TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO MÔN HỌC**

**WIRELESS AND MOBILE NETWORK SECURITY**

**XÂY DỰNG HỆ THỐNG MẠNG KHÔNG DÂY CHO CÔNG TY TECHBASE**

Người hướng dẫn: **GV BÙI QUY ANH**

Người thực hiện:**LÊ MINH HIẾU – 51702016**

**TẠ VĂN TRỌNG – 51702048**

**NGUYỄN DANH BẮC – 51703046**

Lớp: **17050201**

Khoá: **21**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

# LỜI CẢM ƠN

Bọn em xin chân thành gửi lời cảm ơn đến toàn thể Ban giám hiệu Đại học Tôn Đức Thắng và tập thể thầy cô Khoa Công nghệ Thông tin đã giúp đỡ và tạo mọi điều kiện trong suốt quá trình học tập tại trường và củng như trong quá trình hoàn thành đồ án môn học An toàn mạng không dây và di động.

Em xin cảm ơn đến giảng viên Bùi Quy Anh với những kinh nghiệm và kiến thức chuyên môn cao đã hết lòng giúp đỡ, bảo ban và động viên để bọn em hoàn thành tốt được đồ án được giao này.

Cảm ơn các bạn, các anh chị trong khoa đã giúp đỡ em rất nhiều trong quá trình tìm hiểu tài liệu củng như có các ý kiến đóng góp để bài đồ án trở nên hoàn thiện hơn.

Xin cảm ơn bố mẹ, anh chị trong gia đình đã luôn ở bên động viên việc học tập để hoàn thành đồ án quan trọng nhất trong cuộc đời sinh viên.

Trong quá trình làm đồ án chắc chắn vẫn còn mắc phải nhiều sai sót, bọn em rất mong thầy cô bỏ qua. Đồng thời, với kiến thức và kinh nghiệm còn hạn chế bọn em xin sự đóng góp từ thầy cô để đồ án của bọn em được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

**BÁO CÁO ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm báo cáo của riêng chúng em và được sự hướng dẫn của GV Bùi Quy Anh. Các nội dung nghiên cứu, kết quả trong báo cáo này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Lê Minh Hiếu*

*Tạ Văn Trọng*

*Nguyễn Danh Bắc*

**PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN**

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Trình bày tóm tắt vấn đề nghiên cứu, các hướng tiếp cận, cách giải quyết vấn đề và một số kết quả đạt được, những phát hiện cơ bản trong vòng 1 -2 trang.

MỤC LỤC

[LỜI CẢM ƠN ii](#_Toc90649784)

[TÓM TẮT v](#_Toc90649785)

[MỤC LỤC 1](#_Toc90649786)

[DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT 3](#_Toc90649787)

[**CHƯƠNG 1: MÔ TẢ ĐỀ TÀI** 4](#_Toc90649788)

[1.1 Yêu cầu khách hàng 4](#_Toc90649789)

[1.2 Đề xuất hướng giải quyết 4](#_Toc90649790)

[1.3 4](#_Toc90649791)

[**CHƯƠNG 2: CƠ SỞ LÝ THUYẾT** 5](#_Toc90649792)

[2.1 Các khái niệm cơ bản 5](#_Toc90649793)

[2.1.1 Khái niệm mạng máy tính 5](#_Toc90649794)

[2.1.1.1 Mạng máy tính 5](#_Toc90649795)

[2.1.1.2 Lịch sử hình thành mạng máy tính 5](#_Toc90649796)

[2.1.1.3 Thách thức và lợi ích của mạng máy tính 7](#_Toc90649797)

[2.1.1.4 Phân loại mạng 7](#_Toc90649798)

[2.1.2 Khái niệm mạng wifi 10](#_Toc90649799)

[2.1.2.1 Nguyên lý hoạt động 11](#_Toc90649800)

[2.1.2.2 Ưu và nhược điểm 11](#_Toc90649801)

[2.1.2.3 Các mô hình mạng wifi 12](#_Toc90649802)

[2.1.3 Khái niệm an toàn bảo mật không dây 16](#_Toc90649803)

[2.1.3.1 Các hình thức tấn công mạng WLAN 17](#_Toc90649804)

[2.1.3.2 Các phương pháp bảo mật cơ bản 21](#_Toc90649805)

[2.2 Các thiết bị xây dựng mạng 30](#_Toc90649806)

[2.2.1 Card mạng 31](#_Toc90649807)

[2.2.2 Cầu nối Bridge 33](#_Toc90649808)

[2.2.3 Repeater 34](#_Toc90649809)

[2.2.4 Bộ chia Hub 36](#_Toc90649810)

[2.2.5 Bộ chuyển mạch Switch 37](#_Toc90649811)

[2.2.6 Router 38](#_Toc90649812)

[2.2.7 Modem 40](#_Toc90649813)

[2.2.8 Gateway 40](#_Toc90649814)

[CHƯƠNG 3: MÔ HÌNH DEMO 42](#_Toc90649815)

[3.1 Mô hình đề xuất 42](#_Toc90649816)

[3.1.1 Bảng địa chỉ 42](#_Toc90649817)

[3.2 Cấu hình các thiết bị 42](#_Toc90649818)

[3.3 Kết quả chạy chương trình 42](#_Toc90649819)

[CHƯƠNG 4: KẾT LUẬN 43](#_Toc90649820)

# DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

**CÁC KÝ HIỆU**

**CÁC CHỮ VIẾT TẮT**

**CHƯƠNG 1: MÔ TẢ ĐỀ TÀI**

* 1. Yêu cầu khách hàng

Xây dựng hệ thống mạng cho công ty techbase gồm có 3 tầng, mỗi tầng có 1 wireless riêng biệt. Tầng trệt và tầng 1 cung cấp hệ thống mạng cho nhân viên và khách hàng với nhu cầu sử dụng khoảng 10 – 50 kết nối. Tầng 2 sẽ cung cấp hệ thống mạng cho các trưởng phòng, quản lý hoặc giám đốc.

* 1. Đề xuất hướng giải quyết

Dựa trên yêu cầu của khách hàng sẽ xây dựng một hệ thống gồm: Dns - Dhcp Server, Web Server, Radius Server và 3 Wifi riêng biệt. Wifi ở tầng trệt và tầng 1 cung cấp wifi cho nhân viên và khách hàng nên sẽ sử dụng bảo mật WPA2-Personal. Wifi ở tầng 2 được dùng cho các trưởng phòng, quản lý hoặc giám đốc nên sẽ sử dụng bảo mật WPA-Enterprise để dễ dàng kiểm soát.

**CHƯƠNG 2: CƠ SỞ LÝ THUYẾT**

* 1. Các khái niệm cơ bản
     1. Khái niệm mạng máy tính
        1. Mạng máy tính

Mạng máy tính nổi tiếng nhất hiện nay là mạng Internet. Mạng máy tính là mạng viễn thông kỹ thuật số cho phép các nút mạng chia sẽ tài nguyên qua lại. Trong các mạng máy tính, các thiết bị máy tính trao đổi dữ liệu qua lại với nhau bằng các kết nối giữa các nút hoặc liên kết dữ liệu giữa các nút. Các liên kết dữ liệu này được thiết lập qua cáp mạng như dây, cáp quang hoặc là các phương tiện không dây như Wi-Fi.

Các thiết bị máy tính mạng có nhiệm vụ là khởi động, định tuyến và chấm dứt dữ liệu được gọi là các nút mạng. Các nút mạng thường được xác định bởi địa chỉ mạng và có thể bao gồm máy chủ mạng như là máy tính cá nhân, điện thoại và máy chủ cũng như phần cứng mạng như bộ định tuyến và chuyển mạch. Hai thiết bị được coi là kết nối với nhau khi một thiết bị có thể trao đổi thông tin với thiết bị kia, cho dù có kết nói trực tiếp với nhau hay không. Phần lớn các trường hợp, các giao thức truyền thông dành riêng cho ứng dụng được xếp lớp (mạng theo trọng tải) so với các giao thưc truyền thông chung khác.

Mạng máy tính hỗ trợ trong phần lớn các ứng dụng và dịch vụ trong thực tế như truy cập WWW (World Wide Web), video kỹ thuật số, âm thanh kỹ thuật số, sử dụng các máy chủ lưu trữ và ứng dụng, máy in, máy fax, email,…Mạng máy tính khác nhau về cách thức truyền tin được sử dụng để mang tín hiệu, giao thức truyền thông để tổ chức lưu lượng mạng, kích thước của mạng, cấu trúc liên kết, cơ chế điều khiển lưu lượng, ý định tổ chức mạng.

* + - 1. Lịch sử hình thành mạng máy tính

Năm 1940, các thiết bị cơ-điện tử kích thước lớn và rất dễ hư hỏng. Với sự ra đời của transistor bán dẫn vào năm 1947 tạo ra cơ hội để làm ra chiếc máy tính nhỏ gọn và chắc chắn hơn.

Năm 1950, các máy tính lớn mainframe chạy bởi các chương trình trên thẻ đục lỗ (punched card) được ra đời. Nó giúp máy tính có khả năng được lập trình tuy nhiên củng tạo ra khó khăn trong việc tạo ra các chương trình trên thẻ này.

Cuối 1950, mạch tích hợp (IC) được phát minh ra chứa nhiều transistor trên một mẫu bán dẫn nhỏ. Đây là bước tạo ra sự nhảy vọt trong việc chế tạo ra các máy tính mạnh hơn, nhanh và nhỏ hơn. IC có thể chứ hàng triệu transistor trên nhiều mạch.

Cuối 1960 đầu 1970, máy tính minicomputer được xuất hiện.

Năm 1977, công ty máy tính Apple đã ra mắt máy vi tính hay còn được gọi là máy tính cá nhân (Personal Computer - PC).

IBM đã đưa ra máy tính cá nhân đầu tiên năm 1981, với sự nhỏ gọn và sự tinh vi của các IC đã đưa máy tính cá nhân được sử dụng trong kinh doanh và sử dụng tại nhà.

Vào giữa thập niêm 1980, người dùng máy tính bắt đầu chia sẻ các tập tin bằng cách dùng các modem kết nối với các máy tính khác. Cách này được gọi là điểm nối điểm hoặc truyền theo kiểu quay số. Khái niệm này được mở rộng thông qua cách dùng các máy tính trung tâm truyền tin trong một kết nối quay số. Các máy tính đó được gọi là sàn thông báo (Bulletin Board). Các người dùng kết nối đến đây, để lại hoặc lấy đi các thông điệp hoặc gửi lên hay tải về các tập tin. Tuy nhiên, hạn chế của cách này là có rất ít hướng truyền tin. Ngoài ra, các máy tính tại sàn thông báo cần một modem để cho mỗi kết nối, khi số lượng trở nên quá nhiều thì hệ thống sẽ không đáp ứng được.

Qua các thập niên 1950, 1970, 1980, 1990, Bộ Quốc phòng Hoa Kỳ đã phát triển các mạng diện rộng WAN có độ tin cậy cao nhằm phục vụ các mục đích quân sự và khoa học. WAN là công nghệ truyền tin điểm nối điểm, nó cho phép nhiều máy tính kết nối lại với nhau bằng các đướng dẫn khác nhau. Bản than mạng sẽ xác định dữ liệu di chuyển từ máy tính này đến máy tính khác như thế nào. Sau này, WAN đã trở thành Internet.

* + - 1. Thách thức và lợi ích của mạng máy tính

Thách thức:

* Lạm dụng hệ thống mạng để làm điều phi pháp: tin tặc, ăn cắp tài sản công dân, ăn cắp thông tin cá nhân hoặc thẻ ngân hàng,…
* Các phần mềm độc hại Malware xuất hiện khắp mọi nơi.
* Khó kiểm soát được các mặt hàng buôn bán trong hệ thống mạng.
* Vấn đề trong giáo dục: không kiểm soát được thong tin các bạn trẻ đang xem, các vấn đề độc hại trên mạng,…
* Các phần mềm quảng cáo (adware) và thư rác (spam mail).

