MỞ ĐẦU

Lý do chọn đề tài

Yêu cầu quan trọng đối với sinh viên Công nghệ thông tin là vận dụng kiến thức đã học vào thực tiễn để đạt được những kinh nghiệm nhất định. Tuy nhiên, trong môi trường Đại học thì khó tránh khỏi không có đầy đủ trang thiết bị để thực hành mà ở đây là các thiết bị mạng do chi phí lắp đặt để cho sinh viên thực hành rất đắt đỏ. Ngoài ra, sinh viên cũng là người chưa có nhiều kinh nghiệm nên việc thực hành dễ dẫn đến hư hỏng các thiết bị mạng nếu không biết cách thiết lập đúng. Để có thể nắm vững kiến thức đã học thì việc thực hành liên quan đến kiến thức đó là cần thiết.

Để làm được điều đó, đồng thời trang bị tốt những kiến thức về mạng máy tính, đồng thời trang bị được các kỹ năng cơ bản về thiết kế, triển khai các hệ thống mạng.

Chính vì thế, tôi đã chọn đề tài "Xây dựng hệ thống mạng không dây" là phần mềm mô phỏng mạng dưới dạng đồ họa, cho phép người dùng mô phỏng nhiều thiết bị mạng và các hệ thống mạng khác nhau, kết nối mạng ảo với mạng thật và ngoài ra còn nhiều chức năng khác .

Mục đích nghiên cứu

- Tìm hiểu tổng quan về phần mềm Cisco Packet Tracer, từ đó đưa ra các đánh giá về khả năng ứng dụng để thực hành các kỹ năng về xây dựng thiết kế, quản trị các hệ thống mạng.

- Thực hiện mô phỏng một mô hình mạng đơn giản gồm một số Router, Switch, PC, Wireless Router, Smartphone, Laptop và cấu hình định tuyến, cài đặt dịch vụ web, chia Vlan để kiểm chứng khả năng hoạt động trên một mô hình mạng cụ thể.

Đối tượng và phạm vi nghiên cứu

- Đối tượng nghiên cứu chính: phần mềm Cisco Packet Tracer.
- Phạm vi nghiên cứu: Xây dựng hệ thống mạng không dây và thực hiện mô phỏng, cấu hình một hệ thống mạng.

LỜI CẢM ƠN

Lời đầu tiên, em xin gửi lời cảm ơn chân thành và sự tri ân sâu sắc đối với các thầy/cô của trường Đại học Trà Vinh, đặc biệt là thầy Huỳnh Văn Thanh đã tận tình truyền đạt kiến thức để em thực hiện đồ án này. Với vốn kiến thức được tiếp thu trong quá trình chỉ dạy không chỉ là nền tảng cho quá trình nghiên cứu bài báo cáo đồ án mà nó còn là hành trang quý báu em áp dụng cho sau này. Đồng thời em cũng xin cảm ơn đến các giảng viên khác cũng như bộ môn đã tạo điều kiện để em thực hiện đồ án chuyên nghành này.

Do còn hạn chế về kiến thức cũng như những kinh nghiệm thực tế cho nên trong quá trình thực hiện đề tài cũng không tránh khỏi sai sót, mặc dù đã hoàn thành đề tài nhưng có thể vẫn còn nhiều thiếu sót. Rất mong được sự góp ý từ quý thầy cô và hội đồng.

Xin chân thành cảm ơn!

Trà Vinh, tháng 1 năm 2024

Người thực hiện

Nguyễn Ngọc Thịnh

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

Trà Vinh, ngày ….. tháng …… năm ……

Giáo viên hướng dẫn

NHẬN XÉT CỦA THÀNH VIÊN HỘI ĐỒNG

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

Trà Vinh, ngày ….. tháng …… năm ……

Thành viên hội đồng

MỤC LỤC

DANH MỤC HÌNH ẢNH

Trang

BẢNG BIỂU

BẢN TÓM TẮT ĐỒ ÁN CHUYÊN NGÀNH

(Đề tài: Xây dựng hệ thống mạng không dây)

Lý do chọn đề tài

Giúp nắm vững kiến thức đã học về mạng khi vận dụng kiến thức đó để xây dựng một hệ thống mạng khi không có đủ cơ sở vật chất.

Giúp trang bị tốt kinh nghiệm, những kỹ năng cơ bản về thiết kế, cách thức triển khai hệ thống mạng trong quá trình thực hiện.

Vấn đề nghiên cứu

Mạng máy tính: khái niệm mạng máy tính, các thành phần cơ bản của mạng máy tính, cách thức hoạt động của mạng máy tính, địa chỉ IP và các khái niệm liên quan.
Định tuyến: Khái niệm định tuyến, phân loại định tuyến.

Phần mềm Packet Tracer: Cài đặt và sử dụng phần mềm Packet Tracer , các chế độ cấu hình, các câu lệnh thường dùng trong Packet Tracer.

Quá trình thực hiện và kết quả nghiên cứu

Quá trình thực hiện:
Tìm hiểu các kiến thức về mạng máy tính, mạng không dây và các kiến thức liên quan.
Cài đặt môi trường giả lập mạng máy tính bằng phần mềm Packet Tracer.

Đề xuất một mô hình mạng có sử dụng các thiết bị mạng: Router, Switch, Wireless Router, Smartphone, Server -PT cấu hình định tuyến cho Router, liên thông mạng cho các PC.

Kết quả nghiên cứu:

Có kiến thức cơ bản về mạng máy tính, mạng không dây, xây dựng được một mô hình mạng , định tuyến cho Router, liên thông mạng cho các PC, truy cập được web, bảo mật mạng không dây.

Định hướng phát triển đề tài

Đề xuất và cấu hình một mô hình mạng với nhiều thiết bị phức tạp hơn với các giao thức định tuyến khác, cấu hình thêm các thiết bị như ATM, cloud …
Cấu hình trên các phần mềm chuyên dụng khác, sau đó cấu hình trên máy thật.

Chương 1: TỔNG QUAN MẠNG MÁY TÍNH

1. Mạng máy tính

- Sự hình thành mạng máy tính xuất phát từ nhu cầu chia sẻ, sử dụng chung tài nguyên và giao tiếp trực tuyến.
- Khái niệm cơ bản nhất: Mạng máy tình gồm hai hay nhiều máy tính kết nối với nhau bằng đường truyền vô tính hay hữu tính.
- Mọi mạng máy tính dù đơn giản hay phức tạp thì đều bắt nguồn từ nguyên lý này.
- Một số khái niệm khác: Mạng máy tính là một nhóm các máy tính mà mỗi máy có thể liên lạc được với nhau, cùng chia sẻ tài nguyên.

- Mạng máy tính là tập hợp máy tính được nối với nhau bởi các đường truyền vật lý theo một kiến trúc nào đó.

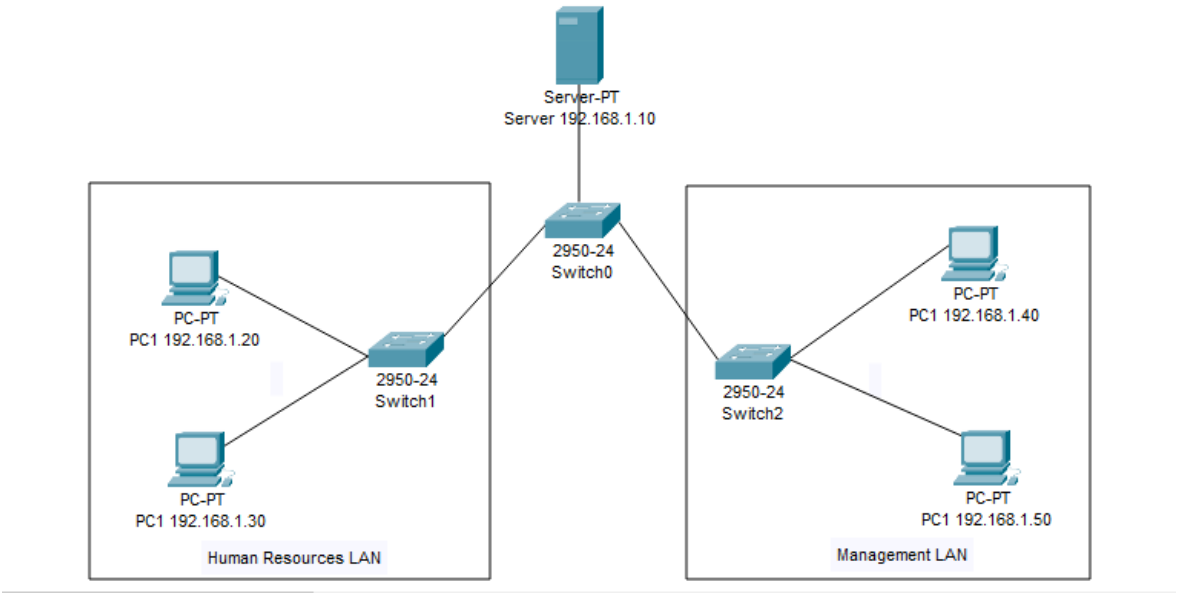
1.1.1Các thành phần cơ bản của mạng máy tính

- Các loại máy tính: PDA, PC, Laptop, …
- Các thiết bị giao tiếp: NIC (Network interface card hay card mạng), Hub (hiện nay ít dùng), Switch (bộ chuyển mạch dùng để mở rộng số cổng kết nối), Router (bộ định tuyến dùng để chuyển các gói dữ liệu đến thiết bị đầu cuối), …
- Môi trường truyền dẫn: Cáp, sóng điện từ, sóng viba, tia hồng ngoại, …
- Giao thức (protocol): TCP/IP, HTTP, HTTPS, POP3, SMTP, …
- Hệ điều hành: Windows, Mac, Linux, …
- Các tài nguyên: tập tin, thư mục

- Các thiết bị ngoại vi: máy in, máy quét, máy fax, …

1.1.2 Cách thức hoạt động

Các thiết bị chuyên dụng thường sử dụng như thiết bị chuyển mạch, router wifi sẽ giúp tạo ra nền tảng cho mạng máy tính. Trong đó, thiết bị chuyển mạch kết nối và giúp các máy tính, máy in, máy chủ và các thiết bị khác được bảo mật nội bộ với mạng trong gia đình hoặc tổ chức.



Hình 1. Mô hình mạng cơ bản.

Bộ định tuyến kết nối mạng với các mạng khác và hoạt động như trung tâm điều phối. Nó sẽ giữ vai trò phân tích dữ liệu được gửi qua một mạng, chọn các tuyến đường tốt nhất và gửi đến địa chỉ đích. Bộ định tuyến không chỉ giúp kết nối mạng gia đình và doanh nghiệp của bạn với thế giới bên ngoài mà còn bảo vệ thông tin khỏi các mối đe dọa bảo mật bên ngoài.

Cơ bản, bộ chuyển mạch và bộ định tuyến không giống nhau, đặc biệt là cách chúng xác định các thiết bị đầu cuối trong mạng. Tuy nhiên, nhiều thiết bị chuyển mạch hiện đại đã được mở rộng chức năng định tuyến. Trong một mạng máy tính, địa chỉ MAC và địa chỉ IP được sử dụng để xác định các thiết bị và kết nối mạng tương ứng.

1.2 Giới thiệu mạng không dây

1.2.1 Khái niệm mạng không dây

Mạng không dây (Wireless) là một hệ thống mạng kết nối giữa các thiết bị có khả năng thu phát sóng như: máy vi tính có gắn Adapter không dây,… Lại với nhau không sử dụng dây dẫn mà tahy vào đó sử dụng sóng vô tuyến, truyền dẫn trong không gian thông qua các trạm thu, phát sóng.

1.2.2 Các ứng dụng của mạng Wireless

Mạng không dây (Wireless) đã mở ra nhiều ứng dụng và tiện ích trong nhiều lĩnh vực khác nhau. Nên thiết lập Wireless ở những nơi có tính chất tạm thời để làm việc, ở những nơi mạng Cable truyền không thể thi công hoặc làm mất thẩm quan như: Các tòa nhà cao tầng, khách sạn, bệnh viện, nhà hàng, quán cafe,…nơi mà khách hàng thường sử dụng mạng không dây với cường độ cao.

Mạng không dây là kỹ thuật thay thế cho mạng LAN, nó cung cấp mạng cuối cùng với khoảng cách kết nối tối thiểu và mạng trong nhà hoặc người người dùng di động trong các cơ quan.

1.2.3 Nguyên lý hoạt động

Nguyên lý hoạt động của mạng wireless dựa trên việc sử dụng sóng điện từ (vô tuyến và tia hồng ngoại) để truyền thông tin từ điểm này sang điểm khác mà không cần sử dụng bất kỳ kết nối vật lý nào. Mạng truyền thông không dây, hay còn gọi là mạng wireless, là mạng điện thoại hoặc mạng máy tính sử dụng sóng radio làm nguồn sóng truyền dẫn tín hiệu. Mạng wireless hoạt động thông qua việc sử dụng sóng điện từ để truyền thông tin từ một điểm đến điểm khác mà không cần sự kết nối vật lý. Wi-Fi là một công nghệ không dây cho phép các thiết bị kết nối với internet mà không cần sử dụng cáp vật lý. Nó hoạt động bằng cách truyền tín hiệu qua kết nối không dây. Wi-Fi thường được sử dụng trên các thiết bị như điện thoại, máy tính bảng, laptop và smart TV.

1.2.4 Ưu nhược điểm của mạng không dây

1.2.4.1 Ưu điểm của mạng không dây

- Mạng không dây cho phép kết nối mọi nơi trong vùng phủ sóng, giúp tăng cường sự di động và linh hoạt.
- Cài đặt và triển khai mạng không dây thường nhanh chóng hơn so với mạng có dây, không cần phải lắp đặt dây cáp.
- Mạng không dây có khả năng mở rộng một cách dễ dàng bằng cách thêm điểm truy cập mới mà không cần lắp đặt dây cáp mới.
- Cho phép thiết lập mạng ở những nơi khó tiếp cận hoặc trong các môi trường đòi hỏi sự linh hoạt cao.

- Thường có chi phí triển khai thấp hơn so với mạng có dây, đặc biệt trong các môi trường đòi hỏi sự linh hoạt và di động.
- Linh hoạt trong việc kết nối và quản lý nhiều thiết bị di động cùng một lúc.

1.2.4.2 Nhược điểm của mạng không dây

- Thường có hiệu suất thấp hơn so với mạng có dây, đặc biệt trong môi trường có nhiều thiết bị kết nối cùng một lúc.
- Có nguy cơ bảo mật cao hơn do dữ liệu truyền qua không gian và dễ bị nhiễm sóng.
- Môi trường như tường, cửa, và vật cản có thể làm giảm vùng phủ sóng và ảnh hưởng đến hiệu suất.
- Kết nối có thể không ổn định khi di chuyển, đặc biệt là trong các ứng dụng yêu cầu băng thông cao.
- Yêu cầu quản lý cao để duy trì và theo dõi các thiết bị kết nối và vùng phủ sóng.
- Cần phải tuân thủ các tiêu chuẩn và đảm bảo tương thích giữa các thiết bị để tránh vấn đề không tương thích.
- Thường chấp nhận điều khoản kết nối thấp hơn so với mạng có dây, đặc biệt trong môi trường có nhiều người sử dụng.

1.3 Giới thiệu về công nghệ mạng không dây

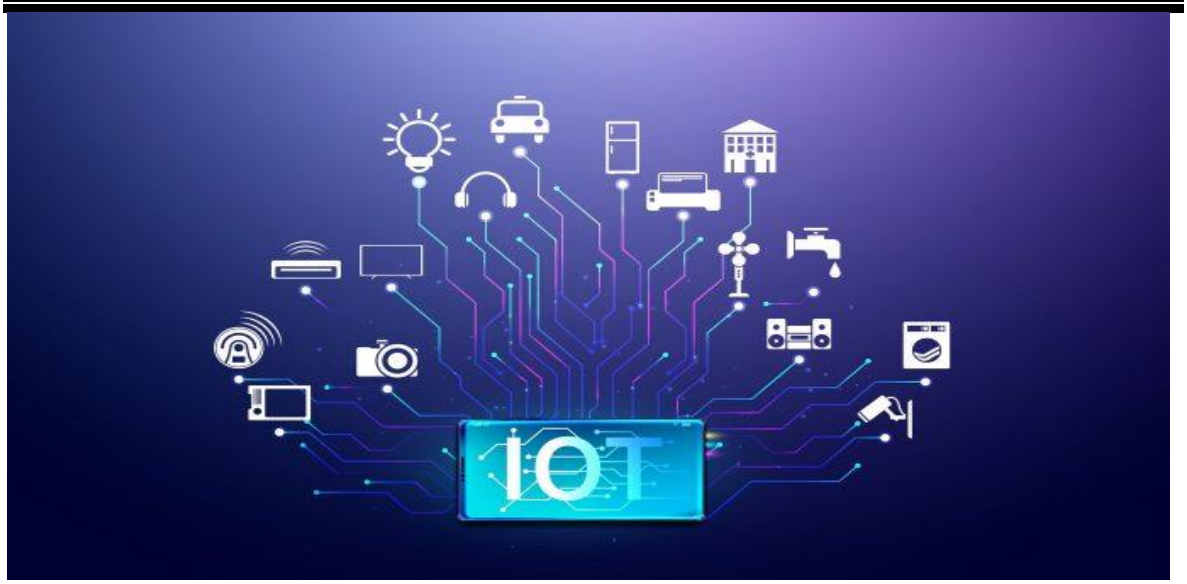
1.3.1 Công nghệ mạng không dây

- Công nghệ không dây là một lĩnh vực quan trọng trong ngành công nghiệp và cuộc sống hàng ngày, đặc biệt là trong thời đại hiện đại. Dưới đây là một số khía cạnh chính của công nghệ không dây:

+ Kết nối Internet không dây (Wi-Fi): Công nghệ Wi-Fi cho phép thiết bị kết nối với internet mà không cần sử dụng dây cáp. Điều này giúp linh hoạt hơn và thuận tiện hơn trong việc truy cập mạng ở nhiều địa điểm.

+ Công nghệ di động (3G, 4G, 5G): Các thế hệ mạng di động không dây giúp truyền tải dữ liệu di động với tốc độ cao và đảm bảo kết nối liên tục trên diện rộng, từ điện thoại di động đến các thiết bị thông minh khác.

+ Mạng cảm biến không dây: Các cảm biến không dây được sử dụng để thu thập dữ liệu từ môi trường xung quanh, từ đo lường chất lượng không khí đến giám sát động đất và nước.



Hình 2. Công nghệ mạng không dây.

1.3.2 CSMA/CA

CSMA/CA là viết tắt của "Carrier Sense Multiple Access with Collision Avoidance," là một phương thức truy cập truyền thông không dây được sử dụng trong mạng không dây để quản lý việc truyền dữ liệu giữa các thiết bị. Nó là một phương pháp cải tiến so với CSMA/CD (Carrier Sense Multiple Access with Collision Detection), mà thường được sử dụng trong mạng có dây.

- Nghe trước: trước khi bắt đầu truyền dữ liệu, thiết bị kiểm tra xem kênh truyền có đang được sử dụng hay không. Nếu kênh đang được sử dụng, thiết bị sẽ đợi để tránh xung đột dữ liệu.

- Tránh xung đột: thay vì phát hiện xung đột sau khi nó đã xảy ra (như trong CSMA/CD), CSMA/CA cố gắng tránh xung đột trước khi chúng xảy ra. Nó sử dụng một quy trình kiểm soát để tránh cho các thiết bị gửi dữ liệu cùng một lúc, giảm khả năng xung đột.

