TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO CUỐI KÌ MÔN AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐÔNG**

**THIẾT LẬP MẠNG TRƯỜNG HỌC**

*Người hướng dẫn:* **TS. BÙI QUY ANH**

*Người thực hiện*: **ĐOÀN NGUYỄN LÂM – 51800567**

**LÂM THẾ HUÂN – 51800548**

**TỪ HUY VẠN - 51800263**

*Lớp*: **503075**

*Khoá:* **22**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO CUỐI KÌ MÔN AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐÔNG**

**THIẾT LẬP MẠNG TRƯỜNG HỌC**

*Người hướng dẫn:* **TS. BÙI QUY ANH**

*Người thực hiện*: **ĐOÀN NGUYỄN LÂM – 51800567**

**LÂM THẾ HUÂN – 51800548**

**TỪ HUY VẠN - 51800263**

*Lớp*: **503075**

*Khoá:* **22**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

# LỜI CẢM ƠN

Cám ơn thầy đã dạy những kiến thức thú vị về môn học này, những kiến thức về môn học này đã giúp ích cho chúng em rất nhiều trong việc tìm hiểu, phát hiện, bổ sung kiến thức hữu ích về lập trình mạng không dây. Chúng em xin chân thành cảm ơn !

**CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI   
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi và được sự hướng dẫn khoa học của TS Bùi Quy Anh. Các nội dung nghiên cứu, kết quả trong đề tài 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 luận văn 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 luận văn 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)*

*Đoàn Nguyễn Lâm*

*Lâm Thế Huân*

*Từ Huy Vạn*

# 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 TẮC

Trong thời đại công nghiệp lần thứ 4 và quá trình tiếp thu những kiến thức từ internet khiến các trường học đang gặp nhiều khó khăn trong quá trình tiếp cận. Chính vì vậy, trường học luôn cần phải nắm bắt chính xác và kịp thời những thông tin, xu hướng của xã hội để tránh thụt lùi, lạc hậu. Trong đó, hệ thống mạng đóng vai trò cũng hết sức quan trọng trong việc tiếp thu, nắm bắt. Hệ thống mạng là một phần không thể thiếu trong hầu hết các trường học để hỗ trợ việc giảng dạy và giao tiếp giữa các ban ngành đoàn thể.

Với tầm quan trọng của nó, việc trang bị một hệ thống mạng tối ưu và toàn diện cho thầy cô và học sinh sinh viên là một điều hết sức cần thiết.

Tài liệu để biên soạn cho đồ án Thiết lập hệ thống mạng được biên soạn để đáp ứng nhu cầu nghiên cứu, học tập của sinh viên trường Đại học Tôn Đức Thắng.

Tài liệu gồm 4 chương với sự tham gia của các thành viên:

Đoàn Nguyễn Lâm – Biên soạn chương 1: Mô tả đề tài, chương 3: Mô hình demo

Lâm Thế Huân – Biên soạn chương 2: Các cơ sở lý thuyết

Từ Huy Vạn – Biên soạn chương 3: Mô hình demo, chương 4: Kết luận

Hướng tiếp cận được phát triển từ ý tưởng xây dựng 1 hệ thống mạng cho trường học gồm nhiều máy tính và các thiết bị kết nối không dây. Các thiết bị có thể trao đổi, chia sẻ với nhau, sẽ có các thiết bị được thiết lặp trong phạm vi cụ thể để bảo đảm tính bảo mật, riêng tư cho từng khu vực.

Mỗi khu vực sẽ có hoạt động, nhu cầu sử dụng khác nhau. Vì vậy có một quy trình thiết kế hệ thống mạng Lan, Wifi chuyên nghiệp sẽ giúp doanh nghiệp xác định nhu cầu cũng như lựa chọn những thiết bị mạng phù hợp nhất, hỗ trợ các tính năng thỏa mãn chính xác nhu cầu sử dụng.

Việc thiết kế và dự toán hệ thống mạng góp phần giúp trường học tính toán chính xác số lượng thiết bị cần sử dụng Internet cùng lúc, dự tính khả năng mở rộng trong tương lai. Từ đó, giúp tránh tình trạng bị quá tải băng thông, quá tải người và thiết bị sử dụng, loại bỏ được tình trạng mạng bị treo, chậm yếu, chập chờn.

Bản vẽ thiết kế hệ thống mạng sẽ giúp xác định chính xác vị trí tốt nhất để lắp đặt thiết bị. Điều này giúp các thiết bị phát huy tối đa khả năng truyền tín hiệu mạng, không bị chặn, bị gẫy nhiễu do các vật cản trong văn phòng. Bên cạnh đó cũng đảm bảo được tính thẩm mỹ cho nội thất văn phòng.

Mặc dù đã cố gắng tham khảo nhiều nguồn tài liệu khác nhau và đút kết được nhiều kinh nghiệm từ các tài liệu đó. Tuy nhiên, đây là tài liệu học tập được biên soạn lần đầu tiên nên sẽ còn nhiều thiếu sót không tránh được. Nhóm sinh viên rất mong được sự góp ý của quý thầy/cô để tài liệu ngày càng được cải tiến và hoàn thiện hơn. Nhóm sinh viên sinh chân thành cảm ơn quý thầy/cô đã giúp đỡ chúng em trong quá trình biên soạn.

**MỤC LỤC**

[LỜI CẢM ƠN 3](#_Toc91794108)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN 5](#_Toc91794109)

[TÓM TẮC 6](#_Toc91794110)

[DANH MỤC HÌNH 11](#_Toc91794111)

[DANH MỤC BẢNG 14](#_Toc91794112)

[CHƯƠNG 1 - MÔ TẢ ĐỀ TÀI 15](#_Toc91794113)

[1.1. Yêu cầu khách hàng 15](#_Toc91794114)

[1.2. Đề xuất hướng giải quyết 16](#_Toc91794115)

[1.2.1. Xác định yêu cầu thiết kế 16](#_Toc91794116)

[1.2.2. Đặc điểm hệ thống mạng 16](#_Toc91794117)

[1.2.2.1. Lên kế hoạch mua các thiết bị mạng 17](#_Toc91794118)

[1.3. Thiết kế mạng Topology 17](#_Toc91794119)

[CHƯƠNG 2 - CƠ SỞ LÝ THUYẾT 19](#_Toc91794120)

[2.1. Các khái niệm cơ bản 19](#_Toc91794121)

[2.1.1. Khái niệm mạng máy tính 19](#_Toc91794122)

[2.1.2. Khái niệm và các chuẩn của mạng không dây 22](#_Toc91794123)

[2.1.2.1. Các thuật ngữ mạng không dây: 23](#_Toc91794124)

[2.1.2.2. Các tiêu chuẩn của mạng không dây 26](#_Toc91794125)

[2.1.2.2.1. Chuẩn 802.11a 26](#_Toc91794126)

[2.1.2.2.2. Chuẩn 802.11b 26](#_Toc91794127)

[2.1.2.2.3. Chuẩn 802.11g 26](#_Toc91794128)

[2.1.2.2.4. Chuẩn 802.11i 26](#_Toc91794129)

[2.1.2.2.5. Chuẩn 802.16 27](#_Toc91794130)

[2.1.2.2.6. Chuẩn Bluetooth 27](#_Toc91794131)

[2.1.2.3. Ưu điểm của mạng không dây: 27](#_Toc91794132)

[2.1.2.4. Nhược điểm của mạng không dây 28](#_Toc91794133)

[2.1.3. Khái niệm tấn công mạng 28](#_Toc91794134)

[2.1.4. Khái niệm an toàn và bảo mật mạng không dây và các phương pháp mã hóa mạng không dây 34](#_Toc91794135)

[2.1.4.1. Khái niệm 34](#_Toc91794136)

[2.1.4.2. Các phương pháp mã hóa mạng không dây 34](#_Toc91794137)

[2.1.4.2.1. Wired Equivalent Privacy – WEP 34](#_Toc91794138)

[2.1.4.2.2. WPA, WPA2, WPA3 36](#_Toc91794139)

[2.1.5. Mô hình kiến trúc hạ tầng mạng 37](#_Toc91794140)

[2.1.5.1. Mô hình hệ thống mạng phân cấp 37](#_Toc91794141)

[2.1.5.2. Mô hình kiến trúc mạng doanh nghiệp 37](#_Toc91794142)

[2.1.5.2.1. Lớp mạng trung tâm (Core layer) 38](#_Toc91794143)

[2.1.5.2.2. Lớp mạng phân bố (Distribution Layer) 39](#_Toc91794144)

[2.1.5.2.3. Lớp mạng truy cập (Access Layer) 40](#_Toc91794145)

[2.2. Phương pháp xác thực mạng không dây và lỗ hổng của mạng không dây 41](#_Toc91794146)

[2.2.1. Phương pháp xác thực mạng không dây 41](#_Toc91794147)

[2.2.1.1. Hệ thống xử lý xác thực 41](#_Toc91794148)

[2.2.1.2. Chia sẻ quá trình xác thực khóa 41](#_Toc91794149)

[2.2.1.3. Xác thực mạng không dây sử dụng máy chủ tập trung 41](#_Toc91794150)

[2.2.2. Lỗ hổng của mạng không dây 42](#_Toc91794151)

[2.3. Các phương pháp bảo mật mạng không dây cơ bản 42](#_Toc91794152)

[2.3.1. Thay đổi tên mạng (SSID) 42](#_Toc91794153)

[2.3.2. Thay đổi tên người dùng và mật khẩu 42](#_Toc91794154)

[2.3.3. Sử dụng mã hóa mạnh để bảo mật wifi 43](#_Toc91794155)

[2.3.4. Chọn mật khẩu mạnh 44](#_Toc91794156)

[2.3.5. Thay đổi mật khẩu wifi 44](#_Toc91794157)

[2.3.6. Vô hiệu hóa mạng khách 44](#_Toc91794158)

[2.3.7. Bật tường lửa để bảo vệ wifi 44](#_Toc91794159)

[2.3.8. Sử dụng VPN 45](#_Toc91794160)

[2.3.9. Tắt WPS 45](#_Toc91794161)

[2.3.10. Quản lý firmware của bộ định tuyến 45](#_Toc91794162)

[2.3.11. Tắt quản lý từ xa/ dịch vụ không cần thiết 46](#_Toc91794163)

[CHƯƠNG 3 - MÔ HÌNH DEMO 47](#_Toc91794164)

[3.1. Mô hình đề xuất 47](#_Toc91794165)

[3.2. Cấu hình thiết bị 51](#_Toc91794166)

[3.2.1. Cấu hình Server 55](#_Toc91794167)

[3.2.2. Cấu hình WirelessGroundRouter 57](#_Toc91794168)

[3.2.3. LAN Settings 57](#_Toc91794169)

[3.2.4. Wireless Setting 57](#_Toc91794170)

[3.2.5. Cấu hình WirelessRouter Class2.Flr1 58](#_Toc91794171)

[3.2.6. LAN Settings 58](#_Toc91794172)

[3.2.7. Wireless Setting Class2Flr1 58](#_Toc91794173)

[3.2.8. Cấu hình WirelessRouter Class1.Flr1 59](#_Toc91794174)

[3.2.9. Wireless Setting Class1Flr1 59](#_Toc91794175)

[3.2.10. Cấu hình WirelessRouter Class2.Flr2 60](#_Toc91794176)

[3.2.11. LAN setting Class2.Flr2 60](#_Toc91794177)

[3.2.12. Wireless Setting Class2.Flr2 60](#_Toc91794178)

[3.2.13. Cấu hình WirelessRouter Class1.Flr2 61](#_Toc91794179)

[3.2.14. LAN Settings Class1.Flr2 61](#_Toc91794180)

[3.2.15. Cấu hình PC 62](#_Toc91794181)

[3.2.16. Cấu hình máy in 62](#_Toc91794182)

[3.2.17. Cấu hình Laptop 63](#_Toc91794183)

[3.2.18. Cấu hình SmartPhone 64](#_Toc91794184)

[3.2.19. Cấu hình Tablet 65](#_Toc91794185)

[3.3. Kết quả chạy chương trình 66](#_Toc91794186)

[3.3.1. Ping PC Staff 1 sang PC Teacher 1 66](#_Toc91794187)

[3.3.2. Ping PC Staff 1 sang Server 66](#_Toc91794188)

[3.3.3. Ping PC Staff 1 sang PC GM 5 67](#_Toc91794189)

[3.3.4. Ping PC Staff 1 sang PC Network 3 67](#_Toc91794190)

[3.3.5. Ping PC Staff 1 sang PC lab1.1 67](#_Toc91794191)

[3.3.6. Ping PC Staff 1 sang PC lab2.25 68](#_Toc91794192)

[3.3.7. Ping Laptop 2 Class2.Flr2 sang server 68](#_Toc91794193)

[3.3.8. Ping Laptop 2 Class2.Flr2 sang Laptop 3 Class2.Flr2 68](#_Toc91794194)

[3.4. Chi phí thiết bị 69](#_Toc91794195)

[3.4.1. Chi tiết thiết bị 70](#_Toc91794196)

[CHƯƠNG 4 - KẾT LUẬN 79](#_Toc91794197)

# DANH MỤC HÌNH

[Hình 1‑1 Mô hình mạng trường học 17](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098128)

[Hình 2‑1 Mô hình mạng máy tính 20](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098129)

[Hình 2‑2 Mô hình mạng Khách - Chủ 21](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098130)

[Hình 2‑3 Mạng không dây 24](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098131)

[Hình 2‑4 Mạng WRAN 24](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098132)

[Hình 2‑5 Mạng WAN 25](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098133)

[Hình 2‑6 Mạng WMAN 25](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098134)

[Hình 2‑7 Mạng WLAN 26](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098135)

[Hình 2‑8 Mạng WPAN 26](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098136)

[Hình 2‑9 Các chuẩn mạng không dây 28](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098137)

[Hình 2‑10 Tấn công mạng là gi 30](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098138)

[Hình 2‑11 Malware 31](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098139)

[Hình 2‑12 Phishing attack 31](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098140)

[Hình 2‑13 SQL Injection 32](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098141)

[Hình 2‑14 Tấn công từ chối dịch vụ 33](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098142)

[Hình 2‑15 Khai thác lỗ hổng Zero Day (Zero Day Attack) 34](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098143)

[Hình 2‑16 Tấn công trung gian (Man in the middle attack - MitM) 34](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098144)

[Hình 2‑17 Cơ chế hoạt động WEP 36](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098145)

[Hình 2‑18 WPA (Wi-Fi Protected Access) 38](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098146)

[Hình 2‑19 Giao thức CCMP 39](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098147)

[Hình 2‑20 Cơ chế hoạt động của WPA 40](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098148)

[Hình 2‑21 Mô hình mạng phân lớp 43](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098149)

[Hình 2‑22 Lớp mạng trung tâm 44](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098150)

[Hình 2‑23 Các chức năng của lớp phân bố. Nguồn Microsoft 45](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098151)

[Hình 2‑24 Thay đổi tên mạng 47](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098152)

[Hình 2‑25 Thay đổi username và password 48](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098153)

[Hình 2‑26 Sử dụng mã hóa WPA2 Personal và thuật toán mã hóa AES 48](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098154)

[Hình 2‑27 Chọn mật khẩu mạnh 49](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098155)

[Hình 2‑28 Bật tường lửa 49](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098156)

[Hình 2‑29 Sử dụng VPN 50](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098157)

[Hình 2‑30 Quản lý firmware 51](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098158)

[Hình 2‑31 Tắt các dịch vụ từ xa không cần thiết 51](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098159)

[Hình 3‑1 Mô hình để xuất 52](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098160)

[Hình 3‑2 Mô phỏng mạng cho phòng thí nghiệm 52](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098161)

[Hình 3‑3 Mô phỏng mạng cho phòng học 53](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098162)

[Hình 3‑4 Mô phỏng mạng cho phòng nhân viên 53](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098163)

[Hình 3‑5 Mô phỏng cho mạng phòng giáo viên 54](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098164)

[Hình 3‑6 Mô phỏng cho mạng phòng GM 54](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098165)

[Hình 3‑7 Mô phỏng cho mạng phòng quán lý mạng 54](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098166)

[Hình 3‑8 Mô phỏng kết nối tới mạng internet 55](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098167)

[Hình 3‑9 Cấu hình DNS sẻver 61](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098168)

[Hình 3‑10 HTTP: ON , HTTPS: ON 61](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098169)

[Hình 3‑11 Cấu hình Server 0 61](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098170)

[Hình 3‑12 Cấu hình c wireless ground router 62](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098171)

[Hình 3‑13 LAN setting 62](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098172)

[Hình 3‑14 Cấu hình wireless 62](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098173)

[Hình 3‑15 3.2.5. Cấu hình WirelessRouter Class2.Flr1 63](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098174)

[Hình 3‑16 3.2.6. LAN Settings 63](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098175)

[Hình 3‑17 3.2.7. Wireless Setting Class2Flr1 63](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098176)

[Hình 3‑18 3.2.8. Cấu hình WirelessRouter Class1.Flr1 64](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098177)

[Hình 3‑19 Wireless Setting Class1Flr1 64](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098178)

[Hình 3‑20 Cấu hình WirelessRouter Class2.Flr2 65](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098179)

[Hình 3‑21 3.2.11. LAN setting Class2.Flr2 65](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098180)

[Hình 3‑22 3.2.12. Wireless Setting Class2.Flr2 65](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098181)

[Hình 3‑23 3.2.13. Cấu hình WirelessRouter Class1.Flr2 66](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098182)

[Hình 3‑24 3.2.14. LAN Settings Class1.Flr2 66](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098183)

[Hình 3‑25 Wireless Setting Class1.Flr2 66](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098184)

[Hình 3‑26 3.2.16. Cấu hình PC 67](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098185)

[Hình 3‑27 3.2.17. Cấu hình máy in 67](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098186)

[Hình 3‑28 Cấu hình Laptop 68](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098187)

[Hình 3‑29 Các bước vào mạng wireless 69](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098188)

[Hình 3‑30 3.2.19. Cấu hình SmartPhone 70](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098189)

[Hình 3‑31 Cấu hình Tablet 71](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098190)

[Hình 3‑32 Ping PC Staff 1 sang PC Teacher 1 71](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098191)

[Hình 3‑33 Ping PC Staff 1 sang Server 71](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098192)

[Hình 3‑34 Ping PC Staff 1 sang PC GM 5 72](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098193)

[Hình 3‑35 Ping PC Staff 1 sang PC Network 3 72](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098194)

[Hình 3‑36 Ping PC Staff 1 sang PC lab1.1 72](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098195)

[Hình 3‑37 Ping PC Staff 1 sang PC lab2.25 73](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098196)

[Hình 3‑38 Ping Laptop 2 Class2.Flr2 sang server 73](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098197)

[Hình 3‑39 3.3.8. Ping Laptop 2 Class2.Flr2 sang Laptop 3 Class2.Flr2 73](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098198)

[Hình 3‑40 Switch 24 cổng 75](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098199)

[Hình 3‑41 Switch 16 cổng 76](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098200)

[Hình 3‑42 Switch 10 cổng 78](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098201)

[Hình 3‑43 Wireless router 80](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098202)

[Hình 3‑44 Cáp mạng 82](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098203)

# DANH MỤC BẢNG

[Bảng 1‑1 Bảng thống kê các thiết bị hạ tầng mạng 18](#_Toc91098204)

[Bảng 1‑2 Bảng thông tin chi tiết thiết bị 18](#_Toc91098205)

[Bảng 3‑1 Bảng địa chỉ IP 59](#_Toc91098206)

[Bảng 3‑2 Bảng thông tin WLAN 60](#_Toc91098207)

[Bảng 3‑3 Chi phí thiết bị 74](#_Toc91098208)

[Bảng 3‑4 Thông tin cấu hình Switch 24 cổng 76](#_Toc91098209)

[Bảng 3‑5 Cấu hình chi chi switch 16 cổng 77](#_Toc91098210)

[Bảng 3‑6 Cấu hình chi tiết switch 10 cổng 80](#_Toc91098211)

[Bảng 3‑7 Cấu hình chi tiết wireless router 81](#_Toc91098212)

[Bảng 3‑8 Server 82](file:///C:\Users\DELL\OneDrive\Máy%20tính\Network\Final_Network.docx#_Toc91098213)

[Bảng 3‑9 Cấu hình chi tiết server 82](#_Toc91098214)

# MÔ TẢ ĐỀ TÀI

## Yêu cầu khách hàng

Kịch bản đưa ra là phát triển hệ thống mạng LAN cho một trường đại học với 200 sinh viên, 15 giáo viên, 12 nhân viên tiếp thị và quản trị, 5 quản lý cấp cao hơn bao gồm trưởng phòng học thuật và giám đốc lập trình, 3 quản trị viên mạng máy tính. Và 50 máy tính phòng thí nghiệm sinh viên, 35 máy tính cho nhân viên, 3 máy in tài nguyên. Và bản thân tòa nhà có 3 tầng, tất cả máy tính và máy in đều ở tầng trệt ngoài các phòng thí nghiệm CNTT - một phòng thí nghiệm nằm ở tầng một và một phòng thí nghiệm khác nằm ở tầng hai.

