Chương 1: Mạng không dây

1. Các thành phân của hạ tầng mạng không dây
   1. Wireless host:

- Trong mạng không dây, Wireless host được gọi là 1 end-system (hệ thống đầu cuối), là một thuật ngữ trong ngành mạng máy tính để chỉ 1 máy tính được kết nối với các mạng máy tính khác, Gọi là đầu cuối (end) vì các máy tính này nằm tại rìa mạng hay Internet. Người dùng đầu cuối luôn luôn tương tác với các hệ thống đầu cuối.

- Các hệ thống của Internet còn bao gồm một số máy tính mà người dùng đầu cuối không tương tác. Các máy này bao gồm các máy chủ thư điện tử và máy chủ web.

- Các hệ thống đầu cuối mà kết nối với Internet còn được gọi trong tiếng Anh là hosts, bởi vì chúng có (host) những ứng dụng Internet như trình duyệt web hay ứng dụng lấy thư điện tử.

Ví dụ: laptop, smartphone, destop computer.

* 1. Wireless link:

- Một Wireless host kết nối tới một base station hoặc kết nối tới một host khác thông qua wireless comunication link.

- Các công nghệ wireless link khác nhau có sự khác nhau ở tốc độ truyền(transmision rate) và khoảng cách truyền(distance).

* 1. Base Station:

- Định nghĩa: BS là một trạm phát sóng trên mặt mặt đất trong dịch vụ di động trên mặt đất.

- Trong mạng không dây, BS là máy thu / phát vô tuyến đóng vai trò là trung tâm của mạng không dây cục bộ và cũng có thể là cổng vào giữa mạng có dây và mạng không dây. BS thường bao gồm một máy phát công suất thấp và bộ định tuyến không dây .

- Base station là một phần quan trọng của wireless network infrastructure. BS có trách nhiệm nhận và gửi dữ liệu từ và cho một Wireless host mà ở gần BS đó và Wireless host sử dụng BS để kết nối tới mạng có quy mô lớn hơn như mạng Internet.

Ví dụ: Cell Tower ở trong cellular networks(mạng di động) và Acess point trong 802.11 Wireless LANs

* 1. Network Infracstructure

-Là tài nguyên phần cứng (routers, switches ,wireless routers, cables,…) , phần mềm (các ứng dụng bảo mật mạng, firewall,…) và dịch vụ (T-1 Line, DSL, Wireless protocols,…) của toàn bộ mạng cho phép kết nối mạng, truyền thông, vận hành và quản lý mạng doanh nghiệp. Nó cung cấp các liên kết và dịch vụ liên lạc giữa người dùng, quy trình, ứng dụng, dịch vụ và internet bên ngoài.

- Đây là một mạng quy mô lớn (mạng internet,…) mà các Wireless host muốn được kết nối

- Tác dụng: ngăn chặn các tác nhân nội bộ truy cập hệ thống, ngăn chặn tin tặc bên ngoài xâm nhập vào tài khoản, ngăn chặn việc dữ liệu bị phá hủy,…

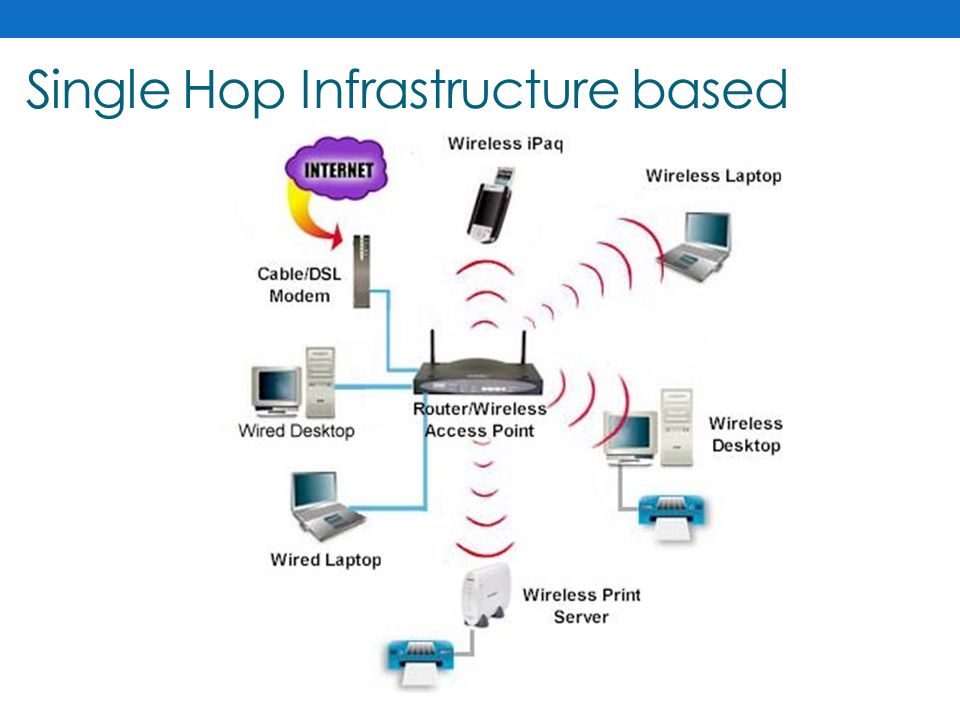
A close up of a device

Description automatically generated

Hình: Các thành phần của mạng không dây

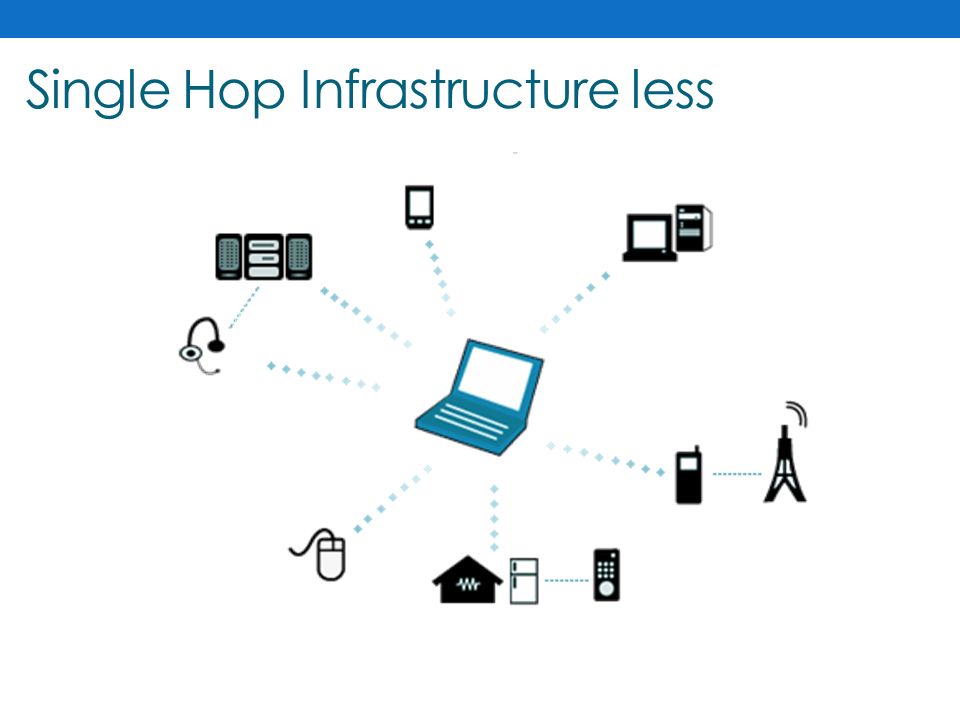
1. Phân chia các lớp mạng không dây
   1. Single-hop, infrastructure-based

Là lớp mạng có Base Station để kết nối tới mạng dây quy mô lớn(Network Infrastructure) như mạng Internet. Tất cả kết nối giữa Wireless host và Base Station thông qua một lần truyền không dây (Single-hop). Mạng không dây theo chuẩn 802.11 mà ta thường dùng trong phòng học, quán Cafe, thư viện và mạng 3G di động nằm trong lớp này.