1.3.3 Tiêu chuẩn không dây – 802.11 a/b/g/n

Các tiêu chuẩn không dây 802.11a, 802.11b, 802.11g và 802.11n là các tiêu chuẩn được phát triển bởi IEEE (Institute of Electrical and Electronics Engineers) để đặc tả các chuẩn giao thức truyền thông trong mạng WLAN (Wireless Local Area Network). Mỗi tiêu chuẩn này đều đặc trưng bởi những đặc điểm và tốc độ truyền khác nhau. Dưới đây là mô tả ngắn về mỗi tiêu chuẩn:

- 802.11a: Tiêu chuẩn này hoạt động trong băng tần 5 GHz và sử dụng phương thức modulasi OFDM (Orthogonal Frequency Division Multiplexing). 802.11a cung cấp tốc độ truyền tải dữ liệu tương đối cao và ít bị ảnh hưởng bởi nhiễu từ các thiết bị khác hoạt động trong băng tần 2.4 GHz.
- 802.11b: 802.11b hoạt động trong băng tần 2.4 GHz và sử dụng phương thức modulasi DSSS (Direct Sequence Spread Spectrum). Mặc dù tốc độ truyền tải dữ liệu của 802.11b thấp hơn so với 802.11a, nhưng nó được sử dụng rộng rãi do chi phí thấp và khả năng tương thích với nhiều thiết bị.
- 802.11g: 802.11g cũng hoạt động trong băng tần 2.4 GHz và sử dụng modulasi OFDM. Nó tương thích ngược với 802.11b, nâng cấp tốc độ truyền dữ liệu lên mức cao hơn. 802.11g trở thành một lựa chọn phổ biến khi nó kết hợp tính tương thích của 802.11b với tốc độ cao hơn.

- 802.11n: Tiêu chuẩn này cũng hoạt động trong băng tần 2.4 GHz hoặc 5 GHz và sử dụng nhiều kỹ thuật như MIMO (Multiple Input Multiple Output) và OFDM để cải thiện tốc độ truyền dữ liệu và độ phủ sóng. 802.11n có thể cung cấp tốc độ truyền dữ liệu rất cao và có khả năng tương thích ngược với các tiêu chuẩn trước đó.

1.3.4 Thế hệ mới – 802.11ac

Tiêu chuẩn 802.11ac là một trong những phiên bản mới và tiên tiến của chuẩn truyền thông không dây được phát triển bởi IEEE (Institute of Electrical and Electronics Engineers). Dưới đây là một số đặc điểm chính của 802.11ac:

- Tần số hoạt động: 802.11ac thường hoạt động trong băng tần 5 GHz, khác với 802.11n có thể hoạt động cả ở băng tần 2.4 GHz hoặc 5 GHz. Việc sử dụng băng tần 5 GHz giúp giảm nhiễu và cung cấp một lựa chọn tốt hơn cho môi trường có nhiều thiết bị không dây.
- MIMO (Multiple Input Multiple Output): 802.11ac thường hỗ trợ MIMO, một công nghệ sử dụng nhiều anten để truyền và nhận dữ liệu đồng thời. Điều này cải thiện tốc độ truyền dữ liệu và độ phủ sóng.
- Kênh rộng: 802.11ac hỗ trợ các kênh rộng hơn so với 802.11n, điều này nâng cao khả năng truyền dữ liệu. Thông thường, nó sử dụng kênh rộng 80 MHz hoặc thậm chí 160 MHz.

- Beamforming: Công nghệ này được tích hợp trong 802.11ac để tập trung tín hiệu không dây vào một hướng cụ thể, giúp tăng cường độ phủ sóng và hiệu suất của mạng.

- Tốc độ truyền dữ liệu: 802.11ac có thể cung cấp tốc độ truyền dữ liệu rất cao, thậm chí có thể vượt qua 1 Gbps (gigabit trên giây), tùy thuộc vào cấu hình và điều kiện môi trường.

1.3.5 So sánh 802.11 a/b/g/n và 802.11ac

Dưới đây là một so sánh giữa các tiêu chuẩn không dây trước đây (802.11a, 802.11b, 802.11g, 802.11n) và tiêu chuẩn mới hơn 802.11ac:

	802.11 a/b/g/n	**802.11ac**
Tần số hoạt động	802.11a: 5 GHz. 802.11b/g: 2.4 GHz. 802.11n: Cả 2.4 GHz và 5 GHz.	802.11ac: 5 GHz.
Tốc độ truyền dữ liệu tối đa	802.11a: 54 Mbps. 802.11b: 11 Mbps. 802.11g: 54 Mbps. 802.11n: 600 Mbps (thậm chí có thể lên đến 900 Mbps với MIMO).	802.11ac: Có thể vượt qua 1 Gbps, thậm chí lên đến vài Gbps với MIMO và kênh rộng.
Số kênh và kênh rộng	802.11a: Thường sử dụng kênh rộng 20 MHz. 802.11b/g: Thường sử dụng kênh rộng 20 MHz. 802.11n: Hỗ trợ kênh rộng 20 MHz và 40 MHz, thậm chí có thể sử dụng 80 MHz.	802.11ac: Hỗ trợ kênh rộng 20 MHz, 40 MHz, 80 MHz, và thậm chí 160 MHz.
Beamforming	802.11a/b/g/n: Thường không hỗ trợ hoặc hỗ trợ có hạn.	802.11ac: Hỗ trợ Beamforming, giúp tối ưu hóa hướng của tín hiệu không dây để cải thiện độ phủ sóng và hiệu suất.

Tương thích ngược	802.11a/b/g/n: Tương thích ngược với các tiêu chuẩn trước đó.	802.11ac: Tương thích ngược với 802.11n, nhưng không tương thích ngược hoàn toàn với 802.11a/b/g.
Ứng dụng	802.11a/b/g/n: Thường được sử dụng trong nhiều môi trường khác nhau, từ gia đình đến doanh nghiệp.	802.11ac: Thường được sử dụng trong các môi trường đòi hỏi tốc độ cao như doanh nghiệp, giáo dục, và giải trí gia đình.

Bảng 1. So sánh 802.11 a/b/g/n và 802.11ac.

1.3.6 Hoạt động mạng LAN không dây

1.3.6.1 Wireless 802.11 Frame

Khung (Frame) trong mạng không dây 802.11 là một gói dữ liệu cơ bản, được sử dụng để truyền thông giữa các thiết bị trong mạng. Mỗi khung chứa các trường thông tin cần thiết để quản lý giao tiếp và đảm bảo là dữ liệu được truyền đúng cách. Dưới đây là mô tả của một số trường quan trọng trong một khung 802.11:

- Trường Tiêu đề (Header):

+ Frame Control: Chứa các thông tin quản lý như kiểu khung, trạng thái truyền và kiểm soát xung đột.

+ Duration/ID: Xác định thời gian mà kênh truyền dữ liệu sẽ được giữ (dành cho truyền tải dữ liệu) hoặc ID của trạm đích (dành cho quy trình học giảng).

- Địa chỉ (Address) Điều khiển:

+ Receiver Address (RA): Địa chỉ MAC của trạm đích.

+ Transmitter Address (TA): Địa chỉ MAC của trạm nguồn.

+ Basic Service Set Identifier (BSSID): Địa chỉ MAC của trạm chính trong BSS (Basic Service Set).

- Địa chỉ (Address) Truyền và Đích:

+ Source Address (SA): Địa chỉ MAC của trạm nguồn.

+ Destination Address (DA): Địa chỉ MAC của trạm đích.

+ BSSID: Địa chỉ MAC của trạm chính trong BSS.

- Trường Dữ liệu (Data): Chứa dữ liệu thực sự được truyền qua mạng.

- Trường FCS (Frame Check Sequence): Dùng để kiểm tra lỗi trong dữ liệu và tiêu đề.
- Trường Frame Body: Chứa dữ liệu thực sự cần truyền.
- Trường Frame Trailer: Bao gồm FCS để kiểm tra lỗi.

1.3.6.2 Hoạt động mạng LAN không dây

Hoạt động của mạng không dây (Wireless LAN - WLAN) bao gồm một loạt các quy trình và giao thức để cho phép truyền thông không dây giữa các thiết bị.

CSMA/CA

- CSMA/CA là giao thức mạng được sử dụng trong mạng không dây để tránh xung đột khi nhiều thiết bị cố gắng truyền dữ liệu đồng thời.
- Không giống như mạng có dây sử dụng CSMA/CD (Phát hiện va chạm), mạng không dây sử dụng CSMA/CA để cảm nhận môi trường trước khi truyền để tránh xung đột.

Wireless Clients and Access Point Association

- Máy khách không dây là thiết bị (ví dụ: máy tính xách tay, điện thoại thông minh) kết nối với mạng không dây.
- Điểm truy cập (AP) là các thiết bị hỗ trợ giao tiếp không dây bằng cách kết nối máy khách với mạng có dây.
- Liên kết là quá trình một máy khách không dây kết nối với một điểm truy cập để có quyền truy cập vào mạng.

Association Parameters

Trong quá trình liên kết, một số tham số nhất định sẽ được đàm phán giữa máy khách và điểm truy cập. Các tham số này bao gồm tốc độ dữ liệu, cài đặt bảo mật và các chi tiết cấu hình khác.

Discovering Aps

- Máy khách không dây có thể khám phá các điểm truy cập thông qua một quá trình được gọi là quét.
- Quét tích cực bao gồm việc máy khách gửi yêu cầu thăm dò để khám phá các điểm truy cập có sẵn.
- Quét thụ động liên quan đến việc máy khách lắng nghe các khung báo hiệu được truyền bởi các điểm truy cập gần đó.

Authentication

- Xác thực là quá trình xác minh danh tính của thiết bị hoặc người dùng trước khi cấp quyền truy cập vào mạng.

- Trong mạng không dây, các phương thức xác thực thường được sử dụng bao gồm WPA (Truy cập được bảo vệ Wi-Fi) và WPA2/WPA3, cung cấp mức độ bảo mật cao hơn thông qua mã hóa.

1.3.6.3 Quản lí kênh

Quản lý kênh liên quan đến việc lập kế hoạch, phát triển và kiểm soát các kênh tiếp thị hoặc kênh phân phối thông qua đó sản phẩm hoặc dịch vụ được chuyển từ nhà sản xuất đến người dùng cuối. Nó bao gồm các chiến lược và hoạt động mà một công ty thực hiện để đảm bảo rằng sản phẩm của mình tiếp cận thị trường mục tiêu một cách hiệu quả và hiệu quả.

Độ bão hòa kênh tần số:

- Bão hòa kênh tần số thường đề cập đến tình huống trong đó các kênh tần số sẵn có để liên lạc hoặc phát sóng đã bị chiếm dụng hoặc sử dụng hoàn toàn. Khái niệm này thường gặp trong bối cảnh giao tiếp không dây, chẳng hạn như kênh tần số vô tuyến (RF) hoặc kênh Wi-Fi.

- Ý nghĩa: Trong trường hợp bão hòa kênh tần số, nó có thể dẫn đến nhiễu, giảm chất lượng tín hiệu và suy giảm hiệu suất truyền thông nói chung. Đây là thách thức thường gặp ở những khu vực đông đúc hoặc đông dân cư với nhiều thiết bị điện tử sử dụng cùng phổ tần số.

Chọn kênh:

- Chọn kênh tiếp thị: Điều này liên quan đến việc quyết định các kênh thích hợp nhất mà qua đó sản phẩm hoặc dịch vụ của công ty sẽ được phân phối để tiếp cận khách hàng mục tiêu. Các lựa chọn có thể bao gồm bán hàng trực tiếp, đối tác bán lẻ, nền tảng trực tuyến, nhà phân phối.
- Kênh truyền thông: Theo nghĩa rộng hơn, việc chọn kênh cũng có thể đề cập đến việc chọn kênh truyền thông phù hợp để tiếp thị và quảng bá. Điều này bao gồm việc quyết định có nên sử dụng phương tiện truyền thông xã hội, quảng cáo truyền thống, tiếp thị qua email, dựa trên đối tượng mục tiêu và mục tiêu tiếp thị.

- Kênh tần số: Trong bối cảnh hệ thống truyền thông, việc chọn kênh có thể liên quan đến việc chọn các kênh tần số cụ thể cho liên lạc không dây để giảm thiểu nhiễu và tối ưu hóa hiệu suất.

1.4 Thành phần cơ sở hạ tầng không dây

Mạng cục bộ không dây (WLAN) đề cập đến một loại mạng máy tính cho phép các thiết bị liên lạc và kết nối không dây trong một khu vực địa lý giới hạn, chẳng hạn như nhà riêng, văn phòng hoặc khuôn viên trường. Dưới đây là một số khái niệm cơ bản liên quan đến mạng LAN không dây:

- Phổ tần số vô tuyến (RF):

+ Mạng WLAN hoạt động ở phổ tần số vô tuyến, sử dụng sóng vô tuyến để truyền dữ liệu không dây.

+ Các dải tần 2,4 GHz và 5 GHz thường được sử dụng cho mạng WLAN, dải tần sau cung cấp nhiều kênh hơn và ít nhiễu hơn.

- Điểm truy cập (AP):

+ Điểm truy cập là thiết bị hỗ trợ giao tiếp không dây giữa các thiết bị và mạng có dây.

+ Chúng hoạt động như cầu nối giữa các máy khách không dây và cơ sở hạ tầng mạng có dây.

- Chế độ cơ sở hạ tầng so với Chế độ đặc biệt:

+ Trong chế độ cơ sở hạ tầng, các máy khách không dây giao tiếp thông qua một điểm truy cập, tạo thành BSS.

+ Chế độ đặc biệt cho phép liên lạc trực tiếp giữa các máy khách không dây mà không cần điểm truy cập.

- SSID (Mã định danh bộ dịch vụ): SSID là mã định danh duy nhất cho mạng WLAN. Về cơ bản, nó là tên mạng mà khách hàng sử dụng để kết nối với một mạng không dây cụ thể.

- Bảo mật không dây:

+ Bảo mật là rất quan trọng trong mạng WLAN. Các biện pháp bảo mật phổ biến bao gồm WEP (Quyền riêng tư tương đương không dây), WPA (Truy cập được bảo vệ Wi-Fi) và WPA2/WPA3.

+ Các giao thức mã hóa như WPA2-PSK (Khóa chia sẻ trước) hoặc WPA3 cung cấp khả năng liên lạc an toàn.

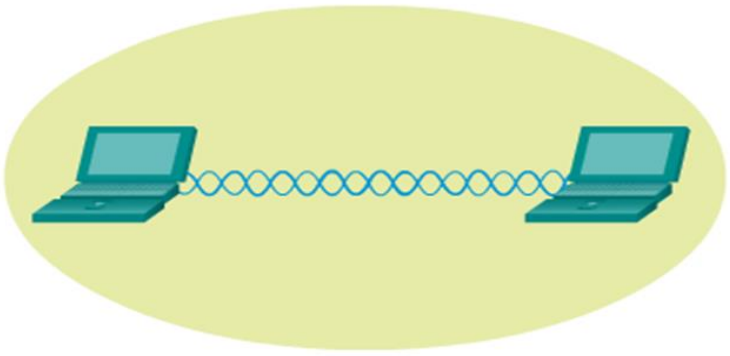
- Tiêu chuẩn không dây: Các tiêu chuẩn như IEEE 802.11 xác định các thông số kỹ thuật cho mạng WLAN. Các tiêu chuẩn phổ biến bao gồm 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac và 802.11ax.

1.4.1 Ad Hoc vs Infrastructure

Ad Hoc vs Infrastructure là hai chế độ liên lạc không dây khác nhau trong mạng cục bộ (LAN). Dưới đây là so sánh chi tiết hơn giữa chế độ Ad Hoc và chế độ Cơ sở hạ tầng:

Ad Hoc Mode:

- Giao tiếp trực tiếp giữa thiết bị với thiết bị: Ở chế độ Ad Hoc, các thiết bị không dây giao tiếp trực tiếp với nhau mà không cần điểm truy cập trung tâm (AP).
- Mạng phi tập trung: Mạng Ad Hoc được phân cấp, nghĩa là không có cơ sở hạ tầng cố định hoặc điểm kiểm soát trung tâm. Các thiết bị tự động thiết lập kết nối với nhau.
- Mạng tạm thời: Mạng Ad Hoc thường được sử dụng để tạo mạng tạm thời một cách nhanh chóng, chẳng hạn như trong các cuộc họp đặc biệt, chia sẻ tệp ngang hàng hoặc phiên chơi trò chơi.
- Khả năng mở rộng hạn chế: Mạng Ad Hoc không có khả năng mở rộng như mạng Cơ sở hạ tầng. Chúng hoạt động tốt cho một số ít thiết bị ở gần nhau.
- Thiết lập đơn giản: Việc thiết lập mạng Ad Hoc thường đơn giản và nhanh hơn vì không cần định cấu hình và quản lý điểm truy cập trung tâm.
- Chuyển vùng hạn chế: Khả năng chuyển vùng bị hạn chế ở chế độ Ad Hoc vì các thiết bị cần thiết lập kết nối trực tiếp với nhau. Việc di chuyển giữa các thiết bị có thể dẫn đến gián đoạn kết nối.

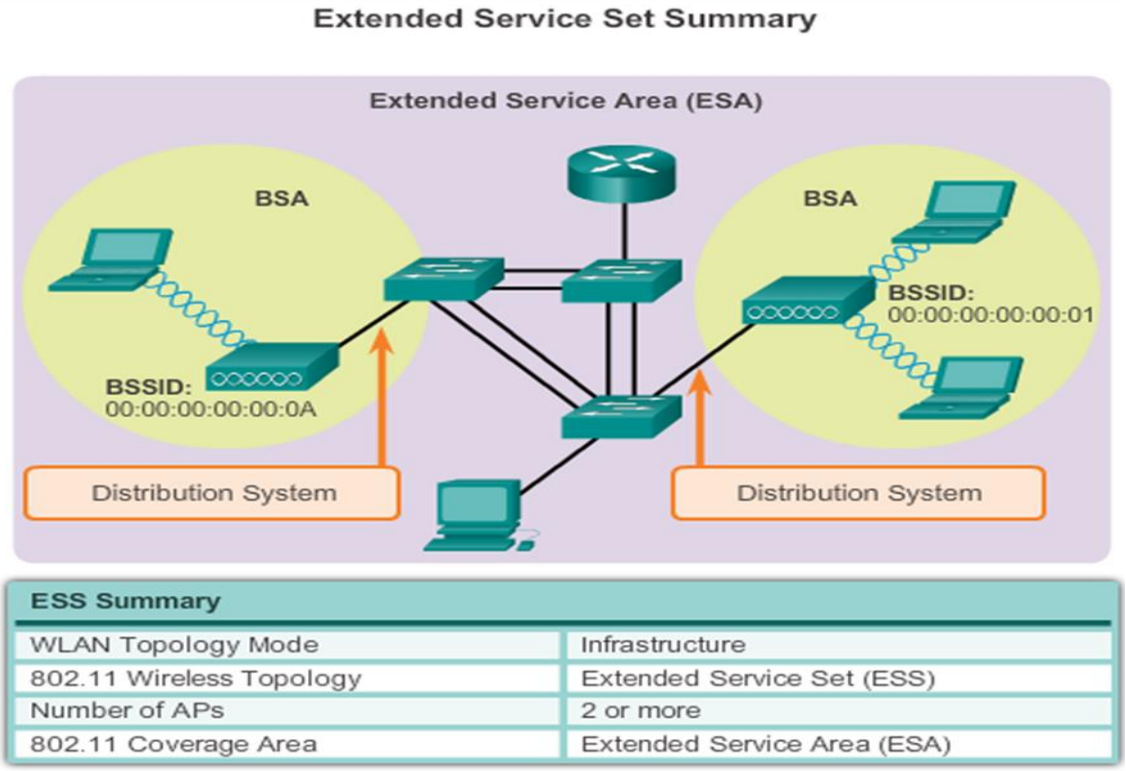


IBSS Summary	
WLAN Topology Mode	Ad Hoc
802.11 Wireless Topology	Independent BSS
Number of APs	None
802.11 Coverage Area	Basic Service Area (BSA)

Hình 3. Ad Hoc.

