MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

AAA	Authentication, Authorization, Accountting	Xác thực, cấp quyền, tính cước
ACK	Acknowlegment	Bản tin báo nhận
ADSL	Asymmetric Digital Subscriber Line	Đường dây thuê bao bất đối xứng
ASK	Amplitude shift keying	Khóa dịch biên độ
AP	Access Point	Điểm truy cập
BPSK	Binary phase-shift keying	Khóa dịch pha
CCK	Complementary Code Keying	Khóa mã bổ sung
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình host tự động
EAP	Extensible Authentication Protocol	Giao thức chứng thực mở rộng
FSK	Frequency Shift keying	Đánh giá tín hiệu tần số
IP	Internet protocol	Giao thức IP
IEEE	Institute of Electrical and Electronics Engineer	Viện kỹ thuật và điện tử
LAN	Local area network	Mạng cục bộ

MAN	Metropolitant Area	Mạng khu vực đô thị
MAC	Medium Access Control	Điều khiển truy cập truyền thông
PSK	phase shift keying	Kỹ thuật khóa chuyển pha
PC	Personal Computer	Máy tính cá nhân
RADIUS	Remote Authentication Dial In User Service	Dịch vụ chứng thực người dùng
SSID	Subsystem identification	Sự nhận biết hệ thống con
WPA	Wi-Fi Protected Access WEP	Giao thức bảo mật mạng không dây
WEP	WIRED EQUIVALENT PRIVACY	Giao thức bảo mật mạng không dây
Wifi	Wireless fidelity	Công nghệ mạng không dây
WLAN	Wireless local area network	Mạng cục bộ không dây

DANH MỤC CÁC BẢNG VÀ HÌNH VẼ

CÁC BẢNG

HÌNH VẼ

MỞ ĐẦU

Trong xã hội hiện đại, hệ thống thông tin liên lạc đã len lỏi vào từng ngóc ngách của đời sống. Sự gia tăng nhu cầu truyền số liệu và các thiết bị thông minh của người dung đã đặt ra thách thức đối với mạng có dây truyền thống. Điều này khiến cho xu hướng phát triển mạng không dây là tất yếu.

Trường Đại học Dân Lập Hải Phòng đã phát triển mạng không dây ngay từ những ngày thành lập trường. Hệ thống mạng này đã hoạt động rất tốt trong thời gian dài. Tuy nhiên, một vài học kỳ gần đây do số lượng người dùng tăng mạnh đòi hỏi nhà trường phải đưa ra một phương thức quản lý mạng không dây mạnh mẽ, chính xác để có thể đáp ứng được các nhu cầu học tập, trao đổi thông tin của cán bộ giảng viên và học sinh trong trường.

Em đã chọn đề tài *"Xây dựng điểm kiểm soát truy cập mạng không dây Hotspot Gateway có chứng thực dựa trên Mikrotik Router"* làm đồ án tốt nghiệp của mình. Với đồ án này em mong muốn góp một phần nhỏ sức lực vào việc cải thiện chất lượng phục vụ mạng không dây tại nhà Trường.

Được sự chỉ bảo, hướng dẫn tận tình của các thầy, cô trong Khoa, đặc biệt là thầy giáo, Thạc sỹ Bùi Huy Hùng, em đã hoàn thành đồ án với 03 nội dung chính:

Thứ nhất là đưa ra cái nhìn tổng quát về mạng máy tính

Thứ hai là xây dựng mô hình điểm kiểm soát truy cập có chứng thực dựa trên Mikrotik Router Os.

Thứ ba là một số giải pháp khác và kết quả đạt được sau khi triển khai hệ thống chứng thực dựa trên Mikrotik Router Os.

Em mong rằng đồ án sẽ đưa ra cho mọi người một cái nhìn tổng quát về mạng máy tính. Ngoài ra đồ án giới thiệu thêm một giải pháp quản lý mạng không dây có quy mô với chi phí đầu tư thấp và hiệu quả. Mặc dù nhận được sự chỉ bảo tận tình của các thầy cô, nhưng do trình độ, thời gian có hạn nên đề tài vẫn mắc phải những thiếu sót. Vì vậy em rất mong nhận được sự chỉ bảo, phê bình và góp ý quý báu đến từ thầy cô và các bạn.

Em xin chân thành cảm ơn!

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG MÁY TÍNH

1.1 Khái niệm cơ bản về mạng máy tính

Mạng máy tinh là tập hợp các máy tính được kết nối với nhau bởi các đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại cho nhau.

Trong ba thế kỷ qua, mỗi một thế kỷ đều bị chi phối bởi một công nghệ. Thế kỷ 18 là thời đại của các hệ thống cơ khí lớn cùng cuộc cách mạng công nghiệp. Thế kỷ 19 là thời của máy hơi nước. Trong suốt thế kỷ 20 công nghệ chủ yếu là thu thập, xử lý và phân phối thông tin. Cùng với những phát triển khác, ta thấy sự thiết lập các mạng điện thoại trên khắp thế giới, đặc biệt trong thời kỳ này có sự khai sinh và phát triển chưa từng thấy của nền công nghiệp máy tính.

Trong quá trình phát triển của mạng máy tính, các công ty, tổ chức đã lần lượt đưa ra nhiều loại mạng như: ARPANET, NFSNET, APPLE TALK, NOVELL NETWARE và WINDOWS NT

Vào giữa những năm 50 những hệ thống máy tính đầu tiên ra đời, sử dụng các bóng đèn điện tử có kích thước khá cồng kềnh và tiêu tốn nhiều năng lượng. Việc nhập dữ liệu vào máy tính được thông qua các bìa đục lỗ và kết quả được đưa ra máy in, việc này làm mất nhiều thời gian và bất tiện cho người sử dụng.

Vào những năm 60 cùng với sự phát triển của các ứng dụng trên máy tính và nhu cầu troa đổi thông tin với nhau, một số nhà chuyên sản xuất máy tính đã nghiên cứu chế tạo thành công các thiết bị truy cập từ xa tới các máy tính của họ, và đấy cũng là những dạng sơ khai của hệ thống máy tính.

Những năn 70 hệ thống thiết bị đầu cuối 3270 của IBM ra đời cho phép mở rộng khả năng tính toán của các trung tâm máy tính đến các vùng ở xa. Đến giữa những năm 70 IBM đã giới thiệu một loạt các thiết bị đầu cuối được thiết kế cho các ngành ngân hàng thương mại. Thông qua dây cáp mạng và các thiết bị đầu cuối có thể truy cập cùng một lúc đến một máy tính dùng chung. Đến năm 1977, công ty Datapoint Corporation đã tung ra thị trường hệ điều hành mạng của mình là Attache Resource

Computer Network cho phép liên kết các máy tính và các thiết bị đầu cuối lại bằng đây cáp mạng, và đó chính là hệ điều hành mạng đầu tiên.

Đường truyền là một hệ thống các thiết bị truyền dẫn có dây, không dây dùng để chuyển các tín hiệu điện tử từ máy này sang máy khác.

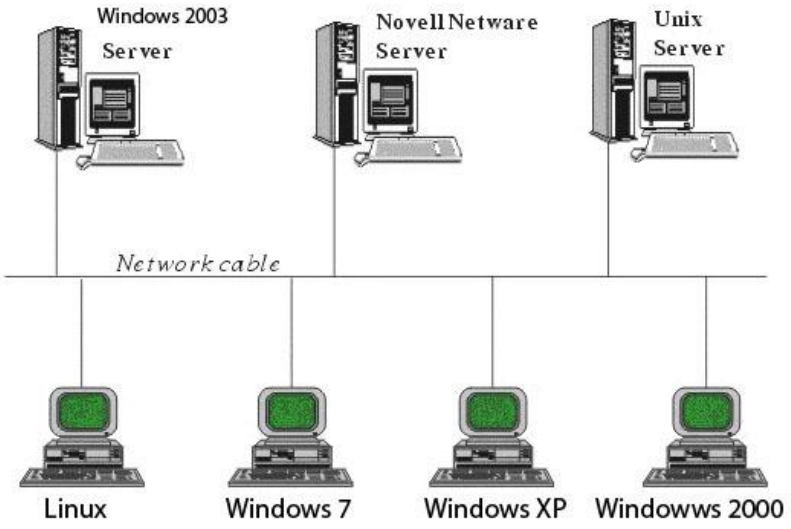
Đường truyền kết nối có thể là: Cáp đồng trục, cáp đôi xoắn, cáp quang, các đường truyền tạo nên cấu trúc mạng.

Mạng máy tinh ra đời xuất phát từ nhu cầu chia sẻ và dùng chung dữ liệu.

Không có hệ thống mạng thì dữ liệu trên các máy tính độc lập muốn chia sẻ với nhau phải thông qua việc in ấn, sao chép qua đĩa mềm, CD ROM,…điều này gây ra rất nhiều bất tiện cho người sử dụng.

Lợi ích của mạng máy tính

- Chia sẻ tài nguyên phần cứng; máy in, máy Fax, modem…
- Chia sẻ tài nguyên phần mềm; tài liệu, phim, ảnh…
- Tăng độ tin cậy của hệ thống.



Hình 1.1: Mô hình liên kết các máy tính trong liên kết mạng

1.1.1 Phân biệt các loại mạng

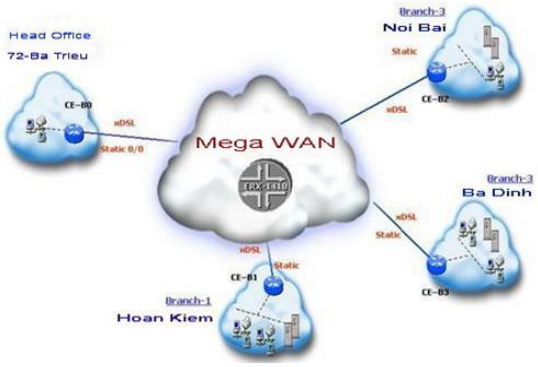
Máy tính ngày nay phát triển khắp nơi với những ứng dụng ngày càng đa dạng cho nên để phân biệt một cách đầy đủ và chi tiết các loại mạng là một việc rất phức tạp.

1.1.1.1 Phân loại mạng theo phân vùng địa lý:

GAN (Global Aera Network) : là kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thông qua mạng viễn thông.

Hình 1.2 : Mô hình mạng GAN

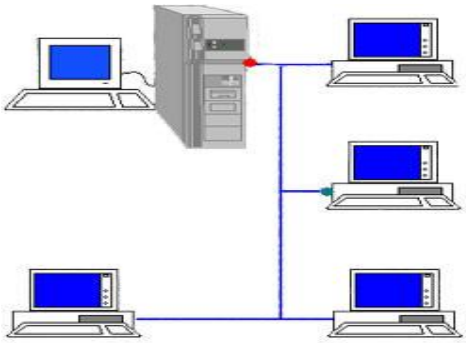
WAN (Wide Area Network) : mạng diện rộng, dùng để kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong một vùng châu lục. Thông thường kết nối này thường được thực hiện thông qua mạng viễn thông. Các mạng WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.



Hình 1.3: Mô hình mạng WAN

MAN (Metropolitan Area Network) : kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50-100 Mbit/s).

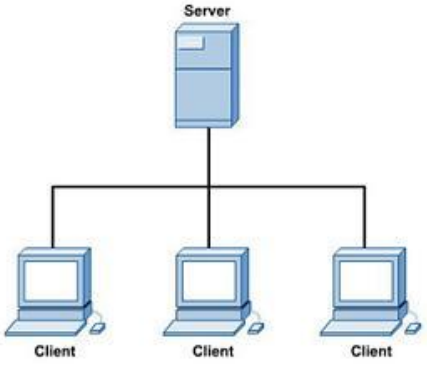
LAN (Local Area Network) : mạng cục bộ, kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao: ví dụ cáp đồng trục, cáp đôi xoắn, cáp quang. LAN thường được sử dụng trong một cơ quan / tổ chức.. như trường học, phòng thực hành… các LAN có thể được kết nối với nhau qua WAN.



Hình 1.4: Mô hình mạng LAN

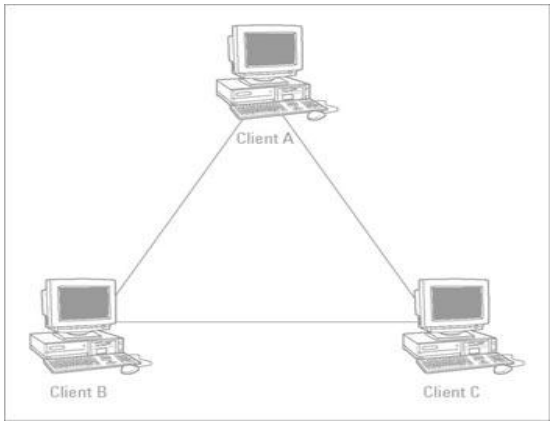
1.1.1.2 Phân loại mạng theo chức năng

Mạng **Client-Server**: Một hay một số máy tính được thiết lập để cung cấp các dịch vụ như file server, mail server…Các máy tính được thiết lập để cung cấp các dịch vụ được gọi là Server, còn các máy tính truy cập và sử dụng dịch vụ thì được gọi là Client.



Hình 1.5: Mô hình mạng Client- Server

Mạng **Peer-to-Peer**: Các máy tính trong mạng có thể hoạt động vừa như một Client vừa như một Server.



Hình 1.6: Mô hình mạng Peer- to- Peer

Mạng kết hợp:Các mạng máy tính thường được thiết lập theo cả hai chức năng, Client-Server và Peer- to- Peer.

1.1.2 Phân loại mạng theo cấu trúc (Topology)

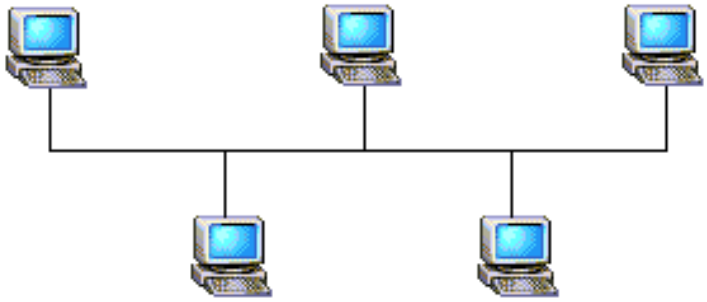
Topology là cấu trúc hình học không gian của mạng, thực chất nó là cách bố trí vật lý các điểm và cách thức kết nối chúng lại với nhau. Điển hình và sử dụng nhiều nhất là các cấu trúc: dạng hình sao, dạng hình tuyến, dạng vòng cùng với các dạng kết hợp của chúng.

1.1.2.1 Mạng dạng xương sống (Bus topology)

Thực hiện theo cách bố trí hành lang, các máy tính và các thiết bị khác- các nút, đều được kết nối với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu. tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bít bởi một thiết bị gọi là Terminator. Các tín hiệu và dữ liệu khi truyền đi dây cáp đều mang theo địa chỉ đến nơi đến.

Ưu điểm: Loại hình này dùng dây cáp ít nhất, dễ lắp đặt giá thành rẻ.

Nhược điểm: Sự ùn tắc giao thông khi di truyển dữ liệu với lưu lượng lớn. khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống. Cấu trúc này ngày nay ít sử dụng.



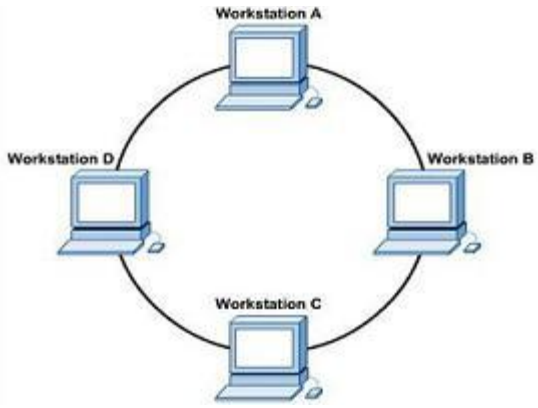
Hình 1.7 Cấu trúc mạng dạng xương sống (Bus topology)

1.1.2.2 Mạng dạng vòng (Ring topology)

Mạng dạng này, bố trí theo dạng xoay vòng, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có địa chỉ kèm theo cụ thể của mỗi trạm tiếp nhận.

Ưu điểm : Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Mỗi trạm có thể đạt được tốc độ tối đa khi truy nhập.

Nhược điểm: Đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.



Hình 1.8 Cấu trúc mạng dạng vòng (Ring topology)

1.1.2.3 Mạng dạng hình sao (Star topology)

Mạng dạng hình sao bao gồm một bộ kết nối trung tâm và các nút. Các nút này là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Bộ kết nối trung tâm của mạng điều phối mọi hoạt động trong mạng.

Mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (Hub) bằng cáp, giải pháp này cho phép nối trực tiếp máy tính với Hub không cần thông qua trục bus, tránh được các yếu tố gây ngưng trệ mạng.

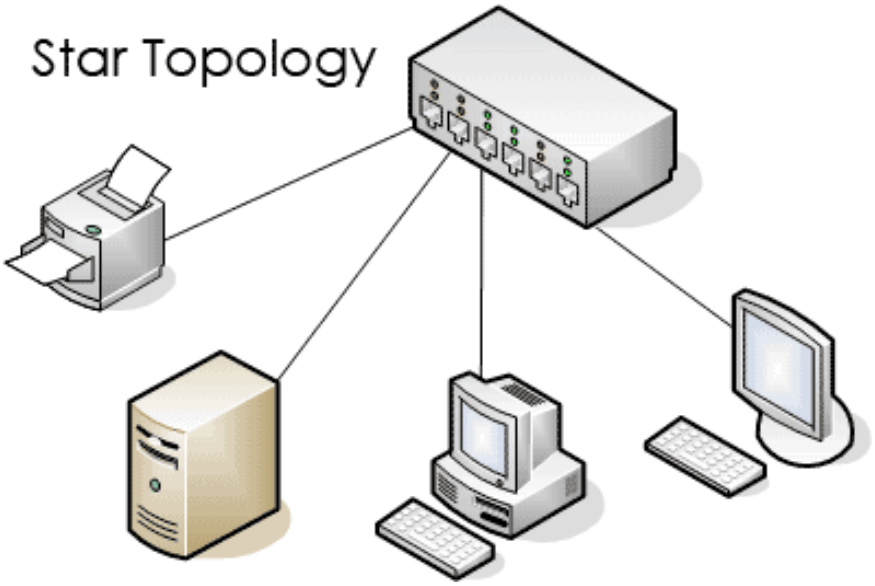
Mô hình kết nối hình sao ngày nay đã trở lên hết sức phổ biến. Với việc sử dụng các bộ tập trung hoặc bộ chuyển mạch, cấu trúc hình sao có thể được mở rộng bằng cách tổ chức nhiều mức phân cấp, do vậy dễ dàng cho việc quản lý và vận hành.

+ Các ưu điểm của mạng hình sao:

- Hoạt động theo nguyên lý nối song song nên nếu có một nút thông tin bị hỏng thì mang vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
- Mạng có thể dễ dàng mở rộng hoặc thu hẹp.

+ Các nhược điểm mạng dạng hình sao:

- Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm
- Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.
- Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).



Hình 1.9 Cấu trúc mạng hình sao (Star topology)

Mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (Hub) bằng cáp, giải pháp này cho phép nối trực tiếp các máy tính với Hub, không cần thông qua trục Bus, tránh được các yếu tố gây nhưng trệ mạng.

1.1.2.4 Mạng dạng kết hợp

Kết hợp hình sao và hình tuyến: Cấu hình mạng dạng này có bộ phận tách tín hiệu(Spitter) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn Ring Topology hoặc Linear Bus Topology. Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở xa cách nhau. Cấu hình dạng kết hợp Star/ Ring Topology có một thẻ bài liên lạc được chuyển vòng quanh một cái Hub trung tâm. Mỗi trạm làm việc được nối với Hub là cầu nối giữa các trạm làm việc và tăng khoảng cách cần thiết.

1.2 Mạng cục bộ LAN (Local Area Network)

1.2.1 Khái niệm về mạng LAN

Các mạng cục bộ, thường được gọi là LAN (Local Area Network), là các mạng được sở hữu riêng bên trong một cao ốc hoặc một khu sân bãi có khoảng cách lên đến vài Km. Các mạng này được sử dụng rộng rãi để kết nối các máy tính cá nhân và các trạm làm việc (Workstation) trong các văn phòng công ty hoặc các nhà máy xí nghiệp để sử dụng chung các nguồn tài liệu.

Các LAN được phân biệt với các mạng khác bởi 3 đặc tính:

- Kích thước (hay khoảng cách).
- Công nghệ truyền trên mạng .
- Sự sắp xếp hình học của mạng (có thể là các topo mạng).

Các LAN bị hạn chế về khoảng cách. Điều này có nghĩa là thời gian truyền trong trường hợp xấu nhất bị giới hạn và được biết trước. Việc biết giới hạn này giúp ta có thể sử dụng các loại thiết kế nào sao cho phù hợp. điều này cũng làm đơn giản việc quản lý mạng.

Các LAN có thể sử dụng công nghệ truyền bao gồm một cáp nối với tất cả các máy được gắn vào cáp này. Các LAN truyền thông hoạt động ở các tốc độ từ 10 Mbp/s =>100 Mbp/s, có trì hoãn nhỏ và tạo ra rất ít lỗi. Các LAN mới hơn hoạt động ở tốc độ lên đến 10 Gbps.

1.2.2 Mô hình và giao thức

Giao thức mạng là tập hợp các quy tắc, quy ước truyền thông của mạng mà tất cả các thực thể của mạng phải tuân theo.

1.2.2.1 Mô hình OSI (Open Systems Interconnect)

a. Mô hình OSI

Mô hình OSI được chia làm 7 tầng, mỗi tầng bao gồm những hoạt động, thiết bị và giao thức mạng khác nhau.

7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Datalink
1: Physical

Bảng 1.1 Mô hình OSI

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết và giao thức không liên kết:

- Giao thức có liên kết: Trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết này, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.
- Giao thức không liên kết: Trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó. Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt.

b. Chức năng của các tầng trong mô hình OSI

Tầng 1: Tầng vật lý (Physical layer)

Tầng vật lý là tầng dưới cùng của mô hình OSI: Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng, các dây cáp có thể dài bao nhiêu … Mặt khác tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không quy định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hinh OSI ý nghĩa của các bit truyền ở tầng vậy lý sẽ được xác định.