Nhiệm vụ là phát triển một hệ thống mạng phù hợp với những điều kiện trên và không đòi hỏi nhiều tài nguyên hơn số tài nguyên đã cho. Tôi quyết định xây dựng tòa nhà trước vì chúng tôi có 200 sinh viên nhưng đây là một trường đại học nên lịch học sẽ khác với lịch học cấp ba với 200 nhưng chỉ có 100 sinh viên học vào buổi sáng và 100 sinh viên học vào buổi tối. Vì vậy chúng tôi sẽ xây dựng một tòa nhà có 4 phòng học, 2 phòng Lab, 1 phòng giáo viên, 1 phòng giáo viên, 1 phòng quản lý, 1 phòng quản lý mạng.

Để làm được điều này, chúng ta phải có một cái nhìn tổng quan về hệ thống mạng và cách thức hoạt động của nó. Nói cách khác, chúng ta phải có một thiết kế bao gồm các thiết bị mạng và để làm như vậy chúng ta phải biết về vai trò của chúng trong hệ thống và một số cấu trúc liên kết mà chúng ta có thể sử dụng để phát triển một hệ thống mạng theo các nhiệm vụ đã cho ở trên.

|  |  |  |  |
| --- | --- | --- | --- |
| LAB 2 | CLASS 201 | CLASS 202 | |
| LAB 1 | CLASS 101 | CLASS 102 | |
| STAFF ROOM | TEACHER ROOM | GM ROOM | NETWORK MANAGER |

Hình ‑ Mô hình mạng trường học

## Đề xuất hướng giải quyết

### Xác định yêu cầu thiết kế

Đây là bước thu thập thông tin yêu cầu thiết kế của khách hàng. Yêu cầu về khả năng mở rộng cũng như hạ tầng mạng. Từ đó đề xuất mô hình phác thảo ban đầu để đánh giá chọn lọc những thiết bị tối ưu cho khách hàng. Thông qua đó đánh giá được bức tranh tài chính đối với dự án.

Tiến hành thu thập thông tin từ nhiều đối tượng khách nhau như đội ngũ kỹ thuật điều hành hệ thống, từ phía người dùng cá nhân, quan điểm của người quản lý,… Hệ thống phải đảm bảo đáp ứng được các yêu cầu tối thiểu của khách hàng chẳng hạn như băng thông, độ trễ, thời gian phản hồi.

Các bước cần thiết để thiết kế một mạng:

Bước 1. Xác minh các mục tiêu và yêu cầu kỹ thuật.

Bước 2. Xác định các tính năng và chức năng cần thiết để đáp ứng các nhu cầu đã xác định trong Bước 1.

Bước 3. Thực hiện đánh giá mức độ sẵn sàng của mạng.

Bước 4. Lập giải pháp và kế hoạch nghiệm thu hiện trường.

Bước 5. Tạo kế hoạch dự án

### Đặc điểm hệ thống mạng

Mục đích của việc thu thập thông tin khách hàng là nhằm xác định mong muốn của khách hàng trên mạng mà chúng ta thiết lập. Những câu hỏi cần được giải đáp như:

Công ty/cơ quan/… anh/chị thiết lập mạng để làm gì ?

Các thiết bị nào sẽ kết nối với mạng ?

Những phòng/ban/cá nhân nào sẽ được kết nối vào mạng, mức độ khai thác sử dụng mạng của từng người/nhóm người ?

Trong tương lai có cần mở rộng thêm không. Nếu có thì ở đâu, bao nhiêu ?

Một công việc cũng rất quan trọng là việc xem xét tình hình thực tế để có thể nắm bắt được kết cấu cơ sở hạ tầng của cty/cơ quan/trường học/… Dự kiến đường đi của dây mạng, đưa ra các lựa chọn công nghệ phù hợp. Một điểm cũng đáng nhắc tới là tính thẩm mỹ sau khi thiết lập mạng.

Trong quá trình khảo sát ta cũng phải kết hợp với việc trao đổi thông tin với các phòng ban, bộ phận,… mức độ và lượng thông tin trao đổi như thế nào.

#### Lên kế hoạch mua các thiết bị mạng

Do chi phí của các dự án đều có hạn, công ty/doanh nghiệp/trường học/… chỉ dành 1 khoảng chi phí nhất định nên việc ta chọn lựa thiết bị hoặc mua thiết bị phải lên danh sách một cách cụ thể, rõ ràng để tránh việc mua thừa hoặc thiết bị không sử dụng được. Vì vây ta cần xây dựng một số bảng như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Tên thiết bị** | **Hãng sản xuất** | **Số lượng** | **Giá** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

Bảng 1‑1 Bảng thống kê các thiết bị hạ tầng mạng

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên thiết bị** | **Thông tin chi tiêt** |
| 1 |  |  |
| 2 |  |  |

Bảng 1‑2 Bảng thông tin chi tiết thiết bị

## Thiết kế mạng Topology

Đây là bước quan trọng nhất mang tính chất quyết định lên toàn bộ hệ thống. Việc thiết kế phải dựa trên điều kiện thực tế mà công ty/cơ quan/trường học/… đang hiện có. Một mô hình thiết kế hợp lý cần phải đảm bảo yếu tố sẵn sàng, độ tin cậy, yếu tố bảo mật, khả năng mở rộng, cũng như yếu tố về mặt hiệu xuất hoạt động. Gồm các bước cơ bản sau:

Thiết kế lớp ứng dụng và dịch vụ mạng: dịch vụ chia sẻ tập tin, chia sẻ, máy in, dịch vụ web, dịch vụ thư điện tử, thiết kế hệ thống truy cập Internet cho hệ thống mạng.

Lựa chọn công nghệ: các công nghệ áp dụng cho hệ thống

Quy hoạch IP: Do bất kì thiết bị mạng nào cũng cần 1 địa chỉ IP để phân biệt và trao đổi thông tin. Như vậy khi xây hệ thống mạng ta cần xác định rõ địa chỉ IP của từng loại mạng.

Thiết kế về mặt định tuyến: Để các mạng khác nhau có thể kết nối được với nhau thì chúng ta cần phải sử dụng Router để định tuyến, giúp các mạng biết thông tin về nhau. Router là thiết bị lớp 3 thường được sử dụng để cấu hình định tuyến giữa các mạng. Trên router có thể cấu hình nhiều giao thức định tuyến, mỗi giao thức có một ưu và nhược điểm riêng.

Thiết kế bảo mật: tham gia vào mạng thì chúng ta còn phải đối đầu với những nguy cơ bị các hacker tấn công vào hệ thống với các ý đồ, mục đích khác nhau. Vì thế ta cần thiết lập các lớp bảo mật cho từng loại mạng, từng phòng ban với từng mục đích khác nhau.

Thiết kế hạ tầng(logic): Đưa ra mô hình, bố trí và liên kết giữa các thiết bị.

Thiết kế mô hình vật lý: sơ đồ mạng ở mức vật lý mô tả chi tiết về vị trí, đường đi của dây mạng, vị trí của các thiết bị nối kết mạng như Hub, Switch, Router, vị trí các máy chủ và các máy trạm.

Thiết kế hệ thống tài liệu: nhằm lưu trữ các thông tin cấu hình, cách thức vận hành sử dụng của từng loài thiết bị trong mạng.

# CƠ SỞ LÝ THUYẾT

## Các khái niệm cơ bản

### Khái niệm mạng máy tính

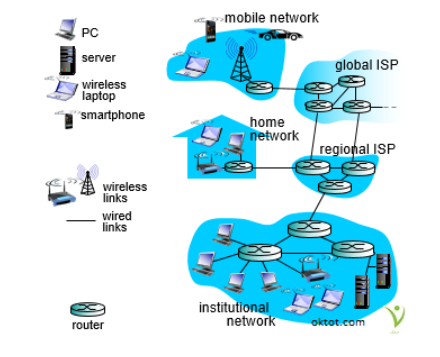
Mạng máy tính là một hệ thống gồm nhiều máy tính và các thiết bị được kết nối với nhau bởi đường truyền vật lý theo một kiến trúc mạng (Network Architecture) nào đó nhằm thu thập, trao đổi dữ liệu và chia sẽ tài nguyên cho nhiều người sử dụng.

Các máy tính được kết nối với nhau có thể trong cùng một phòng, một tòa nhà, một thành phố hoặc trên phạm vi toàn cầu.

Mạng máy tính bao gồm ba thành phần chính:

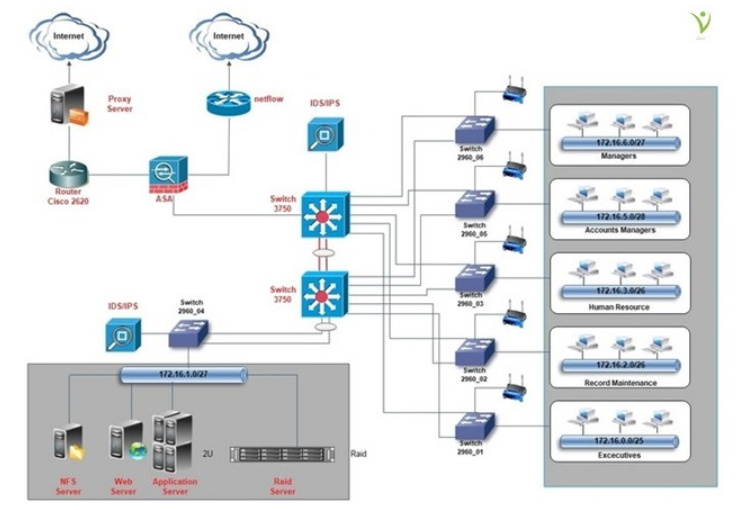
Các máy tính.

Các thiết bị mạng đảm bảo kết nối các máy tính với nhau.

Phần mềm cho phép thực hiện việc trao đổi thông tin giữa các máy tính.

Hình ‑ Mô hình mạng máy tính

**Phân loại mạng theo chức năng:**

* Mô hình mạng ngang hàng (peer - to - peer)
  + Trong mô hình này, tất cả các máy tính tham gia đều có vai trò giống nhau. Mỗi máy vừa có thể cung cấp trực tiếp tài nguyên của mình cho các máy khác, vừa có thể sử dụng trực tiếp tài nguyên của các máy khác trong mạng. Mô hình này chỉ thích hợp với mạng có quy mô nhỏ, tài nguyên được quản lý phân tán, chế độ bảo mật kém.
* Mô hình mạng Khách - Chủ (Client - Server)
  + Trong mô hình này, một hoặc vài máy sẽ được chọn để đảm nhận việc quản lý và cung cấp tài nguyên (chương trình, dữ liệu, thiết bị,…) được gọi là máy chủ (Server), các máy khác sử dụng tài nguyên này được gọi là máy khách (Client).
  + Máy chủ là máy tính đảm bảo việc phục vụ các máy khách bằng cách điều khiển việc phân phối tài nguyên nằm trong mạng với mục đích sử dụng chung. Máy khách là máy sử dụng tài nguyên do máy chủ cung cấp.
  + Mô hình khách – chủ có ưu điểm là dữ liệu được quản lý tập trung, bảo mật tốt, thích hợp với các mạng trung bình và lớn.

Hình ‑ Mô hình mạng Khách - Chủ

* Mô hình dựa trên nền Web
  + Ngày nay, do sự phát triển của Internet nên có rất nhiều công ty và cá nhân sử dụng Internet như một mạng “xương sống” và kết nối với mọi người trên toàn cầu. Mạng trên phạm vi Internet được gọi là mạng liên kết nối và ngày càng trở nên phổ biến. Người dùng chỉ cần trình duyệt Web và một kết nối Internet để chia sẻ các tập tin, tải các ứng dụng, xem video hoặc tham gia học tập trực tuyến

**Phân loại mạng máy tính:**

* Dưới góc độ địa lý, mạng máy tính có thể phân thành: mạng cục bộ và mạng diện rộng.
  + Mạng cục bộ (Local Area Network - LAN):
  + LAN là mạng kết nối các máy tính bên trong một vùng diện tích địa lý tương đối nhỏ, chẳng hạn như trong một phòng, một tòa nhà, một xí nghiệp, một trường học,…
  + Kết nối với LAN: Cho dù mạng LAN được thiết kế là mạng dựa trên máy chủ hay mạng ngang hàng, người dùng cần phải kết nối với mạng LAN thì mới tham gia được vào mạng. Kết nối với mạng LAN yêu cầu:
    - Một card giao tiếp mạng (NIC: Network Interface Card)
    - Thiết bị truyền thông (có dây hoặc không dây)
* Mạng diện rộng (Wide Area Network - WAN)
  + **WAN** là mạng kết nối các máy tính ở cách nhau những khoảng cách lớn. Mạng diện rộng thường bao gồm hai hay nhiều LAN bao phủ một vùng diện tích rộng (ví dụ như trong cùng một thành phố hoặc một quốc gia), các LAN được kết nối sử dụng các đường dây của nhà cung cấp dịch vụ truyền tải công cộng.
  + Xét một doanh nghiệp lớn với các văn phòng nằm ở các vị trí khác nhau trên toàn cầu. Mỗi văn phòng có một LAN riêng được sử dụng để chia sẻ tài nguyên cục bộ. Tuy nhiên, nếu công ty cần chia sẻ tài nguyên với các văn phòng khác, các LAN có thể được kết nối với nhau sử dụng các đường dây truyền thông được cung cấp bởi các nhà cung cấp dịch vụ truyền tải công cộng. Khi hai hay nhiều LAN được kết nối sử dụng mạng công cộng, WAN được tạo ra. WAN lớn nhất trên thế giới chính là Internet.

**Các tính năng chính để phân biệt LAN với WAN là:**

* LAN bị bó hẹp trong phạm vi kết nối cục bộ tại gia đình hoặc được thiết lập trong phạm vi một văn phòng. Trong LAN, tổ chức sở hữu mọi thành phần. Đối với WAN, tổ chức phải thuê một vài thành phần cần thiết để truyền tải dữ liệu, chẳng hạn như đường truyền tốc độ cao.
* LAN cũng thường có tốc độ cao hơn WAN. Ví dụ, hầu hết các card Ethernet truyền tải dữ liệu ở tốc độ 100 hoặc 10000 Mbps, nếu sử dụng Gigabit Ethernet thì dữ liệu di chuyển với tốc độ 40 Gbps. Tuy nhiên, một kết nối WAN chuẩn chỉ có thể chạy với tốc độ 1.5 Mbps đến 100 Mbps hoặc hơn tùy theo công nghệ sử dụng.

### Khái niệm và các chuẩn của mạng không dây

Mạng không dây (tiếng Anh: wireless network) là mạng điện thoại hoặc mạng máy tính sử dụng sóng radio làm sóng truyền dẫn hay tầng vật lý.

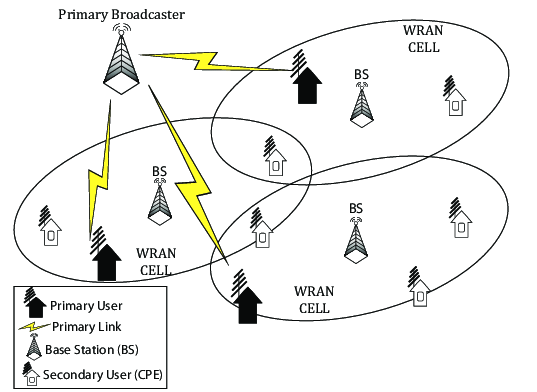
Một mạng không dây là một mạng máy tính sử dụng các kết nối dữ liệu không dây giữa các nút mạng. Mạng không dây được ưa thích bởi các hộ gia đình, các doanh nghiệp hay các cơ sở kinh doanh vừa và lớn có nhu cầu kết nối internet nhưng không thông qua quá nhiều cáp chuyển đổi. Các mạng không dây được quản lý bởi hệ thống truyền thông vô tuyến của các nhà mạng. Những hệ thống này thường được đặt tập trung hoặc rời rạc tại những cơ sở lưu trữ của các nhà mạng. Cấu trúc mạng thường được sử dụng là cấu trúc OSI.

Những ví dụ điển hình về mạng không dây là: mạng wifi, mạng 3G, mạng điện thoại di động, mạng bluetooth, mạng nội bộ không dây (WLAN), mạng cảm biến không dây, mạng truyền thông vệ tinh và mạng sóng mặt đất.

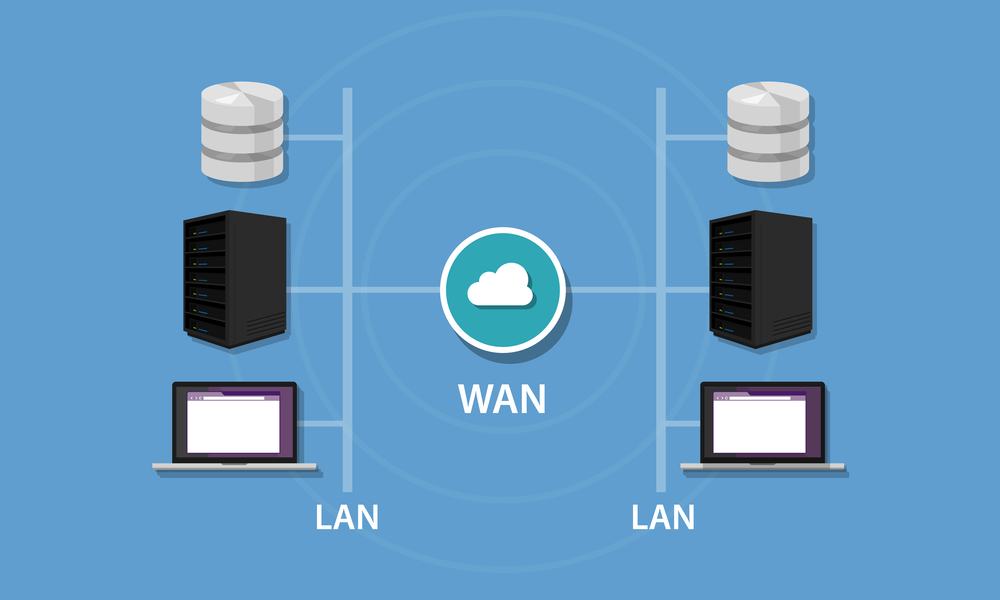
****

Hình ‑ Mạng không dây

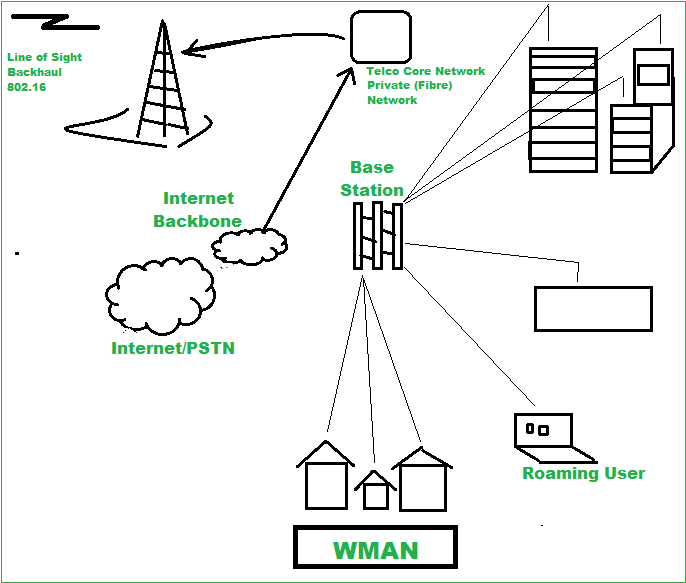
#### Các thuật ngữ mạng không dây:

* Mạng RAN không dây (WRAN) - mạng vô tuyến khu vực:
  + WRAN có khả năng phát sóng xa từ hàng chục đến hàng trăm kilomet, với tốc độ 22Mbps. Tốc độ truy nhập của máy tính từ mạng này hoàn toàn "ổn" theo đánh giá của IEEE.