Infrastructure:

- Điểm truy cập trung tâm (AP): Ở chế độ Cơ sở hạ tầng, các thiết bị không dây giao tiếp thông qua điểm truy cập trung tâm (AP), đóng vai trò là cầu nối giữa máy khách không dây và mạng có dây.
- Mạng tập trung: Mạng cơ sở hạ tầng được tập trung hóa, với AP quản lý và điều phối liên lạc giữa các máy khách không dây. Điều này cung cấp một môi trường mạng có tổ chức và được kiểm soát tốt hơn.
- Mạng cố định: Mạng cơ sở hạ tầng được thiết kế để lắp đặt lâu dài hoặc lâu dài hơn, chẳng hạn như trong nhà, văn phòng hoặc không gian công cộng.
- Khả năng mở rộng: Mạng cơ sở hạ tầng có khả năng mở rộng cao hơn mạng Ad Hoc. Các điểm truy cập bổ sung có thể được triển khai để mở rộng phạm vi phủ sóng và hỗ trợ số lượng lớn hơn các máy khách không dây.
- Chuyển vùng liền mạch: Chế độ cơ sở hạ tầng hỗ trợ chuyển vùng liền mạch giữa các điểm truy cập khác nhau trong cùng một mạng. Điều này đặc biệt quan trọng để duy trì kết nối trong không gian lớn hơn.
- Quản lý mạng: Có thể quản lý mạng tập trung ở chế độ Cơ sở hạ tầng, cho phép quản trị viên giám sát và kiểm soát toàn bộ mạng từ một vị trí trung tâm.



Hình 4. Infrastructure.

1.5 Giới thiệu phần mền Cisco Packet tracer

1.5.1 Tổng quan

Packet Tracer là một phần mềm mô phỏng mạng được phát triển bởi Cisco Systems. Được thiết kế để hỗ trợ người học và chuyên gia mạng trong việc hiểu và thử nghiệm các khái niệm và kỹ thuật mạng, Packet Tracer là một công cụ mô phỏng mạng ảo, giúp người sử dụng tạo, kết nối và kiểm thử các môi trường mạng mà không cần sử dụng thiết bị vật lý thực tế.

Hình 5. Giao diện chính của packet tracer.

1.5.2 Chức năng

- Cho phép người sử dụng tạo, mô phỏng và thử nghiệm các mạng máy tính ảo.
- Cung cấp giao diện đồ họa thân thiện và dễ sử dụng, giúp người dùng tạo và cấu hình mạng một cách trực quan.
- Hỗ trợ nhiều loại thiết bị mạng như router, switch, hub, bridge, firewall, wireless devices, và nhiều thiết bị khác.
- Cho phép người sử dụng thực hiện các lệnh trên giao diện dòng lệnh của các thiết bị mạng.
- Hỗ trợ nhiều chuẩn mạng như Ethernet, Wi-Fi, TCP/IP, IPv6, DHCP, DNS, và nhiều giao thức khác.
- Cho phép người sử dụng tạo và thực hiện các kịch bản thử nghiệm để kiểm tra và hiểu rõ hơn về cách mạng hoạt động.
- Cung cấp khả năng ghi lại và phát lại các hoạt động trong mạng để kiểm tra và đánh giá.

- Được tích hợp trong các chương trình học, giúp sinh viên và học viên học môn học về mạng máy tính và chứng chỉ của Cisco.
- Cung cấp khả năng kết nối với dịch vụ đám mây Cisco, giúp mô phỏng các kịch bản liên quan đến môi trường đám mây.
- Thường được sử dụng để giảng dạy và học môn học về mạng máy tính, đặc biệt là các khóa học và chứng chỉ CCNA của Cisco.
- Cisco cung cấp phiên bản miễn phí của Packet Tracer và cũng có thể sử dụng nó trực tuyến qua Cisco Networking Academy.

Chương 2: NGHIÊN CỨU LÝ THUYẾT

2. Địa chỉ IP

Tổng quan:

IP (Internet Protocol) là một tập hợp các quy tắc để giao tiếp qua internet như gửi mail, phát video trực tuyến hoặc kết nối với một trang web.

Địa chỉ IP cung cấp danh tính của các thiết bị được kết nối mạng, giúp các thiết bị trên mạng Internet phân biệt và nhận ra nhau, từ đó có thể giao tiếp với nhau.

Có hai loại địa chỉ IP: IPv4 và IPv6. Chúng ta có thể phân biệt chúng bằng cách đếm các con số.

Địa chỉ IPv4: chứa một chuỗi bốn số, từ 0 (trừ số đầu tiên) đến 255, mỗi số được phân tách với số tiếp theo bằng dấu chấm. Ví dụ: 5.62.42.77.

Địa chỉ IPv6: biểu thị dưới dạng tám nhóm gồm bốn chữ số thập lục phân, với các nhóm được phân tách bằng dấu hai chấm. Ví dụ: 2620: 0aba2: 0d01: 2042: 0100: 8c4d: d370: 72b4.

Trong phần này, tôi đề cập chủ yếu đến địa chỉ IPv4

Địa chỉ IP là địa chỉ có cấu trúc, được chia làm hai phần: Network id (phần mạng) và host id (phần host). Network id dùng để xác định mạng mà thiết bị kết nối vào, host id để xác định thiết bị của mạng đó.

Địa chỉ IP là một dãy số có kích thước 32 bit được chia làm 4 octet (hoặc byte), mỗi octet gồm 8 bit.

Các khái niệm liên quan

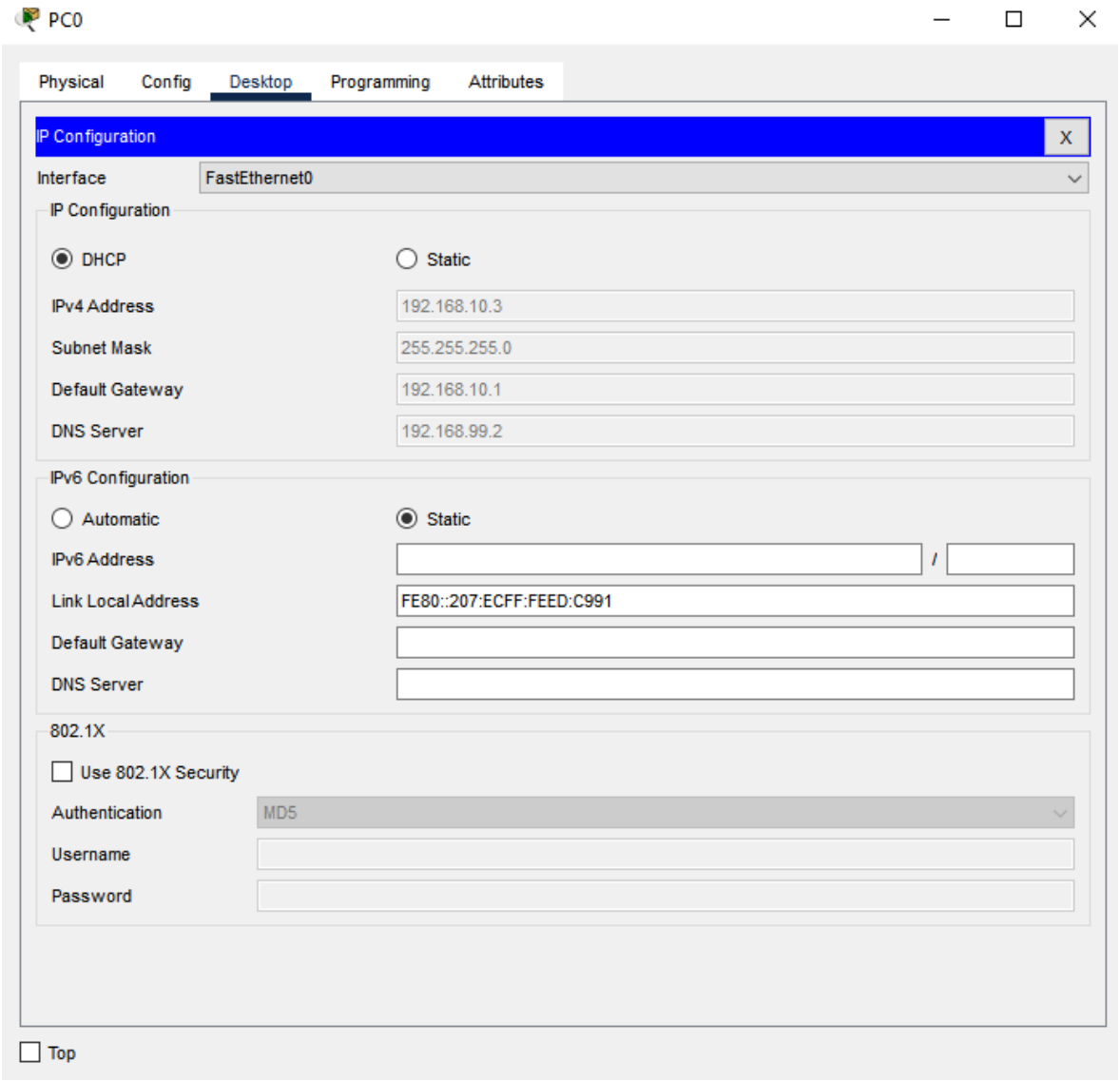
Subnet mask, hay mặt nạ mạng con, là một chuỗi 32 bit tương tự như địa chỉ IP. Nó có đặc điểm là phân chia thành hai vùng, với vùng bên trái chứa toàn bộ bit 1 và vùng bên phải chứa toàn bộ bit 0. Phần của địa chỉ IP tương ứng với vùng bit 1 của subnet mask được gọi là vùng Network của địa chỉ đó. Có ba mặt nạ mạng con chuẩn là 255.0.0.0 dành cho các địa chỉ mạng lớp A, 255.255.0.0 dành cho các địa chỉ mạng lớp B, và 255.255.255.0 dành cho các địa chỉ mạng lớp C.

Mỗi khi gửi một gói tin đến một địa chỉ nào đó, máy tính sẽ xác định đường gửi thông qua một bảng được gọi là bảng định tuyến (routing table). Tuy nhiên, không phải máy tính nào cũng biết đường gửi gói tin đến một địa chỉ IP cụ thể. Do

đó, Default Gateway (hay còn gọi là Gateway) được sử dụng để giải quyết vấn đề này. Nếu không có đường gửi nào đến địa chỉ cần đến trong bảng định tuyến, máy tính sẽ gửi gói tin đó qua gateway. Nhiệm vụ của gateway thường là chuyển tiếp gói tin đến nơi đích cần đến.

Đặt địa chỉ IP cho máy ảo

Khi sử dụng phần mềm Packet trace, ta phải cấu hình router để cấp địa chỉ ip cho các PC, cấu hình định tuyến động cho chúng để chúng có thể kết nối được với nhau.



Hình 6. Đặt địa chỉ IP cho máy ảo.

2.1 Bộ định tuyến (Router)

2.1.1 Khái niệm Router

Router (Bộ định tuyến) là một thiết bị mạng chịu trách nhiệm định tuyến dữ liệu giữa các mạng khác nhau. Chức năng cơ bản của router là chuyển tiếp gói tin từ một địa chỉ mạng nguồn đến địa chỉ mạng đích thông qua các đường giao tiếp mạng khác nhau. Điều này giúp kết nối và quản lý giao tiếp giữa các mạng khác nhau, đảm bảo rằng dữ liệu được chuyển đến đúng đích một cách hiệu quả.

Định tuyến (Router) là thiết bị mạng chịu trách nhiệm kết nối và chuyển tiếp dữ liệu giữa các mạng khác nhau. Chức năng chính của router là định tuyến gói tin từ một mạng nguồn đến một mạng đích thông qua các giao diện mạng khác nhau. Điều này giúp mạng hoạt động hiệu quả bằng cách định tuyến dữ liệu và quản lý giao tiếp giữa các mạng khác nhau.

Định tuyến giúp hoạt động giao tiếp mạng diễn ra hiệu quả. Lỗi giao tiếp mạng khiến người dùng chờ lâu để tải trang web. Lỗi giao tiếp mạng cũng có thể khiến máy chủ trang web bị sập vì không thể xử lý số lượng người dùng lớn. Định tuyến giúp giảm thiểu lỗi mạng bằng cách quản lý lưu lượng truy cập dữ liệu để mạng có thể phát huy tối đa khả năng của mình mà không gây ra tình trạng tắc nghẽn.

Có hai loại định tuyến là định tuyến tĩnh và định tuyến động.

- Định tuyến tĩnh là quá trình xác định lộ trình chuyển tiếp gói tin đến mạng đích dựa trên hiểu biết của người quản trị về mạng hiện thời.

- Định tuyến động là một phương pháp tự động trong việc chia sẻ thông tin định tuyến giữa các router. Trong quá trình này, router sẽ tự động chuyển động thông tin định tuyến của mình (có thể là toàn bộ bảng định tuyến hoặc một số route trong bảng định tuyến) cho các router láng giềng (neighbor), giúp router tự động xác định đường đi tối ưu nhất đến một mạng đích.

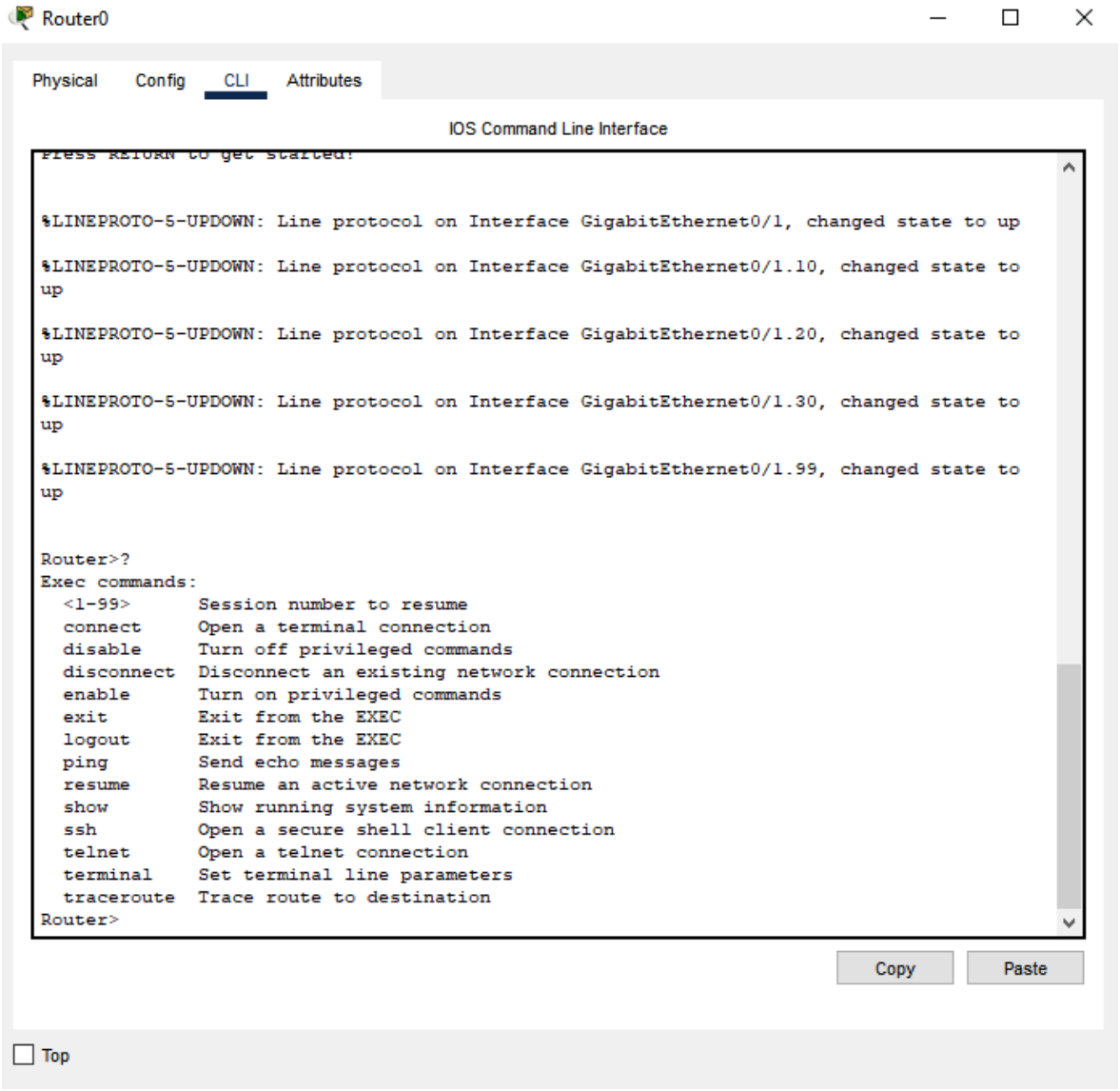
- Mô hình định tuyến động thường sử dụng các giao thức định tuyến động như RIP (Routing Information Protocol), OSPF (Open Shortest Path First), hoặc EIGRP (Enhanced Interior Gateway Routing Protocol). Các giao thức này giúp router không chỉ biết về các mạng trực tiếp kết nối mà nó quản lý, mà còn biết được về các mạng thông qua các router láng giềng. Để thực hiện được điều đó định tuyến động sẽ sử dụng các giao thực định tuyến như: RIP, OSPF, EIGRP, …

	Định tuyến tĩnh	Định tuyến động
Lựa chọn đường đi	Sử dụng một tuyến đường được cấu hình sẵn.	Cung cấp nhiều tuyến đường khả dụng đến đích.
Khả năng cập nhật lộ trình	Quản trị viên mạng phải cầu hình lại các tuyến tĩnh theo cách thủ công để điều chỉnh các tuyến.	Định tuyến động sử dụng các thuật toán đề tự động cập nhật với sự thay đổi tuyến đường ưu tiên.
Sử dụng giao thức và thuật toán	Định tuyên tĩnh không sử dụng các giao thức hoặc thuật toán định tuyến phức tạp.	Định tuyến động sử dụng các giao thức vectơ khoảng cách, chẳng hạn như RIP và IGRP, và các giao thức trạng thái liên kết, chăng hạn như OSPF và IS-IS, đề điều chỉnh các tuyến đường.
Yêu cầu về tính toán và băng thông	Yêu cầu ít năng lượng tính toán và băng thông hơn vì nó chỉ có một tuyến đường được cấu hình sẵn.	Yêu cầu nhiều tính toán và băng thông hơn để tạo ra nhiều khả năng định tuyến.
Bảo mật	Bảo mật tốt hơn do không chia sẻ các tuyến trên toàn bộ mạng.	Tạo ra nhiều rủi ro bảo mật hơn vì nó chia sẻ các bảng định tuyến hoàn chỉnh trên toàn mạng.
Trường hợp sử dụng	Sử dụng tốt nhất trong các mạng nhỏ hơn với ít bộ định tuyển hơn và lý tưởng cho các mạng có kiến trúc mạng không thay đổi.	Phù hợp với các mạng lớn hơn, phức tạp hơn có nhiều bộ định tuyển và tính linh hoạt của nó làm cho nó trở nên lý tưởng cho các kiến trúc mạng thường xuyên thay đổi.

Bảng 2. So sánh định tuyến tĩnh và động.

2.1.2 Các chế độ cấu hình router

Phím trợ giúp (?): Khi chúng ta gõ chấm hỏi khi đang cấu hình router thì giao diện console sẽ hiển thị một loạt danh sách các lệnh tương ứng với chế độ cấu hình.



Hình 7. Xem các lệnh khả dụng.

