không.

Từ máy PC0 sang PC1 và các trường hợp còn lại.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	--	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC3	PC4	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC4	PC5	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC5	PC6	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC6	PC7	ICMP		0.000	N	7	(edit)	(delete)
	Successful	PC7	PC8	ICMP		0.000	N	8	(edit)	(delete)
	Successful	PC8	PC9	ICMP		0.000	N	9	(edit)	(delete)
	Successful	PC9	PC10	ICMP		0.000	N	10	(edit)	(delete)
	Successful	PC10	PC11	ICMP		0.000	N	11	(edit)	(delete)
	Successful	PC11	PC12	ICMP		0.000	N	12	(edit)	(delete)
	Successful	PC12	PC13	ICMP		0.000	N	13	(edit)	(delete)
	Successful	PC13	PC14	ICMP		0.000	N	14	(edit)	(delete)
	Successful	PC14	PC15	ICMP		0.000	N	15	(edit)	(delete)
	Successful	PC15	Server	ICMP		0.000	N	16	(edit)	(delete)
	Successful	Server	PC15	ICMP		0.000	N	17	(edit)	(delete)

Hình 35: Thử nghiệm kiểm tra lại các kết nối

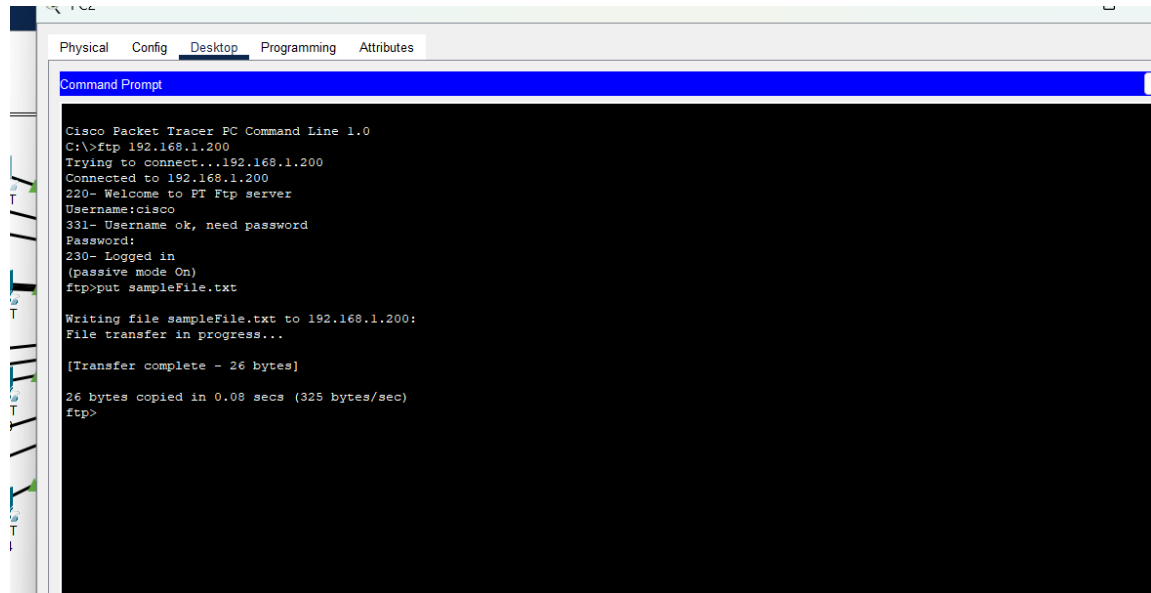
Để mô phỏng khi truy cập dịch vụ web của server ta cần mở dịch vụ HTTP và kết quả mô phỏng.



Hình 36: Mô phỏng truy cập web

Mô phỏng chia sẻ File qua FTP, mục tiêu là giúp các máy tính trong cùng mạng LAN chia sẻ dữ liệu. Để sử dụng, ta cần tài khoản để truy cập vào server mặc

định là cisco mật khẩu cũng là cisco. Sử dụng lệnh put sampleFile.txt để upload lên server.



The screenshot shows the 'Command Prompt' window of a PC in Cisco Packet Tracer. The window title is 'Command Prompt'. The text inside shows the following commands and output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.200
Trying to connect...192.168.1.200
Connected to 192.168.1.200
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put sampleFile.txt