Tầng 2: Tầng Liên kết dữ liệu (Data link layer)

Tầng liên kết dữ liệu là tầng mà ở đó ý nghĩa được gán cho các bit được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. Nó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "điểm - điểm" và phương thức "điểm – nhiều điểm". Với phương thức "điểm - điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "điểm - điểm" tất cả các máy phân chia chung một đường truyền vật lý.

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Tầng 3: Tầng Mạng (Network layer)

Tầng mạng nhắm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. Nó xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Nó luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng. Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. Hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). Tầng mạng là quan trọng nhất khi liên kết hai loại mạng khác nhau như mạng Ethernet với mạng Token Ring khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Tầng 4: Tầng vận chuyển (Transport layer)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. Nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trặng bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng.

Tầng 5: Tầng giao dịch (Session layer)

Tầng giao dịch thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xạ giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịnh ứng dụng của họ.

Tầng 6: Tầng trình diễn (Presentation layer)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình diễn (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình diễn cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng trình diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bùng trở lại để được dữ liệu ban đầu.

Tầng 7: Tầng Ứng dụng (Application)

Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

1.2.2.2 Bộ giao thức TCP/IP (Transmission Control Protocol/Internet Protocol)

a. Tổng quan về TCP/IP

TCP/IP là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. TCP/IP được sử dụng rộng rãi trong LAN.

TCP/IP được xem là giản lược của mô hình OSI với 4 tầng như sau:

- Tầng liên kết mạng (Network Access Layer).
- Tầng Internet (Internet Layer).
- Tầng giao vận (Host-to-Host Transport Layer).
- Tầng ứng dụng (Application Layer).

Tầng liên kết: (Network Access Layer).

Tầng liên kết (còn được gọi là tầng liên kết dữ liệu hay là tầng giao tiếp mạng) là tầng thấp nhất trong mô hình TCP/IP, bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua thiết bị giao tiếp mạng đó.

Tầng Internet: (Internet Layer)

Tầng internet (còn gọi là tầng mạng) xử lý quá trình truyền gói tin trên mạng. Các giao thức của tầng này bao gồm: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Messages Protocol).

Tầng giao vận: (Host-to Host Transport Layer)

Tầng giao vận phụ trách luồng dữ liệu giữa hai trạm thực hiện các ứng dụng của tầng trên. Tầng này có hai giao thức chính: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol).

TCP cung cấp một luồng dữ liệu tin cậy giữa hai trạm, nó sử dụng các cơ chế như chia nhỏ các gói tin của tầng trên thành các gói tin có kích thước thích hợp cho tầng mạng bên dưới, báo nhận gói tin,đặt hạn chế thời gian time-out để đảm bảo bên nhận biết được các gói tin đã gửi đi. Do tầng này đảm bảo tính tin cậy, tầng trên sẽ không cần quan tâm đến nữa.

UDP cung cấp một dịch vụ đơn giản hơn cho tầng ứng dụng. Nó chỉ gửi các gói dữ liệu từ trạm này tới trạm kia mà không đảm bảo các gói tin đến được tới đích. Các cơ chế đảm bảo độ tin cậy cần được thực hiện bởi tầng trên.

Tầng ứng dụng: (Application Layer)

Tầng ứng dụng là tầng trên cùng của mô hình TCP/IP bao gồm các tiến trình và các ứng dụng cung cấp cho người sử dụng để truy cập mạng. Có rất nhiều ứng dụng được cung cấp trong tầng này, mà phổ biến là: Telnet: sử dụng trong việc truy cập mạng từ xa, FTP (File Transfer Protocol): dịch vụ truyền tệp, Email: dịch vụ thư tín điện tử, WWW (World Wide Web).

Cũng tương tự như trong mô hình OSI, khi truyền dữ liệu, quá trình tiến hành từ tầng trên xuống tầng dưới, qua mỗi tầng dữ liệu được thêm vào một thông tin điều khiển được gọi là phần header. Khi nhận dữ liệu thì quá trình xảy ra ngược lại, dữ liệu được truyền từ tầng dưới lên và qua mỗi tầng thì phần header tương ứng được lấy đi và khi đến tầng trên cùng thì dữ liệu không còn phần header nữa.

b. Một số giao thức cơ bản trong TCP/IP

Giao thức liên mạng IP (Internet Protocol)

Giao thức liên mạng IP là một trong những giao thức quan trọng nhất của bộ giao thức TCP/IP. Mục đích là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu.

Giao thức IPv_4

IPv_4 gồm 32 bit chia thành 4 octet (1octet = 8 bit), các octet cách nhau bởi dấu chấm (.). $0 \leq$ 1octet ≤ 255.

Ví dụ: 11001100. 1111000. 00001100. 10000001

Để ngắn gọn ta chuyển sang hệ thập phân.

204.240.12.129

Địa chỉ IPv_4: được chia thành 5 lớp A,B,C,D,E; trong đó 3 lớp địa chỉ A,B,C được dùng đề cập nhất, các lớp này được phân chia bởi các bit đầu tiên trong địa chỉ.

IPv_4 lớp A: có giá trị 00000001 ÷ 01111111; (1 ÷ 127)

Octet 1 (địa chỉ mạng). octet 2.octet 3. octet 4 (địa chỉ Host)

Lớp này thường được dùng cho các mạng có số trạm cực lớn, thường dành cho các công ty cung cấp dịch vụ lớn.

IPv_4: lớp B có giá trị 10000000 ÷10111111; (128 ÷ 191).

Octet 1. octet2(địa chỉ mạng). octet 3. octet 4(địa chỉ Host).

Lớp địa chỉ này phù hợp với nhiều yêu cầu nên được cấp phát nhiều nên hiện nay đã khá hiếm.

TPv_4: lớp C có giá trị 11000000 ÷ 11011111, (192 ÷ 233).

Octet 1. octet 2. octet 3 (địa chỉ mạng). Octet 4(địa chỉ Host).

Lớp này được dùng cho các mạng có ít trạm.

IPv_4: lớp D có giá trị 11100000 ÷ 11101111, (224 ÷ 239).

Dùng để gửi gói tin IP đến một nhóm các trạm trên mạng.

IPv_4: lớp E có giá trị 11110000 ÷ 11111111, (240 ÷ 255)

Lớp địa chỉ này dành cho nghiên cứu chưa được sử dụng.

Ngoài giao thức IPv_4 còn sử dụng giao thức liên mạng IPv_6

IPv_6 sử dụng địa chỉ lớn 128 bit do đó cung cấp không gian địa chỉ lớn hơn IPv_4 nhiều.

Tạo ra nhiều mức phân cấp và linh hoạt trong địa chỉ hóa và định tuyến còn đang thiếu trong IPv_4.

Giao thức UDP (User Datagram Protocol)

UDP là giao thức không liên kết, cung cấp dịch vụ không tin cậy, được sử dụng thay thế cho TCP trong tầng giao vận, khác với TCP, UTP không có chức năng thiết lập và giải phóng liên kết, không có cơ chế báo nhận (ACK), không sắp xếp tuần tự các đơn vị dữ liệu (Datagram) đến, có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không hề có thông báo lỗi cho người gửi.

Giao thức TCP (Transmission Control Protocol)

TCP và UTP là 2 giao thức nằm ở tầng giao vận và cùng sử dụng giao thức IP tầng mạng , TCP cung cấp dịch vụ sử dụng liên kết tin cậy và có liên kết.

TCP cung cấp khả năng điều khiển luồng. Mỗi đầu của liên kết TCP có vùng đệm giới hạn do đó TCP tại trạm nhận chỉ cho phép trạm gửi truyền một lượng dữ liệu nhất định. Điều này tránh xảy ra trường hợp trạm có tốc độ cao chiếm toàn bộ vùng đệm của trạm có tốc độ trậm hơn.

So sánh giữa OSI và TCP/IP

Giống nhau: Cả 2 đều là phân lớp.

Cả 2 đều có lớp ứng dụng , qua đó có nhiều dịch vụ khác nhau.

Kỹ thuật chuyển mạch gói được chấp nhận.

Khác nhau.

Mỗi tầng trong TCP/IP có thể là 1 hoặc nhiều tầng trong OSI

Bảng sau chỉ rõ mối tương quan giữa các tầng trong TCP/IP và OSI

OSI	TCP/IP
Phycical Layer & Data Link Layer	Data Link Layer
Network Layer	Internet Layer
Transport Layer	Transport Layer
Session Layer	Application Layer
Presentation Layer	
Application Layer	

Bảng 1.2 Sự khác nhau giữa OSI và TCP/IP

Tầng ứng dụng trong TCP /IP bao gồm luôn cả 3 tầng trên của mô hình OSI. Tầng giao vận trong TCP/IP không phải luôn đảm bảo độ tin cậy truyền tin như trong tầng gia vận của OSI mà cho phép thêm 1 lựa chọn khác là UDP

1.2.3 Các thiết bị trong mạng LAN

Để hệ thống mạng làm việc trơn tru, hiệu quả và khả năng kết nối tới những hệ thống mạng khác đòi hỏi phải sử dụng những thiết bị mạng chuyên dụng. Những thiết bị này rất đa dạng và phong phú về chủng loại nhưng đều dựa trên những thiết bị cơ bản là: Hệ thống cáp, Repeater, Hub, Swich, Router và Gateway.

Các thiết bị dùng để kết nối

1.2.3.1 Card mạng (NIC)

Hình 1.10 Card mạng TP-LINK (NIC)

Để một máy tính kết nối vào mạng LAN máy tính đó bắt buộc có NIC, mỗi NIC sẽ có một địa chỉ duy nhất không trùng với bất kỳ NIC nào khác. Địa chỉ này gọi địa chỉ MAC hay địa chỉ vật lý, khi sản xuất nhà sản xuất gán cứng địa chỉ MAC vào bộ nhớ ROM của NIC, khi NIC được gán vào máy tính địa chỉ MAC của NIC sẽ là địa chỉ vật lý của máy tính trong mạng, khi máy tính khởi động địa chỉ MAC sẽ được nạp từ ROM của NIC vào bộ nhớ RAM của máy tính.

1.2.3.2 Bộ lặp tín hiệu (Repeater)

Hình 1.11 Bộ lặp tín hiệu (Repeater)

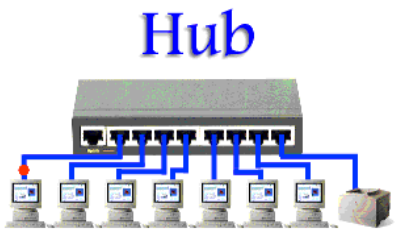
Repeater là thiết bị đơn giản nhất trong các thiết bị kết nối mạng, Repeater nhận tín hiệu từ một phần của mạng và chuyển phát tín hiệu này tới phần còn lại trong mạng. Repeater không có cơ chế xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu và khuếch đại tín hiệu đã suy hao khôi phục lại tín hiệu ban đầu. Do đó Repeater được sử dụng nhằm làm tăng thêm chiều dài của mạng. Có hai loại Repeater được sử dụng hiện nay là Repeater điện và Repeater điện quang.

1.2.3.3 Bộ tập trung (Hub)

Hub là điểm kết nối trung tâm của mạng, tất cả các trạm trên LAN được kết nối thông qua Hub với các đầu cắm. Hub thực sự là những Repeater đa port, Hub thường có từ 4 đến 24 port còn Repeater có 2 port.

Có ba loại Hub:

- Hub thụ động (Passive Hub)
- Hub chủ động (Active Hub)
- Hub thông minh (Intelligent Hub)



Hình 1.12 Bộ tập trung (Hub)

1.2.3.4 Bộ cầu nối (Bridge)

Bridge là một thiết bị hoạt động ở tầng 2 trong mô hình OSI. Bridge làm nhiệm vụ chuyển tiếp các khung từ nhánh mạng này sang nhánh mạng khác. Điều quan trọng là Bridge « thông minh » , nó chuyển frame một cách có chọn lọc dựa vào địa chỉ MAC của các máy tính. Bridge còn cho phép các mạng có tầng vật lý khác nhau có thể giao tiếp được với nhau. Bridge chia liên mạng ra thành những vùng đụng độ nhỏ, nhờ đó cải thiện được hiệu năng của liên mạng tốt hơn so với liên mạng bằng Repeater hay Hub.

Hình 1.13 Bộ cầu nối (Bridge)

1.2.3.5 Bộ chuyển mạch (Switch)

Switch là sự tiến hóa của Bridge, với nhiều cổng hơn và các mạch tích hợp nhanh để giảm độ trễ của việc chuyển khung dữ liệu và hỗ trợ nhiều tính năng mới chưa có ở Bridge.

Switch giữ bảng địa chỉ MAC của mỗi cổng và thực hiện giao thức Spanning-Tree. Switch cũng hoạt động ở tầng data link và trong suốt với các giao thức ở tầng trên nó.

Hình 1.14 Bộ chuyển mạch (Switch)

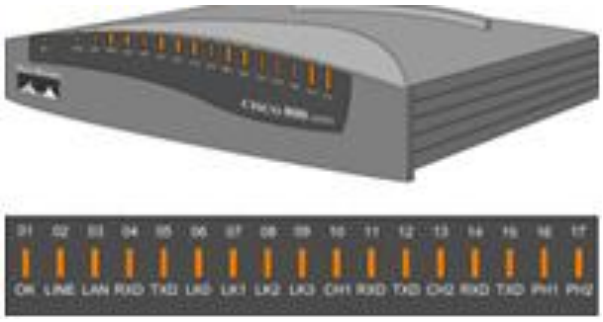
1.2.3.6 Bộ định tuyến (Router)

Là thiết bị hoạt động tại tầng ba trong mô hình OSI, tuy nhiên vẫn có thể hoạt động tại tầng hai và tầng một.

Nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối mạng khác nhau, để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối.

Router có thể được sử dụng để nối nhiều mạng lại với nhau và cho phép các gói tin trong gói tin có thể đi theo nhiều đường khác nhau để tới đích . Router truy cập nhiều thông tin trong gói dữ liệu và dùng thông tin để cải thiện việc phân phát gói dữ

liệu. Các bộ định tuyến có thể chia sẻ thông tin trạng thái và thông tin định tuyến với nhau sử dụng thông tin này để bỏ qua các kết nối hỏng hoặc chậm.



Hình 1.15: Bộ định tuyến (Router)

1.2.3.7 Điều chế và giả điều chế (Modem)

Modem là thiết bị tích hợp của một bộ điều chế và một bộ giả điều chế. Là thiết bị có chức năng chuyển đổi tín hiệu số thành tín hiệu tương ứng và ngược lại để kết nối các máy tính qua đường điện thoại.

Hình 1.16 Modem ADSL

1.3 Mạng không dây WLAN (Wireless Lan)

WLAN là mạng kết hợp giữa mạng LAN, dữ liệu được truyền trong dây dẫn và mạng Wi-fi, dữ liệu được truyền dẫn sử dụng sóng vô tuyến. Các thành phần trong mạng sử dụng sóng điện từ để truyền thông với nhau.

1.3.1 Ưu, nhược điểm của mạng không dây WLAN

1.3.1.1 Ưu điểm của mạng không dây

- Sự tiện lợi: Mạng không dây cho phép người dùng có thể truy xuất tài nguyên mạng ở bất kỳ đâu trong phạm vi được phủ sóng. Ưu điểm này được thể hiện ngày càng rõ khi các thiết bị di động gia tăng nhanh chóng.

- Khả năng di động; Người dùng có thể di chuyển bất kỳ đâu trọng khu vực triển khai mà không bị mất kết nối.

- Khả năng triển khai: Chỉ cần 1 Access point là có thể triển khi một mạng không dây nhỏ. Việc triển khai mạng không dây đơn giản hơn so với mạng có dây trong một số trường hợp như địa hình không thuận lợi...

- Khả năng mở rộng: Mạng không dây có thể đáp ứng được sự gia tăng đột ngột người dùng trong khi mạng có dây phải lắp thêm cáp, thiết bị...

1.3.1.2 Nhược điểm của mạng không dây

- Khả năng bảo mật: Do môi trường truyền là không khí nên khả năng bảo mật kém, người dùng rất dễ bị tấn công.

- Phạm vi triển khai: Một mạng với chuẩn 802.11 và các thiết bị thông thường chỉ có thể phủ sóng trong phạm vi vài chục mét. Vì vậy đối với các môi trường lớn thì cần các thiết bị chuyên dụng và các repeater để nối các mạng với nhau. Điều này làm tăng đáng kể chi phí lắp đặt.

- Độ tin cậy của mạng: Do môi trường truyền dẫn là không khí nên mạng bị ảnh hưởng bởi các loại sóng khác, gây ra nhiễu, giảm cường độ sóng. Điều này ảnh hưởng trực tiếp tới chất lượng của mạng.

- Tốc độ của mạng: Mạng không dây thường có tốc độ từ 1-1300 Mbps, chậm hơn rất nhiều so với mạng có dây (10 - 10000 Mbps).

1.3.2 Các thiết bị cơ bản

1.3.2.1 (Wireless NIC)

Card mạng không dây (Wireless Card) là thiết bị kết nối giữa máy tính với access point. Wireless card đóng vai trò như một bộ thu phát tín hiệu giúp các thiết bị số trao đổi dữ liệu với nhau hoặc truy cập Internet tốc độ cao theo chuẩn IEEE 802.11g hoặc IEEE 802.11b hoặc IEEE 802.11a trong bán kính 100m (nếu ở trong nhà) và 300m (nếu ở ngoài trời). Lợi điểm lớn nhất của wireless card chính là việc giúp người dùng loại bỏ các sợi cáp lằng nhằng bất tiện, người dùng có thể mang máy tính, PDA đến bất cứ đâu có "phủ sóng" để kết nối Internet mà không cần cáp cũng như các khai báo phức tạp.

Hình 1.17 Card mạng không dây chuẩn PCI

Hình 1.18 Card mạng không dây chuẩn PCMCIA

Hình 1.19 Usb wifi TpLink

1.3.2.2 Modem không dây (Acess point)

Access Point là thiết bị nối kết giữa mạng có dây và mạng không dây. Các thiết bị này hỗ trợ băng thông 11Mbps, 54Mbps, … và hoạt động tại băng tầng 2.4GHz, 5 GHz , hỗ trợ mã hóa (WEP) 64/128bit, hỗ trợ DHCP, hỗ trợ firewall, hỗ trợ Port Ethernet, …

Hình 1.20 Access Point

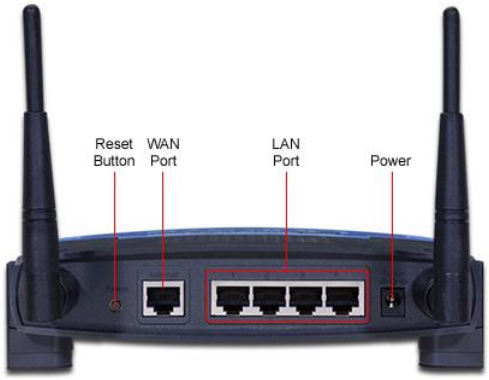
1.3.2.3 Bridge không dây (Wbridge)

Wbridge (Bridge không dây) tương tự như các điểm truy cập không dây trừ trường hợp chúng được sử dụng cho các kênh bên ngoài. Wbridge được thiết kế để nối các mạng với nhau, đặc biệt với các mạng không dây có khoảng cách xa lên tới 32 km. Wbridge có thể lọc lưu lượng và đảm bảo các hệ thống mạng không dây được kết nối tốt mà không bị mất lưu lượng.

Hình 1.21 Wbridge

1.3.2.4 Wireless Router

Wireless Router – Một Wireless Router cũng làm công việc nối kết các máy computer cùng một network giống như access point, nhưng wireless router có thêm những bộ phận phần cứng khác giúp nó nối kết giữa những network khác nhau lại. Internet là một hệ thống network khổng lồ và khác với hệ thống LAN của bạn. Để có thể nối kết với một hệ thống network khác chẳng hạn như internet, thì bạn phải dùng wireless router. Wireless Router sẽ giúp tất cả các máy computer của bạn nối kết vào internet cùng một lúc. Sự khác biệt mà bạn có thể phân biệt dễ dàng là wireless router có thêm một lỗ cắm ghi WAN để cắm vào DSL hoặc Cable modem.



Hình 1.22 Các cổng kết nối của 1 wireless router thông thường

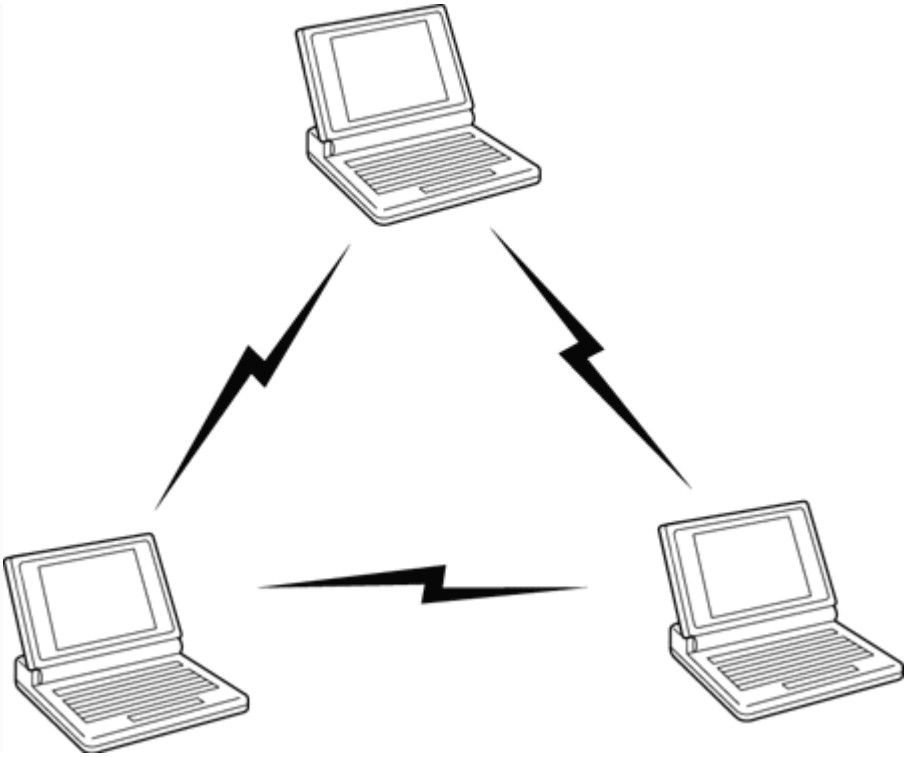
Nên sử dụng Access Point hay Wireless Router? Nếu không cần sử dụng internet mà chỉ cần nối kết tất cả các máy trong nhà lại bằng hệ thống wireless thì chúng ta sử dụng Wireless Access Point vì nó rẻ tiền hơn. Còn nếu muốn nối kết tất cả các máy trong nhà lại và vào được luôn internet cùng một lúc thì bạn sử dụng wireless router.