Khi cấu hình router, router có lưu lại một số các lệnh chúng ta đã sử dụng. Điều này đặc biệt có ích khi chúng ta muốn lặp lại các câu lệnh dài và phức tạp. Mặc định là router sẽ lưu lại 10 câu lệnh trong bộ đệm. Chúng ta có thể thay đổi số lượng câu lệnh mà router lưu lại bằng lệnh terminal history size hoặc historysize. Tối đa là 255 câu lệnh có thể lưu lại được.

Nếu chúng ta muốn gọi lại câu lệnh vừa mới sử dụng gần nhất thì chúng ta nhấn Ctrl-P hoặc phím mũi tên (↑). Nếu chúng ta tiếp tục nhấn thì mỗi lần nhấn như

vậy chúng ta sẽ gọi lại tuần tự các câu lệnh trước đó nữa. Nếu chúng ta muốn gọi lui lạ một câu lệnh sau đó thì chúng ta nhấn Ctrl-N hoặc nhấn phím mũi tên (↓). Tương tự, nếu chúng ta tiếp tục nhấn như vậy thì mỗi lần nhấn chúng ta sẽ gọi lại một lệnh đó.

Khi gõ lệnh, chúng ta chỉ cần gõ các ký tự đủ để router phân biệt với mọi câu kệnh khác rồi nhấn phím Tab thì router sẽ tự động hoàn tất câu lệnh cho chúng ta. Khi chúng ta dùng phím Tab mà router hiển thị được đủ câu lệnh thì có nghĩa là router đã nhận biết được câu lệnh mà chúng ta muốn nhập.

Ngoài ra, hầu hết các router đều có thêm chức năng cho chúng ta đánh dấu khối và copy. Nhờ đó chúng ta có thể copy câu lệnh trước đó rồi dán hoặc chèn vào câu lệnh hiện tại.

Một số câu lệnh còn có thể viết tắt để thuận tiện cho việc cấu hình.
Ví dụ: lệnh enable có thể viết tắt là en, configure terminal có thể viết tắt là conf t,…

2.1.3 Các chế độ cấu hình Router

Chế độ (mode)	**Cách thức truy nhập**	**Dấu nhắc**	**Cách thức thoát**
User EXEC	Login	Router>	Logout command
Privileged EXEC	Từ User EXEC mode, sử dụng lệnh enable	Router#	Để trở về User EXEC mode, dùng lệnh disable. Để vào global configuration mode, dùng lệnh configure terminal
Global configuration (Cấu hình toàn cục)	Từ Privileged EXEC mode, dùng lệnh configure terminal	Router(configure)#	Để ra privileged EXEC mode, dùng lệnh exit hay end hay gõ Ctrl + Z. Để vào interface configuration mode, gõ lệnh interface.

Interface configuration	Từ global configuration mode, gõ lệnh interface.	Router(configure-if)#	Để ra global configuration mode, dùng lệnh exit. Để ra privileged EXEC mode, dùng lệnh exit hay Ctrl+Z. Để vào subinterface configuration mode, xác định subinterface bằng lệnh interface.
Subinterface configuration	Từ interface configuration mode, xác định subinterface bằng lệnh interface	Router(config-subif)#	Để ra global configuration mode, dùng lệnh exit. Để vào privileged EXEC mode, dùng lệnh end hoặc dùng Ctrl + Z.

Bảng 3. Các chế độ cấu hình Router.

2.1.4 Lỗi và cách khắc phục:

Khi chúng ta gõ một câu lệnh bị sai thì chúng ta sẽ gặp dấu báo lỗi (^). Dấu báo lỗi (^) đặt ở vị trí mà câu lệnh bắt đầu bị sai. Dựa vào đó và vận dụng chức năng trợ giúp của hệ thống chúng ta sẽ tìm ra và chỉnh sửa lại lỗi cú pháp của câu lệnh.

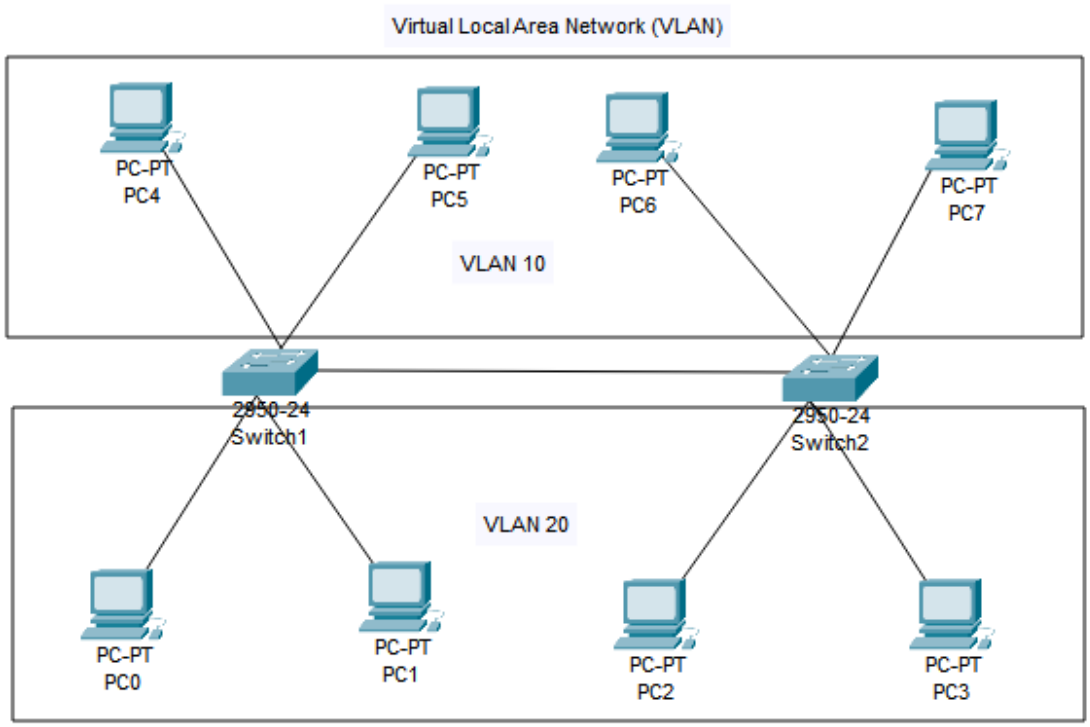
```
Router(config-subif)#ex
Router(config)#ip add 192.168.99.1 255.255.255.0
^
% Invalid input detected at '^' marker.
Router(config)#int g0/1.99
Router(config-subif)#ip add 192.168.99.1 255.255.255.0
Router(config-subif)#ex
```

Khi chúng ta gõ nhầm lệnh hoặc thiếu lệnh thì hệ thống sẽ báo lỗi ngay phần lệnh bị sai, chúng ta chỉ cần sửa câu lệnh cho đúng cú pháp thì sẽ khắc phục được. Nếu không khắc phục được thì chúng ta có thể đã và sai chế độ cấu hình.

2.2 Cấu hình VLAN (Virtual Local Area Network)

2.2.1 Khái niệm VLAN

VLAN (Virtual Local Area Network) là một khái niệm trong lĩnh vực mạng máy tính, được thiết kế để chia nhỏ một mạng vật lý thành nhiều mạng ảo độc lập nhau. Điều này giúp cải thiện quản lý và an toàn trong mạng, đồng thời giảm tải cho các thiết bị chuyển mạch (switch) và tăng tính linh hoạt.



Hình 8. Sơ đồ Virtual Local Area Network.

2.2.2 Phân loại VLAN

Port - based VLAN

Là một phương pháp trong việc triển khai và quản lý các VLAN trên một switch mạng. Trong hệ thống này, các cổng trên switch được gán vào các VLAN dựa trên số cổng của chúng. Điều này có nghĩa là mỗi cổng trên switch sẽ thuộc về một VLAN cụ thể, và các thiết bị kết nối vào cổng đó sẽ thuộc về VLAN đó.

MAC address based VLAN

Là một phương pháp quản lý và phân chia VLAN dựa trên địa chỉ MAC (Media Access Control) của các thiết bị mạng. Trong hệ thống này, mỗi thiết bị được gán vào một VLAN cụ thể dựa trên địa chỉ MAC duy nhất của nó. Điều này tạo ra một cách linh hoạt để quản lý VLAN, nơi mà thiết bị có thể chuyển giữa các VLAN mà không cần thay đổi cấu hình trên switch.

Protocol - based VLAN

Là một phương pháp phân chia và quản lý VLAN dựa trên loại giao thức được sử dụng bởi các gói dữ liệu trong mạng. Trong mô hình này, các VLAN được xác định và phân biệt dựa trên loại giao thức (ví dụ: IP, IPX, ARP) của các gói dữ liệu thay vì chỉ dựa trên cổng hoặc địa chỉ MAC.

2.2.3 Ưu điểm và nhược điểm của VLAN

Mạng VLAN có những ưu điểm và nhược điểm riêng mà bạn cần cân nhắc trước khi lựa chọn sử dụng.

Ưu điểm của VLAN

- VLAN giúp cô lập quyền truy cập giữa các phần khác nhau của mạng, giảm khả năng truy cập từ các thiết bị không ủy quyền.
- Áp dụng biện pháp an ninh và kiểm soát truy cập tinh vi bằng cách giới hạn giao tiếp giữa các VLAN, giảm nguy cơ bị tấn công mạng.
- Có thể phân loại mạng thành các đơn vị nhỏ hơn để dễ quản lý hơn, giúp quản trị viên tối ưu hóa cấu hình và theo dõi từng VLAN một cách dễ dàng.
- Dễ Dàng Thêm, Sửa Đổi, Xóa: Thêm, sửa đổi hoặc xóa VLAN có thể được thực hiện mà không ảnh hưởng đến các phần khác của mạng.
- Có thể kiểm soát và quản lý lưu lượng mạng bằng cách chia mạng thành các VLAN dựa trên yêu cầu cụ thể.
- Ngăn chặn đụng độ và tối ưu hóa hiệu suất bằng cách chia mạng thành các đơn vị nhỏ hơn.
- Dễ dàng phân loại và xử lý các gói dữ liệu dựa trên loại giao thức.
- Kiểm soát và quản lý băng thông mạng một cách hiệu quả thông qua việc cấu hình VLAN tương ứng với yêu cầu băng thông cụ thể.

Nhược điểm của VLAN

- Việc triển khai và quản lý VLAN yêu cầu kiến thức kỹ thuật cao, đặc biệt là trong việc cấu hình và duy trì các cài đặt phức tạp.
- Nếu cấu hình không đúng, có thể có nguy cơ thông tin lộ lạc giữa các VLAN, đặc biệt là khi không thực hiện chặt chẽ quản lý quyền truy cập.
- Nếu không quản lý địa chỉ IP một cách cẩn thận, có thể xảy ra đụng độ địa chỉ IP giữa các VLAN khác nhau.
- Để triển khai VLAN, switch cần hỗ trợ công nghệ VLAN. Những switch giá rẻ hoặc thiết bị cũ có thể không hỗ trợ đầy đủ chức năng VLAN.
- Nếu không cấu hình STP (Spanning Tree Protocol) một cách đúng đắn, có thể xảy ra loop mạng khi sử dụng VLAN.
- Thiết bị mạng có khả năng hỗ trợ VLAN thường có chi phí cao hơn so với các thiết bị không hỗ trợ.
- Trong môi trường VLAN, quản lý băng thông có thể trở nên phức tạp và hạn chế nếu không được cấu hình đúng.
- Mặc dù VLAN có thể hỗ trợ môi trường mạng động, nhưng cũng có thể gặp hạn chế trong việc mở rộng cho các mô hình mạng lớn và phức tạp.

2.2.4 Ứng dụng và lợi ích của VLAN

VLAN ngày càng trở nên phổ biến và được ứng dụng rộng rãi, bởi một số lợi ích tuyệt vời mà nó mang lại:

Ứng Dụng của VLAN:

- Phân vùng mạng theo từng đơn vị chức năng, phòng ban hoặc ứng dụng cụ thể.
- Tạo VLAN đặc biệt cho các dịch vụ này để ưu tiên và quản lý hiệu suất.
- Sử dụng VLAN để giới hạn lưu lượng mạng và ưu tiên băng thông cho các ứng dụng quan trọng.
- Ngăn chặn truy cập không ủy quyền giữa các phòng ban, nhóm làm việc hoặc thiết bị.
- Tạo VLAN dựa trên ngôn ngữ để tối ưu hóa giao tiếp cho người sử dụng ngôn ngữ cụ thể.

Lợi ích của VLAN:

- Tăng cường an ninh thông qua cô lập các phần của mạng và kiểm soát quyền truy cập.
- Quản lý và kiểm soát lưu lượng mạng để tối ưu hóa hiệu suất.
- Phân loại mạng thành các đơn vị quản lý dễ dàng và hỗ trợ mở rộng mạng một cách linh hoạt.
- Có thể phục hồi nhanh chóng sau sự cố hoặc thay đổi trong mạng.
- Hỗ trợ dịch vụ đa phương tiện như video, âm thanh và dữ liệu trên cùng một mạng.
- Ngăn chặn phổ cập địa chỉ IP và giảm nguy cơ đụng độ địa chỉ.
- Cấu hình và quản lý dễ dàng trên các switch và router hỗ trợ VLAN.

Chương 3: HIỆN THỰC HÓA NGHIÊN CỨU

3.1 Mô hình mạng

Mô hình mạng được sử dụng trong một môi trường văn phòng nhỏ. Mạng bao gồm các máy tính trạm và máy chủ (server). Các máy tính trạm bao gồm các máy tính cá nhân (PC), máy tính xách tay (laptop) và điện thoại thông minh (smartphone). Các máy tính trạm được kết nối với nhau thông qua một bộ định tuyến không dây (wireless router). Bộ định tuyến không dây cung cấp kết nối Internet cho các máy tính trạm và cho phép chúng chia sẻ tài nguyên với nhau, chẳng hạn như file, máy in và máy quét.

Các máy chủ bao gồm máy chủ web, máy chủ DNS và máy chủ lưu trữ file. Các máy chủ được kết nối với nhau thông qua một bộ định tuyến. Bộ định tuyến cung cấp kết nối Internet cho các máy chủ và cho phép chúng giao tiếp với nhau.

Mạng được chia thành ba VLAN (Virtual Local Area Network). VLAN là một cách để chia một mạng LAN thành nhiều mạng ảo. Điều này có thể được thực hiện để tăng bảo mật, cải thiện hiệu suất hoặc để phân tách các nhóm người dùng.

VLAN 20 bao gồm các máy tính trạm của nhân viên văn phòng. VLAN 99 bao gồm các máy chủ web và máy chủ DNS. VLAN 10 bao gồm các máy chủ lưu trữ file. Mạng được kết nối với Internet thông qua một modem cáp. Modem cáp cung cấp kết nối Internet cho toàn bộ mạng.

+ Vị trí: Mạng được đặt trong một văn phòng nhỏ ở thành phố Trà Vinh, Việt Nam.

+ Kích thước: Mạng bao gồm khoảng 20 máy tính.

+ Chức năng: Mạng được sử dụng cho các mục đích kinh doanh, bao gồm email, web, in ấn và lưu trữ file.

+ An ninh: Mạng được bảo vệ bằng tường lửa và mã hóa.

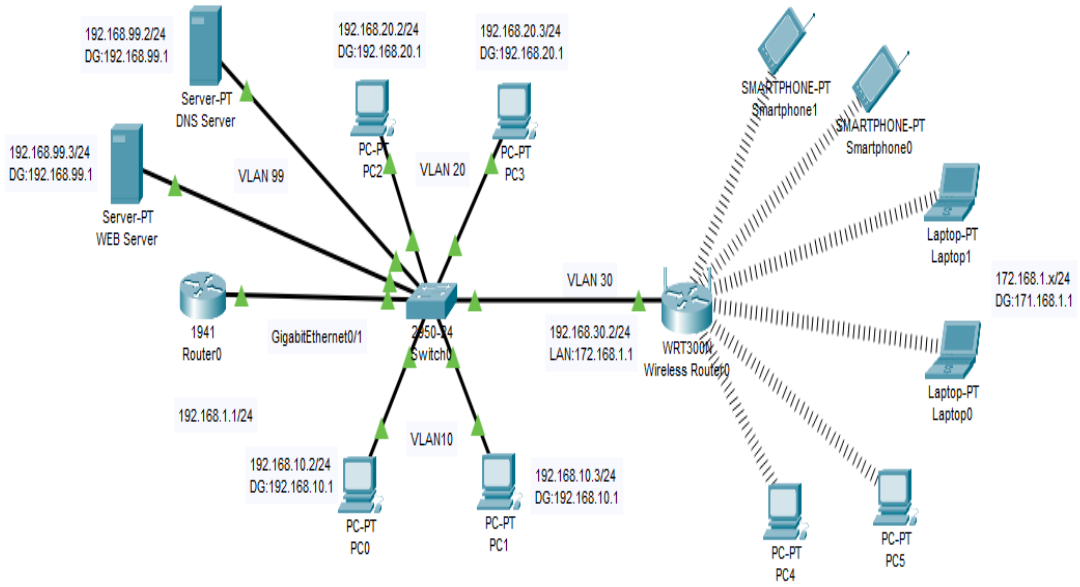
- Một số chi tiết bổ sung về môi trường hoạt động của mạng:

+ Các máy tính trạm được sử dụng cho các tác vụ như email, duyệt web, xử lý văn bản và bảng tính.

+ Các máy chủ web được sử dụng để lưu trữ và cung cấp các trang web cho công ty.

+ Các máy chủ DNS được sử dụng để phân giải tên miền thành địa chỉ IP.

+ Các máy chủ lưu trữ file được sử dụng để lưu trữ các file quan trọng của công ty.



Hình 9. Mô hình mạng.

Addressing Table

Device	Interface	Ip Address	Subnet Mask	Default Gateway
Router	g0/1 g0/1.10 g0/1.20 g0/1.30 g0/1.99	192.168.1.1 192.168.10.1 192.168.20.1 192.168.30.1 192.168.99.1	255.255.255.0	N/A N/A N/A N/A
Switch	VLAN10 VLAN20 VLAN30 VLAN99	192.168.10.0 192.168.20.0 192.168.30.0 192.168.99.0	255.255.255.0	192.168.10.1 192.168.20.1 192.168.30.1 192.168.99.1
PC0/ PC1	NC	192.168.10.2/3	255.255.255.0	192.168.10.1
PC2/ PC3	NC	192.168.20.2/3	255.255.255.0	192.168.20.1
Wireless Router	NC	192.168.30.2	255.255.255.0	192.168.30.1
DNS Server	NC	192.168.99.2	255.255.255.0	192.168.99.1
WEB Server	NC	192.168.99.3	255.255.255.0	192.168.99.1

Bảng 4. Addressing Table.

VLAN Table

VLAN	Name	Interface Assigned
10	VLAN10	fa0/2, fa0/3
20	VLAN20	fa0/4, fa0/5
30	VLAN30	fa0/6
99	VLAN99	fa0/7, fa0/8

Bảng 5. VLAN Table.

3.2 Quá trình thực hiện

3.2.1 Cấu hình VLAN trên Switch

Các câu lệnh trong quá trình thực hiện :

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#int fa0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#int fa0/4
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa0/5
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config)#vlan 30
```

```
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#int fa0/6
Switch(config-if)#switchport access vlan 30
Switch(config-if)#ex
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN99
Switch(config-vlan)#int fa0/7
Switch(config-if)#switchport access vlan 99
Switch(config-if)#int fa0/8
Switch(config-if)#switchport access vlan 99
Switch(config-if)#ex
```

Sao khi hoàn thành quá trình cấu hình vlan chúng ta có thể kiểm ra thử xem coi các cổng có cấu hình đúng vlan chưa bằng lệnh show vlan.