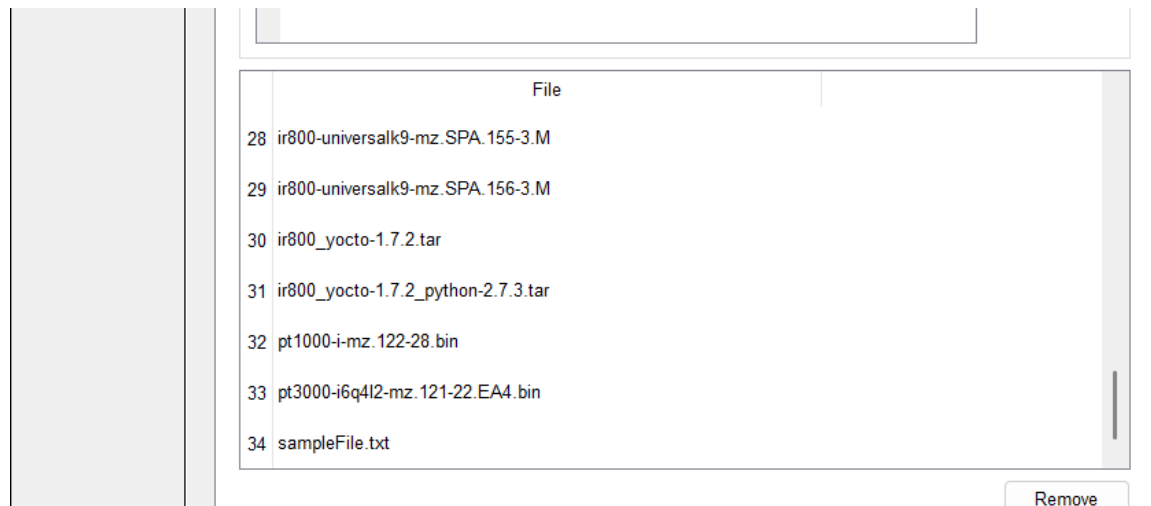
Writing file sampleFile.txt to 192.168.1.200:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.08 secs (325 bytes/sec)
ftp>
```

Hình 37: Mô phỏng gửi dữ liệu qua FTP

Ở bên phía server ta thấy sampleFile.txt ở hàng thứ 34.



Hình 38: Kết quả kiểm tra gửi sample file

3.3.2. Cấu hình định tuyến (routing) cho mạng WAN.

Sử dụng giao thức OSPF

```

R0(config)#router ospf 10
R0(config-router)#network 172.16.10.0 0.0.0.255 area 0
R0(config-router)#network 192.168.10.0 0.0.0.255 area 0
R0(config-router)#exit

```

Hình 39: Cấu hình định tuyến sử dụng OSPF

Để cấu hình định tuyến sử dụng giải thuật OSPF, ta thực hiện các bước code line như trên hình.

- Trong đó địa chỉ IP là địa chỉ IP có byte cuối là host 0, Subnet Mask là 0.0.0.255 dùng để đọc byte cuối.

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 10
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#
00:17:30: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.10.1 on Serial2/0 from LOADING to FULL, Loading Done

```

Hình 40: Thông báo routing thành công

Làm tương tự với các router khác, sau khi cấu hình địa chỉ IP khớp với Serial connection của router trước đó, ta sẽ nhận được dòng thông báo *Loading Done*.

Sau khi đã kết nối các network address, ta có thể kiểm tra lại các kết nối đó bằng cách sử dụng lệnh '*show ip route ospf*'. Lệnh này cho phép ta xem lại các kết nối ta đã cấu hình trên giải thuật định tuyến OSPF.

```

R3#
%SYS-5-CONFIG_I: Configured from console by console
show ip route ospf
    10.0.0.0/24 is subnetted, 1 subnets
O       10.1.1.0 [110/128] via 192.168.20.1, 00:00:41, Serial2/0
    172.16.0.0/24 is subnetted, 1 subnets
O       172.16.10.0 [110/193] via 192.168.20.1, 00:00:41, Serial2/0
O       192.168.10.0 [110/192] via 192.168.20.1, 00:00:41, Serial2/0

```

Hình 41: Hiển thị các IP đã routing

Hoặc ta có thể sử dụng lệnh *show ip route*


```

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.1.0 [110/128] via 192.168.20.1, 00:00:47, Serial2/0
    172.16.0.0/24 is subnetted, 1 subnets
C      172.16.10.0 [110/193] via 192.168.20.1, 00:00:47, Serial2/0
C     192.168.10.0/24 [110/192] via 192.168.20.1, 00:00:47, Serial2/0
C     192.168.20.0/24 is directly connected, Serial2/0
C     200.200.200.0/24 is directly connected, FastEthernet0/0

```

Hình 42: Hiện thị tất cả các IP route

Lệnh này cho phép ta xem tất cả các kết nối mà ta đã cấu hình trên router đó được link với các router có IP address khác trong mạng WAN.

Để test liên kết các định tuyến, ta có thể dụng lệnh *ping IP address* trên CLI hoặc Commant Prompt

Sử dụng giao thức RIP

Với sơ đồ ví dụ như hình trên, tiến hành cấu hình định tuyến RIP cho các router như sau:

Cấu hình router R1: sử dụng RIP version 2

```

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.10.0
R1(config-router)#network 10.1.1.0

```

Cấu hình router R2: sử dụng RIP version 2

```

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.1.1.0

```

R2(config-router)#network 192.168.20.0

Tóm lại, để cấu hình RIP cho router thì sử dụng các câu lệnh cơ bản sau:

Router (config) # router rip

Router (config-router) # version 2

Router (config-router) # network mang_can_quang_ba

Ngoài ra còn có các option sau:

- Auto-summary (gộp các subnet lại thành một network chung)
- Default-information originate (quảng bá tuyến default route của nó cho các router cùng chạy RIP bên trong)
- Redistribute static (quảng bá những static route của nó cho các router cùng chạy RIP bên trong)
- Distance (set giá trị AD)
- Passive-interface (không cho gửi thông tin RIP đến các cổng connected với host để giảm traffic vô ích)

Sử dụng giao thức EIGRP

Để cấu hình định tuyến cho router trong mạng WAN sử dụng giao thức EIGRP (Enhanced Interior Gateway Routing Protocol), bạn có thể thực hiện theo các bước sau:

Sử dụng lệnh sau để bật EIGRP và chỉ định một Autonomous System (AS) number (số AS phải giống nhau trên tất cả các router trong cùng một miền EIGRP):

```
router eigrp <AS-number>
```

```
router eigrp 100
```

Dùng lệnh network để chỉ định các mạng mà router sẽ quảng bá và tham gia vào EIGRP. Bạn cần nhập địa chỉ mạng và wildcard mask (hoặc subnet mask đảo ngược).