Wireless router có thể hoạt động như một access point, các máy tính nối vào 2 thiết bị này đều cùng thuộc một lớp mạng nếu ta dùng cáp chéo nối port LAN của ADSL modem sang port LAN bên wireless router. Tuy nhiên ta nên sử dụng router với đúng chức năng là một router, lúc này hệ thống sẽ có 2 nút mạng, trở nên bảo mật hơn và router có thể tận dụng được đúng với tính năng định tuyến của nó và một số chức năng nâng cao khác như: NAT, firewall, điều phối băng thông, …

1.3.3 Các mô hình mạng không dây

1.3.3.1 Mô hình mạng Ad-hoc

Trong mô hình mạng ad-hoc, các client kết nối trực tiếp với nhau mà không cần thông qua Access point nhưng phải ở trong phạm vi cho phép. Mô hình mạng nhỏ nhất trong chuẩn 802.11 là 2 máy client liên lạc trực tiếp với nhau. Thông thường mô hình này được thiết lập bao gồm một số client được cài đặt dùng chung mục đích cụ thể trong khoảng thời gian ngắn .Khi mà sự liên lạc kết thúc thì mô hình add-hoc này cũng được giải phóng.



Hình 1.23 Mô hình mạng Ad-hoc

1.3.3.2 Mô hình mạng cơ sở (BSSs)

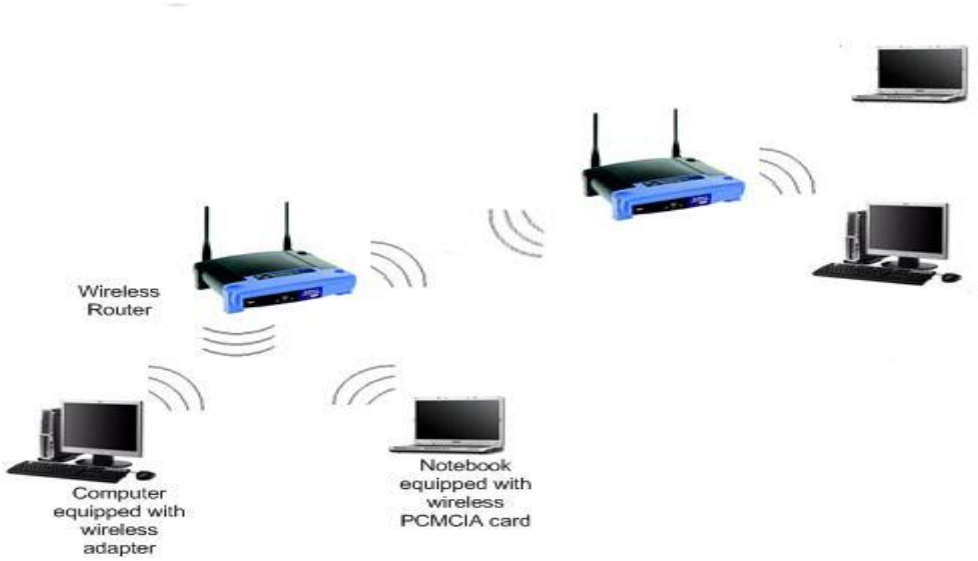
The Basic Service Sets (BSS) là một kiến trúc nền tảng của mạng 802.11. Các thiết bị giao tiếp tạo nên một BSS với một AP duy nhất với một hoặc nhiều client. Các máy trạm kết nối với sóng wireless của AP và bắt đầu giao tiếp thông qua AP. Các máy trạm là thành viên của BSS được gọi là "có liên kết".

Thông thương các Access point được kết nối với một hệ thống phân phối trung bình (DSM), nhưng đó không phải là một yêu cầu cần thiết của một BSS. Nếu một Access point phục vụ như là cổng để vào dịch vụ phân phối, các máy trạm có thể giao tiếp, thông qua Access point, với nguồn tài nguyên mạng ở tại hệ thống phân phối trung bình. Nó cũng cần lưu ý là nếu các máy client muốn giao tiếp với nhau, chúng phải chuyển tiếp dữ liệu thông qua các Access point. Các client không thể truyền thông trực tiếp với nhau, trừ khi thông qua các Access point.

Hình 1.24 Mô hình mạng cơ sở BSSs

1.3.3.3 Mô hình mạng mở rộng (ESSs)

Mô hình mạng mở rộng ESSs là một tập hợp các mạng cơ sở BSSs. Các mạng BSSs giao tiếp với nhau thông qua Access point. Các mạng BSSs chồng chéo lên nhau tạo ra sự liên tục cho client khi client di chuyển từ vùng này sang vùng khác của ESSs.



Hình 1.25 Mô hình mạng mở rộng ESSs

1.3.4 Các chuẩn IEEE 802.11 thông dụng

Hiện nay, wireless network, cụ thể hơn là wireless LAN dùng các chuẩn dạng 802.11. Chuẩn này được ra đời vào năm 1997. Đây là chuẩn sơ khai của mạng ko dây,

nó mô tả cách truyền thông trong mạng ko dây sử dụng các phương thức như DSSS, FHSS và Infrared

Tốc độ hoạt động từ 1 - 2 Mbs, hoạt động trong băng tần 2.4GHz. Sau này chuẩn này còn được bổ sung thêm nhiều chuẩn mới có dạng 802.11x.

a. 802.11: ra đời năm 1997. Đây là chuẩn sơ khai của mạng không dây, nó mô tả cách truyền thông trong mạng không dây sử dụng các phương thức như DSSS, FHSS, infrared (hồng ngoại). Tốc độ hoạt động tối đa là 2 Mbps, hoạt động trong băng tần 2.4 GHz ISM. Hiện nay chuẩn này rất ít được sử dụng trong các sản phẩm thương mại.

b. 802.11b : đây là một chuẩn mở rộng của chuẩn 802.11, nó cải tiến DSSS để tăng băng thông lên 11 Mbps, cũng hoạt động ở băng tần 2.4 GHz và tương thích ngược với chuẩn 802.11. Chuẩn này trước đây được sử dụng rộng rãi trong mạng WLAN nhưng hiện nay thì các chuẩn mới với tốc độ cao hơn như 802.11a và 802.11g có giá thành ngày càng hạ đã dần thay thế 802.11b.

c. 802.11a : Chuẩn này sử dụng băng tần *5 GHZ UNII* nên nó sẽ không giao tiếp được với chuẩn 802.11 và 802.11b. Tốc độ của nó lên đến 54 Mbps vì nó sử dụng công nghệ *OFDM*. Chuẩn này rất thích hợp khi muốn sử dụng mạng không dây tốc độ cao trong môi trường có nhiều thiết bị hoạt động ở băng tần 2.4 Ghz vì nó không gây nhiễu với các hệ thống này.

d. 802.11g : chuẩn này hoạt động ở băng tần 2.4 GHz, sử dụng công nghệ OFDM nên có tốc độ lên đến 54 Mbps (nhưng không giao tiếp được với 802.11a vì khác tần số hoạt động). Nó cũng tương thích ngược với chuẩn 802.11b vì có hỗ trợ thêm DSSS (và hoạt động cùng tần số). Điều này làm cho việc nâng cấp mạng không dây từ thiết bị 802.11b ít tốn kém hơn. Trong môi trường vừa có cả thiết bị 802.11b lẫn 802.11g thì tốc độ sẽ bị giảm đáng kể vì 802.11b không hiểu được OFDM và chỉ hoạt động ở tốc độ thấp.

e. 802.11e : đây là chuẩn bổ sung cho chuẩn 802.11 cũ, nó định nghĩa thêm các mở rộng về chất lượng dịch vụ (QoS) nên rất thích hợp cho các ứng dụng như multimedia như voice

f. 802.11f : được phê chuẩn năm 2003. Đây là chuẩn định nghĩa các thức các AP giao tiếp với nhau khi một client roaming từng vùng này sang vùng khác. Chuẩn này còn được gọi là Inter-AP Protocol (IAPP). Chuẩn này cho phép một AP có thể phát

hiện được sự hiện diện của các AP khác cũng như cho phép AP "chuyển giao" client sang AP mới (lúc roaming), điều này giúp cho quá trình roaming được thực hiện một cách thông suốt.

g. 802.11i : là một chuẩn về bảo mật, nó bổ sung cho các yếu điểm của WEP trong chuẩn 802.11. Chuẩn này sử dụng các giao thức như giao thức xác thực dựa trên cổng 802.1X, và một thuật toán mã hóa được xem như là không thể crack được đó là *thuật toán AES* (Advance Encryption Standard), thuật toán này sẽ thay thế cho thuật toán RC4 được sử dụng trong WEP.

h. 802.11h : chuẩn này cho phép các thiết bị 802.11a tuân theo các quy tắc về băng tần 5 Ghz ở châu âu. Nó mô tả các cơ chế như tự động chọn tần số (DFS = Dynamic Frequency Selection) và *điều khiển công suất truyền* (TPC = Transmission Power Control) để thích hợp với các quy tắc về tần số và công suất của Châu Âu.

i. 802.11j : được phê chuẩn tháng 11/2004 cho phép mạng 802.11 tuân theo các quy tắc về tần số ở băng tần 4.9 Ghz và 5 Ghz ở Nhật Bản

k. 802.11d : chuẩn này chỉnh sửa lớp MAC của 802.11 cho phép máy trạm sử dụng FHSS có thể tối ưu các tham số lớp vật lý để tuân theo các quy tắc của các nước khác nhau nơi mà nó được sử dụng.

l. 802.11s : định nghĩa các tiêu chuẩn cho việc hình thành *mạng dạng lưới* (mesh network) một cách tự động giữa các AP 802.11 với nhau.

Chuẩn này đang được xây dựng, có tốc độ rất cao, từ 200 - 540 Mbps, hoạt động ở 2 giải băng tần là 2,4 GHz và 5 GHz.

m.802.11ac: Ngày 8/12/201, nhà sản xuất chip truyền thông công bố chuẩn Wifi mới 802.11ac. Chuẩn này cho phép cung cấp thông lượng lên tới 1.3Gbps với phạm vi dài hơn và khả năng xuyên tường tốt hơn. Chuẩn 802.11ac là một bước tiến lớn từ 802.11n – chuẩn hiện hành thường có tốc độ khoảng 450 Mbps.

CHƯƠNG 2: XÂY DỰNG ĐIỂM KIỂM SOÁT TRUY CẬP MẠNG KHÔNG DÂY HOTSPOT GATEWAY CÓ CHỨNG THỰC DỰA TRÊN MIKROTIK ROUTER OS

2.1 Hotspot và vấn đề bảo mật

2.1.1 Hotspot và công nghệ Captive Portal là gì

Hospot là một địa điểm với công nghệ Captive Portal sẽ bắt buộc máy tính muốn sử dụng mạng thì trước tiên phải sử dụng trình duyệt để được chuyển hướng tới một trang đặc biệt xác thực người dùng.

Hotspot cung cấp các dịch vụ kết nối không dây và dịch vụ truy cập Internet tốc độ cao thông qua hoạt động thu phát của các các thiết bị phát sóng không dây (Wireless Access Point). Bạn có thể gia nhập vào điểm Hotspot để sử dụng các dịch vụ đó nếu bạn trong vùng phủ sóng và máy tính hoặc thiết bị ... của bạn có trang bị card mạng không dây. Hiện nay số lượng các điểm Hotspot đang tăng nhanh chóng, đặc biệt tại các khu vực công cộng như nhà hàng, sân bay, ga tầu, quán cafe...

Những điều cần thiết để tham gia vào một điểm truy cập Hotspot

Máy tính hoặc thiết bị di động của bạn cần trang bị tính năng không dây. Trong trường hợp thiết bị chưa có thì bạn cần mua thêm các loại Card mạng không dây phù hợp. Hiện nay phần lớn các điểm Hotspot đều sử dụng các thiết bị thu phát sóng chuẩn n (802.11n).

Đối với các Hotspot miễn phí, chỉ cần một số thông tin để tham gia vào mạng. Còn đối với các Hotspot thương mại hoặc có chứng thực thì cần đăng ký tài khoản trước khi tham gia lần đầu. Tài khoản này được cung cấp bởi người quản trị của điểm hotspot đó.

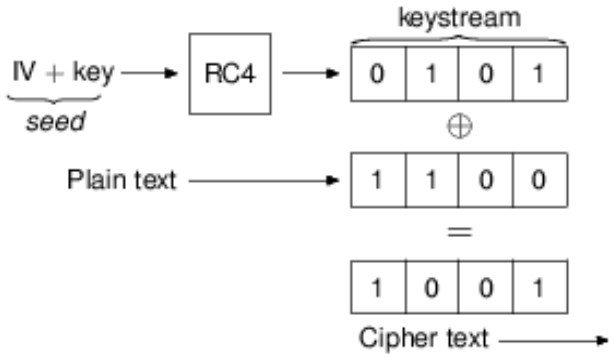
2.1.2 Vấn đề bảo mật tại các điểm Hotspot

Đối với các điểm Hotspot miễn phí, vì mục đích đơn giản hóa quá trình tham gia của người dùng nên những tính năng bảo mật không được kích hoạt hoặc kích hoạt hạn chế.

Đối với các điểm Hotspot thương mại thì yêu cầu mức độ bảo mật cao hơn. Người dùng muốn gia nhập mạng cần qua một số bước chứng thực bằng key, địa chỉ Mac, hoặc tài khoản mật khẩu... Người dùng muốn tham gia mạng cần liên hệ với người quản trị để có thể được chứng thực.

Giao thức WEP

WEP (Wired Equivalent Privacy) nghĩa là bảo mật tương đương với mạng có dây (Wired LAN). Khái niệm này là một phần trong chuẩn IEEE 802.11. Theo định nghĩa, WEP được thiết kế để đảm bảo tính bảo mật cho mạng không dây đạt mức độ như mạng nối cáp truyền thống. Đối với mạng LAN (định nghĩa theo chuẩn IEEE 802.3), bảo mật dữ liệu trên đường truyền đối với các tấn công bên ngoài được đảm bảo qua biện pháp giới hạn vật lý, tức là hacker không thể truy xuất trực tiếp đến hệ thống đường truyền cáp. Do đó chuẩn 802.3 không đặt ra vấn đề mã hóa dữ liệu để chống lại các truy cập trái phép. Đối với chuẩn 802.11, vấn đề mã hóa dữ liệu được ưu tiên hàng đầu do đặc tính của mạng không dây là không thể giới hạn về mặt vật lý truy cập đến đường truyền, bất cứ ai trong vùng phủ sóng đều có thể truy cập dữ liệu nếu không được bảo vệ.



Hình 2.1: Quy trình mã hóa WEP sử dụng thuật toán RC4

WEP cung cấp bảo mật cho dữ liệu trên mạng không dây qua phương thức mã hóa sử dụng thuật toán đối xứng RC4, được Ron Rivest - thuộc hãng RSA Security Inc phát triển. Thuật toán RC4 cho phép chiều dài của khóa thay đổi và có thể lên đến 256 bit. Chuẩn 802.11 đòi hỏi bắt buộc các thiết bị WEP phải hỗ trợ chiều dài khóa tối thiểu là 40 bit, đồng thời đảm bảo tùy chọn hỗ trợ cho các khóa dài hơn. Hiện nay, đa số các thiết bị không dây hỗ trợ WEP với ba chiều dài khóa: 40 bit, 64 bit và 128 bit. Với phương thức mã hóa RC4, WEP cung cấp tính bảo mật và toàn vẹn của thông tin trên mạng không dây, đồng thời được xem như một phương thức kiểm soát truy cập. Một máy nối mạng không dây không có khóa WEP chính xác sẽ không thể truy cập đến Access Point (AP) và cũng không thể giải mã cũng như thay đổi dữ liệu trên đường truyền.

Giao thức WAP

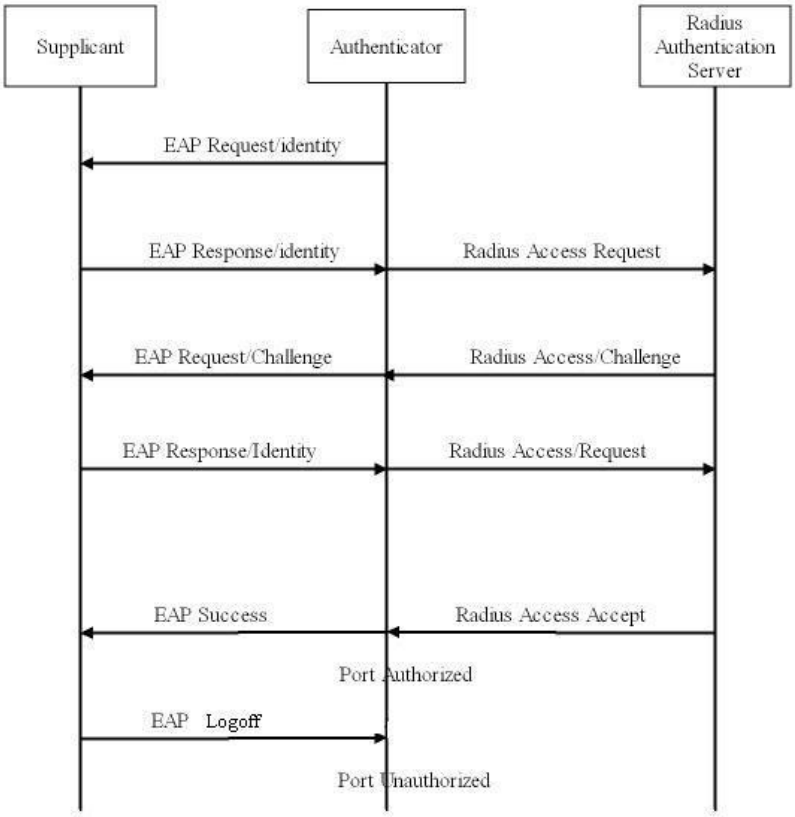
Wi-Fi Alliance đã đưa ra giải pháp gọi là Wi-Fi Protected Access (WPA). Một trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP (Temporal Key Integrity Protocol). WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu. Không những thế, WPA còn bao gồm cơ chế kiểm tra tính toàn vẹn của thông tin (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. Một trong những điểm hấp dẫn nhất của WPA là không yêu cầu nâng cấp phần cứng. Các nâng cấp miễn phí về phần mềm cho hầu hết các card mạng và điểm truy cập sử dụng WPA rất dễ dàng và có sẵn.

WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn này đều sử dụng cơ chế mã hóa TKIP (Temporal Key Integrity Protocol), sử dụng thuật toán RC4 để mã hóa với 128bit cho mã hóa và 64bit cho chứng thực, và sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm. Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc.

Trong khi Wi-Fi Alliance đã đưa ra WPA, và được coi là loại trừ mọi lỗ hổng dễ bị tấn công của WEP, nhưng người sử dụng vẫn không thực sự tin tưởng vào WPA. Có

một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal. Khi mà sử dụng hàm thay đổi khoá TKIP được sử dụng để tạo ra các khoá mã hoá bị phát hiện, nếu hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khoá khởi tạo không dễ đoán (đừng sử dụng những từ như "password, 123456, abcdef, …" để làm mật khẩu).

Điều này cũng có nghĩa rằng kỹ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không truyền dữ liệu "mật" về những thương mại, hay các thông tin nhạy cảm... WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.



Hình 2.2: Messages trao đổi trong quá trình authentication.

Giao thức WAP2

WPA2 là một chuẩn ra đời sau WPA và được kiểm định lần đầu tiên và ngày 1/9/2004. WPA2 được National Institute of Standards and Technology (NIST) khuyến

cáo sử dụng. WPA2 cũng có cấp độ bảo mật rất cao tương tự như chuẩn WPA, nhằm bảo vệ cho người dùng và người quản trị đối với tài khoản và dữ liệu. Nhưng trên thực tế WPA2 cung cấp hệ thống mã hóa mạnh hơn so với WPA, và đây cũng là nhu cầu của các tập đoàn và doanh nghiệp có quy mô lớn. WPA2 sử dụng rất nhiều thuật toán để mã hóa dữ liệu như TKIP, RC4, AES và một vài thuật toán khác. Những hệ thống sử dụng WPA2 đều tương thích với WPA.

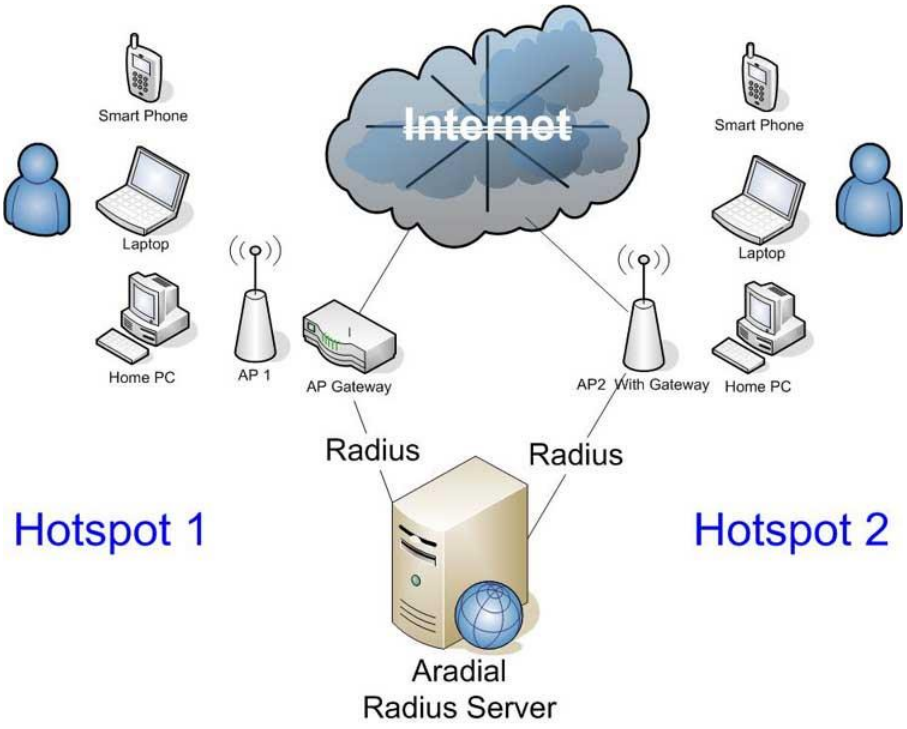
Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là chuẩn mã hoá nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Tuy nhiên thuật toán này đổi hỏi một khả năng tính toán cao (high computation power). Do đó, 802.11i không thể update đơn giản bằng phần mềm mà phải có một bộ xử lý chuyên dụng (dedicated chip). Tuy nhiên điều này đã được ước tính trước bởi nhiều nhà sản xuất nên hầu như các chip cho card mạng Wifi từ đầu năm 2004 đều thích ứng với tính năng của 802.11i.