Lợi ích:

* Mọi người đều có thể sử dụng chung một phần mềm tiện ích.
* Việc trao đổi thông tin trở nên dễ dàng qua email, chat, dịch vụ truyền fiel FTP, dịch vụ web,…
* Dữ liệu được quản lý bảo mật an toàn, backup dữ liệu tốt.
* Sử dụng chung các thiết bị máy in, máy scanner, đĩa cứng và các thiết bị khác.
* Xóa bỏ rào cản về khoảng cách địa lý giữa các máy tính trong hệ thống mạng.
* An toàn cho dữ liệu và phầm mềm nhờ có dự quản lý quyền truy cập của các tài khoản người dùng.
  + - 1. Phân loại mạng

LAN

LAN – Local Area Network hay còn gọi là mạng cục bộ, là mạng tư nhân trong một tòa nhà, một khu vực trong khoảng vài km. LAN nối các máy chủ và các trạm trong các văn phòng và nhà máy để chia sẻ tài nguyên và trao đổi thông tin. LAN có 3 đặc điểm:

* Phạm vi hoạt động từ từ vài mét đến 1km.
* Thường dùng kỹ thuật đơn giản chỉ có một đường dây cáp nối tất cả các máy. Vận tốc truyền dữ liệu thông thường là 10 Mbps, 100 Mbps, 1 Gbps và 100 Gbps.
* Các kiến trúc mạng của mạng LAN:
  + Mạng bus hay mạng tuyến tính. Các máy nối nhau một cách liên tục thành một hàng từ máy này sang máy khác. Ví dụ: Ethernet (IEEE 802.3).
  + Mạng vòng. Các máy nối nhau một cách liên tục thành một hàng từ máy này sang máy khác nhưng đến máy cuỗi lại được nối ngược trở về máy đầu tiên tạo thành vòng kín. Ví dụ: IBM token ring.
  + Mạng sao

MAN

MAN – Metropolitan Area Network hay còn gọi là mạng đô thị, là mạng có cở lớn hơn LAN với phạm vi vài km. Nó có thể bao gồm các văn phòng trong cùng một thành phố và có thể là công cộng hoặc tư nhân. MAN có các đặc điểm:

* Chỉ có tối đa hai dây cáp nối
* Không dùng các kỹ thuật nối chuyển.
* Có thể hỗ trợ chung vận chuyển dữ liệu và đàm thoại, truyền hình. Ngày nay, cáp quang (Fiber Optical) được sử dụng nhiều để truyền tín hiệu. Vận tốc hiện nay có thể đạt đến 10 Gbps.

WAN

WAN – Wide Are Network hay còn gọi là mạng diện rộng, là mạng dùng trong vùng địa lý lớn như quốc gia, châu lục hay cả lục địa và có phạm vi từ vài tram đến vài ngàn km. WAN bao gồm tập hợp các máy chạy các chương trình cho người dùng. Các máy này được gọi là máy lưu trữ (host) hoặc máy chủ, máy đầu cuối (end system). Các máy chính được nối với nhau bằng mạng truyền thông con (communication subnet) hay là mạng con (subnet). Nhiệm vụ của các mạng con là truyền tải các thông điệp (message) từ máy chủ này sang máy chủ khác.

Mạng con bao gồm:

* Các đường dây vận chuyển còn gọi là mạch (circuit), kênh (channel), đường trung chuyển (trunk).
* Các thiết bị nối chuyển. Đây là loại máy tính chuyện biệt hoá dùng để nối hai hay nhiều đường trung chuyển nhằm di chuyển các dữ liệu giữa các máy. Khi dữ liệu đến trong các đường vô, thiết bị nối chuyển này phải chọn (theo thuật toán đã định) một đường dây ra để gửi dữ liệu đó đi. Tên gọi của thiết bị này là [nút chuyển gói](https://vi.wikipedia.org/w/index.php?title=N%C3%BAt_chuy%E1%BB%83n_g%C3%B3i&action=edit&redlink=1) (packet switching node) hay [hệ thống trung chuyển](https://vi.wikipedia.org/w/index.php?title=H%E1%BB%87_th%E1%BB%91ng_trung_chuy%E1%BB%83n&action=edit&redlink=1) (intermediate system). Máy tính dùng cho việc nối chuyển gọi là "bộ chọn đường" hay "bộ định tuyến" (router).

Chart, bubble chart

Description automatically generated

Hầu hết các WAN bao gồm nhiều đường cáp hay là đường dây điện thoại, mỗi đường dây nối với một cặp bộ định tuyến. Nếu hai bộ định tuyến không nối chung đường dây thì sẽ liên lạc với nhau bằng cách gián qua nhiều bộ định tuyến trung gian khác.

Có nhiều kiểu cấu hình cho WAN dùng nguyên lý điểm tới như là dạng sao, dạng vòng, dạng cây, dạng hoàn chỉnh hay bất định.

* + 1. Khái niệm mạng wifi

WIFI là viết tắt của Wireless Fidelity được hiểu là sử dụng sóng vô tuyến để truyền tín hiệu. Loại sóng này có khả năng kết nối với các mạng khác hoặc với máy tính bằng sóng vô tuyến. Nó tương tự như sóng điện thoại, truyền hình, radio. Hầu hết các thiết bị điện tử hiện nay đều có thể kết nối wifi để truy cập mạng.

Kết nối wifi hiện nay được dựa trên chuẩn liên kết IEEE 802.11 và chạy trên băng tần 54Mbps với quy mô phát tín hiệu trong vòng 30km với điều kiện không có vật cản vì khi có vật cản sẽ làm giảm tốc độ truyền dẫn tín hiệu đi nhiều.

* + - 1. Nguyên lý hoạt động

Nguyên lý hoạt động của wifi gồm 4 thành phần:

* Đường truyền mạng: là kết nối internet băng thông rộng. Với kết nối này, tốc độ sẽ nhanh hơn so với dịch vụ kết nối quay số.
* Cổng mạng: Cổng mạng này có nhiệm vụ ngăn chặn những người truy cập vào wifi của bạn mà không được phép. Và đồng thời nó cung cấp cho bạn những công cụ trong việc quản lý như: kiểm tra mạng và các dịch vụ khác thông qua IP.
* Mạng LAN không dây: Là một hệ thống kết nối máy tính của bạn với các thiết bị khác bằng sóng vô tuyến.
* Kết nối Adapter không dây: Đây là phương tiện để người khác có thể truy cập vào Wifi của bạn. Adapter không dây có thể được tích hợp sẵn, hoặc là một thiết bị rời được cắm vào máy tính.
  + - 1. Ưu và nhược điểm

Ưu điểm của mạng không dây:

* Chi phí lắp đặt giảm đáng kể so với mạng có dây.
* Công nghệ mạng không dây được tích hợp cho tất cả các thiết bị dị động cũng như máy tính xách tay. Đảm bảo tất cả mọi tiết bị đều có tính năng kết nối mạng không dây.
* Mạng không dây tạo được sự thoải mái trong việc truyền tải dữ liệu mà không có sự ràng buộc về khoảng cách và không gian giữa các thiết bị. Chỉ cần di chuyển ở bất kì nơi nào trong phạm vi phủ sóng.
* Mạng không dây sử dụng sóng hồng ngoại và sóng radio để truyền dữ liệu giữa các thiết bị. Sóng radio truyền tín hiệu đi xa hơn, lâu và rộng hơn, băng thông cao hơn. Vì vậy sóng radio được sử dụng rộng rãi hơn tia hồng ngoại.

Nhược điểm của mạng không dây:

* Tốc độ mạng không dây phụ thuộc vào băng thông, và tốc độ này thường thấp hơn mạng có dây.
* Rất khó quản lý thông tin và có khả năng đánh rơi dữ liệu trên đường truyền.
  + - 1. Các mô hình mạng wifi

Mô hình mạng độc lập (Ad-hoc)

Mạng IBSSs (Independent Basic Service Set) hay còn gọi là mạng ad-hoc, trong mô hình mạng ad-hoc các client liên lạc trực tiếp với nhau mà không cần thông qua AP nhưng phải ở trong phạm vi cho phép.

Các nút di động (máy tính có hỗ trợ card mạng không dây) tập trung lại trong một không gian nhỏ để hình thành nên kết nối ngang cấp (peer-to-peer) giữa chúng. Các nút di động có card mạng wireless là chúng có thể trao đổi thông tin trực tiếp với nhau , không cần phải quản trị mạng. Mô hình mạng nhỏ nhất trong chuẩn 802.11 là 2 máy client liên lạc trực tiếp với nhau.

Mô hình mạng Ad-hoc này có nhược điểm lớn về vùng phủ sóng bị giới hạn, mọi người sử dụng đều phải nghe được lẫn nhau.

Diagram

Description automatically generated

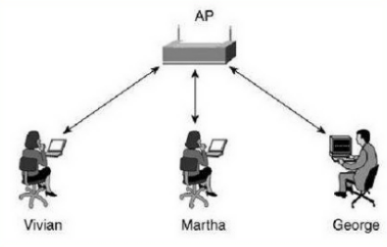
Diagram

Description automatically generated

Mô hình mạng cơ sở

The Basic Service Sets (BSS) là một topology nền tảng của mạng 802.11. Các thiết bị giao tiếp tạo nên một BSS với một AP duy nhất với một hoặc nhiều client.

BSS bao gồm các điểm truy nhập AP (Access Point) gắn với mạng đường trục hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell. AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng. Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP. Các cell có thể chồng lấn lên nhau khoảng 10-15 % cho phép các trạm di động có thể di chuyển mà không bị mất kết nối vô tuyến và cung cấp vùng phủ sóng với chi phí thấp nhất. Các trạm di động sẽ chọn AP tốt nhất để kết nối. Một điểm truy nhập nằm ở trung tâm có thể điều khiển và phân phối truy nhập cho các nút tranh chấp, cung cấp truy nhập phù hợp với mạng đường trục, ấn định các địa chỉ và các mức ưu tiên, giám sát lưu lượng mạng, quản lý chuyển đi các gói và duy trì theo dõi cấu hình mạng.



Diagram

Description automatically generated

Mô hình mạng mở rộng:

Mạng 802.11 mở rộng phạm vi di động tới một phạm vi bất kì thông qua ESS. Trong khi một BSS được coi là nền tảng của mạng 802.11, một mô hình mạng mở rộng ESS (extended service set) của mạng 802.11 sẽ tương tự như là một tòa nhà được xây dựng bằng đá. Một ESS là một tập hợp các BSSs nơi mà các Access Point giao tiếp với nhau để chuyển lưu lượng từ một BSS này đến một BSS khác để làm cho việc di chuyển dễ dàng của các trạm giữa các BSS. Access Point thực hiện việc giao tiếp thông qua hệ thống phân phối. Hệ thống phân phối là một lớp mỏng trong mỗi Access Point mà nó xác định đích đến cho một lưu lượng được nhận từ một BSS. Hệ thống phân phối được tiếp sóng trở lại một đích trong cùng một BSS, chuyển tiếp trên hệ thống phân phối tới một Access Point khác, hoặc gởi tới một mạng có dây tới đích không nằm trong ESS. Các thông tin nhận bởi Access Point từ hệ thống phân phối được truyền tới BSS sẽ được nhận bởi trạm đích.

Diagram

Description automatically generated

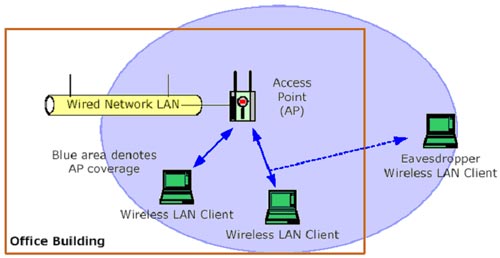
Diagram

Description automatically generated

* + 1. Khái niệm an toàn bảo mật không dây

Để kết nối tới một mạng LAN hữu tuyến ta cần phải truy cập theo đường truyền bằng dây cáp, phải kết nối một PC vào một cổng mạng. Với mạng không dây ta chỉ cần có máy của ta trong vùng sóng bao phủ của mạng không dây. Điều khiển cho mạng có dây là đơn giản: đường truyền bằng cáp thông thường được đi trong các tòa nhà cao tầng và các port không sử dụng có thể làm cho nó disable bằng các ứng dụng quản lý.