* 1. Single-hop, Infrastructure-less

Là lớp mạng mà không có Base Station để làm kết nối trong mạng không dây. Một Wireless host trong lớp mạng này có thể truyền với nhau trực tiếp một lần không dây. Ví dụ cho lớp mạng này chính là mạng Blutooth và mạng không dây chuẩn 802.11 ở trong Ad Hoc Mode

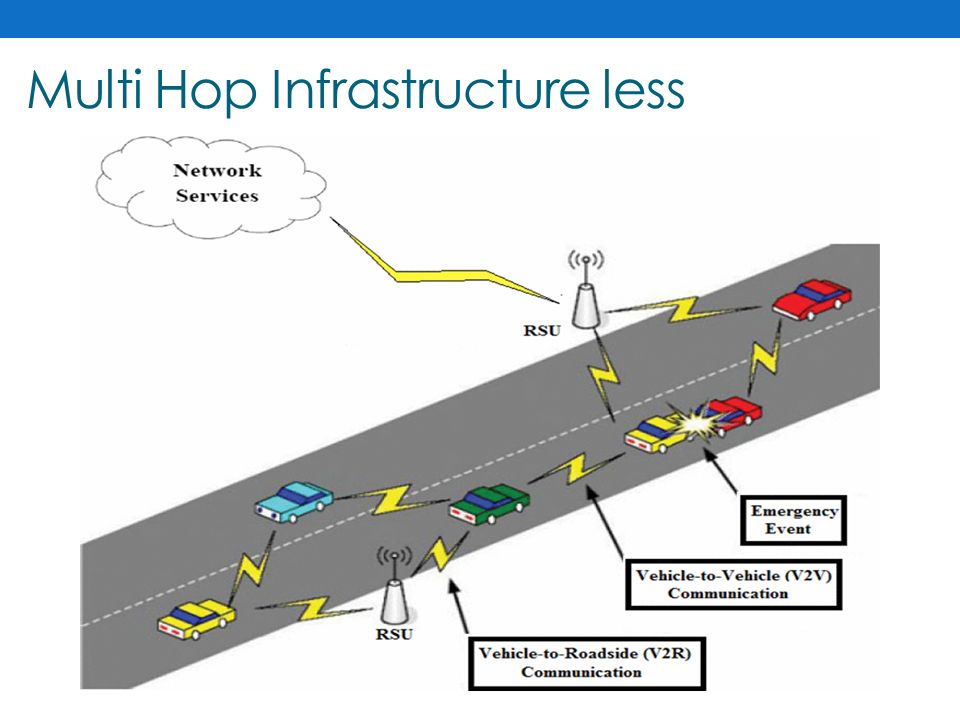


* 1. Multi-hop, infrastructure-based

Lớp mạng này có một Base Station để kết nối tới mạng lớn hơn như mạng Internet. Các Wireless host trong lớp mạng này có thể qua một trung gian là các Wireless host khác để kết nối với Base Station. Một số mạng wireless sensor và một số gọi là wireless mesh networks nằm trong lớp mạng này.

* 1. Multi-hop, infrastructure-less

Lớp mạng này không có Base Station kết nối tới mạng lớn. Các Wireless host phải truyền thông điệp với nhau cho đến khi gặp được đích đến. Nếu wirless host là một chiếc mobile, thì việc kết nối và thay đổi giữa các mobile đươc biết đến là mobile ad hoc networks (MANETs). Nếu wireless host là một phương tiện di chuyển, thì việc kết nối giữa chúng được biết tới vehicular ad hoc network (VANET). Việc phát triển các giao thức trong lớp mạng này là chủ đề để cho nhiều nghiên cứu.



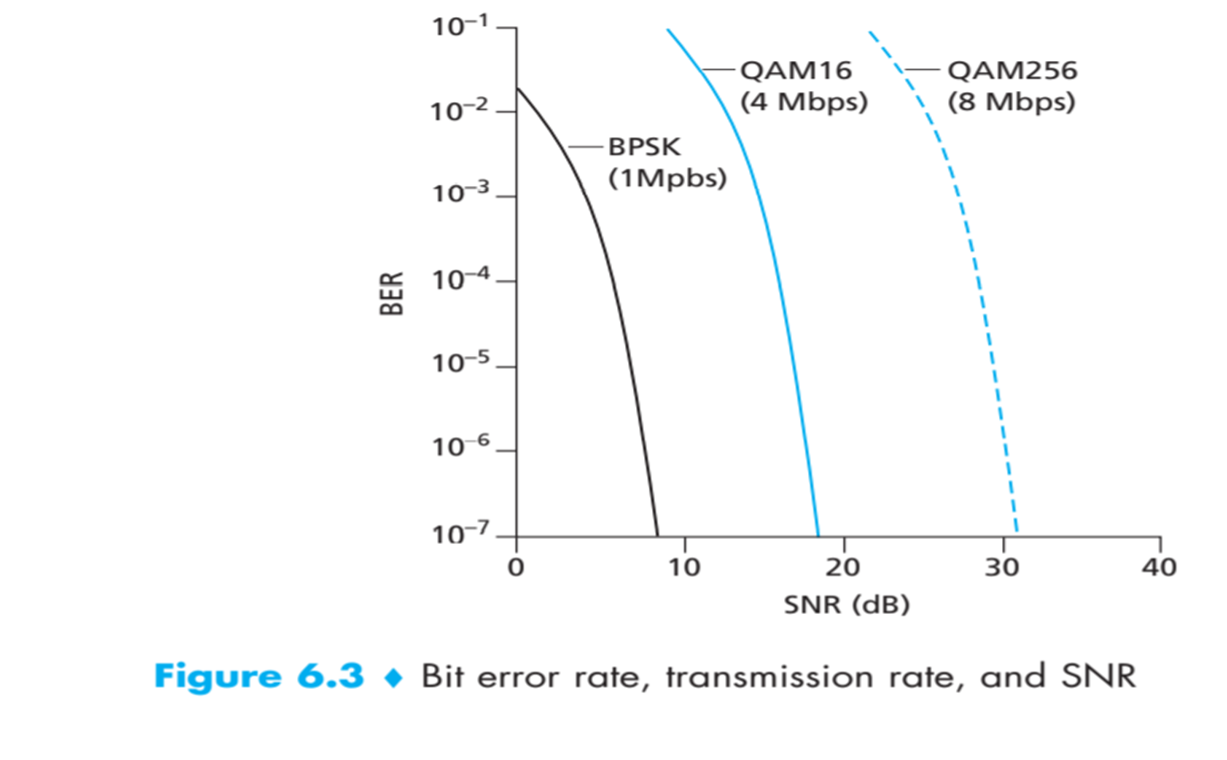
1. Sự khác nhau giữa mạng không dây và mạng có dây

- Cường độ tín hiệu giảm. Suy giảm bức xạ điện từ khi nó đi qua thông qua vật chất (ví dụ: tín hiệu vô tuyến truyền qua tường). Ngay cả trong không gian trống, tín hiệu sẽ phân tán, dẫn đến cường độ tín hiệu giảm (đôi khi gọi là mất tín hiệu) khi khoảng cách giữa người gửi và người nhận tăng.

- Sự can thiệp từ các nguồn khác: Các nguồn vô tuyến truyền trong cùng một dải tần số sẽ giao thoa với nhau. Ví dụ: không dây 2,4 GHz điện thoại và mạng LAN không dây 802.11b truyền trong cùng một dải tần số. Như vậy Người dùng mạng LAN không dây 802.11b có thể nói chuyện trên điện thoại không dây 2,4 GHz rằng cả mạng và điện thoại sẽ không hoạt động tốt. Ngoài ra đến nhiễu từ các nguồn truyền, nhiễu điện từ trong môi trường (ví dụ: động cơ gần đó, lò vi sóng) có thể gây nhiễu.

- Phân tán tín hiệu:Sự lan truyền đa hướng xảy ra khi các phần của sóng điện từ phản xạ khỏi các vật thể và mặt đất, đi theo những con đường khác nhau so với hướng giữa người gửi và người nhận. Điều này dẫn đến việc làm mờ tín hiệu tại máy thu. Di chuyển đối tượng giữa người gửi và người nhận có thể gây ra truyền đa hướng để thay đổi theo thời gian.

* Số bit dữ liệu bị lỗi BER(Bit Error Rate) khi truyền với mạng không dây sẽ cao hơn khi truyền với mạng dây. Các giao thức trong mạng không dây thường tích hợp các mã phát hiện lỗi CRC (Cyclic Redundacy Check) mạnh và các giao thức link-level reliabledata-transfer để truyền lại phần dữ liệu lỗi.



