HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Phạm Huyền Huyên

GIẢI PHÁP BẢO MẬT HỆ THỐNG WLAN, ÁP DỤNG CHO MẠNG TRƯỜNG ĐẠI HỌC HÀ NỘI

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – NĂM 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Phạm Huyền Huyên

GIẢI PHÁP BẢO MẬT HỆ THỐNG WLAN, ÁP DỤNG CHO MẠNG TRƯỜNG ĐẠI HỌC HÀ NỘI

Chuyên nghành: Hệ thống thông tin
Mã số: 8.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. LÊ HỮU LẬP

HÀ NỘI – NĂM 2020

LỜI CAM ĐOAN

Học viên cam đoan đề tài: "***GIẢI PHÁP BẢO MẬT HỆ THỐNG WLAN, ÁP DỤNG CHO MẠNG TRƯỜNG ĐẠI HỌC HÀ NỘI***" là công trình nghiên cứu của riêng học viên dưới sự hướng dẫn của **PGS.TS. Lê Hữu Lập.**

Các kết quả, phân tích, kết luận trong luận văn thạc sỹ này (ngoài phần được trích dẫn) đều là kết quả nghiên cứu của tác giả, các số liệu nêu trong luận văn là trung thực và chưa từng được công bố trong bất kỳ công trình nào khác.

Nếu sai học viên xin hoàn toàn chịu trách nhiệm.

Hà Nội, ngày 10 tháng 11 năm 2020

Tác giả

Phạm Huyền Huyên

LỜI CẢM ƠN

Lời đầu tiên cho học viên xin gửi lời cảm ơn chân thành đến các thầy, cô giáo thuộc Học Viện công nghệ Bưu chính viễn thông, Khoa ĐT sau đại học thuộc Học viện Công nghệ Bưu chính viễn thông đã tận tình giảng dạy, truyền đạt các nội dung kiến thức, kinh nghiệm quý báu trong suốt quá trình học viên theo học tại Học viện. Thông qua những bài học quý giá, sự kèm cặp, chỉ bảo và truyền đạt nhiệt tình của các thầy, cô giúp cá nhân học viên trau dồi kiến thức, hoàn thiện hơn nữa hệ thống kiến thức chuyên môn, đáp ứng tốt hơn yêu cầu công việc của đơn vị mình. Đặc biệt, học viên xin gửi lời cảm ơn trân thành tới thầy hướng dẫn khoa học **PGS.TS. Lê Hữu Lập**, Khoa ĐT sau đại học thuộc Học viện Công nghệ Bưu chính viễn thông đã tâm huyết, tận tình chỉ bảo, hướng dẫn, cung cấp tài liệu và các nội dung kiến thức quý báu, đồng thời có sự định hướng đúng đắn giúp học viên hoàn thành được luận văn này.

Học viên cũng xin được bày tỏ sự cảm ơn sâu sắc tới các đồng nghiệp và tập thể lớp Cao học Hệ thống thông tin - Đợt 1 năm 2019 đã đồng hành, khích lệ và chia sẻ trong suốt quá trình học tập.

Xin trân trọng cảm ơn!

Hà Nội, ngày 10 tháng 11 năm 2020

Học viên

Phạm Huyền Huyên

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Từ viết tắt	Tên tiếng Anh	Nghĩa tiếng Việt
AAA	Authentication, Authorization, Access Control	Xác thực, cấp quyền, điều khiển truy xuất
AES	Advanced Encryption Standard	Chuẩn mã hóa tiên tiến
AP	Access Point	Điểm truy cập
BSS	Basic Services Set	Mô hình mạng cơ sở
CHAP	Challenge-handshake authentication protocol	Giao thức xác thực yêu cầu bắt tay
DES	Data Encryption Standard	Chuẩn mã hoá dữ liệu
DSS	Direct Sequence Spectrum	Phổ trình tự trực tiếp
DSSS	Direct Sequence Spread Spectrum	Kỹ thuật trải phổ tuần tự trực tiếp
EAP	Extensible Authentication Protocol	Giao thức xác thực mở rộng
ESS	Extended Service Set	Dịch vụ mở rộng
FHSS	Frequency Hopping Spread Spectrum	Kỹ thuật trải phổ nhảy tần
IAS	Microsoft’s Internet Authentication Service	Dịch vụ xác thực Internet
IBSS	Independent Basic Service Set	Thiết bị dịch vụ cơ bản độc lập
IEEE	Institute of Electrical and Electronics Engineers	Viện kỹ thuật điện và điện tử Mỹ
IPSec	Internet Protocol Security	Tập hợp các chuẩn chung nhất (industry-defined set) trong việc kiểm tra, xác thực và mã hóa các dữ liệu dạng packet trên tầng Network
ISM	Industrial, Scientific, Medical	Dải tần số vô tuyến dành cho công nghiệp, khoa học và y học
ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
MAC	Medium Access Control	Điều khiển truy cập môi trường

NAS	Network access server	Máy chủ truy cập mạng
NIST	Nation Instutute of Standard and Technology	Viện nghiên cứu tiêu chuẩn và công nghệ quốc gia
OFDM	Orthogonal Frequency Division Multiplex	Phương thức điều chế ghép kênh theo vùng tần số vuông góc
OSI	Open Systems Interconnec	Mô hình tham chiếu kết nối các hệ thống mở
PAN	Personal Area Network	Mạng cá nhân
PDA	Persional Digital Assistant	Máy trợ lý cá nhân dùng kỹ thuật số
PEAP	Protected Extensible Authentication Protocol	Giao thức xác thực mở rộng được bảo vệ
PPP	Point-to-Point Protocol	Giao thức liên kết điểm điểm
PRNG	Pseudo Random Number Generator	Bộ tạo số giả ngẫu nhiên
RADIUS	Remote Authentication Dial-In User Service	Dịch vụ người dùng quay số xác thực từ xa
RF	Radio Frequency	Tần số vô tuyến
SLIP	Serial Line Internet Protocol	Giao thức internet đơn tuyến
SSID	Service set identifier	Bộ nhận dạng dịch vụ
TKIP	Temporal Key Integrity Protocol	Giao thức nhận dạng khoá tạm thời
UDP	User Datagram Protocol	Là một giao thức truyền tải
VPN	Virtual Private Networks	Mạng riêng ảo
WEP	Wired Equivalent Privacy	Bảo mật mạng không giây tương đương với mạng có dây
WIFI	Wireless Fidelity	Mạng không giây trung thực
WLAN	Wireless Local Area Network	Mạng cục bộ không giây
WPA	Wi-Fi Protected Access	Chuẩn mã hóa cải tiến của WEP

DANH MỤC CÁC HÌNH

DANH MỤC CÁC BẢNG BIỂU

MỞ ĐẦU

1. Lý do chọn đề tài:

Cùng với sự phát triển mạnh mẽ của khoa học công nghệ, đặc biệt là công nghệ thông tin và điện tử viễn thông, nhu cầu trao đổi thông tin và dữ liệu của con người ngày càng cao. Mạng máy tính đóng vai trò quan trọng trong mọi lĩnh vực của cuộc sống. Bên cạnh nền tảng mạng máy tính có dây, mạng máy tính không dây ngay từ khi ra đời đã thể hiện những ưu điểm vượt trội về tính tiện dụng, linh hoạt và đơn giản. Mặc dù mạng máy tính không dây đã tồn tại từ lâu, nhưng chúng đã đạt được sự phát triển nổi bật trong thời đại công nghệ điện tử, và chịu ảnh hưởng sâu sắc của nền kinh tế và vật lý hiện đại. Ngày nay, mạng không dây đã trở nên thiết thực trong cuộc sống. Chúng ta chỉ cần các thiết bị như điện thoại thông minh, máy tính xách tay, PDA hoặc bất kỳ phương thức truy cập mạng không dây nào là có thể truy cập mạng tại nhà, cơ quan, trường học, văn phòng và những nơi khác.... Bất cứ nơi nào trong phạm vi phủ sóng của mạng. Do tính chất trao đổi thông tin trong không gian truyền dẫn nên khả năng rò rỉ thông tin là rất cao. Nếu chúng ta không khắc phục điểm yếu này, môi trường mạng không dây sẽ trở thành mục tiêu của các hacker xâm nhập, gây thất thoát thông tin và tiền bạc. Vì vậy, bảo mật thông tin là một vấn đề đang thu hút rất nhiều sự quan tâm. Với sự phát triển của mạng không dây, cần phát triển khả năng bảo mật để cung cấp cho người dùng thông tin hiệu quả và đáng tin cậy.

Vì vậy, việc kết nối mạng nội bộ của cơ quan tổ chức mình vào mạng Internet mà không có các biện pháp đảm bảo an ninh sẽ dẫn đến nguy cơ mất an toàn thông tin và dữ liệu cao. Để nâng cao tính bảo mật cho hệ thống mạng nội bộ phục vụ cho nhu cầu công việc, giảng dạy học tập của trường Đại học Hà Nội, học viên chọn đề tài: "**GIẢI PHÁP BẢO MẬT HỆ THỐNG WLAN, ÁP DỤNG CHO MẠNG TRƯỜNG ĐẠI HỌC HÀ NỘI**".

2. Tổng quan vấn đề nghiên cứu

Nội dung chính của luận văn này là quá trình nghiên cứu, tìm hiểu để từ đó đúc kết ra được những yếu tố đảm bảo tính bảo mật cho hệ thống mạng WLAN:

- Nắm bắt được một số phương pháp tấn công hệ thống mạng thường gặp và các giải pháp bảo mật để có được cách thức phòng chống, cách xử lý sự cố và khắc phục sau sự cố một cách nhanh nhất.

- Đề xuất giải pháp nâng cao tính bảo mật cho hệ thống mạng của Trường Đại học Hà Nội.

3. Mục tiêu nghiên cứu của đề tài

Mục tiêu nghiên cứu của luận văn là nghiên cứu kỹ thuật tấn công mạng WLAN, các giải pháp đảm bảo an toàn mạng WLAN và đề xuất giải pháp nâng cao độ bảo mật cho mạng WLAN tại trường Đại học Hà Nội.

4. Đối tượng và phạm vi nghiên cứu của đề tài

- Đối tượng nghiên cứu của luận văn là mạng WLAN và các vấn đề liên quan đến bảo mật mạng WLAN.

- Phạm vi nghiên cứu của luận văn là các giải pháp bảo mật mạng WLAN và ứng dụng cho mạng WLAN tại trường Đại học Hà Nội.

5. Phương pháp nghiên cứu của đề tài

- Về mặt lý thuyết: Thu thập, khảo sát, nghiên cứu các tài liệu và thông tin có liên quan đến bảo mật mạng WLAN.

- Về mặt thực nghiệm: Khảo sát hệ thống mạng WLAN nội bộ Trường Đại học Hà Nội và đề xuất giải pháp bảo mật cho hệ thống mạng.

6. Bố cục luận văn

Luận văn chia làm 3 chương chính:

Chương 1: Tổng quan về mạng không dây & Nguy cơ tấn công mạng.

1.1 Giới thiệu và WLAN

1.2 Các chuẩn mạng thông dụng của WLAN

1.3 Cơ sở hạ tầng mô hình mạng WLAN

1.4 Các nguy cơ tấn công mạng WLAN

1.5 Kết chương

Chương 2: Các giải pháp bảo mật trong mạng WLAN

2.1 Giới thiệu

2.2 Xác thực qua mã hóa Wifi: WEP; WPA; WPA2; WPA3

2.3 Xác thực Wifi bằng Radius Server

2.3 Kết chương

Chương 3: Bảo mật mạng WLAN của Hanu bằng chứng thực Radius Server

3.1 Khảo sát mạng WLAN Đại Học Hà Nội

3.2 Đề xuất các giải pháp bảo mật cho mạng WLAN tại trường Đại học Hà Nội

3.3 Cài đặt

3.4 Thử nghiệm và đánh giá kết quả

3.5 Kết chương

Trong quá trình thực hiện luận văn, mặc dù bản thân đã cố gắng thu thập tài liệu, củng cố kiến thức... nhưng luận văn vẫn còn những hạn chế nhất định. Học viên rất mong nhận được sự chỉ dạy, đóng góp tận tình của các thầy, cô để luận văn của học viên được hoàn thiện và có tính ứng dụng cao hơn trong thực tiễn.

CHƯƠNG I – TỔNG QUAN VỀ MẠNG WLAN & NGUY CƠ TẤN CÔNG MẠNG

1.1– Giới thiệu về mạng WLAN [2] [8] [6]

Mạng cục bộ không dây (WLAN) là mạng máy tính trong đó các thành phần mạng không sử dụng dây cáp như các mạng thông thường và môi trường giao tiếp trong mạng là không khí. Những thành phần tham gia mạng sử dụng sóng điện từ để liên lạc với nhau. Hỗ trợ mạng cho phép người dùng di chuyển trong phạm vi rộng mà vẫn có thể kết nối mạng.

Công nghệ WLAN xuất hiện vào cuối những năm 1990, khi các nhà sản xuất giới thiệu các sản phẩm hoạt động ở dải tần 900MHz. Các giải pháp này cung cấp tốc độ truyền dữ liệu 1Mbps, thấp hơn nhiều so với tốc độ 10Mbps của hầu hết các mạng có dây hiện thời.

Năm 1992, các nhà sản xuất bắt đầu sử dụng dải tần 2.4 GHz để bán sản phẩm. Mặc dù các sản phẩm này đã có tốc độ truyền dữ liệu cao hơn, nhưng chúng vẫn chưa được phát hành rộng rãi. Nhu cầu về khả năng tương tác thống nhất giữa các thiết bị có tần số khác nhau đã khiến một số tổ chức phát triển các tiêu chuẩn mạng không dây chung.

Năm 1997, IEEE (Viện Kỹ sư Điện và Điện tử) đã phê duyệt chuẩn 802.11, và nó còn được gọi là WIFI (Wireless Fidelity) của WLAN. Chuẩn 802.11 hỗ trợ ba phương pháp truyền dữ liệu, bao gồm một phương pháp truyền tín hiệu vô tuyến ở tần số 2.4 GHz.

Vào năm 1999, IEEE đã thông qua hai cách triển khai chuẩn 802.11, thông qua các phương thức truyền 8.2.11a và 802.11b. Các sản phẩm WLAN 802.11b đã nhanh chóng trở thành công nghệ không dây hữu dụng. Các thiết bị 802.11b phát sóng với tốc độ 2.4GHz, cung cấp tốc độ truyền tải lên đến 11Mbps. So với mạng có dây, mục đích của việc tạo IEEE 802.11b là cung cấp hiệu quả, thông lượng và bảo mật.

Đầu năm 2003, IEEE công bố một tiêu chuẩn khác là 802.11g, có thể truyền thông tin ở dải tần 2.4GHz và 5GHz. Chuẩn 802.11g có thể tăng tốc độ truyền dữ liệu

lên 54Mbps. Ngoài ra, các sản phẩm sử dụng chuẩn 802.11g cũng có thể tương thích với các thiết bị 802.11b. Ngày nay, chuẩn 802.11g đã đạt đến tốc độ 108Mbps-300Mbps.

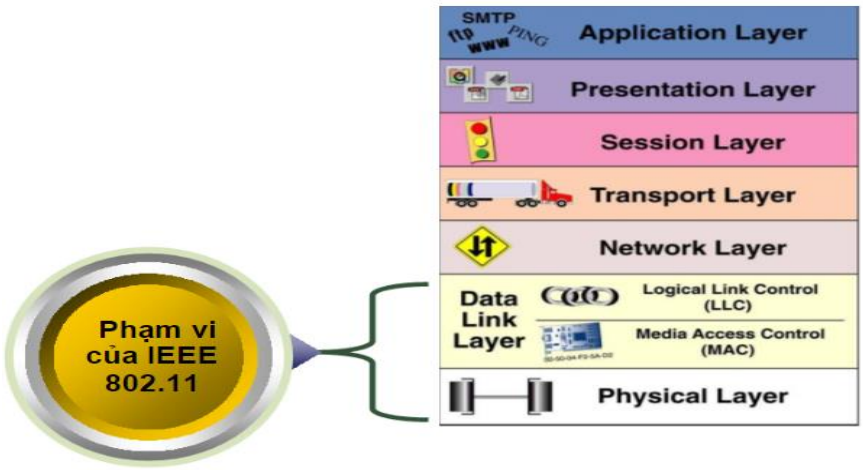
Vào cuối năm 2009, chuẩn 802.11n đã được IEEE phê duyệt để sử dụng chính thức và là sản phẩm tiêu chuẩn được chứng nhận bởi Wi-Fi Alliance. Mục tiêu chính của công nghệ này là tăng tốc độ truyền tải và phạm vi hoạt động của thiết bị bằng cách kết hợp công nghệ tiên tiến. Về lý thuyết, 802.11n cho phép kết nối với tốc độ 300Mbps.

Chuẩn 802.11ac được phát hành vào năm 2013 và được gọi là Wi-Fi 5. 802.11ac sử dụng công nghệ không dây băng tần kép để hỗ trợ kết nối đồng thời trên hai băng tần 2.4 GHz và 5 GHz. 802.11ac cung cấp khả năng tương thích ngược với các chuẩn 802.11b, 802.11g và 802.11n, đồng thời có băng thông lên tới 1300 Mbps trên băng tần 5 GHz và 450 Mbps trên băng tần 2.4 GHz.

Chuẩn 802.11ax được gọi là Wi-Fi 6, là phiên bản mới nhất được chính thức áp dụng vào ngày 16 tháng 9 năm 2019. Chuẩn kết nối không dây thế hệ thứ sáu cung cấp cho người dùng nền tảng kết nối mới mang đến nhiều cải tiến đáng giá, trong đó quan trọng nhất là tốc độ truy cập nhanh, băng thông lớn và độ trễ thấp, so với sản phẩm thế hệ trước ưu việt hơn nhiều lần. Đối với một loạt các ứng dụng hiện đang yêu cầu tốc độ truyền ngày càng cao, điều này đã đạt được một bước tiến lớn: phát trực tuyến phim độ phân giải cực cao lên đến 4K, 8K; ứng dụng/phần mềm thương mại; chơi trò chơi trực tuyến, họp trực tuyến... có thể giúp người dùng nhận được nhiều lợi ích nhất từ cải tiến này.

Sau đây ta sẽ tìm hiểu sâu hơn về các chuẩn.

1.2 - Các chuẩn mạng thông dụng của WLAN [2][8][6]



Hình 1. 1 Phạm vi của WLAN trong mô hình OSI

Các chuẩn của WLAN được Học viện Kỹ nghệ Điện và Điện tử IEEE (Institute of Electrical and Electronics Engineers) qui chuẩn và thống nhất trên toàn thế giới.

1.2.1 - Chuẩn mạng 802.11

Đây là tiêu chuẩn đầu tiên cho hệ thống mạng không dây. Tốc độ truyền từ 1 đến 2 Mbps và hoạt động ở dải tần 2.4GHz. Tiêu chuẩn bao gồm tất cả các công nghệ truyền dẫn hiện tại, bao gồm phổ chuỗi trực tiếp (DSS), trải phổ nhảy tần (FHSS) và tia hồng ngoại. Chuẩn 802.11 là một trong hai chuẩn mô tả hoạt động của sóng truyền (FHSS) trong mạng không dây. Chỉ phần cứng phù hợp với chuẩn 802.11 mới có thể sử dụng hệ thống bằng sóng mang này.

1.2.2 - Chuẩn mạng 802.11a

IEEE đã bổ sung và phê duyệt tiêu chuẩn vào tháng 9 năm 1999 để cung cấp một tiêu chuẩn có thể hoạt động ở tốc độ cao hơn (từ 20 đến 54 Mbit/s) trên băng tần 5 GHz mới. Các hệ thống tuân thủ tiêu chuẩn này hoạt động ở băng tần 5.15 đến 5.25 GHz và 5.75 đến 5.825 GHz với tốc độ dữ liệu lên đến 54 Mbit/s. Tiêu chuẩn sử dụng công nghệ điều chế OFDM (Ghép kênh phân chia theo tần số trực giao) để đạt được tốc độ dữ liệu cao hơn và khả năng chống nhiễu đa đường tốt hơn.

Có thể sử dụng tối đa 8 điểm truy cập (truyền trên 8 kênh Non-overlapping, kênh không chồng chéo phổ), ở dải tần 2.4GHz chức năng này chỉ sử dụng được 3 điểm truy cập (truyền trên 3 kênh không chồng chéo).

Các sản phẩm IEEE 802.11a không tương thích với các sản phẩm IEEE 802.11 và 802.11b vì chúng hoạt động ở các dải tần số khác nhau. Tuy nhiên, các nhà sản xuất chipset đang cố gắng tạo ra những chipset có thể hoạt động ở chế độ 802.11a và 802.11b. Sự hợp tác này được gọi là WiFi5 (WiFi cho công nghệ 5Gbps).

Bảng 1. 1 Một số thông số kỹ thuật của chuẩn 802.11a

Phê duyệt	9/1999
Giải tần	5 Ghz
Tốc độ truyền dữ liệu	54Mbps
Độ khả thông	31Mbps
Phạm vi phủ sóng (outdoor)	~ 50m
Phạm vi phủ sóng (indoor)	~ 35m
Kỹ thuật truy nhập môi trường	CSMA/CA
Kỹ thuật điều chế	OFDM
Phổ tần chiếm dụng	300Mhz

1.2.3 - Chuẩn mạng 802.11b

Giống như tiêu chuẩn IEEE 802.11a, lớp vật lý cũng đã thay đổi so với tiêu chuẩn IEEE.802.11. Các hệ thống tuân thủ tiêu chuẩn này hoạt động ở dải tần 2.400 đến 2.483 GHz và hỗ trợ các dịch vụ thoại, dữ liệu và hình ảnh với tốc độ tối đa 11 Mbit/s. Tiêu chuẩn xác định môi trường truyền DSSS với tốc độ dữ liệu 11 Mbit/s, 5,5 Mbit/s, 2Mbit/s và 1 Mbit/s.

So với các hệ thống tuân thủ IEEE 802.11a, các hệ thống tuân thủ IEEE 802.11b hoạt động trên dải tần số thấp hơn và có khả năng xuyên qua vật thể cứng cao hơn. Các chức năng này làm cho mạng WLAN tuân thủ IEEE 802.11b phù hợp với các môi trường đông đúc và các khu vực rộng lớn, chẳng hạn như các tòa nhà, nhà máy, nhà kho và trung tâm phân phối… Khoảng cách hoạt động của hệ thống khoảng 100 mét.

IEEE 802.11b là tiêu chuẩn được sử dụng rộng rãi nhất trong các mạng cục bộ không dây. Vì băng tần 2.4GHz là dải tần ISM (Băng tần vô tuyến được cấp phép cho

ngành công nghiệp, khoa học và y học) nên nó cũng được sử dụng trong các tiêu chuẩn mạng không dây khác. Ví dụ, Bluetooth và HomeRF không phổ biến như 801.11. Bluetooth được thiết kế để sử dụng với các thiết bị không dây khác ngoài mạng LAN không dây và được sử dụng bởi PAN (Mạng Khu vực Cá nhân). Do đó, mạng LAN không dây sử dụng tiêu chuẩn 802.11b và các thiết bị Bluetooth hoạt động trong cùng một dải tần.

Bảng 1. 2 Một số thông số kỹ thuật của chuẩn 802.11b

Phê duyệt	9/1999
Dải tần hoạt động	2,4 GHz
Tốc độ truyền dữ liệu	11 Mbps
Bán kính phủ sóng	100m (với tần số 11Mbps)
Kỹ thuật điều chế	FHSS, DSSS
Phổ tần chiếm dụng	83,5 MHz

1.2.4 – Chuẩn mạng 802.11g

Các hệ thống tuân theo tiêu chuẩn này hoạt động trên băng tần 2.4 GHz và có thể đạt tốc độ 54 Mbit/s. Giống như IEEE 802.11a, IEEE 802.11g cũng sử dụng công nghệ điều chế OFDM để đạt được tốc độ cao hơn. Ngoài ra, các hệ thống tuân thủ IEEE 802.11g tương thích ngược với các hệ thống IEEE 802.11b vì chúng thực hiện tất cả các chức năng IEEE 802.11b cần thiết và cho phép các máy khách của hệ thống tuân theo hệ thống IEEE 802.11b và chuẩn AP của IEEE 802.11g.