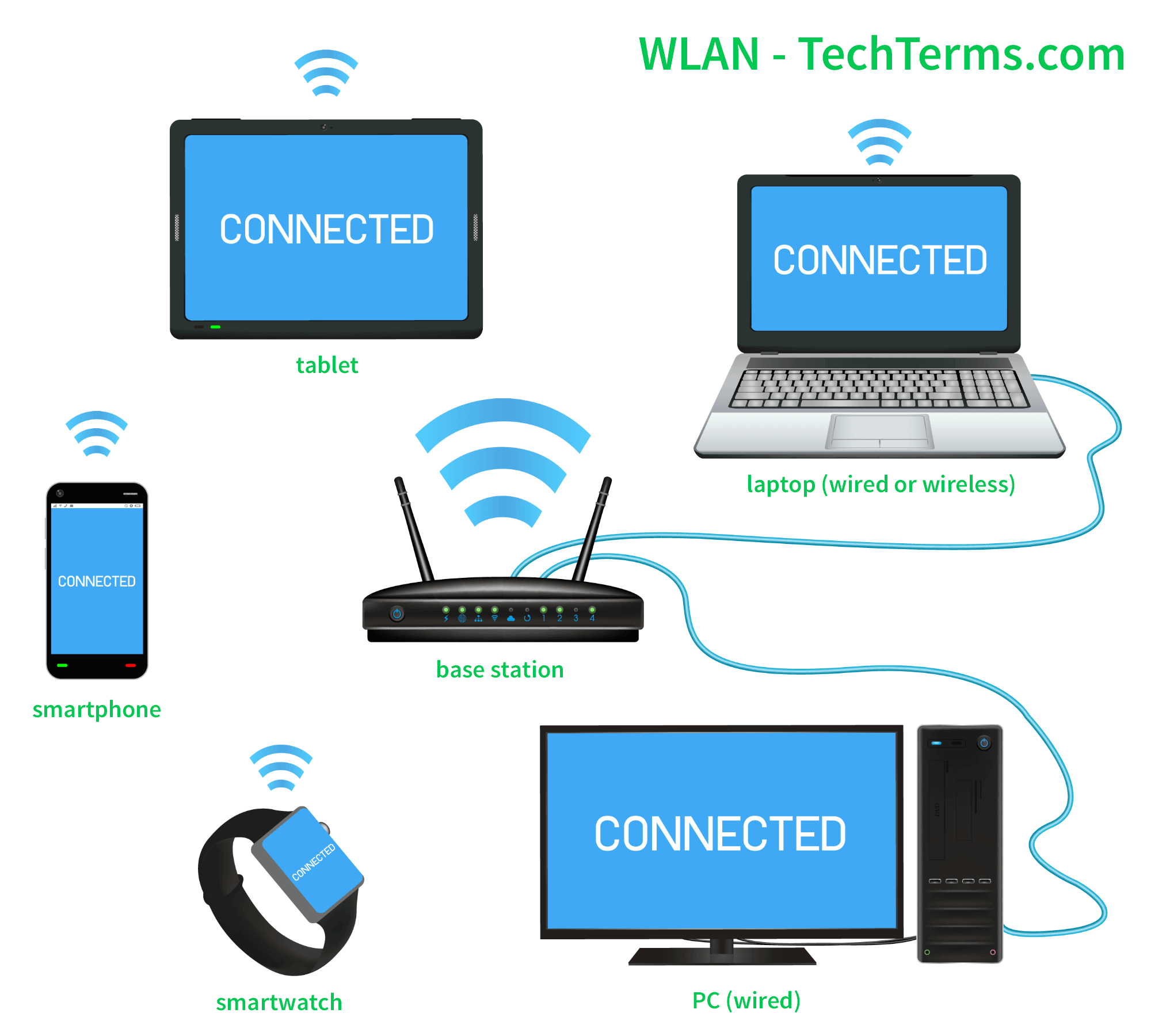
Hình ‑ Mạng WRAN

* Mạng WAN không dây (WWAN) - mạng vô tuyến diện rộng:
  + Mạng không dây diện rộng là mạng không dây thường bao gồm khu vực rộng lớn, chẳng hạn như giữa các thành phố và vùng lân cận.
  + Các mạng này có thể được sử dụng để kết nối các văn phòng chi nhánh của doanh nghiệp hoặc của hệ thống truy cập Internet công cộng.

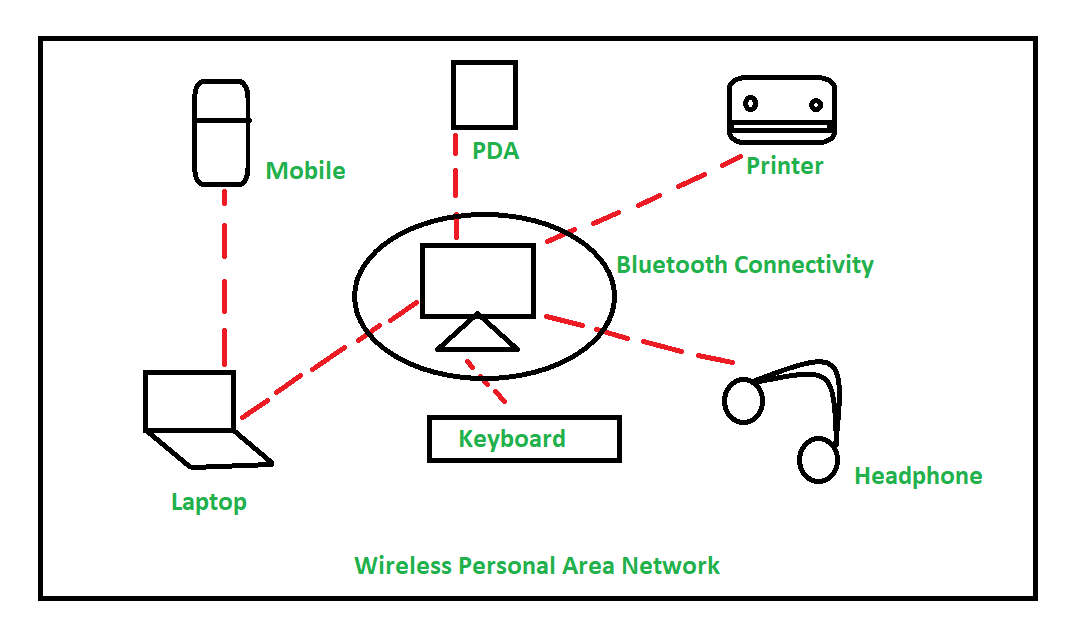
Hình ‑ Mạng WAN

* Mạng MAN không dây (WMAN) - mạng vô tuyến đô thị:
  + Mạng không dây khu vực đô thị là một loại mạng không dây kết nối nhiều mạng LAN không dây. WIMAX là một loại mạng MAN không dây và được mô tả bởi tiêu chuẩn IEEE 802.16.

Hình ‑ Mạng WMAN

* Mạng LAN không dây (WLAN) - mạng vô tuyến cục bộ:
  + Mạng LAN không dây liên kết hai hay nhiều thiết bị trên một khoảng cách ngắn sử dụng phương pháp phân phối không dây. Thường cung cấp một kết nối thông qua một điểm truy cập Internet. Mạng này sử dụng tiêu chuẩn 802.11 và công nghệ point to point liên kết giữa các máy tính hoặc tại hai địa điểm xa nhau.

Hình ‑ Mạng WLAN

* Mạng PAN không dây (WPAN) - mạng vô tuyến cá nhân:

Hình ‑ Mạng WPAN

* + Mạng cá nhân không dây là các thiết bị kết nối trong khu vực tương đối nhỏ, ví dụ: bluetooth, hồng ngoại, …
* GSM - Chuẩn toàn cầu cho truyền thông di động số, thông dụng tại hầu hết các nước ngoại trừ Hàn Quốc và Nhật Bản.
* Mạng di động tùy biến (Mobile ad-hoc network).
* Wi-Fi - một tập các chuẩn tương thích sản phẩm dành cho các mạng WLAN dựa trên đặc tả IEEE 802.11.

#### Các tiêu chuẩn của mạng không dây

##### Chuẩn 802.11a

IEEE đã mở rộng tiêu chuẩn thứ cấp cho chuẩn 802.11 là 802.11a. Do 802.11a có chi phí cao nên chỉ tìm thấy trên mạng doanh nghiệp. Băng thông trên 54Mbps và tín hiệu trong một phổ tần số khoảng 5Ghz.

##### Chuẩn 802.11b

Được mở rộng trên tiêu chuẩn 802.11. Tiêu chuẩn 802.11b sử dụng không kiểm soát tín hiệu vô tuyến truyền tin hiệu (2,4GHz) cũng giống như chuẩn ban đầu 802.11. Tiêu chuẩn 802.11b có chi phí thấp, tín hiệu vô tuyến tốt và không dễ bị cản trở nên được sử dụng rộng rãi. Mặc dù vậy, tốc độ tối đa của chuẩn này là thấp nhất, thiết bị gia dụng có thể ảnh hưởng trên băng tần không được kiểm soát.

##### Chuẩn 802.11g

Được sử dụng trong mạng WLAN, là sự kết hợp của 802.11a và 802.11b với băng thông lên đến 54Mpbs, sử dụng tần số 2,4GHz để có phạm vi rộng. Tiêu chuẩn 802.11g có tốc độ cao, phạm vi tín hiệu tốt, nhưng giá thành cao hơn 802.11b và các thiết bị có thể can thiệp vào tín hiệu tần số không được kiểm soát.

##### Chuẩn 802.11i

Là tiêu chuẩn cho mạng trên diện rộng, nó cung cấp mã hóa cải tiến cho mạng tiêu chuẩn 802.11a, 802.11b, 802.11g.

##### Chuẩn 802.16

Là hệ thống tiêu chuẩn truy cập không dây băng thông rộng, cung cấp đặc tả chính thức cho các mạng MAN không dây băng thông rộng triển khai trên toàn cầu. Tiêu chuẩn này còn được gọi là WirelessMAN (WMAN).

##### Chuẩn Bluetooth

Cung cấp với khoảng cách ngắn (dưới 10m) và có băng thông nhỏ (1-3 Mbps) và được thiết kế cho các thiết bị nguồn yếu như các thiết bị cầm ta

Hình ‑ Các chuẩn mạng không dây

#### Ưu điểm của mạng không dây:

* Giá thành của mạng không dây rất thấp.
* Không bị hạn chế về vị trí kết nối.
* Dễ mở rộng.
* Tiết kiệm thời gian lắp đặt.
* Khả năng di động cao và sự tự do sử dụng.
* Các thiết bị được kết nối với nhau mà không gặp rắc rối nào về dây nối.
* Mạng không dây cho phép kết nối từ bất kỳ thiết bị nào.

#### Nhược điểm của mạng không dây

* Tốc độ của mạng không dây (1 – 125 Mbps) rất chậm so với mạng sử dụng cáp (100 Mbps đến hàng Gbps).
* Nếu hệ thống mạng không dây không được cấu hình chuẩn, các dịch vụ của bạn sẽ bị gián đoạn ngay lập tức.
* Mạng không dây có thể bị nhiễm sóng radio do thời tiết, hoặc các thiết bị không dây khác.
* Khả năng bảo mật của mạng không dây thấp vì môi trường kết nối là không khí nên sẽ khả năng bị tấn công.
* Phạm vị của mạng không dây khá nhỏ, chỉ phù hợp với diện tích của hộ gia đình, doanh nghiệp nhỏ.

### Khái niệm tấn công mạng

Hai chữ “tấn công” thường được hiểu trong chiến đấu, trong thể thao (mang tính đối kháng) là tiến đánh đối phương một cách dữ dội quyết liệt. Với an ninh mạng cũng vậy. Tấn công mạng (cyber attack) là tiến tới xâm nhập vào hệ thống mạng hạ tầng mạng máy tính, cơ sở dữ liệu, website, thiết bị của bất kỳ tổ chức/cá nhân nào.

* **Ai thường bị tấn công mạng?**

Đối tượng “con mồi” mà các hacker ưa thích đó chính là cá nhân, doanh nghiệp, tổ chức hoặc nhà nước. Tin tặc sẽ tiếp cận “con mồi” thông qua mạng nội bộ (gồm máy tính, thiết bị, con người). Thông qua con người, hacker có thể tiếp cận thông qua thiết bị di động, mạng xã hội, ứng dụng phần mềm…..

* **Tấn công mạng để làm gì?**

Trong giới hacker cũng được phân thành “hắc bạch lưỡng đạo”, tốt có mà xấu cũng có. Tấn công mạng bao gồm nhiều hình thức và mục đích khác nhau nhưng chung quy là chia làm hai hướng tốt và xấu. Cụ thể hơn người ta hay gọi là hacker mũ trắng và hacker mũ đen cho dễ phân biệt.

Hacker mũ trắng thường “tấn công mạng” theo kiểu xâm nhập vào một hệ thống mạng, thiết bị, website để tìm ra những lỗ hổng bảo mật, những phần có nguy cơ bị tấn công nhằm bảo vệ cho tổ chức cá nhân.

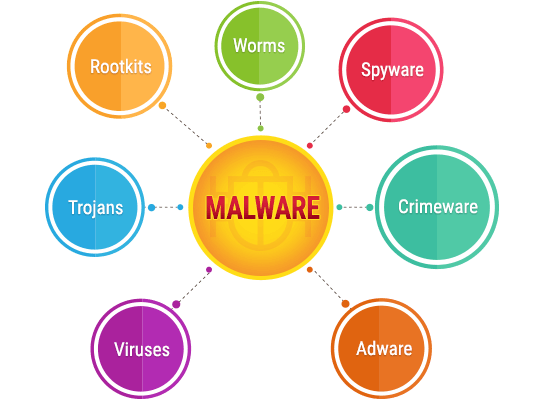
Với hacker mũ đen, họ tấn công vào hệ thống mạng để phá rối, tống tiền, thỏa mãn mục đích cá nhân hay thậm chí…cho vui.

Hình ‑ Tấn công mạng là gi

* **Những phương thức tấn công mạng phổ biến nhất**

1. Dùng phần mềm độc hại (malware)

Trong khoảng 10 năm trở lại đây dưới sự bùng nổ của CNTT thì những phần mềm độc hại (malware) cũng mọc lên như nấm để tấn công chúng ta. Malware là từ chỉ chung của mã độc tống tiền (ransomware), phần mềm gián điệp (spyware), virus và worm. Các hacker thường lợi dụng lỗ hổng bảo mật để cài cắm malware vào nhằm mục đích xấu. Khi dính malware, người dùng khi sử dụng thiết bị gặp rất nhiều phiền toái như bị chặn truy cập, hư hỏng thiết bị/hệ thống, và quan trọng nhất là người dùng sẽ bị theo dõi và đánh cắp dữ liệu.



Hình ‑ Malware

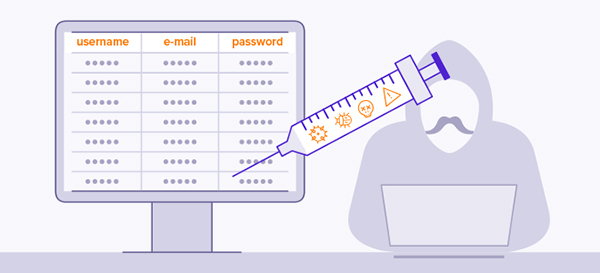
1. Tấn công giả mạo (Phishing attack)

Tấn công giả mạo (Phishing Attack) là hình thức tấn công hầu như là phổ biến nhất hiện nay. Cụ thể, nạn nhân sẽ bị hacker giả danh thành một tổ chức/cá nhân rất uy tín lừa gạt bằng hình thức gửi mail/tin nhắn kèm một đường link yêu cầu click vào kèm theo lời đe dọa là nếu không click thì sẽ bị này kia ảnh hưởng không tốt. Nạn nhân click vào link đó và sẽ được chuyển đến một website giả mạo do chính hacker đó tạo ra, nạn nhân đăng nhập thông tin cá nhân vào và coi như hacker đã có được mọi thứ của nạn nhân để lấy cắp thông tin tài khoản hệ thống/ngân hàng tín dụng….Ví dụ : bạn nhận được một email thông báo là email của ngân hàng nói rằng tài khoản của bạn có vẻ đã được thay đổi, nếu không phải bạn hãy đăng nhập để đổi mật khẩu và báo cáo với chúng tôi bằng đường link kèm theo. Bạn click vào, thấy giao diện hệt như cái web ngân hàng bạn đang xài, bạn cung cấp hết số chứng minh tên thật tên đăng nhập mật khẩu…. và rồi xem như bạn đã “giao trứng cho ác”. Khi phát hiện thì xem lại cái web đó đúng là hệt web ngân hàng, tên miền cũng đúng, chỉ có điều khác cái chấm phía sau mà thôi.

Hình ‑ Phishing attack

Đôi khi tấn công giả mạo là chỉ để lừa nạn nhân cài malware vào thiết bị mà thôi.

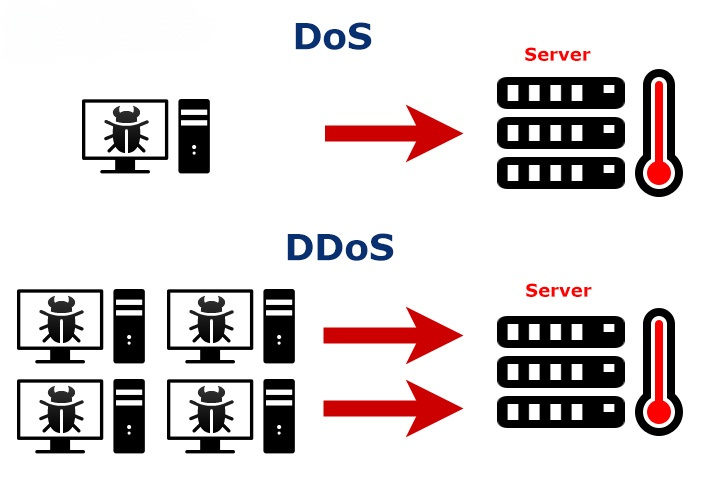
1. Tấn công cơ sở dữ liệu (SQL Injection)

Tấn công cơ sở dữ liệu (SQL Injection) là hình thức tấn công trên các server sử dụng ngôn ngữ SQL, hacker sẽ chèn một đoạn mã độc vào (thường là thông qua các thao tác yêu cầu truy vấn cơ sở dữ liệu) để lấy cắp những dữ liệu quan trọng, và thế là thông tin dữ liệu khách hàng sẽ bị lộ toàn bộ dẫn đến sự lo lắng, mất niềm tin của khách hàng đối với cá nhân/doanh nghiệp, từ đó ảnh hưởng nghiêm trọng thậm chí dẫn đến phá sản.

Hình ‑ SQL Injection

1. Tấn công từ chối dịch vụ

Đánh DoS/đánh DDoS là cụm từ mà chúng ta ít nhiều gì cũng đã nghe trên mọi phương tiện hoặc trong đời sống giữa mọi người với nhau nhất là dân IT. DoS (Denial of Service) là hình thức tấn công mà hacker tạo ra một lưu lượng truy cập vô cùng lớn ở cùng một thời điểm để làm hệ thống quá tải dẫn đến bị sập. Lúc đó người dùng không ai có thể truy cập được.

Đánh DDoS (Distributed Denial of Service) là hình thức biến thể của DoS. Với kiểu tấn công này, hacker sử dụng một mạng lưới các máy tính để làm cho hệ thống website, hệ thống server game hoặc server DNS bị sập hoặc chậm, chập chờn. Đánh DdoS nguy hiểm ở chỗ là ngày càng nhiều hacker sử dụng phương thức này cũng như là chính máy tính trong mạng lưới các máy tính cũng không biết là chính nó đang bị lợi dụng để làm công cụ tấn công mạng.