Các mạng không dây (hay vô tuyến) sử dụng sóng vô tuyến xuyên qua vật liệu của các tòa nhà và như vậy sự bao phủ là không giới hạn ở bên trong một tòa nhà. Sóng vô tuyến có thể xuất hiện trên ñường phố, từ các trạm phát từ các mạng LAN này, và như vậy ai đó có thể truy cập nhờ thiết bị thích hợp. Do đó mạng không dây của một công ty cũng có thể bị truy cập từ bên ngoài tòa nhà công ty của họ.



Để cung cấp mức bảo mật tối thiểu cho mạng WLAN thì ta cần hai thành phần sau:

* Cách thức để xác định ai có quyền sử dụng WLAN - yêu cầu này được thỏa mãn bằng cơ chế xác thực(authentication).
* Một phương thức để cung cấp tính riêng tư cho các dữ liệu không dây – yêu cầu này được thỏa mãn bằng một thuật toán mã hóa (encryption).

Để có thể phòng thủ đối với các sự tấn công, bạn phải hiểu các kiểu đe dọa đến sự bảo mật mạng của bạn. Có 4 mối đe dọa bảo mật:

* Mối đe dọa ở bên trong.
* Mối đe dọa ở bên ngoài.
* Mối đe dọa không có cấu trúc.
* Mối đe dọa có cấu trúc.
  + - 1. Các hình thức tấn công mạng WLAN

Các hình thức tấn công Wlan.

* Tấn công giả mạo (Rogue access point): một client tấn công bên ngoài giả mạo là máy bên trong mạng, xin kết nối vào mạng. Bằng cách giả mạo địa chỉ MAC, địa chủ IP của thiết bị mạng để xin vào kết nối bên trong.

Diagram, timeline

Description automatically generated

* Tấn công yêu cầu xác thực lại (De-authentication flood attack): Mục tiêu tấn công là các người dùng trong mạng wireless và các kết nối của họ. Chèn các frame yêu cầu xác thực lại vào mạng WLAN bằng cách giả mạo địa chỉ MAC nguồn và đích.

Diagram

Description automatically generated

* Tấn công bị động (Passive attack): hacker lắng nghe mọi dữ liệu lưu thông trên mạng. Thu thập password từ những địa chỉ HTTP, email, instant message, FTP session, telnet,…

Diagram

Description automatically generated

* Tấn công chủ động (Active attack): tấn công chủ động có thể sử dụng để truy cập vào server và lấy được những dữ liệu có giá trị hay sử dụng đường kết nối Internet.

Diagram, schematic

Description automatically generated

* Tấn công kiểu chèn ép (Jamming attack): sử dụng bộ phát tín hiệu RF công suất cao hay sweep generator để làm nghẽn tín hiệu của AP.

Diagram, schematic

Description automatically generated

* Tấn công kiểu thu hút (Man in the middle attack): hacker sử dụng một AP để đánh cắp các node di động bằng cách giới thiệu RF mạnh hơn cho AP hợp pháp. Có thể thực hiện chỉ với một laptop và hai PCMCIA card.

Diagram

Description automatically generated

* Fake access point.

Diagram

Description automatically generated

* Tấn công dựa trên sự cảm nhận lớp vật lý: kẻ tấn công lợi dụng giao thức chống đụng độ CSMA/CA làm cho tất cả người dùng nghĩ rằng lúc nào trong mạng củng có một máy tính đang truyền thông. Điều này làm cho các máy tính khác luôn luôn ở trạng thái chờ đợi kẻ tấn công ấy truyền dữ liệu xong nên dẫn đến tình trạng nghẽn trong mạng.
* Tấn công ngắt kết nối (Disassociation flood attack).

Diagram

Description automatically generated

* + - 1. Các phương pháp bảo mật cơ bản

Để cung cấp mức độ bảo mật tối thiểu cho mạng WLAN ta cần hai thành phần sau:

Diagram

Description automatically generated

Mã hóa là biến đổi dữ liệu để chỉ có các thành phần được xác nhận mới có thể giải mã được nó. Quá trình mã hóa là kết hợp plaintext với một khóa để tạo thành văn bản mật (Ciphertext). Sự giải mã được bằng cách kết hợp Ciphertext với khóa để tái tạo lại plaintext gốc. Quá trình xắp xếp và phân bố các khóa gọi là sự quản lý khóa.

Diagram

Description automatically generated

Có 2 loại mật mã:

* Mật mã dòng (stream ciphers).

Diagram

Description automatically generated

* Mật mã khối (block ciphers).

Diagram

Description automatically generated

Giống nhau: hoạt động bằng cách sinh ra một chuỗi khóa (key stream) từ một giá trị khóa bí mật. Chuỗi khóa này được trộn với dữ liệu (plaintext) 🡪 ciphertext.

Khác nhau: kích thước của dữ liệu mà mỗi loại mật mã thao tác tại một thời điểm khác nhau

Các giải pháp bảo mật mạng WLAN:

WEP – Wried Equivalent Privacy:

Diagram

Description automatically generated

Diagram

Description automatically generated

* Chuẩn 802.11 cung cấp tính riêng tư cho dữ liệu bằng thuật toán WEP. WEP dựa trên mật mã dòng đối xứng RC4(Ron’s code 4) được Ron Rivest thuộc hãng RSA Security Inc phát triển.
* Một giá trị có tên Initialization Vector (IV) được sử dụng để cộng thêm với khóa nhằm tạo ra khóa khác nhau mỗi lần mã hóa.
* Hiện nay, trên Internet đã sẵn có những công cụ có khả năng tìm khóa WEP như AirCrack, AirSnort, dWepCrack, WepAttack, WepCrack, WepLab.

WLAN VPN – Virtual Private Networking

* Mạng riêng ảo VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chắn dữ liệu khỏi các truy cập trái phép. VPN tạo ra một tin cậy cao thông qua việc sử dụng một cơ chế bảo mật như IPSec (Internet Protocol Security). IPSec dùng các thuật toán mạnh như Data Encryption Standard (DES) và Triple DES (3DES) để mã hóa dữ liệu, và dùng các thuật toán khác để xác thực gói dữ liệu.
* Khi được sử dụng trên mạng WLAN, cổng kết nối của VPN đảm nhận việc xác thực, đóng gói và mã hóa.

Diagram

Description automatically generated

TKIP – Temporal Key Integrity Protocol

* Là giải pháp của IEEE được phát triển năm Là một nâng cấp cho WEP nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm (hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC (message integrity check) để đảm bảo tính chính xác của gói tin. TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo.

Diagram

Description automatically generated

AES – Advanced Encryption Standard

* Là một chức năng mã hóa được phê chuẩn bởi NIST (Nation Instutute of Standard and Technology). IEEE đã thiết kế một chế độ cho AES để đáp ứng nhu cầu của mạng WLAN. Chế độ này được gọi là CBC-CTR (Cipher Block Chaining Counter Mode) với CBC-MAC (Cipher Block Chaining Message Authenticity Check). Tổ hợp của chúng được gọi là AES-CCM. Chế độ CCM là sự kết hợp của mã hóa CBC-CTR và thuật toán xác thực thông điệp CBC-MAC. Sự kết hợp này cung cấp cả việc mã hóa cũng như kiểm tra tính toàn vẹn của dữ liệu gửi.
* AES-CCM yêu cầu chi phí khá lớn cho cả quá trình mã hóa và kiểm tra tính toàn vẹn của dữ liệu gửi nên tiêu tốn rất nhiều năng lực xữ lý của CPU khá lớn.

802.1x và EAP

- 802.1x: Là chuẩn đặc tả cho việc truy cập dựa trên cổng (port-based) được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn(blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.

- EAP: EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng (password, cetificate,…), giao thức được sử dụng (MD5, TLS\_Transport Layer Security, OTP\_ One Time Password,…) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.

Diagram

Description automatically generated

A close-up of a document

Description automatically generated with low confidence

WPA – WiFi Protected Access

- Cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP. WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin.

- WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền.

- WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu.

WPA 2.

* Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit.

Lọc – Filtering

* Lọc là cơ chế bảo mật cơ bản có thể sử dụng cùng với WEP. Lọc hoạt động giống như Access list trên router, cấm những cái không mong muốn và cho phép những cái mong muốn. Có 3 kiểu lọc cơ bản có thể được sử dụng trong wireless lan:
  + Lọc SSID: là một phương thức cơ bản của lọc và chỉ nên được sử dụng cho việc điều khiển truy cập cơ bản. - SSID của client phải khớp với SSID của AP để có thể xác thực và kết nối với tập dịch vụ. SSID được quảng bá mà không được mã hóa trong các Beacon nên rất dễ bị phát hiện bằng cách sử dụng các phần mềm.

Graphical user interface, text, application

Description automatically generated

* + Lọc địa chỉ MAC: Hầu hết các AP đều có chức năng lọc địa chỉ MAC. Người quản trị có thể xây dựng danh sách các địa chỉ MAC được cho phép Nếu client có địa chỉ MAC không nằm trong danh sách lọc địa chỉ MAC của AP thì AP sẽ ngăn chặn không cho phép client đó kết nối vào mạng Nếu công ty có nhiều client thì có thể xây dựng máy chủ RADIUS có chức năng lọc địa chỉ MAC thay vì AP. Cấu hình lọc địa chỉ MAC là giải pháp bảo mật có tính mở rộng cao.

Diagram

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* + Lọc giao thức: Mạng Lan không dây có thể lọc các gói đi qua mạng dựa trên các giao thức từ lớp 2 đến lớp 7. Trong nhiều trường hợp người quản trị nên cài đặt lọc giao thức trong môi trường dùng chung.

Table

Description automatically generated

* 1. Các thiết bị xây dựng mạng

Thiết bị mạng là tập hợp nhiều thiết bị dùng để kết nối 1 hoặc nhiều mạng LAN với nhau. Chúng hoàn toàn có khả năng kết nối được nhiều segment lại với nhau. Tuy nhiên, số lượng bao nhiêu thì còn phụ thuộc vào số lượng cổng trên thiết bị đó cũng như những thiết bị sử dụng trong mạng.

Để cho dòng dữ liệu giữa hai phần mạng có thể truyền qua lại cho nhau được người ta sử dụng các thiết bị liên kết đặc biệt hay còn gọi là các thiết bị mạng. Một số thiết bị mạng cơ bản mà bạn có thể gặp như: Card Mạng, hub, switch, bridge, router, gateway…

Tùy theo những đặc điểm giống và khác nhau giữa hai phần mạng cần liên kết, có thể thực hiện được bằng cách chọn các loại thiết bị liên kết cho phù hợp trong số các loại kết nối như bộ lặp (repeater), cầu nối (bridge), router và gateway. Những thiết bị liên kết này được chọn theo nhiệm vụ của chúng theo mô hình ISO/OSI.

* + 1. Card mạng

Card mạng hay còn gọi là card dùng để giao tiếp với internet (network card) là một loại bảng mạch giúp cho máy tính có thể giao tiếp với các máy khác thông qua mạng internet, hay còn được gọi với cái tên LAN adapter. Card mạng được cắm trong bo mạch chính của máy tính, giúp máy tính giao tiếp và kết nối với môi trường mạng.



Card mạng được chia làm 2 loại: Card on board và card rời.

* Card on board (tích hợp thẳng vào mainboard). Thường loại này khi hỏng thay thế rất phức tạp nhưng đổi lại nhỏ gọn và giá thành thấp hơn so với card rời.
* Card rời thường được gắn bổ sung vào máy tính thông qua cổng PCI, USB. Nó kết nối thông qua cổng USB dễ cắm, nhỏ gọn và dùng ngay. Card rời có giá cao hơn nhiều, thích hợp với máy xách tay hơn, cho nên đối với người dùng PC thì card PCI vẫn là lựa chọn số một.

Card mạng giúp máy tính chuẩn bị dữ liệu để đưa lên mạng hay nhận dữ liệu từ mạng về máy tính, dữ liệu phải được chuyển đổi từ dạng byte, bit sang loại tín hiệu điện để có thể truyền qua dây cáp và ngược lại nếu như máy tính muốn nhận dữ liệu từ mạng về. Nó giúp các máy tính giao tiếp với nhau truyền dữ liệu qua lại giữa các máy tính, kiểm soát thống kê dữ liệu từ cấp tới máy tính.