Ví dụ: Nếu router có giao diện với địa chỉ IP 192.168.1.1/24 và 10.0.0.1/30, bạn nhập:

```
network 192.168.1.0 0.0.0.255  
  
network 10.0.0.0 0.0.0.3
```

Lưu ý: Chỉ các giao diện thuộc mạng được khai báo mới tham gia EIGRP.

Mặc định, EIGRP tự động tóm tắt các mạng theo ranh giới classful, điều này có thể gây vấn đề trong mạng WAN phức tạp. Để tắt:

```
no auto-summary
```

Điều chỉnh băng thông (bandwidth): Trong mạng WAN, bạn có thể cần chỉ định băng thông chính xác cho giao diện để EIGRP tính toán metric chính xác hơn:

```
interface <interface-name>  
  
bandwidth <value-in-kbps>  
  
interface Serial0/0/0  
  
bandwidth 1544
```

Để tăng cường bảo mật, bạn có thể bật xác thực MD5:

```
key chain <key-chain-name>  
  
key 1  
  
key-string <password>  
  
exit  
  
interface <interface-name>  
  
ip authentication mode eigrp <AS-number> md5  
  
ip authentication key-chain eigrp <AS-number> <key-chain-name>
```

Sau khi cấu hình, kiểm tra trạng thái EIGRP bằng các lệnh:

Xem bảng định tuyến:

```
show ip route
```

Xem các neighbor (hàng xóm) EIGRP:

```
show ip eigrp neighbors
```

Xem thông tin chi tiết về EIGRP:

```
show ip eigrp topology
```

Lưu cấu hình để áp dụng vĩnh viễn:

```
write memory
```

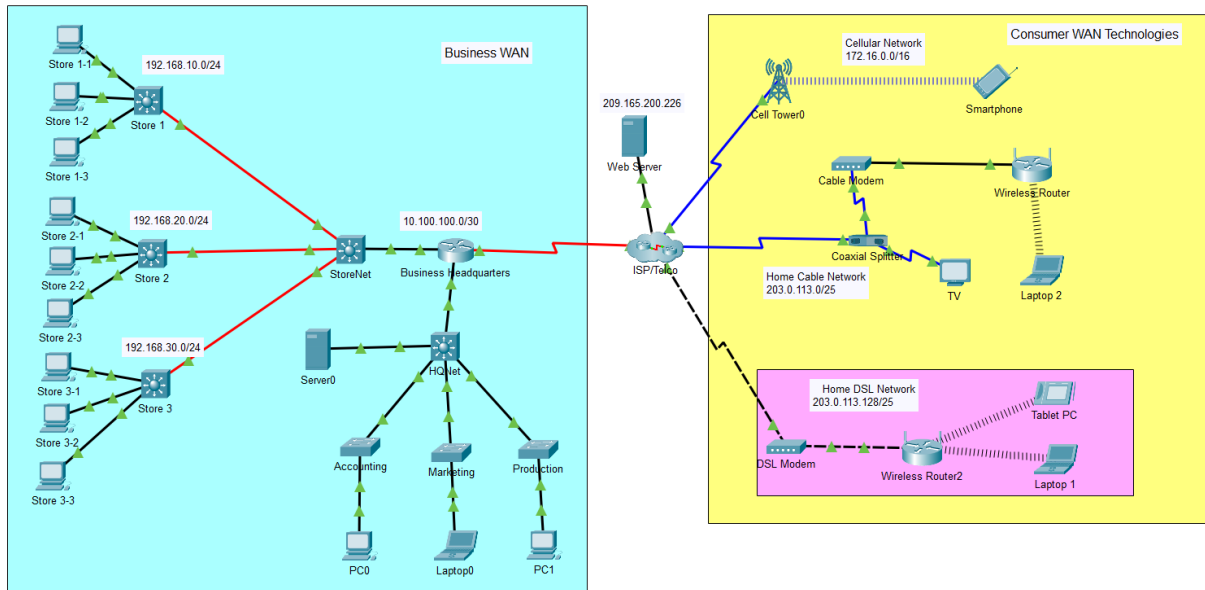
hoặc

```
copy running-config startup-config
```

3.4. Kiểm tra và đánh giá

Các bài toán mô phỏng được xem là cơ bản hoàn thành tốt, các kết nối hoạt động ổn định, tuy là trong mô phỏng các tín hiệu gửi đi có mức độ chậm trễ khác nhau phụ thuộc vào đường dây và số lượng các kết nối. Tuy nhiên nhìn chung các thiết bị hoạt động ổn định và hầu hết đều được cấu hình đầy đủ các chức năng cơ bản. Các bài test tín hiệu giữa các thiết bị đầu cuối mạng LAN dưới lệnh *ping* trả về kết quả rất nhanh và hợp lí. Các bài test kết nối bằng mô phỏng gửi mail cho về kết quả chậm hơn và có phần không rõ ràng trong các thông số, tuy nhiên dựa trên những hình ảnh mô phỏng đường đi của tín hiệu ta cũng có thể dễ dàng tính toán cũng như xem xét được các kết quả mà ta nhận được. Kiểm tra *telnet line* cũng là một phương pháp hữu ích để kiểm tra các kết nối của các thiết bị máy tính được cấu hình liên kết với nhau trong mạng LAN hoặc WAN, tuy nhiên để cấu hình *telnet line* có độ phức tạp cao hơn, kết quả trả về cũng dễ dàng chấp nhận được.