Để đánh giá chuẩn mã hoá này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mỹ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã đối xứng này. Và chuẩn mã hoá này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

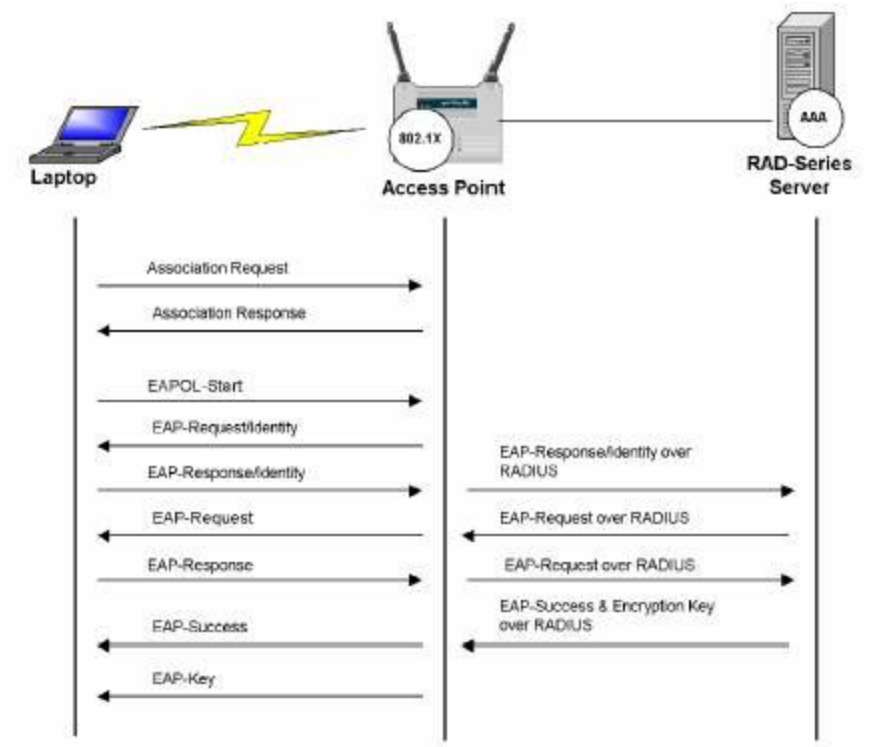
Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard), để đảm bảo về mặt hiệu năng, quá trình mã hoá cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, rất ít người sử dụng mạng không dây quan tâm tới vấn đề này. Hơn nữa, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch đều không tương thích với chuẩn 802.11i.

Giải pháp Radius Server

Việc chứng thực của 802.11 được thực hiện trên một server riêng. Server này sẽ quản lý các thông tin để xác thực người sử dụng như tên đăng nhập (username) và mật khẩu (password), mã số thẻ, dấu vân tay... Khi người dùng gửi yêu cầu chứng thực, server này sẽ tra cứu dữ liệu để xác định người dùng có hợp lê hay không, được cấp quyền truy cập ở mức nào... Server này được gọi là Radius (Remote Authentication Dial-in User Service) Server = Máy chủ cung cấp dịch vụ chứng thực người dùng từ xa.



Hình 2.3 Chứng thực sử dụng Radius Server



Hình 2.4 Messages trao đổi trong quá trình authentication.

2.2 Tính khả thi của mô hình kiểm soát truy cập không dây chứng thực dựa trên Mikrotik Router OS

2.2.1 Tính khả thi về mặt công nghệ

- Do là một hệ điều hành độc chạy dựa trên nhân Linux 2.6 nên yêu cầu cấu hình thấp (ngay cả các máy PIII, dung lượng ổ đĩa còn trống tối thiểu 64MB) nhưng vẫn đáp ứng quản trị được số lượng người dùng cần thiết với tính ổn định cao.

- Kiểm soát người dùng truy cập mạng không dây với tài khoản mật khẩu do người quản trị cung cấp (người dùng có thể tự đổi mất khẩu của mình).

- Kiểm soát dung lượng dữ liệu, thời gian sử dụng.

- Phần mềm cài đặt dễ dàng, khả năng backup, restore khi nhanh chóng.

- Hỗ trợ đa dạng các giao diện tương tác như: dòng lệnh, web, một số công cụ lập trình khác...

2.2.2 Tính khả thi về mặt sử dụng

-Mikrotik đứng thứ 6/10 giải pháp quản lý hệ thống Wi-fi phổ biến thế giới được triển khai tại các địa điểm công cộng, nhà ga... sân bay như sân bay LaGuardia New York, Paul International Minneapolis-St. Ngoài ra Mikrotik còn được triển khai độc quyền tại một tiểu bang của Bzazil.

- Giá thành: 250 USD cho một License theo ổ cứng LV6. Mikrotik hiện cho phép chuyển đổi License sang một ổ cứng khác với giá 10 USD đối với một số tổ chức uy tín nếu ổ cứng họ bị lỗi hoặc hỏng.

- Khả năng tùy biến người dùng cao

- Phù hợp với điều kiện thực tế của trường như tạo người dùng lớn, đơn giản và có quy tắc (hiện đã tạo 1 lần hơn 7700 tài khoản dành cho các Sinh viên, Cán bộ, Giảng viên và Nhân viên toàn Trường).

- Đối với người dùng: có thể quản lý được băng thông, lưu lượng, tốc độ, thời gian sử dụng...

- Hệ thống hỗ trợ thống kê hoàn thiện, nhanh chóng.

- Khả năng áp dụng tại các địa điểm khác của trường cao.

- Tài liệu sử dụng, quản lý đầy đủ.

2.2.3 Tính khả thi về hiệu quả sử dụng

- Tính tương thích cao: Phần mềm tương thích hầu hết với các thiết bị có phần cứng kết nối wifi như laptop, điện thoại di động, tablet... và tương thích với hầu hết các hệ điều hành như Windows, mã nguồn mở, Ios Apple,Rim OS...

- Mikrotik OS cung cấp sẵn giao diện người dùng thông qua web để người dùng có thể tự đổi mật khẩu, thông tin cá nhân mà không cần liên hệ với người quản trị. Đồng thời người dùng có thể kiểm soát chính lưu lượng mà mình đã sử dụng để có thể đưa ra cách sử dụng hợp lý.

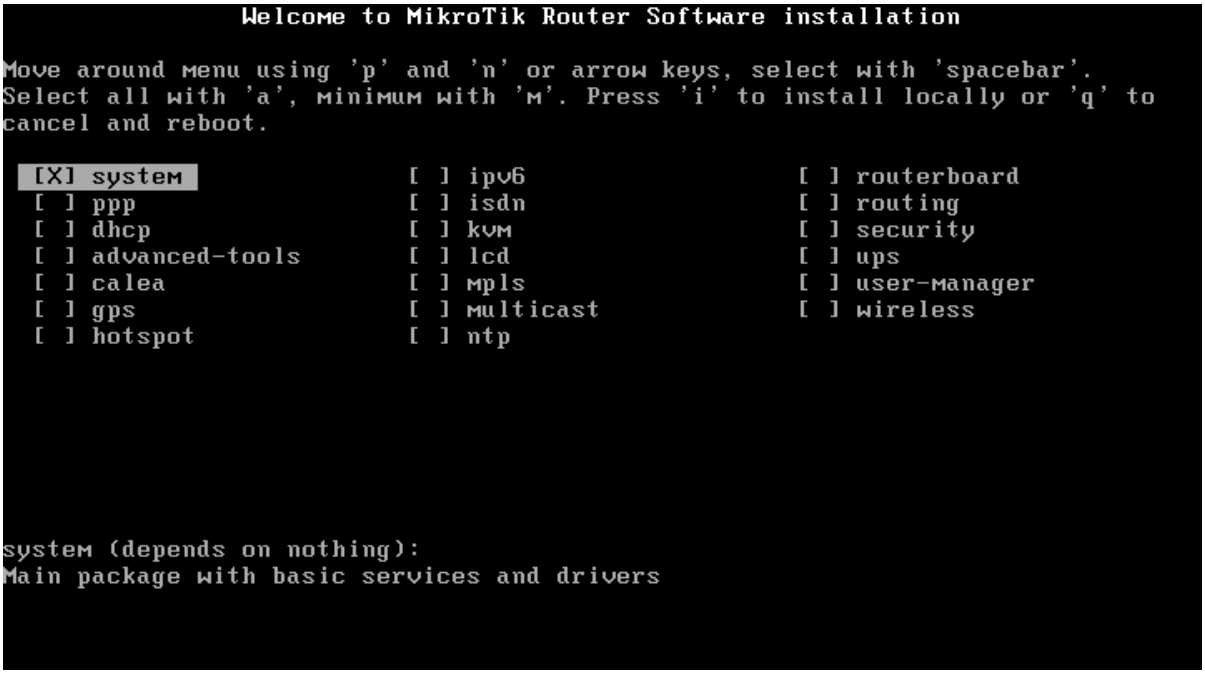
2.3 Cài đặt Mikrotik Router OS

- Chuẩn bị: Tải Mikrotik Router OS v6.0rc14 dành cho PC/x86 dưới dạng ISO (image cdrom) . Ghi file này ra đĩa CD dùng để cài đặt.

- Tùy chỉnh để PC khởi động từ ổ đĩa CD.

- Khởi động PC để bắt đầu cài đặt.

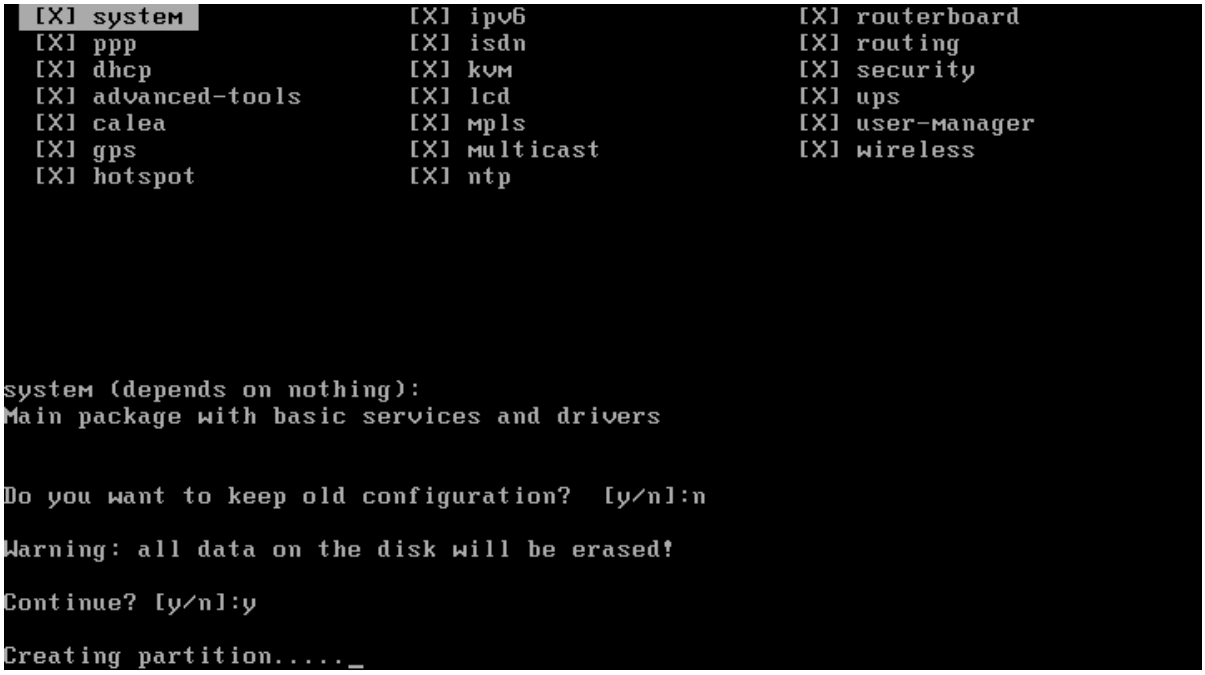
- Giao diện đầu tiên để chọn các thành phần mà người quản trị muốn.



Hình 2.5 Các tùy chọn cài đặt Mikrotik Router OS

- Dùng các phím P, N để di chuyển lên xuống, phím Space để chọn. Hoặc có thể ấn nút A để chọn tất cả.

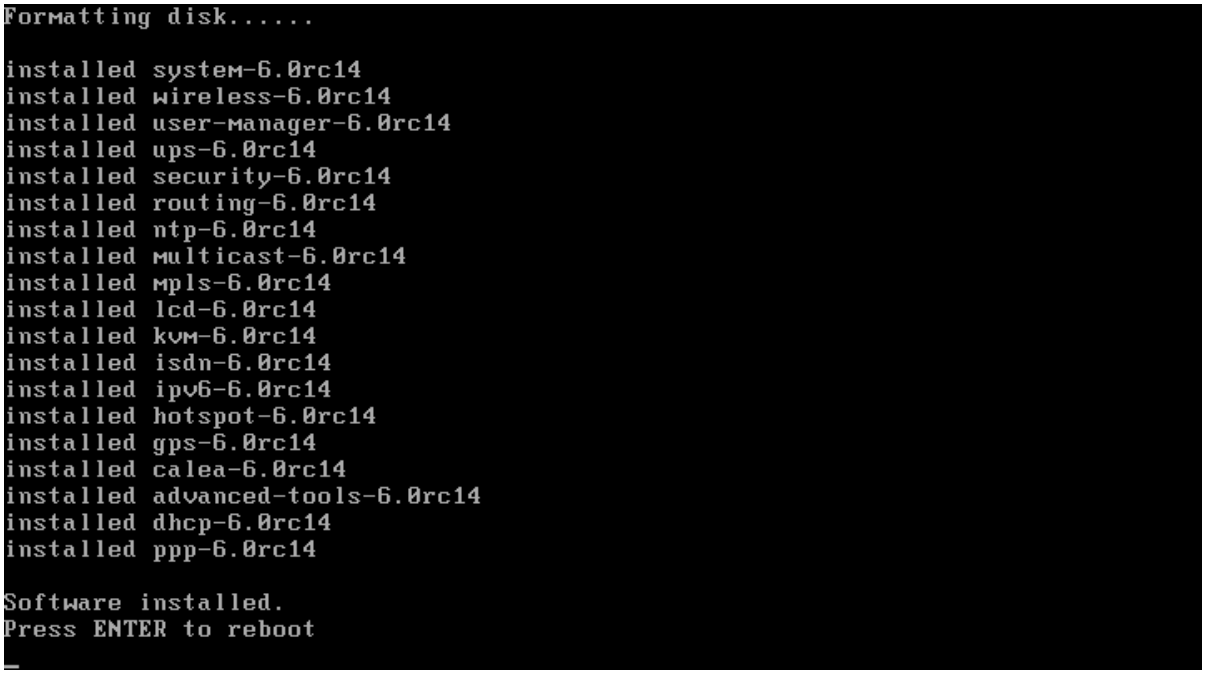
- Sau khi chọn xong ấn nút "I" để bắt đầu cài đặt.



Hình 2.6 Cài đặt Mikrotik Router OS

- Tiến trình cài đặt xuất hiện 2 câu hỏi.
    - Câu 1 chọn "Y" để giữ lại cấu hình cũ. "N" để bỏ qua.
    - Chọn "Y" để bắt đầu cài đặt.

- Sau khi quá trình cài đặt hoàn tất, lấy đĩa CD ra khỏi ổ CD và ấn Enter để khởi động lại máy tính.

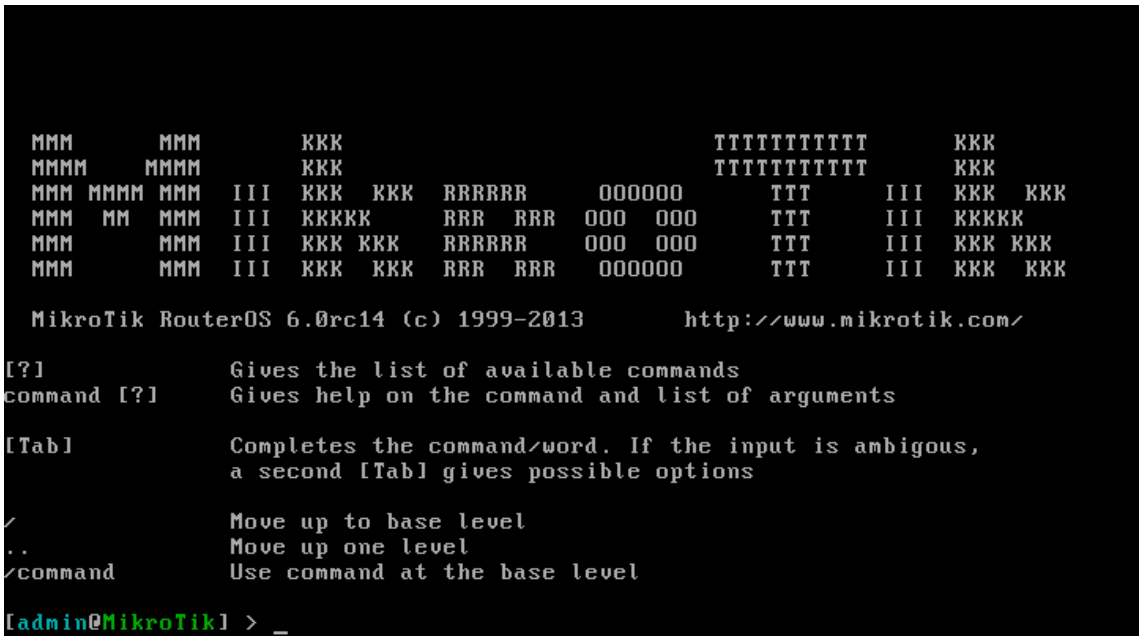


Hình 2.7 Hoàn tất cài đặt Mikrotik Router OS

- Quá trình cài đặt hoàn tất, màn hình hiện lên yêu cầu đăng nhập hệ thống. Ta sử dụng tài khoản admin và mật khẩu để trắng để đăng nhập lần đầu tiên.

Hình 2.8 Giao diện đăng nhập Mikrotik Router OS

- Giao diện chính sau khi đăng nhập:



Hình 2.9 Giao diện chính Mikrotik Router OS

2.4 Cấu hình Mikrotik Router OS sử dụng giao diện command line

2.4.1 Cấu hình địa chỉ IP

- Máy tính cần đảm bảo có 2 card mạng (NIC) còn hoạt động tốt. Ta cấu hình IP cho NIC 1 kết nối với internet (NIC WAN).

- Cấu hình IP ra Internet của NIC 1 là: 192.168.0.150/24

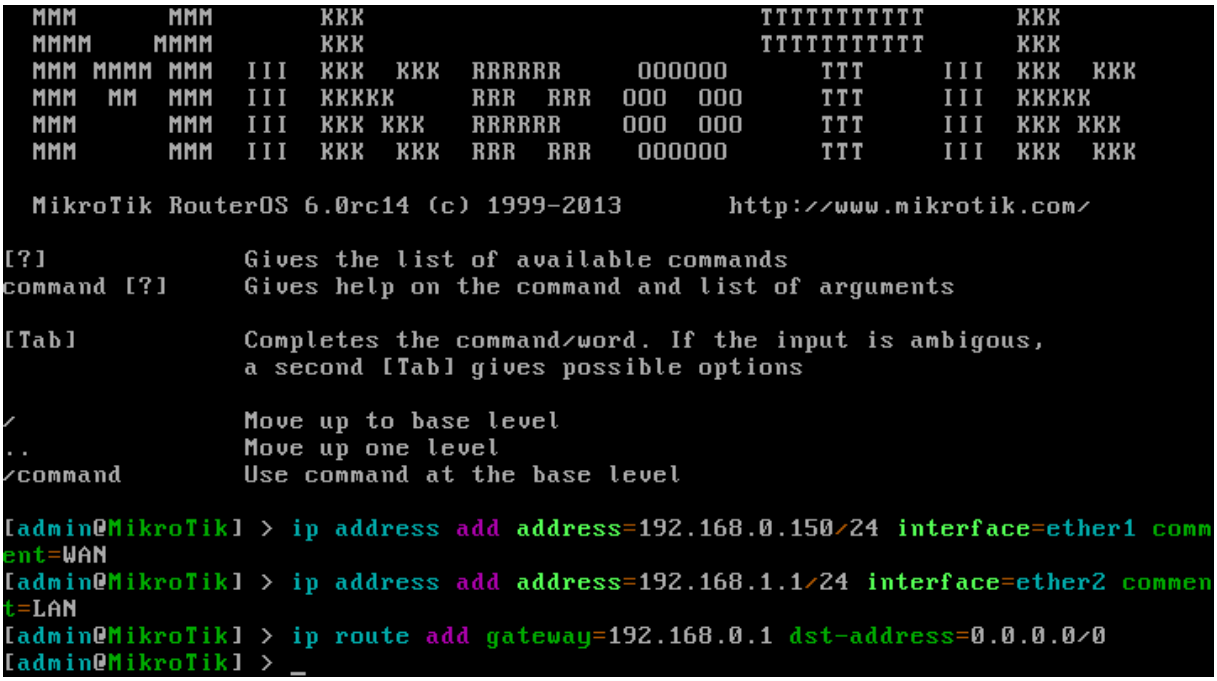
[admin@MikroTik] >/ip address add address=192.168.0.150/24 interface=ether1 comment=WAN

- Cấu hình IP cho NIC 2 kết nối với các AP hay mạng LAN của các máy con là 192.168.1.1/24.