- Mặt khác, do ảnh hưởng của các yếu tố vật lý(Cường độ tín hiệu giảm, sự can thiệp từ các nguồn khác,...) dẫn đến việc tín hiệu ở máy thu có thể lẫn tạp âm, tín hiệu yếu,...Ta thường sử dụng một thước đo là SNR(Signal to noise ratio) với đơn vị đo là (dB). Từ đó, ta có thể phân tích được một số tính chất sau:

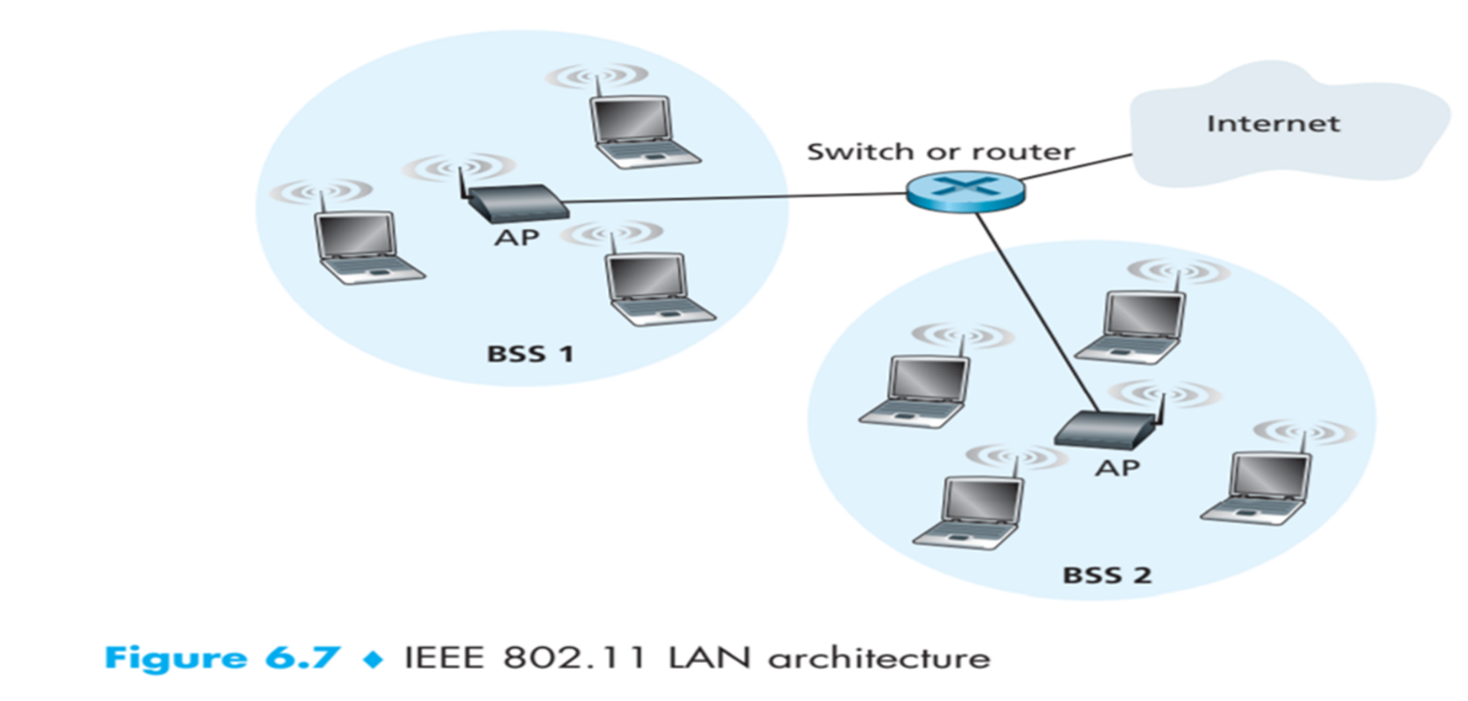
+ Với một kỹ thuật xử lí và điều chế tín hiệu cho trước, SNR càng cao, BER càng thấp.

+ Với SNR cố định, kỹ thuật xử lí và điều chế tín hiệu nào có tốc độ truyền bit cao hơn(transmit rate) thì BER cao hơn.

+ Lựa chọn động các kỹ thuật xử lí và điều chế tín hiệu để phù hợp với điều kiện kênh(chanel conditions).

Chương 2: IEEE 802.11

1. Giới thiệu về mạng Wifi-802.11



* 1. Định nghĩa:

- IEEE 802.11 là một tập các chuẩn của tổ chức IEEE (tiếng Anh: Institute of Electrical and Electronic Engineers) bao gồm các đặc tả kỹ thuật liên quan đến hệ thống mạng không dây. Chuẩn IEEE 802.11 mô tả một giao tiếp "truyền qua không khí" (tiếng Anh: over-the-air) sử dụng sóng vô tuyến để truyền nhận tín hiệu giữa một thiết bị không dây và tổng đài hoặc điểm truy cập (tiếng Anh: access point), hoặc giữa 2 hay nhiều thiết bị không dây với nhau (mô hình ad-hoc)

- Wi-fi 802.11 nằm trong lớp single-hop, infrastructure-base

- Được sử dụng thông dụng hiện nay trong các quán Cafe, thư viện,nhà ở,...

* 1. Kênh truyền trong 802.11

Trong dải tần của các chuẩn 802.11 khi truyền không dây sẽ chia thành nhiều kênh truyền phân thành hai loại: Kênh không chồng chéo(non-overlapping chanel) và Kênh chồng chéo(overlapping chanel).

* 1. Các chuẩn hiện có

Có nhiều tiêu chuẩn khác nhau của 802.11, ví dụ 802.11a,802.11g,...

* + 1. 802.11a

- Chuẩn 802.11a cũng được phát triển song song với chuẩn 802.11b, tuy nhiên chuẩn a thường được sử dụng trong các mạng của doanh nghiệp thay vì gia đình như chuẩn b vì giá thành khá cao.

- So với chuẩn 802.11b, chuẩn này hỗ trợ tốc độ tối đa gần gấp 5 lần, lên đến 54 Mpbs và sử dụng băng tần vô tuyến 5 GHz có thể tránh tình trạng bị nhiễu do các thiết bị khác. Tuy nhiên do tần số cao hơn nên phạm vi hoạt động của chuẩn 802.11a có phần hẹp hơn (40-100m) và khó xuyên qua các vật cản, vách tường.

* + 1. 802.11b

- chuẩn 802.11b ra đời vào tháng 7 năm 1999 và hỗ trợ tốc độ lên đến 11Mpbs thay vì 2Mbps như trước kia. Tương tự thế hệ đầu tiên, chuẩn kết nối 802.11b cũng sử dụng băng tần 2.4 GHz rất dễ bị gây nhiễu từ các thiết bị điện tử khác như điện thoại di động, lò vi sóng,...

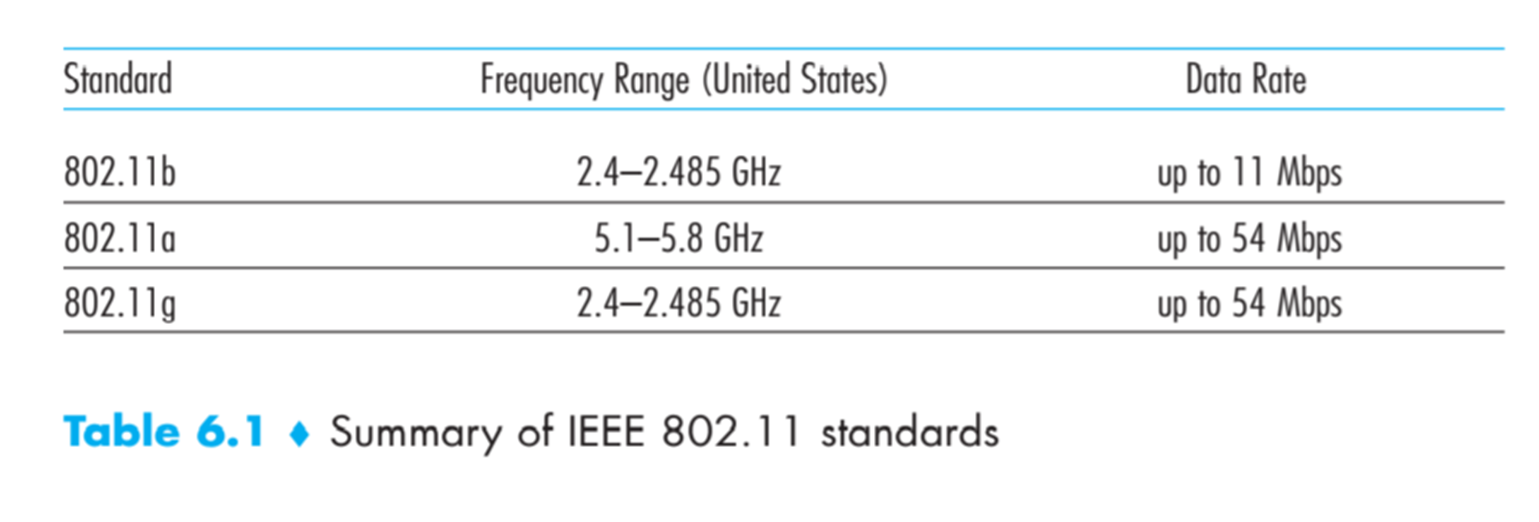
- Chuẩn này được sử dụng rất rộng rãi trên thị trường với giá thành rẻ, phạm vi tín hiệu rộng (70-150m) tuy nhiên tốc độ tối đa khá thấp (11 Mpbs) và dễ bị nhiễu.