Bảng 1. 3 Một số thông số kỹ thuật của chuẩn 802.11g

Phê duyệt	10/2002
Dải tần truyền dữ liệu	2,4 GHz
Tốc độ bit	54 Mbps
Bán kính phủ sóng	100m (với tốc độ11Mbps)
Kỹ thuật điều chế	OFDM

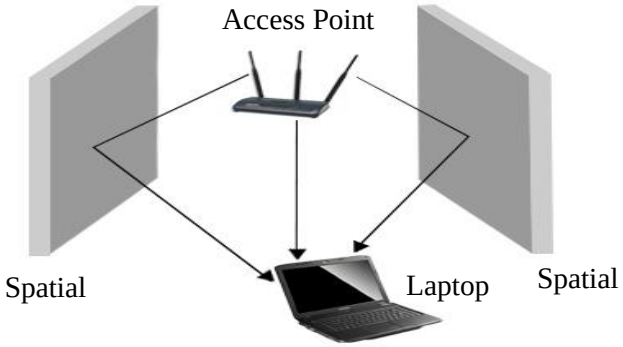
1.2.5 – Chuẩn mạng 802.11n

Chuẩn 802.11n đã được viện IEEE phê duyệt để sử dụng chính thức, đồng thời cũng đã vượt qua thử nghiệm và chứng nhận của Liên minh Wi-Fi (Wi-Fi Alliance) cho các sản phẩm tiêu chuẩn. Chứng nhận Wi-Fi 802.11n là một bản cập nhật bổ sung một số tính năng tùy chọn cho bản dự thảo 802.11n 2.0 (bản nháp 2.0) do Wi-Fi Alliance đưa ra vào tháng 6 năm 2007. Các yêu cầu cơ bản về băng thông, tốc độ, định dạng khung hình, khả năng tương thích ngược không thay đổi.

Về lý thuyết, chuẩn 802.11n cho phép kết nối ở tốc độ 300 Mbps (lên đến 600 Mbps), nhanh hơn 6 lần và mở rộng vùng phủ sóng so với tốc độ đỉnh lý thuyết của các chuẩn trước đó như 802.11g/a. 802.11n (54 Mbps), là mạng Wi-Fi đầu tiên có thể cạnh tranh với mạng có dây 100Mbps về hiệu suất. Chuẩn 802.11n có thể hoạt động ở tần số 2.4GHz và 5GHz, người ta kỳ vọng rằng nó có thể giảm bớt tình trạng "quá tải" ở các chuẩn trước đây.

Thông qua các thông số kỹ thuật đã được phê duyệt, MIMO **(Hình 1.2)** là một công nghệ thiết yếu trong các sản phẩm Wi-Fi 802.11n. Thường kết hợp với ghép kênh phân chia theo tần số trực giao (OFDM). MIMO có thể được tăng lên nhiều lần thông qua đa phân chia theo không gian (spatial multiplexing). Chia chuỗi dữ liệu thành nhiều chuỗi dữ liệu nhỏ hơn và gửi/nhận nhiều chuỗi nhỏ hơn song song trong cùng một kênh.

MIMO giúp cải thiện phạm vi phủ sóng và độ tin cậy của thiết bị thông qua một kỹ thuật được gọi là đa dạng không gian. Kết hợp với công nghệ MIMO là 2 công nghệ: STBC (Space Time Block Coding) cải thiện khả năng thu/truyền trên nhiều anten và chế độ HT Duplicate (MCS 32) - Cho phép gửi thêm gói tin tương tự cùng lúc lên mỗi kênh 20MHz khi thiết bị hoạt động ở chế độ 40MHz - giúp cải thiện độ tin cậy của thiết bị phát.



Hình 1. 2 Hệ thống MIMO NxM (N kênh phát và M kênh thu)

Ngoài công nghệ MIMO, thiết bị còn có thể được tích hợp các công nghệ khác để tăng tốc độ. Đầu tiên là công nghệ khoảng thời gian bảo vệ ngắn (SGI) cũng có thể tăng tốc độ bằng cách giảm khoảng cách giữa các biểu tượng (Symbol). Tiếp theo là một số công nghệ lớp vật lý, các cải tiến của nó được thiết kế để giảm overhead (gói tin mào đầu), góp phần cải thiện tốc độ trực tiếp.

Để giảm overhead, 802.11n sử dụng công nghệ kết hợp khung (FA) kết hợp hai hoặc nhiều khung thành một khung để truyền. Chuẩn 802.11n sử dụng hai công nghệ ghép khung: A-MSDU (Đơn vị dữ liệu dịch vụ tổng hợp-MAC) hoặc MSDU-tăng kích thước khung hình được sử dụng để truyền khung hình qua MAC (Điều khiển truy cập phương tiện) và A-MPDU (Tổng hợp-MAC) Đơn vị dữ liệu giao thức) -Tăng kích thước tối đa của khung 802.11n được truyền lên 64K byte (tiêu chuẩn trước đó chỉ là 2304 byte).

1.2.6 Chuẩn mạng 802.11ac (tên gọi WiFi 5)

802.11ac là chuẩn WiFi mới nhất và phổ biến nhất hiện nay. 802.11ac sử dụng công nghệ không dây băng tần kép để hỗ trợ kết nối đồng thời trên băng tần 2.4 GHz và 5 GHz. 802.11ac cung cấp khả năng tương thích với các chuẩn 802.11b, 802.11g và 802.11n, băng thông của băng tần 5 GHz lên đến 1300 Mbps và băng thông của 2.4 GHz lên đến 450 Mbps.

Trong chuẩn mạng Wifi 802.11ac có rất nhiều đặc điểm và chúng là ưu điểm lợi ích mà loại hình này mang lại như:

- Băng thông kênh rộng. Bởi vậy, tốc độ truyền dữ liệu nhanh hơn. Wi-Fi 802.11ac hoạt động trên dải tần 5GHz và hỗ trợ các kênh với các tùy chọn băng thông như 20MHz, 40MHz, 80MHz hoặc 160MHz.

- Mang lại nhiều luồng dữ liệu hơn. Nếu như trên wifi 802.11n, nó chịu trách nhiệm truyền tải tới 4 luồng không gian (luồng dữ liệu là quá nhiều công nghệ anten (MIMO), thì trên wifi 802.11ac, nó có thể xử lý gấp đôi, tức là 8 luồng dữ liệu, mỗi luồng dữ liệu 1 anten sẽ được sử dụng nên tương ứng với 8 luồng sẽ có 8 anten.

- Hỗ trợ Mutil user-MIMO. Nếu Wi-Fi 802.11n chỉ có thể truyền nhiều luồng không gian, nhưng tối đa chỉ một địa chỉ, thì cũng có thể hiểu rằng có thể truyền nhiều luồng thông tin nhưng dữ liệu chỉ có thể được nhận đến một thiết bị hoặc một người dùng tại một thời điểm dừng lại. Mặt khác, Wi-Fi 802.11ac thì khác, chúng có thể gửi nhiều luồng không gian nhưng cho phép nhiều ăng-ten tiếp cận nhiều người dùng và nhiều thiết bị khác nhau trên cùng một dải tần cùng một lúc. Thiết bị không còn phải chờ đợi như trên Wi-Fi 802.11n và nó sẽ không gây ra tình trạng nghẽn cổ chai hay nhiễu sóng. Với hỗ trợ MIMO nhiều người dùng, điều này hoàn toàn có thể.

- Phạm vi bao phủ sóng rộng hơn. Wi-Fi 802.11ac có phạm vi lớn hơn và tốc độ mạng nhanh hơn các chuẩn mạng khác. Nếu sử dụng trong các tòa nhà cao tầng, có thể giảm bớt các bộ lặp và bộ lặp lặp lại để giảm thiểu chi phí.

Ứng dụng của Wi-Fi 802.11ac:

• Tốc độ đường truyền nhanh hơn nên tốc độ đường truyền Internet cũng nhanh hơn. Sẽ tận dụng hết tốc độ mạng.

• Nó có thể được áp dụng để truyền dữ liệu giữa các thiết bị trong mạng cục bộ hoặc mạng gia đình và tốc độ của nó gấp nhiều lần tốc độ hiện nay.

• Giúp đảm bảo rằng việc sử dụng Internet ổn định và không bị nhiễu hoặc bị gián đoạn.

1.2.7 Chuẩn mạng 802.11ax (Wi-Fi thế hệ thứ 6)

Wi-Fi thế hệ thứ sáu là bản cập nhật mới nhất của chuẩn mạng không dây, so với chuẩn Wi-Fi trước đây, chúng có tốc độ nhanh hơn, dung lượng lớn hơn và tiết kiệm năng lượng hơn.

Wi-Fi thế hệ thứ sáu sẽ đáp ứng nhu cầu phát triển của ngành công nghệ thông tin hiện nay và trong tương lai. Theo nguồn thông tin, Wifi 6 sẽ chính thức được sử dụng vào năm 2019.

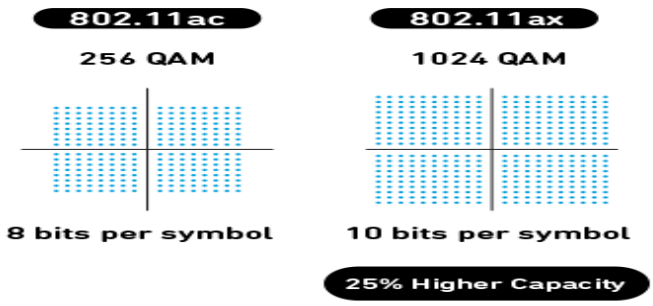
Đặc điểm của Wifi 6:

- Tốc độ cực nhanh: Nếu chuẩn wifi 802.11ac đạt 6.9 Gbps thì chuẩn 802.11ax sẽ cung cấp cho tốc độ 9.6Gbps. Thông qua việc sử dụng kết hợp 1024-QAM và tăng OFDM symbol time, kết nối tốc độ cao hơn có thể đạt được so với thế hệ cũ. Ngoài ra, vùng phủ sóng được mở rộng giúp người dùng xem video 4k mượt mà, bắt sóng wifi dễ dàng mọi nơi trong nhà hay kể cả những nơi hẻo lánh mà không hề tỏ ra yếu, nhiễu wifi.

- Nâng cao hiệu quả: Dung lượng của wifi thế hệ thứ 6 gấp 4 lần thế hệ thứ 5 và có khả năng phân bổ băng thông tối ưu, cả đường truyền tải lên và tải xuống đều đã thay đổi chức năng kết hợp với MU-MIMO. Do sự thay đổi tích cực này, ngay cả khi có nhiều tín hiệu, bộ định tuyến có thể kết nối nhiều thiết bị hơn.

– Điều chế cấp cao hơn 1024 - QAM: **(Hình 1.3)**

Trước đây mỗi symbol 1024-QAM sẽ mang 8 bits, bây giờ chúng sẽ có 10 bits, và so với chuẩn cũ, tốc độ truyền sẽ tăng 25%.



Hình 1. 3 Điều chế 1024 QAM - Chuẩn mạng Wifi 6

- Symbol OFDM x 4: Các ký hiệu OFDM và GI được sử dụng bởi chuẩn mạng 802.11ax dài hơn và sóng mang được tạo ra gấp 4 lần so với chuẩn 802.11ac. Điều này đồng nghĩa với việc nó sẽ giúp mở rộng phạm vi phủ sóng, khi sử dụng thì tốc độ WiFi cũng sẽ nhanh hơn cùng với sự ổn định của mạng WiFi.

- Độ rộng kênh 160MHz trên một luồng: Chuẩn mạng wifi thế hệ thứ sáu sẽ mang đến đường truyền rộng hơn (độ rộng kênh lên tới 160MHz, trong khi chuẩn cũ chỉ là 80MHz).

- OFDMA – Loại bỏ hoàn toàn độ trễ: Chuẩn 802.11ax sử dụng công nghệ OFDMA để truy cập nhanh hơn và hiệu quả hơn. Kể từ khi OFDMA chia phổ thành các đơn vị tài nguyên và phân bổ chúng cho nhiều người dùng khác nhau, nó hoàn toàn loại bỏ độ trễ, do đó tăng khả năng truy cập đến các mức cao hơn.

- 8x8 MU-MIMO: Chuẩn 802.11ax có thể hỗ trợ truyền đa người dùng MIMO đường lên và đường xuống bằng cách tạo nhiều luồng 802.11ax, do đó nhân hiệu suất của 802.11ac bằng cách tạo ra tối đa 8 luồng theo một hướng. Điều này sẽ hướng luồng đến nhiều thiết bị truy cập đồng thời.

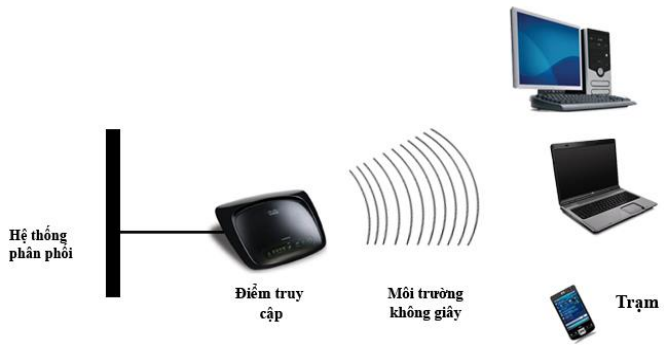
- Target Wake Time: Lịch kết nối của khách hàng sẽ phụ thuộc vào thời gian đánh thức mục tiêu, vì họ sẽ cho thiết bị biết thời gian và tần suất gửi và nhận dữ liệu. Điều này sẽ giảm thiểu điện năng tiêu thụ.

1.3 – Cơ sở hạ tầng mô hình mạng WLAN [2][8]

1.3.1 - Cấu trúc của mạng WLAN cơ bản (Hình 1.4)

Một mạng sử dụng chuẩn 802.11 bao gồm có 4 thành phần chính:

- Hệ thống phân phối (DS)
- Điểm truy cập (AP)
- Tần liên lạc vô tuyến (Wireless Medium)
- Trạm (Stations)



Hình 1. 4 Cấu trúc cơ bản của một mạng WLAN

1.3.2 - Điểm truy cập: AP (Hình 1.5)

AP là một thiết bị song công, và mức độ thông minh của nó tương đương với một bộ chuyển mạch Ethernet (Switch) phức tạp. Cung cấp điểm truy cập mạng cho máy khách (client).

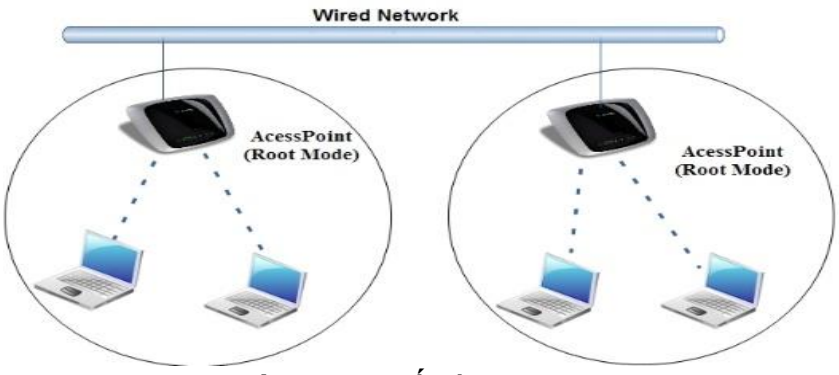
Hình 1. 5 Access Point TP Link

Chế độ hoạt động của AP:

AP có thể giao tiếp với các máy không dây, với mạng có dây truyền thống và với các AP khác. AP có 3 chế độ làm việc chủ yếu:

Chế độ gốc (Root mode): (Hình 1.6)

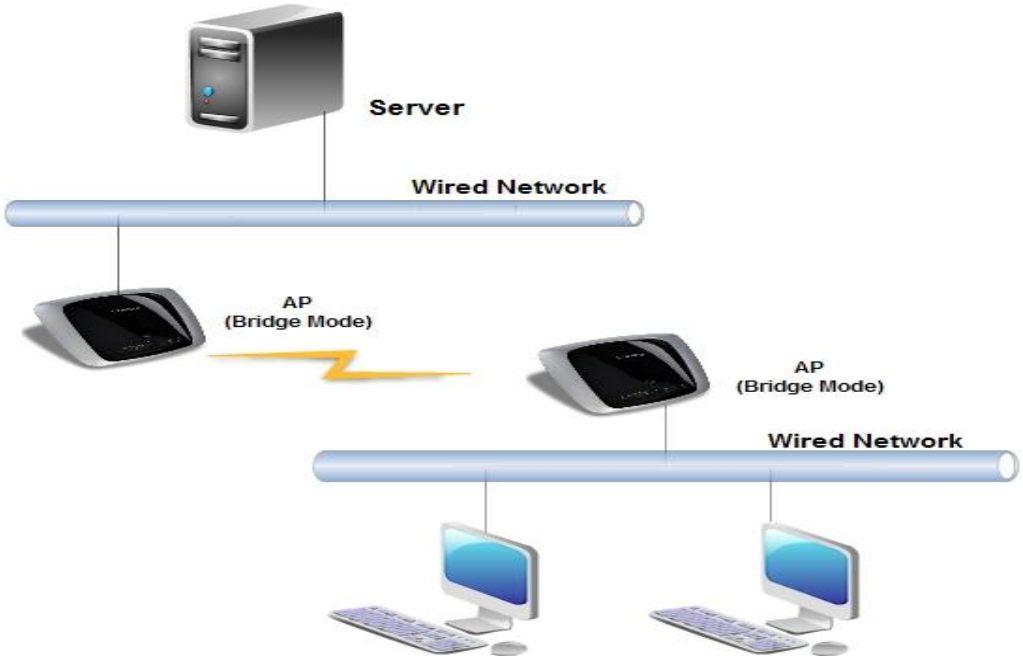
Khi AP được kết nối với đường trục có dây thông qua giao diện có dây (thường là Ethernet), nó sẽ sử dụng chế độ gốc. Hầu hết các AP sẽ hỗ trợ các chế độ khác với chế độ gốc, nhưng chế độ gốc là cấu hình mặc định của các AP. Khi AP được kết nối với phân đoạn mạng có dây thông qua cổng Ethernet của nó, nó sẽ được cấu hình để hoạt động ở chế độ gốc. Ở chế độ root mode, các AP được kết nối với cùng một hệ thống phân phối có dây có thể giao tiếp với nhau thông qua phân đoạn mạng có dây. Máy khách không dây có thể giao tiếp với các máy khách không dây khác nằm trong các ô khác nhau (ô hoặc vùng phủ sóng AP) thông qua các AP tương ứng được kết nối với chúng và sau đó các AP này sẽ giao tiếp với chúng. Liền kề nhau qua các đoạn mạng hữu tuyến.



Hình 1. 6 Chế độ Root Mode

- **Chế độ cầu nối (Bridge mode): (Hình 1.7)**

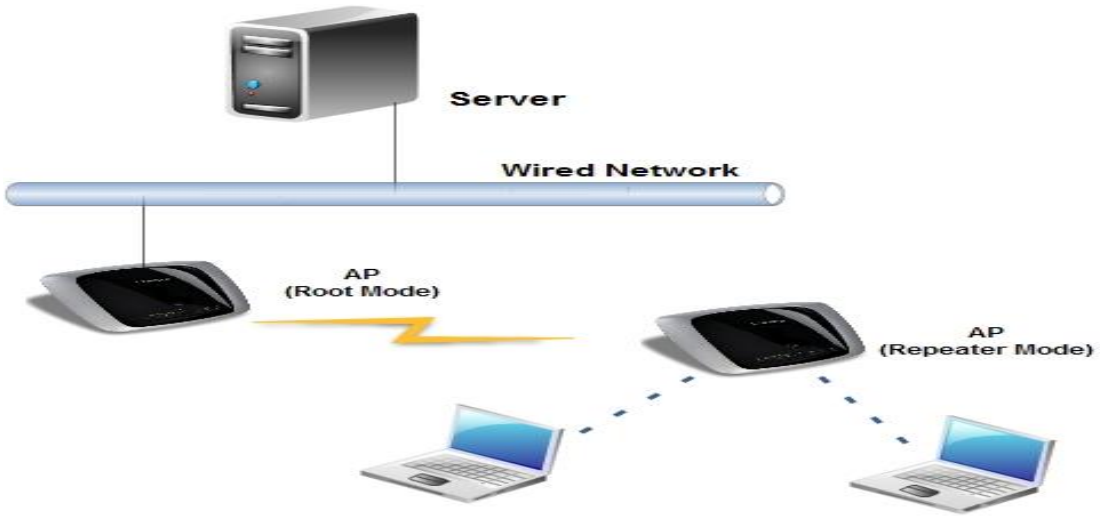
Ở chế độ Bride mode, nguyên lý hoạt động của AP hoàn toàn tương tự như cầu nối không dây. Chỉ có một số AP trên thị trường hỗ trợ chức năng cầu nối, điều này sẽ khiến giá thiết bị tăng lên đáng kể. Máy khách không kết nối với Bridge, nhưng sử dụng Bridge để kết nối 2 hoặc nhiều đoạn mạng có dây với nhau thông qua kết nối không dây.



Hình 1. 7 Chế độ Bridge Mode

- **Chế độ lặp (Repeater mode): (Hình 1.8)**

Trong Repeater mode, AP có thể cung cấp kết nối không dây ngược dòng tới mạng có dây thay vì kết nối có dây thông thường. Như trong **hình 1.8**, Một AP hoạt động như chế độ gốc và AP còn lại hoạt động như một bộ lặp không dây. AP ở chế độ lặp kết nối với máy khách dưới dạng AP và kết nối với AP ngược dòng với tư cách là máy khách. Trừ khi thực sự cần thiết, chắc chắn không nên sử dụng các AP ở chế độ lặp lại, vì trong trường hợp này, các ô xung quanh mỗi AP phải trùng nhau ít nhất 50%. Cấu hình này làm giảm đáng kể phạm vi mà máy khách có thể kết nối với bộ lặp AP. Ngoài ra, AP lặp lại giao tiếp với máy khách và AP ngược dòng thông qua kết nối không dây, điều này sẽ làm giảm thông lượng của phân đoạn mạng không dây.

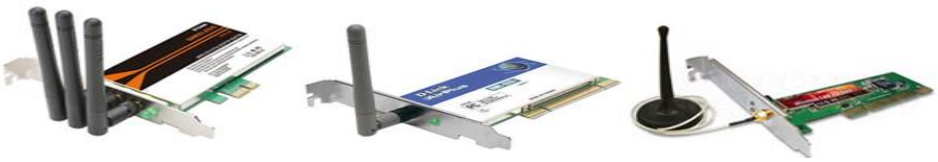


Hình 1. 8 Chế độ Repeater Mode

1.3.3 – Các thiết bị máy khách trong mạng WLAN

- Card PCI Wireless: **(Hình 1.9)**

Đây là thành phần phổ biến nhất trong mạng WLAN. Được sử dụng để kết nối máy khách với mạng không dây. Cắm nó vào khe PCI trên máy tính. Loại này thường được sử dụng cho máy tính để bàn kết nối mạng không dây.



Hình 1. 9 Card PCI Wireless

- Card PCMCIA Wireless: **(Hình 1.10)**

Hình 1. 10 Card PCMCIA Wireless

Trước đây được sử dụng cho máy tính xách tay (notebook computer) và thiết bị trợ lý kỹ thuật số cá nhân PDA (Personal Digital Associasion). Hiện nay, do sự phát triển của công nghệ, PCMCIA Wireless ít được sử dụng do các nguyên nhân như

máy tính xách tay và PDA… Tất cả các thiết bị đều có Card Wireless tích hợp trong thiết bị.