```
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- ---
1    default                          active
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   VLAN10                           active    Fa0/2,a0/3
20   VLAN20                           active    Fa0/4,Fa0/5
30   VLAN30                           active    Fa0/6
99   VLAN99                           active    Fa0/7,Fa0/8
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Sao khi show vlan ta thấy các cổng fa0/2 fa0/3 thuộc VLAN 10, cổng fa0/4 fa0.5 thuộc VLAN 20, cổng fa0/6 thuộc VLAN 30, các cổng fa0/7 fa0/8 thuộc

VLAN 99. Kế tiếp cấu hình đường trunk cho VLAN để chuyển giao dữ liệu từ nhiều VLAN khác nhau qua cùng một kết nối vật lý.

```
Switch#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1,  changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1,  changed state to up
```

Để xem cấu hình thành công hay chưa ta dùng lệnh show int trunk:

```
Switch#show int trunk
Port        Mode         Encapsulation  Status
Native vlan
Fa0/1       on           802.1q       trunking1
Port        Vlans allowed on trunk
Fa0/1       1-1005
Port       Vlans allowed and active in management domain
Fa0/1       1,10,20,30,99
Port     Vlans in spanning tree forwarding state
and not pruned
Fa0/1       1,10,20,30,99
```

3.2.2 Định tuyến Router

Các câu lệnh định tuyến cho router trong quá trình thực hiện:

```
Router(config-if)#ex
Router(config)#int g0/1.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.10,
changed state to up
```

```
     %LINEPROTO-5-UPDOWN: Line protocol on Interface
     GigabitEthernet0/1.10, changed state to up
     Router(config-subif)#encapsulation dot1Q 10
     Router(config-subif)#ex
     Router(config)#int g0/1.10
     Router(config-subif)#ip add 192.168.10.1
255.255.255.0
     Router(config-subif)#ex
     Router(config)#int g0/1.20
     Router(config-subif)#
     %LINK-5-CHANGED: Interface GigabitEthernet0/1.20,
changed state to up
     %LINEPROTO-5-UPDOWN: Line protocol on Interface
     GigabitEthernet0/1.20, changed state to up
     Router(config-subif)#encapsulation dot1Q 20
     Router(config-subif)#ex
     Router(config)#int g0/1.20
     Router(config-subif)#ip add 192.168.20.1
255.255.255.0
     Router(config-subif)#ex
     Router(config)#int g0/1.30
     Router(config-subif)#
     %LINK-5-CHANGED: Interface GigabitEthernet0/1.30,
changed state to up
     %LINEPROTO-5-UPDOWN: Line protocol on Interface
     GigabitEthernet0/1.30, changed state to up
     Router(config-subif)#encapsulation dot1Q 30
     Router(config-subif)#ex
     Router(config)#int g0/1.30
     Router(config-subif)#ip add 192.168.30.1
255.255.255.0
     Router(config-subif)#ex
```

```
Router(config)#int g0/1.99
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.99, changed state to up
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ex
Router(config)#int g0/1.99
Router(config-subif)#ip add 192.168.99.1
255.255.255.0
Router(config-subif)#ex
```

Để kiểm tra xem quá trình đóng gói các vlan và phân chia mạng vật lý thành nhiều mạng ảo ta dùng lệnh show ip int brief.

```
Router#show ip int brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset
administratively down down
GigabitEthernet0/1 192.168.1.1 YES manual up up
GigabitEthernet0/1.10 192.168.10.1 YES manual up up
GigabitEthernet0/1.20 192.168.20.1 YES manual up up
GigabitEthernet0/1.30 192.168.30.1 YES manual up up
GigabitEthernet0/1.99 192.168.99.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
```

Chúng ta cấu hình dhcp cho các vlan :

```
Router#configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#service dhcp
Router(config)#ip dhcp pool VLAN10
Router(dhcp-config)#network 192.168.10.0
255.255.255.0
```

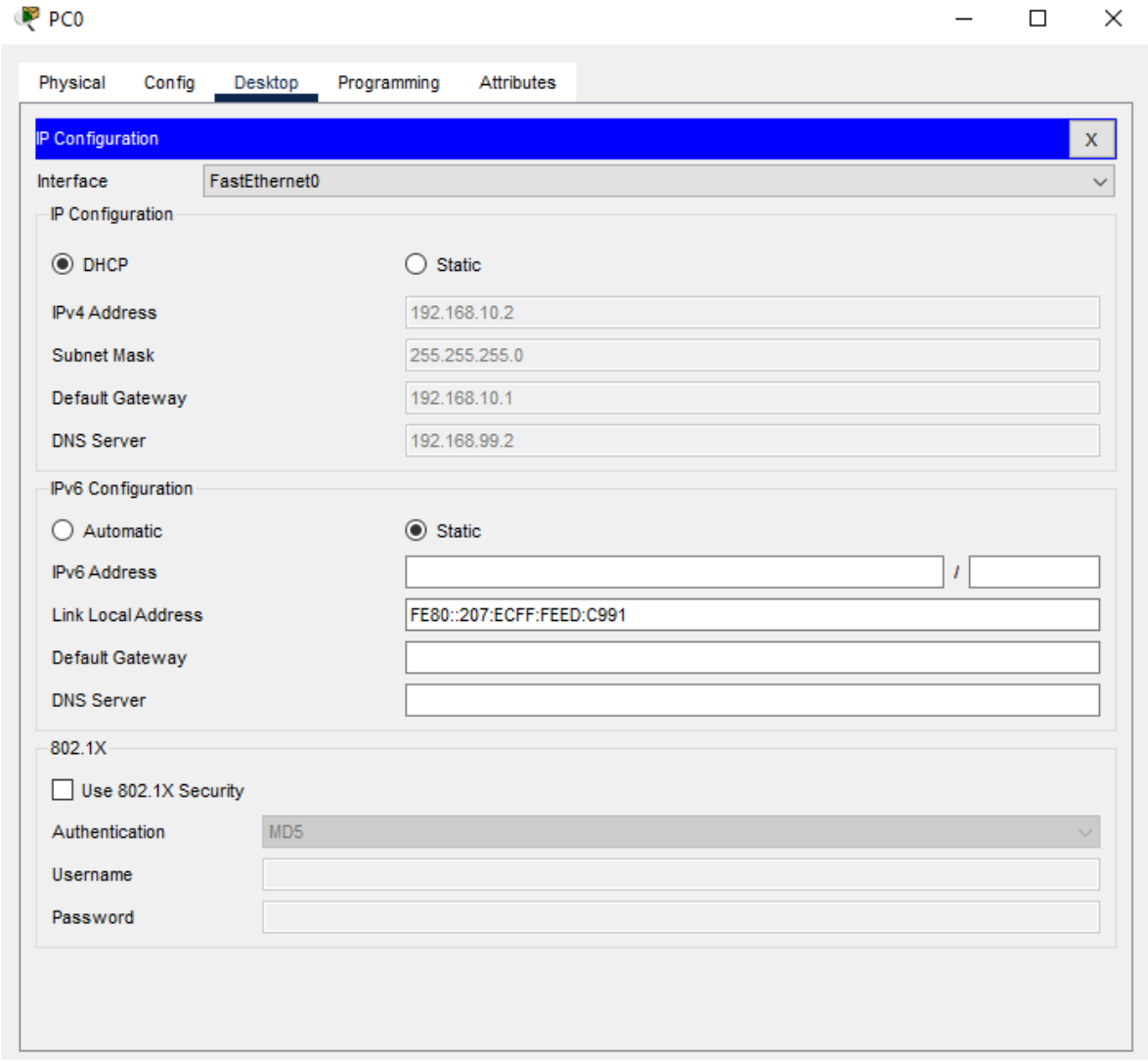
```
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool VLAN20
Router(dhcp-config)#network 192.168.20.0
255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool VLAN30
Router(dhcp-config)#network 192.168.30.0
255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool VLAN99
Router(dhcp-config)#network 192.168.99.0
255.255.255.0
Router(dhcp-config)#default-router 192.168.99.1
Router(dhcp-config)#ex
Router(config)#
```

Cấu hình DNS-Server

```
Router>en
Router#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#ip dhcp pool VLAN10
Router(dhcp-config)#dns-server 192.168.99.2
Router(dhcp-config)#ex
Router(config)#ip dhcp pool VLAN20
Router(dhcp-config)#dns-server 192.168.99.2
Router(dhcp-config)#ex
Router(config)#ip dhcp pool VLAN30
Router(dhcp-config)#dns-server 192.168.99.2
Router(dhcp-config)#ex
```

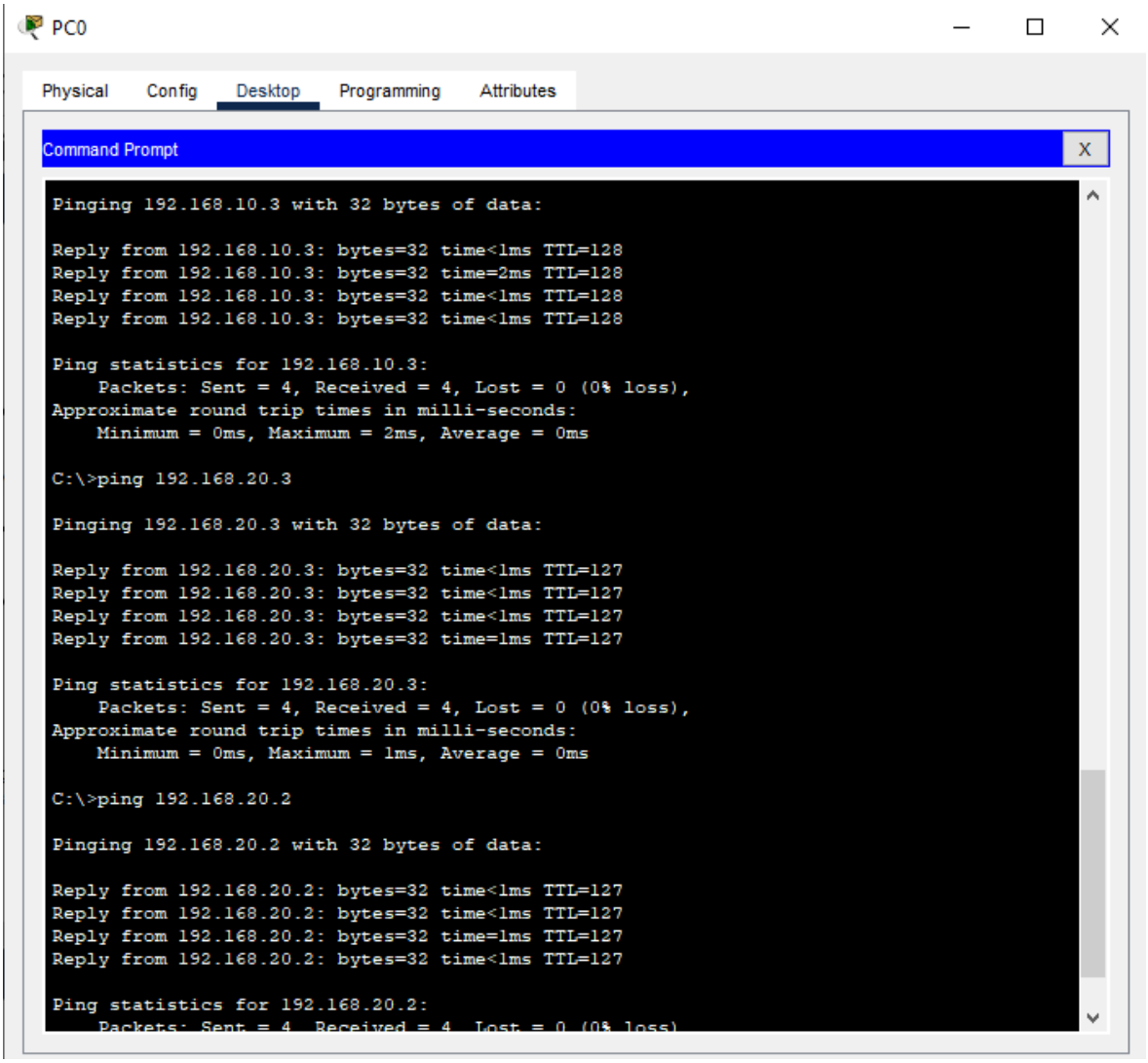
```
Router(config)#ip dhcp pool VLAN99
Router(dhcp-config)#dns-server 192.168.99.2
Router(dhcp-config)#ex
```

Thực hiện cấp địa chỉ ip dhcp cho các PC, Wireless Router, DNS Server, WEB Server.



Hình 10. Quá trình cấp địa chỉ ip cho PC.

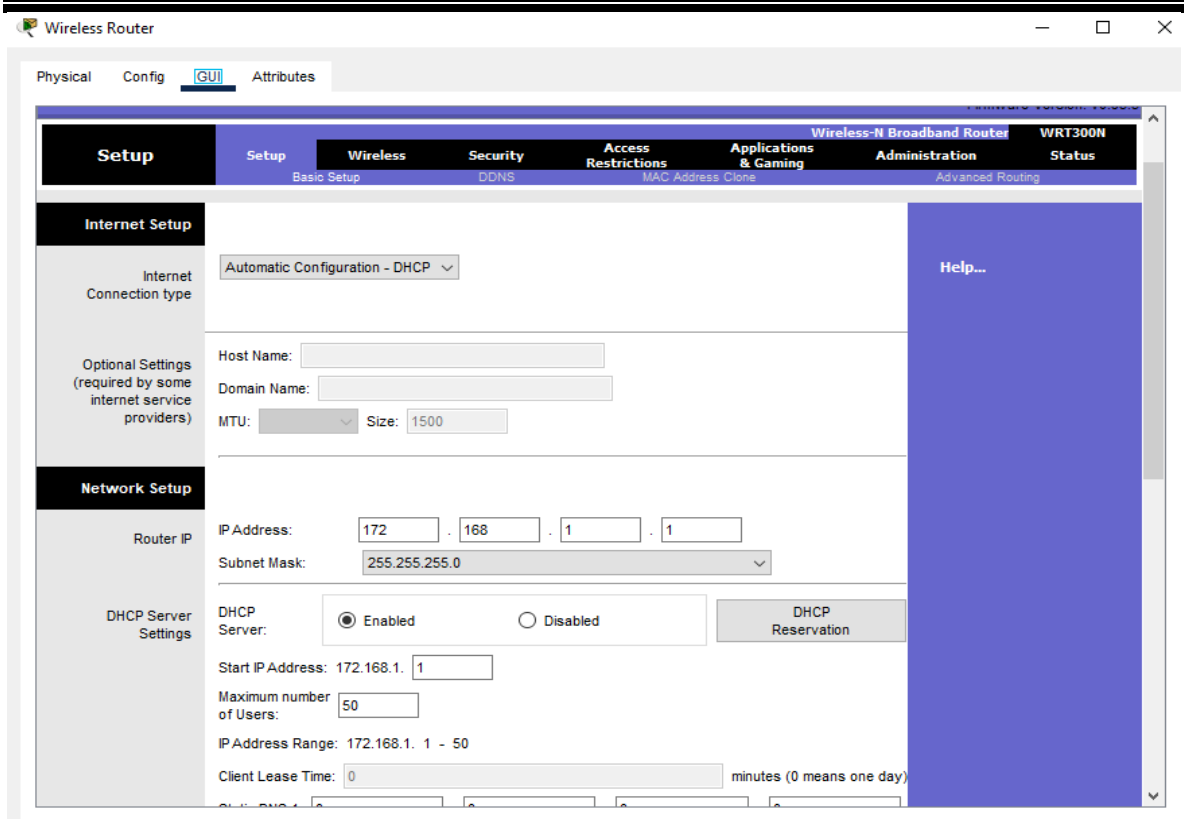
Thực hiện câu lệnh ping để xem các máy có thông với nhau hay chưa. Chúng ta dùng câu lệnh ping từ PC0 đến PC1 băng câu lệnh ping 192.168.10.3 và thực hiện tiếp câu lệnh ping 192.168.20.3 khác VLAN xem thử chúng có thông với nhau chưa.



Hình 11. Ping các PC với nhau.

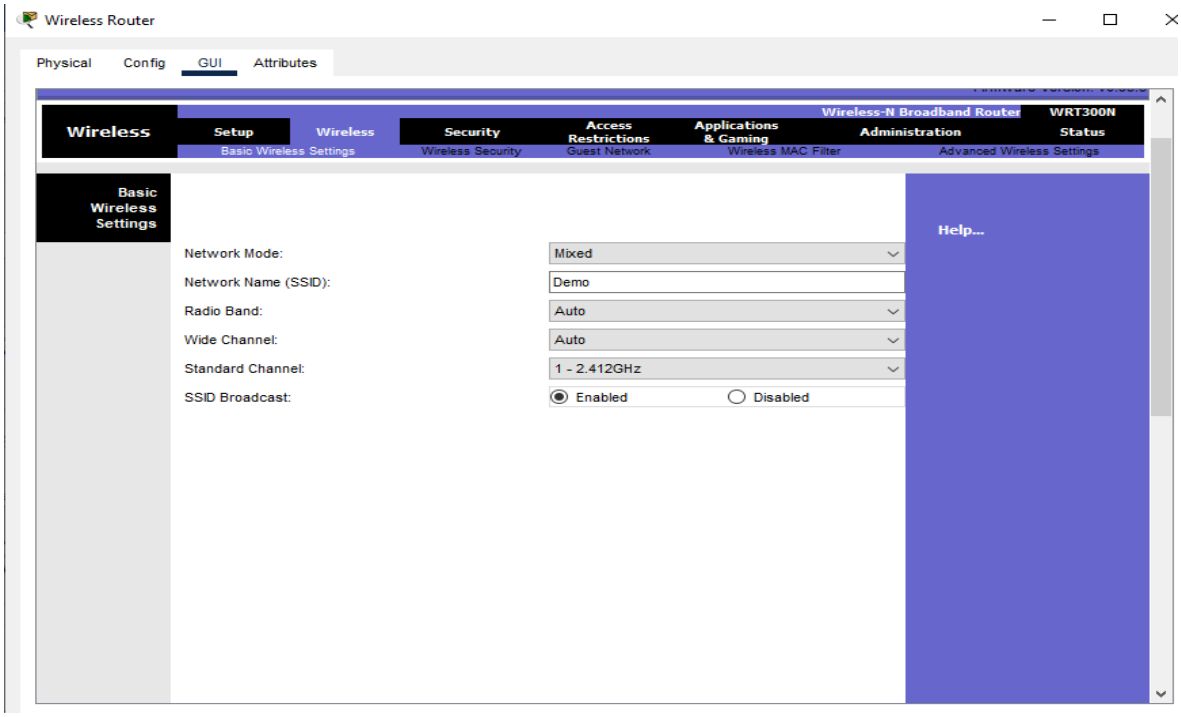
3.2.3 Cấu hình Wireless Router

Bước 1: Vào giao diện chính của Wireless Router sao đó vào phần GUI → Setup để cập nhật địa chỉ cổng LAN, sao đó lưu lại quá trình thực hiện.