[admin@MikroTik] >/ip address add address=192.168.1.1/24 interface=ether2 comment=LAN

- Cấu hình địa chỉ IP cho gateway là 192.168.0.1 và những yêu cầu nào gateway không biết sẽ được trỏ thẳng ra internet qua địa chỉ 0.0.0.0/0

[admin@MikroTik] > ip route add gateway=192.168.0.1 dst-address=0.0.0.0/0



Hình 2.10 Cấu hình IP cho Mikrotik OS

2.4.2 Cấu hình dhcp-server

- Thêm các thông tin DNS cho máy chủ. Nếu trong mạng có máy chủ DNS thì ta thêm địa chỉ máy chủ này vào.

[admin@MikroTik] /ip dns set servers=203.162.0.182,8.8.8.8,8.8.4.4

- Gõ lệnh sau để hiển thị các dòng yêu cầu nhập thông tin dhcp-server:

[admin@MikroTik] > ip dhcp-server setup

dhcp server interface: ether2

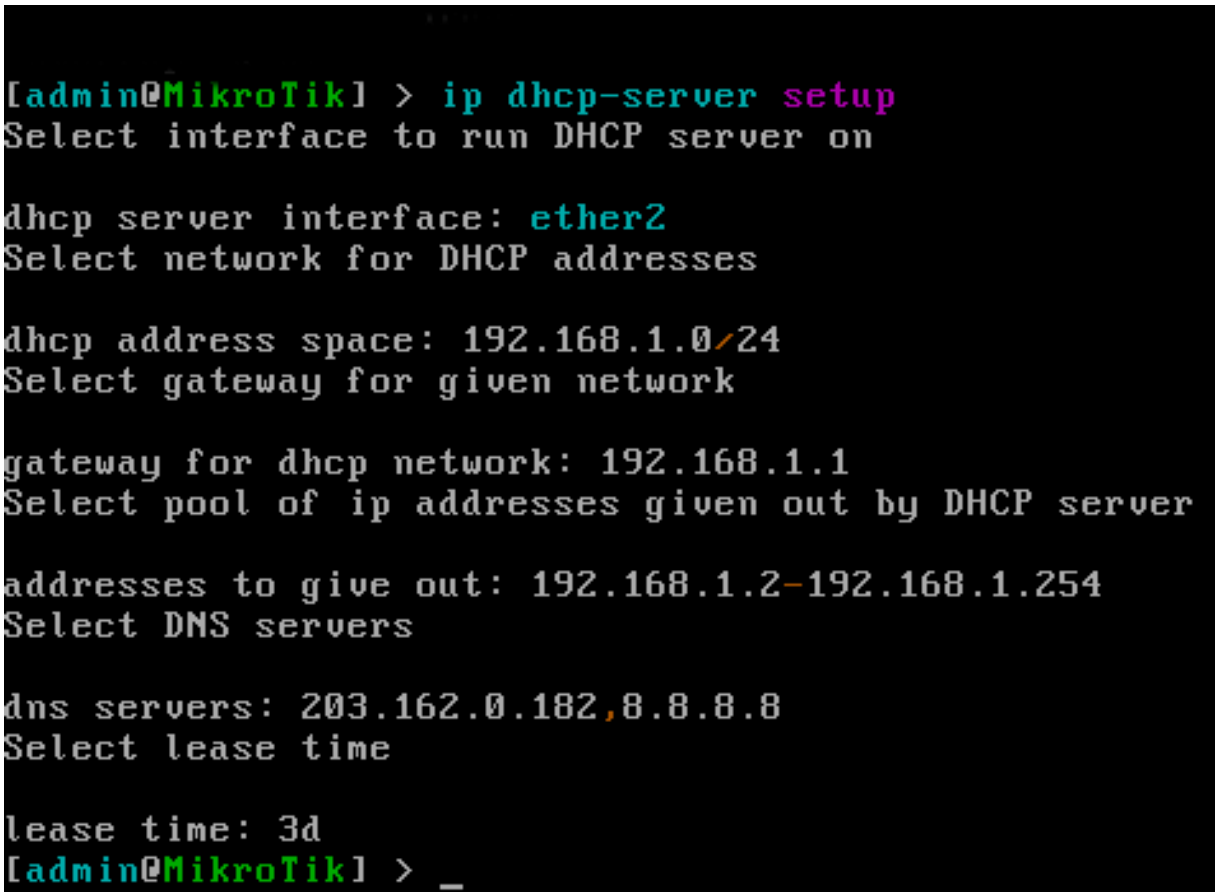
dhcp address space: 192.168.1.0/24

gateway for dhcp network: 192.168.1.1

addresses to give out: 192.168.1.2-192.168.1.254 (Đây là dải IP mà dịc vụ dhcp sẽ cấp cho các máy con khi kết nối)

dns servers: 203.162.0.182,8.8.8.8 (Ở đây nhập địa chỉ IP của máy chủ DNS server, nếu trong mạng có máy chủ DNS thì nhập IP của máy chủ đó. Nếu không thì nhập ip primary và second dns server cách nhau bởi dấu phẩy)

lease time: 3d (Thời gian cho thuê mặc định là 03 ngày)



Hình 2.11 Cấu hình dhcp-server

2.4.3 Cấu hình Hotspot

- Gõ lệnh sau để hiển thị các dòng yêu cầu nhập thông tin hotspot:

[admin@MikroTik] > ip hotspot setup

hotspot interface: ether2

local address of network: 192.168.1.1/24

masquerade network: yes

address pool of network: 192.168.1.2-192.168.1.254

select certificate: none *(mặc định xuất hiện dòng import-other-certificate, chúng ta xóa dòng đó và nhập vào none)*

ip address of smtp server: 0.0.0.0 *(Nếu trong mạng có máy chủ smtp thì nhập địa chỉ của máy chủ đó vào, nếu không có thì để mặc định là 0.0.0.0)*

dns servers: 203.162.0.182,8.8.8.8

dns name:

name of local hotspot user: user *(Tạo account cho hệ thống dùng để đăng nhập hotspot)*

password for the user: 123 *(Mật khẩu của tài khoản trên).*

```
[admin@MikroTik] > ip hotspot setup
Select interface to run HotSpot on

hotspot interface: ether2
Set HotSpot address for interface

local address of network: 192.168.1.1/24
masquerade network: yes
Set pool for HotSpot addresses

address pool of network: 192.168.1.2-192.168.1.254
Select hotspot SSL certificate

select certificate: none
Select SMTP server

ip address of smtp server: 0.0.0.0
Setup DNS configuration

dns servers: 203.162.0.182,8.8.8.8
DNS name of local hotspot server

dns name:
Create local hotspot user

name of local hotspot user: user
password for the user: 123
[admin@MikroTik] > _
```

Hình 2.12 Cấu hình Hotspot

2.4.4 Cấu hình NAT

[admin@MikroTik] > ip firewall nat add chain=srcnat action=masquerade out-interface=ether1

Hình 2.13 Cấu hình NAT

2.4.5 Một số lệnh cơ bản

- Lệnh thay đổi mật khẩu tài khoản admin

[admin@MikroTik] >> password

old-password: (Để trắng nếu thay đổi mật khẩu lần đầu)

new-password: (Mật khẩu mới)

confirm-new-password: (Gõ lại mật khẩu mới)

- Lệnh liên quan IP, gateway

[admin@MikroTik] > ip address print detail

[admin@MikroTik] > ip route print detail

- Lệnh xóa địa chỉ IP khi nhập sai:

[admin@MikroTik] > ip route remove x

[admin@MikroTik] > ip address remove x

(Trong đó x là số thứ tự của IP, số thứ tự đánh từ 0 trở lên)

- Lệnh tắt và khởi động lại máy:

[admin@MikroTik] >> system reboot

Reboot, yes? [y/N]: (Chọn Y để khởi động lại)

[admin@MikroTik] >> system shutdown

Reboot, yes? [y/N]: (Chọn Y để tắt máy)

- Lệnh thiết lập lại toàn bộ cấu hình

[admin@MikroTik] > system reset

Dangerous! Reset anyway? [y/N]: (Chọn Y để thực hiện)

2.5 Cấu hình hệ thống Hotspot với giao diện GUI thông qua Winbox

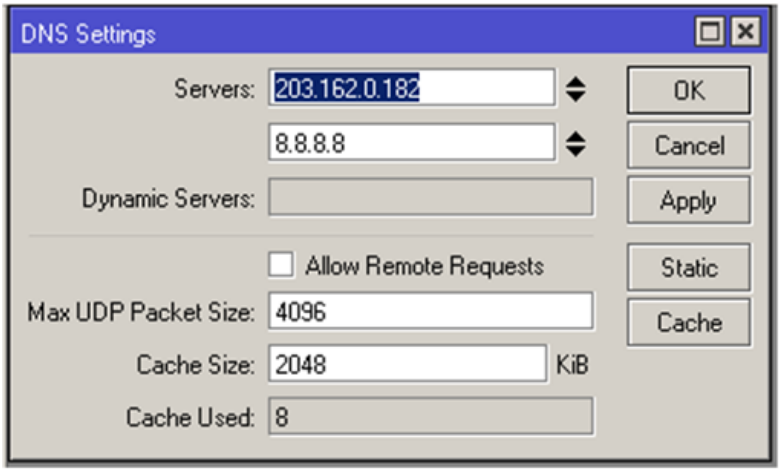
Sau khi cài đặt xong Mikrotik Router OS, ta cấu hình địa chỉ IP (như trong phần 2.4.1). Sử dụng phần mềm Winbox trên một máy tính khác trong cùng mạng để kết nối tới máy chủ Mikrotik qua địa chỉ IP của NIC1 (NIC WAN).

Hình 2.14 Giao diện Winbox

2.5.1 Cấu hình DNS và dhcp-server

- Trong menu chính chọn IP>DNS

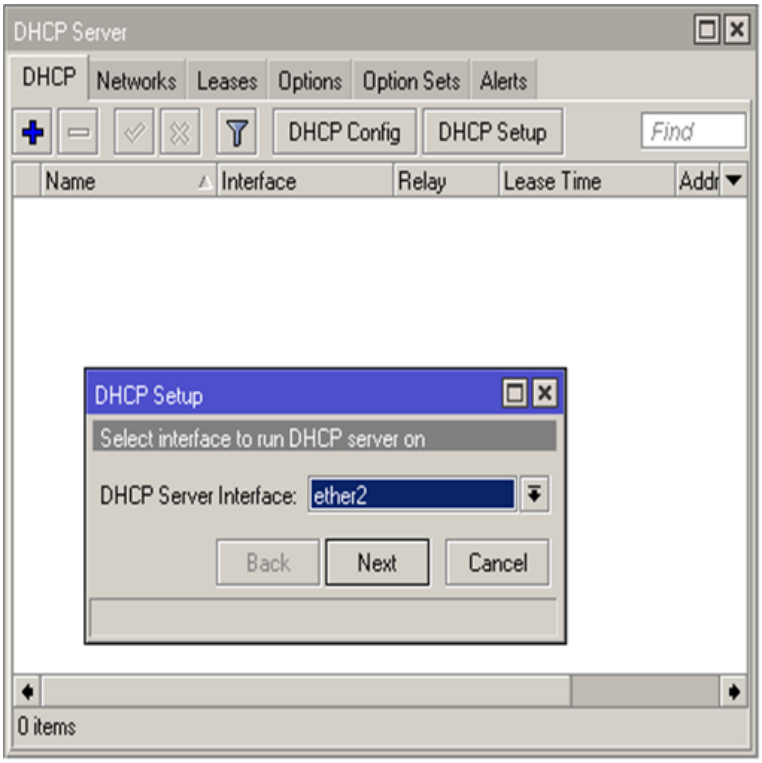
- Trong bảng DNS Settings điền thông tin DNS như hình dưới. Nếu trong mạng có máy chủ DNS thì điền IP của máy chủ đó vào.



Hình 2.15 Cấu hình DNS bằng giao diện GUI

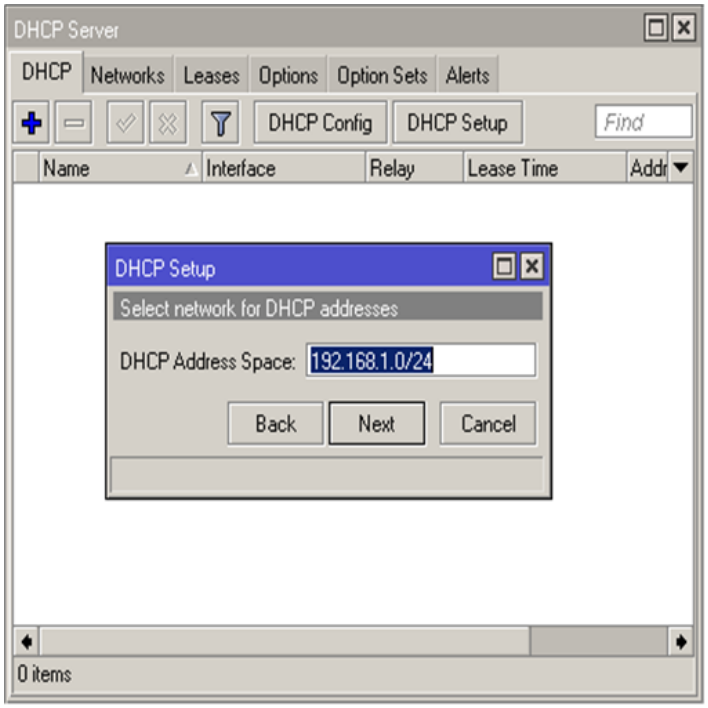
- Từ menu chính bên trái chọn IP>DHCP Server

- Trong bảng DHCP Server chọn DHCP Setup và làm theo hình dưới:



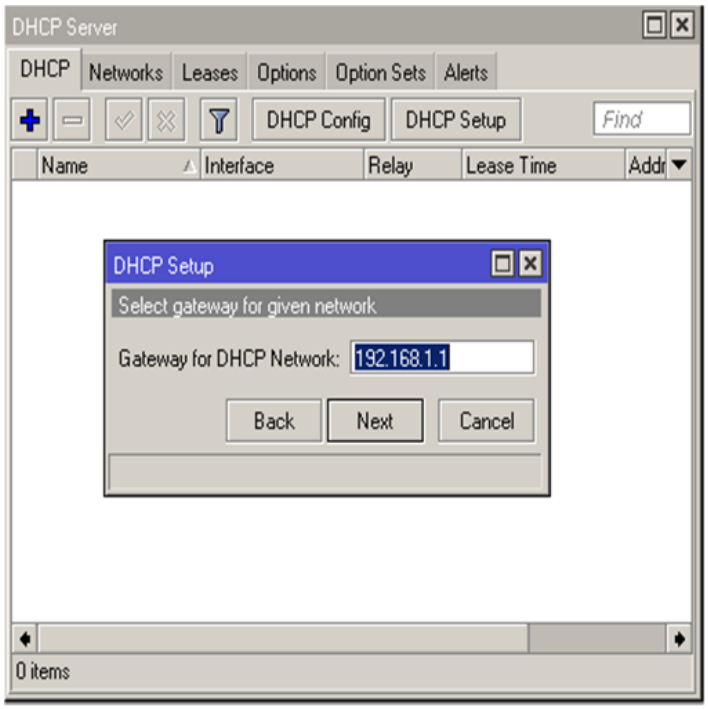
Hình 2.16 Cấu hình DHCP Server qua giao diện GUI

- Trong mục DHCP server Interface chọn ether2. Nhấn Next để tiếp tục.



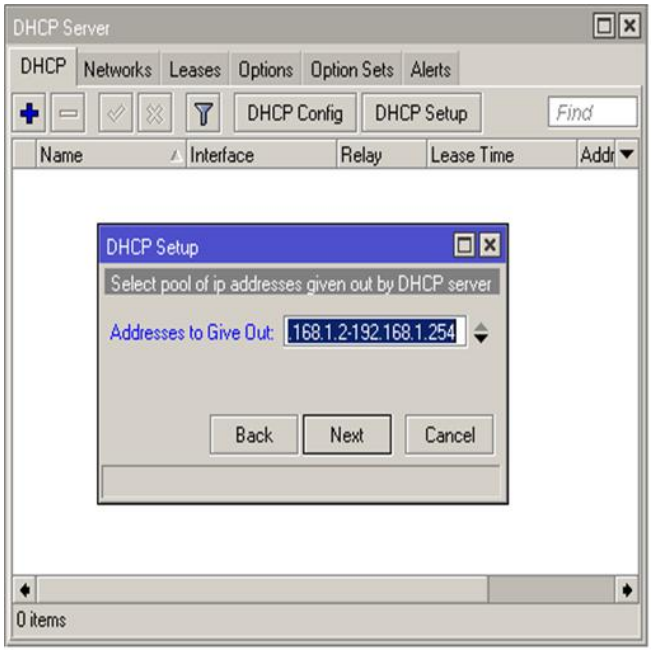
Hình 2.17 Cấu hình DHCP Server qua giao diện GUI

- Giữ nguyên địa chỉ Gateway và chọn Next



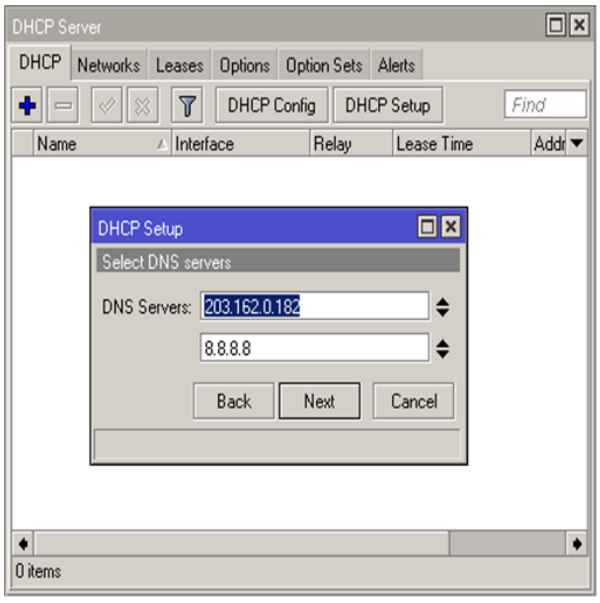
Hình 2.18 Cấu hình DHCP Server qua giao diện GUI

- Dãy địa chỉ IP DHCP sẽ cấp phát cho các client khi kết nối.



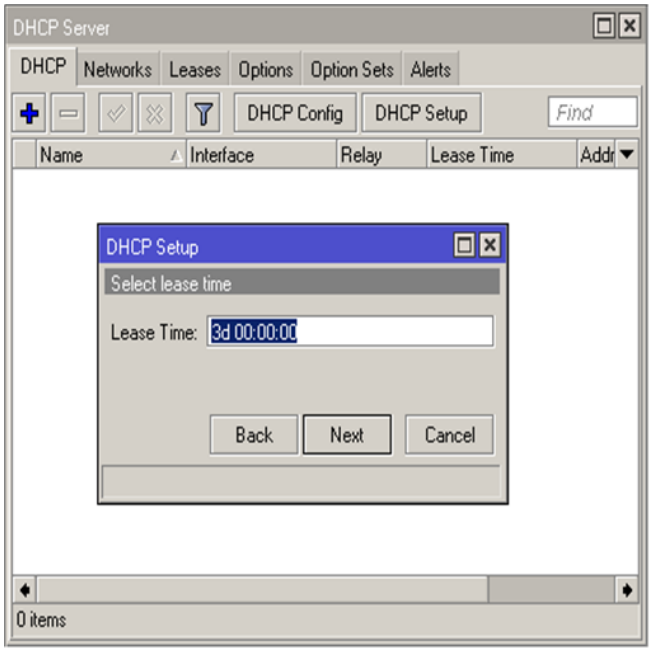
Hình 2.19 Cấu hình DHCP Server qua giao diện GUI

- Tiếp theo ta sẽ khai báo DNS, do đã thiết lập DNS ở trên nên ta để mặc định và nhấn Next.



Hình 2.20 Cấu hình DHCP Server qua giao diện GUI

- Chọn thời gian cho thuê địa chỉ IP, mặc định là 3 ngày. Nhấn Next để tiếp tục. Cuối cùng chọn OK để hoàn thành quá trình cấu hình dịch vụ DHCP Server.

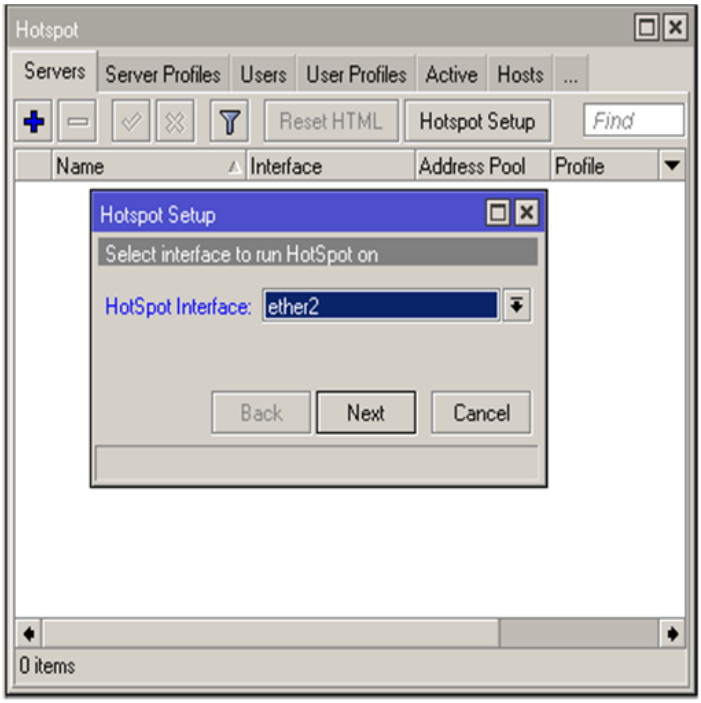


Hình 2.21 Cấu hình DHCP Server qua giao diện GUI

2.5.2 Cấu hình Hotspot

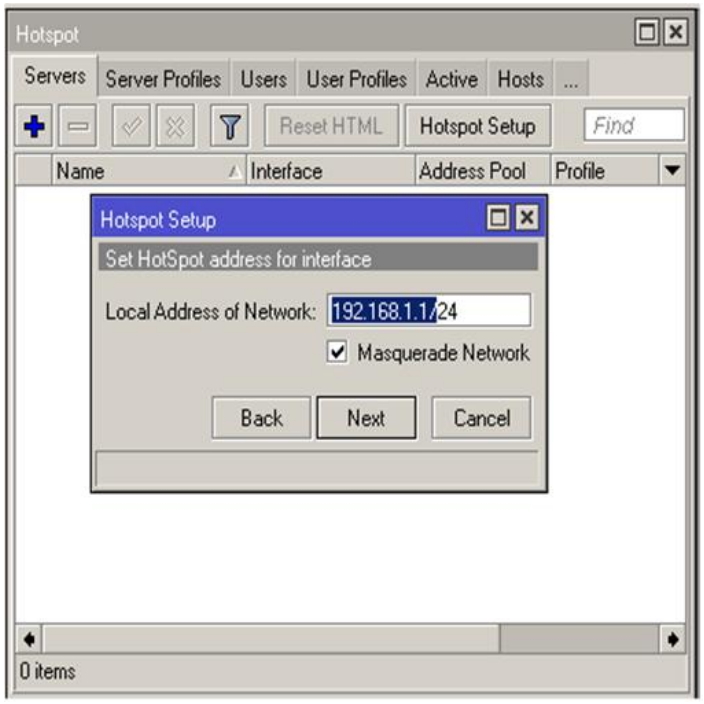
- Từ menu chính bên trái chọn: IP > Hotspot

- Trong bảng Hotspot chọn Hotspot Setup



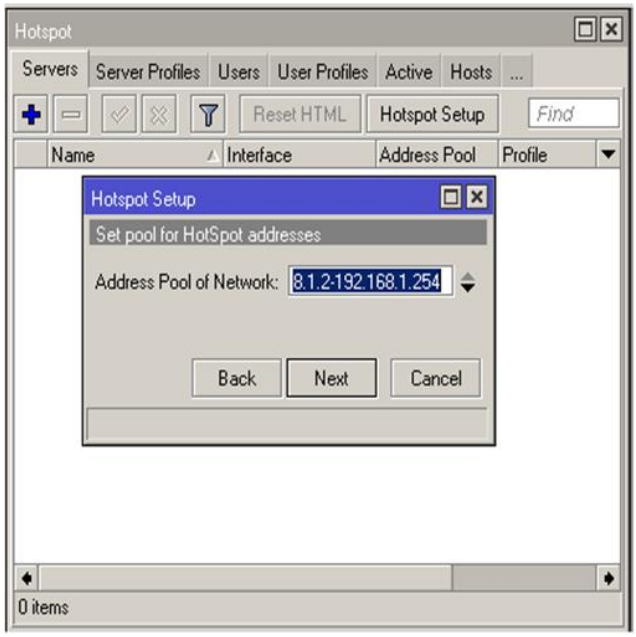
Hình 2.22 Cấu hình Hotspot qua giao diện GUI

- Trong mục Hotspot Interface chọn ether2. Nhấn Next để tiếp tục.