* + 1. 802.11g

- Năm 2003, chuẩn WiFi thế hệ thứ 3 ra đời được đặt là chuẩn 802.11g, chuẩn WiFi này thậm chí còn được sử dụng ở nhiều mạng WiFi các gia đình hiện nay. Chuẩn 802.11g được xem là kết hợp giữa chuẩn a và b trước kia, với giá thành khá rẻ (tuy có phần đắt hơn chuẩn b).

- Chuẩn 802.11g hỗ trợ tốc độ đến 54 Mpbs như chuẩn a nhưng sử dụng băng tần 2.4 GHz như chuẩn b, vì vậy chuẩn này có tốc độ cao, phạm vi tín hiệu tốt (80-200m).

- Nhược điểm là dễ bị nhiễu từ các thiết bị phát sóng khác. Do sự giống nhau về nhiều thông số, chuẩn kết nối 802.11g có khả năng tương thích ngược với chuẩn 802.11b và ngược lại



1. Cơ chế kết nối Access Point

- Hiện nay, mạng Wifi chở nên thông dụng, hiển nhiên xuất hiện nhiều điểm truy cập Acess Point (WiFi jungle). Để phân biệt giữa các điểm truy cập Acess Point, administrator phải cài đặt một nhận diện Acess Point là SSID (Service Set Identifier). Mỗi một Acess Point sẽ phục vụ cho một vùng là basic service set (BSS).

- Có 2 cách thức kết nối tới AP của wireless

+ kết nối chủ động (active scanning).

Wireless-host chủ động gửi Probe Request frame trong phạm vi sóng của nó, khi AP nhân được frame này, sẽ gửi lại Probes Response frame cho host. Sau đó Wireless host sẽ gửi Association Request frame tới AP, sau khi AP gửi lại Association Response frame thì việc kết nối coi như thành công.

+ kết nối bị động(passive scanning).

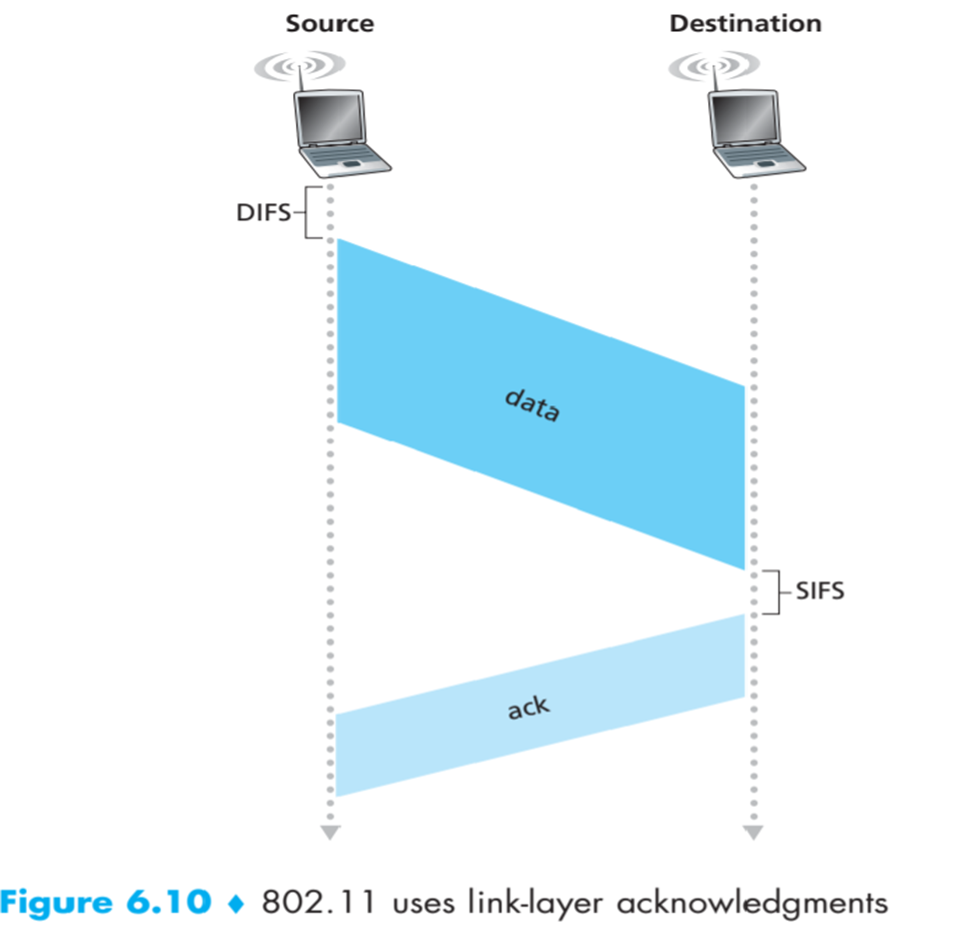
Wireless-host tự động quét các chanel tìm kiếm các beacon frames (mang thông tin của các AP). Wireless host sẽ chọn các AP có sóng tín hiệu mạnh nhất.Sau đó Wireless host sẽ gửi Association Request frame tới AP, sau khi AP gửi lại Association Response frame thì việc kết nối coi như thành công.

A picture containing clock

Description automatically generated

Hình: 2 hình thức kết nối tới AP của wireless

1. Multiple Access Protocol



- 802.11 sử dụng lớp random acess trong multiple access protocols. Chi tiết hơn là CSMA/CA(carrier sense multiple access with collison avoidance) khác biệt với mạng dây sử dụng CSMA/CD(carrier sense multiple access with collison detection).

- Khi receivers station nhận được một frame dữ liệu mà qua kiêm tra của CRC(cyclic redundancy check) station chờ đợi một khoảng thời gian là Short Inter-frame Spacing (SIFS), sau đó gửi lại một acknowledgment frame (ACK). Nếu sender station không nhận được ACK frame này, nó sẽ dùng CSMA/CA để truy cập lại kênh truyền và thực hiện truyền lại frame dữ liệu. Sau một số lần truyền mà được mặc định, thì sender station hủy bỏ truyền frame dữ liệu, kể cả khi nhận được ACK frame hay không.

- Quy trình CSMA/CA khi truyền frame dữ liệu của sender station:

1. Khi sender lắng nghe kênh truyền rỗi, nó sẽ truyền frame dữ liệu sau một khoảng thời gian là Distributed Inter-frame Space (DIFS).

2. sender sẽ lựa chọn một giá trị ngẫu nhiên(backoff value) là lũy thừa nhị phân và đếm ngược(counter) nó khi nó lắng nghe kênh truyền rỗi, dừng lại khi nó lắng nghe kênh truyền bận.

3. khi counter có giá trị bằng 0, sender truyền lại cả frame dữ liệu, sau đó chờ đợi ACK frame.

4. nếu nhận được ACK sender station sẽ coi việc truyền thành công và sẽ dừng việc truyền. Nếu qua một khoảng thời gian không nhận được ACK frame, nó sẽ tiếp tục quy trình CSMA/CA ở bước 2 với back off value lớn hơn.

Chương 3: Tấn công và bảo mật cho mạng không dây

1. Vấn đề ẩn thiết bị đầu cuối trong 802.11

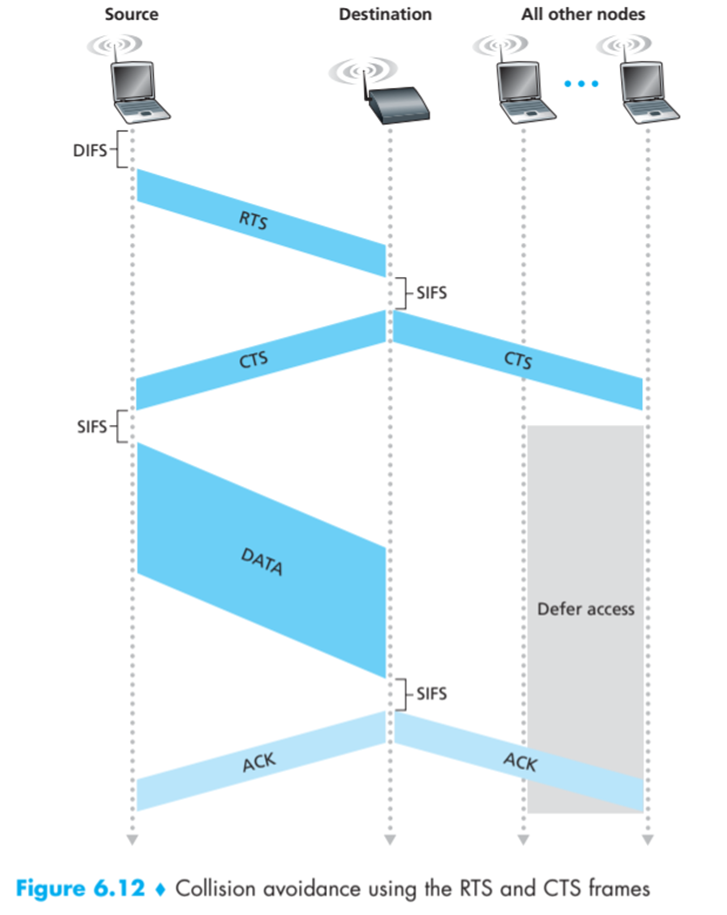
A close up of a logo

Description automatically generated

- Giả thiết đặt ra có hai Wireless station (end-point) và một AP. Hai wireless – station không nằm trong vùng sóng của nhau nhưng nằm trong vùng phủ sóng của AP.