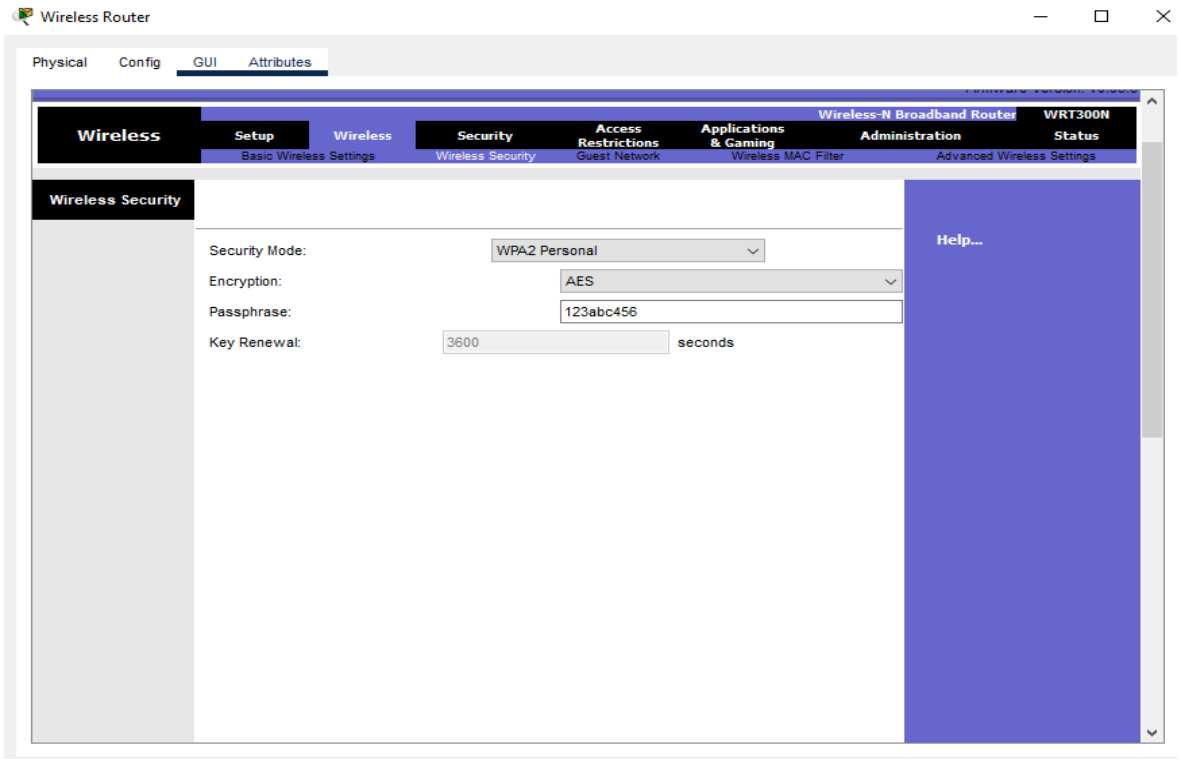
Hình 12. Giao diện của Wireless Router.

Bước 2: Vào phần Wireless → Basic Wireless Settings → Network Name (SSID) đặt tên cho thiết bị wifi sao đó lưu lại.



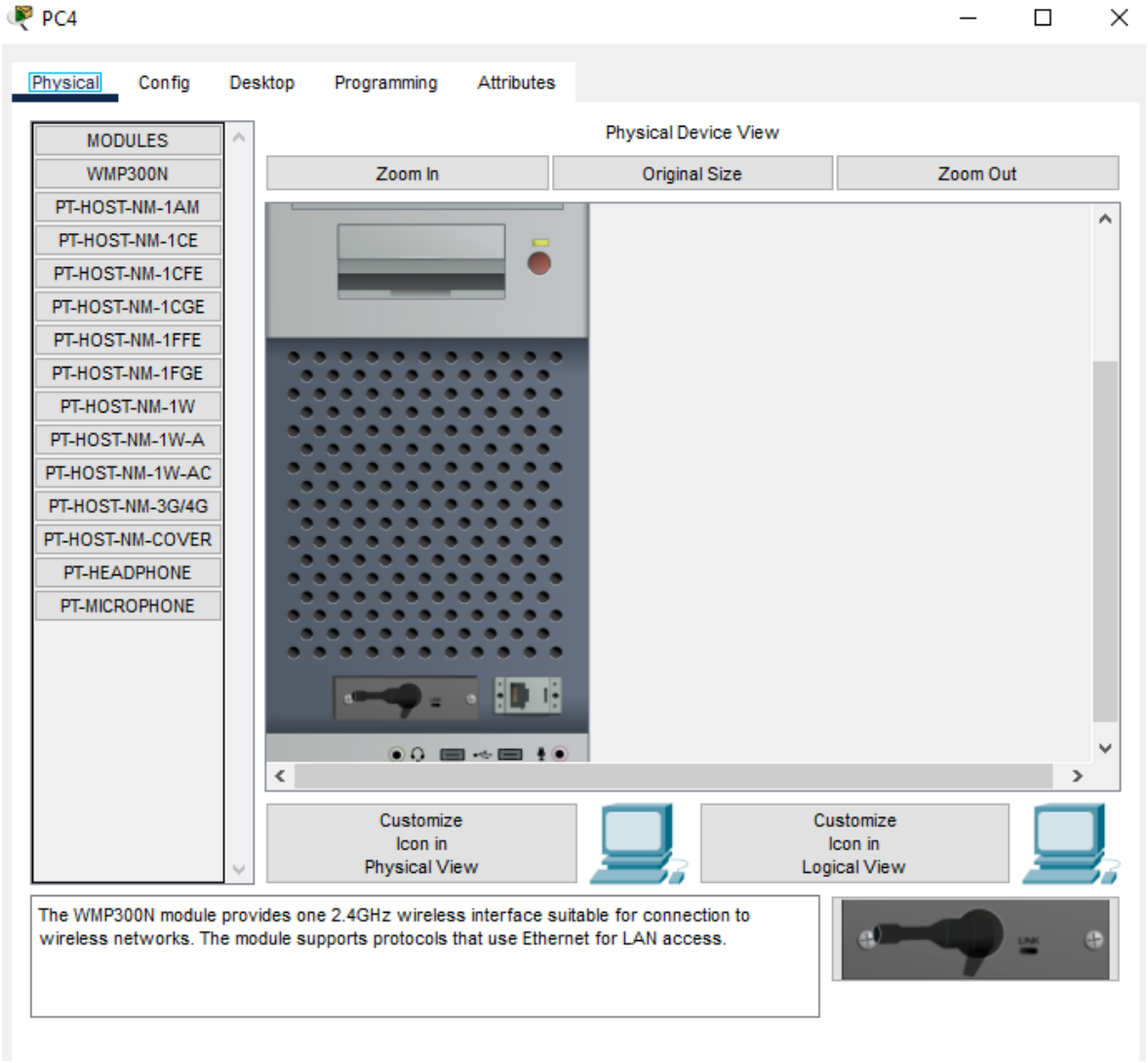
Hình 13. Đặt tên cho thiết bị Wireless Router.

Bước 3: Tiến hành đặt khẩu bảo mật cho thiết bị wifi, ta vào phần Wireless Security → Security Mode → chọn WPA2 Personal → Passphrase đặt mật khẩu cho thiết bị wifi rồi sao đó lưu lại quá trình thực hiện.



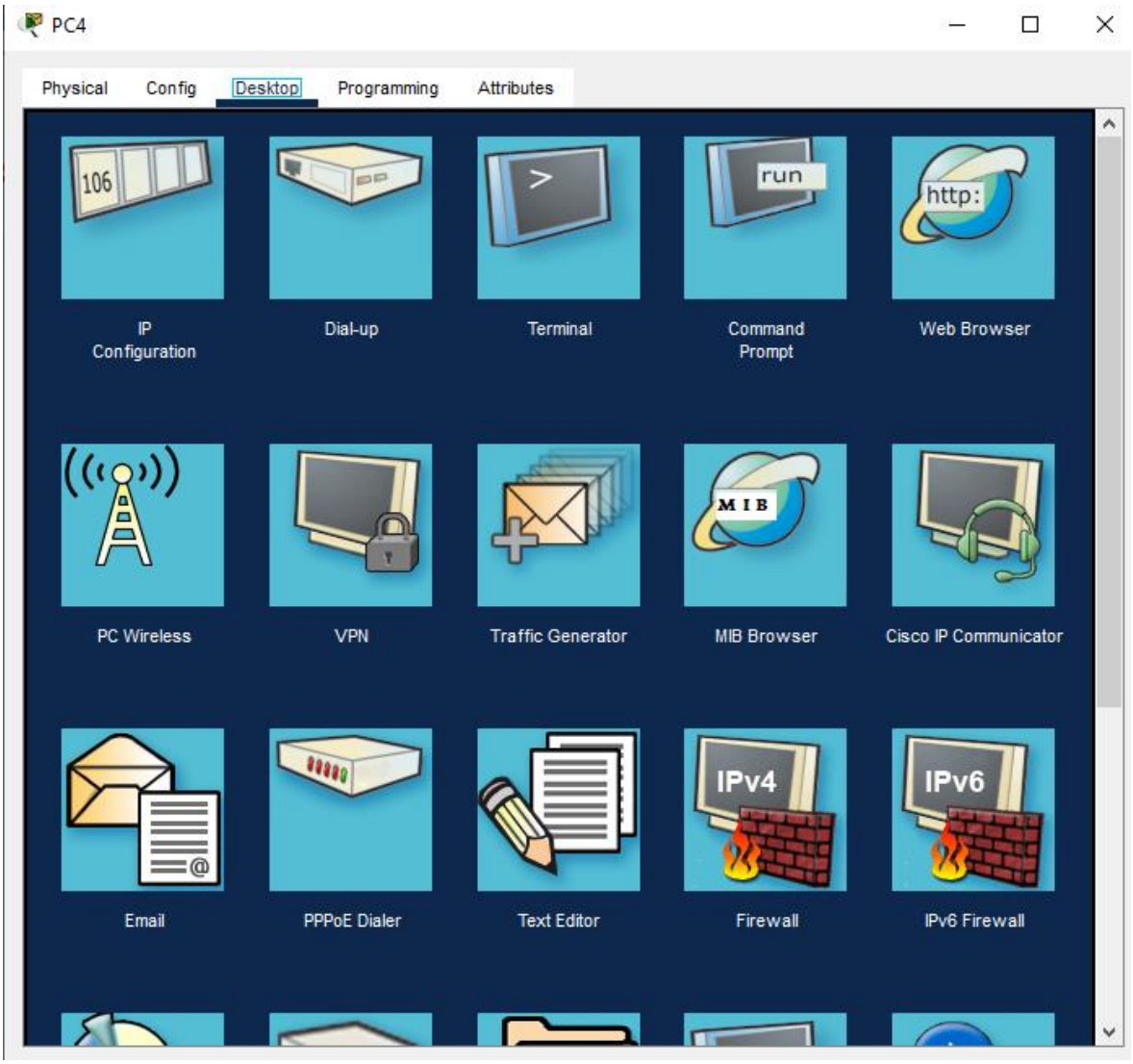
Hình 14. Đặt mật khẩu cho Wireless Router.

Bước4: Chọn một PC, Laptop, Smartphone,… các thiết bị muốn kết nối với wifi bất kì, ta tiến hành tắt thiết bị PC sao đó thay cổng kết nối bằng cổng WMP300N của thiết bị wifi và chúng ta bật lại thiết bị PC để tiến hành kết nối mạng.



Hình 15. Thay đổi cổng kết nối cho phù hợp với Wireless Router.

Bước 5: Để tiến hành kết nối ta vào phần PC Wireless để kết nối.



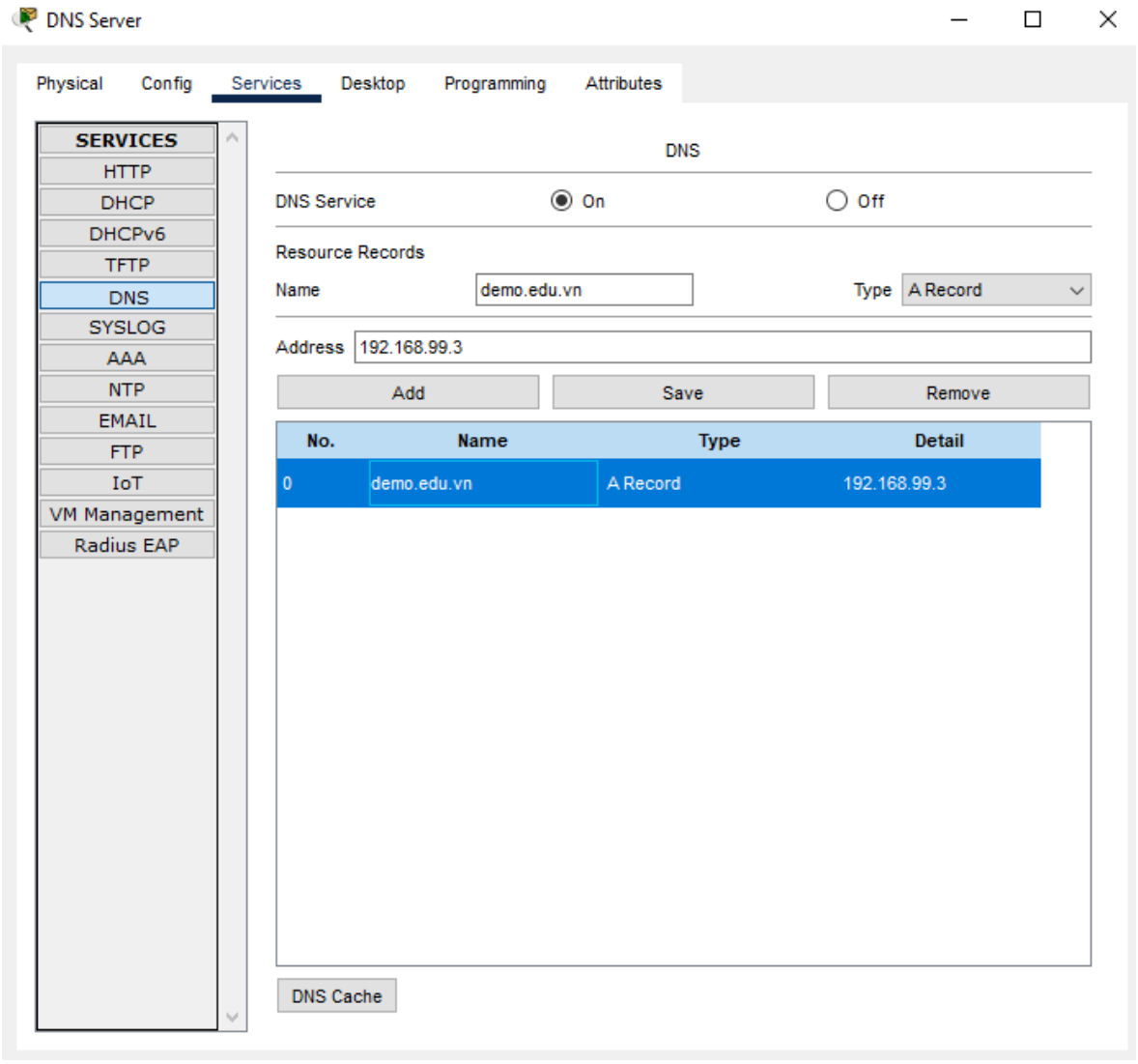
Hình 16. Chọn PC Wireless để kết nối.

Bước 6: Để chọn wifi ta vào phần Connect để chọn wifi cần kết nối sao đó nhập mật khẩu là có thể kết nối với wifi.

Hình 17. Tìm kiếm Wireless để kết nối.

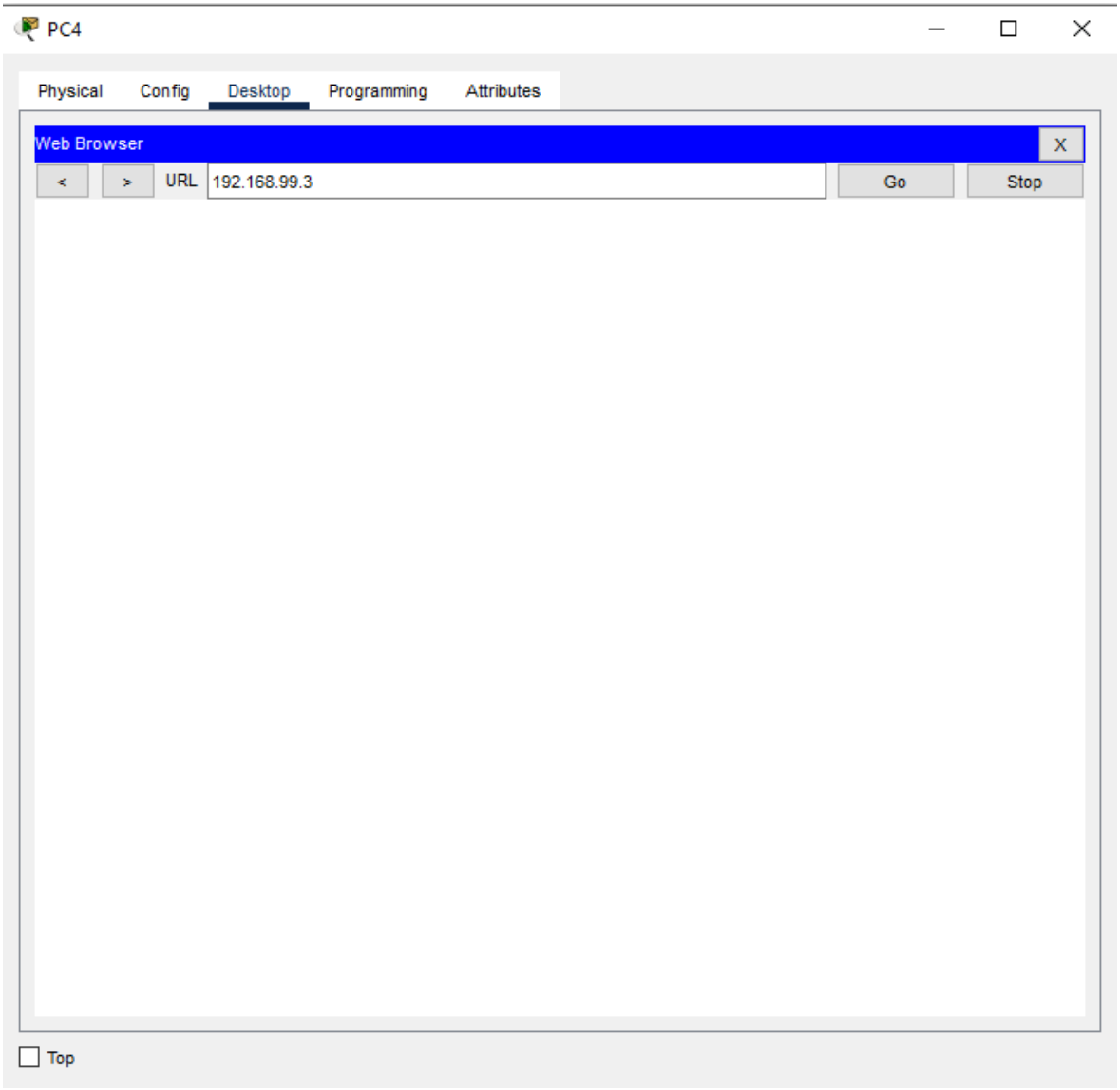
3.2.4 Cấu hình DNS Server

Services → chọn DNS → ta bậc On cho DNS Service → Name đặt địa chỉ tên miền cho web → Address dán địa chỉ ip của Web Server → Type chọn A Record → sao đó Add lại và Save .