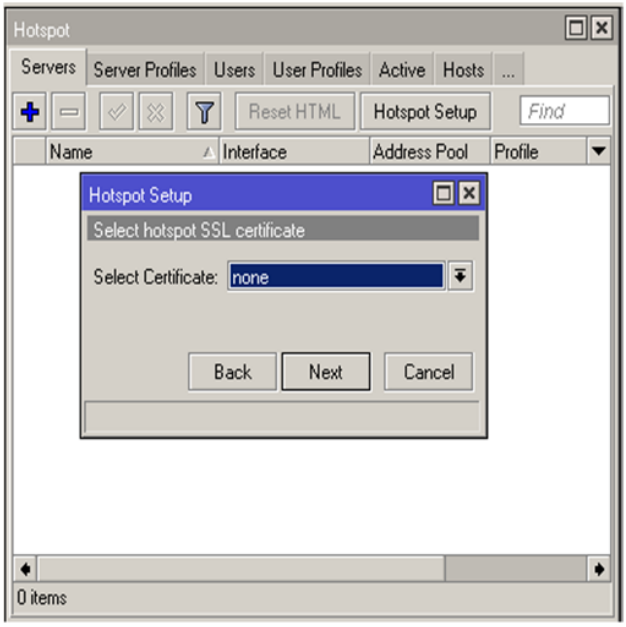
Hình 2.23 Cấu hình Hotspot qua giao diện GUI

- Giữ nguyên giá trị Local Address of Network. Nhấn Next để tiếp tục.



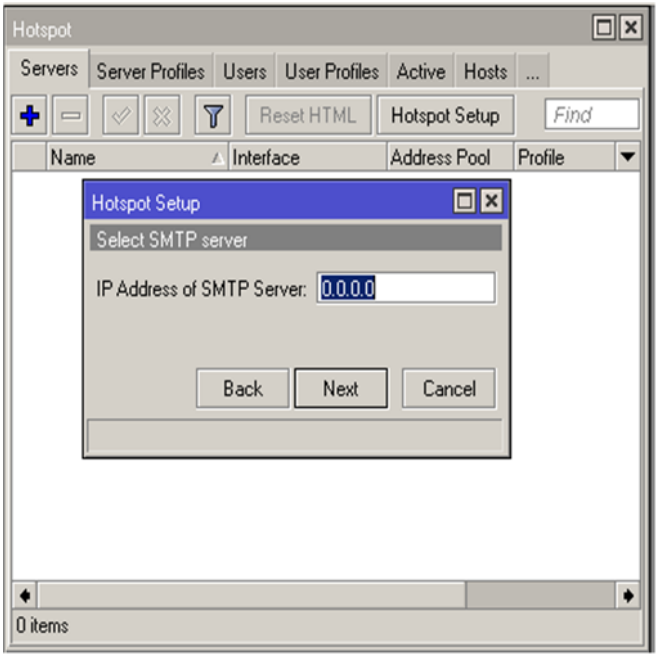
Hình 2.24 Cấu hình Hotspot qua giao diện GUI

- Address Pool of Network là dải địa chỉ IP mà hotspot sẽ cấp cho client khi tham gia vào mạng. Nhấn Next để tiếp tục.



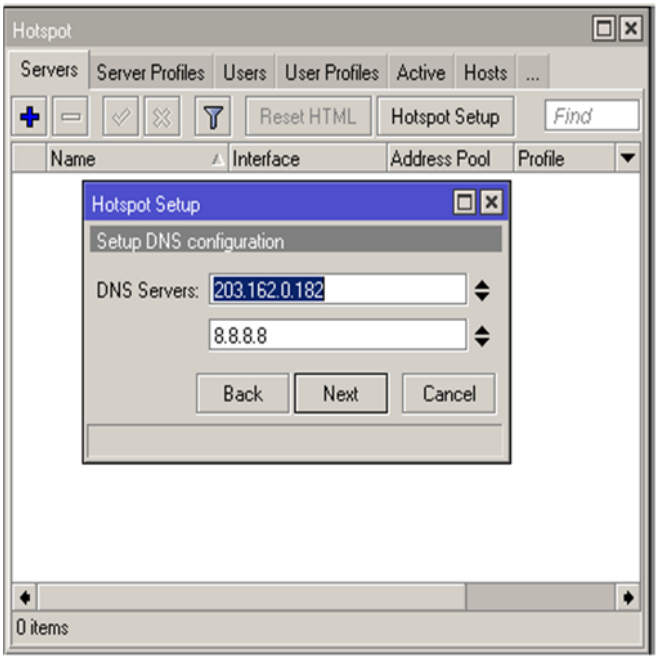
Hình 2.25 Cấu hình Hotspot qua giao diện GUI

- Chọn none cho Select Certificate. Nhấn Next để tiếp tục.



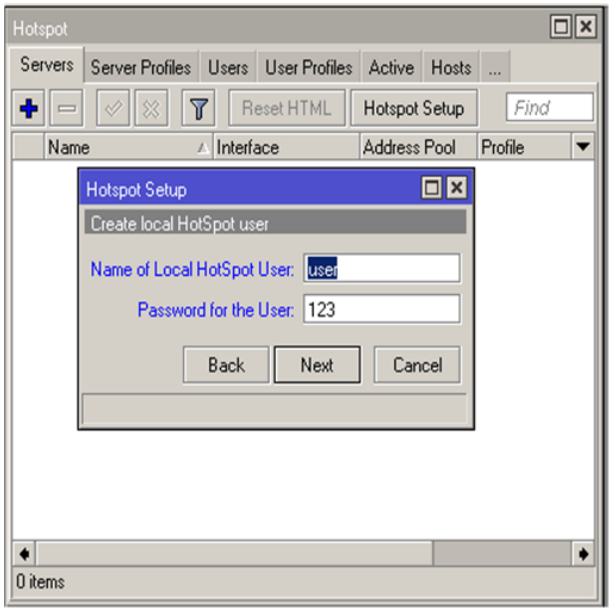
Hình 2.26 Cấu hình Hotspot qua giao diện GUI

- Nhập địa chỉ máy chủ SMTP. Nhấn Next để tiếp tục.



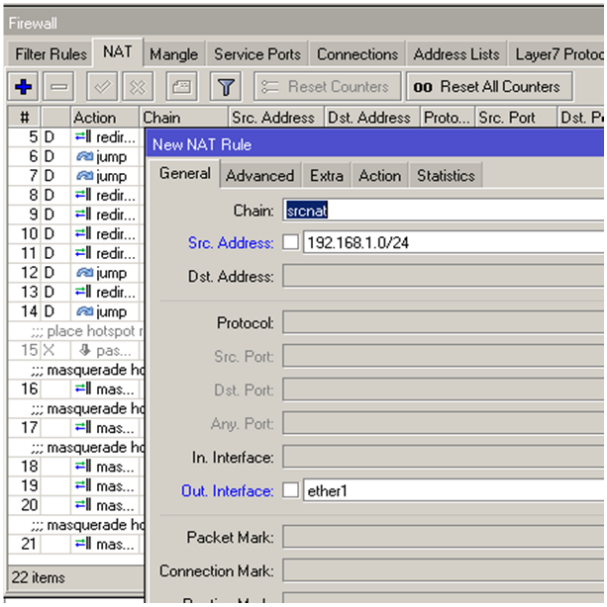
Hình 2.27 Cấu hình Hotspot qua giao diện GUI

- Nhập địa chỉ của máy chủ DNS và tiếp tục.



Hình 2.28 Cấu hình Hotspot qua giao diện GUI

- Nhập tên của máy chủ DNS nếu có, hoặc để trắng nếu trong mạng không có máy chủ DNS Server. Nhấn Next để tiếp tục.

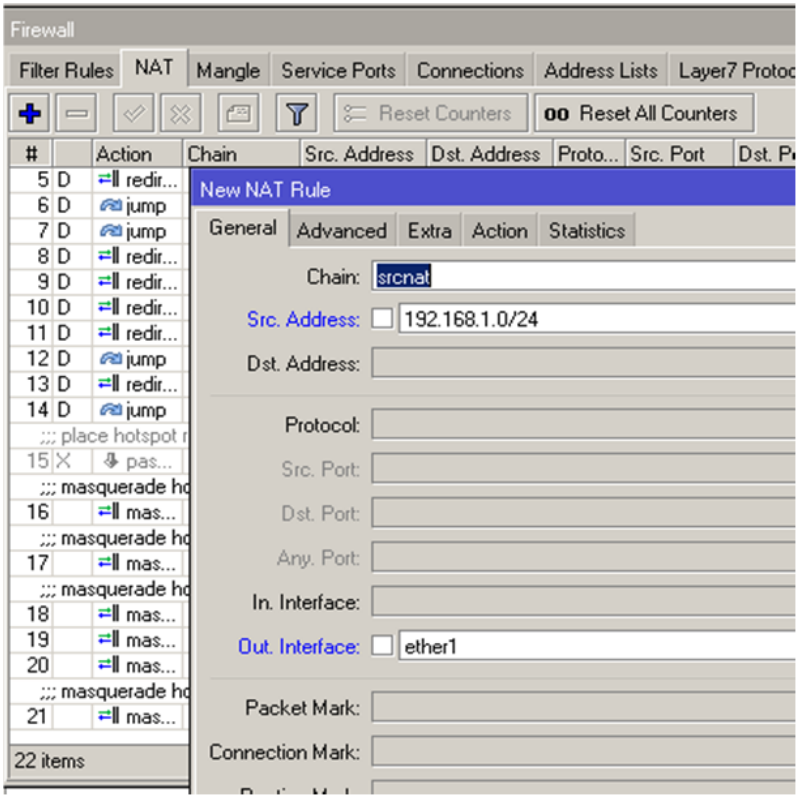


Hình 2.29 Cấu hình Hotspot qua giao diện GUI

- Nhập tên của tài khoản Hotspot và mật khẩu. Đây là tài khoản dùng để đăng nhập thử Hotspot. Nhấn Next để tiếp tục. Nhấn Ok để kết thúc quá trình cài đặt Hotspot.

2.5.3 Cấu hình NAT

- Trên menu chính bên trái chọn: IP > Firewall. Trong bảng Firewall chọn tab NAT. Nhấp + để thêm.



Hình 2.30 Cấu hình NAT thông qua giao diện GUI

- Chain= srcnat

- Src.Address= 192.168.1.0/24 (Đây là dải IP mà DHCP sẽ cấp cho các máy con khi kết nối vào mạng).

- Out.Interface = ether1 (NIC WAN)

- Tiếp theo chọn tab Action, chọn Action=Masquerade. Nhấn Apply để áp dụng, OK để hoàn thành.

2.6 Cấu hình Radius

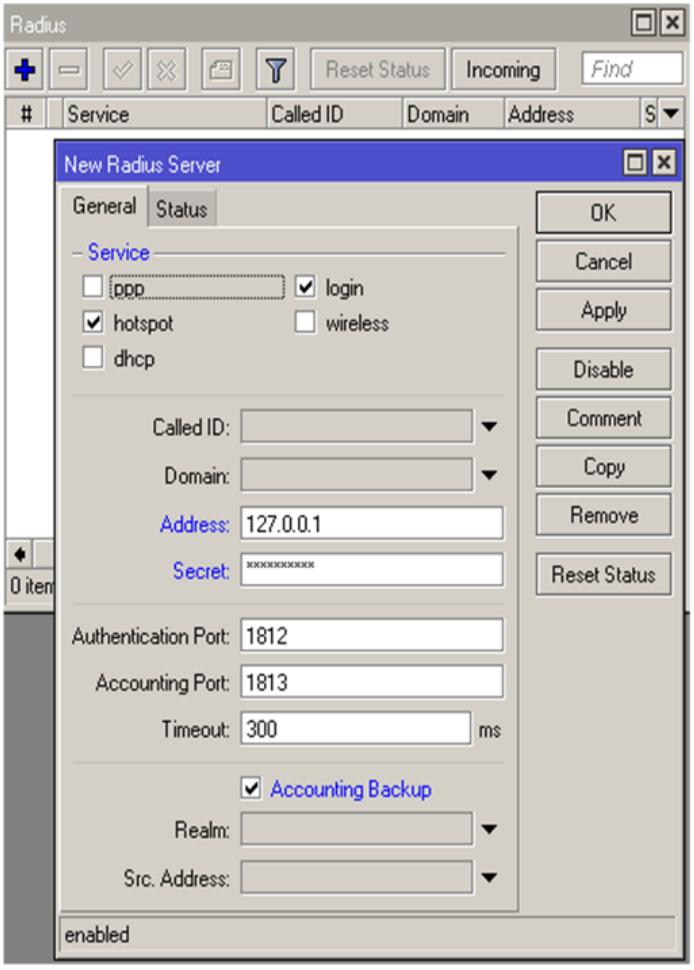
Trong menu chính bên trái chọn : Radius

Trong bảng Radius chọn thêm radius

Trong bảng New Radius Server:

- Chọn hotspot, login trong mục Services
- Address: 127.0.0.1
- Secret:hpu.edu.vn

- Chọn Accounting backup



Hình 2.31 Cấu hình Radius qua giao diện GUI

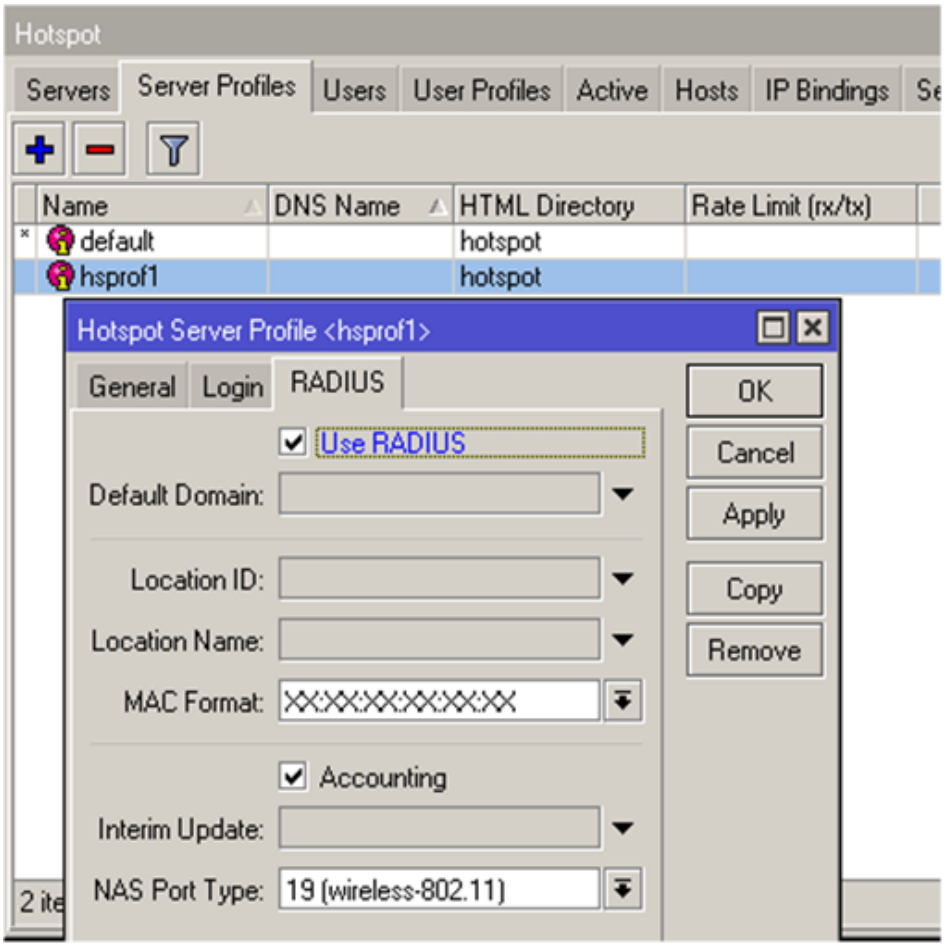
Chọn Apply và Ok để hoàn thành thêm Radius

Trong menu chính bên trái chọn : IP>Hotspot

Trong bảng Hotspot, chọn tab Server Profile

Nhấp chọn profile: hsprof1 để bảng cấu hình Hotspot Server Profile

Trong tab Radius chọn Use RADIUS



Hình 2.32 Cấu hình Radius qua giao diện GUI

Nhấp Apply và Ok để hoàn thành.

Thực hiện tương tự đối với Profile default

Đăng nhập trang quản trị User manager với địa chỉ: 192.168.0.150 với tài khoản admin và mật khẩu để trống.

Thêm một Router với thông tin sau:

- Name: HS
- Ip address:127.0.0.1
- Shared secret: hpu.edu.vn

Hình 2.33 Cấu hình Radius qua giao diện GUI

CHƯƠNG 3: THỰC NGHIỆM VÀ TRIỂN KHAI HỆ THỐNG

3.1 Đặt vấn đề

Hệ thống mạng không dây của trường Đại học Dân Lập Hải Phòng đã được xây dựng từ những năm 2008 và không ngừng được nâng cấp, lắp mới điểm phát sóng hàng năm. Từ khi xây dựng cho đến nay, hệ thống mạng vẫn hoạt động dựa trên sự "tự giác" của người dùng (bao gồm cả Sinh viên và CBCNV), trong những giai đoạn đầu hệ thống hoạt động tốt và đem lại hiệu quả cao. Tuy nhiên, trong thời gian 3 kỳ học gần đây (kỳ 1, 2 năm 2012 và kỳ 1 năm 2013), phòng Quản trị mạng nhận được khá nhiều ý kiến đến từ Sinh viên, Cán bộ giảng viên... phản hồi về chất lượng cũng như những sự cố thường xuyên gặp phải khi sử dụng mạng không dây. Có những thời điểm hầu hết các điểm truy cập (Access Point) không thể phục vụ. Nhiều người sử dụng các ứng dụng hỗ trợ download chiếm băng thông lớn, gây tê liệt hệ thống dẫn đến những lãng phí không đáng có và sự mất công bằng giữa các người sử dụng. Người vào trước thì sử dụng "vô tội vạ", người chậm chân thì không có khả năng "chen chân" vào mạng.

Trước thực trạng như vậy, Ban lãnh đạo nhà trường đã yêu cầu phòng Quản trị mạng xây dựng phương án quản lý wifi mới nhằm đảm bảo các yêu cầu chính như sau:

- Phục vụ đúng người dùng trong trường (hơn 7700 Sinh viên và hơn 300 Giảng viên, các cán bộ nhân viên khác...) thông qua tài khoản, mật khẩu cho từng đối tượng.
- Đảm bảo quyền lợi mỗi cá nhân khi tham gia sử dụng mạng wifi phải công bằng, được đảm bảo những nhu cầu cơ bản nhất phục vụ công tác nghiên cứu giảng dạy, học tập, trao đổi thông tin, tra cứu tài liệu...
- Tối ưu hệ thống, tránh lãng phí, khai thác tối đa nguồn lực hiện có.
- Xây dựng cơ chế phù hợp để tiến tới áp dụng hình thức thu phí trong quá trình phục vụ của mạng không dây sau này.

3.2 Một số giải pháp đề xuất

3.2.1 Phát triển trên Radius Of Windows

RADIUS (Remote Authentication Dial In User Service) là một giao thức được định nghĩa trong RFC 2586 với khả năng cung cấp xác thực tập trung, cấp phép và điều

khiển truy nhập (Authentication, Authorization, và Access Control – AAA) cho các phiên làm việc với SLIP và PPP Dial-up – như việc cung cấp xác thực của các nhà cung cấp dịch vụ Internet (ISP) đều dựa trên giao thức này để xác thực người dùng khi họ truy cập Internet. Nó cần thiết trong NAS Network Access Server để làm việc với username và password cho việc cấp phép.

Giao thức Remote Authentication Dial In User Service (RADIUS) được định nghĩa trong RFC 2865 như sau: Với khả năng cung cấp xác thực tập trung, cấp phép và điều khiển truy cập (Authentication, Authorization, và Accounting – AAA) cho các phiên làm việc với SLIP và PPP Dial-up –như việc cung cấp xác thực của các nhà cung cấp dịch vụ Internet (ISP) đều dựa trên giao thức này để xác thực người dùng khi họ truy cập Internet.