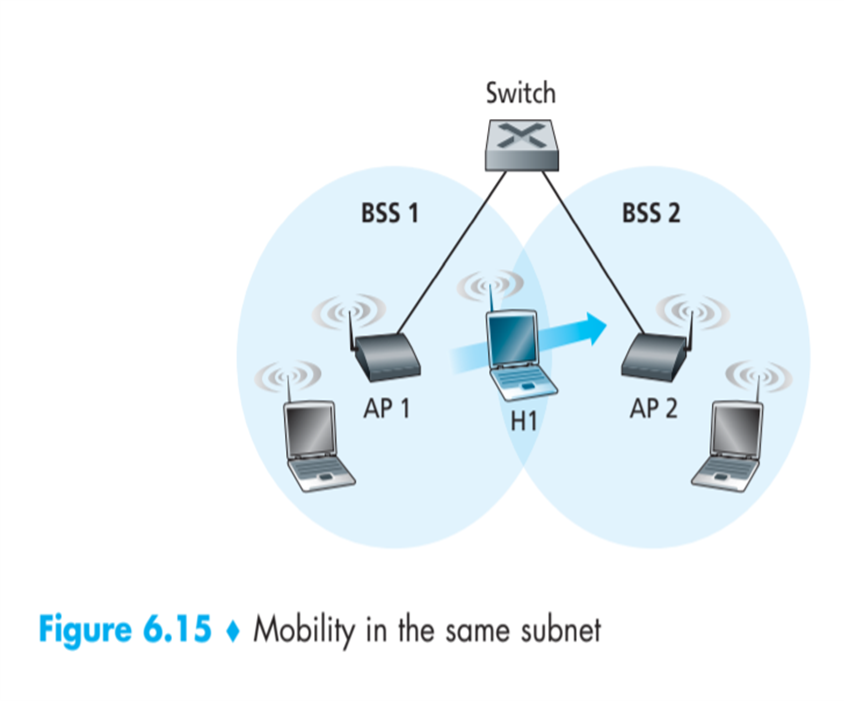
- Trường hợp xảy ra khi sử dụng truyền frame(chưa xét đến truyền frame trong 802.11): Khi H1 truyền fram đến AP nhưng chưa hoàn thành.Lúc này H2 cũng muốn truyền một frame tới AP, vì H1 và H2 không nằm trong vùng phủ sóng của nhau. H2 không biết được H1 đang truyền, H2 truyền fram đi và gây ra xung đột(collison). Kênh truyền sẽ bị lãng phí trong suốt quá trình truyền của H1 và quá trình truyền của H2

- Giải quyết trong 802.11:



802.11 cho phép host sử dụng một frame điều khiển ngắn là Request to Send (RTS) qua kênh truyền gửi tới AP. Sau đó Ap gửi Clear to Send (CTS) tới kênh truyền mà nhận được RTS. Khi đó host (gửi RTS) sẽ được phục vụ cho việc truyền tải và các host khác sẽ không sử dụng kênh truyền cho tới khi quá trình truyền của host (gửi RTS) được hoàn tất.

1. Vấn đề Di chuyển cùng mạng con IP



- Giả thiết: Để tăng vùng phủ sóng cho một mạng con IP, người ta có thể cài đặt một hay nhiều AP nằm trong cùng một mạng con. Nếu một wireless host di chuyển từ vùng phủ sóng AP1 này qua vùng phủ sóng AP2(thường set cùng SSID với AP1) khác mà vẫn giữ nguyên kết nối như kết nối TCP

- Giải quyết: Khi host di chuyển khỏi vùng phủ sóng AP1 cũ, tín hiệu AP1 cũ kém dần, host sẽ tự động quyét luồng tín hiệu mạnh hơn và lấy beacon frame từ AP2, AP2 sẽ làm thủ tục kết nối tới host mà giữ nguyên địa chỉ IP cho host, gửi thông tin vị trí host tới switch, switch với cơ chế ”self learning” cập nhật lại bảng forwarding tables, từ đó các dữ liệu kết nối TCP của host sẽ truyền thông qua AP2.

1. Vấn đề tấn công từ chối dịch vụ
   1. Tấn công tầng vật lý

Do các đặc thù của mạng không dây(tín hiệu vật lý,...) cho phép kẻ tấn công dễ dàng quan sát thông tin liên lạc giữa các thiết bị không dây và khởi chạy các cuộc tấn công Dos đơn giản chống lại các mạng không dây bằng cách gây nhiễu hoặc can thiệp giao tiếp.Các cuộc tấn công như vậy trong lớp vật lý không thể giải quyết thông qua cơ chế bảo mật thông thường. Kẻ tấn công có thể bỏ qua giao thức truy cập mạng không dây(medium acess protocol) và liên tục gửi dữ liệu trên một kênh không dây. Do đó, kẻ tấn công sẽ ngăn chặn người dùng từ việc sử dụng các hoạt động MAC hợp pháp bị ảnh hưởng bởi việc xảy ra các xung đột khi truyền gói dữ liệu và lặp lại giá trị back\_offs(xem lại CSMA/CA).

***->Biện pháp***:Khi tỷ lệ truyền gói thành công giảm xuống dưới mức cho phép, sử dụng phép đo tín hiệu(tìm hiểu trong điều chế tín hiệu) để xem việc tỷ lệ truyền thành công có liên quan đến việc tín hiệu giảm hay không. Ngoài ra, có thể sử dụng các phương thức để tính toán vị trí của thiết bị đầu cuối, để xác định liệu thiết bị có ở vùng nhiều vật chắn hay không(núi đá, nhà bê tông,...). Khi xác định có tấn công DOS xảy ra thì tại Base Station cần có các giao thức chặn kết nối của kẻ tấn công.

* 1. Tấn công tại MAC (Medium Access Control)

Kẻ tấn công có thể lợi dụng lỗ hổng xác thực để thực hiện giả mạo các gói điều khiển giao thức gây việc nhẫm lân của các node mạng. Ví dụ, kẻ tấn công có thể giả mạo các gói ngắt kết nối để phá kết nối giữa node và acess point hoặc giả mạo các gói Request-To-Send(RTS),Clear-To-Send(CTS) để ngăn chặn kết nối của các node trong Basic Sẻvice Set(BSS), kẻ tấn công có thể tạo và gửi liên túc các gói tin rác mà không phá vỡ giao thức MAC để lấy băng thông nhiều hơn các nút khác. Kẻ tấn công có thể lợi dụng hàm đánh giá kênh Clear Channel Assessment của giao thức 802.11 (một trong các kĩ thuật carrie-sense) để tạo ra một kênh luôn trong trạng bận rộn đối với các node khác.

***->Biện pháp:*** mở rộng xác thực đối với các gói điều khiển giao thức.

* 1. Tấn công vào tầng mạng

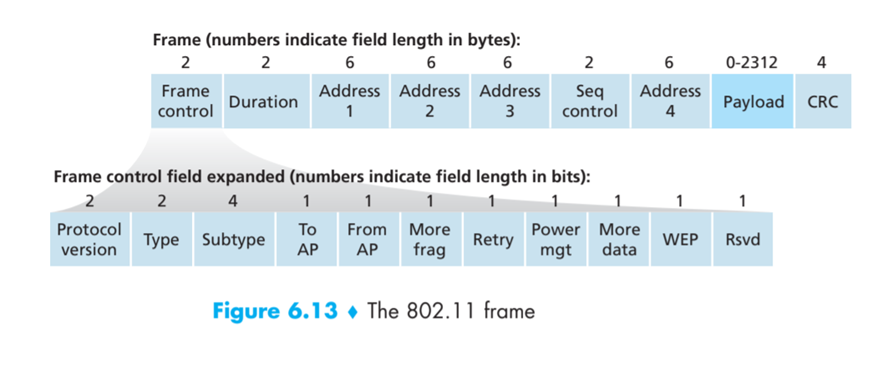
Các cuộc tấn công DoS trong lớp mạng chủ yếu tập trung vào khai thác các giao thức định tuyến và chuyển tiếp trong các mạng không dây(tìm hiểu dưới đây).