Địa chỉ IP:

Địa chỉ IP (Internet Protocol) là địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để bắt tay và liên lạc với nhau theo giao thức Internet trên mạng máy tính. Ip có 2 phiên bản là Ipv4 và Ipv6.

* Ipv4: Địa chỉ IP được sử dụng theo phiên bản IPv4 sử dụng 32bit để mã hoá dữ liệu. Ví dụ địa chỉ IP: 192.168.1.1
* Ipv6: Địa chỉ IP được sử dụng theo phiên bản IPv6 sử dụng 128bit để mã hoá dữ liệu. Ipv6 cho phép sử dụng nhiều địa chỉ hơn so với IPv4.

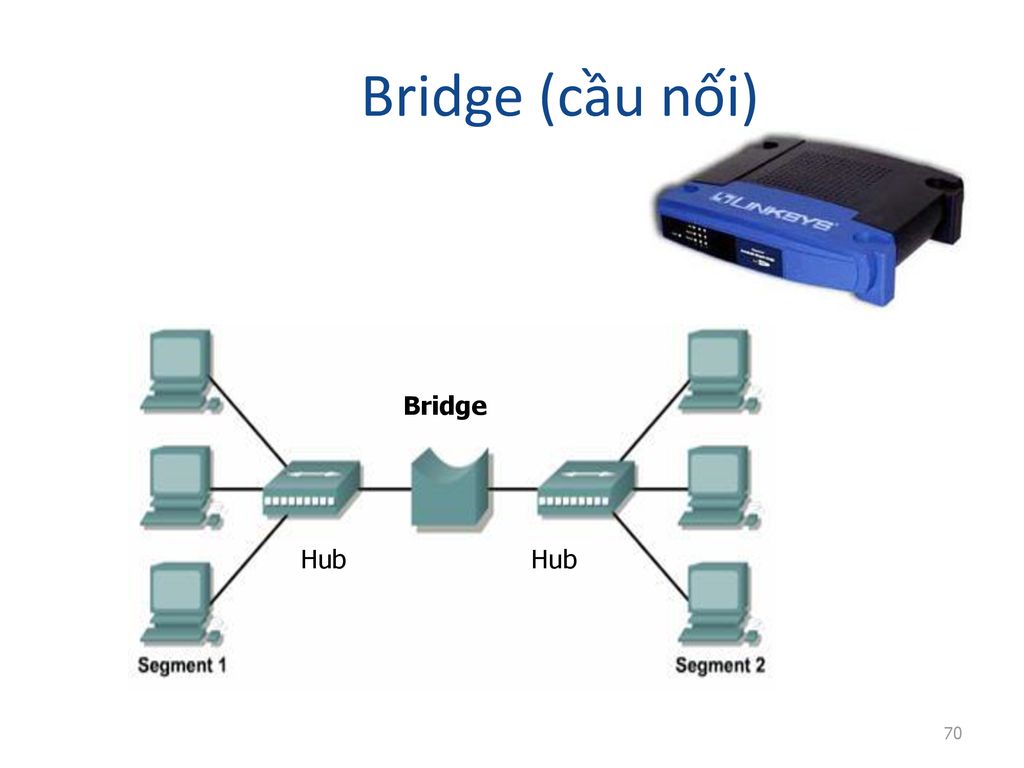
Địa chỉ MAC:

Mỗi card mạng cần có 1 địa chỉ MAC và địa chỉ đó là duy nhất không trùng lặp để nó phân biệt các card mạng với nhau trên internet, địa chỉ MAC này được cung cấp bởi IEEE (viện công nghệ điện và điện tử) và các nhà sản xuất card mạng sẽ cố định địa chỉ MAC do viện cung cấp đến các card mạng của mình sản xuất.

Địa chỉ MAC gồm 6byte (48bit) trong số đó thì 3byte là mã số của chính nhà sản xuất ra card mạng và 3byte sau là số seri của các card mạng do hãng đó sản xuất, và những người am hiểu hay gọi là địa chỉ vật lý.

* + 1. Cầu nối Bridge

Bridge là một thiết bị mạng thuộc lớp 2 của mô hình OSI (Data Link Layer). Cầu nối Bridge được sử dụng để ghép nối 2 mạng để tạo thành một mạng lớn duy nhất. Bridge được sử dụng phổ biến để làm cầu nối giữa hai mạng, nó quan sát các gói tin (packet) trên mọi mạng. Khi thấy một gói tin từ một máy tính thuộc mạng này chuyển tới một máy tính trên mạng khác, Bridge sẽ sao chép và gửi gói tin này tới mạng đích.



Chế độ làm việc của một cầu nối: đối chiếu với mô hình OSI thì một cầu nối làm việc trên cơ sở lớp LLC, tức phần trên của lớp 2. Như vậy, nó sẽ phải thực hiện các giao thức phía dưới lớp này cho cả hai phần mạng để có thể chuyển đổi các bức điện qua lại. Bản thân một cầu nối không có địa chỉ mạng riêng.

Ưu điểm của Bridge là hoạt động trong suốt các máy tính thuộc các mạng khác nhau vẫn có thể gửi các thông tin với nhau đơn giản. Một Bridge thì có thể xử lý được nhiều lưu thông trên mạng như: Banyan, Novell… cũng như là địa chỉ IP cùng một lúc.

Nhược điểm của Bridge là chỉ kết nối những mạng cùng loại và sử dụng Bridge cho những mạng hoạt động nhanh sẽ khó khăn nếu chúng không nằm gần nhau về mặt vật lý.

* + 1. Repeater

Để mở rộng khoảng cách truyền cũng như nâng cao số trạm tham gia thì cách thông thường là sử dụng các bộ lặp (repeater). Tín hiệu từ một trạm phát ra trên đường truyền khi tới các trạm khác bao giờ cũng bị suy giảm và biến dạng, ít hay nhiều tùy theo đặc tính của cáp truyền và đặc tính tần số của tín hiệu. Chính vì vậy mà có sự liên quan ràng buộc giữa tốc độ truyền (quyết định tần số tín hiệu) với chiều dài tối đa của dây dẫn.

Mặt khác, các chuẩn truyền dẫn như RS-485 cũng qui định chặt chẽ đặc tính điện học của các thiết bị ghép nối (được coi như tải), dẫn đến sự hạn chế về số trạm tham gia.



Vai trò của bộ lặp là sao chép, khuếch đại và hồi phục tín hiệu mang thông tin trên đường truyền. Hai phần mạng có thể liên kết với nhau qua một bộ lặp được gọi là các đoạn mạng (segment), chúng phải giống nhau hoàn toàn cả về tất cả các lớp giao thức và kể cả đường truyền vật lý.

Chức năng của một bộ lặp có thể coi như thuộc phần dưới của lớp vật lý nếu đối chiếu với mô hình OSI. Chú ý rằng, bộ lặp chỉ nối được hai đoạn đường dẫn của cùng một hệ thống truyền thông, thực hiện cùng một giao thức và môi trường truyền dẫn cũng hoàn toàn giống nhau.

Khác với một bộ khuếch đại tín hiệu, một bộ lặp không chỉ làm nhiệm vụ khuếch đại các tín hiệu bị suy giảm, mà còn chỉnh dạng và tái tạo tín hiệu trong trường hợp tín hiệu bị nhiễu. Một bộ lặp tuy không có một địa chỉ riêng, không tham gia trực tiếp vào các hoạt động giao tiếp nhưng vẫn được coi là một trạm, hay một thành viên trong mạng.

* + 1. Bộ chia Hub

Hub là một Repeater có nhiều cổng. Cứ một Hub có từ 4 đến 24 cổng và có thể nhiều hơn. Thường trong các trường hợp, Hub được sử dụng trong các mạng 10BASE-T hay 100BASE-T. Hub đóng vai trò là trung tâm của mạng, khi cấu hình mạng là hình sao (Star topology). Với một Hub, khi thông tin vào từ một cổng và sẽ được đưa đến tất cả các cổng khác.

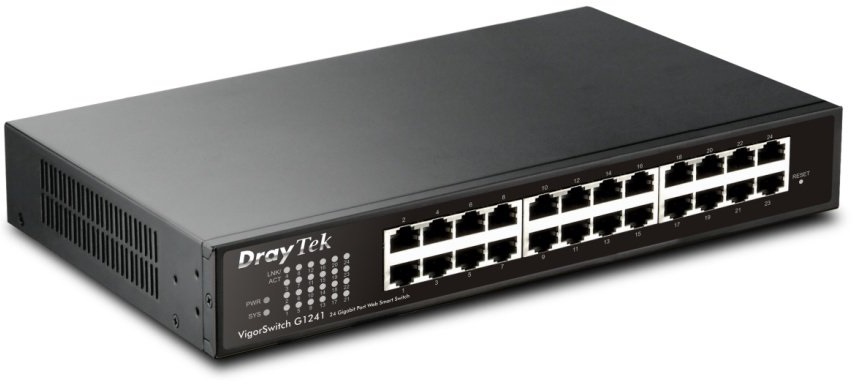


Hub có 2 loại: Active Hub và Smart Hub.

* Active Hub: Đây là loại Hub được dùng phổ biến, cần được cấp nguồn khi hoạt động, được sử dụng để khuếch đại tín hiệu đến và cho tín hiệu ra những cổng còn lại, đảm bảo mức tín hiệu cần thiết.
* Smart Hub (Intelligent Hub): Smart Hub có chức năng tương tự như Active Hub, nhưng có tích hợp thêm chip có khả năng tự động dò lỗi – rất hữu ích trong trường hợp dò tìm và phát hiện lỗi trong mạng.
  + 1. Bộ chuyển mạch Switch

Bộ chuyển mạch Switch đôi khi được mô tả như là một Bridge có nhiều cổng. Trong khi một Bridge chỉ có 2 cổng để liên kết 2 mạng với nhau, thì Switch lại có khả năng kết nối được nhiều mạng lại với nhau tuỳ thuộc vào số cổng (port) trên Switch.

Cũng giống như Bridge, Switch cũng lấy thông tin của mạng thông qua các gói tin (packet) mà nó nhận được từ các máy trong mạng. Switch sử dụng các thông tin này để xây dựng lên bảng Switch, bảng này cung cấp thông tin giúp các gói thông tin đến đúng địa chỉ.



Ngày nay, trong các giao tiếp dữ liệu, Switch thường có 2 chức năng chính là chuyển các khung dữ liệu từ nguồn đến đích, và xây dựng các bảng Switch. Switch hoạt động ở tốc độ cao hơn nhiều so với Repeater và có thể cung cấp nhiều chức năng hơn như khả năng tạo mạng LAN ảo (VLAN).

* + 1. Router

Router là một thiết bị mạng lớp 3 của mô hình OSI (Network Layer). Router giúp kết nối hai hay nhiều mạng IP với nhau. Các máy tính trên mạng phải “nhận thức” được sự tham gia của một router, nhưng đối với các mạng IP thì một trong những quy tắc của IP là mọi máy tính kết nối mạng đều có thể giao tiếp được với router.



Ưu điểm của thiết bị mạng Router: Về mặt vật lý, Router có thể kết nối với các loại mạng khác lại với nhau, từ những Ethernet cục bộ tốc độ cao cho đến đường dây điện thoại đường dài có tốc độ chậm.

Nhược điểm của thiết bị mạng Router: Router chậm hơn Bridge vì chúng đòi hỏi nhiều tính toán hơn để tìm ra cách dẫn đường cho các gói tin, đặc biệt khi các mạng kết nối với nhau không cùng tốc độ. Một mạng hoạt động nhanh có thể phát các gói tin nhanh hơn nhiều so với một mạng chậm và có thể gây ra sự nghẽn mạng. Do đó, Router có thể yêu cầu máy tính gửi các gói tin đến chậm hơn.

* + 1. Modem

Modem (modulator and demodulator) là thiết bị giao tiếp với mạng lưới của các nhà cung cấp dịch vụ Internet (ISP). Thông qua hệ thống cáp nối đồng trục hoặc cáp quang từ các trạm cung cấp Internet nối đến nhà bạn.



Modem sẽ đóng vai trò chuyển hóa các gói dữ liệu do ISP cung cấp thành kết nối Internet cho router hoặc các thiết bị có liên kết mạng khác. Trong khi đó, modem DSL (dạng quay số) kết nối trực tiếp tới đường dây điện thoại.