- Card USB Wireless: **(Hình 1.11)**

Do tính nhỏ gọn và khả năng di động, một loại rất phổ biến ngày nay được sử dụng cho các thiết bị kết nối với mạng không dây. Chức năng tương tự như card không dây PCI, nhưng chuẩn cắm được hỗ trợ là USB (Universal Serial Bus). Nó có thể được tháo rời nhanh chóng (không cần phải lắp cố định như thẻ không dây PCI) và hỗ trợ lắp vào khi máy tính đang chạy.

Hình 1. 11 Card USB Wireless

1.3.4 - Các mô hình mạng WLAN

Mạng WLAN bao gồm 3 mô hình cơ bản sau:

- Mô hình mạng độc lập (IBSS) hay còn gọi là mạng Ad hoc.
- Mô hình mạng cơ sở (BSS).
- Mô hình mạng mở rộng (ESS).

1.3.4.1 - Mô hình mạng độc lập (IBSS) hay gọi mạng AD HOC **(Hình 1.12)**

Các trạm làm việc (máy tính hỗ trợ card mạng không dây) được tập trung trong một không gian nhỏ để tạo thành một kết nối ngang hàng giữa chúng. Các nút di động

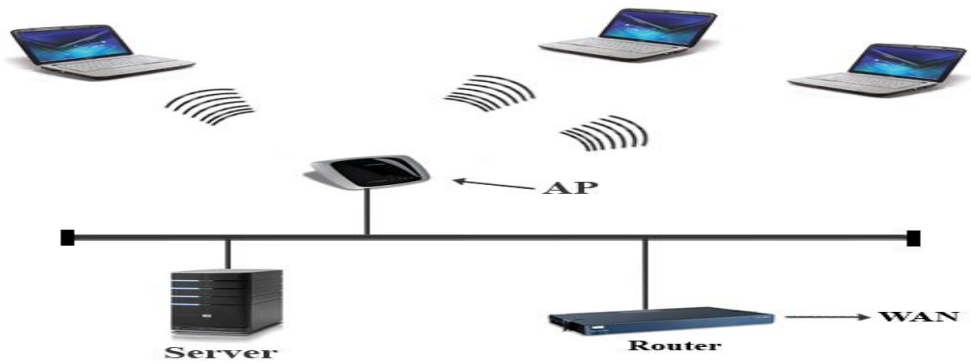
Hình 1. 12 Mô hình mạng IBSS

có card mạng không dây và chúng có thể giao tiếp trực tiếp với nhau mà không cần quản trị viên mạng. Vì các mạng tạm thời này có thể được thực hiện nhanh chóng và dễ dàng, chúng thường có thể được thiết lập mà không cần các công cụ hoặc kỹ năng đặc biệt, vì vậy chúng rất thích hợp để sử dụng trong các hội nghị thương mại hoặc trong các nhóm làm việc tạm thời. Tuy nhiên, chúng có thể có nhược điểm là phạm vi phủ sóng hạn chế và tất cả người dùng phải lắng nghe lẫn nhau.

- **Ưu điểm**: Kết nối ngang hàng không cần điểm truy cập, chi phí thấp, cấu hình và cài đặt đơn giản.
- **Khuyết điểm**: Khoảng cách giữa các máy trạm bị hạn chế, số lượng người dùng cũng hạn chế, không thể tích hợp vào mạng có dây hiện có.

1.3.4.2 - Mô hình mạng cơ sở (BSS): **(Hình 1.13)**

Trong mô hình mạng cơ sở, các máy khách muốn giao tiếp với nhau phải sử dụng một điểm truy cập (AP). AP là điểm trung tâm để quản lý mọi thông tin liên lạc trong mạng, do đó máy khách không thể giao tiếp trực tiếp như trong BSS độc lập. Để giao tiếp với nhau, máy khách phải gửi các Frame (khung dữ liệu) đến AP, sau đó AP sẽ gửi đến máy thu.

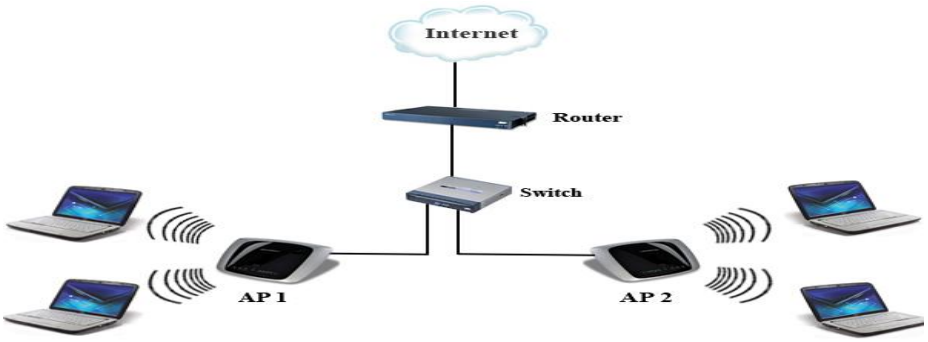


Hình 1. 13 Mô hình mạng BSS

- **Ưu điểm**: Các máy trạm không thể được kết nối trực tiếp với nhau và các máy trạm trên mạng không dây có thể được kết nối với mạng có dây.
- **Khuyết điểm**: So với mô hình Ad-Hoc, chi phí cao và việc cài đặt, cấu hình phức tạp hơn.

1.3.4.3 - Mô hình mạng mở rộng (ESS): **(Hình 1.14)**

Nhiều mô hình BSS được kết hợp với nhau và được gọi là mô hình mạng ESS. Đây là mô hình sử dụng 2 hoặc nhiều AP để kết nối mạng. Sau đó, các điểm truy cập này sẽ được kết nối với nhau để trở thành một mạng lớn hơn với phạm vi phủ sóng rộng hơn, thuận tiện và đáp ứng cho các khách hàng di động. Đảm bảo hoạt động của tất cả các khách dùng.



Hình 1. 14 Mô hình mạng ESS

1.4 – Các nguy cơ tấn công mạng WLAN [5] [7]

Mạng máy tính không dây cũng có những đặc điểm cơ bản của mạng máy tính nên các biện pháp tấn công và ngăn chặn trên mạng không dây cũng tương tự như trên mạng có dây. Ngoài ra, do các đặc điểm đặc biệt của mạng không dây trong không gian, nó sẽ phải chịu các kiểu tấn công khác nhau và cần có các biện pháp ngăn chặn khác.

Ngày nay, các cuộc tấn công và phòng chống WLAN đã trở thành vấn đề được các chuyên gia trong lĩnh vực bảo mật rất quan tâm. Nhiều giải pháp tấn công và phòng thủ đã được đưa ra, nhưng không có giải pháp nào thực sự được gọi là bảo mật hoàn chỉnh. Cho đến nay, tất cả các giải pháp bảo vệ được đề xuất là tương đối, có nghĩa là bảo mật trong mạng WLAN vẫn có thể bị phá vỡ theo nhiều cách. Chương này trình bày về các kiểu tấn công phổ biến, khái niệm, chức năng tấn công và một số phương pháp phòng chống trong mạng WLAN.

Hiện nay, có rất nhiều công nghệ có thể tấn công mạng WLAN, điển hình là các công nghệ sau:

. Phương thức bắt gói tin (Sniffing)

. De-authentication Attack (Tấn công yêu cầu xác thực lại)

. Replay Attack (Tấn công phát lại)

. Rogue Access Point (Giả mạo AP)

. Tấn công dựa trên sự cảm nhận lớp vật lý

. Disassociation Attack (Tấn công ngắt kết nối)

1.4.1 – Phương thức bắt gói tin (Sniffing)

Đánh hơi là một khái niệm cụ thể của khái niệm chung "nghe trộm" được sử dụng trong mạng máy tính. Nó có thể là phương pháp đơn giản nhất, nhưng nó vẫn hiệu quả để chống lại các cuộc tấn công WLAN. Bắt gói có thể hiểu là phương thức lấy cắp thông tin khi đầu thu nằm trong hoặc gần vùng phủ sóng. Nếu thiết bị không thực sự được kết nối với AP để nhận gói dữ liệu, ngay cả khi thiết bị nằm trong hoặc gần vùng phủ sóng của mạng, thì cuộc tấn công bắt gói sẽ khó phát hiện ra sự hiện diện của thiết bị.

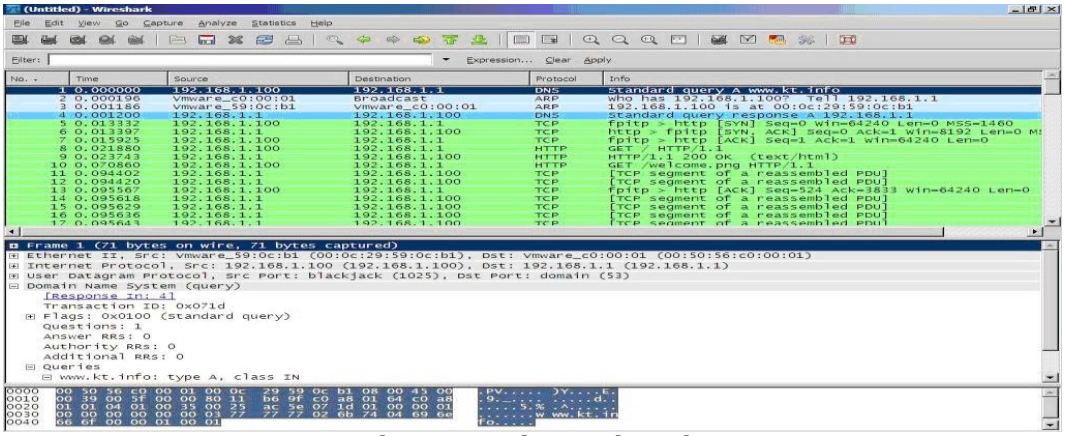
Chụp gói dữ liệu có dây thường được thực hiện dựa trên các thiết bị phần cứng mạng, chẳng hạn như sử dụng phần mềm bắt gói dữ liệu trên phần điều khiển đầu vào của card mạng máy tính. Bạn cũng cần biết loại thiết bị phần cứng bạn muốn sử dụng, tìm cách cài đặt phần mềm chụp gói trên đó, v.v. Đối với mạng không dây, các nguyên tắc trên vẫn được áp dụng, nhưng không nhất thiết phải sử dụng chúng, vì có nhiều cách đơn giản và dễ dàng để lấy thông tin. Bởi vì đối với mạng không dây, thông tin được phát qua phương tiện truyền thông và bất kỳ ai cũng có thể nhận được.

Chương trình bắt gói có thể giao tiếp với các trang HTTP, email, chương trình nhắn tin tức thời, phiên FTP, phiên telnet (nếu giao tiếp bằng văn bản rõ ràng). Một số chương trình có thể lấy mật khẩu trên mạng không dây của trao đổi khách-máy chủ khi mật khẩu được nhập để đăng nhập. Cũng từ việc bắt gói dữ liệu, có thể nắm bắt thông tin, phân tích lưu lượng mạng (phân tích lưu lượng), phổ năng lượng trong không gian khu vực. Từ đó, kẻ tấn công có thể biết được đâu là sóng lan truyền tốt, đâu là lan truyền chưa tốt và đã thu được nhiều máy ở đâu.

Ngoài việc trợ giúp trực tiếp cho quá trình phá hủy, việc nắm bắt các gói dữ liệu còn gián tiếp trở thành điều kiện tiên quyết cho các phương pháp phá hủy khác.

Nắm bắt gói dữ liệu là cơ sở của các phương thức tấn công, chẳng hạn như đánh cắp thông tin, thu thập thông tin về phân phối mạng (di chuyển), phát hiện mã, bẻ khóa mã (bẻ khóa).

Hình 1.15 là một ví dụ về Bắt gói tin bằng phần mềm Wireshark



Hình 1. 15 Bắt gói tin bằng phần mềm Wireshark

Các biện pháp ngăn chặn bắt gói tin: Vì "bắt gói tin" là phương thức tấn công thụ động nên rất khó phát hiện, đồng thời do đường truyền trên không phận nên không thể ngăn kẻ tấn công nghe trộm. Giải pháp ở đây là nâng cao khả năng mã hóa thông tin để kẻ tấn công không thể giải mã được, và khi đó thông tin thu được sẽ vô giá trị đối với kẻ tấn công. Cách tốt nhất để ngăn chặn việc đánh hơi là sử dụng IPSec để mã hóa thông lượng.

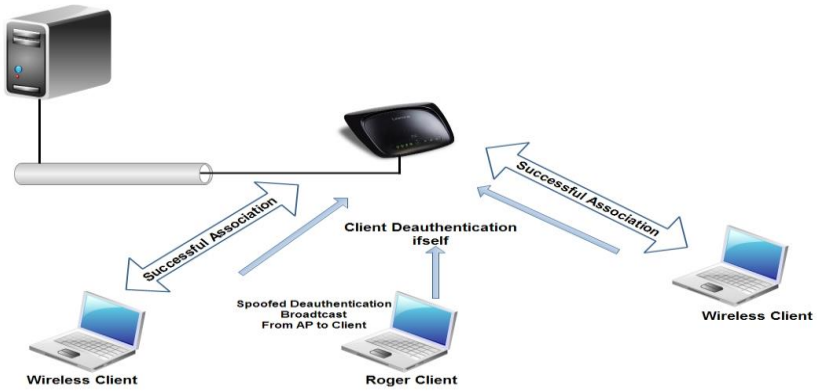
1.4.2 - Tấn công yêu cầu xác thực lại: (Hình 1.16)

Đây là một cách để khai thác hiệu quả các lỗi trong chuẩn 802.11. Trong mạng 802.11, khi một nút mới muốn tham gia vào mạng, nó phải trải qua quá trình xác minh danh tính và liên kết. Khi các yêu cầu được đáp ứng, nút sẽ được cấp quyền truy cập vào mạng.

Rất dễ lấy địa chỉ AP trên mạng. Khi kẻ tấn công biết địa chỉ AP, nó sẽ sử dụng địa chỉ quảng bá để gửi thông báo khử xác thực đến tất cả các nút trong mạng. Nút sẽ chấp nhận thông báo xác minh chắc chắn và thực hiện các biện pháp để xác minh xem thông báo hủy xác minh có được gửi từ AP hay không.

Bước tiếp theo trong quá trình này là tất cả các nút nhận được việc hủy xác thực sẽ kết nối lại, ủy quyền lại và liên kết lại với AP. Việc các nút cùng lúc được sửa

chữa khiến hệ thống mạng bị tắc nghẽn. Hoặc sau khi kết nối lại, kẻ tấn công sẽ liên tục gửi thông báo đến người dùng yêu cầu xác thực lại, từ đó ngăn người dùng truy cập mạng.



Hình 1. 16 Mô hình Deauthentication Attack

1.4.3 - Giả mạo AP:

Giả mạo AP là một cuộc tấn công điển hình "người ở giữa". Đây là kiểu tấn công mà kẻ tấn công ở giữa và đánh cắp lưu lượng giữa hai nút. Loại tấn công này rất mạnh mẽ vì kẻ tấn công có thể tận dụng tất cả lưu lượng truy cập trong mạng. Rất khó để tạo ra một cuộc tấn công "man in the middle" trên mạng có dây vì kiểu tấn công này yêu cầu quyền truy cập thực tế vào liên kết. Trong mạng không dây, kiểu tấn công này rất dễ bị tấn công. Kẻ tấn công cần tạo ra một AP thu hút nhiều sự lựa chọn hơn các AP chính thống. Bạn có thể đặt AP giả này bằng cách sao chép tất cả các cấu hình của một AP hợp pháp: SSID, địa chỉ MAC, ...

Bước tiếp theo là để nạn nhân thiết lập kết nối với AP giả mạo. Phương pháp đầu tiên là đợi người dùng kết nối thủ công. Phương pháp thứ hai là gây ra các cuộc tấn công từ chối dịch vụ DoS trong các AP chính thống, vì vậy người dùng sẽ phải kết nối lại với các AP giả mạo. Trong mạng 802.11, việc lựa chọn AP phụ thuộc vào cường độ của tín hiệu nhận được. Điều duy nhất mà kẻ tấn công phải làm là đảm bảo rằng AP của mình có cường độ tín hiệu mạnh hơn. Vì lý do này, kẻ tấn công phải đặt AP của mình gần nạn nhân hơn AP thực, hoặc sử dụng công nghệ ăng-ten định hướng. Sau khi nạn nhân kết nối với AP giả, nạn nhân vẫn hoạt động như bình thường, vì vậy nếu nạn nhân kết nối với một AP hợp pháp khác, dữ liệu của nạn nhân sẽ chuyển

qua AP giả. Khi nói chuyện với máy chủ web, kẻ tấn công sẽ sử dụng một tiện ích để ghi lại mật khẩu của nạn nhân. Bằng cách này, kẻ tấn công có thể lấy được tất cả thông tin mà hắn muốn đăng nhập vào mạng chính thống.

Kiểu tấn công này tồn tại vì 802.11 không yêu cầu xác thực lẫn nhau giữa AP và nút. AP phát tới toàn bộ mạng. Điều này rất dễ bị kẻ tấn công nghe trộm, vì vậy kẻ tấn công có thể lấy được tất cả thông tin mà chúng cần. Các nút trong mạng sử dụng WEP để xác thực các AP, nhưng WEP cũng có các lỗ hổng có thể bị khai thác. Kẻ tấn công có thể nghe trộm thông tin và sử dụng công cụ phân tích mật khẩu để đánh cắp mật khẩu của người dùng.

1.4.4 - Tấn công dựa trên sự cảm nhận lớp vật lý

Kẻ tấn công đã sử dụng giao thức chống va chạm CSMA/CA, khiến tất cả người dùng luôn nghĩ rằng có một máy tính trong mạng. Điều này khiến các máy tính khác luôn phải đợi kẻ tấn công hoàn tất việc truyền dữ liệu, dẫn đến tình trạng nghẽn mạng.

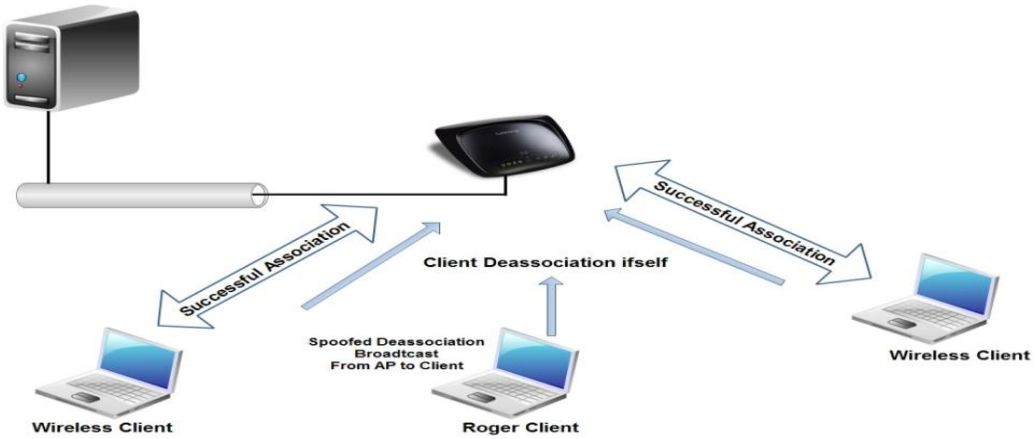
Tần số là một lỗ hổng bảo mật trong mạng không dây. Mức độ nguy hiểm phụ thuộc vào sự xuất hiện của lớp vật chất. Một số thông số xác định độ bền của mạng: công suất phát, độ nhạy của máy thu, tần số RF (tần số vô tuyến), băng thông và hướng anten. Trong 802.11, thuật toán đa truy cập nhận thức sóng mang (CSMA) được sử dụng để tránh va chạm.

CSMA là một phần không thể thiếu của lớp MAC. CSMA được sử dụng để đảm bảo không xảy ra xung đột dữ liệu trên đường truyền. Cuộc tấn công này không sử dụng tiếng ồn để gây ra lỗi trong mạng mà nó sử dụng chính tiêu chuẩn. Có nhiều cách để sử dụng giao thức cảm biến sóng mang vật lý. Một phương pháp đơn giản là làm cho các nút trên mạng tin tưởng rằng hiện có một nút đang truyền. Cách dễ nhất để đạt được điều này là tạo một nút giả giao tiếp liên tục. Một phương pháp khác là sử dụng bộ tạo tín hiệu RF. Một cuộc tấn công tinh vi hơn là làm cho card mạng vào chế độ kiểm tra, trong đó card mạng liên tục truyền chế độ kiểm tra. Tất cả các nút trong phạm vi của nút giả đều rất nhạy cảm với sóng mang, và nếu có nút gửi thì không nút nào sẽ truyền.

1.4.5 - Tấn công ngắt kết nối: (Hình 1.17)

Quá trình tấn công như sau:

- Kẻ tấn công xác định mục tiêu (máy khách không dây) và mối quan hệ giữa AP và máy khách.
- Sau đó, kẻ tấn công gửi một khung ngắt kết nối bằng cách giả mạo MAC nguồn và MAC mục tiêu tới AP và máy khách tương ứng.
- Máy khách sẽ nhận được các khung này và nghĩ rằng khung bị ngắt kết nối đến từ AP. Đồng thời, kẻ tấn công cũng gửi một khung hủy liên kết đến AP.
- Sau khi ngắt kết nối một máy khách, kẻ tấn công tiếp tục thực hiện thao tác tương tự trên các máy khách còn lại, khiến máy khách tự động ngắt kết nối khỏi AP.
- Sau khi máy khách ngắt kết nối, họ sẽ ngay lập tức kết nối lại với AP. Kẻ tấn công tiếp tục gửi khung ngắt kết nối đến AP và máy khách.



Hình 1. 17 Mô hình Disassociation Attack

Ngoài các kiểu tấn công mạng không dây nêu trên, còn một số kiểu tấn công WLAN khác như: Deny of Service Attack (DoS); Man in the middle Attack (MITM); Active Attack (Tấn công chủ động); Dictionary Attack (Tấn công bằng phương pháp dò từ điển); Jamming Attacks (Tấn công chèn ép),….

1.5 – Kết luận chương 1

Mạng không dây có nhiều ưu điểm, tuy nhiên hacker vẫn có thể sẽ tấn công để lấy dữ liệu và làm hỏng hệ thống. Vì phương tiện truyền dẫn là không dây nên việc đảm bảo an ninh của mạng cục bộ không dây là rất quan trọng. Ngày nay, do sự

phổ biến của mạng LAN không dây, bảo mật đã trở thành một trong những điểm yếu lớn nhất của mạng WLAN. Do điều kiện truy cập của mạng này, khả năng tiếp cận của các thiết bị bên ngoài trong không gian quảng bá là rất lớn. Đồng thời, khả năng bị nhiễu là không thể tránh khỏi. Để sử dụng mạng WLAN một cách an toàn, nghiên cứu sâu về các giải pháp bảo mật mạng WLAN là rất cần thiết. Trong chương II luận văn sẽ trình bày về vấn đề này.

CHƯƠNG II – CÁC GIẢI PHÁP BẢO MẬT TRONG MẠNG WLAN

2.1 – Giới thiệu

Trong hệ thống mạng, tính bảo mật và bí mật của hệ thống thông tin có vai trò rất quan trọng. Thông tin chỉ có giá trị nếu nó chính xác, và chỉ sau khi người có thẩm quyền lưu giữ thông tin biết được thông tin thì thông tin đó mới được bảo mật. Khi chúng ta không có thông tin hoặc việc sử dụng hệ thống thông tin không phải là phương tiện duy nhất để quản lý và vận hành, bảo mật đôi khi bị bỏ qua. Tuy nhiên, một khi hiểu được tầm quan trọng của tính bền vững của hệ thống và giá trị thực của thông tin hiện có, chúng ta có thể đánh giá tính bảo mật và an toàn của hệ thống thông tin ở một mức độ nhất định. Để đảm bảo an toàn cho hệ thống phải kết hợp cả yếu tố phần cứng, phần mềm và con người.