+ Tấn công định tuyến: Nếu kẻ tấn công thay đổi địa chỉ IP đích của gói dữ liệu nạn nhân, thi nạn nhân sẽ không thể tiếp cận được dịch vụ yêu cầu.

***-.>Biện pháp:*** cần phải bảo mật các giao thức định tuyến là giải pháp ngăn chặn các cuộc tấn công DOS định tuyến.

+ Tấn công chuyển tiếp:Tương tự như các cuộc tấn công định tuyến, kẻ tấn công cũng có thể khai thác hành vi chuyển tiếp. Tấn công điển hình phương pháp tiếp cận bao gồm tiêm các gói rác, bỏ các gói và các gói rối loạn trong hợp pháp gói. Kẻ tấn công có thể sử dụng các gói giả mạo để ngụy trang hành vi tấn công của chúng hoặc tìm đối tác để đánh lừa những người bảo vệ. Mục tiêu là làm cạn kiệt băng thông hoặc phá vỡ kết nối để dịch vụ không thể được cung cấp.

1. Frame trong 802.11



- Các trường(field) trong frame được tính theo byte, mỗi trường có thể nhiều trường con(sub-field) được tính theo bit, các trường(field) được tạo ra để phục vụ cho truyền tải không dây và truyền tải có dây.

Cụ thể:

+ Payload : chứa Ip datagram và ARP package

+ CRC : chưa các code check lỗi dữ liệu

+ Address1: chứa địa chỉ MAC của station nhận frame

+ Address2: chứa địa chỉ MAC của station truyền frame

+ Address3: chứa địa chỉ MAC của router

+ Address4: sử dụng khi các AP chuyển tiếp khung cho nhau trong chế độ ad hoc.

+ Sequence number: chứa thứ tự của khung khi truyền.

+ Duration: chứa thời lượng của khung tồn tại.

+ Control: chứa thông tin giao thức và các cờ điều khiển

Chương 4. IEEE 802.11i – Cải tiến an ninh cho chuẩn 802.11

* Đặt vấn đề: 2 nét đặc trưng của mạng LAN có dây mà LAN ko dây ko có

1. Để truyền dữ liệu trên 1 mạng LAN có dây, 1 máy (station) phải được kết nối vật lý trực tiếp với mạng LAN, nhưng LAN không dây thì bất kì máy nào nằm trong vùng phủ song của LAN đó thì đều có thể truyền dữ liệu đi. Ở 1 khía cạnh nào đó, có 1 hình thức xác thực với mạng LAN có dây mà yêu cầu những hoạt động có thể quan sát được để kết nối 1 station với 1 mạng LAN có dây
2. Tương tự, để nhận dữ liệu từ 1 station là 1 thành phần của 1 mạng LAN có dây, station nhận dữ liệu cũng phải đươc gắn vào mạng LAN đó, mặt khác, với mạng LAN ko dây, bất kì máy nào nằm trong vùng phủ sóng thì đều có thể nhận. Do đó, 1 mạng LAN có dây thì sẽ có tính riêng tư, giới hạn việc nhận dữ liệu từ các máy đã kết nối với mạng LAN

=> Cần 1 cơ chế và dịch vụ bảo mật mạnh mẽ cho các mạng LAN ko dây

1. IEEE 802.11i vs IEEE 802.11

- Các tính năng bảo mật về tính bí mật và tính xác thực trong 802.11 ban đầu khá yếu

- Về tính bí mật: Trong 802.11 chuẩn, thuật toán Wired Equivalent Privacy (WEP) có chứa những lỗ hổng bảo mật

- Để gia tang tính bảo mật cho mạng WLAN, Wi-Fi Alliance đã ban hành chuẩn wifi mới: WiFi Protected Access (WPA) là tập hợp các cơ chế bảo mật mà loại bỏ hầu hết các vấn đề bảo mật của 802.11 và dựa trên trạng thái hiện tại của chuẩn 802.11i

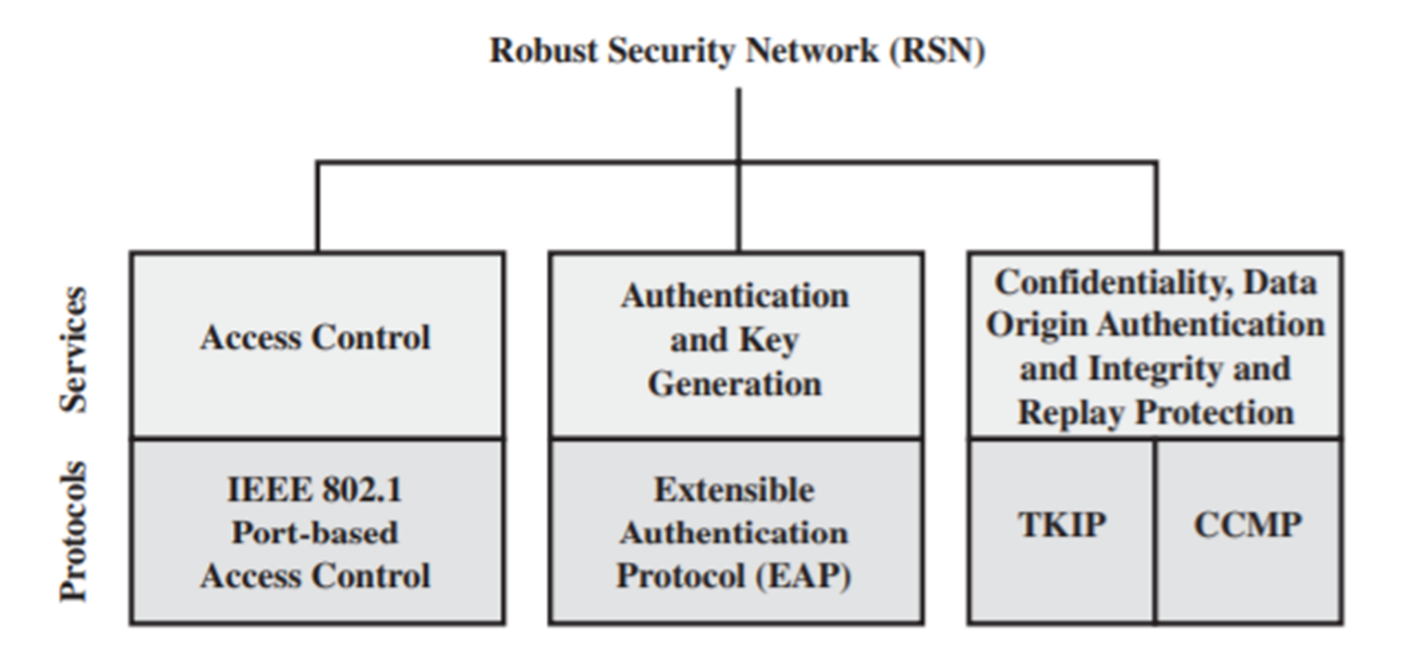
- Form cuối của chuẩn 802.11i là Robust Security NetWork (RSN)