3.5. Mô phỏng hệ thống mạng thực tế



Hình 43: Mô phỏng hệ thống mạng WAN công cộng

Mô tả về mô phỏng hệ thống mạng WAN thực tế:

Mạng máy tính là một phần không thể thiếu trong cả môi trường kinh doanh và tiêu dùng hiện đại. Chúng ta đang sống trong một thế giới nơi công nghệ kết nối đóng vai trò cốt lõi, từ việc đảm bảo hiệu suất làm việc của doanh nghiệp đến việc tạo sự tiện nghi trong cuộc sống thường ngày. Mô hình mô phỏng hệ thống mạng trong hình ảnh cung cấp cái nhìn toàn diện về cách thiết lập và quản lý các mạng trong các kịch bản khác nhau. Phân tích này sẽ tập trung vào các thành phần mạng, vai trò của chúng và ý nghĩa của sự phối hợp này đối với cuộc sống hàng ngày.

Hệ thống mạng doanh nghiệp

Trong mô hình này, mạng doanh nghiệp được phân chia thành các vùng mạng (subnet) để quản lý dễ dàng hơn. Các cửa hàng chi nhánh, chẳng hạn như Cửa hàng 1, 2 và 3, mỗi chi nhánh đều có một dải địa chỉ IP riêng biệt (192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24). Điều này không chỉ giúp tối ưu hóa lưu lượng mạng mà còn hỗ trợ trong việc phát hiện và xử lý sự cố.

Trung tâm của hệ thống mạng doanh nghiệp là StoreNet, nơi đóng vai trò trung gian kết nối các cửa hàng với Business Headquarter (Trụ sở). Trụ sở này lại quản lý nhiều bộ phận, từ Kế toán, Marketing đến Sản xuất, qua các thiết bị quan

trọng như Server0 và PC1. Địa chỉ mạng 10.100.100.0/30 là minh chứng cho cách quản lý hiệu quả, giúp tối ưu hóa việc giao tiếp nội bộ giữa các phòng ban.

Máy chủ web của doanh nghiệp, với địa chỉ IP 209.165.200.226, kết nối trực tiếp với ISP, đóng vai trò không chỉ trong quản lý nội bộ mà còn trong việc cung cấp dịch vụ và sản phẩm cho khách hàng trực tuyến. Sự kết hợp này là minh chứng cho việc doanh nghiệp đã tích hợp công nghệ tiên tiến để thích nghi với xu hướng kinh doanh hiện đại.

Hệ thống mạng tiêu dùng

Đối lập với sự phức tạp và quy mô lớn của mạng doanh nghiệp, các mạng tiêu dùng được thiết kế để phục vụ các cá nhân và gia đình. Trong mô hình, chúng ta thấy ba loại công nghệ tiêu biểu:

- + Mạng di động: Với địa chỉ mạng 172.16.0.0/16, mạng này cho phép các thiết bị như điện thoại thông minh kết nối, mang lại sự tiện lợi và linh hoạt.

- + Mạng truyền hình cáp gia đình: Kết nối với TV và bộ định tuyến không dây qua modem cáp, dải địa chỉ 203.0.113.0/25 cho phép phát sóng truyền hình và truy cập Internet tốc độ cao.

- + Mạng DSL gia đình: Cung cấp kết nối không dây cho laptop và máy tính bảng, qua dải địa chỉ 203.0.113.128/25, đóng vai trò quan trọng trong học tập, làm việc và giải trí.

Cáp đồng trục trong mạng tiêu dùng

Cáp đồng trục là lựa chọn phổ biến trong môi trường tiêu dùng vì những đặc điểm sau:

- + Phù hợp với nhu cầu phổ thông: Mạng tiêu dùng như truyền hình cáp và Internet băng thông rộng tại hộ gia đình không đòi hỏi sự ổn định quá cao hoặc khả năng truyền dữ liệu qua khoảng cách lớn. Cáp đồng trục hoàn toàn đáp ứng được những yêu cầu này.

- + Chi phí thấp: Một ưu điểm quan trọng của cáp đồng trục là giá thành rẻ, giúp các nhà cung cấp dịch vụ dễ dàng triển khai trên diện rộng mà không làm tăng chi phí cho người tiêu dùng.

+ Khả năng chịu nhiễu tốt: Cấu trúc đặc biệt của cáp đồng trục bao gồm lớp lõi dẫn, lớp cách điện, và lớp chống nhiễu, giúp nó truyền tín hiệu ổn định trong môi trường gia đình có nhiều thiết bị điện tử.

+ Ứng dụng rộng rãi: Cáp đồng trục thường được sử dụng trong các kết nối ngắn, ví dụ từ nhà mạng đến modem của người dùng, và hỗ trợ tốt cho các dịch vụ truyền hình cáp và Internet tốc độ cao.

Cáp nối tiếp trong mạng doanh nghiệp

Trong môi trường doanh nghiệp, nơi đòi hỏi kết nối mạng phải ổn định, đáng tin cậy và có khả năng hoạt động qua khoảng cách xa, cáp nối tiếp được lựa chọn vì các lý do sau:

+ Khả năng truyền dữ liệu qua khoảng cách lớn: Doanh nghiệp thường cần kết nối giữa các chi nhánh hoặc giữa chi nhánh và trụ sở chính. Cáp nối tiếp được thiết kế để truyền tải tín hiệu qua những khoảng cách lớn này mà vẫn đảm bảo chất lượng dữ liệu.