Modem dùng để khai thác dịch vụ Internet của các ISP cần phải đúng loại (DSL, đồng hoặc quang) mới có thể chạy với hạ tầng mà ISP cung cấp.

Ngoài ra, trên modem còn kết nối Ethernet đầu ra cho phép truyền Internet (tín hiệu Digital đã được giải mã) tới bất kỳ một router hoặc máy tính đơn lẻ ở “phía sau”.

* + 1. Gateway

Gateway được sử dụng để liên kết các hệ thống mạng khác nhau (các hệ thống bus khác nhau).



Chức năng chính của gateway là chuyển đổi giao thức ở cấp cao, thường được thực hiện bằng các thành phần phần mềm. Như vậy, gateway không nhất thiết phải là một thiết bị đặc biệt, mà có thể là một máy tính PC với các phần mềm cần thiết. Tuy nhiên, cũng có các sản phẩm phần cứng chuyên dụng thực hiện chức năng gateway.

CHƯƠNG 3: MÔ HÌNH DEMO

* 1. Mô hình đề xuất
     1. Bảng địa chỉ

3.1.1.1 Bảng địa chỉ server

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP Address** |
| Router | Gig0/0 | 203.162.0.1/24 |
| Gig0/1 | 192.168.1.1/24 |
| RADIUS Server | NIC | 192.168.1.10/24 |
| DNS Server  DHCP Server | NIC | 192.18.1.2/24 |
| Web Server | NIC | 192.168.1.3/24 |

3.1.1.2 Bảng địa chỉ tầng trệt

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP Address** |
| PC01 | NIC | DHCP |
| PC02 | NIC | DHCP |
| PC03 | NIC | DHCP |
| PC04 | NIC | DHCP |
| PC05 | NIC | DHCP |
| PC06 | NIC | DHCP |
| PC07 | NIC | DHCP |
| PC08 | NIC | DHCP |
| PC09 | NIC | DHCP |
| PC010 | NIC | DHCP |
| Printer01 | NIC | DHCP |
| Tablet PC0 | Wireless | DHCP |
| Laptop0 | Wireless | DHCP |
| Smartphone0 | Wireless | DHCP |

3.1.1.3 Bảng địa chỉ tầng 1

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP Address** |
| PC1 | NIC | DHCP |
| PC2 | NIC | DHCP |
| PC3 | NIC | DHCP |
| PC4 | NIC | DHCP |
| PC5 | NIC | DHCP |
| PC6 | NIC | DHCP |
| PC7 | NIC | DHCP |
| PC8 | NIC | DHCP |
| PC9 | NIC | DHCP |
| PC10 | NIC | DHCP |
| Printer01 | NIC | DHCP |
| Printer02 | NIC | DHCP |
| Tablet PC1 | Wireless | DHCP |
| Laptop1 | Wireless | DHCP |
| Smartphone2 | Wireless | DHCP |

3.1.1.4 Bảng địa chỉ tầng 2

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP Address** |
| PC001 | NIC | DHCP |
| PC002 | NIC | DHCP |
| PC003 | NIC | DHCP |
| PC004 | NIC | DHCP |
| PC005 | NIC | DHCP |
| Tablet PC2 | Wireless | DHCP |
| Laptop1 | Wireless | DHCP |
| Laptop2 | Wireless | DHCP |
| Smartphone3 | Wireless | DHCP |

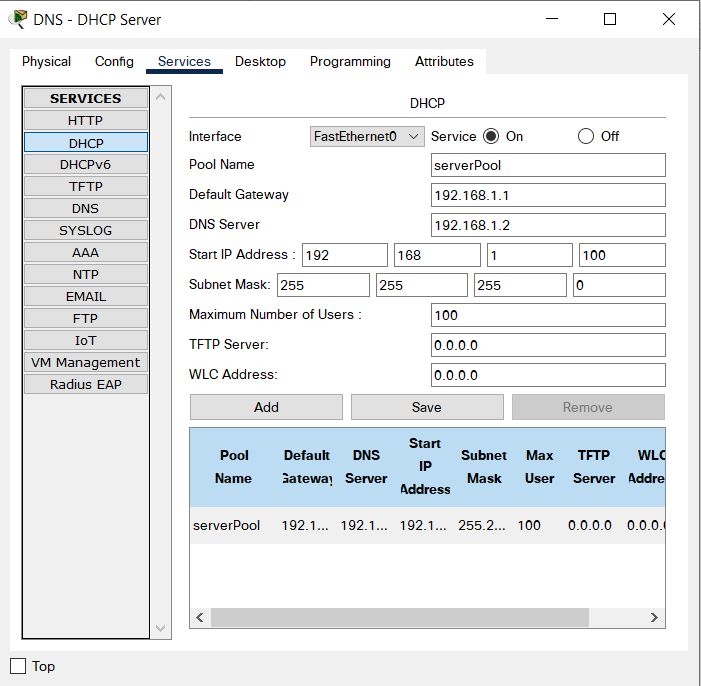
* + 1. Thông tin wireless

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Wireless** | **SSID** | **Authentication** | **Username** | **Password** |
| Tầng trệt | Tầng Trệt | WPA2-Personal | N/A | Techbase |
| Tầng 1 | Floor 1 | WPA2-Personal | N/A | TechbaseFloor1 |
| Tầng 2 | Techbase | WPA-Enterprise | admin | admin123 |

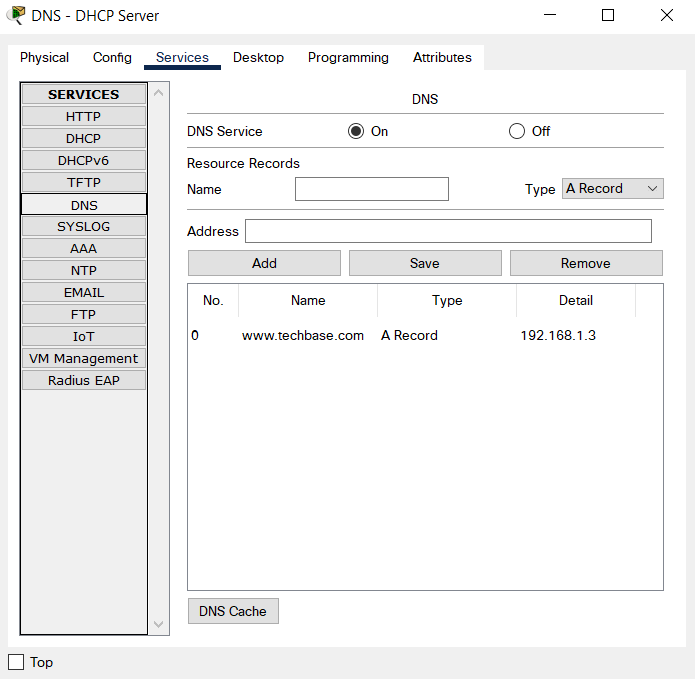
* 1. Cấu hình các thiết bị

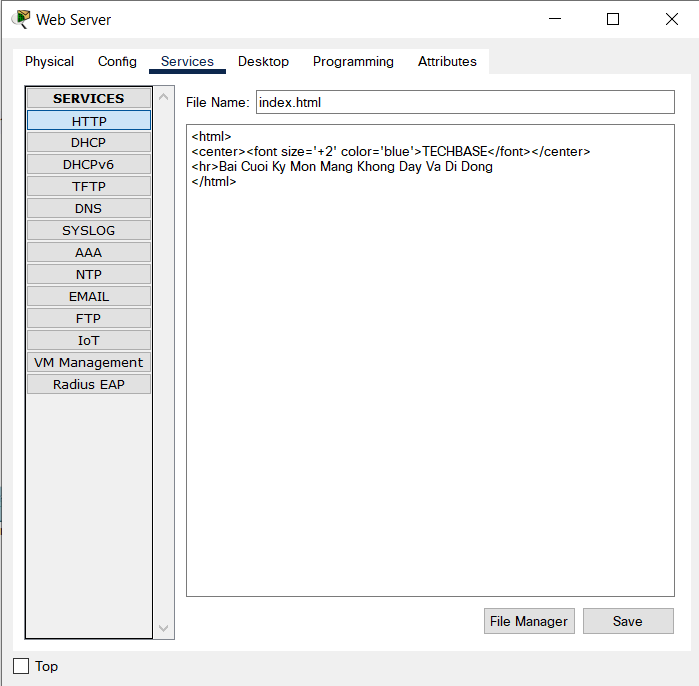
3.2.1 Cấu hình DHCP, DNS, Web và RADIUS Server