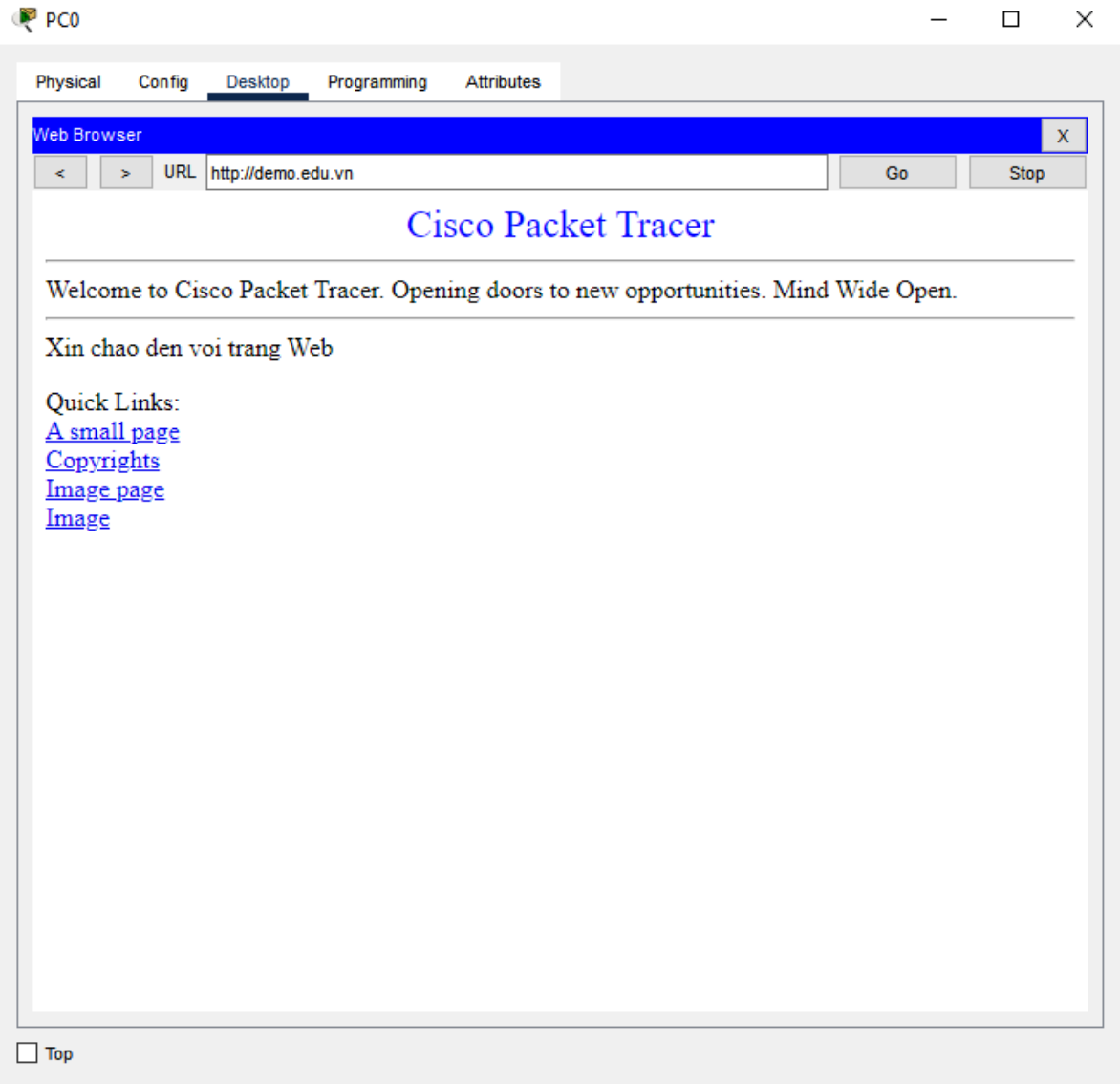
Hình 18. Cấu hình DNS Server.

Để kiểm tra xem địa chỉ web có hoạt động hay chưa ta vào một PC, Laptop, Smartphone và vào phần Web browser nhập địa chỉ ip của Web server.



Hình 19. Kiểm tra địa chỉ ip của Web Server.

Sao nhập địa chỉ ip của Web server ta được trang Web sau.



Hình 20. Giao diện chính của Web Server.

3.3 Bảo mật mạng WLAN

Bảo mật mạng WLAN (Wireless Local Area Network) là một phần quan trọng của quản lý mạng, đặc biệt là khi ngày càng nhiều tổ chức và cá nhân sử dụng kết nối không dây.

SSID (Service Set Identifier):

- SSID là tên của mạng WLAN, được sử dụng để nhận diện và kết nối vào mạng.
- Tuy nhiên, việc sử dụng SSID không bảo mật lắm vì nó có thể dễ dàng bị nhìn thấy và xâm phạm.
- Secure SSID: Trên cả hai loại SSID, bạn có thể kết hợp nhiều dịch vụ nhận dạng nếu cần.

Ví dụ: người dùng khách trải qua đánh giá tư thế, nhân viên trải qua MDM, nhân viên trải qua cổng web sau khi xác thực thiết bị, .

Hình 21. SSID an toàn.

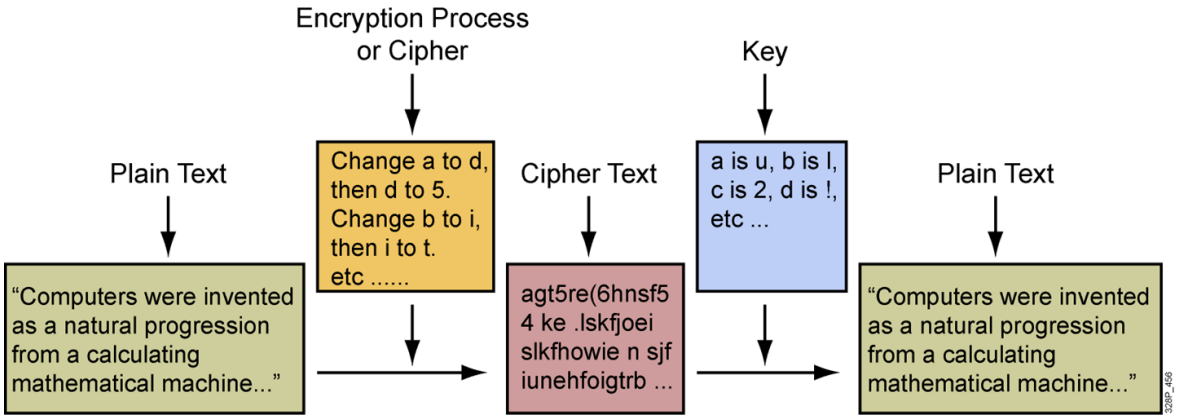
- Open SSID: SSID an toàn không thể quay lại để mở.

Ví dụ: người dùng không hỗ trợ 802.1X không thể quay lại xác thực cổng web trên cùng SSID với người dùng doanh nghiệp.

Khóa chia sẻ trước (PSK) và khóa có nguồn gốc từ 802.1X không thể cùng tồn tại trên SSID an toàn.

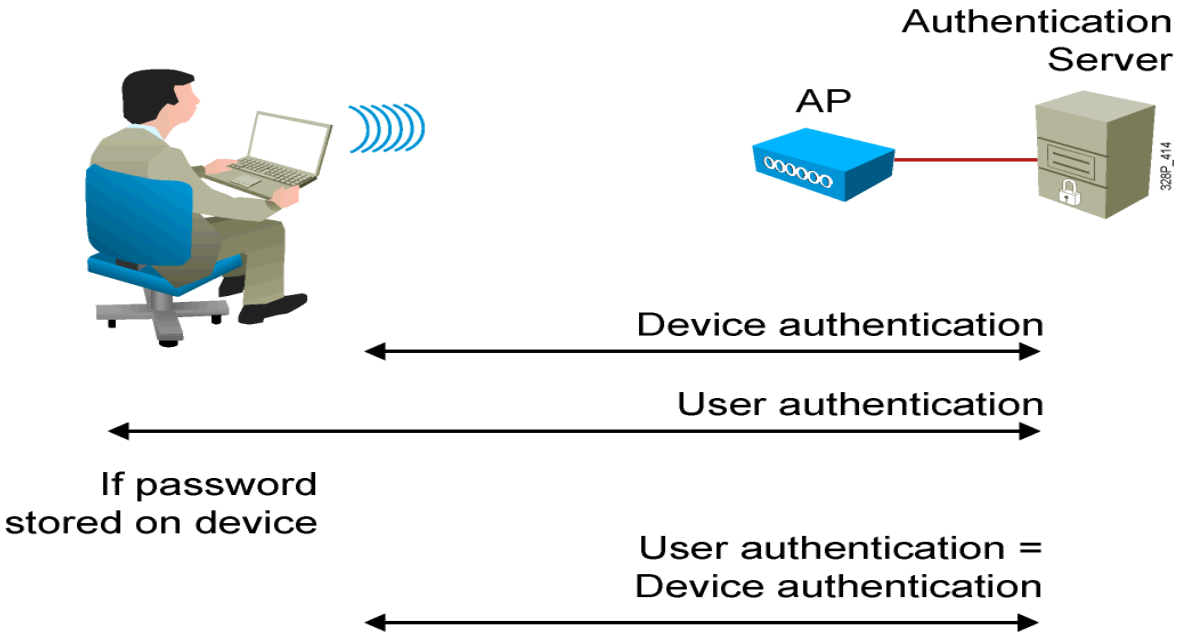
Hình 22. SSD không an toàn.

Encryption (Mã hóa): Mã hóa dữ liệu là một yếu tố quan trọng để ngăn chặn người truy cập trái phép. WPA (Wi-Fi Protected Access) và WPA2/WPA3 là các tiêu chuẩn phổ biến cho việc mã hóa mạng WLAN.



Hình 23. SSID không an toàn.

Authentication (Xác thực): Các phương thức xác thực, như WPA2-PSK (Pre-Shared Key) hoặc WPA3, đảm bảo rằng chỉ các thiết bị có mã xác thực mới có thể kết nối vào mạng.



Hình 24. Quá trình xác thực.

3.3.1 Các lỗ hổng và mối đe dọa mạng không dây

Mạng không dây (Wireless Network) đối mặt với nhiều lỗ hổng và mối đe dọa bảo mật.

Các lỗ hổng:

- Tin tặc có thể nghe lén giao tiếp không dây giữa các thiết bị, đánh cắp thông tin nhạy cảm như mật khẩu hoặc dữ liệu cá nhân.

- Tin tặc chèn mình vào giữa quá trình giao tiếp giữa hai bên, có thể đọc, sửa đổi hoặc thậm chí chặn thông tin.
- Thiết bị trái phép giả mạo làm Access Point để thu thập thông tin hoặc tấn công.
- Tấn công nhằm vào quá trình xác thực, thường bằng cách thử và kiểm tra mật khẩu.
- Gửi lượng truy cập lớn đến mạng để làm cho dịch vụ trở nên không khả dụng.
- Gửi thông báo giả mạo để làm cho thiết bị hoặc người dùng bị đuổi khỏi mạng.
- Gửi sóng tần số để làm gián đoạn và làm yếu hiệu suất mạng.
- Tấn công vào thiết bị có Bluetooth để gửi tin nhắn không mong muốn hoặc đánh cắp dữ liệu.

Cách khắc phục:

- Phòng ngừa: Sử dụng mã hóa dữ liệu, như WPA2 hoặc WPA3, để bảo vệ thông tin truyền qua mạng.
- Sử dụng kết nối an toàn với SSL/TLS, HTTPS, và tránh sử dụng mạng không dây không an toàn.
- Quản lý và giám sát kết nối không dây, sử dụng chứng thực mạnh mẽ.
- Sử dụng mật khẩu mạnh, kích hoạt xác thực hai yếu tố, và cập nhật giao thức xác thực.
- Sử dụng các giải pháp chống tấn công DoS, lọc gói tin, và quản lý băng thông.
- Giám sát hoạt động mạng và sử dụng các giải pháp bảo vệ chống tấn công này.
- Sử dụng kỹ thuật chống tấn công jamming và theo dõi tần số.
- Tắt Bluetooth khi không sử dụng, sử dụng cài đặt an toàn, và cập nhật phần mềm.

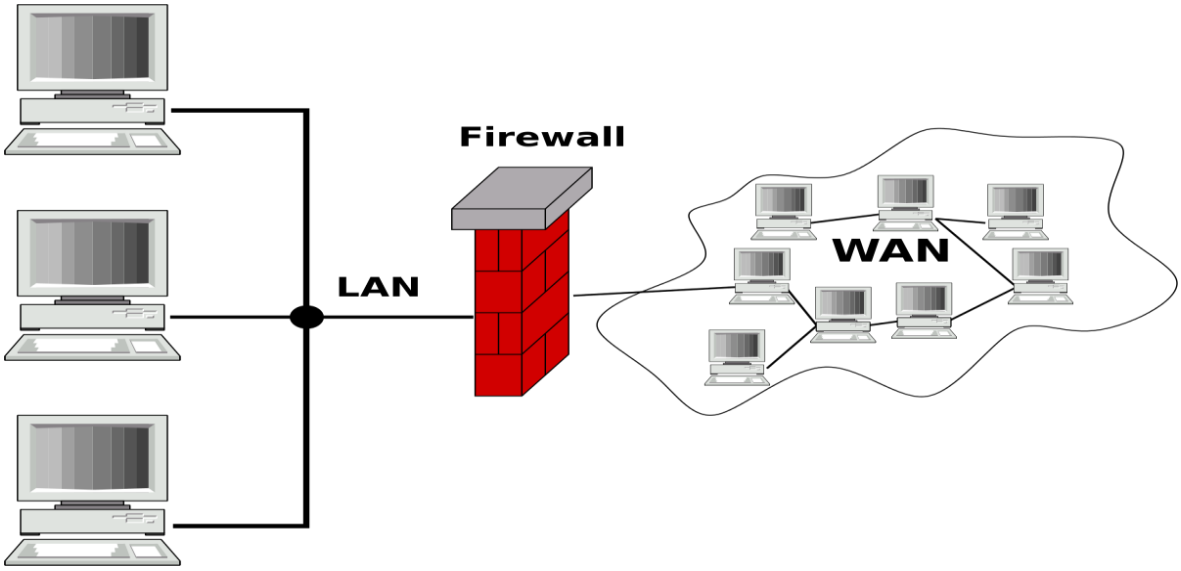
3.3.2 Công nghệ giảm thiểu mối đe dọa

Các công nghệ giảm thiểu mối đe dọa đề cập đến một bộ công cụ, phương pháp thực hành và chiến lược được thiết kế để xác định, ngăn chặn và ứng phó với nhiều loại mối đe dọa bảo mật khác nhau. Những mối đe dọa này có thể bao gồm nhiều loại rủi ro, bao gồm các mối đe dọa trên mạng, rủi ro bảo mật vật lý và các mối nguy hiểm tiềm ẩn khác đối với tổ chức hoặc hệ thống.

- Tường lửa:

+ Tường lửa mạng: Chúng giám sát và kiểm soát lưu lượng mạng đến và đi dựa trên các quy tắc bảo mật được xác định trước.

+ Tường lửa ứng dụng: Tập trung vào việc bảo vệ các ứng dụng cụ thể khỏi sự truy cập và tấn công trái phép.



Hình 25. Tường lửa.

- Hệ thống phát hiện xâm nhập (IDS) và Hệ thống ngăn chặn xâm nhập (IPS):

+ IDS giám sát các hoạt động mạng hoặc hệ thống để phát hiện các hoạt động độc hại hoặc vi phạm chính sách.

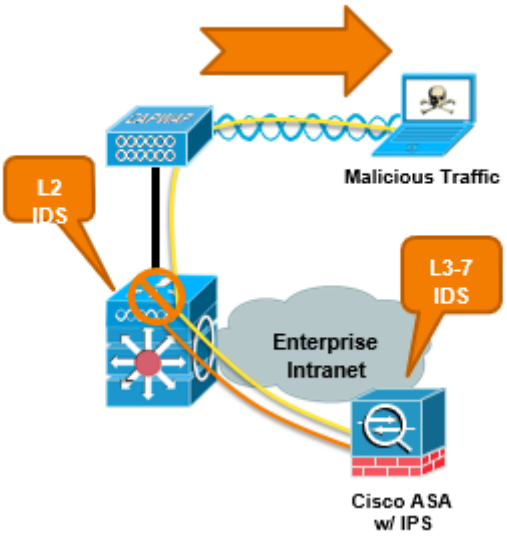
+ IPS tiến một bước xa hơn bằng cách chủ động ngăn chặn hoặc ngăn chặn các mối đe dọa được phát hiện.

+ Kiểm tra luồng lưu lượng truy cập để tìm các ứng dụng có hại và chặn kết nối máy khách không dây.

+ Kiểm tra gói sâu lớp 3-7

+ Loại bỏ nguy cơ lây nhiễm từ các máy khách không dây.

+ Phản hồi không ngày đối với vi-rút, phần mềm độc hại và chữ ký đáng ngờ.



Hình 26. Hệ thống ngăn chặn xâm nhập (IPS).

- Phần mềm chống vi-rút và chống phần mềm độc hại: Phát hiện, ngăn chặn và loại bỏ phần mềm độc hại (malware) như virus, sâu và Trojan.

- Bảo vệ điểm cuối: Giải pháp bảo mật bảo vệ các thiết bị riêng lẻ (điểm cuối) như máy tính, máy tính xách tay và thiết bị di động khỏi các mối đe dọa bảo mật.

- Mã hóa: Bảo vệ dữ liệu nhạy cảm bằng cách chuyển đổi nó sang định dạng được mã hóa mà chỉ có thể giải mã được bằng khóa thích hợp.

- Mạng riêng ảo (VPN): Đảm bảo liên lạc an toàn qua internet bằng cách tạo một mạng riêng từ kết nối internet công cộng.

3.3.3 Xác thực và mã hóa

Nguyên tắc cơ bản về bảo mật 802.11: Thiết lập liên kết 802.11 an toàn

- Xác thực (Authentication): Xác thực là quá trình xác định xem một thực thể (người dùng, thiết bị, hệ thống) có quyền truy cập vào hệ thống hay không.

- Phương tiện xác thực:

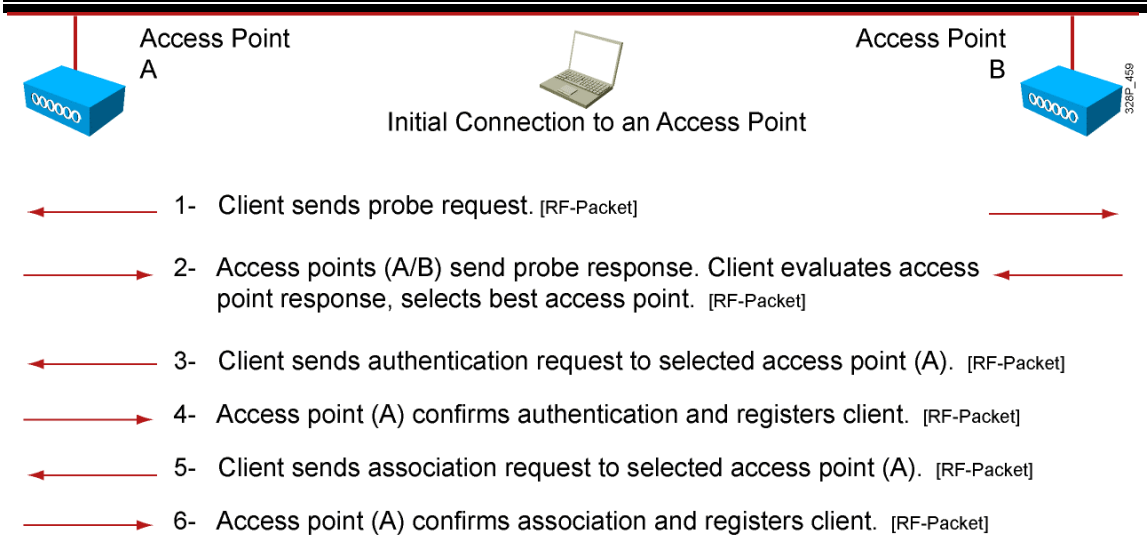
+ Mật khẩu: Xác thực thông qua việc nhập mật khẩu.

+ Mã xác nhận (OTP): Sử dụng mã được tạo một lần để xác thực.

+ Chứng chỉ: Sử dụng chứng chỉ số học để xác thực.