+ Độ ổn định cao: Mạng doanh nghiệp đòi hỏi sự liên tục và không bị gián đoạn. Cáp nối tiếp đáp ứng tốt nhu cầu này, đặc biệt trong các ứng dụng quan trọng như kết nối máy chủ hay giao tiếp giữa các phòng ban.

+ Tương thích với công nghệ mạng WAN: Mạng doanh nghiệp thường sử dụng các giao thức WAN tiên tiến như PPP (Point-to-Point Protocol) hoặc Frame Relay, những công nghệ yêu cầu kết nối qua cáp nối tiếp để đạt hiệu suất tối đa.

+ Hỗ trợ thiết bị chuyên dụng: Các thiết bị mạng lớn trong doanh nghiệp, như router WAN, thường yêu cầu kết nối qua cáp nối tiếp, giúp quản lý và vận hành hệ thống hiệu quả.

Kết luận

Mô hình mô phỏng mạng này minh họa rõ ràng sự đa dạng và tinh tế trong cách các hệ thống mạng được triển khai và vận hành. Đối với doanh nghiệp, mạng là nền tảng để đảm bảo hiệu quả hoạt động và kết nối liên tục giữa các bộ phận. Trong khi đó, đối với người dùng cá nhân, mạng mang đến sự tiện nghi và hỗ trợ các nhu cầu hàng ngày từ giao tiếp, giải trí đến công việc. Nhìn chung, mạng máy

tính không chỉ là một công nghệ mà còn là cầu nối giữa con người và thế giới số hóa.

4. Nhận xét

4.1. Ưu điểm của phương pháp mô phỏng so với thực tế.

Phương pháp mô phỏng mạng, đặc biệt khi sử dụng phần mềm như Cisco Packet Tracer, mang lại nhiều lợi thế vượt trội so với việc triển khai mạng trên phần cứng thực tế.

Thứ nhất, mô phỏng giúp tiết kiệm chi phí đáng kể. Việc mua sắm và duy trì các thiết bị mạng như router, switch, cáp nối và các phụ kiện khác đòi hỏi một khoản đầu tư lớn, trong khi phần mềm mô phỏng cho phép người dùng xây dựng và thử nghiệm mạng hoàn toàn miễn phí hoặc với chi phí rất thấp. Điều này đặc biệt hữu ích trong môi trường học tập hoặc các dự án thử nghiệm không có ngân sách lớn.

Thứ hai, phương pháp mô phỏng mang lại sự linh hoạt cao. Người dùng có thể dễ dàng thay đổi cấu hình, thêm hoặc bớt thiết bị, thử nghiệm các giao thức khác nhau mà không cần lo lắng về việc làm hỏng phần cứng hoặc gây gián đoạn hệ thống thực tế. Quá trình này cũng cho phép quay lại trạng thái ban đầu chỉ với vài thao tác, giúp tiết kiệm thời gian so với việc xử lý sự cố trên thiết bị vật lý.

Thứ ba, mô phỏng cung cấp khả năng quan sát trực quan và chi tiết. Trong Cisco Packet Tracer, người dùng có thể theo dõi luồng dữ liệu, kiểm tra cách các gói tin di chuyển qua mạng, và phân tích hiệu suất thông qua các công cụ tích hợp. Điều này không chỉ hỗ trợ việc học tập mà còn giúp người dùng hiểu rõ hơn về cách hoạt động của mạng, điều mà thực tế khó thực hiện nếu không có thiết bị giám sát chuyên dụng.

Thứ tư, phương pháp mô phỏng giảm thiểu rủi ro. Trong môi trường thực tế, một lỗi cấu hình có thể dẫn đến mất kết nối, hỏng thiết bị hoặc ảnh hưởng đến toàn bộ hệ thống. Ngược lại, trong môi trường ảo, người dùng có thể thoải mái thử nghiệm, thậm chí mô phỏng các sự cố như đứt cáp hay quá tải mạng, mà không gây hậu quả nghiêm trọng.

Cuối cùng, mô phỏng cho phép thử nghiệm các ý tưởng sáng tạo mà không bị giới hạn bởi nguồn lực vật lý. Người dùng có thể xây dựng các mô hình mạng quy mô lớn hoặc tích hợp nhiều công nghệ khác nhau để đánh giá hiệu quả, điều mà thực tế có thể không khả thi do hạn chế về thiết bị hoặc không gian.

4.2. Hạn chế gặp phải trong quá trình cấu hình.

Mặc dù phương pháp mô phỏng mang lại nhiều lợi ích, quá trình cấu hình mạng trong Cisco Packet Tracer cũng gặp phải một số hạn chế đáng chú ý:

Thứ nhất, phần mềm có giới hạn về tính năng và thiết bị hỗ trợ. Cisco Packet Tracer chủ yếu tập trung vào các thiết bị và giao thức cơ bản, do đó không thể mô phỏng đầy đủ các thiết bị mạng cao cấp hoặc các công nghệ mới nhất. Ví dụ, một số dòng router hoặc switch hiện đại của Cisco, cũng như các sản phẩm từ các nhà cung cấp khác, không được hỗ trợ, khiến mô hình mạng bị giới hạn trong phạm vi đơn giản.

Thứ hai, tính chân thực của mô phỏng không hoàn toàn phản ánh thực tế. Các yếu tố như độ trễ vật lý của cáp, hiệu suất thực tế của phần cứng, hoặc các lỗi phát sinh từ môi trường (như nhiễu điện từ) không được tái hiện chính xác trong Cisco Packet Tracer. Điều này có thể dẫn đến sự khác biệt giữa kết quả mô phỏng và triển khai thực tế, đặc biệt khi áp dụng vào các hệ thống mạng phức tạp.