* + - 1. Cấu hình DHCP Server

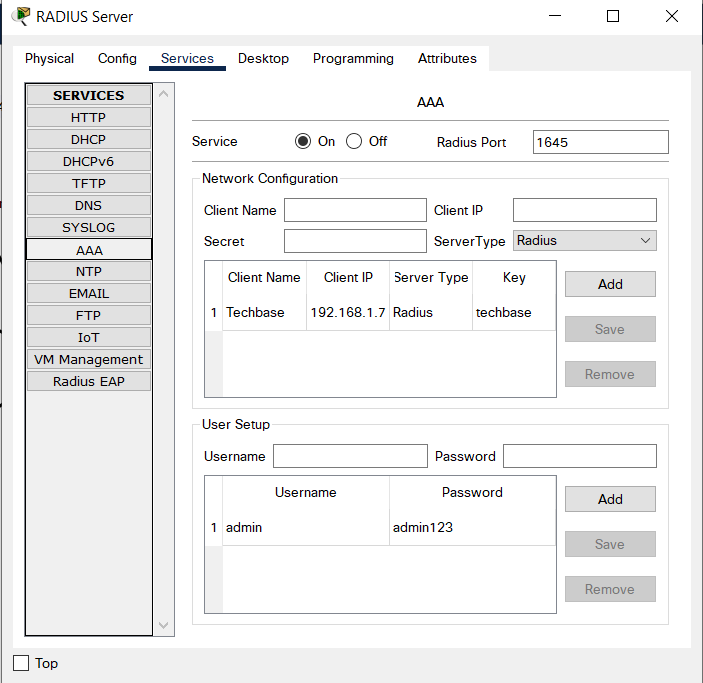


* + - 1. Cấu hình DNS và WEB Server



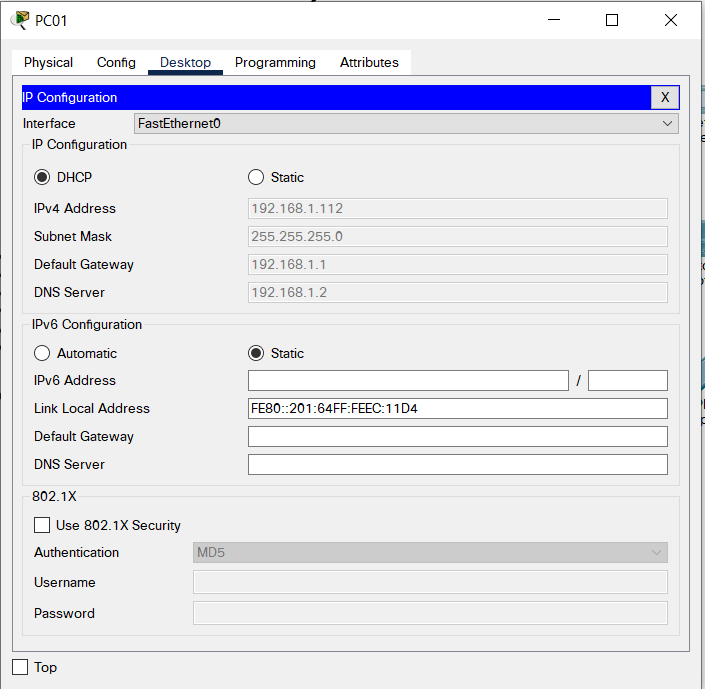


* + - 1. Cấu hình RADIUS Server

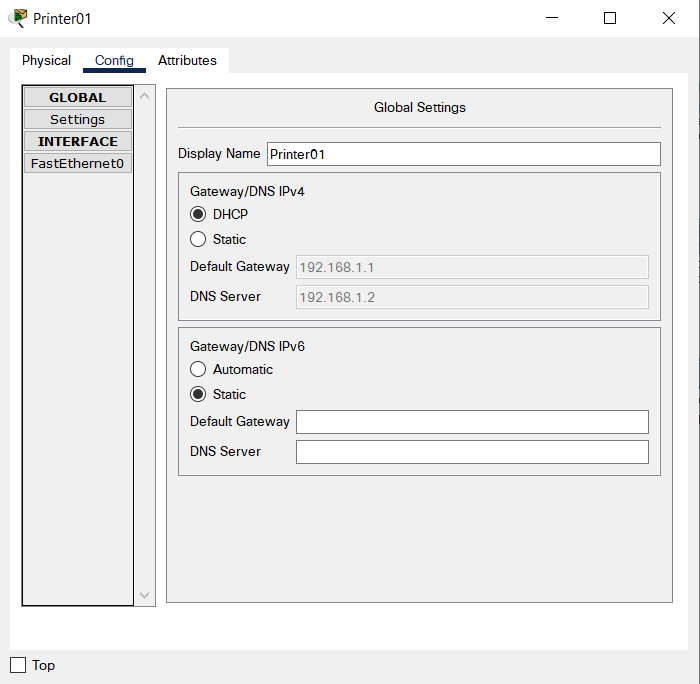


* + 1. Cấu hình tầng trệt

3.2.2.1 Cấu hình PC



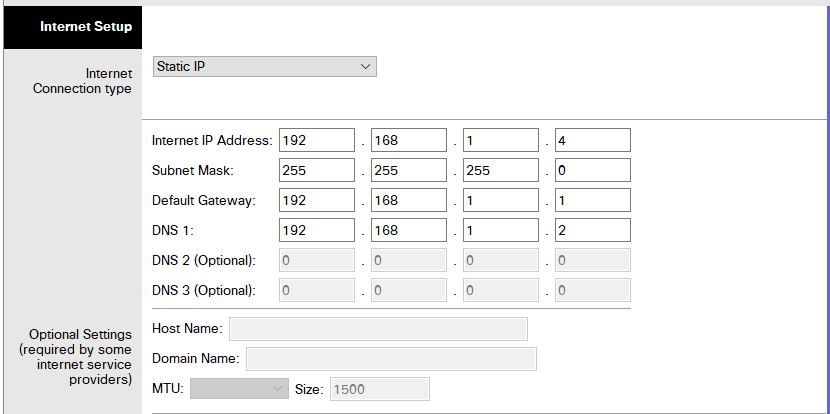
3.2.2.2 Cấu hình Printer



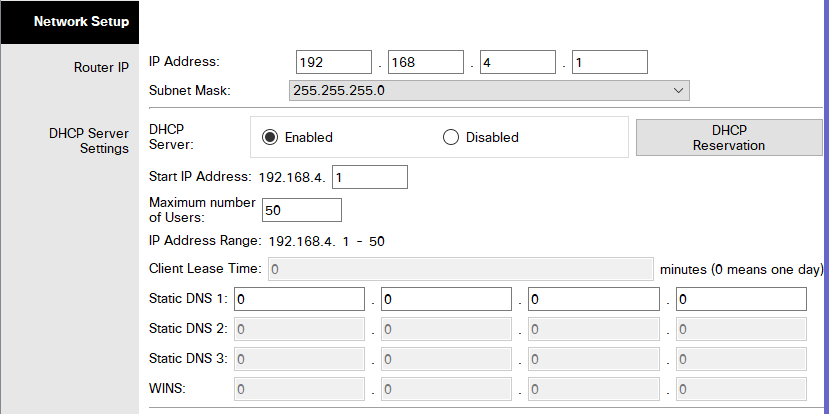
3.2.2.3 Cấu hình HomeRouter và kết nối với client

- Cấu hình HomeRouter

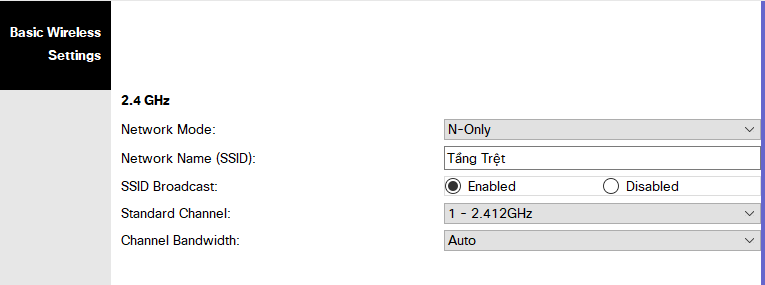
Bước 1: Thiết lập loại kết nối internet



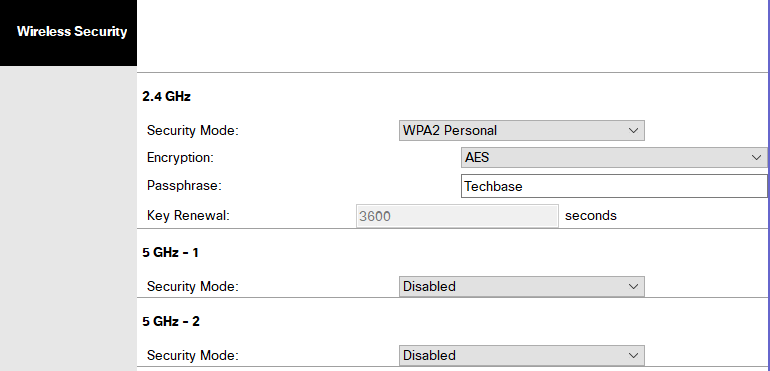
Bước 2: Thiết lập mạng



Bước 3: Thiết lập mạng không dây

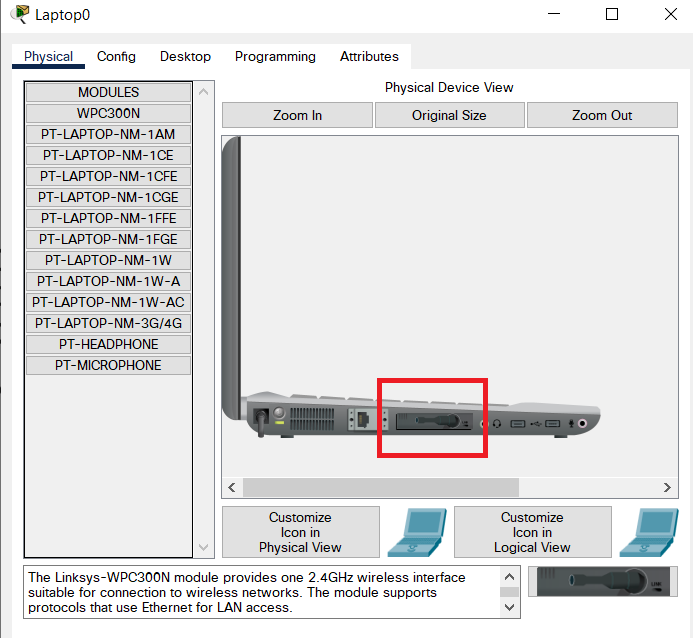


Bước 4: Thiết lập chế độ bảo mật(WPA2 Personal)