Nó cần thiết trong tất cả các Network Access Server (NAS) để làm việc với danh sách các username và password cho việc cấp phép, RADIUS AccessRequest sẽ chuyển các thông tin tới một Authentication Server, thông thường nó là một AAA Server (AAA – Authentication, Authoriztion, và Accounting).

Trong kiến trúc của hệ thống nó tạo ra khả năng tập trung các dữ liệu, thông tin của người dùng, các điều kiện truy cập trên một điểm duy nhất (single point), trong khi có khả năng cung cấp cho một hệ thống lớn, cung cấp giải pháp NASs.

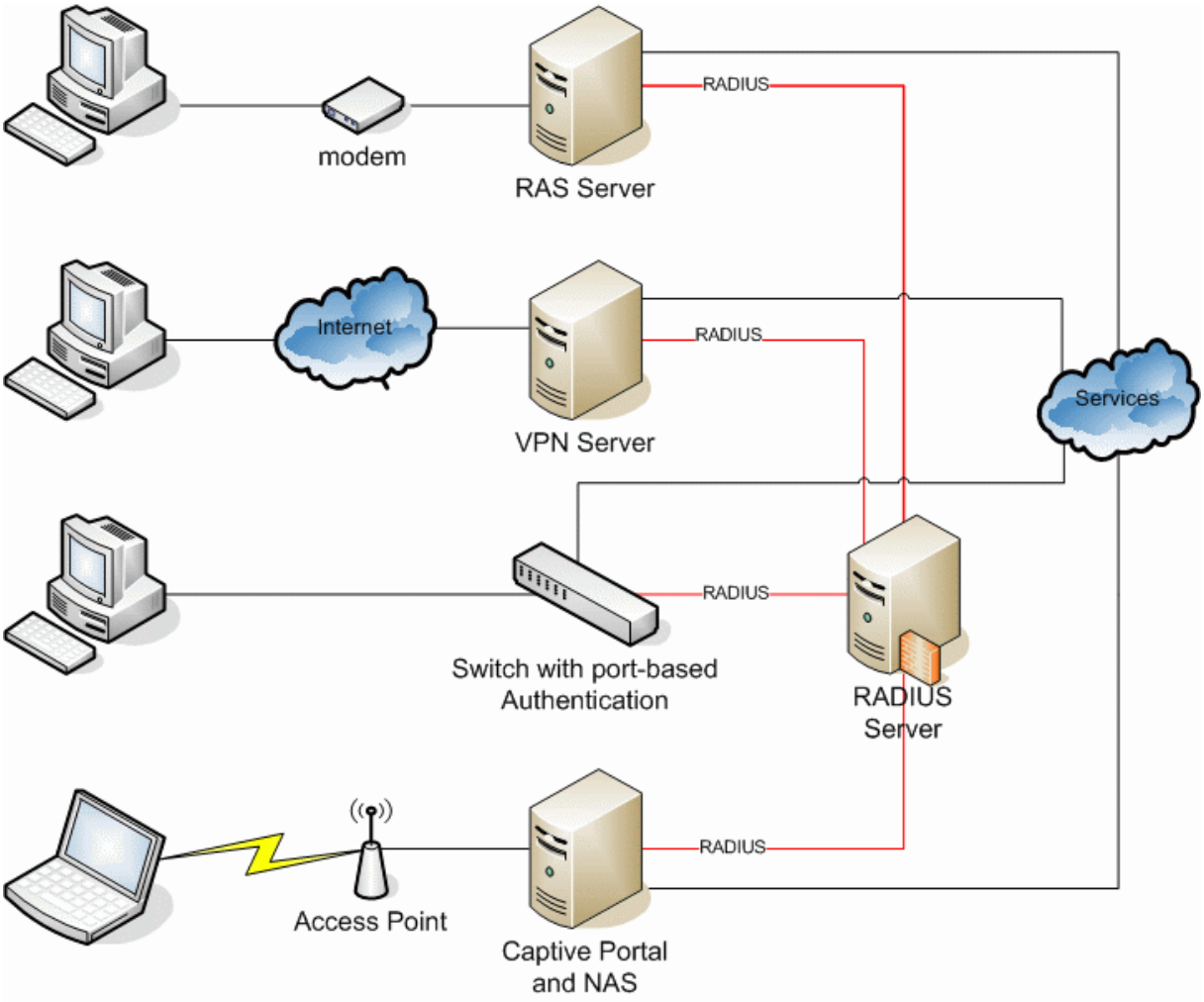
Khi một user kết nối, NAS sẽ gửi một message dạng RADIUS Access-Request tới máy chủ AAA Server, chuyển các thông tin như username và password, thông qua một port xác định, NAS identify, và một message Authenticator.

Sau khi nhận được các thông tin máy chủ AAA sử dụng các gói tin được cung cấp như NAS identify, và Authenticator thẩm định lại việc NAS đó có được phép gửi các yêu cầu đó không. Nếu có khả năng, máy chủ AAA sẽ tìm kiểm tra thông tin username và password mà người dùng yêu cầu truy cập trong cơ sở dữ liệu. Nếu quá trình kiểm tra là đúng thì nó sẽ mang một thông tin trong AccessRequest quyết định quá trình truy cập của user đó là được chấp nhận.

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 sẽ chuyển thông tin đến người dùng từ xa (với ví dụ này sử dụng CHAP). Khi đó người dùng sẽ phải trả lời đúng các yêu cầu xác nhận (trong ví dụ này, đưa ra lời đề nghị mã hoá password), sau đó NAS sẽ chuyển tới máy chủ AAA một message RADIUS Access-Request.

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 thoả mãn máy chủ AAA sẽ trả về một tin RADIUS Access-Reject và NAS sẽ ngắt kết nối với user.

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



Hình 3.1 Mô hình xác thực giữa Client và RADIUS Server

+ **Ưu điểm:**

- Khả năng xác thực mạnh mẽ, độ tin cậy cao được sử dụng phổ biến trên khắp thế giới.
- Khả năng tương thích cao với hệ thống mạng có sẵn của trường.
- Tài liệu hướng dẫn cài đặt và vận hành đầy đủ.

+ **Nhược điểm**

- Yêu cầu một Server có cấu hình cao chạy hệ điều hành Windows Server 2000/2003/2008 do đó khoản tiền nhà trường phải đầu tư mua Server mới và bản quyền Windows Server là khá lớn.
- Với khuyến cáo trong việc triển khai Radius Server bằng phương thức sử dụng Windows Server của Microsoft thì sẽ đáp ứng được trong khoảng 500 người dung đối với mỗi Server. Như vậy với khoảng 8000 cán bộ giảng viên và sinh viên của trường thì cần khoảng 10 Radius Server.

3.2.2 Phát triển trên FreeRadius

FreeRadius là một mô đun có hiệu suất cao được phát triển và phân phối miễn phí dưới GNU General Public License v.2. Hiện nay FreeRadius là máy chủ mã nguồn mở được triển khai rộng rãi nhất trên thế giới. Ngoài khả năng cung cấp các tính năng xác thực như Radius of windows, FreeRadius còn tương thích với hầu hết các cơ sở dữ liệu như LDAP, MySQL, PostgreSQL, Oracle…

+ **Ưu điểm**

- Được cung cấp miễn phí
- Có thể được hỗ trợ từ cộng đồng người sử dụng phát triển rộng lớn.

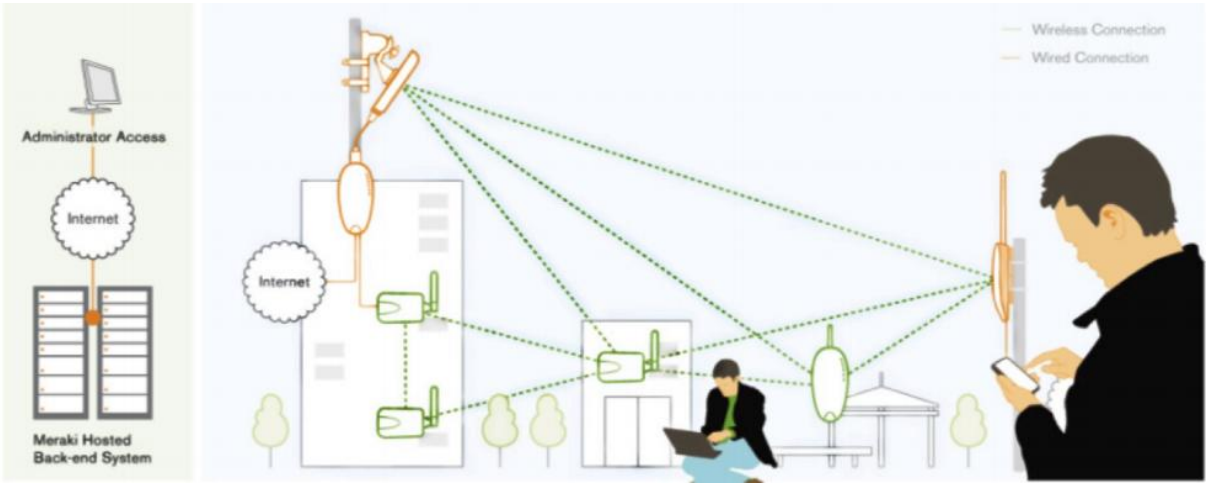
+ **Nhược điểm**

- Cần một Server cấu hình mạnh sử dụng nhân Linux hoặc Unix.
- Khó tiếp cận do hệ thống mạng của trường được xây dựng trên nền tảng Windows.
- Mặc dù chưa có con số cụ thể số người dùng mà một FreeRadius Server chạy trên nền tảng mã nguồn mở có thể đáp ứng, nhưng đã có kết quả khoảng 1000 trong một số thực nghiệm được đưa ra. Như vậy để đáp ứng được yêu cầu của nhà trường thì cần khoảng 5 Server.

3.2.3 Sử dụng giải pháp của Meraki

Meraki một giải pháp quản lý wifi của một công ty Meraki, công ty này được thành lập từ năm 2006 bởi các thành viên của phòng thí nghiệm khoa học máy tính

thuộc Viện CNTT Massachusett (MIT). Meraki vốn được hỗ trợ bởi 2 quỹ Sequoia Capital và Google Inc. Công ty cung cấp các giải pháp, công nghệ wifi, chuyển mạch, an ninh và quản lý thiết bị di động từ đám mây. Các giải pháp này phù hợp với các doanh nghiệp tầm trung. Hiện Meraki được được mua lại bởi Cisco.



Hình 3.2 Mô hình Mesh của Meraki

Meraki cung cấp công nghệ mạng với các tính năng "cấu hình tự động, hồi phục sóng tự động, load-balancing tự động và báo động sự cố tự động", đặc biệt được quản lý trực tuyến với webbased controller tiện lợi và "được hỗ trợ FREE".

THIẾT BỊ: Trang nhã, gọn nhẹvà bền bỉ. Chuẩn a/b/g/N tương thích hoàn toàn với nhau, sóng phủ theo hình quảcầu (360^o), tạo thành "ma trận sóng dày & mạnh, hạn chế "điểm chết" (dead-spot) .

TRIỂN KHAI: Rất dễdàng và đơn giản (giảm thiểu việc chạy cáp mạng đến thiết bị) nhờ truyền sóng l3 bước không dây, riêng thiết bị MR58 có thể truyền sóng 10 bước không dây. Vì vậy rất có lợi cho việc triển khai mạng diện rộng.

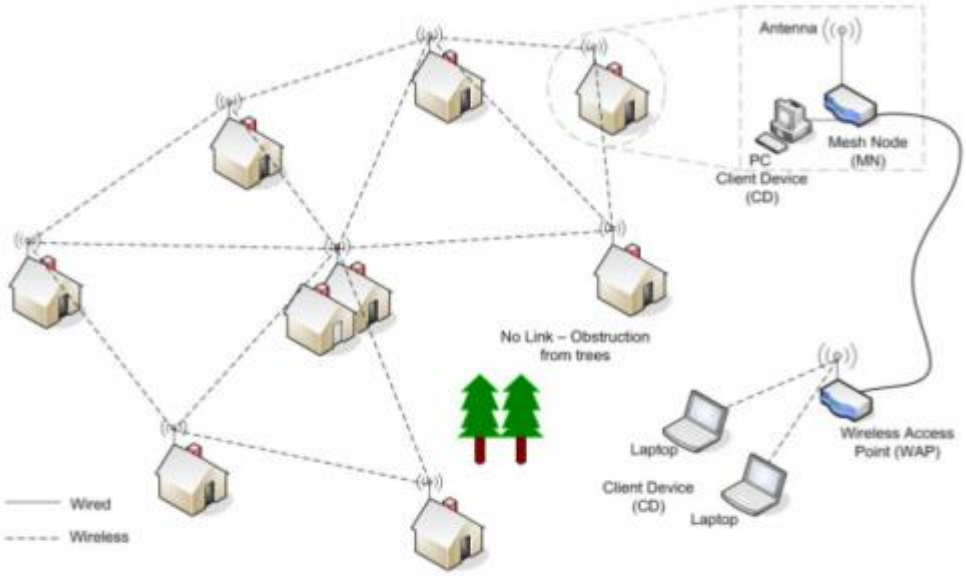
HOẠT ĐỘNG MẠNG: Rất ổn định và độ tin cậy cao nhờ các tính năng vượt trội của công nghệ MESH độc đáo có một không hai:

Tự động cấu hình (self-configuring): khi cắm vào nguồn điện là thiết bị tự động cấu hình và tự động nối kết với các thiết bị trong cùng mạng để tạo mesh. Nếu bị mất nguồn điện hoặc Internet và có trở lại sau đó, mạng hay thiết bị sẽ tự động cấu hình lại rất nhanh.

Tự động khôi phục sóng (self-healing): mạng tự cấu hình lại sau mỗi 30 giây để tìm đường sóng nhanh nhất cho mỗi node. Vì vậy, nếu có thiết bị nào bịyếu sóng thì sẽ được khôi phục ngay sau đó. Nếu có thiết bị bị gián đoạn hoạt động (do mất nguồn), khu vực đó vẫn có sóng của những node khác phủ đến nên người sử dụng không bị gián đoạn.

Tự động cân bằng tải (auto load-balancing):Mạng Meraki tự động cân bằng tải giữa các gateway và giữa các nodes với nhau nên giảm bớt tình trạng quá tải tại một khu vực.

Tự động báo động (self-notifying):chức năng cập nhật thông báo trước sự cố cho người quản trị mạng để kịp thời sửa chữa trước khi khách hàng than phiền.



Hình 3.3 Mô hình Mesh

- Một số giải pháp bảo mật của hãng thứ 3 khác:
- Aradial WiFi - http://www.aradial.com
- Bridgewater Wi-Fi AAA - http://www.bridgewatersystems.com
- Cisco Secure Access Control Server - http://www.cisco.com/
- Funk Odyssey - http://www.funk.com/
- IEA RadiusNT - http://www.iea-software.com/
- Infoblox RADIUS One Appliance - http://www.infoblox.com/
- Interlink Secure XS - http://www.interlinknetworks.com/
- LeapPoint AiroPoint Appliance - http://www.leappoint.com/
- Meetinghouse AEGIS - http://www.mtghouse.com/
- OSC Radiator - http://www.open.com.au/radiator/
- Vircom VOP Radius - http://www.vircom.com

3.2.4 Mikrotik Router Os

- Mikrotik Router OS được phát triển bởi công ty Mikrotik. Công ty này thành lập năm 1995 tại thủ đô Riga, Latvia. Công ty chuyên phát triển các thiết bị định tuyến và hệ thống IPS không dây. Công ty hiện cung cấp cả các thiết bị phần cứng và các giải pháp phần mềm để kết nối internet cho hầu hết các nước trên thế giới.

- Trang chủ: http://www.mikrotik.com

- Mikrotik Router OS là hệ điều hành phần cứng của RouterBOARD Mikrotik. Nó cũng có thể được đặt trên một máy tính độc lập và sẽ biến máy tính đó thành một bộ định tuyến với tất cả các tính năng cần thiết như: Định tuyến, tường lửa, quản lý băng thông, điểm truy cấp không dây...

- Hiện Mikrotik router os đang dừng lại ở phiên bản chính thức là v5.25. Phiên bản không chính thức là v6.0rc14. Hiện em đang sử dụng phiên bản v6.0rc14 để demo trong quá trình thực hiện đồ án.

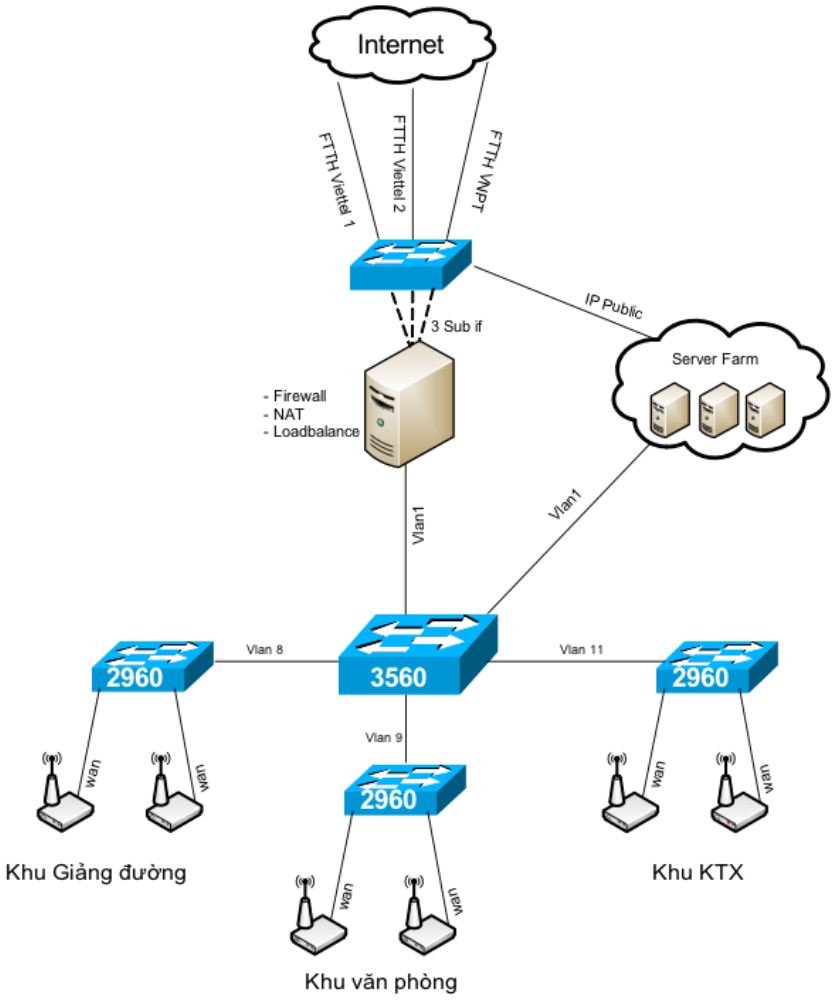
- Mikrotik router os từ phiên bản 5.0 trở về sau được xây dựng dựa trên Linux kernel version 2.6.35. Do vậy dung lượng của OS nhỏ, có thể ghi vào đĩa CD hoặc thậm chí đĩa mini-cd.

- Liên kết tải: http://www.mikrotik.com/download

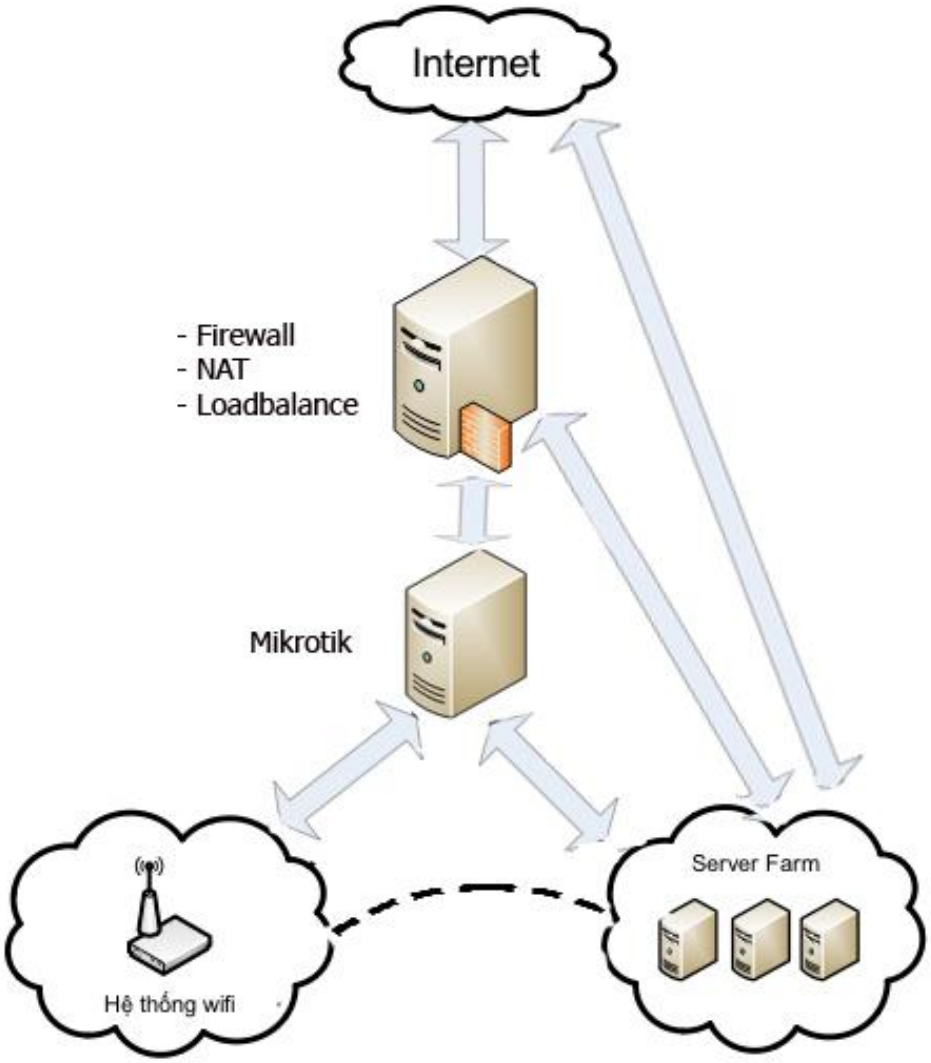
  - CD Image phiên bản v6.0rc14 có dung lượng 18.40 mb.
  - CD Image phiên bản v5.25 có dung lượng 20.85 mb.