Thứ ba, quá trình cấu hình đôi khi gặp khó khăn do giao diện hoặc lỗi phần mềm. Mặc dù Cisco Packet Tracer có giao diện thân thiện, nhưng việc cấu hình qua dòng lệnh có thể không mượt mà như trên thiết bị thật, hoặc phần mềm có thể gặp trục trặc như treo ứng dụng khi mô phỏng mạng lớn. Điều này làm gián đoạn quá trình thực hành và phân tích.

Thứ tư, thiếu sự tương tác với phần cứng thực tế là một hạn chế lớn. Cisco Packet Tracer hoạt động hoàn toàn trong môi trường ảo, không thể kết nối với các thiết bị vật lý hoặc mạng thực, khiến người dùng không có cơ hội trải nghiệm các tình huống thực tế như lắp đặt cáp, kiểm tra tín hiệu hay xử lý lỗi phần cứng.

Cuối cùng, việc phụ thuộc quá nhiều vào mô phỏng có thể làm giảm kỹ năng thực hành thực tế của người dùng. Nếu chỉ quen với môi trường ảo, người học hoặc kỹ sư có thể gặp khó khăn khi làm việc với thiết bị thật trong công việc sau này.

4.3. Đề xuất cải tiến mô hình mạng.

Dựa trên các ưu điểm và hạn chế đã phân tích, dưới đây là một số đề xuất để cải tiến mô hình mạng trong nghiên cứu này, nhằm nâng cao hiệu quả và tính thực tiễn:

Thứ nhất, bổ sung thêm các thiết bị và giao thức nâng cao vào mô hình. Mặc dù Cisco Packet Tracer có giới hạn, người dùng có thể tối ưu hóa mô hình bằng cách tích hợp các giao thức định tuyến động như OSPF thay vì chỉ sử dụng RIP, hoặc thêm các VLAN để phân đoạn mạng LAN, từ đó tăng tính linh hoạt và hiệu suất của hệ thống.

Thứ hai, kết hợp mô phỏng với thực hành thực tế nếu có điều kiện. Để khắc phục nhược điểm về tính chân thực, có thể sử dụng Cisco Packet Tracer để thiết kế ban đầu, sau đó triển khai một phần mô hình trên thiết bị thật (như router và switch cơ bản) để so sánh kết quả. Điều này giúp người dùng vừa tận dụng được lợi ích của mô phỏng, vừa làm quen với phần cứng thực tế.

Thứ ba, mở rộng quy mô mô hình để mô phỏng các kịch bản phức tạp hơn. Ví dụ, thay vì chỉ kết nối hai mạng LAN qua WAN, có thể thêm nhiều chi nhánh, tích hợp máy chủ (server) để mô phỏng dịch vụ như web hoặc email, và kiểm tra khả năng chịu tải của mạng khi lưu lượng tăng cao. Điều này giúp đánh giá toàn diện hơn về hiệu suất và khả năng mở rộng của mô hình.

Thứ tư, sử dụng thêm các công cụ mô phỏng khác để hỗ trợ. Nếu Cisco Packet Tracer không đáp ứng được yêu cầu về tính năng nâng cao, có thể kết hợp với GNS3 – một phần mềm mạnh mẽ hơn, hỗ trợ thiết bị thực tế và các giao thức phức tạp. Sự kết hợp này sẽ giúp mô hình mạng sát với thực tế hơn, dù đòi hỏi kỹ năng và tài nguyên cao hơn.

Cuối cùng, cải thiện việc phân tích hiệu suất bằng cách sử dụng các công cụ đo lường trong phần mềm. Người dùng nên tận dụng tính năng Simulation Mode của Cisco Packet Tracer để theo dõi chi tiết luồng dữ liệu, độ trễ, và tỷ lệ mất gói tin, từ đó đưa ra các điều chỉnh cụ thể như tối ưu hóa băng thông hoặc thay đổi cấu hình định tuyến.

Những đề xuất này không chỉ giúp khắc phục hạn chế của mô hình hiện tại mà còn nâng cao giá trị ứng dụng thực tế, đáp ứng tốt hơn nhu cầu học tập và công việc trong lĩnh vực mạng máy tính.

5. Kết luận và hướng phát triển

5.1. Kết luận

Sau khi thực hiện đề tài nghiên cứu về tầm quan trọng của mạng LAN/WAN và vai trò của phần mềm mô phỏng trong thiết kế, cấu hình mạng, nhiều kết quả

đáng chú ý đã được ghi nhận, đồng thời mang lại những bài học giá trị trong quá trình học tập và ứng dụng thực tiễn:

Trước hết, nghiên cứu đã hoàn thành việc tìm hiểu cách sử dụng phần mềm Cisco Packet Tracer để cấu hình các hệ thống mạng LAN và WAN cơ bản. Thông qua việc thiết lập các thiết bị như router, switch và PC, cùng với việc áp dụng các giao thức định tuyến và gán địa chỉ IP, một mô hình mạng mẫu đã được xây dựng thành công. Mô hình này mô phỏng các kịch bản thực tế như kết nối mạng nội bộ trong một văn phòng và liên kết giữa các chi nhánh qua mạng diện rộng. Quá trình phân tích hiệu quả hoạt động của mô hình, bao gồm tốc độ truyền dữ liệu, độ trễ và tính ổn định, đã giúp làm rõ cách các thành phần mạng tương tác với nhau trong môi trường ảo.