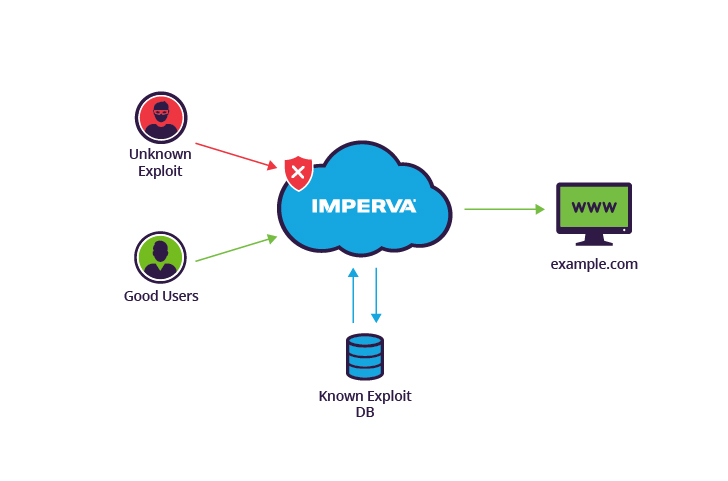
Hình ‑ Tấn công từ chối dịch vụ

1. Khai thác lỗ hổng Zero Day (Zero Day Attack)

Zero-day hay lỗ hổng zero-day là thuật ngữ dùng để chỉ những lỗ hổng đang được hacker khai thác một cách mạnh mẽ, tích cực. Tuy nhiên, những lỗ hổng này lại chưa được xác định hoặc chưa được khắc phục, vá lại bởi các cơ quan có chức năng giảm thiểu lỗ hổng bảo mật, bao gồm cả các doanh nghiệp phát triển, kinh doanh hệ thống phần mềm và phần cứng.

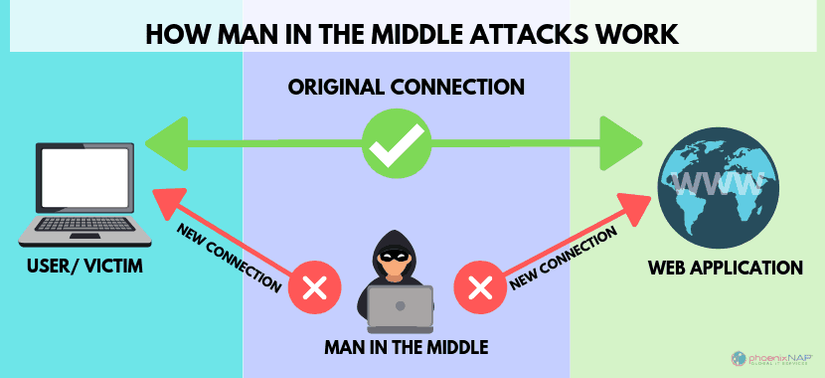
Thậm chí, ngay cả khi đã được phát hiện, hacker vẫn có thể tiếp tục khai thác lỗ hổng zero-day để đánh cắp thông tin hoặc các hành vi xấu khác. Những cuộc tấn công nhắm vào lỗ hổng zero-day được gọi là zero-day exploit hoặc zero-day attack.

Các cuộc tấn công zero-day attack được coi là mối đe dọa nghiêm trọng bởi vì chưa được phát hiện nên chẳng có bản vá hay phần mềm nào chống lại lỗ hổng zero-day. Bản chất này cũng khiến tỷ lệ khai thác thành công các lỗ hổng zero-day cao hơn nhiều và các cuộc tấn công thường ảnh hưởng tới hàng trăm ngàn, hàng triệu người dùng.

Với mức độ nguy hiểm của mình, lỗ hổng zero-day luôn được các hacker săn lùng. Thông tin về lỗ hổng zero-day luôn được bán giá cao.

Hình ‑ Khai thác lỗ hổng Zero Day (Zero Day Attack)

1. Tấn công trung gian (Man in the middle attack - MitM)

Tấn công MitM xảy ra khi ai đó ở giữa hai máy tính (máy tính xách tay và máy chủ từ xa) và có khả năng chặn lưu lượng truy cập. Kẻ đó có thể nghe trộm hoặc thậm chí chặn liên lạc giữa hai máy và đánh cắp thông tin nhạy cảm. Các cuộc tấn công man-in-the-middle là một vấn đề bảo mật nghiêm trọng.

Hình ‑ Tấn công trung gian (Man in the middle attack - MitM)

Cuộc tấn công MitM nhằm nghe trộm trên mạng để lấy thông tin hoặc ảnh hưởng đến giao dịch, hội thoại và truyền dữ liệu thời gian thực. Kẻ tấn công có thể làm điều này bằng cách khai thác các điểm yếu trong mạng hoặc bất kỳ thành phần nào của mạng, chẳng hạn như trình duyệt hoặc VoIP.

Một nhân tố khác được biết đến với việc sử dụng MitM là các chính phủ luôn tổ chức theo dõi công dân của họ, vượt qua bảo mật công nghệ, theo dõi các quốc gia thù địch, đánh cắp dữ liệu nhạy cảm hoặc tấn công các tổ chức tài chính của các quốc gia khác để lấy tiền cho các dự án của họ (như trường hợp rất thường xảy ra với Bắc Hàn).

### Khái niệm an toàn và bảo mật mạng không dây và các phương pháp mã hóa mạng không dây

#### Khái niệm

Bảo mật không dây là việc ngăn chặn truy cập trái phép hoặc làm hỏng máy tính hoặc dữ liệu bằng cách sử dụng mạng không dây, bao gồm cả mạng Wi-Fi.

Thuật ngữ này cũng có thể đề cập đến việc bảo vệ chính mạng không dây khỏi những kẻ thù tìm cách làm hỏng tính bảo mật, tính toàn vẹn hoặc tính khả dụng của mạng.

#### Các phương pháp mã hóa mạng không dây

##### Wired Equivalent Privacy – WEP

1. WEP là gì?

WEP là giao thức mạng không dây cũ từ năm 1997, cung cấp thuật toán bảo mật cho dữ liệu khi truyền trong mạng không dây.

WEP cung cấp bảo mật cho dữ liệu trên mạng không dây qua phương thức mã hóa sử dụng thuật toán RC4. Với phương thức mã hóa RC4, WEP cung cấp tính bảo mật toàn vẹn thông tin trên mạng không dây, đồng thời được xem như là một phương thức kiểm tra rà soát truy cập. Mỗi máy kết nối mạng không dây không có khóa WEP chính xác sẽ không thể truy cập đến AP và cũng không thể giải mã cũng như thay đổi dữ liệu trên đường truyền.

Đây là một tiêu chuẩn bảo mật nổi tiếng là yếu: mật khẩu mà nó sử dụng thường có thể bị bẻ khóa trong vài phút bằng máy tính xách tay cơ bản và các công cụ phần mềm có sẵn rộng rãi. WEP đã được thay thế vào năm 2003 bởi WPA hay còn gọi là Wi-Fi Protected Access.

1. Cơ chế hoạt động

Hình ‑ Cơ chế hoạt động WEP

CRC-32 (cyclic redundancy check) là một loại hàm băm (hash), được sử dụng để sinh ra giá trị kiểm thử (validation value) của một chuỗi bit có chiều dài 32bit, của các gói tin vận chuyển qua mạng hay một khối nhỏ của tệp dữ liệu. Giá trị kiểm thử dùng để dò lỗi khi dữ liệu được truyền hay lưu vào thiết bị lưu trữ. Giá trị của CRC sẽ được lưu vào trong ICV và ICV sẽ đính kèm ở cuối của khung dữ liệu (data frame).

24Bit vector khởi tạo (IV: initialization vector) kết hợp với khóa WEP (được lấy từ nơi lưu trữ khóa) để tạo ra một khóa (key) 64bit làm đầu vào cho RC4 để tạo ra dãy các bit ngẫu nhiên (keystream).

Sau đó, dãy các bit được XOR với dữ liệu và ICV tạo ra dữ liệu được mã hóa. IV và dữ liệu mã hóa được đưa vào MAC frame để truyền đi.

1. Lỗ hổng trong mã hóa WEP

Khóa bảo mật có chiều dài 64bit, điều này sẽ dễ dàng cho các hacker sử dụng biện pháp tấn công vét cạn để tìm ra khóa.

Mã hóa sử dụng thuật toán mã hóa dòng bit RC4, vì vậy cần đảm bảo cho các dữ liệu giống nhau sẽ không cho ra kết quả giống nhau. Chính vì vậy, một giá trị IV (vector khởi tạo) được sinh ra ngẫu nhiên và cộng thêm vào với khóa để tạo ra các khóa khác nhau cho mỗi lần mã hóa. Do đó giá trị IV không được mã hóa và đặt trong header của gói dữ liệu, nên bất cứ ai lấy được dữ liệu trên mạng đều có thể thấy được. Với các giá trị IV được sử dụng với cùng một khóa trên một gói dữ liệu mã hóa (gọi là va chạm IV), hacker có thể bắt gói dữ liệu và tìm ra khóa WEP.

1. Cách tấn công WEP

Đầu tiên, ta sẽ bắt đầu với thiệt bị mạng không dây (như modem) và đưa vào kênh truyền.

Kiểm tra tín hiệu của thiết bị mạng không dây ở điểm truy cập.

Sử dụng công cụ giống như Airplay để giả mạo xác thực tới điểm truy cập.

Wifi bắt đầu đi vào công cụ như Airodum hoặc CAIN&Abel với bộ lọc ID để tìm kiếm các IV.

Công cụ mã hóa các gói wifi bắt đầu như Airplay trong ARP được gửi đi để lấy tín hiệu trong các gói.

Chạy công cụ phá khóa như CAIN&Abel hoặc aircrack để giải mã hóa key từ các IV.

1. Biện pháp chống tấn công WEP

Sử dụng khóa WEP có độ dài 128bit (khóa WEP cho phép sử dụng khóa dài 40bit, 64bit, 128bit). Sử dụng khóa 128bit gia tăng số lượng gói dữ liệu, hacker cần phải phân tích IV, gây khó khăn và kéo dài thời gian giải mã WEP.

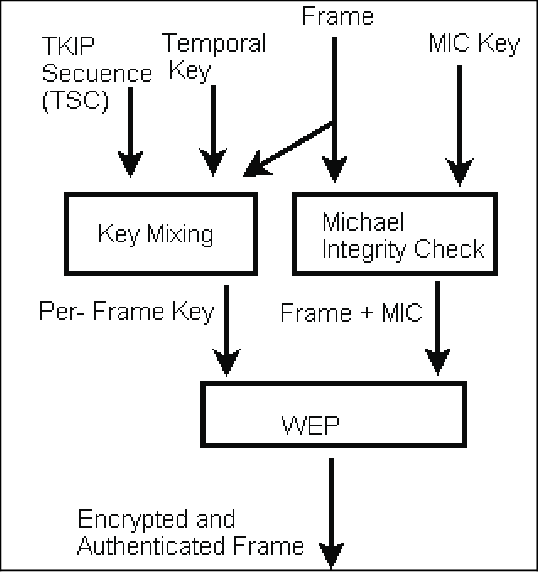
Thay đổi khóa WEP định kì. Do WEP không hỗ trợ phương thức thay đổi khóa tự động nên chúng ta cần phải tự thay đổi khóa, để tránh tình trạng bị lỗ khóa.

Sử dụng các công cụ theo dõi số liệu thống kê trên đường truyền không dây. Do các công cụ dò khóa WEP cần phải bắt được thông số lượng gói dữ liệu và hacker có thể phải sử dụng các công cụ phát sinh dữ liệu nên sự biến đổi về lưu lượng dữ liệu có thể là dấu hiệu của một cuộc tấn công WEP. Điều đó giúp các nhà quản trị mạng phát hiện và có biện pháp phòng chống kịp thời.

##### WPA, WPA2, WPA3

1. WPA, WPA2 và WPA3 là gì?
   1. WPA

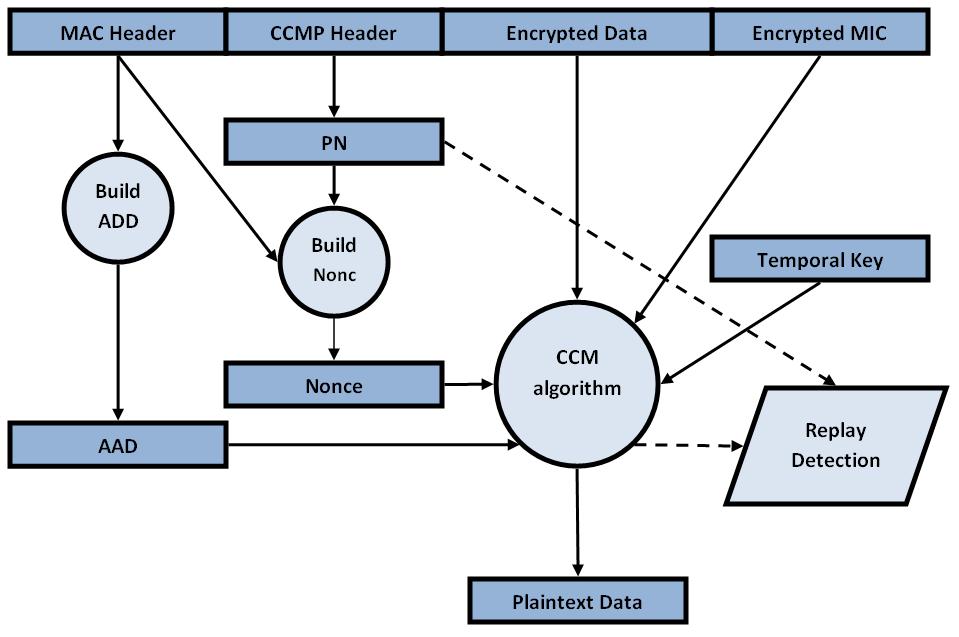
WPA (Wi-Fi Protected Access) là chuẩn bảo mật được phát triển để thay thế WEP do mã hóa WEP đã lỗi thời và dễ dàng bị phá vỡ.

WPA có nhiều cải tiến so với WEP như hỗ trợ TKIP (Temporal Key Integrity Protocol) để ngăn chặn việc đánh cắp các gói tin truyền trong wifi và MIC (Message Integrity Check) nhằm đảm bảo dữ liệu không bị giả mạo. Tuy vậy, WAP vẫn còn tồn đọng một vài lỗ hổng từ WEP.

Hình ‑ WPA (Wi-Fi Protected Access)

* 1. WPA2

WPA2 là chuẩn bảo mật thay thế cho WPA kể từ năm 2006. WPA2 còn thay thế TKIP bằng giao thức CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol).

CCMP là một giao thức truyền dữ liệu và kiểm soát tính truyền dữ liệu thống nhất để bảo đảm cả tính bảo mật và nguyên vẹn của dữ liệu được truyền đi. Hiện nay, phần lớn bộ định tuyến wifi đều sử dụng WPA2.

Hình ‑ Giao thức CCMP

* 1. WPA3

WPA3 là chuẩn bảo mật wifi mới nhất hiện nay và được áp dụng trên một số bộ định tuyến sản xuất trong năm 2019. WPA3 được nâng cấp tối ưu hơn so với chuẩn bảo mật WPA2.

WPA3 mang đến khả năng bảo mật trên các mạng wifi công cộng, ngăn chặn việc hacker có thể xem trộm hay đánh cắp thông tin khi bạn kết nối với wifi công cộng như ở sân bay, nhà hàng,...

Với chuẩn bảo mật WPA3, hacker khó có thể đoán mật khẩu wifi của bạn, đồng thời ngăn chặn hacker giải mã lưu lượng ngay cả khi họ đã từng biết mật khẩu của wifi.

1. Cơ chế hoạt động của WPA, WPA2
2. Cơ chế hoạt động của WPA

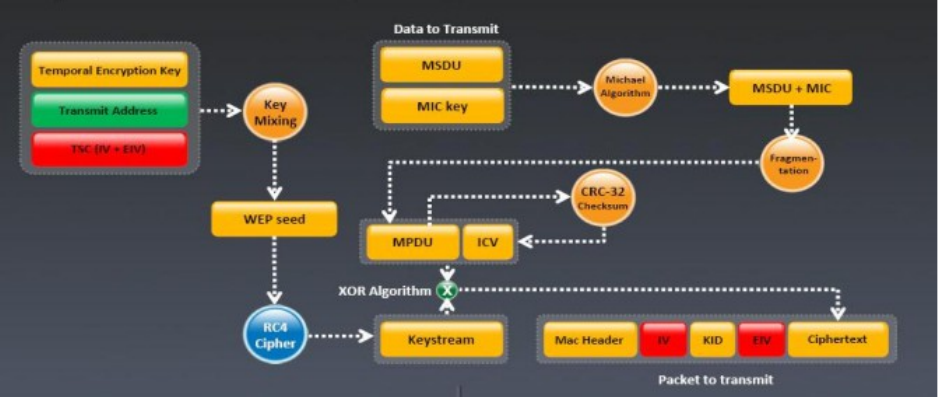
Mã hóa key temporal, truyền địa chỉ và TKIP đếm liên tục được sử dụng như dữ liệu đầu vào để RC4 sinh ra dạy khóa.

MAC Service Data Unit (MSDU) và hộp thoại kiểm tra tính toàn vẹn (MIC) được tổ hợp sử dụng thuật toán Michael.

Tổ hợp của MSDU và MIC được băm để sinh ra MAC protocol data unit (MPDU).

32bit kiểm tra tính toàn vẹn ICV được tính toán cho MPDU.

Tổ hợp của MPDU và ICV được phân theo từng bit xor với dãy khóa để sinh ra dữ liệu mã hóa.

IV thêm dữ liệu mã hóa để sinh ra MAC frame.

Hình ‑ Cơ chế hoạt động của WPA

1. Cơ chế hoạt động WPA2

CCMP dựa trên CCM là một chế độ mật mã của AES được sử dụng để xác thực một khối được mã hóa. Trong CCM, kích thước khối 128 bit được mã hóa. Cipher Block Chaining MAC (CBC-MAC) được sử dụng trong CCM để xác thực và bảo vệ tính toàn vẹn. Để ngăn chặn các cuộc tấn công phát lại, CCMP sử dụng một nonce được xây dựng bằng cách sử dụng số thứ tự PN 48-bit. CCMP được coi là giải pháp tốt nhất cho cả tính bảo mật và tính toàn vẹn. Nó sử dụng cùng một khóa mật mã cho cả tính bảo mật và tính toàn vẹn, làm giảm độ phức tạp. CCMP cung cấp tính toàn vẹn của cả tiêu đề gói và gói payload.

1. Cách tấn công WPA/WPA2

WPA PSK: sử dụng password do người sử dụng cài đặt để chạy TKIP, không thể phá khóa giống như các gói key nhưng các key có thể bị tấn công bằng phương pháp vét cạn theo từ điển.

Vét cạn WPA keys: có thể sử dụng công cụ như aircrack, airplay, Kismac để giải mã khóa WPA.

Offline attack: chỉ cần ở gần các điểm truy cập và mất vài giây để lấy được WPA/WPA2 từ các thiết bị cầm tay, do lấy được đúng các kiểu gói dữ liệu, hacker có thể phá khóa WPA một cách độc lập.

Tấn công không xác thực (deauthentication attack):

* Kẻ tấn công xác định mục tiêu tấn công là các người dùng trong mạng wireless và các kết nối của họ (Access Point đến các kết nối của nó).
* Sau đó chèn các frame yêu cầu xác thực lại vào mạng WLAN bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của AP và các người dùng.
* Người dùng wireless khi nhận được frame yêu cầu xác thực lại thì nghĩ rằng chúng do AP gửi đến.
* Sau khi ngắt được một người dùng ra khỏi dịch vụ không dây, kẻ tấn công tiếp tục thực hiện tương tự đối với các người dùng còn lại.
* Thông thường người dùng sẽ kết nối lại để tiếp tục dịch vụ nhưng kẻ tấn công sẽ nhanh chóng tiếp tục gửi các gói yêu cầu xác thực lại cho người dùng.

1. Biện pháp phòng chống tấn công WPA

Passphrases: con đường để phá WPA là kiểm tra password với các thiết bị cầm tay xử lý xác thực và nếu password được làm phức tạp thêm thì sẽ có khó thể phá giải.

Client setting (cài đặt người dùng): chỉ sử dụng WPA2 với mã hóa AES/CCMP. Do người dùng cài đặt (làm đúng theo server, đúng địa chỉ).

Additional Controls (tăng thêm các trình điều khiển/quản lý): sử dụng mạng cá nhân (VPN), công cụ điều khiển truy cập mạng (NAC) hoặc bảo vệ truy cập mạng (NAP).