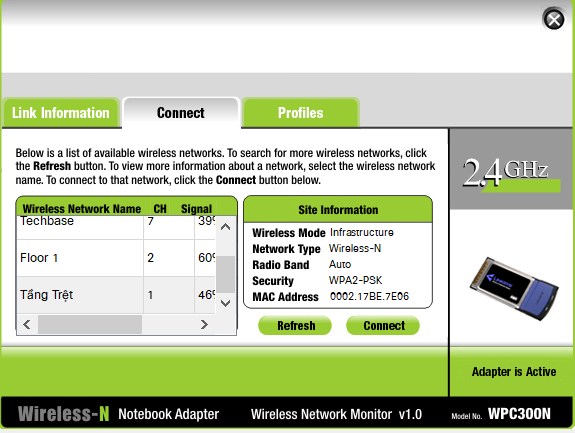


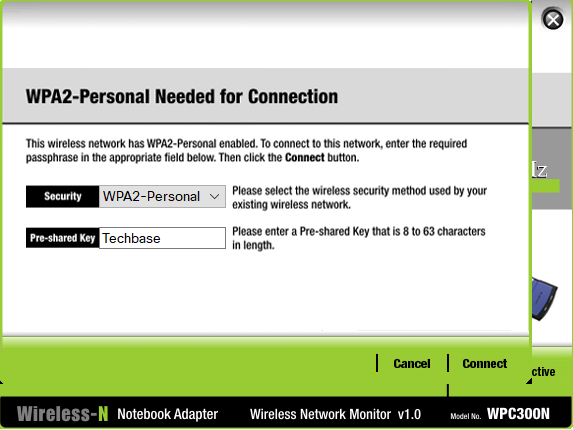
- Kết nối laptop với HomeRouter

Bước 1: Thay cổng WPC300N vào cho laptop

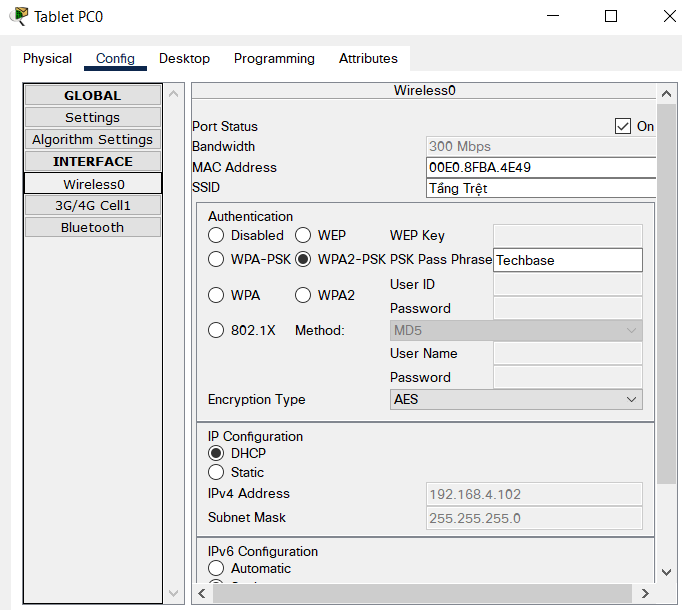


Bước 2: … làm giùm t. t chụp hình sẵn hết rồi, Hiếu ghi các bước dùm t nha

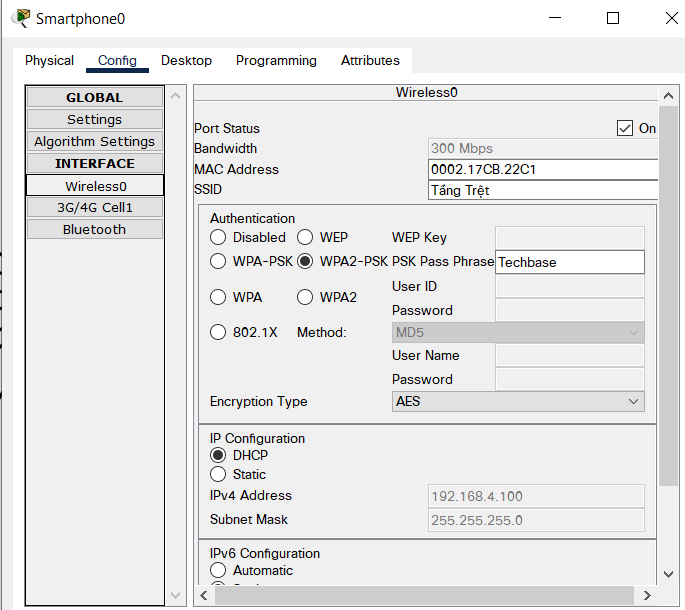




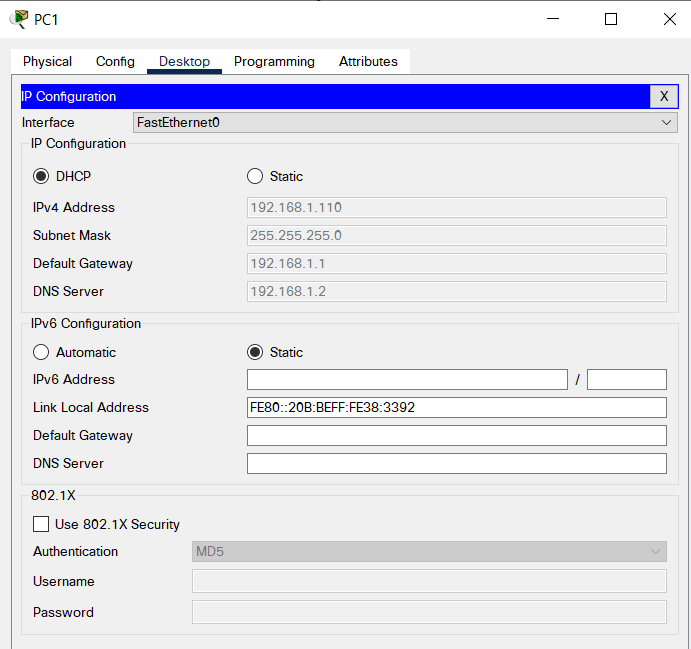
- Kết nối tablet vơi HomeRouter



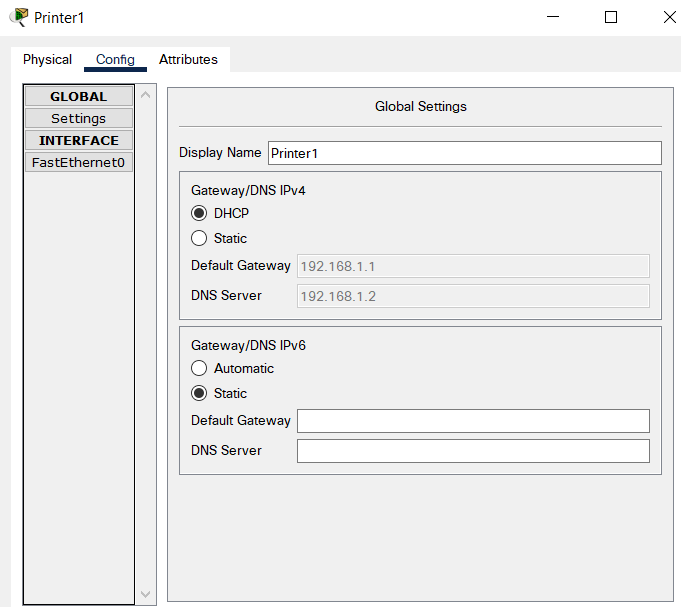
- Kết nối Smartphone với HomeRouter



* + 1. Cấu hình tầng 1
       1. Cấu hình PC



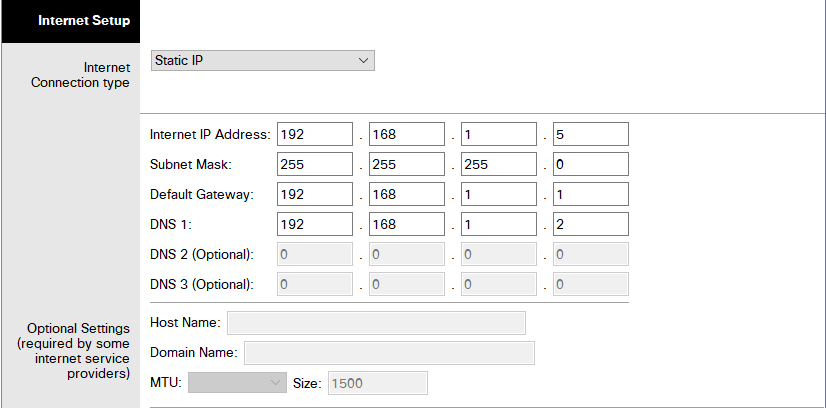
* + - 1. Cấu hình Printer

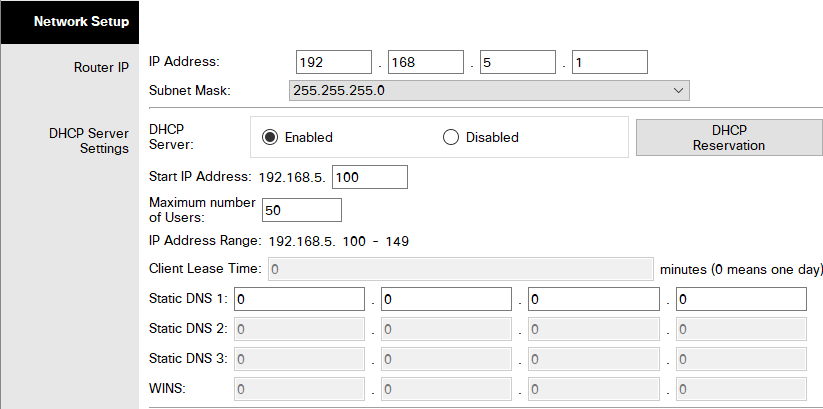


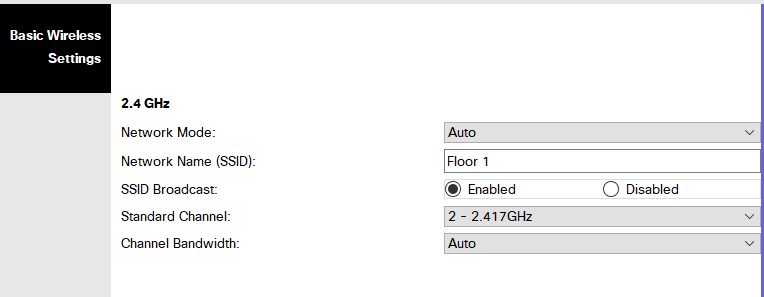
* + - 1. Cấu hình HomeRouter và kết nối với client

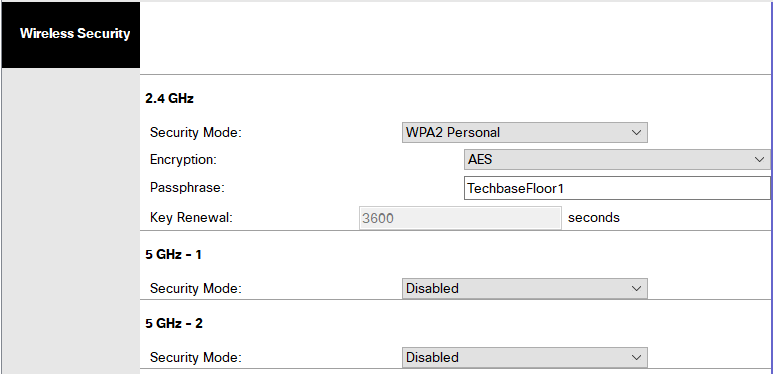
Hiếu ghi các bước theo hình giúp tao.