Từ quá trình thực hiện, nhiều bài học quan trọng đã được rút ra. Thứ nhất, việc sử dụng phần mềm mô phỏng không chỉ giúp nắm vững lý thuyết về mạng máy tính mà còn rèn luyện kỹ năng thực hành, từ cách cấu hình thiết bị đến xử lý các vấn đề cơ bản như lỗi kết nối hay xung đột địa chỉ IP. Thứ hai, nghiên cứu đã cho thấy sự tiện lợi của mô phỏng trong việc thử nghiệm và điều chỉnh mạng mà không cần đến phần cứng thực tế, qua đó tiết kiệm thời gian, chi phí và giảm thiểu rủi ro. Thứ ba, quá trình này cũng giúp nhận diện những hạn chế của mô phỏng, chẳng hạn như sự khác biệt giữa môi trường ảo và thực tế, từ đó nâng cao ý thức về việc kết hợp lý thuyết, mô phỏng và thực hành để đạt hiệu quả tối ưu.

Đề tài đã khẳng định rõ vai trò quan trọng của phần mềm mô phỏng, đặc biệt là Cisco Packet Tracer, trong việc học tập và triển khai mạng. Đối với học tập, phần mềm này là một công cụ trực quan, dễ tiếp cận, giúp sinh viên và người mới bắt đầu hiểu rõ các khái niệm mạng phức tạp thông qua trải nghiệm thực tế mà không cần đầu tư lớn. Đối với triển khai mạng, mô phỏng đóng vai trò như một bước thử nghiệm ban đầu, cho phép các kỹ sư kiểm tra cấu hình, phát hiện lỗi và tối ưu hóa hệ thống trước khi áp dụng vào thực tế. Dù không thể thay thế hoàn toàn phần cứng vật lý, phần mềm mô phỏng vẫn là một cầu nối hiệu quả giữa lý thuyết và ứng dụng, góp phần nâng cao chất lượng đào tạo và phát triển kỹ năng trong lĩnh vực công nghệ thông tin.

Tóm lại, nghiên cứu không chỉ hoàn thành các mục tiêu đề ra mà còn nhấn mạnh giá trị thực tiễn của phần mềm mô phỏng trong bối cảnh mạng máy tính ngày càng trở nên thiết yếu. Đây là nền tảng để tiếp tục khám phá các công nghệ mạng tiên tiến hơn trong tương lai, đồng thời khẳng định tầm quan trọng của việc kết hợp

công cụ mô phỏng với thực hành thực tế để đáp ứng nhu cầu ngày càng cao của xã hội hiện đại.

5.2. Hướng phát triển

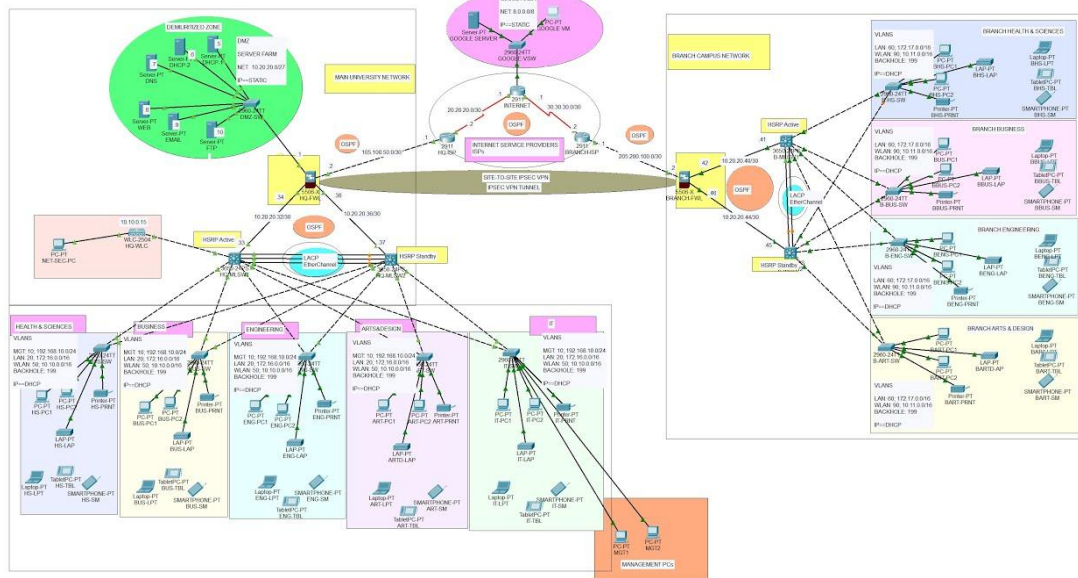
5.2.1. Mở rộng mô hình với các giao thức phức tạp hơn

Công nghệ VLAN: VLAN là công nghệ chia mạng vật lý thành nhiều mạng logic riêng biệt mà không cần thêm phần cứng. Mỗi VLAN hoạt động như một mạng riêng, tăng cường bảo mật và giảm xung đột lưu lượng. Tích hợp với các hệ thống quản lý mạng thông minh (SDN - Software-Defined Networking) để tự động hóa việc cấu hình VLAN. Ứng dụng trong các trung tâm dữ liệu lớn để phân đoạn lưu lượng và tối ưu hóa hiệu suất. Kết hợp với IoT để quản lý số lượng lớn thiết bị trong các mạng doanh nghiệp.