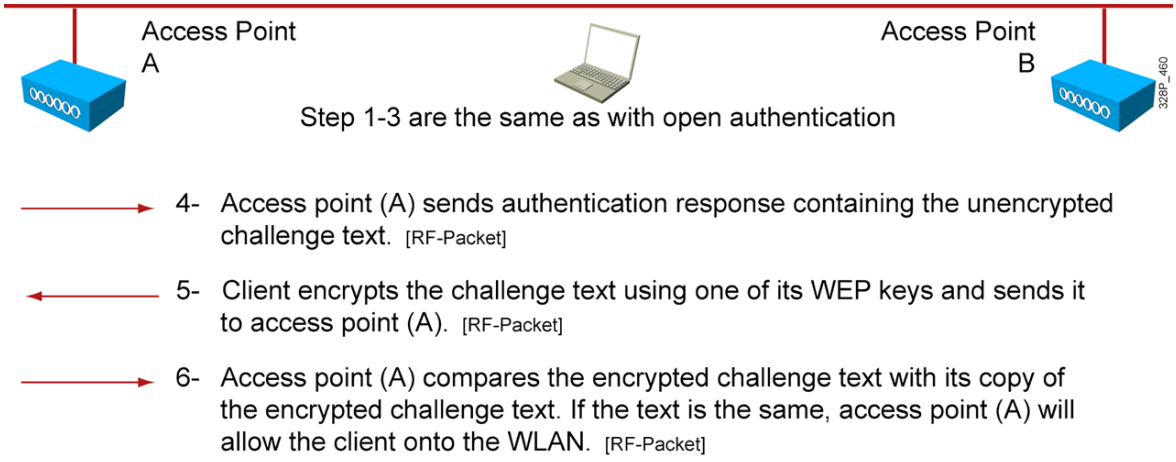
Vân tay, nhận diện khuôn mặt, và các phương tiện khác: Sử dụng các đặc điểm sinh học để xác thực.

Authentication: Open



Hình 27. Authentication: Open.

Authentication: PSK (WEP)



Hình 28. Authentication: PSK (WEP).

thành dạng không đọc được nếu không có khóa giải mã.

- Loại mã hóa:

+ Mã hóa đối xứng (Symmetric Encryption): Cùng một khóa được sử dụng để mã hóa và giải mã dữ liệu.

+ Mã hóa không đối xứng (Asymmetric Encryption): Sử dụng cặp khóa: một khóa để mã hóa và một khóa khác để giải mã.

Bảo vệ thông tin khỏi việc truy cập trái phép bằng cách biến dữ liệu thành một dạng mà chỉ người hoặc thiết bị có khóa giải mã mới có thể đọc được.

3.3.4 Xác thực mạng WLAN

IEEE 802.1X là một tiêu chuẩn mạng được sử dụng để xác thực và kiểm soát quyền truy cập vào mạng có dây hoặc không dây. Nó là một phần của chuỗi tiêu chuẩn IEEE 802, cụ thể là phần của chuẩn IEEE 802.1, liên quan đến kiến trúc mạng LAN (Local Area Network). 802.1X được thiết kế để cung cấp phương tiện để xác thực người dùng và thiết bị trước khi chúng được phép truy cập vào mạng.

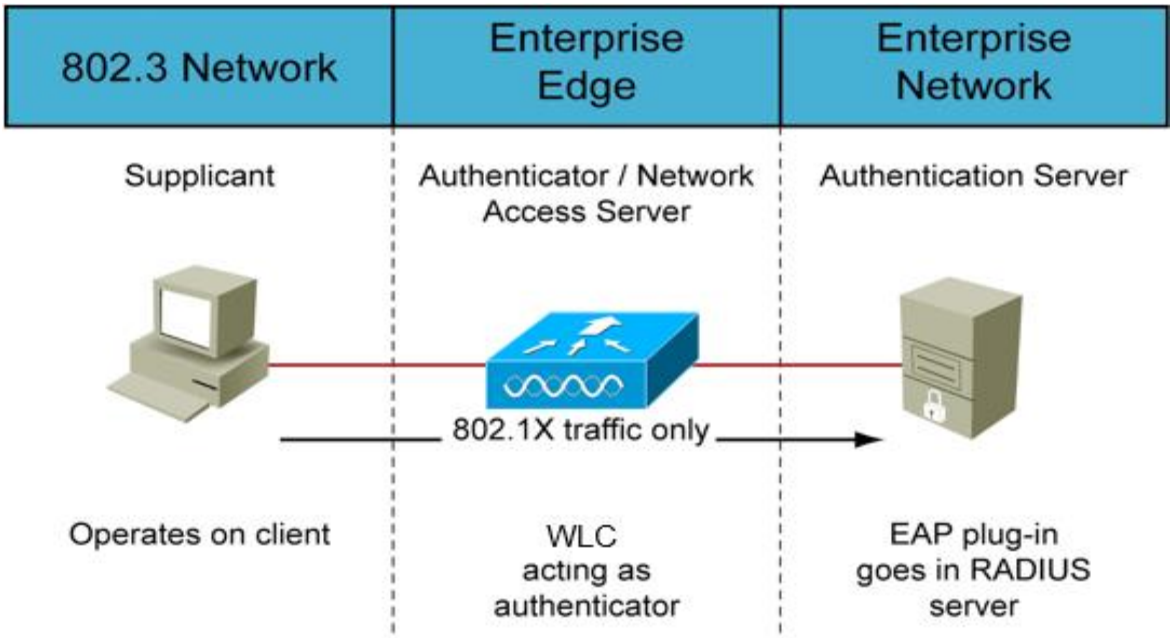
- Xác thực (Authentication): IEEE 802.1X sử dụng các phương thức xác thực như EAP (Extensible Authentication Protocol) để xác thực người dùng và/hoặc thiết bị trước khi chúng có thể kết nối với mạng.
- Supplicant, Authenticator, và Authentication Server:

+ Supplicant: Là người dùng hoặc thiết bị cố gắng kết nối vào mạng và cần phải xác thực.

+ Authenticator: Là thiết bị mạng (chẳng hạn switch hoặc wireless access point) trực tiếp kết nối với supplicant và kiểm soát quyền truy cập.

+ Authentication Server: Là máy chủ xác thực (thường là một máy chủ RADIUS) thực hiện xác thực người dùng.

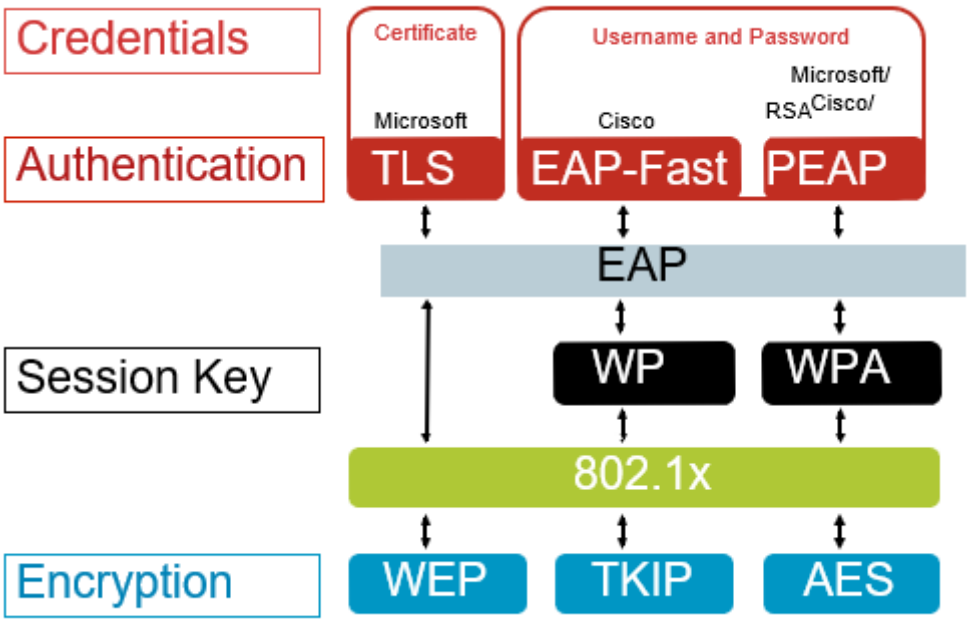
- Flexibility with EAP Methods: 802.1X không giới hạn vào một phương thức cụ thể của EAP, mà cho phép sử dụng nhiều phương thức xác thực khác nhau như EAP-TLS, EAP-PEAP, EAP-TTLS.



Hình 29. 802.1X.

Kiến trúc IEEE 802.1X được thiết kế để cung cấp khả năng kiểm soát truy cập mạng dựa trên cổng (PNAC) thông qua việc sử dụng khung xác thực. Nó thường được sử dụng để bảo mật cả mạng LAN có dây và không dây bằng cách xác thực các thiết bị đang cố gắng kết nối với mạng.

- Credentials: Thông tin xác thực đề cập đến thông tin được sử dụng để xác thực và xác minh danh tính của người dùng, hệ thống hoặc tổ chức đang tìm kiếm quyền truy cập vào tài nguyên được bảo mật. Các thông tin xác thực này thường bao gồm sự kết hợp giữa tên người dùng và mật khẩu, mặc dù trong các hệ thống xác thực nâng cao hơn, các yếu tố bổ sung như mã thông báo bảo mật, sinh trắc học hoặc thẻ thông minh có thể liên quan. Mục đích của thông tin xác thực là để đảm bảo rằng chỉ những cá nhân hoặc hệ thống được ủy quyền mới có thể truy cập các tài nguyên hoặc dịch vụ cụ thể.
- Authenticator: trình xác thực là một thành phần hoặc thực thể tham gia vào quá trình xác minh danh tính của người dùng hoặc thiết bị, đảm bảo quyền truy cập an toàn vào hệ thống hoặc mạng.
- Session Key: Khóa phiên là khóa mật mã tạm thời được sử dụng để bảo mật thông tin liên lạc và dữ liệu giữa hai bên trong một phiên hoặc giao dịch cụ thể. Mục đích của việc sử dụng khóa phiên là để tăng cường tính bảo mật của dữ liệu bằng cách đảm bảo rằng ngay cả khi khóa bị xâm phạm, tác động sẽ được giới hạn ở một phiên cụ thể.
- Encryption: Mã hóa là một quá trình chuyển đổi thông tin (bản rõ) thành dạng an toàn và không thể đọc được (bản mã) bằng thuật toán và khóa mã hóa. Mục đích chính của mã hóa là để bảo vệ tính bảo mật và tính toàn vẹn của dữ liệu nhạy cảm, gây khó khăn cho các cá nhân hoặc tổ chức trái phép truy cập hoặc sửa đổi thông tin. Mã hóa được sử dụng rộng rãi trong nhiều ứng dụng khác nhau, bao gồm giao tiếp, lưu trữ và xác thực.



Hình 30. 802.1x Architecture.

3.3.5 Các loại thông tin nhận dạng 802.1x

- Kết hợp tên người dùng/mật khẩu:

+ Yêu cầu người dùng sử dụng mật khẩu mạnh, bao gồm cả chữ in hoa, chữ thường, chữ số và ký tự đặc biệt.

+ Hạn chế độ dài tối thiểu cho mật khẩu để đảm bảo độ an toàn.

+ Các loại PEAP-MSCHAPv2, PEAP-GTC, EAP-FAST

- Xác thực hai yếu tố: là một phương pháp bảo mật mà người dùng cần cung cấp hai yếu tố xác thực khác nhau để chứng minh danh tính của họ khi đăng nhập hoặc thực hiện các giao dịch quan trọng. Các loại PEAP-GTC, EAP-FAST/EAP-GTC

- Chứng chỉ: số là một thành phần quan trọng của cơ sở hạ tầng khóa công khai (PKI) và đóng vai trò cơ bản trong việc bảo mật thông tin liên lạc trực tuyến. Các loại EAP: EAP-TLS, EAP-FAST

Local EAP: "EAP cục bộ", thì nó có thể đề cập đến EAP dành riêng cho một địa phương hoặc khu vực cụ thể. Các dịch vụ do EAP cung cấp sẽ được điều chỉnh cho phù hợp với nhu cầu và nguồn lực sẵn có trong khu vực cụ thể đó.

LEAP: là giao thức bảo mật mạng LAN không dây được phát triển bởi Cisco. Hiện nay nó được coi là lỗi thời và không an toàn và phần lớn đã được thay thế bằng các giao thức an toàn hơn như WPA (Wi-Fi Protected Access) và WPA2.

EAP-FAST: Giao thức xác thực mở rộng-xác thực linh hoạt thông qua đường hầm an toàn, là giao thức xác thực mạng thường được sử dụng trong các mạng không dây, đặc biệt để bảo mật kết nối Wi-Fi. Đây là phương thức giao thức xác thực mở rộng (EAP) được thiết kế để cung cấp quy trình xác thực linh hoạt và an toàn.

EAP-TLS: là viết tắt của Giao thức xác thực mở rộng với bảo mật lớp vận chuyển. Nó là một giao thức bảo mật mạng thường được sử dụng để bảo mật các kết nối truy cập điểm và truy cập từ xa. EAP-TLS là một phần của khung giao thức xác thực mở rộng (EAP) rộng hơn và cung cấp cơ chế xác thực mạnh mẽ.

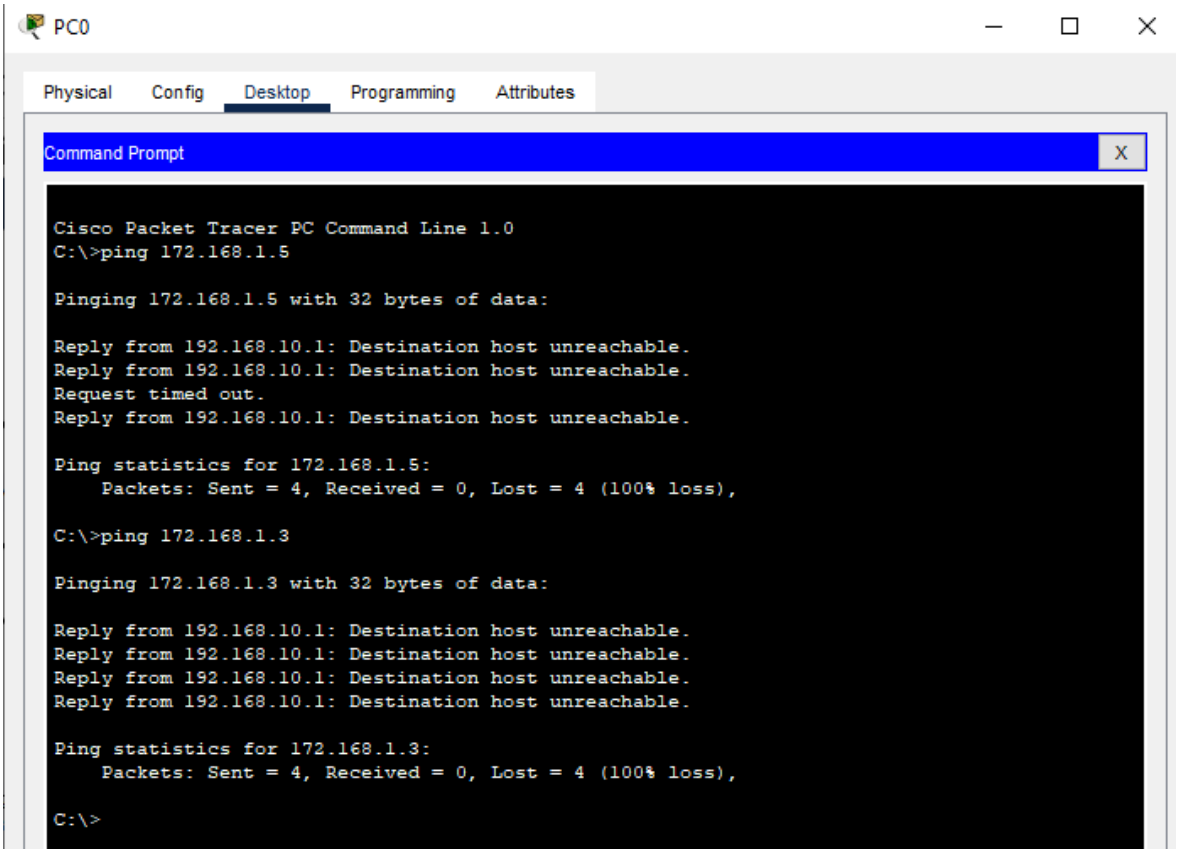
PEAP: hay giao thức xác thực mở rộng được bảo vệ, là một giao thức xác thực khác được sử dụng trong mạng không dây và kết nối truy cập từ xa. Nó được thiết kế để tăng cường tính bảo mật của giao thức xác thực mở rộng (EAP) bằng cách cung cấp kênh được bảo vệ để xác thực. PEAP thường được sử dụng trong mạng không dây doanh nghiệp.

CCX: là viết tắt của tiện ích mở rộng tương thích của Cisco. Đây là một tập hợp các cải tiến độc quyền được Cisco Systems phát triển để cải thiện khả năng tương thích và hiệu suất của mạng Wi-Fi với cơ sở hạ tầng không dây của Cisco. CCX được thiết kế để tăng cường sự tương tác giữa các thiết bị không dây của Cisco, chẳng hạn như điểm truy cập và máy khách không dây, nhằm tối ưu hóa hiệu suất và bảo mật tổng thể của mạng không dây.

Chương 4: KẾT QUẢ NGHIÊN CỨU

Sao khi hoàn thành nghiên cứu rút ra được một số kết quả sau:

- Có thể ping các PC cùng vlan và các vlan khác nhau.
- Có thể ping các PC không dây sang PC có dây.
- Cài đặt được dịch vụ web để các PC truy cập được web.
- Bảo mật mạng không dây khỏi các thiết bị lạ.
- Riêng nhánh Wifi chỉ ping vào được các PC có dây, từ thiết bị có dây ping sang thiết bị không dây không được có thể do hạn chế của thiết bị ảo.



Hình 31. Ping từ PC có dây sang PC không dây.

Chương 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1 Kết luận

Sao khi nghiên cứu thực hiện đồ án Xây dựng hệ thống mạng không dây qua quá trình làm đạt được những kết quả sau:

- Tìm hiểu được mạng máy tính, mạng không dây.
- Định tuyến router.
- Cấu hình VLAN.
- Cấu hình Wireless router.
- Bảo mật mạng không dây.
- Cài đặt dịch vụ web để các PC truy cập được web.

Những đề xuất mới:

- Kết hợp trí tuệ nhân tạo để tối ưu hóa tự tổ chức và quản lý mạng mesh.
- Áp dụng công nghệ blockchain để tăng cường bảo mật trong mạng Wi-Fi.
- Phát triển hệ thống xác thực và quản lý khóa sử dụng smart contracts.
- Nghiên cứu và triển khai hệ thống mạng sử dụng băng tần mới 6 GHz của Wi-Fi 6E.

5.2 Hướng phát triển

- Xây dựng hệ thống mạng không dây cho doanh nghiệp.
- Phát triển các tiêu chuẩn mới cho mạng không dây, tiêu chuẩn liên quan đến mạng 5G.
- Tích hợp trí tuệ nhân tạo vào quá trình bảo mật phát hiện và ngăn chặn các tấn công mạng.
- Tích hợp tính năng giám sát mạng để đưa ra gợi ý và cải thiện dịch vụ.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Chuyen de TT & Mang khong day-20231116T060951Z-001

[2] https://bkaii.com.vn/tin-tuc/308-nguyen-li-hoat-dong-cua-mang-khong-day

[3] https://viettuans.vn/vlan-la-gi

[4] https://vi.wikipedia.org/wiki/Packet_Tracer

[5] https://fptshop.com.vn/tin-tuc/danh-gia/wpa2-la-gi-154744

[6] https://www.youtube.com/watch?v=ih-Rnmfoiqc&t=677s