### Mô hình kiến trúc hạ tầng mạng

#### Mô hình hệ thống mạng phân cấp

Mô hình phân cấp cho phép chúng ta thiết kế các đường mạng sử dụng những chức năng chuyên môn kết hợp với một tổ chức có thứ bậc. Việc thiết kế mạng đòi hỏi phải xây dựng một mạng thỏa mãn nhu cầu hiện tại và có khả năng mở rộng trong tương lai.

Thiết kế mạng phân cấp: Một thiết kế mạng LAN truyền thống phân cấp có ba lớp:

* Lớp lõi thực hiện quá trình vận chuyển nhanh chóng giữa các thiết bị chuyển mạch phân phối trong mạng.
* Lớp phân phối cung cấp kết nối dựa trên nền tảng ứng xử.
* Lớp truy cập cung cấp cho nhóm làm việc và người sử dụng truy cập vào mạng.

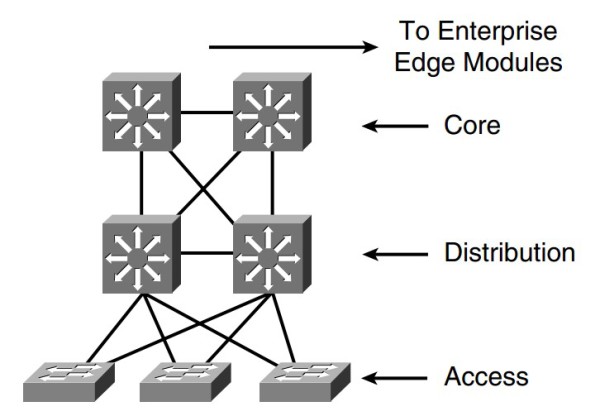
Cách tiếp cận này cung cấp khả năng lập kế hoạch chính xác hơn và tổng chi phí cho quá trình triển khai mạng nhỏ nhất. Chúng ta không phải thực hiện các lớp phân cấp như các thực thể vật lý riêng biệt, chúng được định nghĩa để hỗ trợ sự thành công thiết kế mạng và đại diện chức năng hoạt động bên trong một mạng.

* Ưu điểm của mạng phân lớp:
* Tiết kiệm chi phí
* Dễ triển khai
* Có khả năng mở rộng mạng
* Dễ quản lí, khắc phục sự cố

#### Mô hình kiến trúc mạng doanh nghiệp

Mô hình phân cấp cho phép chúng ta thiết kế các đường mạng mà sử dụng những chức năng chuyên môn kết hợp với một tổ chức có thứ bậc. Việc thiết kế mạng đơn giản là nhiệm vụ đòi hỏi phải xây dựng một mạng mà nó thỏa mãn nhu cầu hiện tại và có thể phát triển tiếp theo nhu cầu ở tương lai. Mô hình phân cấp sử dụng các lớp để đơn giản nhiệm vụ kết nối mạng, mỗi lớp có thể chỉ tập trung vào một chức năng cụ thể, cho phép chúng ta lựa chọn các tính năng và các hệ thống thích hợp cho mỗi lớp.

Mô hình phân cấp áp dụng cho việc thiết kế cả mạng LAN và mạng WAN, việc sử dụng mô hình phân cấp cho thiết kế mạng của bạn mang lại những lợi ích sau:

* Có khả năng mở rộng.
* Dễ dàng triển khai.
* Khắc phục lỗi.
* Quản lý dễ dàng

Hình ‑ Mô hình mạng phân lớp

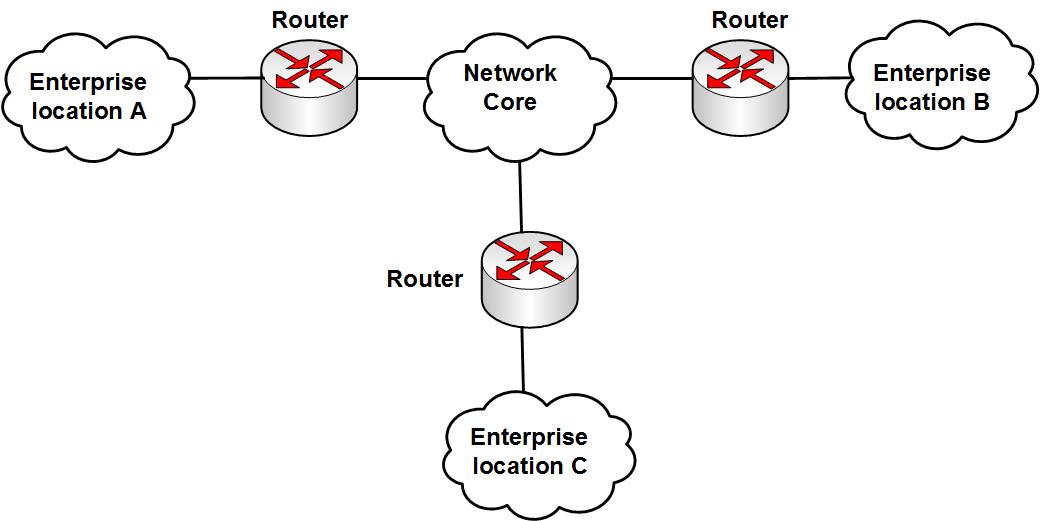
##### Lớp mạng trung tâm (Core layer)

Tốc độ vận chuyển dữ liệu rất nhanh, liên kết với các lớp mạng truy cập và lớp mạng phân bố khác. Lớp này còn được coi là đại lộ liên kết các đường nhỏ với nhau.

Nếu có một sự hư hỏng xảy ra ở lớp lõi, hầu hết các người dùng trong mạng LAN đều bị ảnh hưởng. Vì vậy, sự dự phòng là rất cần thiết tại lớp này. Do lớp lõi vận chuyển một số lượng lớn dữ liệu, nên độ trễ tại lớp lõi phải là cực nhỏ.Tại lớp lõi, ta không nên làm bất cứ một điều gì có thể ảnh hưởng đến tốc độ chuyển mạch tại lớp lõi như là tạo các access list, routing giữa các VLAN với nhau hay packet filtering.

Bao gồm các đặc điểm sau:

* Vận chuyển dữ liệu nhanh.
* Độ tin cậy cao.
* Có tính dự phòng.
* Khả năng chịu lỗi.
* Chính sách QoS (Chất lượng dịch vụ)

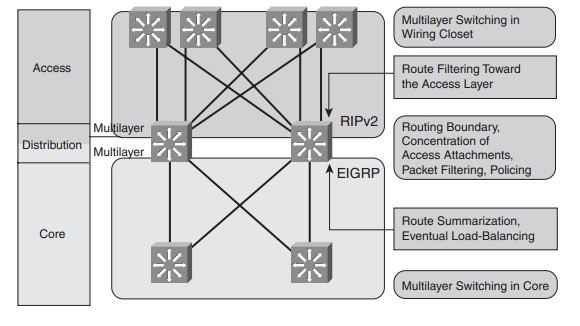


Hình ‑ Lớp mạng trung tâm

##### Lớp mạng phân bố (Distribution Layer)

Phối là xử lý dữ liệu như là: định tuyến (routing), lọc gói (filtering), truy cập mạng WAN, tạo access list... Lớp Phân Phối phải xác định cho được con đường nhanh nhất mà các yêu cầu của user được đáp ứng. Sau khi xác định được con đường nhanh nhất, nó gửi các yêu cầu đến lớp Lõi. Lớp Lõi chịu trách nhiệm chuyển mạch các yêu cầu đến đúng dịch vụ cần thiết.Lớp Phân Phối là nơi thực hiện các chính sách (policies) cho mạng.

Lớp này nằm giữa lớp mạng truy cập và lớp mạng trung tâm, có thể có một số vai trò đáp ứng một số giao tiếp giúp giảm tải cho lớp mạng trung tâm.

* Chính sách cơ sở kết nối.
* Cân bằng tải.
* Chính sách QoS.
* Tập hợp các kết nối WAN, LAN.
* Chức năng chọn lọc dữ liệu. - Xác định Broadcast và Multicast Domain.
* Định tuyến giữa các VLAN với nhau.
* Thuyên chuyển truyền thông. (ví dụ: giữa mạng Ethernet và Token Ring) - Phân phối định tuyến các Domain.
* Phân chia ranh giới giữa định tuyến động và định tuyến tĩnh. - Route Summarizations.

Hình ‑ Các chức năng của lớp phân bố. Nguồn Microsoft

##### Lớp mạng truy cập (Access Layer)

Mang đến sự kết nối người dùng với các tài nguyên trên mạng hoặc các giao tiếp với lớp mạng phân bố. Lớp này sử dụng các chính sách truy cập chống lại những kẻ xâm nhập bất hợp pháp, mang đến các kết nối như: WAN, Frame Relay, Leased Lines.

* Chuyển mạch lớp 2.
* Bảo mật cổng.
* Tính sẵn sàng cao.
* Ngăn chặn Broadcast.
* Phân loại QoS.
* Kiểm tra giao thức chuyển đổi địa chỉ (ARP).
* Spanning tree.
* Hổ trợ VLAN
* Hổ trợ VLAN cho VoIP

## Phương pháp xác thực mạng không dây và lỗ hổng của mạng không dây

### Phương pháp xác thực mạng không dây

#### Hệ thống xử lý xác thực

* Đầu tiên, khách hàng sẽ gửi một khung 802.11 quản lí xác thực có chứa SSID của khách hàng.
* Điểm truy cập sẽ kiểm tra SSID của khách hàng và gửi lại một khung xác thực.
* Khách hàng có thể kết nối vào mạng.

#### Chia sẻ quá trình xác thực khóa

* Khách hàng gửi một hộp thoại xác thực tới điểm truy cập.
* Điểm truy cập gửi hộp thoại quay trở lại.
* Khách hàng điền thông tin vào, sau đó hộp thoại mã hóa và gửi đến cho điểm truy cập.
* Điểm truy cập giải mã, nếu đúng thì xác thực người dùng.
* Sau đó, khách hàng sẽ kết nối được với mạng.

#### Xác thực mạng không dây sử dụng máy chủ tập trung

* Khách hàng gửi một yêu cầu kết nối tới địa chỉ truy cập (Access Point - AP), AP sẽ gửi lại một yêu cầu và khách hàng trả lời yêu cầu của AP.
* AP gửi yêu cầu của người dùng tới máy chủ, trước tiên yêu cầu được gửi tới cổng không hạn chế.
* Máy chủ gửi cho người dùng thông qua AP, cơ chế xác thực sẽ được sử dụng.
* Sau đó người dùng gửi thông tin đăng nhập tới máy chủ thông qua AP.
* Máy chủ gửi khóa mã hóa xác thực tới AP nếu thông tin đăng nhập được chấp nhận.
* Cuối cùng, AP gửi cho người dùng khóa mã hóa xác thực với phiên sử dụng.

### Lỗ hổng của mạng không dây

Mạng không dây kết nối với các thiết bị sử dụng vô tuyến, bất kỳ thiết bị điện tử nào nằm trong vùng phủ sóng của mạng không dây đều có thể kết nối với mạng. Chính vì thế các đối tượng xấu có thể dễ dàng xâm nhập vào mạng không dây để tấn công người dùng.

Lỗ hổng trong quá trình xác thực người dùng giúp cho kẻ tấn công có thể tấn công vào mạng không dây. Chẳng hạn, kẻ tấn công có thể giả mạo khách hàng gửi thông điệp yêu cầu truy c6ạp mạng đến AP. Sau đó điểm truy cập sẽ trả lời lại bằng một thông điệp và chờ người dùng xác nhận nhưng kẻ tấn công không xác nhận lại.

Trong quá trình xác thực người dùng, người dùng cần phải gửi gói tin đến cho AP, sau đó AP gửi thông điệp phản hồi lại cho người dùng. Chính vì vậy, khi kẻ tấn công xâm nhập vào mạng và giả danh người dùng sau đó gửi thông điệp đến cho AP, AP gửi thông điệp phản hồi lại, kẻ tấn công sẽ dựa vào thông điệp của AP gửi về và có thể sử dụng các công cụ để tìm ra khóa và tấn công vào mạng.

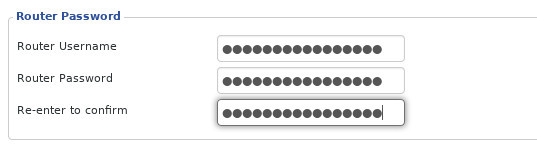
## Các phương pháp bảo mật mạng không dây cơ bản

### Thay đổi tên mạng (SSID)

Thay đổi tên mạng (SSID) là cách bảo mật wifi thường được nhiều gia đình áp dụng bởi cách làm khá đơn giản. Bạn nên thay đổi tên mạng mặc định để tránh trường hợp kẻ tấn công biết được SSID mặc định. Bạn hãy hình dung là, mỗi sản phẩm wifi khi sản xuất ra đều có bộ định tuyến (router) và ISP. Nếu kẻ tấn công tìm ra được bộ định tuyến Router và vào được tên mạng SSID của bạn thì họ sẽ rất dễ dàng tấn công. Do đó việc thay đổi tên mạng SSID là rất cần thiết để đảm bảo an toàn khi truy cập internet bằng mạng không dây.

Hình ‑ Thay đổi tên mạng

### Thay đổi tên người dùng và mật khẩu

Thay đổi tên người dùng và thay đổi mật khẩu cũng là cách để bảo mật wifi. Bởi thông thường các hacker sẽ thường thử tấn công mạng nhà bạn bằng tên người dùng và mật khẩu. Nếu không hack được thì chúng mới áp dụng cách tấn công khác. Điều đặc biệt là các hacker này thường có công cụ để tra cứu dò ra mật khẩu cũng như tên người dùng rất nhanh. Do đó, bạn không nên để mật khẩu quá đơn giản. Lời khuyên cho bạn là hãy thay đổi tên người dùng và mật khẩu bằng một dãy ký tự khó đoán. Bạn cũng nên kết hợp chữ hoa chữ thường và các con số để tạo nên một dãy tên người dùng và mật khẩu vô nghĩa. Điều này sẽ khiến cho những kẻ tấn công khó dò ra được tên người dùng và mật khẩu của bạn hơn.

Hình ‑ Thay đổi username và password

### Sử dụng mã hóa mạnh để bảo mật wifi

Nhiều người cho rằng mạng wifi không cần mã hóa. Tuy nhiên đây là một suy nghĩ sai lầm. Nếu bạn chưa dùng mã hóa cho mạng wifi thì những kẻ tấn công rất dễ hack wifi nhà bạn. Để mã hóa bảo mật wifi bạn có thể chọn “WPA2 Personal” cho mạng nhà mình. Nếu được bạn hãy thiết lập phiên bản mã hóa doanh nghiệp. Những cách thiết lập phiên bản doanh nghiệp khá phức tạp. Bạn cũng cần lưu ý, đối với thuật toán mã hóa bạn nên chọn AES và không nên dùng TKIP. Bởi AES sẽ cung cấp mã hóa mạnh khó tấn công hơn TKIP.

Hình ‑ Sử dụng mã hóa WPA2 Personal và thuật toán mã hóa AES

### Chọn mật khẩu mạnh

Cách bảo mật wifi đơn giản tiếp theo bạn nên áp dụng là chọn mật khẩu mạnh cho wifi nhà mình. Một mật khẩu wifi mạnh cần đảm bảo một vài yếu tố về độ dài (độ dài lý tưởng là ít nhất 15 ký tự), dãy mật khẩu nên có các ký tự đặc biệt.

Hình ‑ Chọn mật khẩu mạnh

### Thay đổi mật khẩu wifi

Dù mật khẩu của bạn đã rất mạnh thì sau khoảng vài ba tháng bạn nên đổi mật khẩu wifi bằng một cụm mật khẩu khác. Cách làm này nhằm đảm bảo mạng wifi nhà bạn được bảo mật tuyệt đối.

### Vô hiệu hóa mạng khách

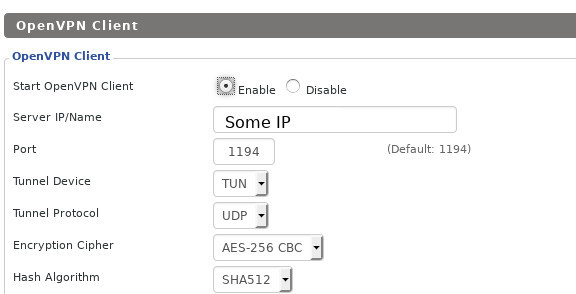
Vô hiệu hóa mạng khách cũng là cách bảo mật mạng không dây an toàn cho gia đình bạn. Nhiều gia đình để mạng wifi chế độ mở giúp ai cũng có thể kết nối wifi mà không cần mật khẩu. Tuy nhiên cách để mạng khách mở như này rất nguy hiểm. Tốt nhất là bạn nên vô hiệu hóa mạng khách bằng một dãy mật khẩu riêng. Và sau khi họ rời đi bạn hãy thay đổi mật khẩu wifi gia đình mình nhé.

### Bật tường lửa để bảo vệ wifi

Một số bộ định tuyến wifi sẽ được cài sẵn tường lửa. Để bảo mật mạng không dây bạn nên bật tường lửa này lên. Tường lửa được ví như hàng phòng thủ giúp bảo vệ mạng không dây của gia đình bạn. Tường lửa có tác dụng quản lý và lọc tất cả các lưu lượng truy cập vào mạng wifi gia đình bạn. Thậm chí nó có thể khóa, ngăn chặn các truy cập nguy hiểm cho mạng không dây.

Hình ‑ Bật tường lửa

### Sử dụng VPN

Một ưu điểm khi sử dụng VPN là bạn có thể ngăn chặn các kẻ tấn công vào mạng wifi của gia đình mình. Cách dùng VPN như sau: Bạn kết nối wifi với máy chủ VPN. Sau đó kết nối wifi với internet. Các lưu lượng truy cập sẽ được quản lý thông qua VPN. Đặc biệt, VPN có thể ẩn danh một phần lưu lượng truy cập mạng. Điều này sẽ giúp bảo mật wifi tốt hơn.

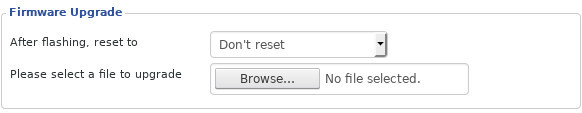
Hình ‑ Sử dụng VPN

### Tắt WPS

WPS được hiểu là một hệ thống được kết nối với wifi đã được mã hóa mà không cần sử dụng mật khẩu. Nhược điểm của WPS là nó có thể tạo điều kiện cho những kẻ tấn công dễ dàng tấn công mạng không dây hơn. Do đó, lời khuyên cho bạn là hãy tắt WPS để đảm bảo an toàn tối đa cho mạng không dây của gia đình.

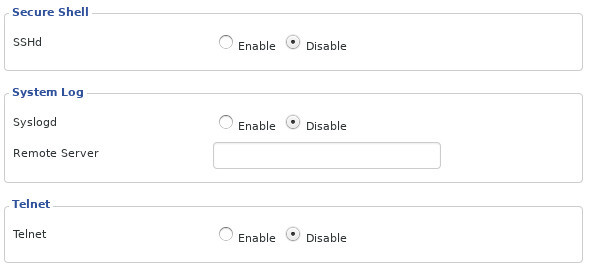
### Quản lý firmware của bộ định tuyến

Bộ định tuyến wifi thường có một hệ điều hành tương tự như máy tính vậy. Nhưng hệ điều hành này không thể tự update của bản cập nhật bảo mật mạng không dây như một chiếc máy tính. Một số bộ định tuyến có thể update các bản cập nhật firmware từ trên mạng.

Còn các trường hợp khác thì bạn phải tải các bản câp nhật xuống rồi lại tải lên bộ định tuyến từ máy tính để cập nhật cho wifi. Lời khuyên cho bạn là vài ba tháng nên update bản cập nhật cho wifi định kỳ để đảm bảo tính bảo mật cho wifi.

Hình ‑ Quản lý firmware

### Tắt quản lý từ xa/ dịch vụ không cần thiết

Một số bộ định tuyến cho phép quản lý từ xa. Điều này có thể sẽ giúp bạn quản lý bộ định tuyến dễ dàng hơn. Nhưng nó cũng tiềm ẩn nhiều rủi ro và nguy hiểm cho mạng không dây nhà bạn. Bởi những kẻ tấn công hoàn toàn có thể hack truy cập vào giao diện quản lý bộ định tuyến và xâm nhập mạng không dây nhà bạn. Do đó, để đảm bảo tính bảo mật wifi bạn nên tắt dịch vụ quản lý từ xa của bộ định tuyến.