Chương này trình bày các phương pháp bảo mật được sử dụng trong WLAN, cũng như các khái niệm cơ bản, phương pháp hoạt động và đặc tính kỹ thuật của mỗi phương pháp. Đồng thời phân tích ưu nhược điểm của từng phương pháp.

2.1.1 – Nguyên nhân phải bảo mật

Mạng WLAN vốn dĩ không an toàn, nhưng dù sử dụng mạng LAN có dây hay WAN cũng không an toàn nếu không có phương pháp bảo mật hiệu quả. Để kết nối với mạng LAN có dây, người dùng cần truy cập đường truyền qua cáp và PC phải được kết nối với cổng mạng. Mạng không dây sử dụng sóng vô tuyến truyền xuyên qua các vật liệu, do vậy, vùng phủ sóng vô tuyến không chỉ trong phạm vi không gian hẹp mà có thể truy cập mạng không dây của công ty từ bên ngoài tòa nhà công ty bằng thiết bị phù hợp.

Khi chi phí xây dựng mạng WLAN ngày càng giảm, ngày càng có nhiều tổ chức, công ty và cá nhân sử dụng nó. Điều này chắc chắn sẽ khiến tin tặc quay sang tấn công và khai thác lỗ hổng trên các nền tảng mạng sử dụng chuẩn 802.11. Sniffer có thể nắm bắt giao tiếp mạng, chúng có thể phân tích và đánh cắp thông tin quan trọng của người dùng. Ngoài ra, tin tặc cũng có thể lấy đi dữ liệu bí mật của công ty; Can thiệp vào các giao dịch giữa tổ chức và khách hàng để lấy thông tin nhạy cảm,

hoặc làm hỏng hệ thống. Những mất mát to lớn cho tổ chức, công ty không thể đo lường trước được. Do đó, cần thiết lập một mô hình và chiến lược bảo mật.

2.1.2 - Đánh giá vấn đề an toàn, bảo mật hệ thống

Để đảm bảo an ninh cho hệ thống mạng, cần thiết lập nhiều tiêu chuẩn để đánh giá mức độ an toàn và bảo mật của hệ thống mạng. Một số tiêu chuẩn đã được công nhận là các biện pháp an ninh mạng.

Từ quan điểm vật lý, thiết bị phải đáp ứng các yêu cầu sau:

- Có thiết bị dự phòng nóng để đối phó với các trường hợp hỏng hóc đột ngột. Có thể trao đổi nhiệt hoàn toàn hoặc một phần (hot-plug, hot-swap).
- Khả năng nâng cấp, bổ sung phần cứng và phần mềm.
- Cần nguồn điện và cung cấp nguồn điện dự phòng trong trường hợp mất đột ngột.
- Theo yêu cầu của môi trường xung quanh: độ ẩm, nhiệt độ, chống sét, chống cháy, v.v.

Về dữ liệu:

- Thực hiện các bước sao lưu dữ liệu thường xuyên thay vì khi có sự cố.
- Thực hiện các biện pháp lưu trữ dữ liệu tập trung và phi tập trung nhằm giảm thiểu rủi ro cháy, nổ, thiên tai, chiến tranh và các trường hợp đặc biệt khác.

Về mặt logic, hệ thống bảo mật phải đáp ứng các yêu cầu sau:

- Tính bí mật (Confidentiality): Nó là đối tượng hạn chế quyền truy cập thông tin. Tùy thuộc vào bản chất của thông tin, mức độ bảo mật có thể khác nhau.
- Tính xác thực (Authentication): Tham gia đảm bảo thông tin liên lạc đáng tin cậy. Trong trường hợp của một tin nhắn (chẳng hạn như tín hiệu báo động hoặc cảnh báo), chức năng của dịch vụ ủy quyền là đảm bảo rằng người nhận tin nhắn đến từ một nguồn mà nó cho là đúng.

Trong trường hợp tương tác đang diễn ra, chẳng hạn như kết nối giữa thiết bị đầu cuối và máy chủ, có hai vấn đề sau: Thứ nhất, khi kết nối được bắt đầu, dịch vụ đảm bảo rằng hai thực thể là đáng tin cậy. Mỗi người trong số họ là một thực thể được xác định. Thứ hai, dịch vụ cần đảm bảo rằng kết nối không bị xáo trộn, vì thực thể

thứ ba có thể mạo danh một trong hai pháp nhân không được phép truyền hoặc nhận thông điệp.

- Tính toàn vẹn (Integrity): Tính toàn vẹn đảm bảo tính toàn vẹn của thông tin và loại bỏ mọi thay đổi cố ý hoặc làm hỏng hoặc mất thông tin do lỗi thiết bị hoặc phần mềm gây ra.
- Tính không xác định đảm bảo rằng người gửi và người nhận không thể từ chối tin nhắn đã gửi. Do đó, khi gửi một tin nhắn, người nhận có thể chứng minh rằng tin nhắn đó thực sự được gửi từ một người gửi hợp pháp. Tương tự, khi một tin nhắn được nhận, người gửi có thể chứng minh rằng nó thực sự được nhận bởi một người nhận hợp lệ.
- Tính khả dụng (Availability)
- Một hệ thống sẵn sàng đảm bảo có nghĩa là dữ liệu có thể được truy cập vào bất kỳ thời điểm nào mong muốn trong một thời gian nhất định. Các cuộc tấn công khác nhau có thể gây ra mất mát hoặc thiếu tính khả dụng của dịch vụ. Tính khả dụng của dịch vụ chứng tỏ khả năng ngăn ngừa và phục hồi các thiệt hại của hệ thống do các cuộc tấn công gây ra.
- Khả năng điều khiển truy nhập (Access Control): Trong bối cảnh an ninh mạng, kiểm soát truy cập là hạn chế khả năng truy cập máy chủ thông qua phương tiện truyền thông. Để đạt được sự kiểm soát này, cần phải xác định hoặc xác minh từng thực thể cố gắng có được quyền truy cập để quyền truy cập của mọi người có thể được thỏa mãn.

2.2 – Xác thực qua mã hóa Wifi [2][8]

2.2.1 - Wired Equivalent Privacy (WEP)

WEP là một thuật toán đơn giản sử dụng PRNG (Pseudo Random Number Generator) và dòng mã RC4. Vào tháng 9 năm 1994, một số người đã công bố mã nguồn của nó trực tuyến. Mặc dù mã nguồn hiện đã có, RC4 đã được đăng ký bởi RSADSI. Cơ sở mã RC4 có thể mã hóa và giải mã rất nhanh, dễ thực hiện và đủ đơn giản để các nhà phát triển phần mềm có thể sử dụng nó để mã hóa phần mềm.

WEP sử dụng khóa mã hóa 64 bits hoặc 128 bits không đổi (nhưng trừ đi 24 bits được sử dụng cho vectơ khởi tạo khóa mã hóa, do đó độ dài khóa chỉ là 40 hoặc 104 bits) cho phép truy cập vào mạng và cũng được sử dụng để mã hóa các thiết bị truyền dữ liệu.

Các khóa mã hóa này dể dàng được “bẻ gãy” bởi thuật toán brute-force và kiểu tấn công thử lỗi (tria-and-error). Phần mềm miễn phí như Aircrack-ng, Airsnort, hoặc WEP crack, nếu hacker thu thập 50 đến 10 triệu gói tin trên mạng không dây, nó sẽ cho phép chúng bẻ khóa mã hóa. Với những khóa mã hóa 128 bit cũng không khá hơn: 24 bit cho khởi tạo mã hóa nên chỉ có 104 bit được sử dụng để mã hoá và cách thức cũng giống như mã hóa có độ dài 64 bits nên mã hoaí 128 bits cũng dễ dàng bị bẻ khóa. Ngoài ra, điểm yếu của vector khởi tạo khóa mã hóa khiến tin tặc có thể tìm thấy mật khẩu nhanh hơn với ít thông tin hơn. Nhược điểm lớn nhất của WEP là nó sử dụng các khóa mã hóa tĩnh. Khi thiết lập cơ chế WEP cho bộ định tuyến, tất cả các thiết bị trên mạng sẽ sử dụng khóa để mã hóa tất cả các gói dữ liệu được truyền. Nhưng thực tế là, các gói dữ liệu mã hóa này không thể tránh khỏi việc bị đánh chặn. Do một số lỗi kỹ thuật "bí truyền", kẻ nghe trộm hoàn toàn có thể đánh chặn đủ số lượng gói tin mã hóa để tìm ra khóa giải mã là gì.

2.2.2 - WPA (Wi-Fi Protected Access)

WEP được thiết kế để bảo vệ mạng không dây khỏi bị nghe trộm. Nhưng ngay sau đó người ta đã phát hiện ra nhiều lỗ hổng trong công nghệ này. Vì vậy, một công nghệ mới mang tên WPA (Wi-Fi Protected Access) đã ra đời, khắc phục được nhiều khuyết điểm của WEP.

Một trong những cải tiến quan trọng nhất đối với WPA là việc sử dụng chức năng Giao thức toàn vẹn khóa tạm thời (TKIP). WPA cũng sử dụng thuật toán RC4 (chẳng hạn như WEP), nhưng sử dụng mã hóa 128-bit đầy đủ. Một chức năng khác của WPA là thay đổi khóa của mỗi gói. WPA không thể sử dụng các công cụ thu thập gói dữ liệu để giải mã khóa mã hóa. Vì WPA liên tục thay đổi khóa, tin tặc sẽ không bao giờ thu thập đủ dữ liệu mẫu để tìm mật khẩu. Ngoài ra, WPA cũng bao gồm kiểm tra tính toàn vẹn của tin nhắn. Do đó, dữ liệu không thể thay đổi trong quá trình

chuyển. Một trong những điểm hấp dẫn nhất của WPA là nó không yêu cầu bất kỳ nâng cấp phần cứng nào. Sử dụng WPA để dễ dàng và tự do nâng cấp phần mềm cho hầu hết các thẻ mạng và điểm truy cập.

Có hai tùy chọn cho WPA: WPA Personal và WPA Enterprise. Cả hai tùy chọn này đều sử dụng giao thức TKIP, sự khác biệt chỉ nằm ở khóa mã hóa ban đầu. WPA Personal thích hợp cho mạng gia đình và mạng văn phòng nhỏ, và khóa khởi tạo sẽ được sử dụng trên các điểm truy cập và thiết bị máy trạm. WPA doanh nghiệp yêu cầu máy chủ xác thực và 802.1x cung cấp khóa khởi tạo cho mỗi phiên.

Mặc dù Wi-Fi Alliance đã ra mắt WPA và được cho là sẽ loại bỏ tất cả các lỗ hổng WEP dễ bị tấn công, nhưng người dùng vẫn chưa thực sự tin tưởng vào WPA. Có một lỗ hổng trong WPA, lỗi này chỉ xảy ra trong WPA Personal. Vì chức năng thay đổi khóa TKIP được sử dụng để tạo khóa mã hóa được phát hiện, nếu một tin tặc có thể đoán khóa khởi tạo hoặc một phần của mật khẩu, họ có thể xác định toàn bộ mật khẩu và do đó có thể giải mã dữ liệu. Tuy nhiên, lỗ hổng này cũng có thể được loại bỏ bằng cách sử dụng các khóa khởi tạo không thể đoán trước. Điều này cũng có nghĩa là công nghệ WPA TKIP chỉ là một giải pháp tạm thời và chưa mang lại mức độ bảo mật cao nhất.

WPA chỉ áp dụng cho các công ty không truyền dữ liệu "bí mật" về thương mại hoặc thông tin nhạy cảm. WPA cũng thích hợp cho các hoạt động hàng ngày và các kỹ thuật thử nghiệm.

2.2.3 - WPA2 (Wi-Fi Protected Access II)

Giải pháp lâu dài là sử dụng Wi-Fi Alliance được chứng nhận 802.11i tương đương với WPA2. WPA2 được phát hành vào năm 2004. Đây là một cải tiến lớn đối với phần mềm mà chúng ta phải sử dụng trước đây, nó sử dụng một thuật toán mã hóa mạnh và được gọi là tiêu chuẩn mã hóa nâng cao AES. AES sử dụng mật mã đối xứng khối Rijndael, sử dụng mã hóa 128 bits, 192 bits hoặc 256 bits. Để đánh giá tiêu chuẩn mã hóa này, NIST đã thông qua thuật toán mật mã đối xứng này.

Mặc dù AES được coi là tốt hơn nhiều so với 128-bit WEP hoặc 168-bit DES (Tiêu chuẩn mã hóa kỹ thuật số). Để đảm bảo hiệu suất, quá trình mã hóa cần được

hoàn thành trong các thiết bị phần cứng như được tích hợp vào chip. Tuy nhiên, ít người dùng mạng không dây quan tâm đến vấn đề này. Ngoài ra, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch không tuân thủ 802.11i.

2.2.4 – WPA3 (Wi-Fi Protected Access III)

WPA3 ra đời nhằm khắc phục những điểm yếu mà thế hệ tiền nhiệm cần khắc phục.

WPA3 đã chính thức ra mắt vào tháng 6 năm 2018, nhưng giống như nhiều tiêu chuẩn kỹ thuật khác, nó vẫn đang được phát triển.

Là phiên bản kế thừa cho thế hệ thứ ba của WPA2, phiên bản thứ ba này có ba mục tiêu chính: cải thiện khả năng mã hóa, đơn giản hóa việc sử dụng và tích hợp, đồng thời trở thành một giải pháp mạnh mẽ cho thiết bị IoT.

Như đã biết, WPA2 có một vấn đề lớn, nó cho phép tin tặc xâm nhập vào mạng không dây như một người dùng bình thường. Thông thường, loại sự cố này sẽ do lỗi của con người trong quá trình thiết lập bộ định tuyến, nhưng không đơn giản để loại bỏ. Đây là điểm yếu cố hữu của tiêu chuẩn an toàn nên không thể khắc phục được.

Đối mặt với các mối đe dọa của hơn 400 triệu mạng không dây, WPA3 phải được giới thiệu nhanh chóng. Tuy nhiên, hiện tại không phải tất cả các bộ định tuyến hoặc thiết bị đều có thể sử dụng WPA3. Do đó, trong tương lai gần, WPA2 sẽ vẫn là một tiêu chuẩn mà các thiết bị được chứng nhận Wi-Fi phải hỗ trợ.

Những điểm mới của WPA3: WPA3 là sự cải tiến của nhiều thay đổi lớn. Đây đều là những nâng cấp đáng giá và hữu ích cho người dùng như:

- Mật khẩu người dùng sẽ khó bị hack hơn: Sử dụng tiêu chuẩn WPA2, ai đó có thể thu thập dữ liệu đã gửi và gửi đến thiết bị của bạn qua Wi-Fi, đồng thời giải mã nó thông qua các cuộc tấn công brute force (liên tục đoán mật khẩu cho đến khi tìm thấy mã chính xác). Tuy nhiên, đối với WPA3, mật khẩu dự đoán sẽ phải được xác minh trực tiếp trong thời gian thực bởi bộ định tuyến mà bạn đang cố gắng kết nối.
- Đơn giản hóa việc kết nối các thiết bị IoT: WPA3 sẽ giúp kết nối thiết bị không màn hình với bộ định tuyến dễ dàng hơn. Với phiên bản mới này, không cần

sử dụng điện thoại kết nối mạng Wi-Fi để vận hành các bước kết nối của từng thiết bị IoT, tất cả những gì cần làm là quét mã QR trên điện thoại.

- Dữ liệu mã hóa bị đánh cắp chỉ có thể được giải mã trong thời gian thực: Đây là một tính năng mới, ngay cả khi kẻ tấn công có mật khẩu chính xác, nó sẽ không thể mã hóa dữ liệu bị đánh cắp từ người dùng trong tương lai. Điều này làm cho mọi dữ liệu bị tin tặc đánh cắp hoàn toàn vô dụng.
- Các điểm truy cập công cộng sẽ bảo mật hơn**:** WPA3 cũng sẽ mã hóa kết nối giữa thiết bị của bạn và điểm phát sóng công cộng (không cần mật khẩu). Đây là một thay đổi lớn, vì WPA2 không mã hóa tín hiệu được gửi và gửi đến các điểm truy cập mạng công cộng. Sử dụng lỗ hổng này, bất kỳ ai cũng có thể dễ dàng tiết lộ thông tin nhạy cảm, chẳng hạn như tài khoản Facebook hoặc tin nhắn, khi sử dụng mạng Wi-Fi miễn phí.
- Mức độ mã hóa cao hơn cho Wi-Fi cấp độ Doanh nghiệp: Theo mặc định, khi ở trạng thái cá nhân hoặc gia đình, WPA3 sẽ sử dụng mã hóa 128-bit. Tuy nhiên, khi chạy ở chế độ doanh nghiệp, WPA3 sẽ sử dụng mã hóa 192-bit và thay thế PSK (Khóa chia sẻ trước) bằng SAE (Xác thực đồng thời bình đẳng).
- Cơ chế PSK là một hệ thống cho phép hai thiết bị có cùng thông tin đăng nhập (như mật khẩu) được kết nối. Thông tin đăng nhập sẽ được người dùng chia sẻ theo cách thủ công.
- Và SAE là một hệ thống sử dụng mật khẩu đăng nhập cùng lúc, được chia sẻ với địa chỉ MAC của hai thiết bị để xác thực dựa trên toán học của nhóm vòng lặp hữu hạn. Đây có phải là kiến thức toán học mà ai cũng cần hay không muốn biết.
- Mặc dù WPA3 dựa vào handshake (bắt tay) an toàn hơn, các nhà nghiên cứu bảo mật đã tìm thấy điểm yếu trong việc triển khai sớm WPA3-Personal, cho phép kẻ tấn công khôi phục mật khẩu WiFi bằng cách lạm dụng timing hoặc rò rỉ kênh bên dựa trên cache. Điều này có thể bị lạm dụng để đánh cắp thông tin nhạy cảm như số thẻ tín dụng, mật khẩu, tin nhắn trò chuyện, email, v.v.
- Các nhà nghiên cứu nhận thấy chế độ chuyển tiếp dễ bị các cuộc tấn công hạ cấp, những kẻ tấn công có thể lạm dụng để thiết lập một AP lừa đảo chỉ hỗ trợ

WPA2, buộc các thiết bị hỗ trợ WPA3 phải kết nối bằng cách sử dụng bắt tay 4 bước của WPA2.

- Hơn nữa, một vị trí trung gian là không cần thiết để thực hiện cuộc tấn công hạ cấp. Thay vào đó, những kẻ tấn công chỉ cần biết SSID của mạng WPA3- SAE.
- Các nhà nghiên cứu cũng mô tả chi tiết hai cuộc tấn công kênh bên (side-channel attacks) dựa trên bộ nhớ cache (CVE-2019-9494) và tấn công dựa trên thời gian (CVE-2019-9494), cho phép kẻ tấn công thực hiện một cuộc tấn công phân vùng mật khẩu, tương tự như một cuộc tấn công dictionary ngoại tuyến, để có được mật khẩu Wi-Fi.
- Bên cạnh đó, các nhà nghiên cứu cũng ghi nhận một cuộc tấn công từ chối dịch vụ có thể được khởi chạy bằng cách làm quá tải *"AP bằng cách khởi động một số lượng lớn các bắt tay với Access Point hỗ trợ WPA3"*, bỏ qua cơ chế chống tắc nghẽn của SAE được cho là để ngăn chặn các cuộc tấn công DoS .

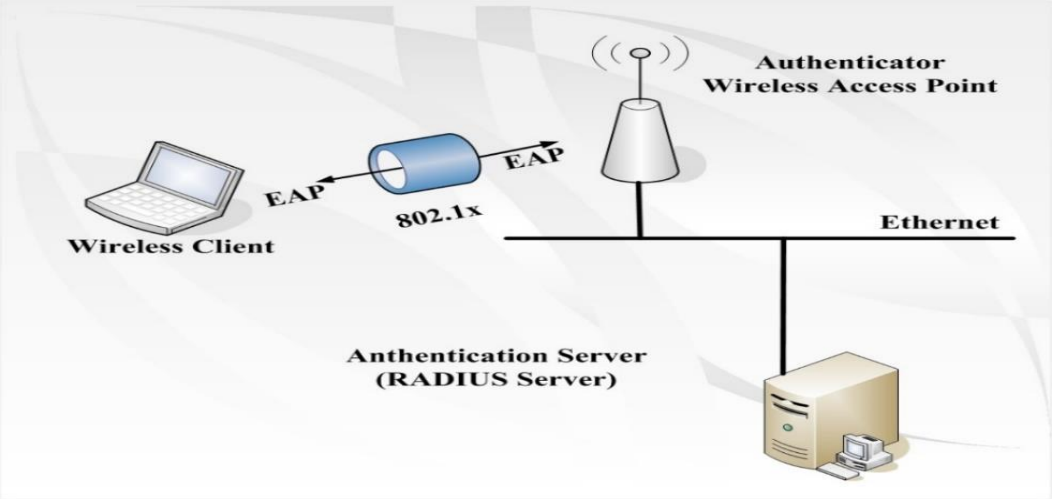
2.3 – Xác thực Wifi bằng RADIUS Server

2.3.1 Tổng quan về giao thức RADIUS

- Giao thức RADIUS: RADIUS thực chất là một giao thức mạng được sử dụng để xác thực và cho phép người dùng truy cập mạng từ xa. RADIUS được giới thiệu lần đầu tiên vào năm 1991. Ngày nay, RADIUS vẫn là một công cụ quản lý truy cập người dùng mạng rất mạnh mẽ.

- RADIUS cho phép xác thực tập trung, ủy quyền và kiểm tra quyền truy cập cho mạng. Ban đầu được phát triển cho cài đặt kết nối từ xa. Radius hiện hỗ trợ máy chủ VPN, điểm truy cập không dây, xác thực trao đổi Internet, truy cập DSL và các loại truy cập mạng khác. RADIUS được mô tả trong RFC 2865, "Dịch vụ người dùng quay số xác thực từ xa (RADIUS), (tiêu chuẩn dự thảo IETF) và RFC 2866," Kế toán RADIUS "(Thông tin).

- Bảo mật WLAN kết hợp tiêu chuẩn 802.1x với xác thực người dùng trên điểm truy cập (AP). Máy chủ thực hiện xác thực trên nền tảng RADIUS là một giải pháp tốt để cung cấp xác thực cho tiêu chuẩn 802.1x.



Hình 2. 1 Mô hình xác thực giữa máy khách không dây và máy chủ RADIUS

2.3.2 Tính chất của RADIUS

RADIUS có các tính chất chính như sau:

Nếu yêu cầu đến máy chủ xác thực chính không thành công, yêu cầu phải được gửi đến máy chủ phụ. Để thực hiện yêu cầu này, một bản sao của yêu cầu phải được lưu trữ trên lớp truyền tải để cho phép truyền thay thế. Điều này có nghĩa là phải có bộ đếm thời gian để truyền lại.

Các yêu cầu về thời gian của RADIUS hoàn toàn khác với yêu cầu của TCP. Một mặt, RADIUS không cần "phản hồi" với việc phát hiện dữ liệu bị mất. Người dùng sẵn sàng đợi một vài giây để hoàn thành ủy quyền. Đối với TCP, truyền lại thường được thực hiện dựa trên thời gian truyền trung bình không cần thiết (bao gồm cả thời gian mất xác nhận phản hồi). Mặt khác, người dùng không thể đợi quá lâu để xác nhận quyền, và việc chờ đợi là không hữu ích. Việc sử dụng hoán đổi nhanh chóng các server sẽ cho phép user truy cập được vào mạng trước khi họ bỏ cuộc.