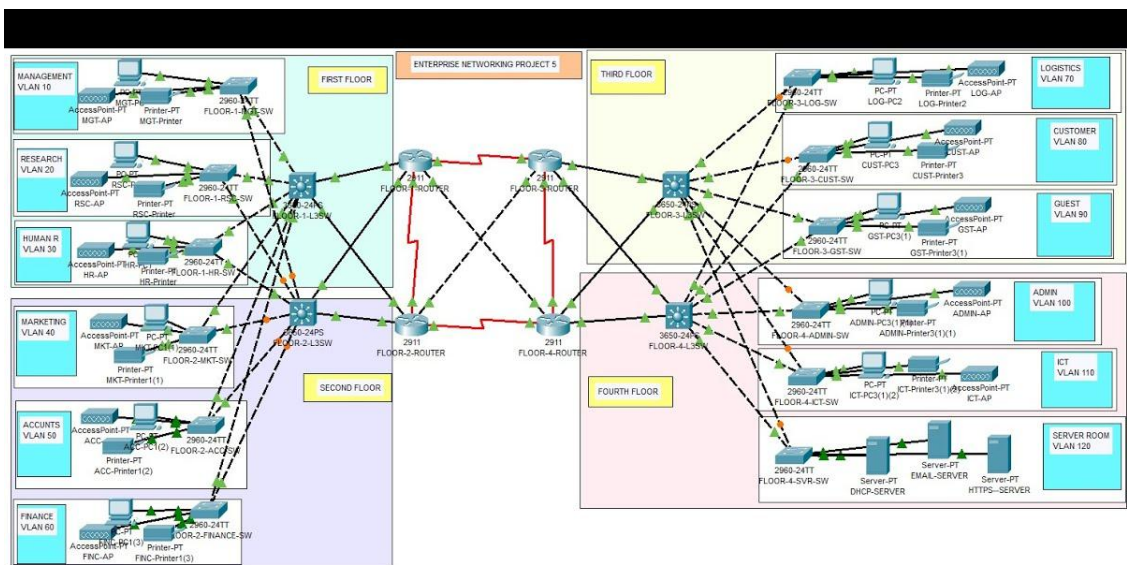
Công nghệ VPN: VPN tạo ra một đường hầm mã hóa qua internet, cho phép người dùng truy cập mạng từ xa một cách an toàn, bảo vệ dữ liệu khỏi bị theo dõi. Chuyển từ VPN truyền thống sang các giải pháp dựa trên đám mây (Cloud VPN) để hỗ trợ làm việc từ xa hiệu quả hơn. Tăng cường bảo mật với các giao thức mã hóa tiên tiến (như WireGuard) và tích hợp xác thực đa yếu tố (MFA). Mở rộng ứng dụng trong các tổ chức phân tán, đặc biệt khi nhu cầu làm việc hybrid (kết hợp tại chỗ và từ xa) tăng cao.

Công nghệ SD-WAN: SD-WAN là một cách tiếp cận dựa trên phần mềm để quản lý và tối ưu hóa mạng diện rộng (WAN), thay thế các giải pháp MPLS truyền thống bằng cách sử dụng internet công cộng và các kết nối khác. Tích hợp AI để tự động định tuyến lưu lượng, dự đoán và xử lý sự cố mạng. Hỗ trợ các ứng dụng thời gian thực (như VoIP, video hội nghị) với độ trễ thấp và chất lượng dịch vụ (QoS) cao. Phát triển thành nền tảng "SASE" (Secure Access Service Edge), kết hợp SD-WAN với bảo mật đám mây để đáp ứng nhu cầu doanh nghiệp hiện đại.

5.2.2. Ứng dụng vào các kịch bản thực tế (doanh nghiệp, trường học).



Hình 44: Mô phỏng mô hình Campus Network



Hình 45: Mô phỏng mô hình Bank Network

6. Tài liệu tham khảo

1. Các thuật toán trong networking. Truy cập từ: <https://wirexsystems.com/resource/protocols>
2. Chức năng của Switch và Router. Truy cập từ: [Tìm hiểu về các thiết bị chuyển mạch sự khác nhau giữa chúng, Sự khác nhau giữa Hub, Switch và Router](#)
3. Hưng Nguyễn. Mạng VLAN là gì? (16/04/2024). Truy cập từ: <https://vietnix.vn/vlan/>
4. Kiến thức mạng máy tính. Truy cập từ: [Part1: Kiến thức mạng máy tính - Giới thiệu về bộ giao thức TCP/IP](#)
5. Kiến thức về Subnetting. Truy cập từ: [Understanding the Role of Subnetting in Computer Networks](#)
6. PGS. Trương Diệu Linh. Các giao thức định tuyến
7. Trương Thị Hồng Nhung. Định tuyến động là gì? Cấu hình định tuyến động RIP như thế nào? (31/12/2015). Truy cập từ: <https://vnpro.vn/thu-vien/dinh-tuyen-dong-la-gi-cau-hinh-dinh-tuyen-dong-rip-nhu-the-nao-2349.html>
8. Topology là gì ?. Truy cập từ: <https://cmcccloud.vn/tin-tuc/topology-la-gi>
9. Sự khác biệt giữa LAN, và WAN. Truy cập từ: [WAN so với LAN - Điểm khác biệt giữa các loại mạng máy tính - AWS](#)
10. Võ Ngọc Tiến, Tăng Anh Tuấn. Sử dụng công nghệ SD-WAN để tăng chất lượng truyền tải trong hệ thống mạng thế hệ mới. Tạp chí Khoa học và Công nghệ, tr. 29-35 (20/07/2022).