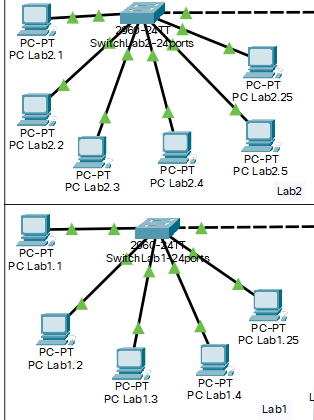
Hình ‑ Tắt các dịch vụ từ xa không cần thiết

# MÔ HÌNH DEMO

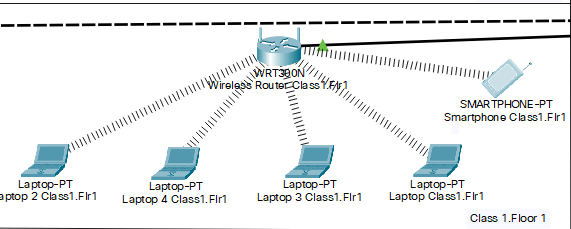
## Mô hình đề xuất

Hình ‑ Mô hình để xuất

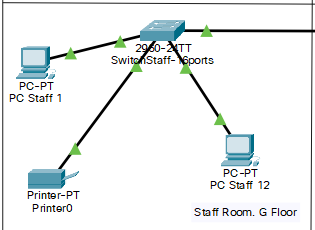
Chúng em phát triển mạng lưới trong tòa nhà 3 tầng, 2 phòng thí nghiệm, 4 phòng học thường, 1 phòng giáo viên, 1 phòng giáo viên, 1 phòng tổng giám đốc, 1 phòng quản lý mạng.

Mỗi phòng thí nghiệm chứa 25 máy tính kết nối với một bộ chuyển mạch 24 cổng:

Hình ‑ Mô phỏng mạng cho phòng thí nghiệm

Mỗi lớp học thông thường có một bộ định tuyến không dây cung cấp cho sinh viên kết nối wifi:

Hình ‑ Mô phỏng mạng cho phòng học

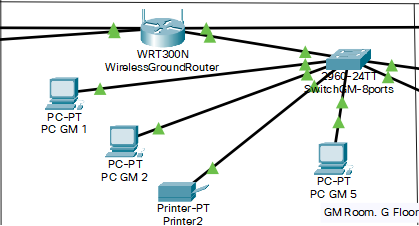
Phòng nhân viên có 12 máy tính cho nhân viên và một máy in kết nối với bộ chuyển mạch 16 cổng:

Hình ‑ Mô phỏng mạng cho phòng nhân viên

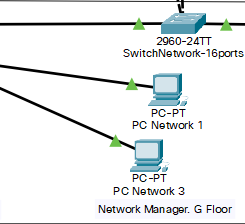
Phòng giáo viên có 15 máy vi tính, cung cấp cho 15 giáo viên làm việc và quản lý, đồng thời có một máy in kết nối với bộ chuyển đổi 16 cổng:



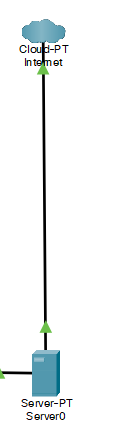
Hình ‑ Mô phỏng cho mạng phòng giáo viên

Phòng GM có 5 máy tính máng cỏ và một máy in kết nối với bộ chuyển mạch 8 cổng:

Hình ‑ Mô phỏng cho mạng phòng GM

Phòng quản lý mạng có 3 máy tính và một bộ chuyển mạch kết nối 3 máy tính và tất cả các bộ chuyển mạch trong tòa nhà:

Hình ‑ Mô phỏng cho mạng phòng quán lý mạng

Switch trong phòng quản lý mạng kết nối với một máy chủ và máy chủ đó kết nối thẳng với Internet:

Hình ‑ Mô phỏng kết nối tới mạng internet

Tóm lại, chúng em, đã thiết kế một hệ thống mạng phù hợp với điều kiện yêu cầu và không cần sử dụng thêm tài nguyên.

Hệ thống bao gồm các tài nguyên đã cho và ba bộ chuyển mạch 24 cổng, hai bộ chuyển mạch 16 cổng, ba bộ chuyển mạch 8 cổng và 4 bộ định tuyến không dây và một máy chủ.

## Cấu hình thiết bị

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP** |
| Web Server | FastEthernet0 | 192.168.5.200/24 |
| WirelessGroundRouter | Internet | DHCP |
| LAN | 192.168.6.1 |
| Wireless Router Class1.Flr1 | Internet | DHCP |
| LAN | 192.168.2.1 |
| Wireless Router Class2.Flr1 | Internet | DHCP |
| LAN | 192.168.3.1 |
| Wireless Router Class1.Flr2 | Internet | DHCP |
| LAN | 192.168.0.1 |
| Wireless Router Class2.Flr2 | Internet | DHCP |
| LAN | 192.168.1.1 |
| PC Network 1 | FastEthernet0 | DHCP |
| PC Network 3 | FastEthernet0 | DHCP |
| PC GM 1 | FastEthernet0 | DHCP |
| PC GM 2 | FastEthernet0 | DHCP |
| Printer2 | FastEthernet0 | DHCP |
| PC Teacher 15 | FastEthernet0 | DHCP |
| PC Teacher 1 | FastEthernet0 | DHCP |
| PC Teacher 2 | FastEthernet0 | DHCP |
| Printer1 | FastEthernet0 | DHCP |
| Printer3 | FastEthernet0 | DHCP |
| PC Staff 12 | FastEthernet0 | DHCP |
| PC Staff 1 | FastEthernet0 | DHCP |
| Smartphone Class2.FLr | Wireless | DHCP |
| Laptop Class2.Flr1 | Wireless | DHCP |
| Smartphone Class1.Flr1 | Wireless | DHCP |
| Laptop Class1.Flr1 | Wireless | DHCP |
| PC Lab1.25 | FastEthernet0 | DHCP |
| PC Lab1.1 | FastEthernet0 | DHCP |
| Smartphone Class2.Flr2 | Wireless | DHCP |
| Laptop Class2.Flr2 | Wireless | DHCP |
| Smartphone Class1.Flr2 | Wireless | DHCP |
| Laptop Class1.Flr2 | Wireless | DHCP |
| PC Lab2.25 | FastEthernet0 | DHCP |
| PC Lab2.1 | FastEthernet0 | DHCP |
| Tablet Class1.Flr2 | Wireless | DHCP |
| Laptop 2 Class1.Flr2 | Wireless | DHCP |
| Smartphone 2 Class1.Flr2 | Wireless | DHCP |
| Laptop 3 Class1.Flr1 | Wireless | DHCP |
| Laptop 4 Class1.Flr1 | Wireless | DHCP |
| Tablet Class2.Flr1 | Wireless | DHCP |
| Tablet 2 Class2.Flr1 | Wireless | DHCP |
| Laptop 2 Class2.Flr1 | Wireless | DHCP |
| Laptop 3 Class2.Flr1 | Wireless | DHCP |
| Laptop 2 Class2.Flr2 | Wireless | DHCP |
| Laptop 3 Class2.Flr2 | Wireless | DHCP |
| PC Lab1.2 | FastEthernet0 | DHCP |
| PC Lab1.3 | FastEthernet0 | DHCP |
| PC Lab1.4 | FastEthernet0 | DHCP |
| PC Lab1.1 | FastEthernet0 | DHCP |
| PC Lab2.2 | FastEthernet0 | DHCP |
| PC Lab2.3 | FastEthernet0 | DHCP |
| PC Lab2.4 | FastEthernet0 | DHCP |
| PC Lab2.5 | FastEthernet0 | DHCP |

Bảng 3‑1 Bảng địa chỉ IP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **WLAN** | **SSID** | **Authentication** | **Username** | **Password** |
| Wireless Router Class2.Flr1 | Class2Flr1 | WPA2 Personal | N/A | class2flr1 |
| Wireless Router Class1.Flr1 | Class1Flr1 | WPA2 Personal | N/A | class1flr1 |
| Wireless Router Class2.Flr2 | Class2Flr2 | WPA2 Personal | N/A | class2flr2 |
| Wireless Router Class1.Flr2 | Class1Flr2 | WPA2 Personal | N/A | class1flr2 |
| WirelessGroundRouter | Default | WPA2 Personal | N/A | GMRoom123 |

Bảng 3‑2 Bảng thông tin WLAN

Cấu hình chi tiết các thiết bị:

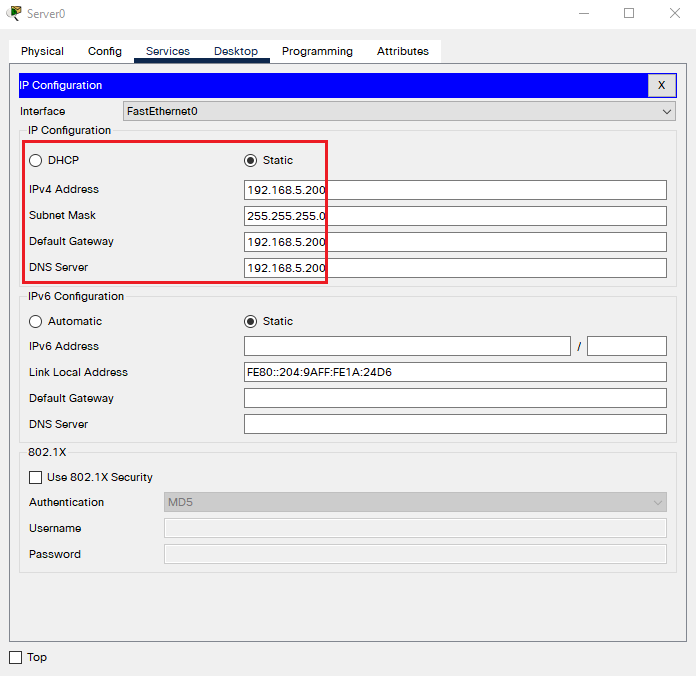
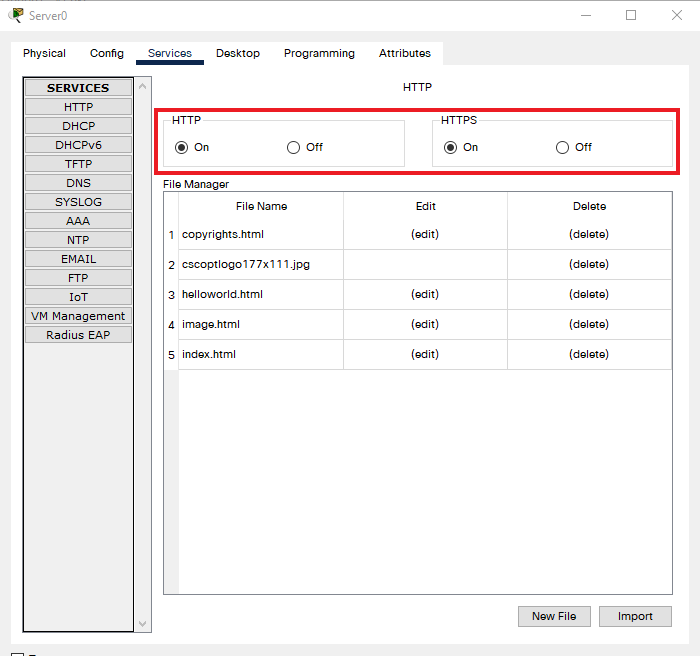
### Cấu hình Server

IPv4 Address : 192.168.5.200

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.5.200

DNS Server : 192.168.5.200



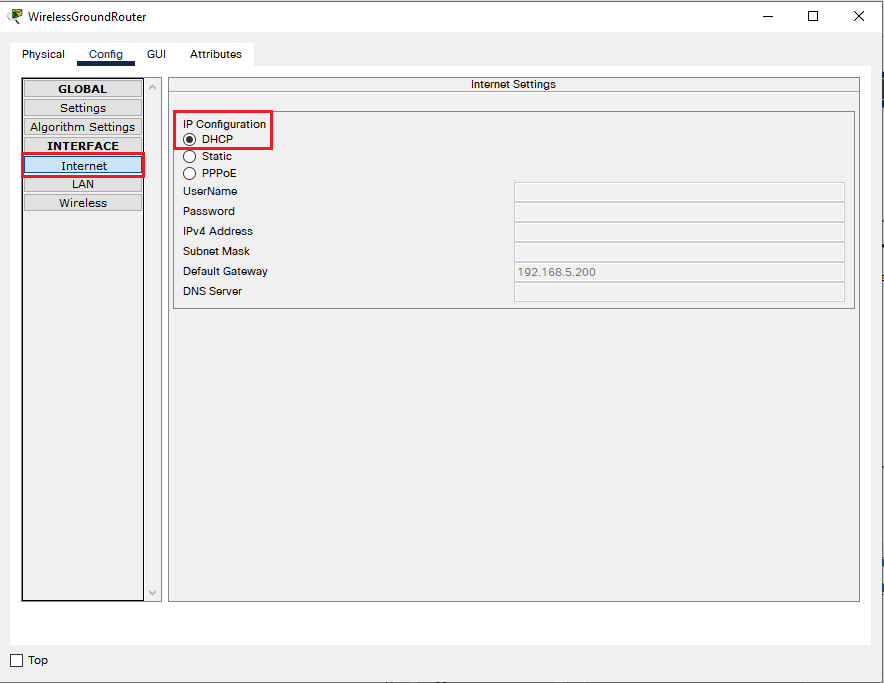
Hình ‑ Cấu hình DNS sẻver

Hình ‑ HTTP: ON , HTTPS: ON

Hình ‑ Cấu hình Server 0

### Cấu hình WirelessGroundRouter

Internet Settings:

IP : DHCP

Hình ‑ Cấu hình c wireless ground router

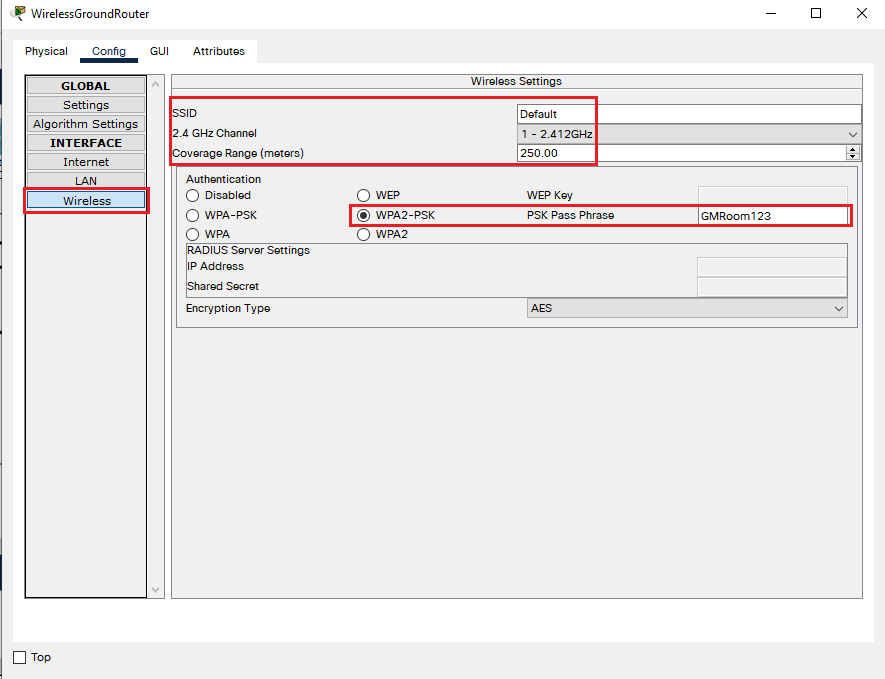
### LAN Settings

Hình ‑ LAN setting

### Wireless Setting

SSID : Default

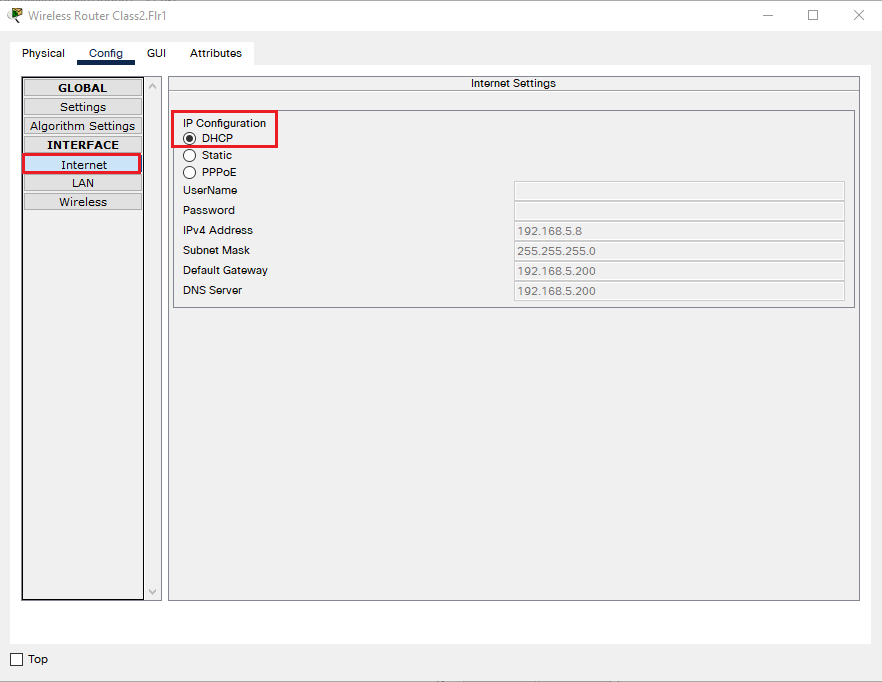
2.4 GHz Channel : 1 - 2.412GHz

WPA2-PSK : GMRoom123

Hình ‑ Cấu hình wireless

### Cấu hình WirelessRouter Class2.Flr1

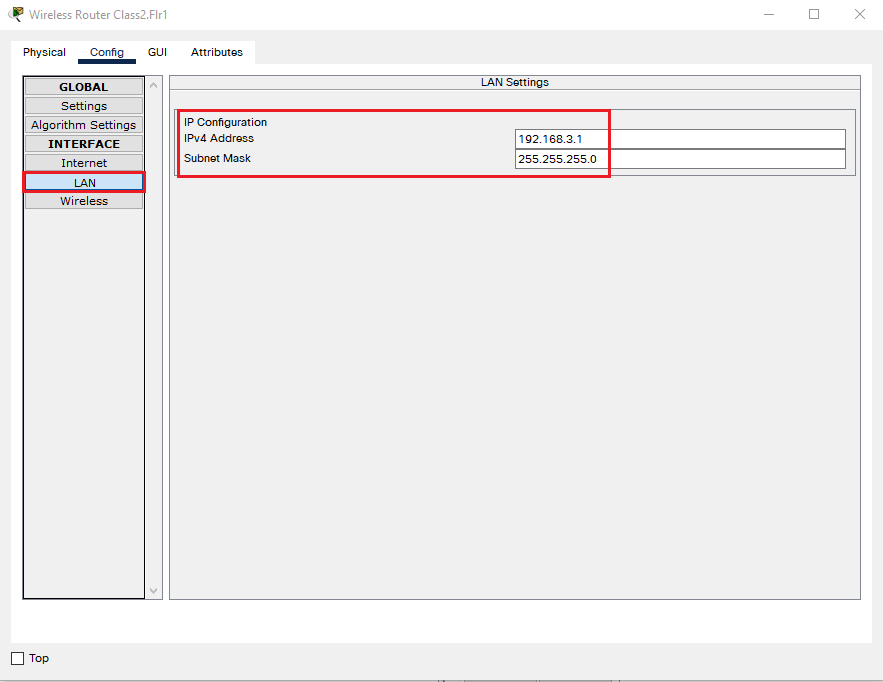
Internet Settings:

IP : DHCP

Hình ‑ 3.2.5. Cấu hình WirelessRouter Class2.Flr1

### LAN Settings

IP: 192.168.3.1

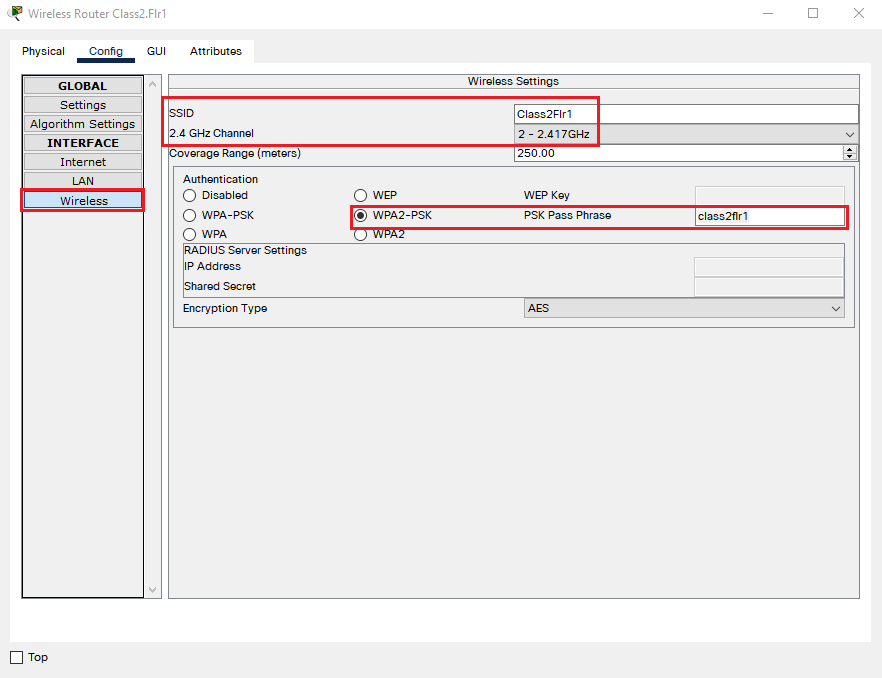
Subnet Mask: 255.255.255.0

Hình ‑ 3.2.6. LAN Settings

### Wireless Setting Class2Flr1

SSID : Class2Flr1

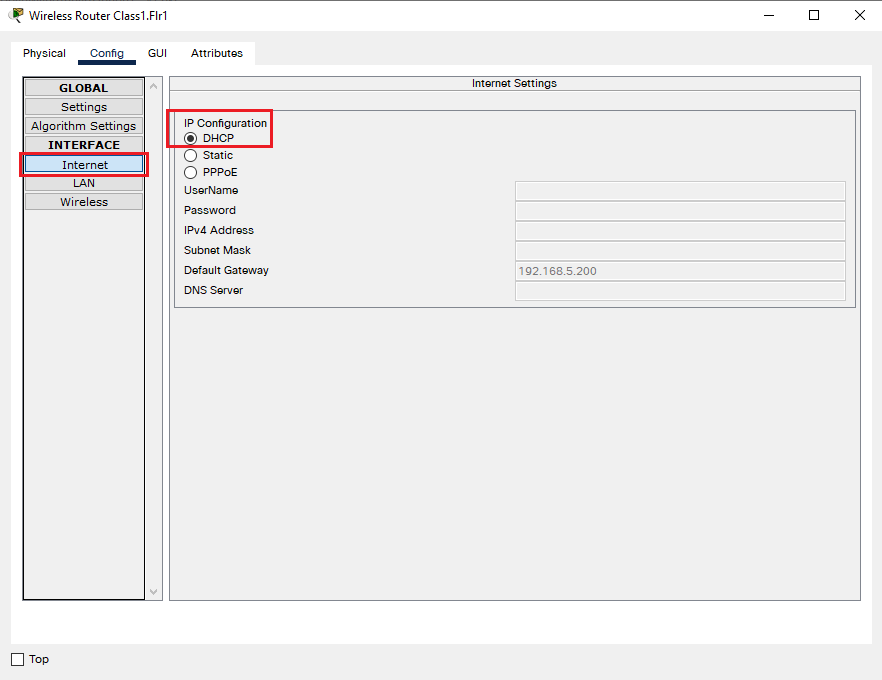
2.4 GHz Channel : 2 - 2.412GHz

WPA2-PSK : class2flr1

Hình ‑ 3.2.7. Wireless Setting Class2Flr1

### Cấu hình WirelessRouter Class1.Flr1

Internet Settings:

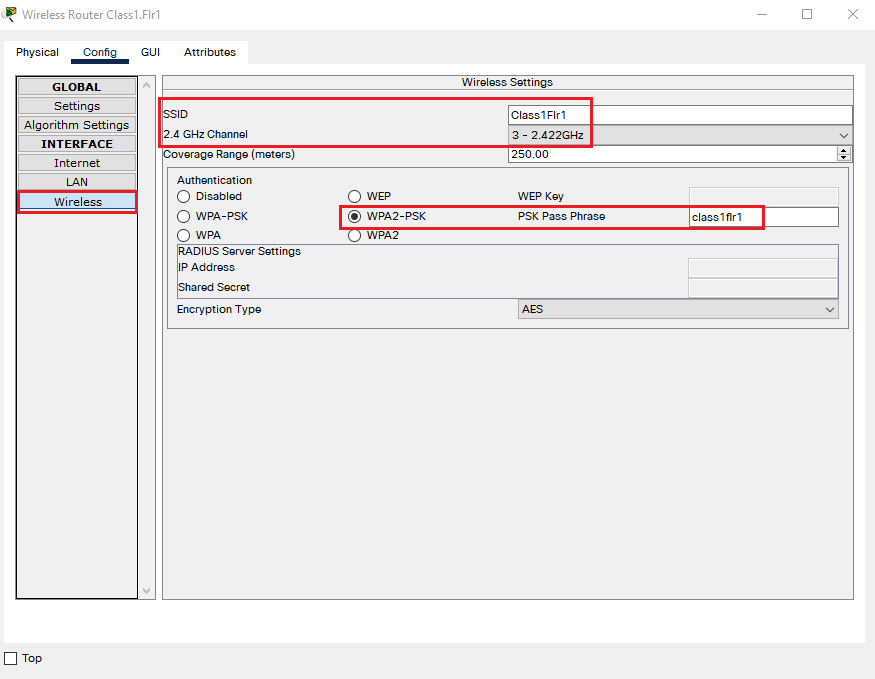
IP : DHCP

Hình ‑ 3.2.8. Cấu hình WirelessRouter Class1.Flr1

### Wireless Setting Class1Flr1

SSID : Class1Flr1

2.4 GHz Channel : 3 - 2.412GHz

WPA2-PSK : class1flr1

Hình ‑ Wireless Setting Class1Flr1

### Cấu hình WirelessRouter Class2.Flr2

Hình ‑ Cấu hình WirelessRouter Class2.Flr2

### LAN setting Class2.Flr2

IP: 192.168.1.1

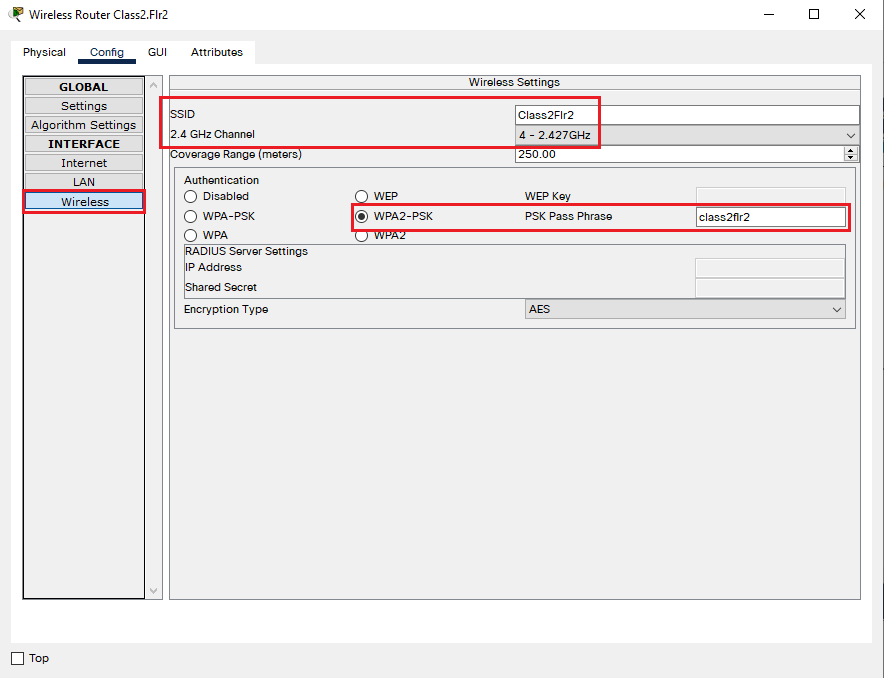
Subnet Mask: 255.255.255.0

Hình ‑ 3.2.11. LAN setting Class2.Flr2

### Wireless Setting Class2.Flr2

SSID : Default

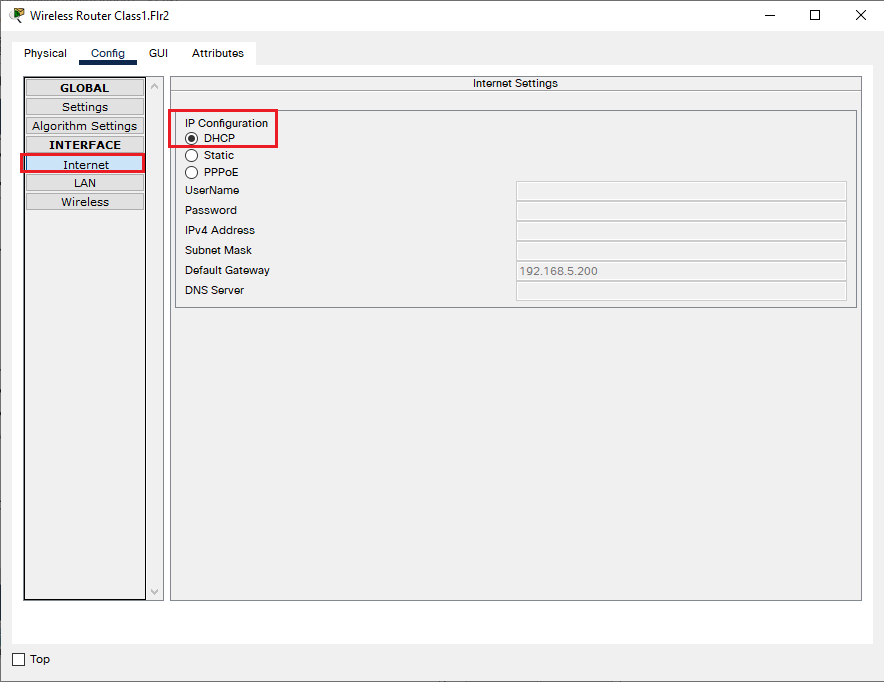
2.4 GHz Channel : 4 - 2.412GHz

WPA2-PSK : class2flr2

Hình ‑ 3.2.12. Wireless Setting Class2.Flr2

### Cấu hình WirelessRouter Class1.Flr2

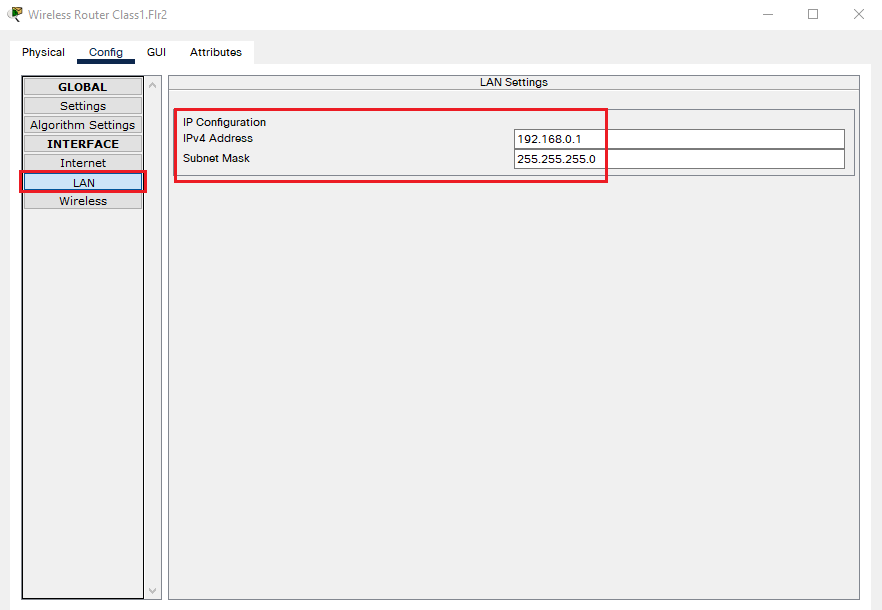
Internet Settings:

IP : DHCP

Hình ‑ 3.2.13. Cấu hình WirelessRouter Class1.Flr2

### LAN Settings Class1.Flr2

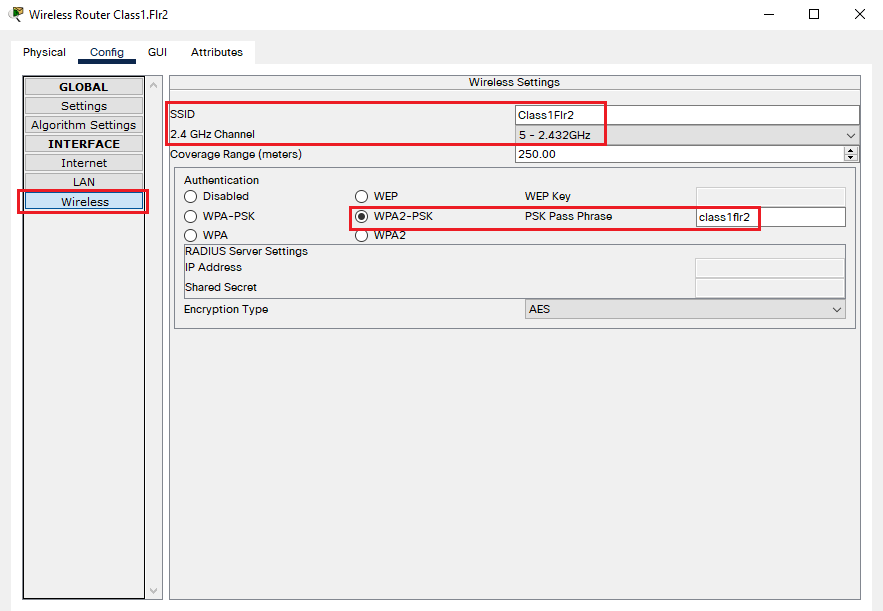
IP: 192.168.0.1

Subnet Mask: 255.255.255.0

Hình ‑ 3.2.14. LAN Settings Class1.Flr2

Wireless Setting Class1.Flr2

SSID : Class1Flr2

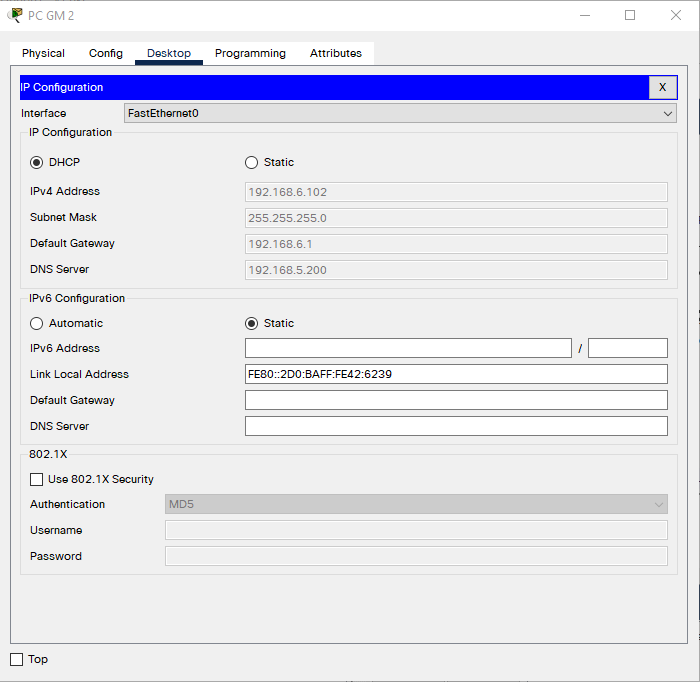
2.4 GHz Channel : 5 - 2.412GHz

Hình ‑ Wireless Setting Class1.Flr2

WPA2-PSK : class1flr2

### Cấu hình PC

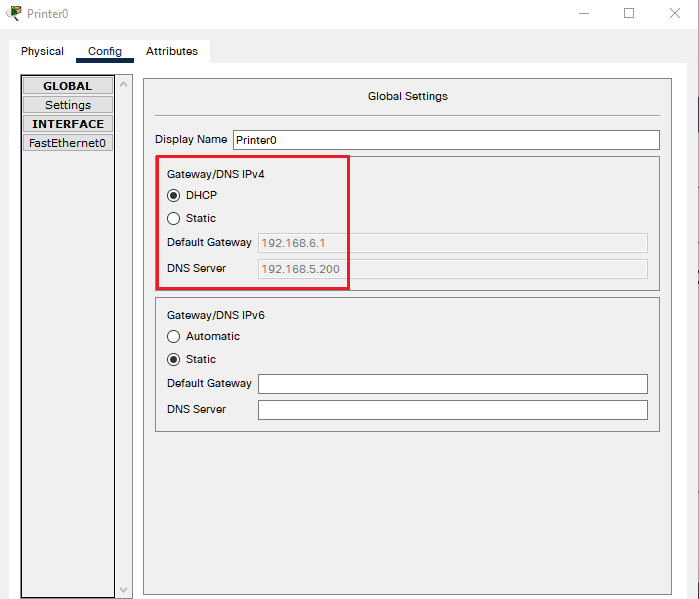
IP Configuration: DHCP

Cấu hình tương tự cho các PC có trong hệ thống mạng

Hình ‑ 3.2.16. Cấu hình PC

### Cấu hình máy in

Gateway/DNS IPv4 : DHCP

IP Configuration : DHCP

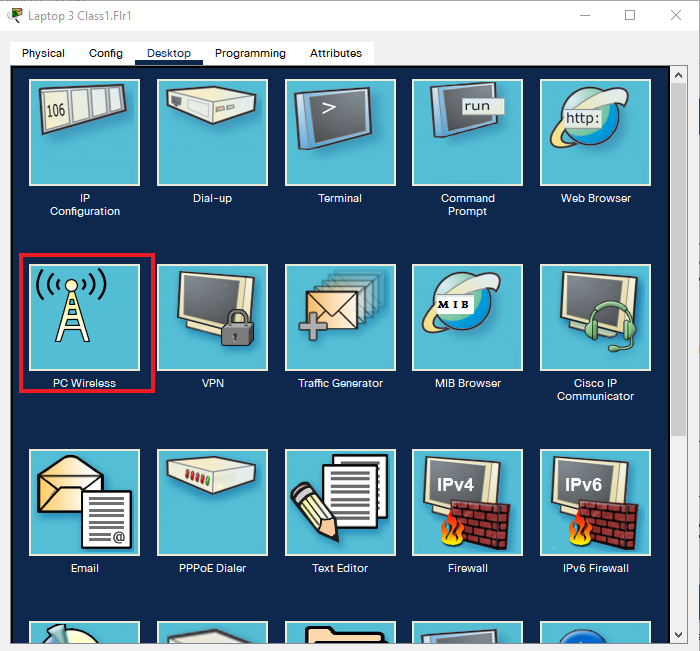
Hình ‑ 3.2.17. Cấu hình máy in

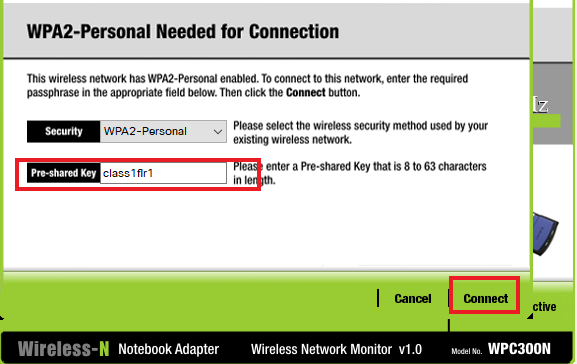
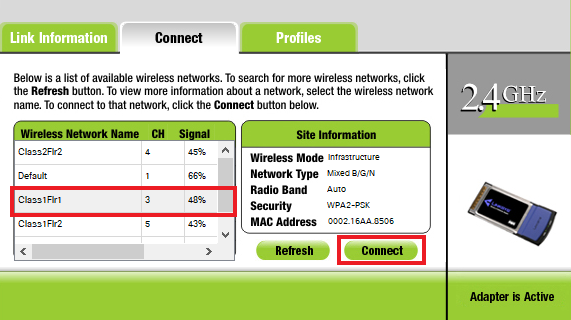
### Cấu hình Laptop