Trạng thái của RADIUS rất thoải mái, đơn giản hóa việc sử dụng UDP. Khách hàng và máy chủ có thể được đăng ký trong hoặc ngoài mạng. Vì một lý do nào đó, hệ thống khởi động lại, ví dụ: mất điện ... nếu có một khoảng thời gian chờ tốt và cầu TCP được xác định, các sự kiện bất thường này thường không nguy hiểm. Tuy nhiên, UDP hoàn toàn bỏ qua những vấn đề đặc biệt này. Máy khách và máy chủ có thể thực

hiện "truyền" dữ liệu UDP tức thì và cho phép chúng truyền các sự kiện có thể xảy ra một cách tự nhiên thông qua mạng.

UDP đơn giản hóa việc triển khai máy chủ. Trong các phiên bản trước, máy chủ là một luồng, có nghĩa là chỉ có một yêu cầu được nhận, xử lý và trả lại tại một thời điểm. Điều này không thể được quản lý trong bối cảnh của các cơ chế bảo mật back-end thời gian thực. Hàng đợi yêu cầu của máy chủ sẽ đầy và trong môi trường mà hàng trăm người được yêu cầu xác nhận quyền mỗi phút, thời gian quay vòng cho các yêu cầu lâu hơn nhiều so với thời gian chờ đợi của người dùng. Do đó, giải pháp được lựa chọn là sử dụng UDP để triển khai máy chủ ở chế độ đa luồng. Quá trình xử lý độc lập sẽ được tạo ra trên máy chủ cho mỗi yêu cầu và các quá trình xử lý này sẽ phản hồi trực tiếp đến NAS của máy khách thông qua các gói dữ liệu UDP đến lớp truyền tải chính của máy khách.

2.3.3 Quá trình trao đổi gói tin

Khi máy khách được cấu hình để sử dụng RADIUS, bất kỳ người dùng máy khách nào cũng sẽ giới thiệu thông tin đăng nhập cho máy khách. Đây có thể là một dấu nhắc lệnh để đăng ký mạng và yêu cầu người dùng nhập tên người dùng và mật khẩu. Người dùng có thể chọn sử dụng giao thức thích hợp để thực hiện việc trình bày thông tin này trong một gói dữ liệu chẳng hạn như PPP.

Mỗi máy khách nhận được thông tin như vậy và nó có thể chọn sử dụng RADIUS để xác thực. Ứng dụng khách sẽ đưa ra một "yêu cầu truy cập" chứa các thuộc tính giống nhau: mật khẩu của người dùng, ID ứng dụng khách và ID cổng mà người dùng sẽ truy cập. Mật khẩu đã nhập sẽ bị ẩn (mã hóa RSA hoặc MD5). "Yêu cầu truy cập" sẽ được gửi đến RADIUS qua mạng. Nếu không có phản hồi trong thời gian quy định, yêu cầu sẽ được gửi lại. Nếu máy chủ chính gặp sự cố hoặc chạy theo kiểu vòng tròn, máy khách có thể chuyển tiếp yêu cầu đến máy chủ dự phòng.

Mỗi khi máy chủ RADIUS nhận được yêu cầu, nó sẽ xác nhận việc gửi của máy khách. Các yêu cầu từ khách hàng không chia sẻ thông tin bí mật với RADIUS sẽ không được xác nhận và trả lời. Nếu máy khách hợp lệ, máy chủ RADIUS sẽ tìm kiếm người dùng có cùng tên trong yêu cầu trong cơ sở dữ liệu. Chỉ mục người dùng

trong cơ sở dữ liệu sẽ chứa danh sách các yêu cầu cần thiết để cho phép người dùng truy cập mạng. RADIUS sẽ luôn xác minh mật khẩu của người dùng và cũng có thể xác minh ID ứng dụng khách và ID cổng mà người dùng được phép truy cập.

Máy chủ RADIUS có thể yêu cầu các máy chủ khác xác nhận yêu cầu. RADIUS sau đó hoạt động như một máy khách.

Nếu bất kỳ điều kiện nào không được đáp ứng, máy chủ RADIUS sẽ gửi phản hồi "Truy cập bị Từ chối", cho biết rằng yêu cầu của người dùng không hợp lệ. Máy chủ có thể bao gồm một thông báo tin nhắn văn bản trong phần từ chối truy cập để máy khách có thể hiển thị nó cho người dùng. Không có thuộc tính nào khác được phép trong quyền truy cập bị từ chối.

Nếu tất cả các điều kiện được đáp ứng và máy chủ RADIUS muốn gửi yêu cầu phản hồi của người dùng, RADIUS sẽ gửi phản hồi "yêu cầu truy cập" (access-challenge), nó có thể ở dạng một tin nhắn văn bản được hiển thị bởi khách hàng cho người dùng hoặc nó có thể là một thuộc tính trạng thái (state attribute). Máy khách sẽ nhận access-challenge, và nếu máy khách được trang bị challenge/ response, nó sẽ hiển thị thông báo nhắc nhở người dùng trả lời yêu cầu. Sau đó, máy khách sẽ gửi lại (re-submit) “yêu cầu truy cập” (original access-request) với một số hiệu yêu cầu (request ID) mới, nhưng thuộc tính tên người dùng và mật khẩu được lấy từ thông tin vừa mới nhập, và bao gồm cả thuộc tính trạng thái từ access-challenge. Máy chủ RADIUS có thể phản hồi các yêu cầu truy cập với sự chấp nhận truy cập, từ chối truy cập hoặc một access-challenge khác.

Nếu tất cả các điều kiện trên cuối cùng được đáp ứng, danh sách giá trị cấu hình của người dùng sẽ được đưa vào câu trả lời “chấp nhận truy cập ". Các giá trị này bao gồm loại dịch vụ (SLIP, PPP, Login...) và các giá trị cần thiết để cung cấp dịch vụ. Ví dụ, đối với SLIP hoặc PPP, các giá trị này có thể là địa chỉ IP, mặt nạ mạng con, phương pháp nén và số lọc gói. Trong chế độ ký tự, các giá trị này có thể là giao thức và tên máy chủ.

2.3.4 - Xác thực, cấp phép và kiểm toán

Giao thức dịch vụ người dùng quay số xác thực từ xa (RADIUS) được định nghĩa trong RFC 2865 như sau: nó có khả năng cung cấp xác thực tập trung, ủy quyền và kiểm soát truy cập (xác thực, ủy quyền và kế toán-AAA) cho các phiên. Được sử dụng kết hợp với SLIP và quay số PPP vì các nhà cung cấp dịch vụ xác thực Nhà cung cấp dịch vụ Internet (ISP) dựa vào giao thức này để xác thực người dùng với Internet.

Danh sách tên người dùng và mật khẩu phải được sử dụng để ủy quyền trong tất cả các máy chủ truy cập mạng (NAS). Một yêu cầu truy cập RADIUS sẽ chuyển thông tin đến máy chủ xác thực, thường là máy chủ AAA.

Trong cấu trúc hệ thống, dữ liệu người dùng, thông tin và các điều kiện truy cập có thể được tập trung vào một điểm (single point), nhà cung cấp giải pháp NAS có khả năng cung cấp các hệ thống quy mô lớn.

Khi người dùng kết nối, NAS sẽ gửi thông báo yêu cầu truy cập RADIUS đến máy chủ AAA, đồng thời truyền thông tin như tên người dùng và mật khẩu thông qua cổng được chỉ định, NAS identify và thông báo xác thực.

Sau khi nhận được các thông tin, máy chủ AAA sử dụng các gói dữ liệu được cung cấp (chẳng hạn như NAS identify), trình xác thực xác minh xem NAS có được phép gửi các yêu cầu đó hay không. Nếu có thể, máy chủ AAA sẽ kiểm tra thông tin tên người dùng và mật khẩu mà người dùng yêu cầu trong cơ sở dữ liệu. Nếu kiểm tra chính xác, nó sẽ mang một thông báo trong "yêu cầu truy cập" xác định quyền truy cập của người dùng có được chấp nhận hay không.

Khi quá trình xác thực bắt đầu được sử dụng, máy chủ AAA có thể sẽ trả về một RADIUS Access-Challenge mang một số ngẫu nhiên. NAS chuyển thông tin đến người dùng từ xa (trong ví dụ này, CHAP được sử dụng). Sau đó, người dùng sẽ phải trả lời chính xác yêu cầu xác nhận (trong ví dụ này, yêu cầu mã hóa mật khẩu được cung cấp), và sau đó NAS sẽ chuyển tiếp thông báo yêu cầu truy cập RADIUS đến máy chủ AAA.

Nếu máy chủ AAA sau khi kiểm tra các thông tin của người dùng hoàn toàn thoả mãn sẽ cho phép sử dụng dịch vụ, nó sẽ trả về một message dạng RADIUS Access-Accept. Nếu không, máy chủ AAA sẽ trả về thông báo bị từ chối quyền truy cập RADIUS và NAS sẽ ngắt kết nối với người dùng.

Sau khi nhận được một gói tin Access-Accept và RADIUS Accounting đã được thiết lập, NAS sẽ gửi một gói tin RADIUS Accounting-Request (Start) tới máy chủ AAA. Máy chủ thêm các thông tin vào tệp nhật ký của nó, với việc NAS sẽ cho phép phiên làm việc với người dùng bắt đầu khi nào, và kết thúc khi nào. RADIUS Accouting làm nhiệm vụ ghi lại quá trình xác thực của người dùng vào hệ thống, khi kết thúc phiên làm việc NAS sẽ gửi một thông báo RADIUS Accounting-Request (Stop).

2.3.5 - Sự bảo mật và tính mở rộng

Tất cả các thông báo RADIUS được đóng gói bởi các biểu đồ dữ liệu UDP, bao gồm các thông tin như: loại thông báo, số thứ tự, độ dài, trình xác thực và các giá trị thuộc tính khác nhau.

Authenticator: Mục đích của Authenticator là cung cấp một chế độ an toàn. Máy chủ NAS và AAA sử dụng trình xác thực để hiểu thông tin được mã hóa của nhau, chẳng hạn như mật khẩu. Trình xác thực cũng có thể giúp NAS phát hiện giả mạo các gói phản hồi RADIUS. Cuối cùng, sử dụng trình xác thực để chuyển đổi mật khẩu thành một số dạng để ngăn mật khẩu của người dùng bị rò rỉ trong thông báo RADIUS.

Authenticator gửi một yêu cầu truy cập với một số ngẫu nhiên. MD5 sẽ băm số ngẫu nhiên thành một định dạng riêng biệt hoặc sử dụng nó làm mật khẩu người dùng, sau đó gửi nó thông qua một yêu cầu truy cập. Sau đó, MD5 sử dụng cùng các tham số bảo mật Authenticator và các tham số phản hồi khác để băm toàn bộ phản hồi RADIUS.

Trình xác thực làm cho giao tiếp giữa NAS và máy chủ AAA được bảo mật, nhưng nếu kẻ tấn công nắm bắt được cả yêu cầu truy cập RADIUS và gói phản hồi truy cập, một "cuộc tấn công từ điển" có thể được thực hiện để phân tích việc đóng gói này. Trong thế giới thực khó giải mã, cần sử dụng các thông số dài hơn và toàn bộ vấn đề truyền dẫn có thể gây hại được mô tả trong RFC 3580.

Attribute-Value Pairs: Thông tin được mang bởi RADIUS được miêu tả trong một dạng Attribute-Value, hỗ trợ nhiều công nghệ khác nhau và nhiều phương pháp xác thực khác nhau. Một chuẩn được định nghĩa trong Attribute-Value pairs (cặp đôi), bao gồm User-Name, User-Password, NAS-IPAddress, NAS-Port, Service-Type. Các nhà sản xuất cũng có thể xác định các cặp thuộc tính-giá trị để mang thông tin của riêng họ, chẳng hạn như "nhà cung cấp cụ thể", tất cả các ví dụ này được mô tả trong RFC 2548 - Định nghĩ Microsoft Attribute-Value pair trong MS-CHAP.

Ngoài ra, trong nhiều năm, nhiều cặp "thuộc tính-giá trị" tiêu chuẩn đã được xác định để hỗ trợ Giao thức xác thực mở rộng (EAP). Các phiên bản trước của giao thức này là giao thức quay số PAP và CHAP. Ta cũng có thể tìm thấy phiên bản mới nhất của RADIUS hỗ trợ EAP trong tài liệu RFC 3579. Trong phần này, tôi sẽ thảo luận thêm về hỗ trợ xác thực cho WLAN, vì tiêu chuẩn EAP được sử dụng cho kiểm soát truy cập cổng 802.1x để kích hoạt xác thực bên ngoài không dây.

2.3.6 - Áp dụng RADIUS cho WLAN

Cơ chế hoạt động:

RADIUS xác định quyền truy cập của người dùng mạng thông qua mô hình máy khách/máy chủ. Tuy nhiên, trên thực tế, yêu cầu truy cập mạng thường được gửi từ hệ thống máy khách và người dùng hoặc điểm truy cập WiFi tới hệ thống máy chủ RADIUS để xác thực.

Máy chủ RADIUS thường là sự kết hợp của các hệ thống tạo, duy trì và quản lý thông tin nhận dạng và cung cấp các dịch vụ xác thực riêng lẻ. Do đó, khi người dùng muốn truy cập mạng được bảo vệ bởi giao thức RADIUS từ xa, họ phải cung cấp thông tin xác thực phù hợp với dữ liệu trong chức năng thư mục liên kết.

Khi người dùng muốn truy cập để cung cấp thông tin đăng nhập đầy đủ, dữ liệu sẽ được truyền từ máy khách đến máy chủ RADIUS thông qua người yêu cầu. Nếu thông tin người dùng khớp với thông tin được lưu trữ trong cơ sở dữ liệu liên kết, một thông báo xác thực sẽ được gửi trở lại máy khách RADIUS để người dùng có thể truy cập để kết nối với mạng. Ngược lại, nếu dữ liệu không khớp, thông báo từ chối sẽ được hiển thị.

- Cấu trúc giao thức: Trong một mạng Wireless sử dụng 802.1x Port Access Control, các máy trạm sử dụng wireless với vai trò Remote User và Wireless Access Point làm việc như một Network Access Server (NAS). Để thay thế cho việc kết nối đến NAS với dial-up như giao thức PPP, wireless station kết nối đến Access Point bằng việc sử dụng giao thức 802.11.

Một quá trình được thực hiện, wireless station gửi một message EAP-Start tới Access Point. Điểm truy cập sẽ yêu cầu trạm nhận ra thông tin này và chuyển nó đến máy chủ AAA và sử dụng thông tin này làm thuộc tính của tên người dùng của yêu cầu truy cập RADIUS.

Máy chủ AAA và trạm không dây hoàn thành quá trình này bằng cách truyền thông tin yêu cầu truy cập và yêu cầu truy cập RADIUS trên điểm truy cập. Được xác định ở trên là một dạng EAP. Thông tin này được truyền trong một đường hầm TLS được mã hóa (Encypted TLS Tunnel).

Nếu máy chủ AAA gửi thông báo chấp nhận quyền truy cập, điểm truy cập và trạm không dây sẽ hoàn tất kết nối và sử dụng WEP hoặc TKIP cho phiên để mã hóa dữ liệu. Cho đến lúc đó, điểm truy cập sẽ không cấm các cổng và trạm không dây gửi và nhận dữ liệu từ mạng một cách bình thường.

Cần lưu ý là mã hoá dữ liệu từ wireless station tới Access Point khác với quá trình mã hoá từ Access Point tới máy chủ AAA Server (RADIUS Server).

Nếu máy chủ AAA gửi một message Access-Reject, Access Point sẽ ngắt kết nối tới trạm. Trạm có thể cố gắng thử quá tình xác thực lại, nhưng AP sẽ cấm trạm này không gửi được các gói tin tới các điểm truy cập gần đó. Xin lưu ý rằng trạm này hoàn toàn có khả năng nghe dữ liệu do các trạm khác gửi về - thực tế thì dữ liệu được gửi qua sóng vô tuyến, đây là câu trả lời cho việc tại sao phải mã hóa dữ liệu khi gửi dữ liệu trong mạng không dây.

Attribute-Value pare bao gồm trong message của RADIUS có thể sử dụng bởi máy chủ AAA để quyết định phiên làm việc giữa Access Point và wireless station, như Sesstion-Timeout hay VLAN Tag (Tunnel-Type=VLAN, Tunnel-Private-

Group-ID=tag). Thông tin chính xác được thêm vào có thể phụ thuộc vào máy chủ AAA hoặc điểm truy cập và trạm được sử dụng.

2.3.7 - Các tùy chọn bổ sung

Điều đầu tiên là phải hiểu vai trò của RADIUS trong quá trình xác thực của WLAN, phải thiết lập một máy chủ AAA hỗ trợ interaction.

Nếu chúng ta có một máy chủ AAA được gọi là RADIUS trên mạng, nó có thể hỗ trợ xác thực 802.1x và cho phép lựa chọn loại EAP. Nếu vậy, chúng ta sẽ chuyển sang bước tiếp theo.

Nếu có máy chủ RADIUS-AAA không hỗ trợ 802.1x hoặc không hỗ trợ loại EAP, chúng tôi có thể lựa chọn bằng cách cập nhật lên phiên bản phần mềm mới hơn của máy chủ hoặc cài đặt máy chủ mới. Nếu bạn cài đặt một máy chủ AAA hỗ trợ xác thực 802.1x, bạn có thể sử dụng chức năng proxy RADIUS để thiết lập một chuỗi máy chủ chia sẻ cùng một cơ sở dữ liệu tập trung. Nó có thể được sử dụng để chuyển yêu cầu xác thực đến máy chủ 802.1x đã xác thực.

Trên cơ sở tập trung - giải pháp sử dụng RADIUS cho mạng WLAN là rất quan trọng, bởi vì nếu mạng của chúng ta có nhiều điểm truy cập, rất khó để cấu hình hệ thống riêng biệt để bảo vệ an ninh của hệ thống. Người dùng có thể xác thực từ nhiều điểm truy cập khác nhau, nhưng điều này không an toàn.

Việc sử dụng RADIUS cho mạng WLAN mang lại sự tiện lợi rất cao, đó là xác thực toàn bộ hệ thống nhiều điểm truy cập, từ đó đưa ra giải pháp thông minh hơn.

2.3.8 - Lựa chọn máy chủ RADIUS như thế nào là hợp lý

Trong phần trước, chúng ta đã thấy rằng máy chủ RADIUS cung cấp xác thực cho kiểm soát truy cập cổng 802.1x. Chúng ta cần xem xét các lựa chọn triển khai cho các giải pháp sử dụng chuẩn 802.1x. Nếu việc triển khai phù hợp với doanh nghiệp thì chi phí quản lý ứng dụng này và chi phí máy chủ RADIUS sẽ là bao nhiêu?

Các doanh nghiệp muốn cải thiện tính bảo mật của hệ thống WLAN của họ, nhưng sử dụng tiêu chuẩn 802.1x - do đó, nên chọn triển khai RADIUS.

Deploy WPA with Preshared Keys: Nâng cấp hệ thống WLAN hiện có từ Quyền riêng tư tương đương có dây (WEP) lên Truy cập được bảo vệ bằng Wi-Fi

(WPA) mà không sử dụng RADIUS nhưng sử dụng khóa chia sẻ trước (PSK) hỗ trợ tiêu chuẩn 802.1x. Khóa chia sẻ trước không thể xác thực từng người dùng, và do nhiều vấn đề bảo mật nên khả năng chống lại "tấn công từ điển" rất kém. Nếu sử dụng giải pháp này, việc kinh doanh sẽ gặp nhiều rủi ro hơn và chỉ phù hợp với môi trường nhỏ nên giải pháp WPA-PSK là hợp lý.

Use Microsoft's RADIUS Server: Nếu có một máy chủ chạy Microsoft Windows Server 2008/2012/2016, có thể sử dụng Dịch vụ xác thực Internet (IAS) của Microsoft. Khi làm việc trên môi trường Windows thì IAS cần thiết cho các nhà quản trị hay các user. Đây cũng là một trong những tính năng nâng cao của Microsoft Wireless Provisioning Service.

Install an Open Source RADIUS Server: Nếu có phiên bản Windows, một tùy chọn khác là sử dụng giải pháp phần mềm nguồn mở, có thể tìm thấy trên trang web sau: http://www.freeRADIUS.org. Bằng cách hỗ trợ 802.1x, Linux, Free hoặc OpenBSD, OSF / Unix hoặc Solaris và các hệ điều hành mã nguồn mở khác đều có thể được sử dụng làm máy chủ RADIUS.

Mua một Commercial RADIUS Server: Đối với các giải pháp chuyên nghiệp cần hỗ trợ đầy đủ tất cả các chức năng, bảo mật và ổn định, bạn có thể mua các phiên bản thương mại có chức năng từ các nhà sản xuất khác để hỗ trợ 802.1x, đây là một máy chủ RADIUS chuyên nghiệp:

- Ruckus Network - https://www.commscope.com/
- LeapPoint AiroPoint Appliance - http://www.leappoint.com/
- Meetinghouse AEGIS - http://www.mtghouse.com/
- OSC Radiator - http://www.open.com.au/radiator/
- Aradial WiFi - http://www.aradial.com
- Bridgewater Wi-Fi AAA - http://www.bridgewatersystems.com
- Cisco Secure Access Control Server - http://www.cisco.com/

2.4 – Kết luận chương 2

Bảo mật WLAN tương tự như bảo mật của các mạng khác. Bảo mật hệ thống phải được áp dụng cho nhiều lớp và thiết bị phát hiện tấn công phải được triển khai.

Hạn chế quyền truy cập tối thiểu của người dùng cơ bản. Dữ liệu đã được chia sẻ và yêu cầu xác thực mới để truy cập nó. Dữ liệu được truyền phải được mã hóa.

Trên đây là một số kỹ thuật và phương pháp phòng chống tấn công mạng WLAN. Phòng thủ tấn công là tương đối quan trọng và không thể phòng thủ hoàn toàn trước tất cả các loại tấn công.

Xác thực Wi-Fi bằng máy chủ Radius là một trong những công nghệ tiên tiến nhất hiện nay, là phương pháp bảo mật hiệu quả nhất dựa trên chuẩn 802.1x, được tối ưu hóa cao và được sử dụng rộng rãi ở nước ta cũng như nhiều nước khác trên thế giới. Tuy nhiên, chi phí lựa chọn máy chủ xác thực người dùng cũng cần được cân nhắc kỹ lưỡng để tránh thất thoát, lãng phí cho đơn vị và doanh nghiệp.

CHƯƠNG III - BẢO MẬT CHO MẠNG WLAN CỦA TRƯỜNG ĐẠI HỌC HÀ NỘI BẰNG CHỨNG THỰC RADIUS SERVER

Chương 3 của luận văn sẽ nghiên cứu đề xuất một giải pháp bảo mật phù hợp cho mạng WLAN tại trường Đại học Hà Nội.