1. Các dịch vụ bảo mật của 802.11i RSN

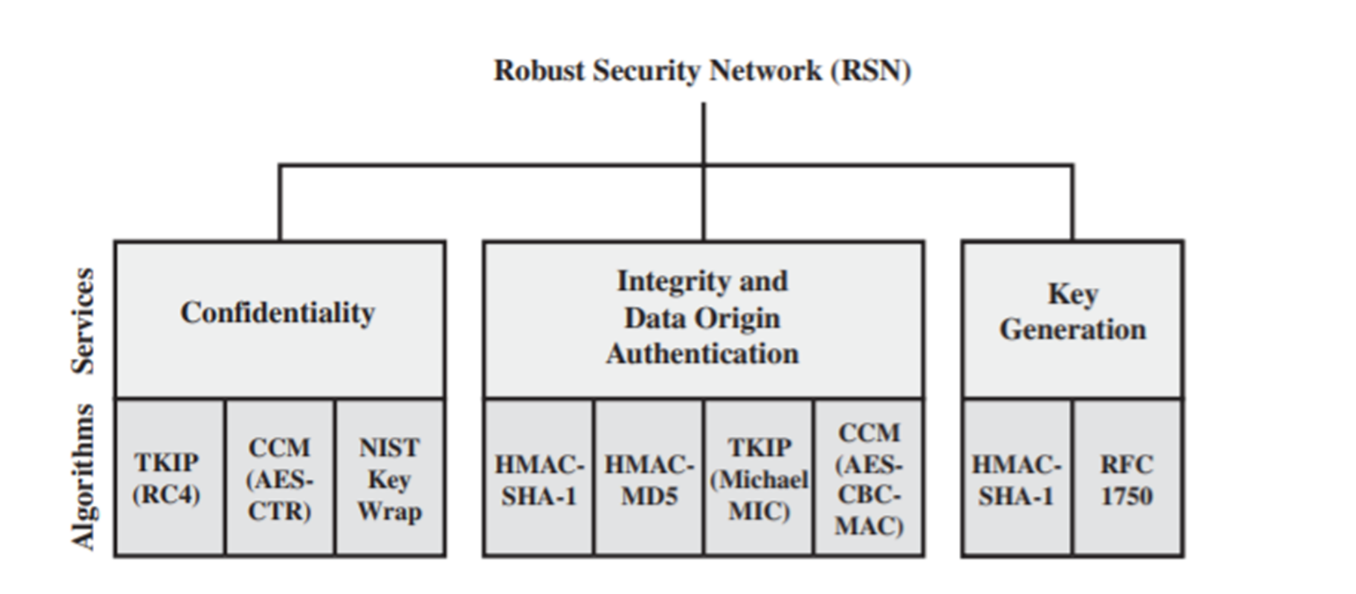
- Xác thực: 1 giao thức được sử dụng để định nghĩa ra sự trao đổi giữa 1 người dùng và 1 Authentication Server nơi mà cung cấp việc xác thực lẫn nhau và sinh ra khóa tạm thời để dùng giữa máy khách và điểm truy cập thông qua liên kết ko dây

- Kiểm soát truy cập: Thực thi các chức năng xác thực, định tuyến thông điệp phù hợp và tạo cơ sở trao đổi khóa. Nó có thể làm việc với nhiều giao thức xác thực khác nhau

- Bảo mật và toàn vẹn thông điệp: Dữ liệu MAC-level được mã hóa bằng 1 mã toàn vẹn thông điệp (MIC) nhằm đảm bảo dữ liệu không bị thay đổi.



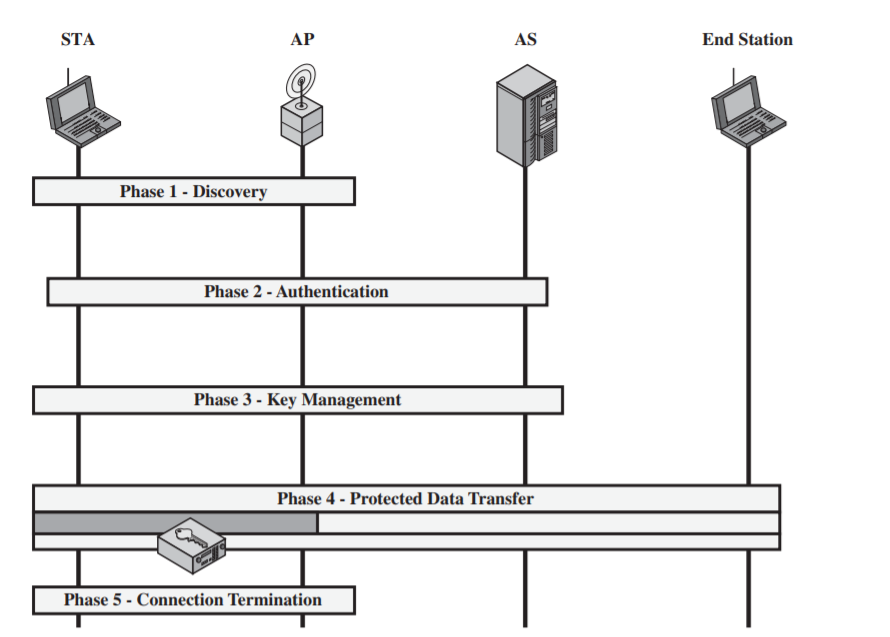
Hình: Các dịch vụ và giao thức RSN



Hình: Các thuật toán bảo mật RSN

1. Các pha vận hành của 802.11i

Có thể được chia thành 5 pha



Hình: 5 pha vận hành

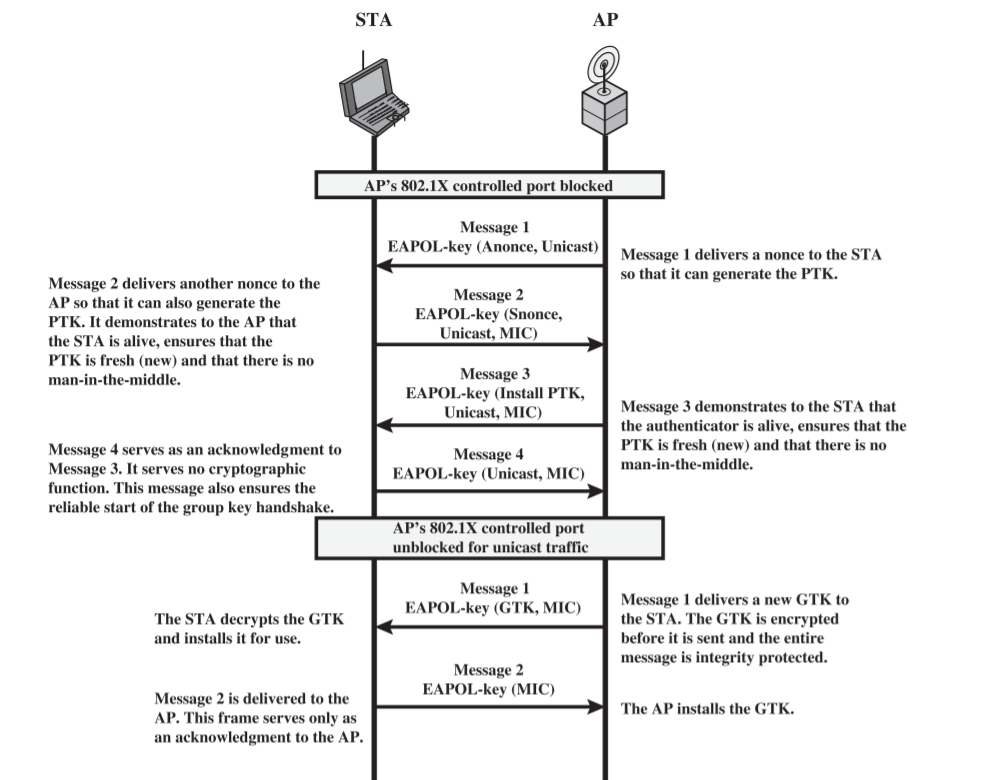
Discovery: 1 Access point (AP) dùng 1 thông điệp được gọi là Beacons và Probe Responses để quảng bá chính sách bảo mật của nó. Station sẽ sử dụng những thông điệp này để xác định 1 AP về 1 mạng WLAN mà nó muốn truy cập. Station sẽ kết hợp với AP (AP mà nó dùng để chọn ra bộ mật mã và cơ chế xác thực khi mà Beacons and Probe Response đưa ra 1 lựa chọn)

Pha xác thực: Trong pha này, STA và Authentication Server (AS) cung cấp định danh của chúng cho nhau. Access point chặn những luồng truyền tải ko được xác thực giữa STA và AS cho tới khi việc xác thực đường truyền thành công. AP sẽ ko tham gia vào việc tham gia vào việc xác thực việc truyền tải ngoại trừ việc theo sau giữa STA và AS

Quản lý khóa: AP và STA thực hiện 1 số thao tác để tạo ra các khóa mã hóa và đặt lên AP và STA. Frame chỉ được trao đổi giữa AP và STA

Bảo vệ việc truyền dữ liệu: Frame được trao đổi giữa STA và station cuối cùng thông qua access point (AP). Dữ liệu bí mật được truyền chỉ xuất hiện giữa STA và AP, tính mật ko được cung cấp khi kết thúc

Chấm dứt kết nối: AP và STA trao đổi frame. Trong kha này, kết nối bí mật bị hủy bỏ và việc kết nối được khôi phục lại trạng thái ban đầu



Hình: Four-Way Handshake và Group Key Handshake

* 1. Pha discovery:

- Giúp cho station và access point nhận ra nhau, đồng ý thiết lập khả năng bảo mật và thành lập các liên kết cho các giao tiếp sử dụng những khả năng bảo mật này

