

An toàn mạng máy tính

Chương 6.

An toàn mạng không dây

Nội dung bài giảng:

1. Giới thiệu về mạng không dây
2. Phân loại mạng không dây
3. Các mô hình hoạt động của mạng không dây
4. Các chuẩn trong IEEE 802.11
5. Các tấn công trong mạng WLAN
6. Bảo mật cho mạng WLAN

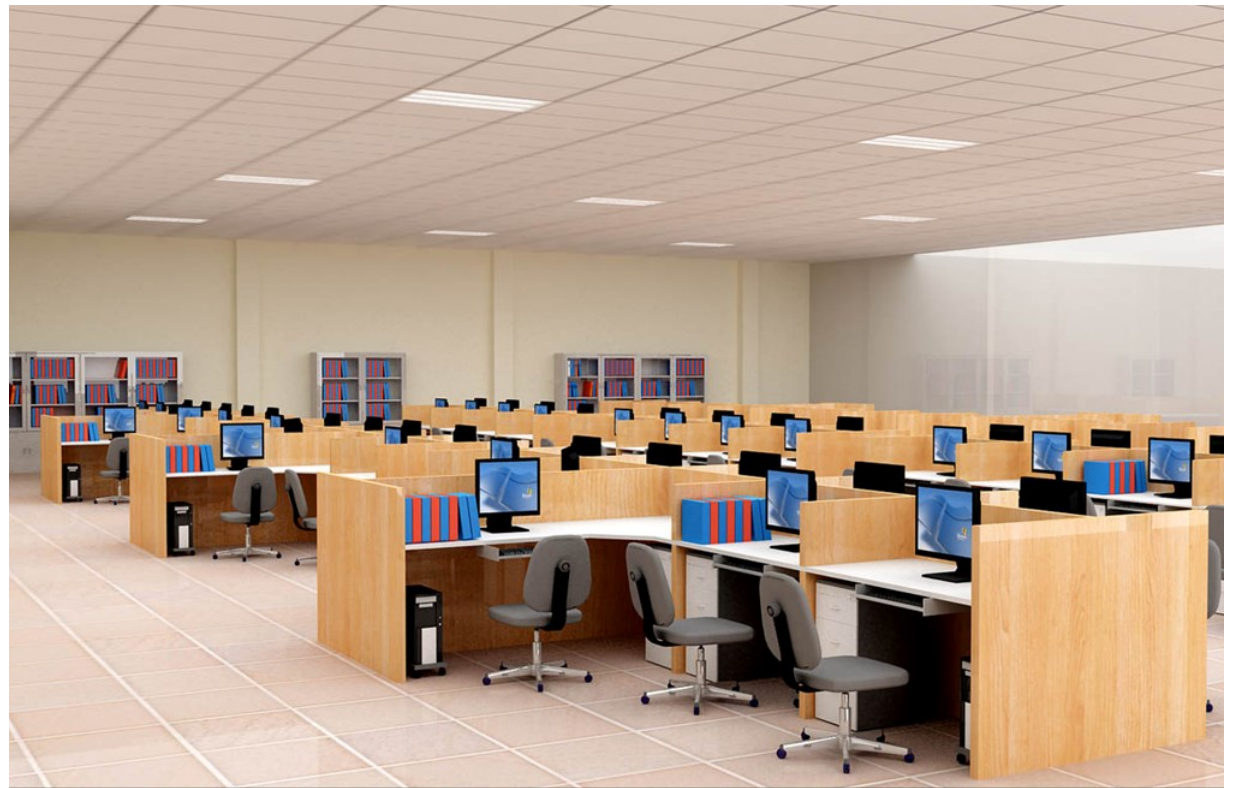
Tài liệu tham khảo:

1. *Wireless Networking in the developing world*. Jane Butler, Ermanno Pietrosevoli. Third Edition, February 2013.
2. *802.11 Wireless Networks: The Definitive Guide*. Matthew Gast. April 2002.
3. NIST SP 800-153. *Guidelines for Securing Wireless Local Area Networks*. 2012.
4. *Handbook - Deploying Wireless Networks*. FORTINET. VERSION 5.2.4.
5. *SANS: Understanding Wireless Attacks and Detection*

1. Giới thiệu

- Xét các mô hình mạng:

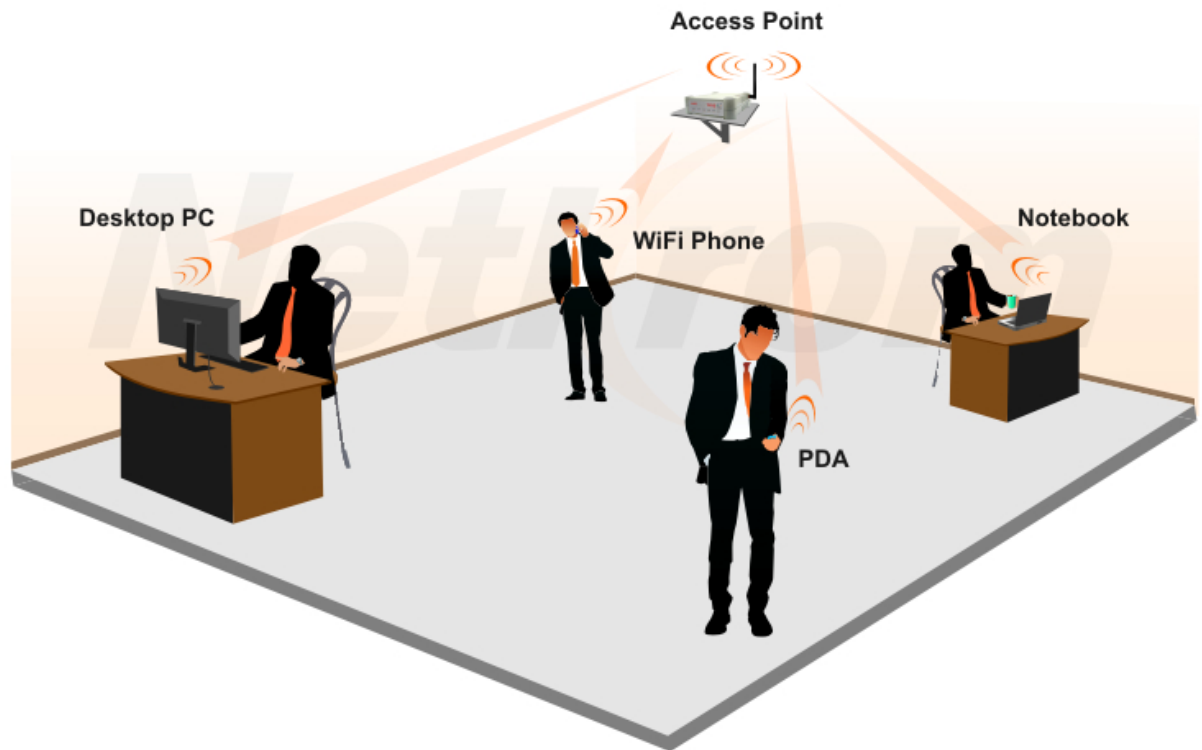
Mạng văn phòng



1. Giới thiệu

■ Xét các mô hình mạng:

Mạng văn phòng



1. Giới thiệu

- Xét các mô hình mạng:

Mạng đô thị



1. Định nghĩa

- Mạng không dây là một hệ thống các thiết bị được nhóm lại với nhau,
- Có khả năng giao tiếp thông qua sóng vô tuyến thay vì các đường truyền dẫn bằng dây.
- Các kết nối được thiết lập theo chuẩn định sẵn: 802.11, 802.15, 802.16...

1. Định nghĩa

■ Ưu điểm:

□ Tính di động:

- Người sử dụng có thể truy cập nguồn thông tin không dây ở bất kỳ vị trí nào (trong phạm vi phủ sóng).

□ Tính đơn giản:

- Việc lắp đặt, thiết lập, kết nối mạng không dây dễ dàng, đơn giản. Tránh việc kéo cáp qua tường và trần nhà.

□ Tính linh hoạt:

- Có thể triển khai những vị trí mà mạng hữu tuyến không thể triển khai được. Sử dụng cho nhiều thiết bị khác nhau: Laptop, ĐTDD, thiết bị cầm tay

□ Tiết kiệm chi phí: thiết bị triển khai ít hơn...

□ Khả năng mở rộng:

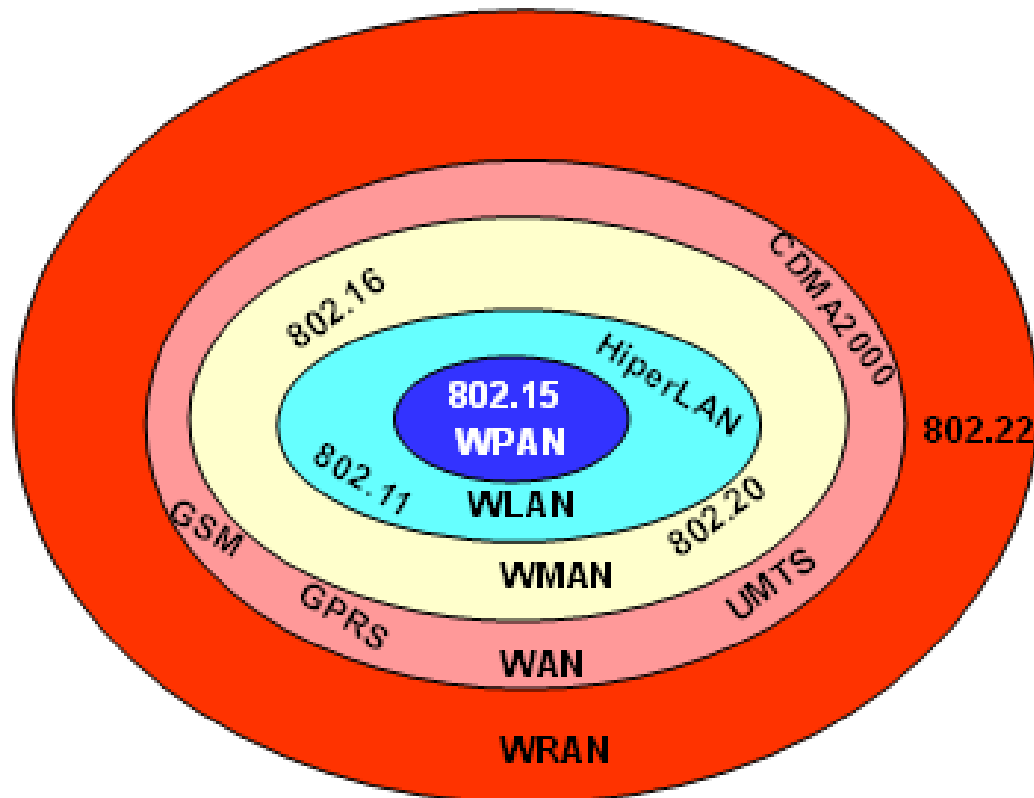
1. Định nghĩa

■ Nhược điểm:

- **Nhiều:** Khả năng bị nhiễu sóng do thời tiết, sóng từ các thiết bị khác, hay bị các vật chắn...
- **Bảo mật:** Vì mọi người dùng đều có thể phát hiện được định danh của mạng vì vậy:
 - Kẻ tấn công có gắng bẻ khóa để vào mạng
 - Chặn bắt thông tin truyền giữa người dùng và Access Point.
- **Phạm vi:** Với mỗi chuẩn và các thiết bị khác nhau ảnh hưởng đến phạm vi phát sóng.
- **Tốc độ:** Tốc độ mạng không dây chậm hơn so với mạng có dây

2. Phân loại

- Phân loại dựa trên vùng phủ sóng:



2.1 WPAN

■ Wireless Personal Area Network:

- Mạng vô tuyến cá nhân. Bao gồm các công nghệ vô tuyến có vùng phủ sóng trong phạm vi vài chục mét.
- Mục đích phục vụ các thiết bị ngoại vi: máy in, bàn phím, chuột, đồng hồ, ĐTDĐ.
- Các công nghệ sử dụng: Bluetooth, Wibree, ZigBee, Wireless USB,
- Chuẩn của công nghệ: IEEE 802.15

2.1 WPAN

■ Sóng Bluetooth:

- Là công nghệ không dây tầm gần giữa các thiết bị điện tử.
- Hỗ trợ truyền dữ liệu ở khoảng cách ngắn giữa các thiết bị di động và cố định.
- Tốc độ tối đa: 1Mbps
- Sóng vô hướng và dải băng tần 2,4 GHz



2.1 WPAN

- Công nghệ Wibree:



2.2 WLAN

■ WLAN (Wireless Local Area Network):

- Mạng vô tuyến cục bộ. Bao gồm các công nghệ vô tuyến có vùng phủ sóng trong phạm vi vài trăm mét.
- Nổi bật là công nghệ Wifi với nhiều chuẩn mở rộng khác nhau thuộc họ 802.11 a/b/g/h/i/n...
- Mục đích phục vụ các thiết bị: Laptop, thiết bị cầm tay, máy in...
- Các công nghệ sử dụng: Wifi, HiperLAN và HiperLAN2
- Chuẩn của công nghệ: IEEE 802.11

2.3 WWAN & WRAN

- **WWAN: Mạng vô tuyến diện rộng:**
 - Công nghệ: UMTS/GSM/CDMA2000:
 - Phạm vi phủ sóng vài chục Km.
 - Mạng 2,5G. 3G
- **WRAN: Mạng vô tuyến khu vực:**
 - Công nghệ: IEEE 802.22
 - Phạm vi phủ sóng 40-100 Km.
 - Tốc độ 22 Mbps
 - Sử dụng băng tần UHF, VHF 6/7/8Mhz
 - Mục đích truyền thông tới các vùng xa xôi hẻo lánh.