3.1 Khảo sát mạng WLAN Đại Học Hà Nội (sau khi đã xin phép và được sự đồng ý từ lãnh đạo nhà trường)

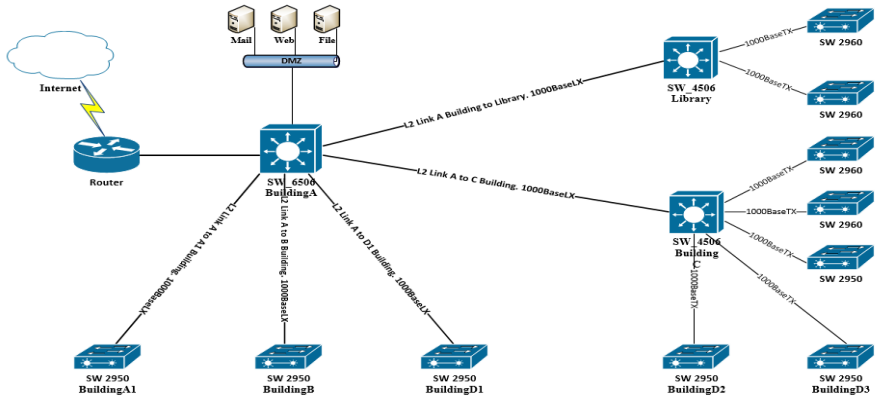
3.1.1 Mô hình kiến trúc, các chức năng và trang thiết bị mạng hiện có trong hệ thống mạng trường Đại học Hà nội

Trường Đại học Hà Nội có một môi trường sư phạm, môi trường văn hoá lành mạnh, cảnh quan xanh, sạch, đẹp, trường nằm trên trục giao thông chính vào trung tâm thành phố Hà Nội. Nhà trường có quần thể kiến trúc và không gian hiện đại và tiện ích, các khu hành chính, giảng đường, thư viện, ký túc xá... tất cả được bố trí trên diện tích tổng thể khoảng 8 ha.

- Tổng thể khuôn viên nhà trường:

Hình 3. 1 Khuôn viên trường Đại học Hà Nội

- Mô hình mạng nội bộ của trường Đại học Hà Nội:



Hình 3. 2 Mô hình hoạt động mạng nội bộ của trường Đại học Hà Nội

Hệ thống mạng máy tính tại trường Đại học Hà nội được xây dựng theo mô hình client server, đồng thời với kiến trúc mạng hình sao ở các tầng, ta sẽ đạt được tốc độ nhanh nhất có thể và kiểm soát tốt khi xảy ra lỗi cũng như mở rộng tùy ý muốn. Hiện nay tại trường Đại học Hà nội đang sử dụng 3 máy chủ đặt tại 3 trung tâm là Nhà A, Nhà C, Thư viện của trường và 1100 máy trạm. Tại khu vực mạng nội bộ, ở mỗi tòa nhà trong trường Đại học Hà Nội đều có các Switch được kết nối thẳng tới Switch tổng để đi ra ngoài mạng cũng như đi vào khu vực máy chủ nội bộ, các máy chủ được kết nối với nhau thông qua switch Cisco 48 port đường 1000Base LX và 1000 Base TX, các máy trạm kết nối với máy chủ thông qua các Switch Cisco 24 port.

Toàn bộ các máy tính trong trường đều được kết nối internet thông qua các máy chủ đặt tại nhà A, nhà C, và Thư viện các máy chủ này chạy hệ điều hành windown 2008 Server, hệ điều hành Linux…. Các máy chủ nội bộ có chức năng chứa dịch vụ của nhà trường: Mail, Web, File, cung cấp DHCP cho các máy trạm theo các Vlan đã định quản lý việc truy cập internet của các máy trạm.

Máy chủ kết nối ra internet thông qua các modem cáp quang tốc độ cao của các nhà cung cấp dịch vụ internet như: FPT, VIETEL VDC, VNPT, CNC…. Khoảng cách từ máy chủ của từng cơ sở tới máy xa nhất là 100m.

Một số Switch được sử dụng tại trường Đại học Hà nội: Switch Cisco 6506, Switch Cisco 4506, Catalyst 2950, Catalyst 2960….

3.1.2. Ứng dụng mạng máy tính trong trường Đại học Hà nội.

- Tra cứu tài liệu phục vụ công việc học tập của sinh viên và công việc của cán bộ trong toàn trường.

- Sinh viên có thể theo dõi thông tin và tình hình học tập của mình trong thời gian học tại trường thông qua cổng thông tin của nhà trường (http://hanu.edu.vn).

- Việc trao đổi thông tin trong toàn trường dễ dàng hơn, khi có những thông báo, quyết định mới đều được phổ cập cho toàn bộ CB trong toàn trường thông qua trang tác nghiệp của trường (http://tacnghiep.hanu.vn)

3.1.3 Nhu cầu sử dụng mạng WLAN từ thực tiễn

Theo Chương trình hành động và nội dung công tác của Đảng bộ Trường Đại học Hà Nội nhiệm kỳ 2020 – 2025 số 01-CTr/ĐU đưa ra ngày 04/09/2020 có nội dung trọng tâm nêu về vấn đề công tác cơ sở vật chất như sau: "Đầu tư nâng cấp hạ tầng, trang thiết bị công nghệ thông tin, mở rộng vùng phủ sóng WIFI để kết nối thông suốt, thuận tiện, hiệu quả trong quản lý, điều hành, cũng như thực hiện các hoạt động đào tào, nghiên cứu, chuyển giao tri thức. Đảm bảo các giải pháp an toàn thông tin và an ninh mạng cho các hệ thống công nghệ thông tin của Trường".

- Mặc dù hệ thống mạng LAN đã tương đối đáp ứng được nhu cầu làm việc, giảng dạy của cán bộ và giảng viên trong toàn trường. Nhưng đây thời kỳ IoT (Internet of Things) nên chỉ dùng mạng LAN là chưa đủ phục vụ cho mọi đối tượng người dùng hiện nay. Nhu cầu sử dụng Internet là rất lớn, ngoài máy tính để bàn cần kết nối Internet còn cả trên Laptop, Ipad, Smart phone.... cần kết nối mạng ở mọi lúc mọi nơi trong khuôn viên nhà Trường để phục vụ học tập, làm việc và giải trí ngày càng nhiều, đòi hỏi Hệ thống phải luôn kết nối được Internet và phải ổn định, an toàn.

- Khi bùng phát dịch COVID - 19 đợt đầu năm lan ra toàn xã hội, yêu cầu giãn cách xã hội để tránh lây nhiễm bệnh, nhu cầu sử dụng mạng WLAN ở cả phòng ban, giảng đường và khu ký túc xá phục vụ cho việc làm việc, giảng dạy và học tập Online của cán bộ, giảng viên và sinh viên ngày càng cao.

- Khả năng cung ứng cao, đáp ứng được một lượng lớn kết nối vào trong hay ra ngoài mạng mà vẫn giữ được sự ổn định, an toàn là một yêu cầu bắt buộc.

- Có khả năng nâng cấp và cải tạo trong tương lai.

3.1.4 Hiện trạng các vấn đề liên quan đến bảo mật trong quá trình sử dụng thiết bị phát WLAN tại trường Đại học Hà Nội

Thực trạng:

- Các đơn vị trong trường (phòng ban, khoa) muốn sử dụng wifi cho mục đích của cán bộ đơn vị mình thì yêu cầu bên TT công nghệ thông tin lắp thêm thiết bị AP phát wifi riêng cho từng phòng ban (hoặc khoa). Các thiết bị này được cài đặt có thể là đặt mật khẩu bảo vệ riêng của đơn vị mình theo kiểu WPA/WPA2 personal (theo khuyến cáo của nhà sản xuất) hoặc thiết bị không đặt mật khẩu bảo vệ để thuận tiện cho việc truy cập vào mạng của người dùng, sau đó thiết bị được cắm vào đường mạng LAN nội bộ của trường.

Nguy cơ: Mất an toàn cho cả người dùng và cơ sở dữ liệu của nhà trường là rất lớn.

- Khi Wi-Fi không dùng mật khẩu để bảo vệ: Thiết bị truyền tải dữ liệu hoàn toàn mở và có thể bị lợi dụng, điểm phát không an toàn và nguy hiểm đối với dữ liệu cá nhân người dùng. Điều này có nghĩa rằng mọi lưu lượng được chuyển tải từ những mạng này, bao gồm tin nhắn, mật khẩu, văn bản,…đều có thể bị những kẻ xấu lợi dụng.

- Khi đặt chế độ bảo mật là WPA/WPA2 Personal: Chức năng thay đổi khóa TKIP được sử dụng để tạo khóa mã hóa được phát hiện, nếu một tin tặc có thể đoán khóa khởi tạo hoặc một phần của mật khẩu, họ có thể xác định toàn bộ mật khẩu và do đó có thể giải mã dữ liệu.

Nỗ lực để hack những mạng này tùy thuộc vào cài đặt bao gồm độ mạnh của mật khẩu. Ví dụ, nếu mật khẩu yếu hoặc dễ đoán được (ví dụ như mật khẩu thường hay đặt một dãy số liên tiếp hay một dãy số lặp) thì tội phạm sẽ dễ dàng giải mã và bất kì thông tin nào được chuyển tải trên mạng này cũng đều không còn an toàn.

Như vậy biện pháp sử dụng Wifi hiện tại của các đơn vị trong trường (có mật khẩu và không có mật khẩu) đều mất an toàn rất cao: Đối tượng tấn công có thể nghe lén, giải mã giao thức mã hóa và đọc được nội dung của các gói tin mà trước đây

được cho là an toàn. Dẫn đến, các thông tin cá nhân, thông tin nhạy cảm như tài khoản ngân hàng, thẻ tín dụng, tài khoản mạng xã hội, thông tin riêng, nội dung chat, thư điện tử, hình ảnh, video…của người dùng có thể bị đánh cắp nếu được truyền qua mạng không dây.

Vì những lý do trên, xây dựng hệ thống bảo mật mạng WLAN trường là hết sức cần thiết để bảo vệ người dùng mạng không dây và cơ sở dữ liệu của nhà trường.

3.2 Đề xuất các giải pháp bảo mật cho mạng WLAN tại trường Đại học Hà Nội

3.2.1 Các giải pháp bảo mật mạng WLAN hiện có tại Hanu

Sử dụng mạng không dây wifi là xu hướng của nhiều phòng ban và khoa hiện nay tại HANU để phục vụ nhu cầu công việc. Tuy nhiên, xu hướng này cũng tiềm ẩn rất nhiều nguy cơ về tính bảo mật thông tin. Để nâng cao tính bảo mật cho tình hình sử dụng WLAN với cơ sở vật chất hiện tại của trường, có thể sử dụng các giải pháp sau để giúp cho việc truy cập internet bằng mạng không dây đảm bảo an toàn hơn.

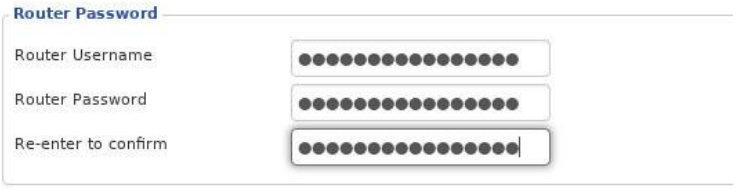
a. Thay đổi tên mạng (SSID):

Nên thay đổi tên mạng mặc định để tránh trường hợp kẻ tấn công biết được SSID mặc định. 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.

b. 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, không nên để mật khẩu quá đơn giản. Lời khuyên là hãy thay đổi tên người dùng và mật khẩu bằng một dãy ký tự khó đoán.

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 hơn.

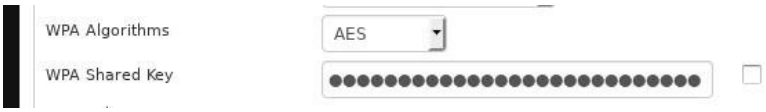


c. Sử dụng mã hóa mạnh để bảo mật wifi:

Khi dùng mạng wifi cần mã hóa. Nếu chưa dùng mã hóa cho mạng wifi thì những kẻ tấn công rất dễ hack wifi. Để mã hóa bảo mật wifi có thể chọn "WPA2 Personal" cho mạng. Đối với thuật toán mã hóa nên chọn AES và không nên dùng TKIP. Bởi AES sẽ cung cấp mã hóa mạnh khó tấn công hơn TKIP.

d. Chọn mật khẩu mạnh:

Cách bảo mật wifi đơn giản là nên áp dụng chọn mật khẩu mạnh cho wifi. 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.



e. Thay đổi mật khẩu wifi:

Dù mật khẩu 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 được bảo mật tuyệt đối.

f. Vô hiệu hóa mạng khách:

Vô hiệu hóa mạng khách cũng là cách bảo mật mạng không dây an toàn. Nếu 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 nên vô hiệu hóa

mạng khách bằng một dãy mật khẩu riêng. Và sau khi khách rời đi thì hãy thay đổi mật khẩu wifi.

g. Bật tường lửa để bảo mật wifi:

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

h. 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, hãy tắt WPS để đảm bảo an toàn tối đa cho mạng không dây.

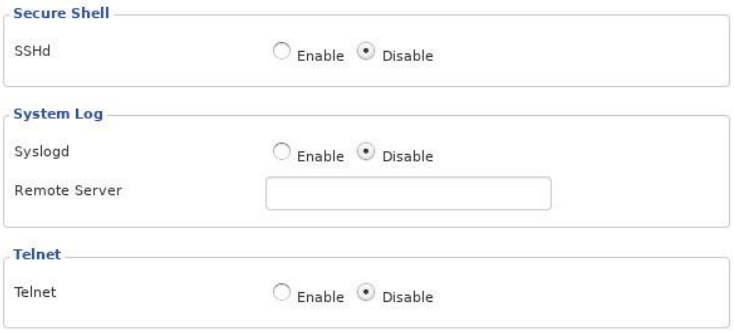
i. Quản lý firmware của bộ định tuyến:

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

k. 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 quản lý bộ định tuyến dễ dàng hơn. Nhưng nó cũng tiềm ẩn nhiều rủi ro và nguy hiểm cho

mạng không dây. 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. Do đó, để đảm bảo tính bảo mật wifi bạn nên tắt dịch vụ quản lý từ xa của bộ định tuyến.



Trên đây chính là các cách bảo mật WLAN cho mạng hiện tại của HANU. Trong số các cách này, nên chú ý tới cách mã hóa và đặt mật khẩu mạnh. Bởi đây chính là cách bảo mật mạng không dây đơn giản, an toàn và dễ thực hiện nhất.

3.2.2 Bảo mật mạng WLAN sử dụng chứng thực Radius Server tại Hanu

Xuất phát từ những lợi ích rất hữu ích như tính linh động, thuật tiện trong việc áp dụng mạng WLAN vào các nơi công cộng như công sở, trường học. Đặc biệt là trường Đại học Hà Nội với số lượng cán bộ, giảng viên khoảng 750 người, sinh viên nhà trường có khoảng 10.000 sinh viên các khóa, các sinh viên ở khu vực KTX có nhu cầu sử dụng mạng internet rất lớn. Học viên xin đề xuất áp dụng mô hình triển khai mạng WLAN với hình thức chứng thực RADIUS cho khu hành chính, giảng đường và ký túc xá trường với đối tượng sử dụng là cán bộ, giảng viên, và sinh viên của trường để quản lý tập trung và nâng cao tính báo mật cho người dùng và cơ sở dữ liệu của nhà trường.

Với đối tượng là Giảng viên, viên chức của trường, các dữ liệu truyền trong mạng cần có sự bảo mật trên đường truyền do đó sẽ tổ chức các đối tượng này vào các Group được phân quyền và áp dụng các chính sách thích hợp đáp ứng nhu cầu bảo mật dữ liệu truyền trên mạng cũng như vấn đề phân quyền.

Đối với đối tượng là Sinh viên, nhu cầu truy cập để sử dụng mạng internet là chính nên các đối tượng này sẽ được tổ chức vào các group thích hợp. Sinh viên có

nhu cầu sử dụng mạng WLAN sẽ được cấp user và password. Cấp cho các user này khoảng thời gian truy cập cũng như các vấn đề về kiểm soát, thu phí…vv.

Để quản lý tập trung dữ liệu và các dịch vụ, đồng thời đảm bảo an toàn thông tin cho hệ thống mạng WLAN, học viên đề xuất giải pháp như sau:

3.2.3 Giải pháp mạng

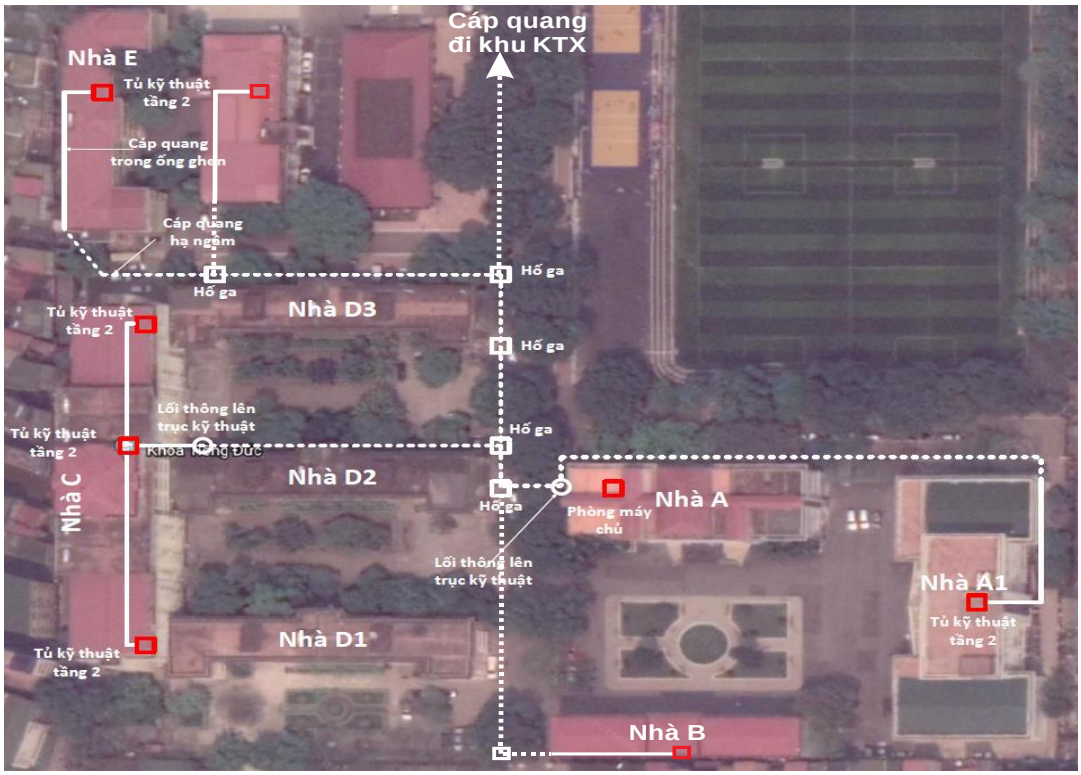
Xây dựng phòng máy chủ tập trung quản lý WLAN tại tầng 3 nhà A sử dụng chứng thực Radius Server để điều khiển và cấp quyền truy cập cho các user kết nối với các AP được lắp tại các khu làm việc, giảng đường và khu ký túc xá sinh viên cũng như khuôn viên nhà trường.

Để việc áp dụng giải pháp sử dụng Radius server được khả thi thì cần tính đến tính hiệu quả kinh tế phù hợp, ngoài các thiết bị ở phòng máy chủ, các switch chia cổng, đường cáp quang đi các tòa nhà,... là cần phải có, để giảm chi phí đầu tư các thiết bị Access Point lắp cho các phòng ban và giảng đường, thư viện,... học viên đề xuất cách phân bổ lắp thiết bị tại các tòa nhà như sau:

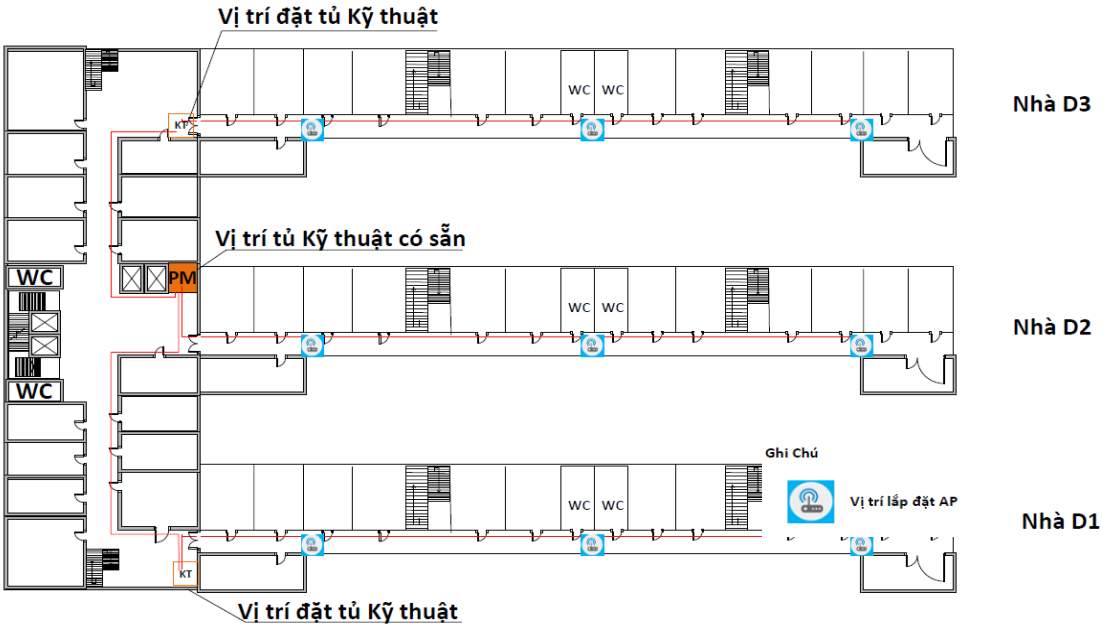
Nhà A là khu hành chính có các phòng ban lắp 3 hoặc 4 chiếc thiết bị phù hợp ngoài hành lang (riêng khu vực phòng máy chủ không lắp thiết bị phát wifi để đảm bảo tính bảo mật cơ sở dữ liệu của nhà trường) phục vụ cho cán bộ sử mạng WLAN (ví dụ có thể dùng TP-Link Archer C50 đáp ứng 20-25 người dùng).

Các tòa nhà giảng đường như nhà B, nhà A1, nhà C, nhà E, D1, D2, D3, thư viện thì trang bị lắp 3 hoặc 4 thiết bị Access Point ở ngoài hành lang các tầng, các thiết bị này có khả năng đáp ứng số lượng lớn người dùng (ví dụ như dùng Wifi Ruckus ZoneFlex AccessPoint 7372 có khả năng đáp ứng được 200 người dùng cùng lúc).

Các khu KTX sinh viên nhà D4, D5, D6, D7, D8, D9, D10: Các nhà này ban quản lý bố trí có 6-8 bạn sinh viên ở 1 phòng, nên sẽ trang bị các thiết bị Access Point rẻ tiền hơn (như TP-Link 840N) vào từng phòng phục vụ đủ nhu cầu số người dùng cho mỗi phòng.



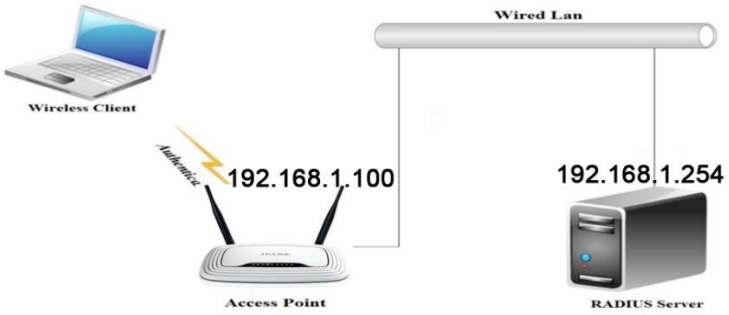
Hình 3. 3 Đường cáp quang từ nhà A đi đến các tòa nhà trong trường



Tầng 2 khu D

Hình 3. 4 Sơ đồ lắp thiết bị AP truy cập tại tầng 2 khu nhà D

3.2.4 Mô tả hệ thống (thử nghiệm)



Hình 3. 5 Hệ thống xác thực RADIUS cho mạng WLAN

Mô tả yêu cầu:

+ 1 Access TP-LINK (hoặc của các hãng khác có hỗ trợ WPA2-Enterprise).

+ 1 PC làm RADIUS server sử dụng hệ điều hành Windows Server 2012 R2 Data center có RAM tối thiểu là 2GB, tạo user và password cho các client dự định tham gia vào mạng.