- Trong pha này xảy ra 3 sự trao đổi chính:

+ Network and security capability discovery: Các station tìm ra những mạng mà nó muốn kết nối. Access point quảng bá security capacibilities của nó theo chu kì, được chỉ ra bởi RSN IE trong 1 kênh riêng thông qua Beacon frame hoặc là phản hồi về yêu cầu của 1 station thông qua 1 khung Probe Response. 1 station kết nối không dây có thể tìm ra các Accesspoint có sẵn và trao đổi thông tin bí mật bằng cách giáo sát thụ động khung Beacons hoặc là tích cực thăm dò các kênh

+ Open system authentication: Dùng để duy trì khả năng thăm dò với máy trạng thái IEEE 802.11, cũng như thực thi trong các thành phần phần cứng IEEE 802.11. Bản chất là station và access point trao đổi định danh lẫn nhau

+ Association: Dùng để đồng ý thiết lập kết nối bảo mật để sử dụng. Station gửi Assocation Request tới access point, station chỉ rõ 1 tập các khả năng phù hợp từ các quảng bá của access point. Nếu ko có bất kì khả năng nào giữa access point và station, AP từ chối Assocation Request, và STA cũng chặn nó, trong tình huống này, có thể là liên quan đến 1 access point giả mạo hoặc có ai đó đang chèn frame 1 cách bất hợp pháp lên đường chuyền của nó

* 1. Pha xác thực

Gồm 3 pha chính sau:

- Kết nối tới Authentication Server (AS): station gửi yêu cầu đến access point của nó để kết nối tới (AS), accesspoint chấp nhận yêu cầu và gửi yêu cầu truy cập tới AS

- EAP exchange: Pha trao đổi này xác thực station và AS lẫn nhau. 1 số trao đổi sẽ phù hợp

- Bảo mật khóa truyền đi: 1 khi việc xác thực được thiết lập, AS sinh ra 1 khóa phiên chính, còn gọi là khóa AAA (Authentication,

Authorization, and Accounting) và gửi cho station. Tất cả các khóa mà station cần để truyền tin bí mật giữa accesspoint của nó cần được sinh ra từ khóa phiên chính này.

* 1. Quản lý khóa

Trong quá trình quản lý khóa, 1 lượng lớn khóa bí mật được sinh ra và phân phối cho các station. Có 2 kiểu khóa: Khóa cặp đôi được sử dụng trong truyền thông giữa station và access point và khóa nhóm được sử dụng trong truyền thông đa hướng

Bảng mô tả 1 số khóa IEEE 802.11i cho các giao thức toàn vẹn và bí mật dữ liệu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ký hiệu | Tên | Mô tả | Kích thước (bit) | Kiểu |
| AAA | Authentication,  Accounting, and  Authorization Key | Dùng để lấy PMK, được dùng với chuẩn xác thực IEEE 802.1X và tiếp cận việc quản lý khóa | >= 256 | Key generation  key, root key |
| PSK | Pre-shared Key | Trở thành Pairwise Master Key trong môi trường Pre-shared Key | 256 | Key generation  key, root key |
| PMK | Pairwise Master Key | Sử dụng với những đầu vào khác nhau để lấy được PTK | 256 | Key generation  key |
| GMK | Group Master Key | Sử dụng với những đầu vào khác nhau để lấy được GTK | 128 | Key generation  key |
| PTK | Pair-wise Transient  Key | Được lấy từ PMK, so sánh EAPOL-KCK, EAPOL-KEK và TK và khóa MAC | 512 (TKIP)  384(CCMP) | Composite key |
| TK | Temporal Key | Dùng với TKIP hoặc CCMP để cung cấp việc bảo mật tính toàn vẹn và tính bí mật cho luồng truyền tải điểm -điểm của người dùng | 256 (TKIP)  128(CCMP) | Traffic key |
| GTK | Group Temporal  Key | Được lấy từ GMK, dùng để bảo mật tính bí mật và tính toán vẹn cho luồng truyền tải điểm – đa diểm hoặc quảng bá của người dùng | 256 (TKIP)  128(CCMP)  40,104(WEP) | Traffic key |

* 1. Pha bảo vệ việc truyền dữ liệu

- IEEE 802 định nghĩa ra 2 phương án để bảo mật dữ liệu được truyền đi trong 802.11 MPDUs: Temporal Key Integrity Protocol (TKIP), và Counter Mode-CBC MAC protocol (CCMP)

MAC Protocol (CCMP).

* + 1. TKIP:

Được thiết kế để chỉ yêu cầu thay đổi về mặt phần mềm trên thiết bị được thực thi với các phương pháp bản mật mạng LAN ko dây cũ. TKIP gồm 2 dịch vụ

- Toàn vẹn thông điệp: TKIP thêm vào 1 đoạn mã MAC vào khung MAC của 802.11 sau trường dữ liệu. Mã MAC được sinh bởi thuật toán Michael, trong giải thuật này tính toán 1 giá trị 64 bit làm giá trị đầu vào và giá trị MAC địa chỉ đầu ra và trường dữ liệu.

- Toàn vẹn dữ liệu: Bằng cách mã hóa MPDU + MAC dùng RC4

* + 1. CMMP:

Được dùng cho thiết bị IEEE 802.11 đời mới hơn, thiết bị mà tương thích với phần cứng hỗ trợ chuẩn này, tương tự TKIP, CCMP hỗ trợ 2 dịch vụ:

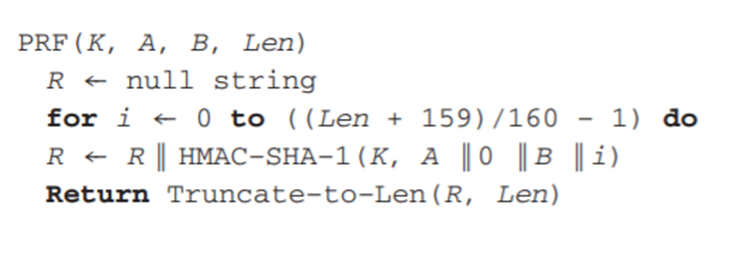
- Toàn vẹn thông điệp: Dùng cơ chế xác thực thông điệp mã hóa chuỗi khối (CBC-MAC)

- Toàn vẹn dữ liệu: Dùng cơ chế mã hóa khối CTR được vận hàng dựa trên thuật toán mã hóa AES để mã hóa. 128 bit khóa AES được dùng để đảm bảo cho cả tính toàn vẹn và bí mật. Phương pháp này sử dụng 1 packet number 48 bít để xây dựng số N1 để ngăn chặn tấn công phát lại

1. Hàm giả ngẫu nhiên

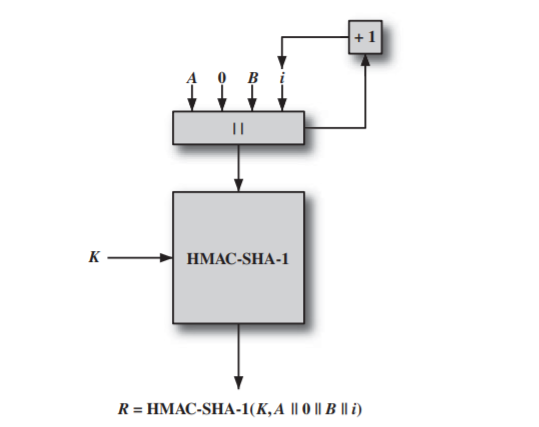
Pseudorandom Function (PRF) được xây dựng trên hàm băm HMAC-SHA-1 để tạo ra 1 dòng các bit giả danh. Nhận 4 tham số đầu vào:

* K: Khóa bí mật
* A: 1 chuỗi ký tự đặc trưng cho ứng dụng
* B: 1 số dữ liệu đặc trưng cho mỗi tình huống
* Len: Số bit giả danh mong muốn



Sơ đồ: Hàm giả danh ngẫu nhiên PRF

Trong đó, hàm HMAC-SHA-1 (K,A || 0 || B || i) hoạt động như sau:



-Khóa K: Có vai trò như là khóa đầu vào của hàm HMAC

-Thông điệp gồm 4 thành phần:

+ Chuỗi ký tự A

+ 1 byte có giá trị = 0

+ Biến B

+ Biến đếm i: Được khởi tạo ban đầu = 0

- Hàm HMAC được chạy 1 lần, sinh ra giá trị băm 160 bit. Nếu được yêu cầu nhiều bit hơn, HMAC được chạy lại với cùng giá trị đầu vào, ngoại trừ biến đếm i được tăng lên mỗi vòng lặp cho tới khi số lượng bit cần thiết được sinh ra