Hình ‑ Cấu hình Laptop

Vào PC Wireless

Vào tab Connect chọn Wireless Network Name tương ứng với phòng đang ở của thiết bị và connect

Nhập Pre-shared Key tương ứng với Router của phòng mà thiết bị đang trong đó dựa theo bảng thông tin WLAN



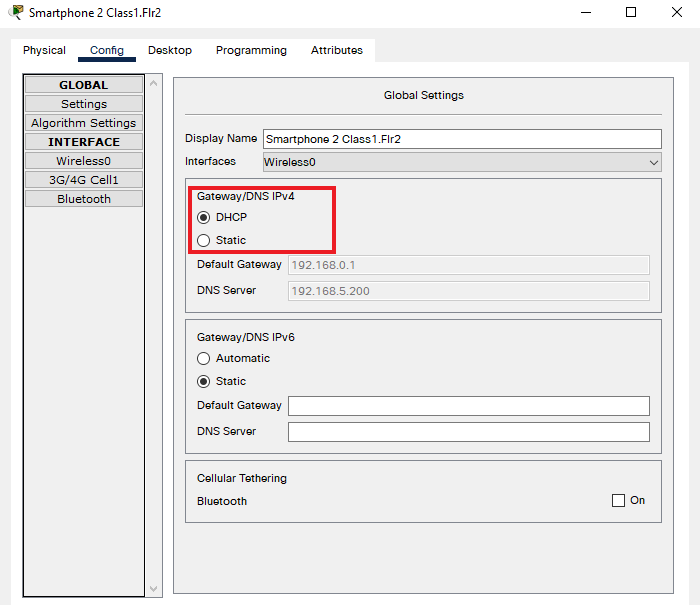
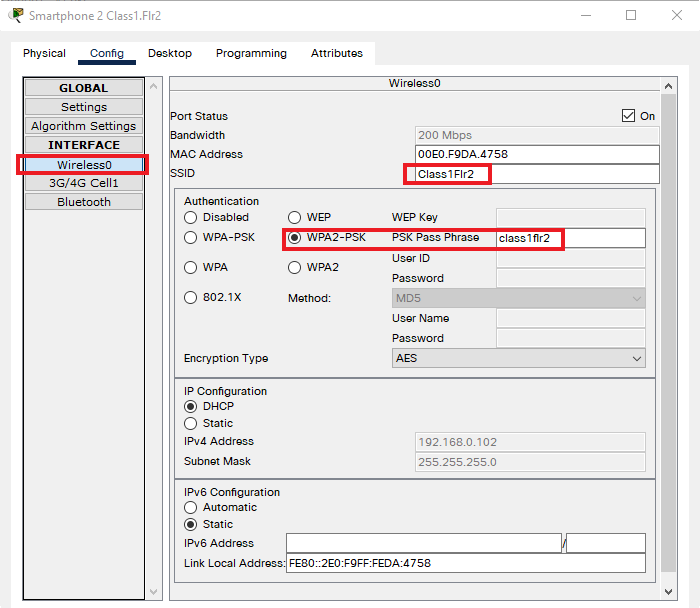
Hình ‑ Các bước vào mạng wireless

### Cấu hình SmartPhone

Gateway/DNS IPv4 : DHCP

Thay đổi SSID theo router tương ứng  với phòng mà thiết bị muốn kết nối tới.

Nhập Pre-shared Key tương ứng với Router của phòng mà thiết bị đang trong đó dựa theo bảng thông tin WLAN

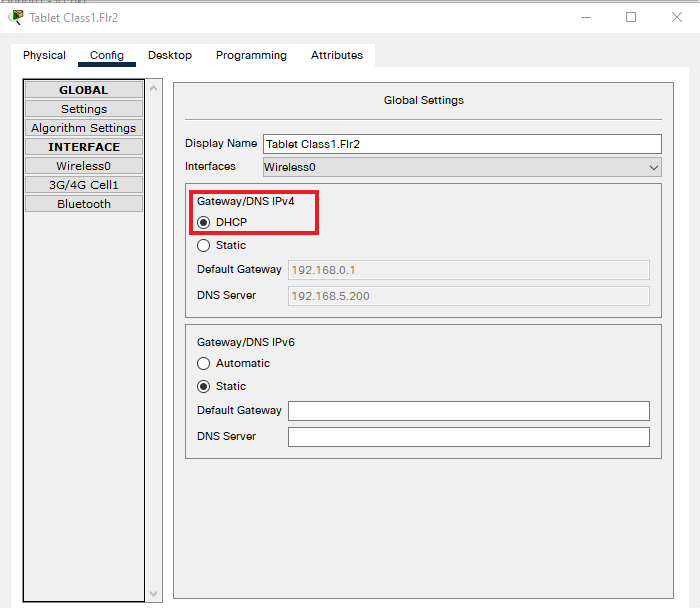


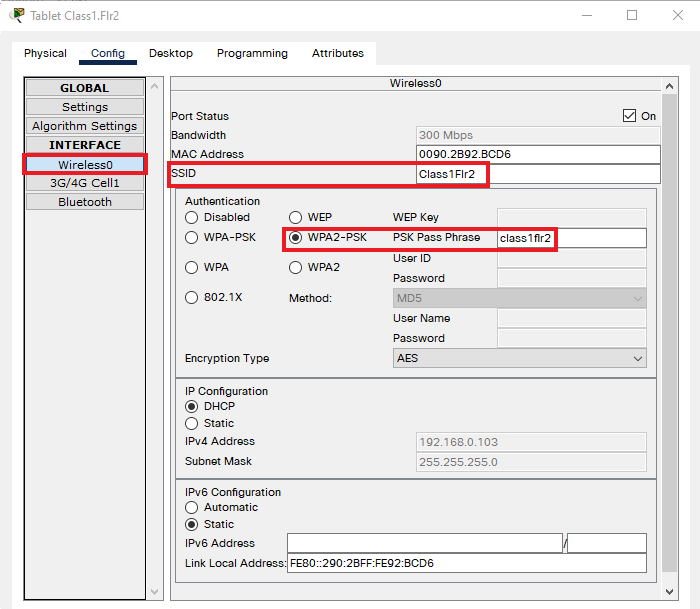
Hình ‑ 3.2.19. Cấu hình SmartPhone

### Cấu hình Tablet

Gateway/DNS IPv4 : DHCP

Thay đổi SSID theo router tương ứng  với phòng mà thiết bị muốn kết nối tới.

Nhập Pre-shared Key tương ứng với Router của phòng mà thiết bị đang trong đó dựa theo bảng thông tin WLAN



Hình ‑ Cấu hình Tablet

## Kết quả chạy chương trình

### Ping PC Staff 1 sang PC Teacher 1

Hình ‑ Ping PC Staff 1 sang PC Teacher 1

### Ping PC Staff 1 sang Server

Hình ‑ Ping PC Staff 1 sang Server

### Ping PC Staff 1 sang PC GM 5

Hình ‑ Ping PC Staff 1 sang PC GM 5

### Ping PC Staff 1 sang PC Network 3

Hình ‑ Ping PC Staff 1 sang PC Network 3

### Ping PC Staff 1 sang PC lab1.1

Hình ‑ Ping PC Staff 1 sang PC lab1.1

### Ping PC Staff 1 sang PC lab2.25

Hình ‑ Ping PC Staff 1 sang PC lab2.25

### Ping Laptop 2 Class2.Flr2 sang server

Hình ‑ Ping Laptop 2 Class2.Flr2 sang server

### Ping Laptop 2 Class2.Flr2 sang Laptop 3 Class2.Flr2

Hình ‑ 3.3.8. Ping Laptop 2 Class2.Flr2 sang Laptop 3 Class2.Flr2

## Chi phí thiết bị

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Tên thiết bị | SL | Giá |
| 1 | 24-Port 10/100 (8 PoE) + 2 T/SFP LAN Base Switch Cisco WS-C2960+24LC-L | 3 | 17.563.000 VND |
| 2 | [16-Port 10/100 Ethernet Switch Cisco SF90D-16](https://www.sieuthivienthong.com/thiet-bi-mang/switch-cisco/16-port-10100-ethernet-switch-cisco-sf90d-16/37903/details.html) | 2 | 1.352.000 VND |
| 3 | 10-Port Gigabit Managed SFP Switch Cisco SG300-10SFP-K9-EU | 3 | 13.845.000 VND |
| 4 | [AC2400 Dual-Band Wireless Router LINKSYS E8350](https://www.sieuthivienthong.com/thiet-bi-mang/thiet-bi-mang-linksys/ac2400-dual-band-wireless-router-linksys-e8350/14468/details.html) | 4 | 6.300.000 VND |
| 5 | Tủ Rack 19-inch 42U APC AR2480 | 1 | 44.380.200 VND |
| 6 | Cáp mạng Dintek CAT.6 S-FTP bọc lưới đồng (1107-04001CH) | 1 | 7.003.500 VND |
| **Tỏng cộng** | | | 242.763.700 VND |

Bảng 3‑3 Chi phí thiết bị

### 24-Port 10/100 (8 PoE) + 2 T/SFP LAN Base Switch Cisco WS-C2960+24LC-LChi tiết thiết bị

Hình ‑ Switch 24 cổng

|  |  |
| --- | --- |
| **Product ID** | **WS-C2960 Plus 24LC-L** |
| Feature set | LAN Base |
| Ports | 24 x 10/100 Ethernet ports 2 (SFP or 1000BASE-T) |
| Number of PoE ports | 8 ports up to 15.4W |
| Switching capacity | 16 Gbps |
| Forwarding capacity | 6.5 mpps |
| Jumbo frame | 9018 bytes |
| RAM | 128 GB |
| Flash Memory | 64 MB |
| Authentication Method | RADIUS, TACACS+ |
| Features | VLAN, ARP, ACL, IPv4, IPv6, Link Aggregation Control Protocol (LACP), MLD snooping, Multiple Spanning Tree Protocol, QoS, Port Aggregation Protocol (PAgP), Port Security, BOOTP, Unicast Storm Control, auto-negotiation, auto-sensing per device, auto-uplink (auto MDI/MDI-X), dynamic IP address assignment, layer 2 switching, load balancing, DHCP, DiffServ, IGMP snooping, IPv6 support |
| Remote Management Protocol | HTTP, RMON 1, RMON 2, SNMP 1, SNMP 2c, SNMP 3, TFTP, Telnet |
| Voltage | 100 to 240 VAC |
| PoE Budget | 123W |
| Dimensions | 4.4 x 45.0 x 33.2 cm |
| Weight | 4.5kg |

Bảng 3‑4 Thông tin cấu hình Switch 24 cổng



Hình ‑ Switch 16 cổng

|  |  |
| --- | --- |
| **Performance** | |
| Switching capacity | 3.2 Gbps |
| Forwarding capacity | 1.4 mpps |
| **Layer 2 Switching** | |
| Head-of-line (HOL) blocking | HOL blocking prevention |
| Jumbo Frame | 9216 bytes |
| **Quality of Service (QoS)** | |
| Priority levels | 4 hardware queues |
| Scheduling | Priority queuing and weighted round-robin (WRR) |
| Class of service | 802.1p priority based |
| **Product Specifications** | |
| Ports | 16 RJ-45 connectors for 10BASE-T/100BASE-TX |
| Cabling type | Unshielded twisted pair (UTP) Category 5 or better for 10BASE-T/100BASE-TX; 1000BASE-T recommended |
| LEDs | System/PWR, Link/Activity, 100M, Gigabit, |
| Standards | 802.3 10BASE-T Ethernet 802.3u 100BASE-TX Fast Ethernet 802.3ab 1000BASE-T Gigabit Ethernet 802.3z Gigabit Ethernet 802.3x flow control 802.1p priority 802.3az, Energy Efficient Ethernet |
| **Environmental** | |
| Dimensions (W x H x D) | 6.2 x 1.71 x 3.5 inches (160 x 43.5 x 90 mm) |
| Unit weight | 0.99 lb. (0.45kg) |
| Power | DC 12V, 1.0A |

Bảng 3‑5 Cấu hình chi chi switch 16 cổng



Hình ‑ Switch 10 cổng

|  |  |
| --- | --- |
| **General** | |
| Device Type | Switch - 10 ports - L3 - managed |
| Enclosure Type | Desktop, rack-mountable - 1U |
| Performance | Switching capacity: 20 Gbps Forwarding performance (64-byte packet size): 14.88 Mpps |
| MAC Address Table Size | 16,000 entries |
| Capacity | 4000 active VLANs |
| Routing Protocol | Static IPv4 routing |
| Remote Management Protocol | SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH, CLI |
| Jumbo Frame Support | 9 KB |
| Authentication Method | SSH, RADIUS, TACACS+ |
| Features | Layer 3 switching, Layer 2 switching, DHCP support, VLAN support, IGMP snooping, Syslog support, DoS attack prevention, port mirroring, DiffServ support, Weighted Round Robin (WRR) queuing, Broadcast Storm Control, IPv6 support, Multicast Storm Control, Unicast Storm Control, firmware upgradable, STP support, RSTP support, MSTP support, TFTP support, ACL support, QoS, Jumbo Frames support, MLD snooping |
| **Compliant Standards** | |
| RAM | 128 MB |
| Flash Memory | 16 MB |
| Status Indicators | Link activity, port transmission speed, system |
| **Expansion / Connectivity** | |
| Interfaces | 10 x SFP (mini-GBIC) 2 x 10BASE-T/100BASE-TX/1000BASE-T - RJ-45 1 x console - 9 pin D-Sub (DB-9) - management |
| Power | |
| Power Device | Internal power supply |
| Voltage Required | AC 120/230V (50/60 Hz) |
| **Miscellaneous** | |
| Width | 11 in. |
| Depth | 6.68 in. |
| Height | 1.73 in. |
| Weight | 4.68 lbs |
| Cables Included | 1 x serial cable |
| Rack Mounting Kit | Included |
| MTBF | 132,151 hours at 45C |
| Compliant Standards | UL 60950, FCC Part 15 A, CSA 22.2 |

Bảng 3‑6 Cấu hình chi tiết switch 10 cổng

Hình ‑ Wireless router

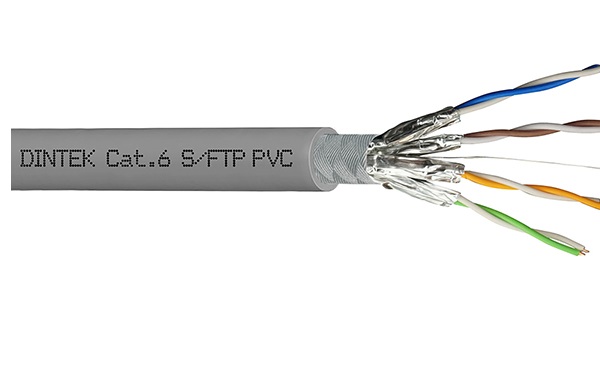
|  |  |
| --- | --- |
| **Network Standards** | IEEE 802.11a |
| IEEE 802.11b |
| IEEE 802.11g |
| IEEE 802.11n |
| IEEE 802.3ac |
| **Radio Frequency Bands** | 2.4 GHz and 5 GHz |
| **Ports** | Power, Internet, Ethernet (1-4), USB 3.0 |
| **LEDs** | Internet, Ethernet (1-4), Wi-Fi, Wi-Fi Protected Setup, Power |
| **Buttons** | Reset, Wi-Fi Portected Setup, Power |
| **Max. Link Rate** | 1733 Mbps |
| **Platform Compatibility** | Windows XP |
| Windows Vista 32/64 |
| Windows 7 32/64 |
| Windows 8 32/64 |
| Windows 8,1 32/64 |
| Mac OS x 10.5.8 Leopard |
| Mac OS x 10.6.1 Snow Leopard |
| Mac OS x 10.7 Lion |
| Mac OS x 10.8 Mountain Lion |
| Mac OS x 10.9 Mavericks |
| **Operating Temperature** | 32ºF to 104ºF (0 to 40ºC) |

Bảng 3‑7 Cấu hình chi tiết wireless router



Bảng ‑ Server

|  |  |
| --- | --- |
| **Rack Height** | 42U |
| **Rack Width** | 19-inch |
| **Protection Class** | IP20. |
| **Dimension (Height x Width x Depth)** | 2057x800x1060 mm. |
| **Net Weight** | 130.5 kg. |
| **Color** | Black |
| **Weight Capacity (static load):.** | 1002.27 kg |
| **Weight Capacity (dynamic load)** | 460.91 kg |

Bảng 3‑9 Cấu hình chi tiết server

Hình ‑ Cáp mạng

Cáp mạng Dintek CAT.6 S-FTP (1107-04001CH)

-       [Cáp mạng](https://www.sieuthivienthong.com/cap-mang-va-phu-kien.html) Dintek CAT.6  S-FTP 4-pairs, bọc nhôm chống nhiễu từng đôi cáp và bọc cả lớp ngoài cùng 4 đôi cáp, 305m/cuộn.

Application:

-       Fast Ethernet(IEEE802.3u)

-       100Vg-AnyLAN(IEEE 802.12)

-       Token Ring(IEEE 802.5)

-       TP-PMD(ANSI X3T9.5)

-       100Base-T Ethernet(IEEE 802.5)

-       155/622 Mbps 1.2/ 2.4 Gbps ATM

-       1000Base-T Ethernet

-       550 MHz Broadband video

*Industry Standard:*

-       According to UL444 Communications Cables, UL AWM  style 2835

-       TIA/EIA 568B.2-1

*Product  Electrical Characteristics:*

-       Impedance:100±15 ohms

-       Mutual Capacitance: nom. 13.6pf/ft

-       DC Resistance: max. 6.8ohm/100m at 20°C

-       Voltage rating: 30V

-       Rated temperature: 60°C

*Cable Data:*

-       No. of Pairs: 4 pair

-       Size of conductor: 23AWG (solid anneal copper wire)

-       Overall Diameter:7.4±0.3mm

-       Individual Shielding: Aluminum-foil laminated tape.

-       Jacket material: PVC or LSZH, flame retardant and/or CM grade.

# KẾT LUẬN

Việc lựa chọn đề tài thiết kế mạng LAN có quản lý cho trường học là một đề tài mang tính phổ dụng. Ngày nay hầu hết không chỉ trường học mà các công ty, doanh nghiệp đã triển khai lắp đặt hệ thống mạng. Thiết kế mạng cho Nhà trường là một đề tài mang tính chất thực tế một phần nó củng cố thêm cho chúng em vể kiến thức của mạng máy tính, phần nữa thông qua đề tài này nó còn cung cấp cho em thêm kiến thức xây dựng mô hình - thiết kế - triển khai lắp đặt được một hệ thống mạng văn phòng thực tế ra sao. Cách đi dây dẫn, bố trí lắp đặt các máy tính PC, kết nối với các thiết bị trung tâm, lựa chọn mô hình mạng cho phù hợp với phòng làm việc.

Càng về sau số lượng học sinh – sinh viên của trường tăng lên, nhu cầu làm việc với phòng máy là điều rất quan trọng giúp sinh viên việc học tập được đi đôi với thực hành, nhà trường cần đặt ra những hướng phát triển hơn, giúp việc học tập của sinh viên và giảng dạy của giáo viên được tốt hơn.

Với nhu cầu kết nối Internet hiện nay, nếu trong hệ thống mạng của chúng ta chỉ có 1 đường truyền thì tốc độ truy cập internet có thể bị chậm do đường truyền bị quá tải, hoặc tại 1 thời điểm không thể truy cập internet vì đường truyền đang bị mất tin hiệu.

Vì thế, chúng em xin rút ra 1 số ý kiến và kết luận như sau: Trong thời gian vận hành, nghiên cứu, tìm hiều sâu về vấn đề an toàn mạng nhằm quản trị hệ thống mạng 1 cách an toàn, hiểu quả đảm bảo tính tin cậy. Chúng em cần phải tiếp tục bổ sung kiến thức mới để đảm bảo hệ thống cần nâng cấp, mở rộng thì sẽ đủ kiến thức và kỹ năng để bảo trì nâng cấp hệ thống.

Vì kỹ năng, kiến thức, kinh nghiệm còn hạn chế nên bài báo cáo còn những sơ suất mong thầy góp ý để chúng em có thể hoàn thành tốt hơn ở những đồ án tiếp theo.