3.3 Triển khai hệ thống quản lý mạng WLAN tại trường ĐHDL HP

3.3.1 Thiết kế logic



Hình 3.4: Hiện trạng hệ thống hiện tại



Hình 3.5: Sơ đồ logic sau khi triển khai Mikrotik

Thiết kế logic đảm bảo các yêu cầu:

- Mỗi người dùng được cung cấp một tài khoản mật khẩu.
- Giải quyết tình trạng các điểm phát sóng AP bị treo.
- Có khả năng tích hợp với hệ thống quản lý tài khoản tập trung.

3.3.2 Thông số cài đặt

Thông số phần cứng: Hệ thống được triển khai trên một Server IBM X236

CPU: Intel®Xeon™ 3.0 GHz/800 MHz

RAM: 2 GB (2x 1 GB) of 800 MHz DDR2 ECC

LAN: 02 Gigabit Ethernet onboard, 01 External RTL-8139/8139C/8139C

HDD: 30 Gb, 5400 RPM

Thông số phần mềm: Mikrotik Router Os version 5.20

3.3.3 Quá trình triển khai

- Phần mềm Mikrotik Router OS được triển khai một máy chủ IBM X236

- Nâng cấp firmware và cấu hình toàn bộ các điểm phát sóng từ cơ chế Router sang cơ chế AP (gồm 17 AP ở khu vực Giảng đường và 35 AP tại Khách sạn Sinh viên)

- Chia lại toàn bộ hệ thống thành 3 VLAN

• Vlan1: Các máy chủ được đặt tại Trường

• Vlan9: Các điểm phát sóng khu Giảng đường

• Vlan11: Các điểm phát sóng khu Khách sạn Sinh viên

- Chỉnh sửa cấu hình thiết bị mạng phù hợp với cách thức quản lý mới

- Tạo tài khoản nhóm và tài khoản người dùng; sinh viên, giảng viên, cán bộ, nhân viên,…

- Xây dựng chính sách đối với từng nhóm, người dùng; mỗi người sử dụng sẽ thuộc một nhóm và các chính sách về tốc độ, thời gian, lưu lượng được áp dụng thông qua các nhóm người dùng.

- Kiểm tra và hiệu chỉnh các thông số; các tham số thời gian lưu giữ phiên kết nối, kiểm soát các dịch vụ, giao thức cần lọc bỏ.

- Viết tài liệu hướng dẫn và hỗ trợ người dùng

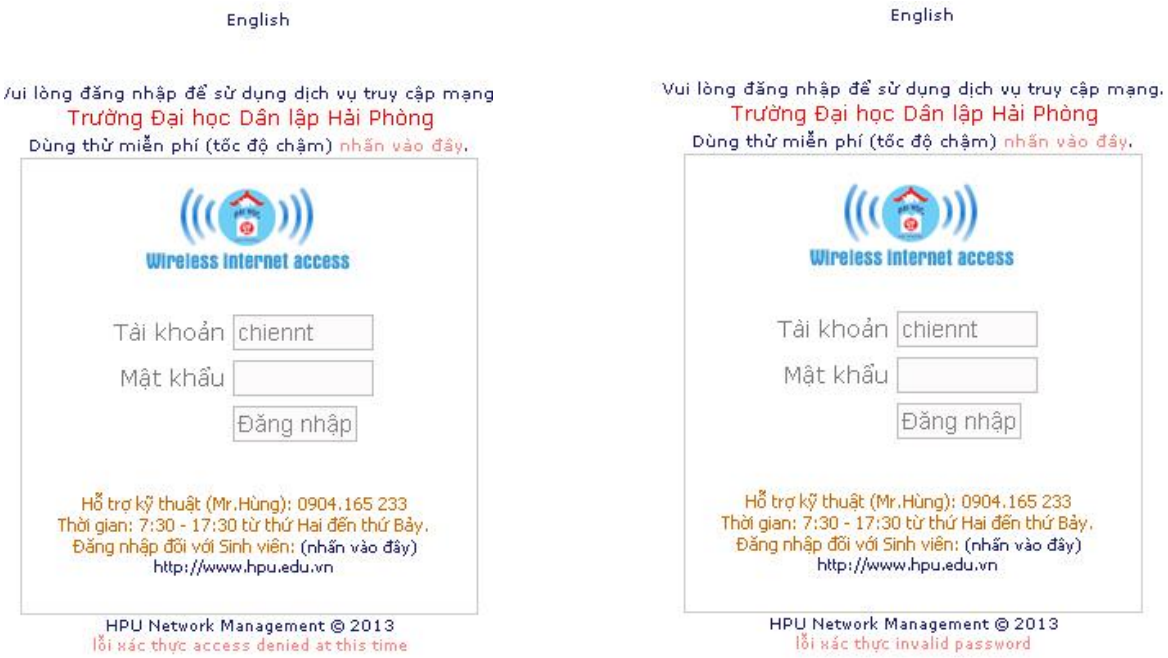
3.3.4 Một số hình ảnh về hệ thống.

Giao diện đăng nhập tiếng việt

Giao diện đăng nhập tiếng anh

Người dùng không hợp lệ

Có hơn 2 thiết bị sử dụng một tài khoản

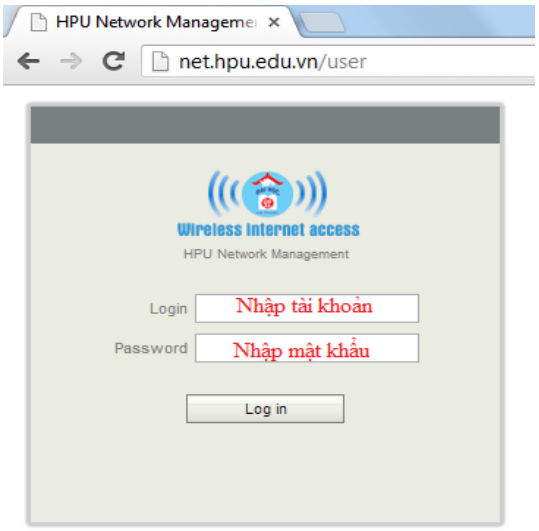


Không cho phép người dùng đăng nhập thời điểm nảy *Sai mật khẩu đăng nhập*

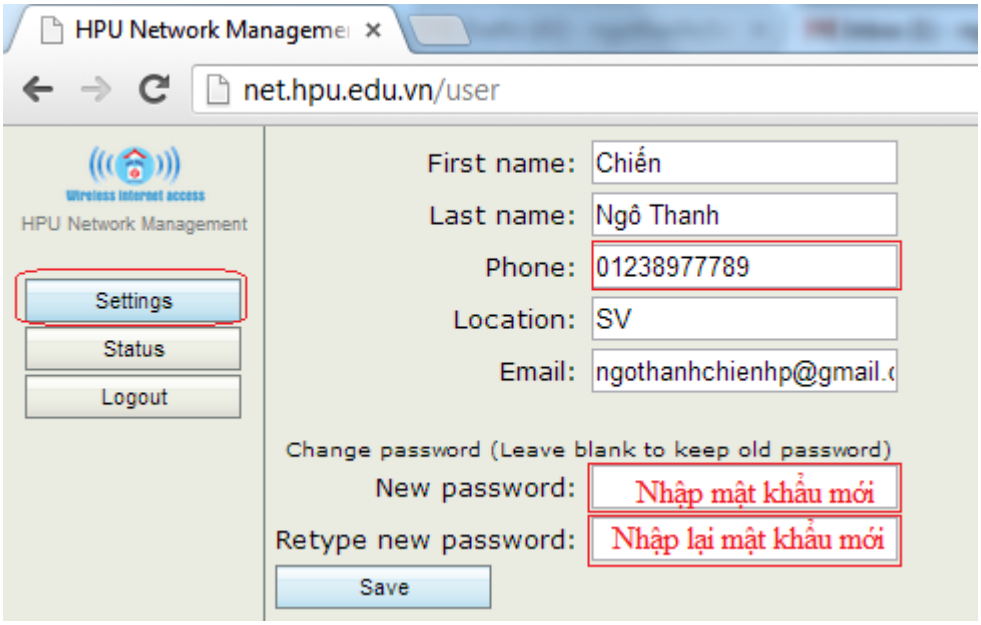
Hình 3.6: Giao diện đăng nhập và một số lỗi thường gặp

- Người sử dụng truy cập vào địa chỉ sau để đổi mật khẩu:

http://net.hpu.edu.vn/user



Hình 3.7: Thay đổi mật khẩu người dùng

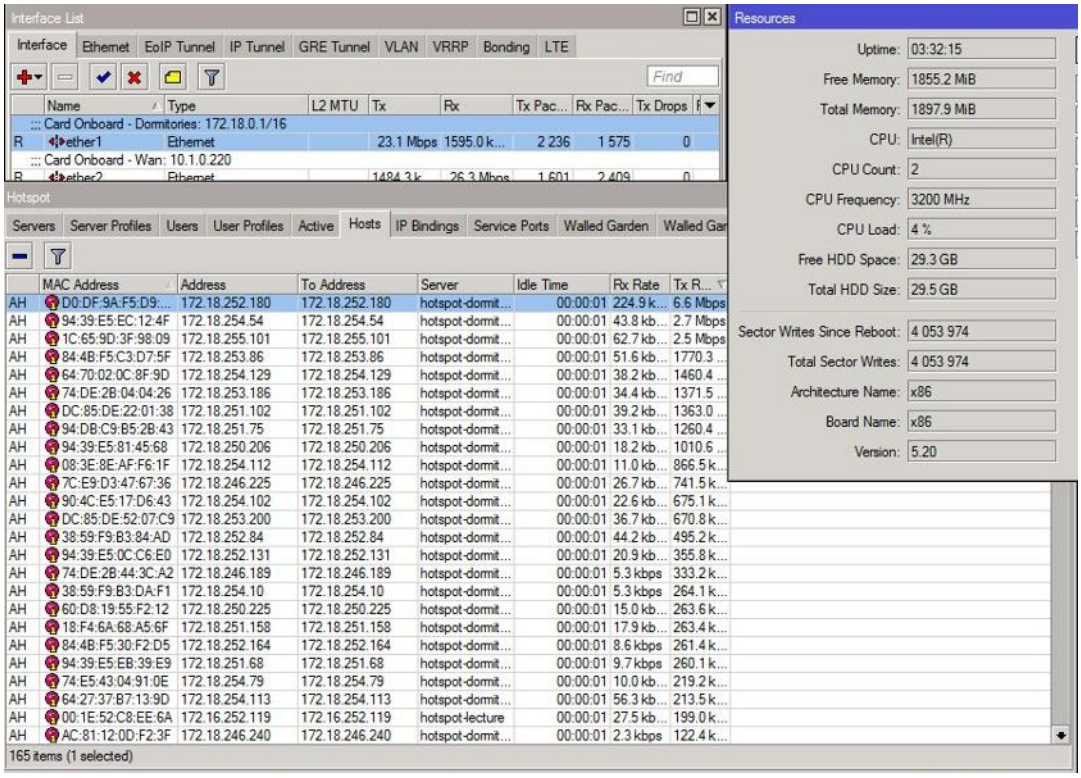


Hình 3.8: Thay đổi mật khẩu người dùng

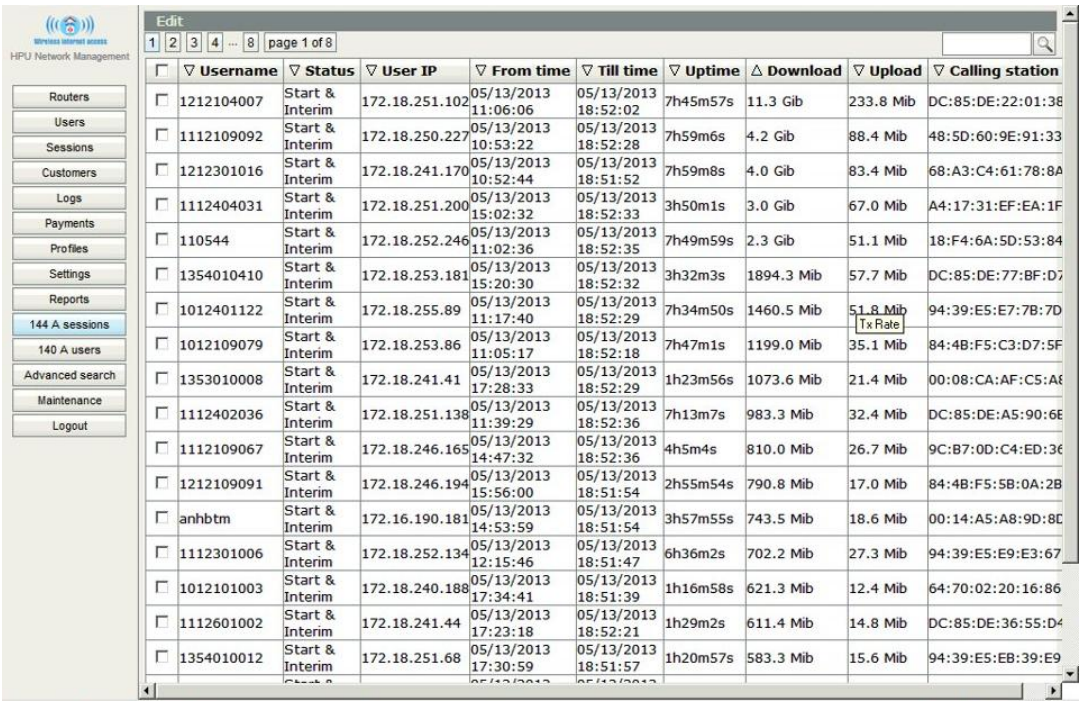
3.4 Kết quả đạt được

Hệ thống quản lý mạng không dây bước đầu đã đạt được một số kết quả nhất định:

- Quản lý mạng không dây tới từng người dùng
- Đáp ứng được các yêu cầu đặt ra từ lãnh đạo Nhà trường
- Giải quyết được sự cố treo thiết bị trong cách thức quản lý trước đây, tăng số lượng người sử dụng đồng thời, tận dụng tối đa tài nguyên hiện có.



- *Hình 3.9 Năng lực hệ thống Mikrotik*

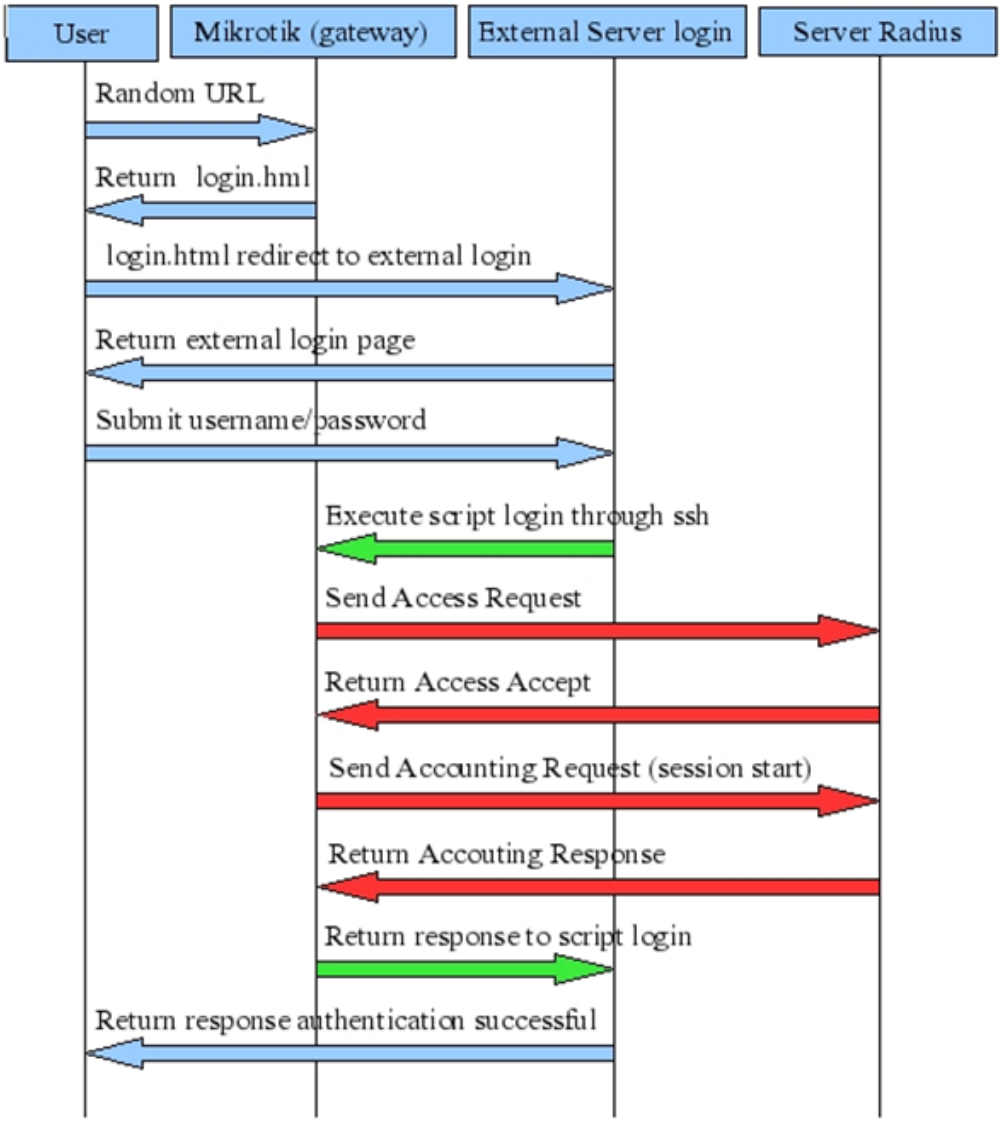


Hình 3.10 Một số phiên làm việc của người dùng

3.5 Đề xuất và kiến nghị

Để có thể nâng cao được chất lượng phục vụ của hệ thống, em xin đưa ra một số kiến nghị như sau:

- Xây dựng các máy chủ Radius làm nhiệm vụ xác thực tập trung và chứa dữ liệu tài khoản người dùng theo mô hình sau:



Hình 3.11 Quy trình xác thực người dùng đề xuất

- Tiếp tục hoàn thiện việc đồng bộ giữa hệ thống quản lý đăng nhập tập trung http://acc.hpu.edu.vn (Hpu Account Service) và hệ thống quản lý mạng không dây

Mikrotik, tạo điều kiện thuận lợi cho người sử dụng chỉ cần một tài khoản và mật khẩu duy nhất, mặt khác cần có sự thống nhất số nhóm người dùng giữa hai hệ thống trên.

- Tăng cường các điểm phát sóng để giải quyết "điểm mù" tại khu vực Giảng đường và Khách sạn sinh viên.
- Nâng cấp dung lượng các đường truyền kết nối internet đảm bảo đáp ứng số lượng người dùng lớn.

KẾT LUẬN

Đồ án "*Xây dựng điểm kiểm soát truy cập mạng không dây Hotspot Gateway có chứng thực dựa trên Mikrotik Router*" đã đạt được một số kết quả như sau:

Về lý thuyết, đồ án đã trình bày và hiểu được:

- Tổng quan về mạng máy tính, cách phân loại mạng máy tính, các thiết bị hoạt động trong mạng máy tính.
- Tìm hiểu về mạng không dây, các chuẩn hiện hành và các thiết bị sử dụng trong mạng WLAN.
- Một số giải pháp bảo mật mạng không dây.
- Một số giải pháp quản lý mạng không dây hiện đang được áp dụng.

Về thực nghiệm, đồ án đã tiến hành

- Cài đặt thử nghiệm chương trình phần mềm Mikrotik trên máy ảo
- Tham gia triển khai thành công hệ thống quản lý wi-fi sử dụng Mikrotik Router Os tại Trường Đại học Dân lập Hải Phòng, hiện hệ thống đang hoạt động ổn định và mang lại hiệu quả cao.

Tuy nhiên trong quá trình thực hiện, do năng lực còn nhiều hạn chế, cùng những nguyên nhân khách quan khác như; thời gian, cơ sở vật chất, khả năng dịch hiểu tiếng Anh trong quá trình trao đổi trên các diễn đàn công nghệ nên chắc chắn trong đồ án còn nhiều sai sót. Em rất mong nhận được sự đóng góp ý kiến của các Thầy Cô và các bạn để em có thêm kiến thức và kinh nghiệm tiếp tục hoàn thiện nội dung nghiên cứu trong đề tài.

Em xin chân thành Cảm ơn!

TÀI LIỆU THAM KHẢO

Sách tham khảo

[1] 802.11 Wireless Networks,The Definitive Guide by Matthew Gast,April 2002

[2] Căn bản mạng không dây (Wireless), Ks Trương Hoàng Vĩ – Đức Hùng, NXB Hồng Đức, 2009

[3] Mạng căn bản, Hồ Đắc Phương, NXB Đại Học Quốc Gia HN, 2006

Website

[4] http://tailieu.hpu.edu.vn/

[5] http://lib.hpu.edu.vn/

[6] http://www.mikrotik.com/

[7] http://wiki.mikrotik.com/wiki/Manual:TOC

[8] http://www.quantrimang.com.vn/

[9] http://meraki.cisco.com/

LỜI CẢM ƠN

Trước hết em xin chân thành gửi lời cảm ơn và lòng biết ơn sâu sắc tới Thầy giáo Th.S Bùi Huy Hùng đã trực tiếp hướng dẫn, chỉ bảo tận tình trong suốt quá trình em thực hiện và triển khai đồ án.

Em xin chân thành cảm ơn các thầy giáo trong Phòng Quản trị mạng Trường Đại Học Dân Lập Hải Phòng đã giúp đỡ, tạo điều kiện cho em trong suốt quá trình làm đồ án.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong trường Đại Học Dân Lập Hải Phòng đã hết lòng dạy bảo chúng em trong những năm học Đại Học, giúp chúng em có những kiến thức và kinh nghiệm quý báu trong chuyên môn và cuộc sống, giúp chúng em bước những bước đi đầu tiên tỏng hành trang vào đời.

Cuối cùng, em xin gửi lời cảm ơn tới những người thân, gia đình, bạn bè đã luôn ủng hộ, động viên em để em có thể hoàn thành đồ án này.

Hải Phòng, tháng 7 năm 2013

Sinh viên

Ngô Thanh Chiến