- Cấu hình HomeRouter

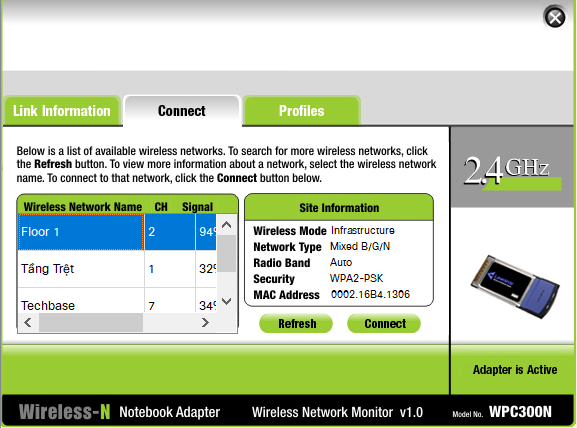


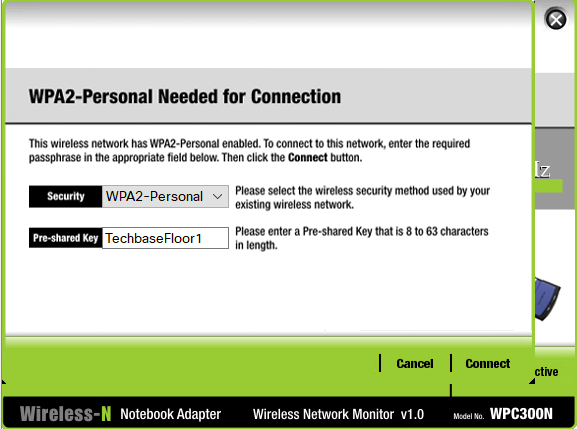




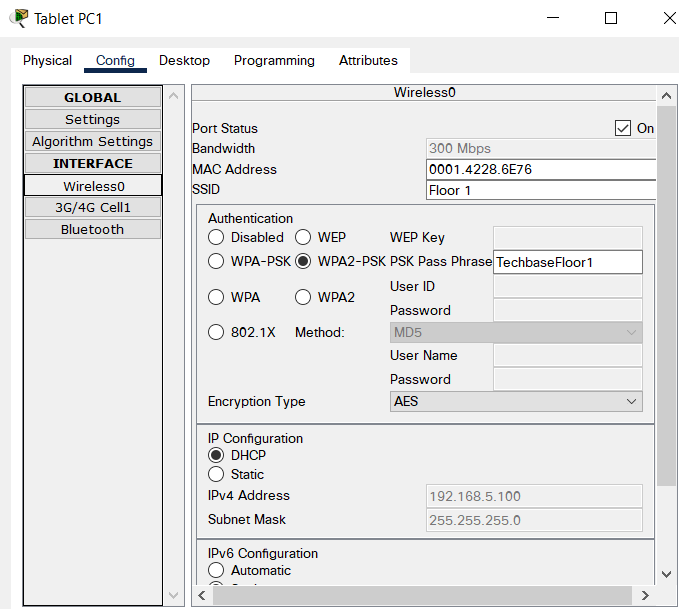


- Kết nối HomeRouter với client

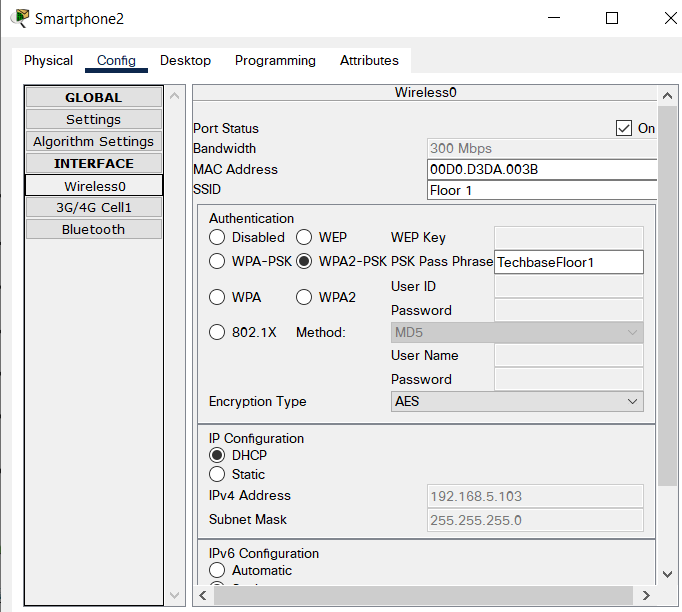




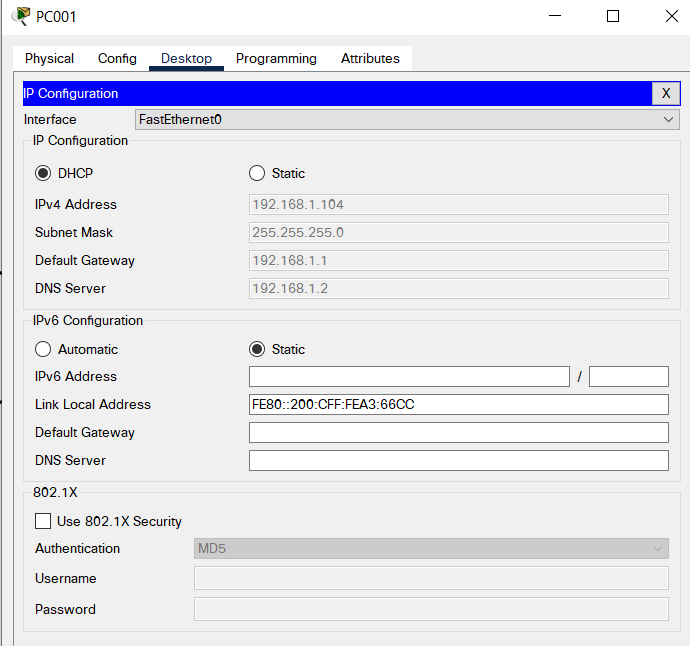
Kết nối với tablet



Kết nối vơi smartphone

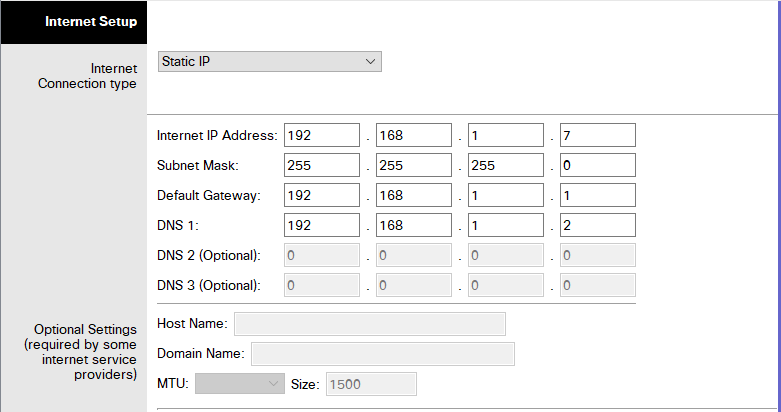


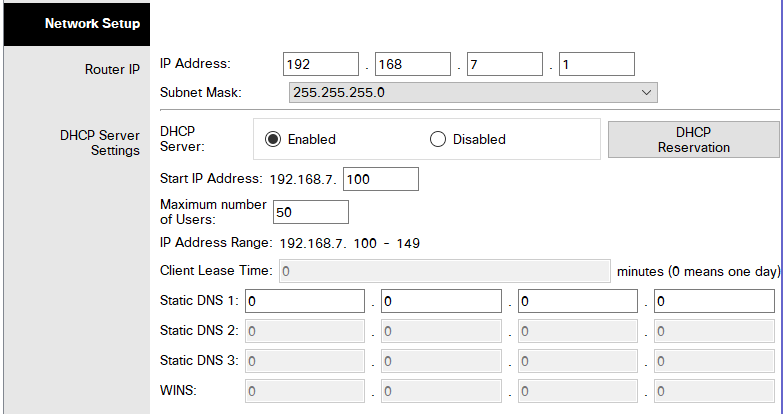
* + 1. Cấu hình tầng 2
       1. Cấu hình PC

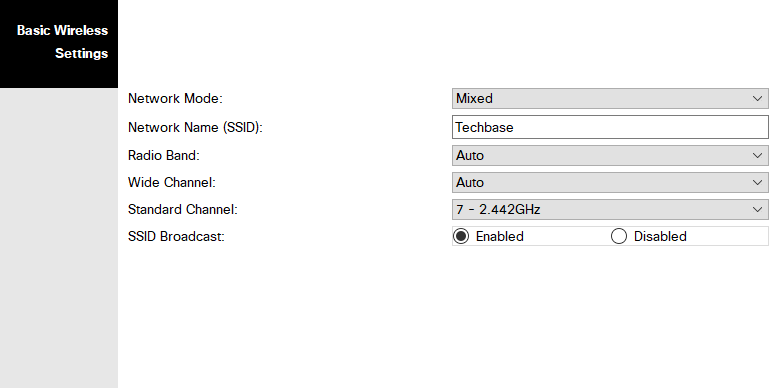


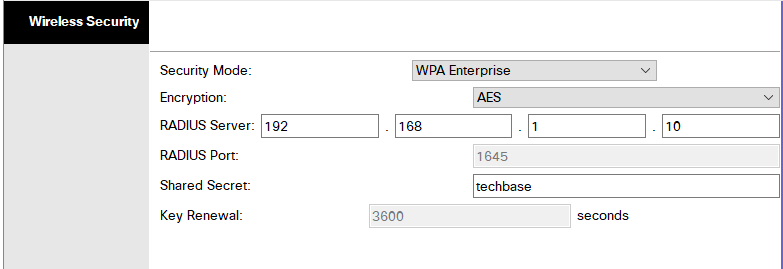
* + - 1. Cấu hình Wireless Router và kết nối với client

- Cấu hình Wireless Router

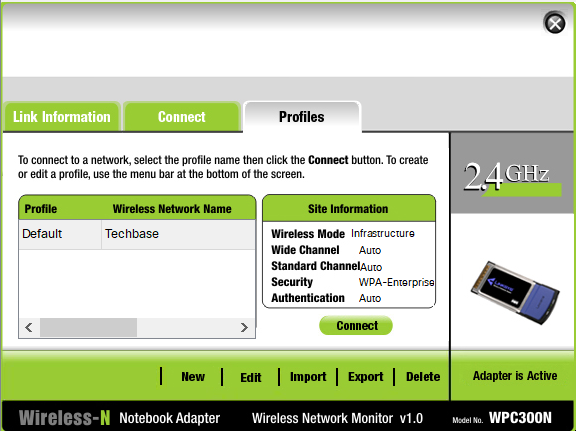


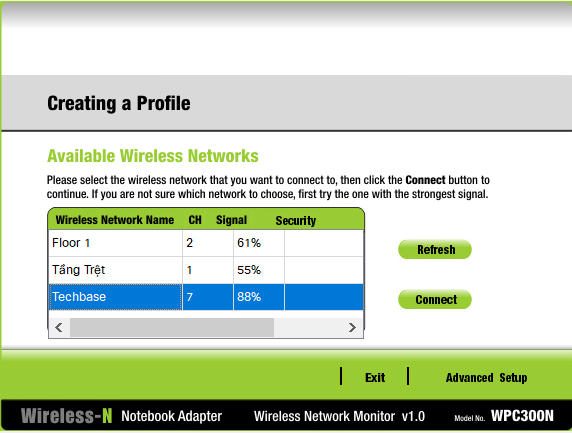


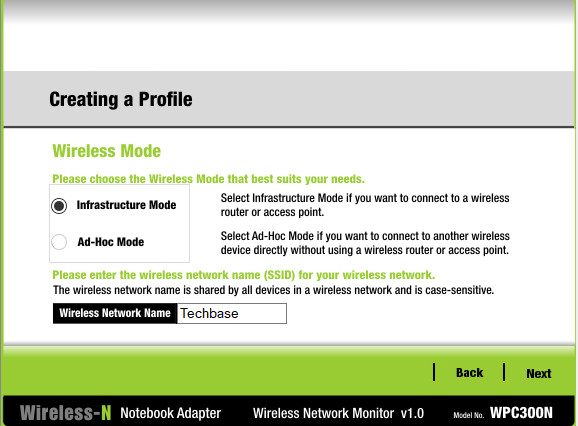


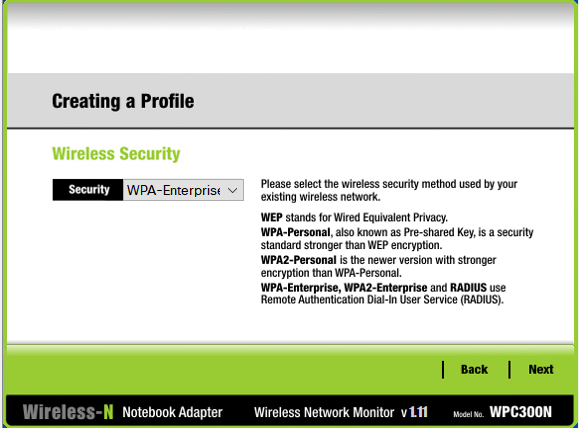


- Kết nối với client



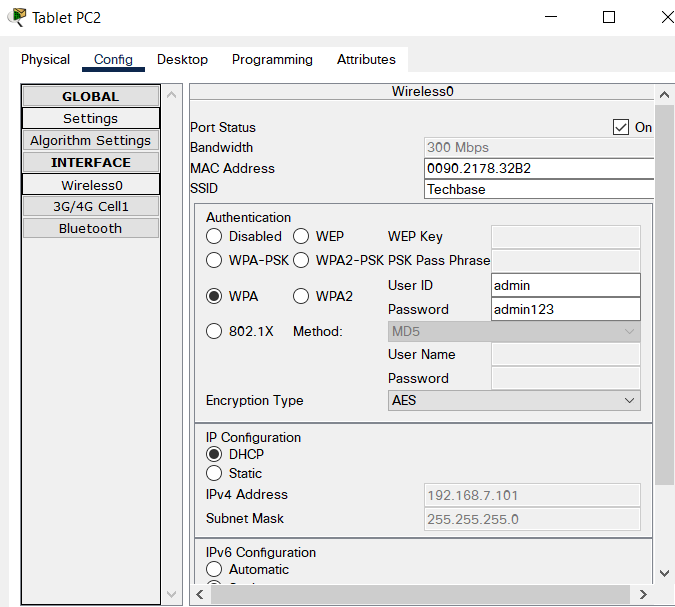




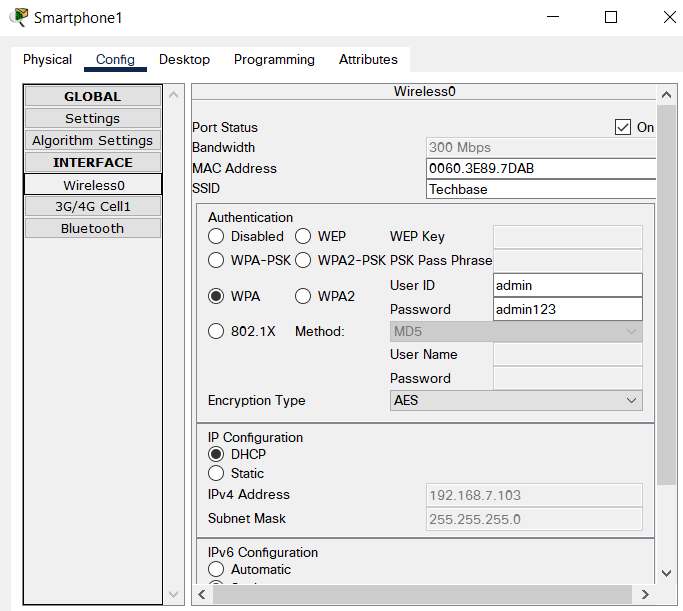




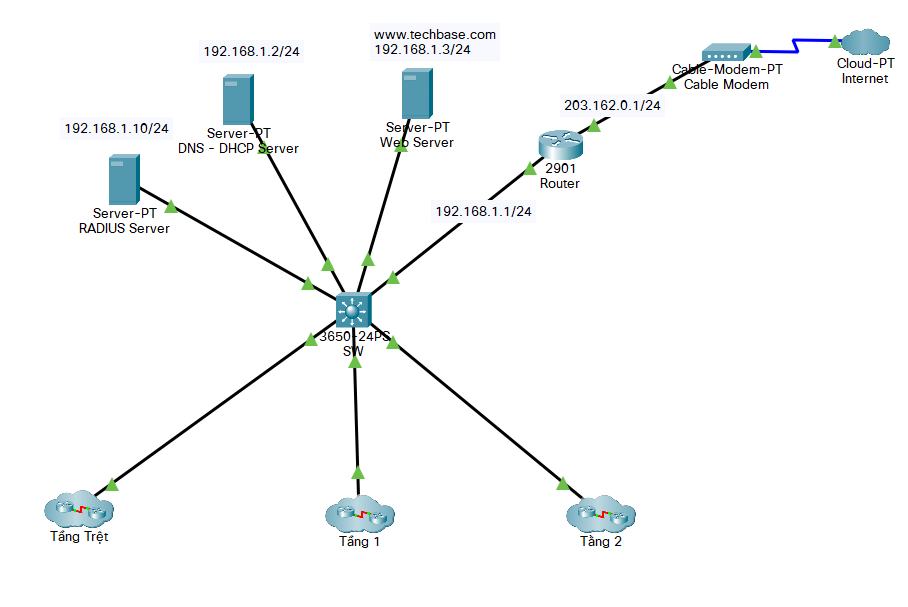
+ kết nối vs tablet



+ kết nối với smartphone



* 1. Kết quả chạy chương trình



CHƯƠNG 4: KẾT LUẬN