+ 1 Laptop có card wireless sử dụng hệ điều hành Windows 7 dùng làm client.

+ Kết nối network giữa access point và Window server 2012 phải thông suốt, không bị chặn bởi firewall.

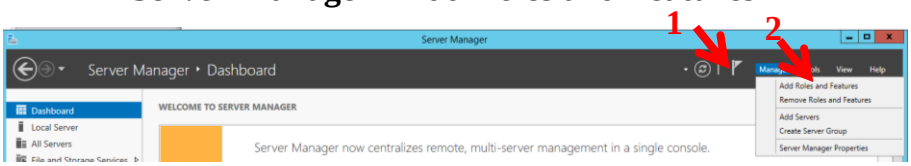
3.3 – Cài đặt

Server phải được đặt IP và trỏ Prefer DNS về chính nó (ở đây học viên đặt IP là 192.168.1.254/24) và đã được nâng cấp Active Director (AD) rồi.

3.3.1. Cài đặt + Cấu hình Active Directory Certificate Services (CA)

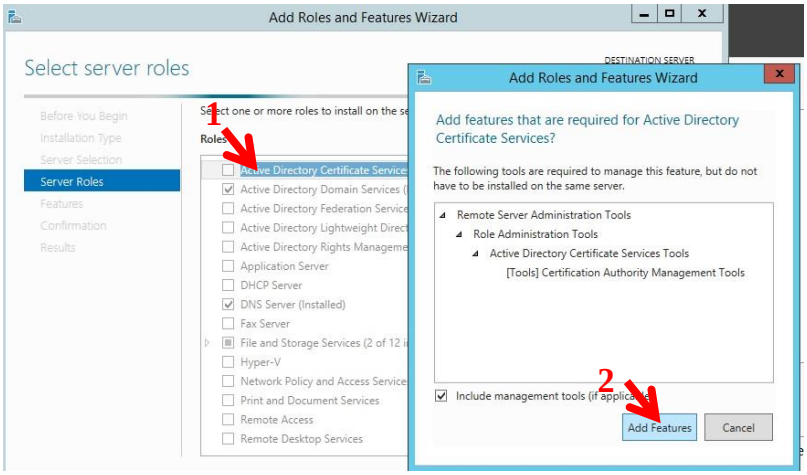
a. Cài đặt CA

– Đầu tiên vào **Server Manager> Add Roles and Features**



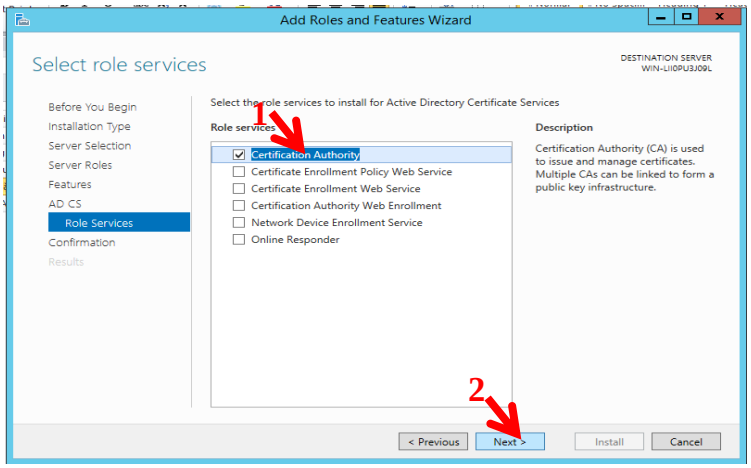
– Chọn **Active Directory Certificate Services**

– Hộp thoại Add Roles and Feature Wizard xuất hiện chọn **Add** và bấm **Next** để tiếp tục

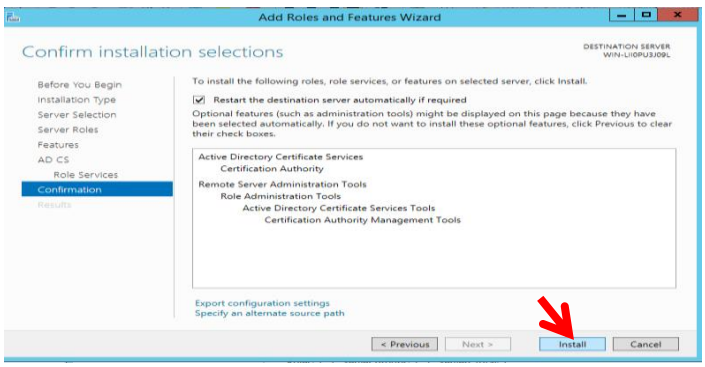


– Hộp thoại Active Directory Certificate Service xuất hiện Click **Next** để đến bước tiếp theo.

– Hộp thoại Select role service xuất hiện bạn tick vào **Certification Authority** và bấm **Next** để tiếp tục.



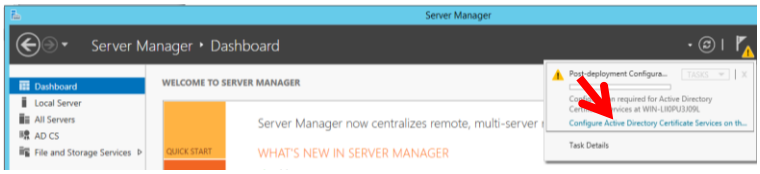
– Hộp thoại Confirm installation selections xuất hiện bấm Install.



– Sau khi install xong, bấm **Close** để hoàn tất bước cài đặt CA.

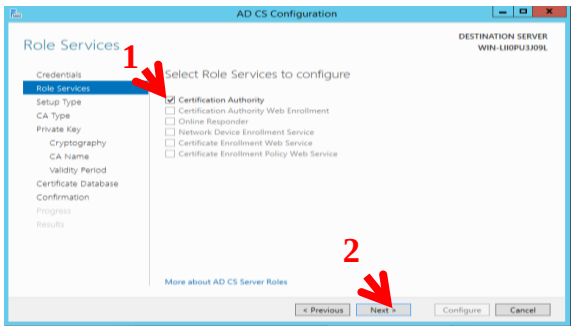
b. Cấu hình CA

– Sau khi cài đặt xong ở Server Manager sẽ thấy dấu chấm than bên góc trên bên tay phải, click vào dấu chấm than, Chọn **Configure Active Directory Certificate Server On th…**



– Hộp thoại Credentials xuất hiện chọn **Next**

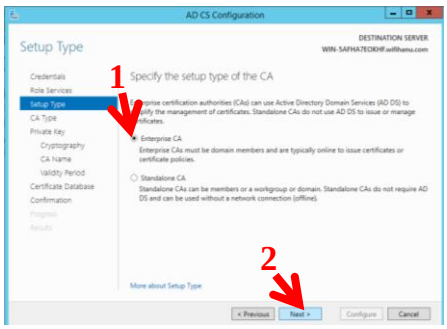
– Hộp thoại Roles Services xuất hiện, chọn **Certification Authority** và bấm **Next** để tiếp tục cấu hình.



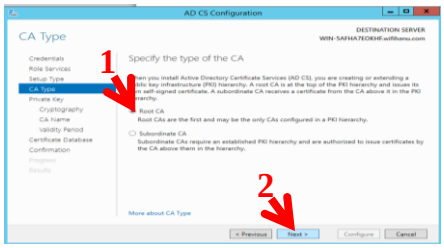
– Hộp thoại Setup Type hiện ra

+ Tick vào **Enterprise CA**

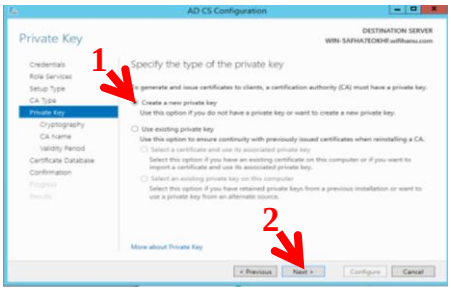
+ Click vào Next để tiếp tục



– Sau đó tick chọn **Root CA** và Click vào **Next** để đến bước tiếp



- Hộp thoại Private key xuất hiện chọn **Create a new private key** và Click vào **Next** để đến bước tiếp



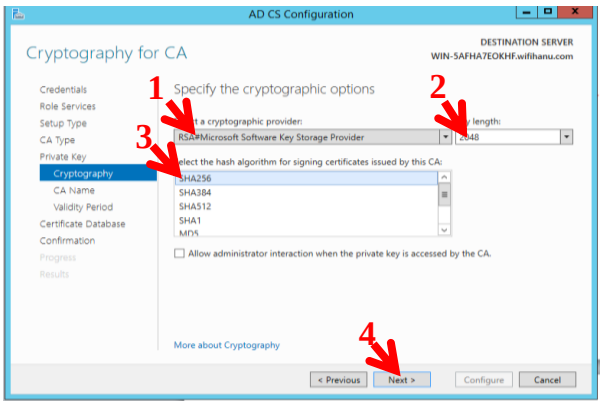
– Hộp thoại Cryptography xuất hiện

+ Select a cryptography provider: Chọn **RSA#Microsoft Software Key Storage Provider**

+ Key length: **2048**

+ Select the hash algrithm for signing certificates issued by this CA: Chọn **SHA256**

– Và Click vào **Next** để đến bước tiếp

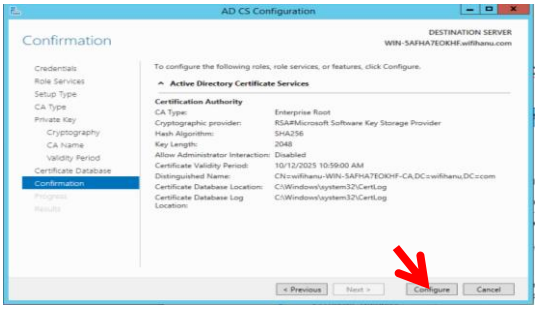


– Hộp thoại CA Name xuất hiện chọn **Next**.

– Hộp thoại Validity Period xuất hiện chọn **Next**.

– Hộp thoại Certificate Database xuất hiện Chọn **Next**.

– Hộp thoại Confirmation xuất hiện Chọn **Configure.**



– Hộp thoại Results xuất hiện chọn **Close**.

3.3.2. Cài đặt NAP và cấu hình NAP (Network Policy and Access Services)

a. Cài đặt NAP

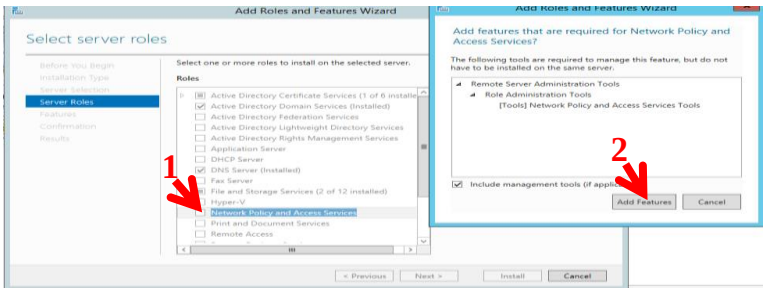
– Tiếp tục vào **Server Manager** -> **Add Roles and Features.**

– Hộp thoại Server Roles xuất hiện:

+ Tick chọn **Network Policy and Access Services.**

+ Hộp thoại Add Role And Feature Wizard xuất hiện chọn **Add Features**

– Click vào **Next** để đến bước tiếp.



– Hộp thoại Features xuất hiện chọn **Next** để tiếp tục.

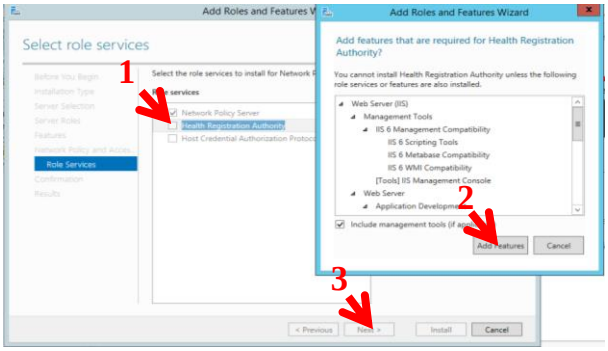
– Hộp thoại Network Policy and Access Serivices xuất hiện chọn **Next**.

– Hộp thoại Role Services xuất hiện:

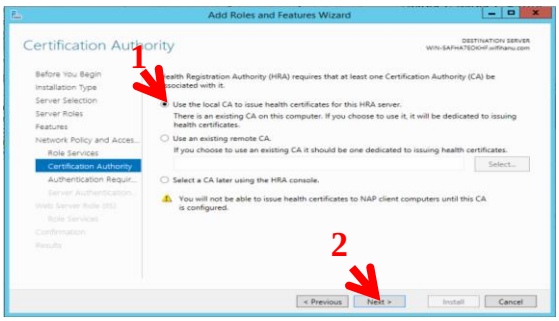
+ Tick chọn **Network Policy Server** và Tick chọn **Heath Registration Authority**

+ Hộp thoại Add Roles and Features Wizard xuất hiện chọn **Add Features**.

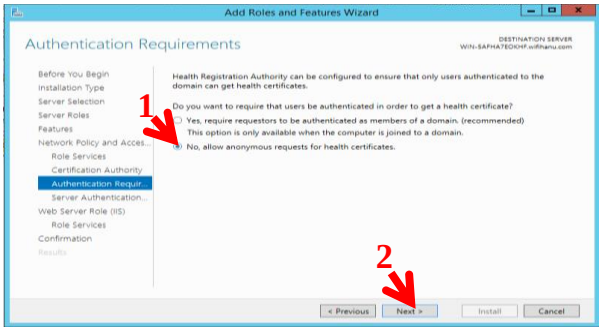
– Click vào **Next** để đến bước tiếp



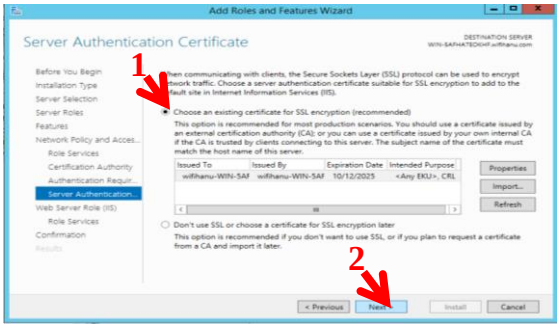
– Hộp thoại Certification Authority xuất hiện chọn: **Use the local CA to issue heath certificates for this HRA server** sau đó Click vào **Next** để đến bước tiếp.



– Hộp thoại Authentication Requirements xuất hiện chọn **No, allow anonymous requests for heath certificates**. và Click vào **Next** để đến bước tiếp.



– Hộp thoại Server Authentication Certificate xuất hiện chọn **Choose an existing certificate for SSL encryption (recommended)** và Click vào **Next** để đến bước tiếp.



– Hộp thoại **Web Server Role (IIS)** xuất hiện chọn **Next**.

– Hộp thoại Select role services xuất hiện chọn **Next.**

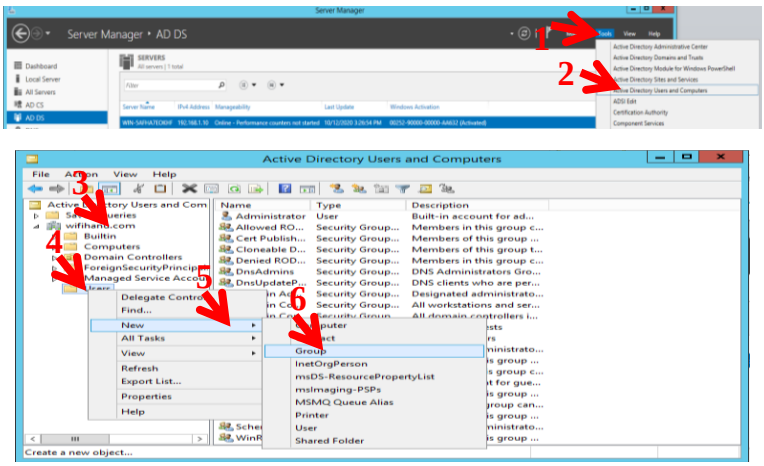
– Hộp thoại Confirm Installation Selections xuất hiện Chọn **Install**

– Sau khi tiến trình cài đặt kết thúc, bấm **Close** để hoàn tất việc cài đặt NAP.

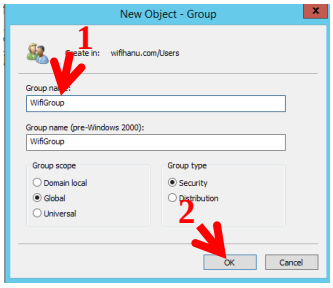
b. Cấu hình NAP

– Để apply NAP cho group user, tiến hành tạo user và add user đó vào group trước. NAP sẽ apply cho Group.

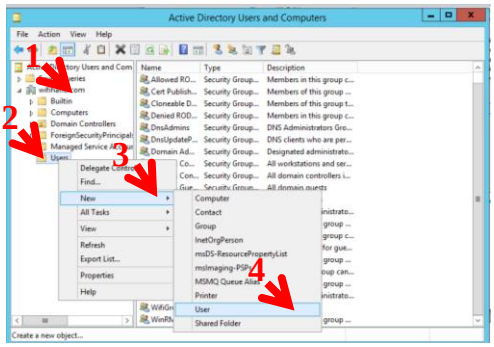
– Tạo GroupWifi: Kích tuần tự các bước từ 1 đến 6 để tạo Gruop



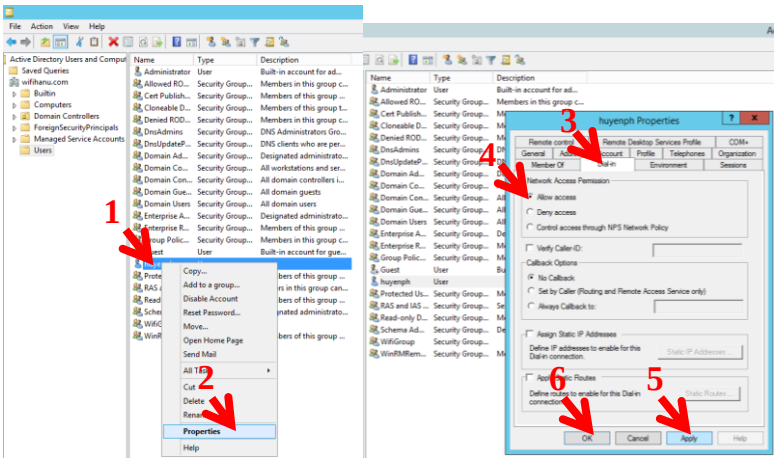
– Xuất hiện hộp thoại new object đặt tên cho Group: Đánh tên và Click **OK**



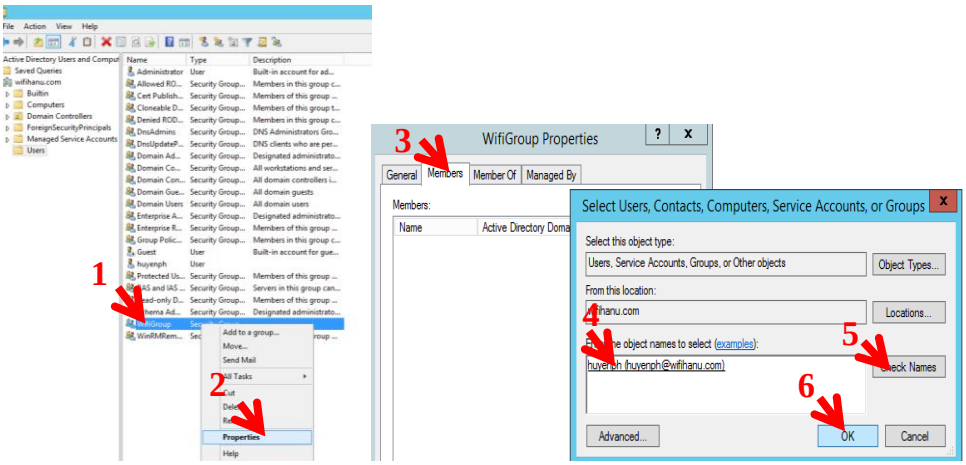
– Tạo user: Kích tuần tự các bước từ 1 đến 12 như hình sau để tạo user:

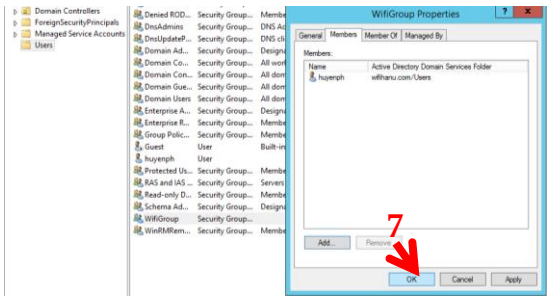


– Set tính chất user cho phép truy cập: Thực hiện tuần tự bước 1 đến 6 như sau



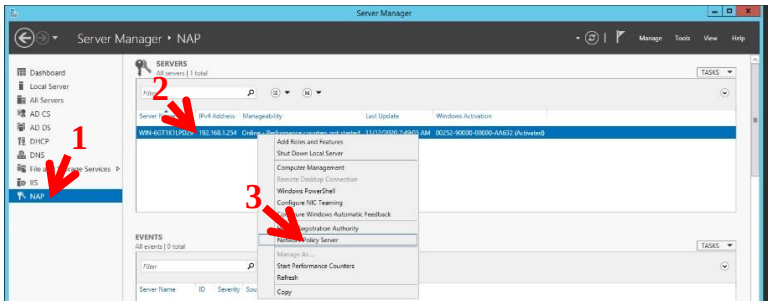
– Add User vào Group: Tuần tự thực hiện các bước từ 1-7 như sau:



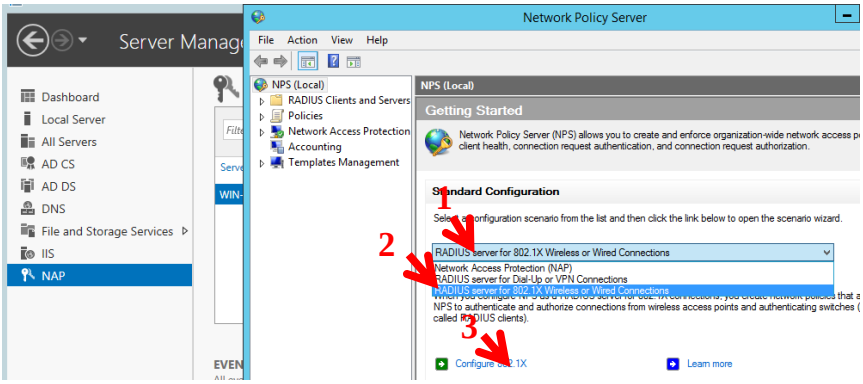


– Ở đây học viên đã tạo user: huyenph là thành viên của group WifiGroup, sau đây học viên sẽ apply NAP vào group này

– Tại Server Manager click chọn NAP, sau đó click chuột phải vào **AD 192.168.1.254 – Online – Performance…** Chọn **Network Policy Server** để vào cấu hình NAP.



- Hộp thoại Network Policy Server xuất hiện tại Standard Configuration xổ drop down list ra chọn **RADIUS server for 802.1X Wireless or Wired Connections**



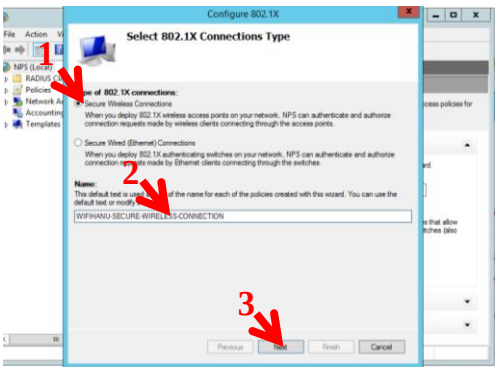
– Và Sau đó chọn **Configure 802.1X**

– Hộp thoại 802.1X Connections Type xuất hiện:

+ Type of 802.1X Connection: Tick chọn **Secure Wiresless Connections**

+ Name: Đặt tên cho Policy.

– Sau khi chọn và điền xong Click vào **Next** để đến bước tiếp.



– Hộp thoại Specify 802.1X Switches xuất hiện chọn Add để Add Radius client

(Lưu ý: Radius client ở đây chính là access point. Nếu có 1 access point thì add 1 cái, có 2 thì add 2, … nếu không add vào thì access point cho dù cố tình trỏ về RADIUS Server cũng không sử dụng được.)

– Sau khi click Add… hộp thoại New RADIUS Client xuất hiện, cần làm như sau:

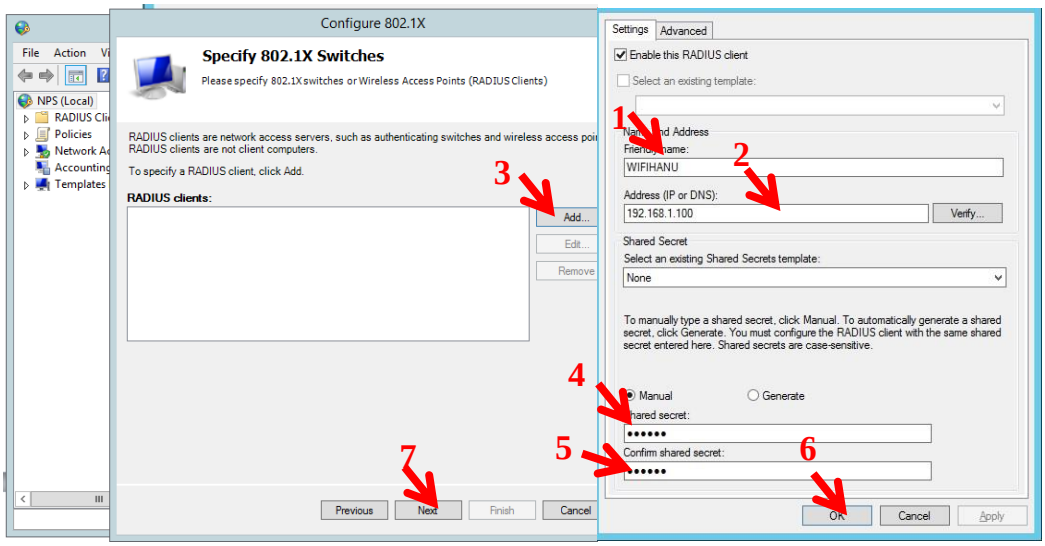
+ Friend Name: Đặt tên cho radius client (lời khuyên là nên đặt trùng với host name của thiết bị wireless sẽ add vào), ở đây học viên đặt tên là WIFIHANU

+ Address: Gõ địa chỉ IP của access point vào (ở đây là 192.168.1.100)

+ Tick vào Manual và gõ chuỗi Shared secret vào rồi confirm nó lại lần nữa. (Lưu ý chuỗi secret này dùng để xác thực giữa access point và Radius server, sẽ điền nó vào access point khi cấu hình ở phần sau)

+ Và bấm OK để hoàn tất việc Add RADIUS Client.

– Sau khi add RADIUS Client xong bấn **Next** để qua bước tiếp theo.



– Hộp thoại Configure an Authentication Method xuất hiện:

– Type xổ ra chọn **Microsoft: Protected EAP(PEAP)**

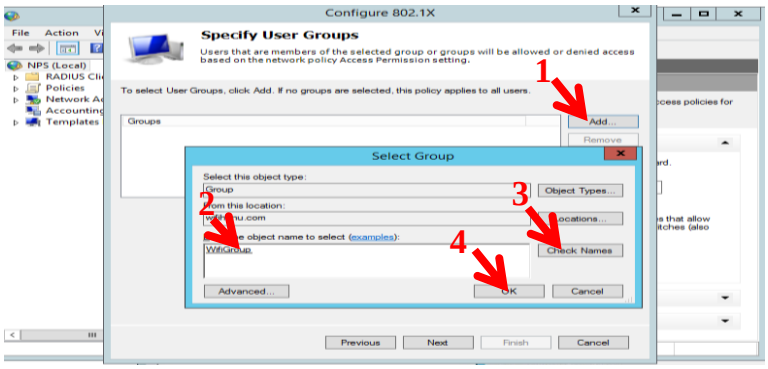
– Sau đó click vào **Configure**.

+ Hộp thoại Edit Protected EAP Properties xuất hiện thấy ở Eap Types dòng **Secured password (EAP-MSCHAP v2)** bấm **OK**

– Hộp thoại Specify User Groups xuất hiện bấn vào Add… để Add group cho phép sử dụng 802.1X chứng thực wifi (ở đây học viên đã tạo sẵn group tên là WifiGroup và add account huyenph vào rồi).

– Sau khi click vào **Add…** chọn gõ tên Group và bấm ok.

– Và Click vào **Next** để đến bước tiếp.



– Hộp thoại Configure Traffic Controls xuất hiện Click vào **Next** để đến bước tiếp.

– Hộp thoại Completing New 802.1X Secure Wired and Wireless Connections and RADIUS clients xuất hiện chọn Finish để hoàn tất.

3.3.3 Cấu hình trên access point và client

a. Cấu hình trên access point:

– Trường hợp access point hỗ trợ DHCP thì có thể tận dụng, trong trường hợp access point không hỗ trợ thì phải setup DHCP Server để cấp IP cho wifi (trong Lab này học viên tắt chức năng cấp DHCP trên AP và đã cấu hình để Window Server cấp DHCP dải từ 192.168.1.150/24 - 192.168.1.180/24 để cấp IP cho Wifi client).

Tại Access Point:

– Truy cập vào access point TP-LINK để cấu hình theo địa chỉ: 192.168.1.1

– Sau khi đăng nhập vào giao diện quản lý wifi, đặt tên cho SSID (ở đây học viên đặt tên là **WIFIHANU** có địa chỉ IP là **192.168.1.100**) rồi bấm phần Security để cấu hình chế độ bảo mật cho AP.

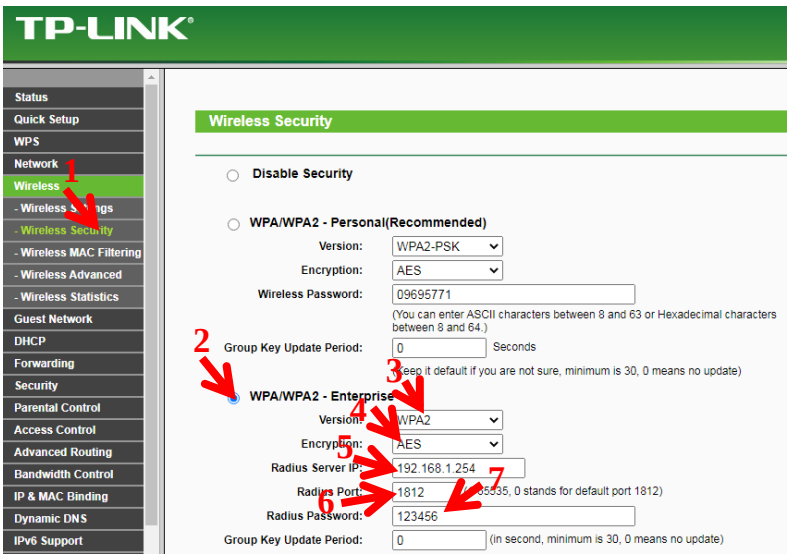
– Tại phần Security phần Wireless Security mode chọn **WPA/WPA2-Enterprise** (chọn Version là **WPA**2 và Encryption là **AES**)

+ Primary RADIUS Server trỏ về RADIUS server (192.168.1.254)

+ Primary RADIUS Server port: **1812**

+ Primary Shared Secret: Gõ chuỗi Secret đã đăng ký trên RADIUS Server.

+ Thực hiện các bước từ 1 đến 7 theo hình dưới đây



– Sau đó bấm Save rồi ấn Apply để hoàn tất phần cấu hình trên Access Point.

b. Cài đặt trên máy Client:

– Tại Client (Máy Laptop chạy Window 7) sẽ thấy chưa có SSID nào được đăng ký trong phần Manage Wireless Networks. (Lưu ý: Cần phải Add SSID cho nó, nếu không wifi sẽ không sử dụng được).

- Tại phần Manage Wireless Networks chọn Add để add SSID vào – Hộp thoại Manual connect to a wireless network, click vào **Manual create a network profile.**

– Ở bước này:

+ Gõ SSID đã đặt trên access point tại Network Name.

+ Security type: Chọn WPA2-Enterpise hoặc WPA2-Enterpise Mix

+ Tick vào Start this connection automatically

+ Và bấm Next để qua bước tiếp theo.

– Sau khi cấu hình xong chọn **Change connection settings** để tùy chỉnh lại.

– Tại phần tùy chỉnh tại tab security làm như sau:

+ Security type: Chọn **WPA2-Enterprise**

+ Encryption type: Chọn **AES**

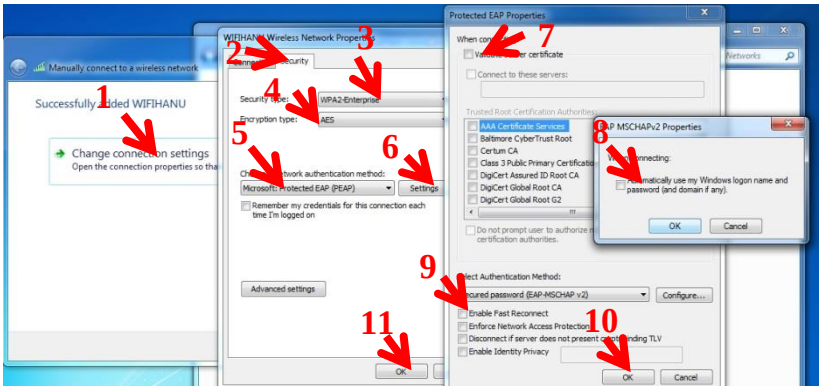
+ Choose a network authentication method: Chọn **Microsoft: Protected EAP (PEAP)**

+ Sau đó chọn Setting, và hộp thoại Protected EAP Properties xuất hiện làm như sau:

- Tick bỏ Validate server certificate…
- Click Configure và bỏ chọn **Automatically use my Windows login name and password**
- Bỏ Tick chọn **Enable Fast Reconnect**
- Bấm OK để hoàn tất ở hộp thoại Protected EAP Properties

+ Cuối cùng bấm OK tại hộp thoại Wireless Network Properties để hoàn tất bước add SSID tại client.

+ Thực hiện các bước từ 1 đến 11 theo hình dưới đây

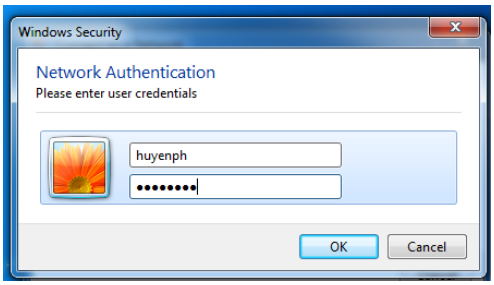


3.4 Thử nghiệm và đánh giá kết quả

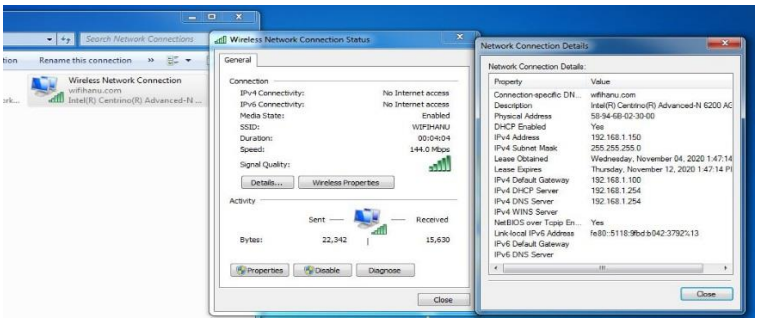
3.4.1 Thử nghiệm

– Trên Laptop chọn sóng Wireless có SSID là **WIFIHANU** gõ username/password (đã set trên AD nằm trong OU Wifi) và bấm OK

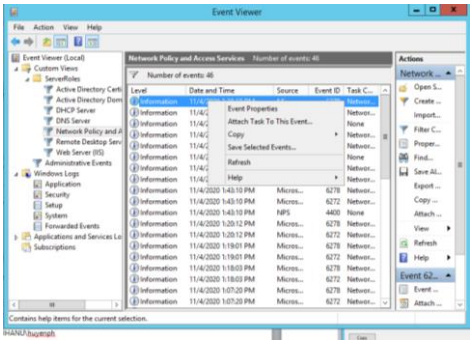
– Máy báo đã kết nối wifi SSID **WIFIHANU** thành công.

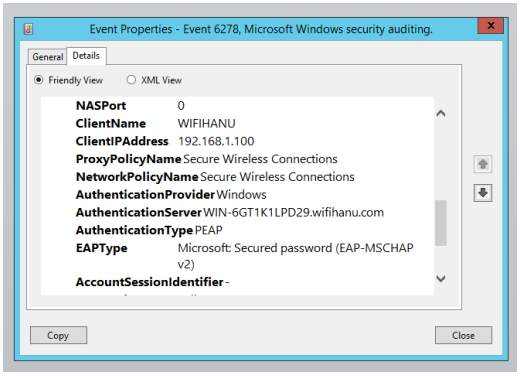


- Kết quả kết nối được thể hiện ở các thông số được cấp bởi DHCP server như IP, DNS server, Default Gateway…



- Trên RADIUS Server, vào Tools ➔ Event Viewer ➔ Tick như hình dưới, sẽ cho thấy kết quả như sau:





+ **System**
  - **Provider**
    [**Name**] Microsoft-Windows-Security-Auditing
    [**Guid**] {54849625-5478-4994-A5BA-3E3B0328C30D}
  EventID 6278
  Version 0
  Level 0
  Task 12552
  Opcode 0
  Keywords 0x8020000000000000
  - **TimeCreated**
    [**SystemTime**] 2020-11-04T21:47:00.694761500Z
  EventRecordID 5649
  Correlation
  - **Execution**
    [**ProcessID**] 520
    [**ThreadID**] 2396
  Channel Security
  Computer WIN-6GT1K1LPD29.wifihanu.com
  Security

- **EventData**

SubjectUserSid	S-1-5-21-2538448755-2924557009-2248267489-1106
SubjectUserName	huyenph
SubjectDomainName	WIFIHANU
FullyQualifiedSubjectUserName	WIFIHANU\huyenph
SubjectMachineSID	S-1-0-0
SubjectMachineName	-
FullyQualifiedSubjectMachineName	-
MachineInventory	-
CalledStationID	F4-F2-6D-53-9E-FC:WIFIHANU
CallingStationID	58-94-6B-02-30-00
NASIPv4Address	192.168.1.100
NASIPv6Address	-
NASIdentifier	-
NASPortType	Wireless - IEEE 802.11
NASPort	0
ClientName	WIFIHANU
ClientIPAddress	192.168.1.100
ProxyPolicyName	Secure Wireless Connections
NetworkPolicyName	Secure Wireless Connections
AuthenticationProvider	Windows
AuthenticationServer	WIN-6GT1K1LPD29.wifihanu.com
AuthenticationType	PEAP
EAPType	Microsoft: Secured password (EAP-MSCHAP v2)
AccountSessionIdentifier	-
QuarantineState	Full Access
ExtendedQuarantineState	-
QuarantineSessionID	-
QuarantineHelpURL	-
QuarantineSystemHealthResult	-

Chi tiết file log như sau:

Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Date: 11/4/2020 1:47:00 PM
Event ID: 6278
Task Category: Network Policy Server
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN-6GT1K1LPD29.wifihanu.com
Description:
Network Policy Server granted full access to a user because the host met the defined health policy.

User:
Security ID: WIFIHANU\huyenph

Account Name:	huyenph
Account Domain:	WIFIHANU
Fully Qualified Account Name:	WIFIHANU\huyenph

Client Machine:

Security ID:	NULL SID
Account Name:	-
Fully Qualified Account Name:	-
OS-Version:	-
Called Station Identifier:	F4-F2-6D-53-9E-FC:WIFIHANU
Calling Station Identifier:	58-94-6B-02-30-00

NAS:

NAS IPv4 Address:	192.168.1.100
NAS IPv6 Address:	-
NAS Identifier:	-
NAS Port-Type:	Wireless - IEEE 802.11
NAS Port:	0

RADIUS Client:

Client Friendly Name:	WIFIHANU
Client IP Address:	192.168.1.100

Authentication Details:

Connection Request Policy Name:	Secure Wireless Connections
Network Policy Name:	Secure Wireless Connections
Authentication Provider:	Windows
Authentication Server:	WIN-6GT1K1LPD29.wifihanu.com
Authentication Type:	PEAP
EAP Type:	Microsoft: Secured password (EAP-MSCHAP v2)
Account Session Identifier:	-

Quarantine Information:

Result:	Full Access
Extended-Result:	-
Session Identifier:	-
Help URL:	-
System Health Validator Result(s):	

3.4.2 Đánh giá kết quả:

Khi bảo mật bằng phương pháp Radius server có sự khác biệt đáng kể với bảo mật khi sử dụng phương pháp khác là là ở hình thức có được khóa PMK (Pair-wise Master Key): Như với chế độ bảo mật WPA/WPA2 Personal, khóa PMK sinh ra từ khóa tĩnh được nhập vào thủ công trên AP và các Station. Còn sử dụng WPA/WPA2 Enterprise trong phương pháp Radius server, khóa PMK nhận được từ quá trình xác thực IEEE 802.1x/EAP. Việc cấp phát khóa này là hoàn toàn tự động và tương đối an toàn. Sau khi đã xác thực lẫn nhau rồi, station và máy chủ xác thực Radius xây dựng khóa PMK dựa trên các thông tin đã biết. Khóa này là giống nhau trên cả station và máy chủ xác thực Radius. Máy chủ xác thực Radius sẽ tiến hành sao chép một bản

khóa PMK này rồi gửi về cho AP. Lúc này, cả AP và Station đều đã nhận được khóa PMK phù hợp và cho phép kết nối mạng. Bởi vậy, phương pháp Radius server sẽ an toàn hơn và thích hợp với triển khai hệ thống ở qui mô lớn như trường học, công ty.

Các máy client muốn vào được mạng wifi phải tiến hành cài đặt, phải được xác thực dựa vào thông tin cung cấp từ máy chủ Radius server. Điều này dẫn tới việc bảo mật cao hơn và an toàn hơn so với các hình thức bảo mật thông thường. Vì vậy sẽ bảo vệ người dùng tránh mất mát dữ liệu và các nguy cơ tấn công của các hacker xâm nhập.

3.5 Kết luận chương 3

Chương 3 của luận văn đã khảo sát mạng có dây và không dây tại trường Đại học Hà Nội, các vấn đề nảy sinh trong quá trình sử dụng và các yêu cầu bảo mật mạng nhằm đáp ứng nhu cầu đào tạo của nhà trường.

Luận văn cũng đề xuất một giải pháp bảo mật cho mạng WLAN của trường Đại học Hà Nội là phương pháp bảo mật dùng RADIUS SERVER. Kết quả thử nghiệm cho thấy giải pháp bảo mật được đề xuất có thể được triển khai trên thực tế và phù hợp với yêu cầu đề ra.

KẾT LUẬN

Ngày nay, mạng không dây đã trở nên thiết thực trong cuộc sống, giúp người dùng có thể kết nối mạng ở mọi lúc, mọi nơi trong phạm vi phủ sóng của thiết bị, đáp ứng nhu cầu học tập, làm việc và giải trí của con người.

Đi đôi với tính tiện lợi, độ mất an toàn của mạng không dây cũng xuất hiện đồng thời tạo kẻ hở cho các Hacker xâm nhập lấy cắp thông tin, dữ liệu bằng các phương pháp khác nhau, đòi hỏi cần có sự phát triển các giải pháp bảo mật để cung cấp cho người dùng thông tin hiệu quả và đáng tin cậy.

Các chuẩn mạng và các phương pháp bảo mật mạng không dây được phát triển qua từng thời kỳ đáp ứng nhu cầu phát triển của kỹ thuật cũng như từ thực tế sử dụng. Hầu hết các thế hệ sau đều cải tiến công nghệ và khắc phục những hạn chế của thế hệ trước đó về tốc độ cũng như về bảo mật để nhằm mục đích phục vụ nhu cầu người dùng đạt hiệu quả tốt nhất có thể.

Trong các phương pháp bảo mật mạng không dây thì phương pháp bảo mật dùng máy chủ RADIUS được xem là hiệu quả tốt nhất ở thời điểm hiện nay. RADIUS cho phép xác thực tập trung, ủy quyền và kiểm tra quyền truy cập cho mạng nên mang đến cho người dùng độ an toàn bảo mật rất cao.

Với mục tiêu nghiên cứu giải pháp bảo mật cho mạng WLAN ứng dụng tại Trường Đại học Hà nội, luận văn đã đạt được một số kết quả sau đây:

- Nghiên cứu các yêu cầu bảo mật cho mạng WLAN.
- Nghiên cứu các giải pháp bảo mật cho mạng WLAN.
- Đề xuất các giải pháp bảo mật có thể triển khai cho mạng nội bộ tại Trường Đại học Hà nội: Sử dụng phương pháp RADIUS xác thực cho các user khi kết nối vào mạng WLAN. Luận văn này học viên đã giới thiệu chi tiết cách cài đặt và kết quả chạy thử nghiệm khi sử dụng RADIUS trên nền Windows Server 2012.

Hướng phát triển tiếp theo của luận văn:

- Tìm hiểu các yêu cầu, mô hình khi thiết kế, triển khai và bảo mật hệ thống Server RADIUS trong thực tế.

- Tìm hiểu, xây dựng hệ thống phát hiện xâm nhập cho mạng WLAN và thực hiện tấn công trên hệ thống này.

DANH MỤC CÁC TÀI LIỆU THAM KHẢO

[1] Lê Tấn Liên, Minh Quân (2009), *Hacking wireless - kỹ thuật thâm nhập mạng không dây*, Nhà xuất bản Hồng Đức.

[2] Nguyễn Gia Thư, Lê Trọng Vĩnh (2011), *Giáo trình thiết kế mạng*, Đại học Duy Tân, NXB Thông tin & Truyền thông.

[3] Nguyễn Thúc Hải (1997), *Mạng máy tính và các hệ thống mở*, NXB Giáo dục

[4] Arthur Pfund, Eric Ouellet, Robert Padjen (2002), *Building A Cisco Wireless LAN*, Syngress Publishing.

[5] Evan Lane (2017), *Wireless Hacking: How to Hack Wireless Networks (Hacking, How to Hack, Penetration testing, Basic Security, Kali Linux book Book 1)*, Evan Lane.

[6] Jack L. Burbank, Julia Andrusenko, Jared S. Everett, William T.M. Kasch (2013), *Wireless Networking: Understanding Internetworking Challenges 1st Edition*, Wiley-IEEE Press.

[7] John Smith (2016), *Hacking: WiFi Hacking, Wireless Hacking for Beginners*, John Smith.

[8] Matthew S. Gast (2005), *802.11 Wireless Networks: The Definitive Guide: The Definitive Guide 2nd Edition*, O'Reilly Media.

[9] Wayne Lewis (2012) *LAN Switching and Wireless: CCNA Exploration Companion Guide (Cisco Networking Academy Program)*, Cisco Systems; Har/Cdr edition.

[10] Các trang Web:

- http://vnpro.org/forum/
- http://www.quantrimang.com/
- http://www.wi-fi.org