3. Các mô hình mạng WLAN

- Mô hình mạng độc lập IBSS hay còn gọi là mạng Ad-hoc: (Independent Basic Service sets)
- Mô hình mạng cơ sở: BSS (Basic Service sets)
- Mô hình mạng mở rộng: ESS (Extended Service sets)

3.1 Mạng Ad-hoc

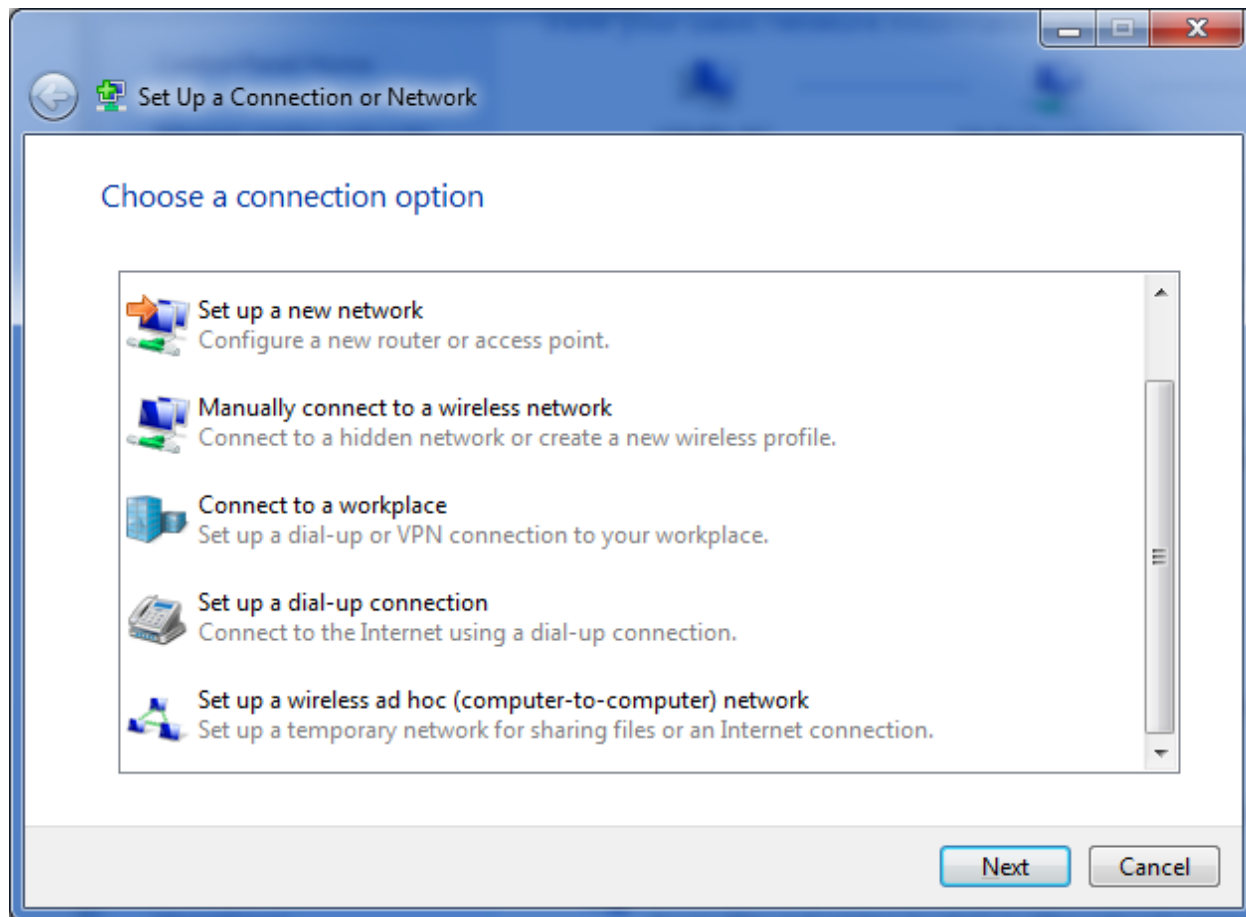
■ Mô hình mạng Ad-hoc:

- Các máy trạm liên lạc trực tiếp với nhau mà không phải thông qua AP nhưng phải trong phạm vi cho phép.
- Các máy trạm có vai trò ngang hàng với nhau. (Peer-to-peer)
- Khoảng cách liên lạc trong phạm vi 100m.
- Sử dụng thuật toán Spokesman Election Algorithm.
- Máy trạm có trang bị card mạng không dây.

3.1 Mạng Ad-hoc



3.1 Mạng Ad-hoc



3.1 Mạng Ad-hoc

■ Cách thiết lập:

- ☐ Thiết bị: Card không dây
- ☐ Trình điều khiển (Driver)
- ☐ Tiện ích.

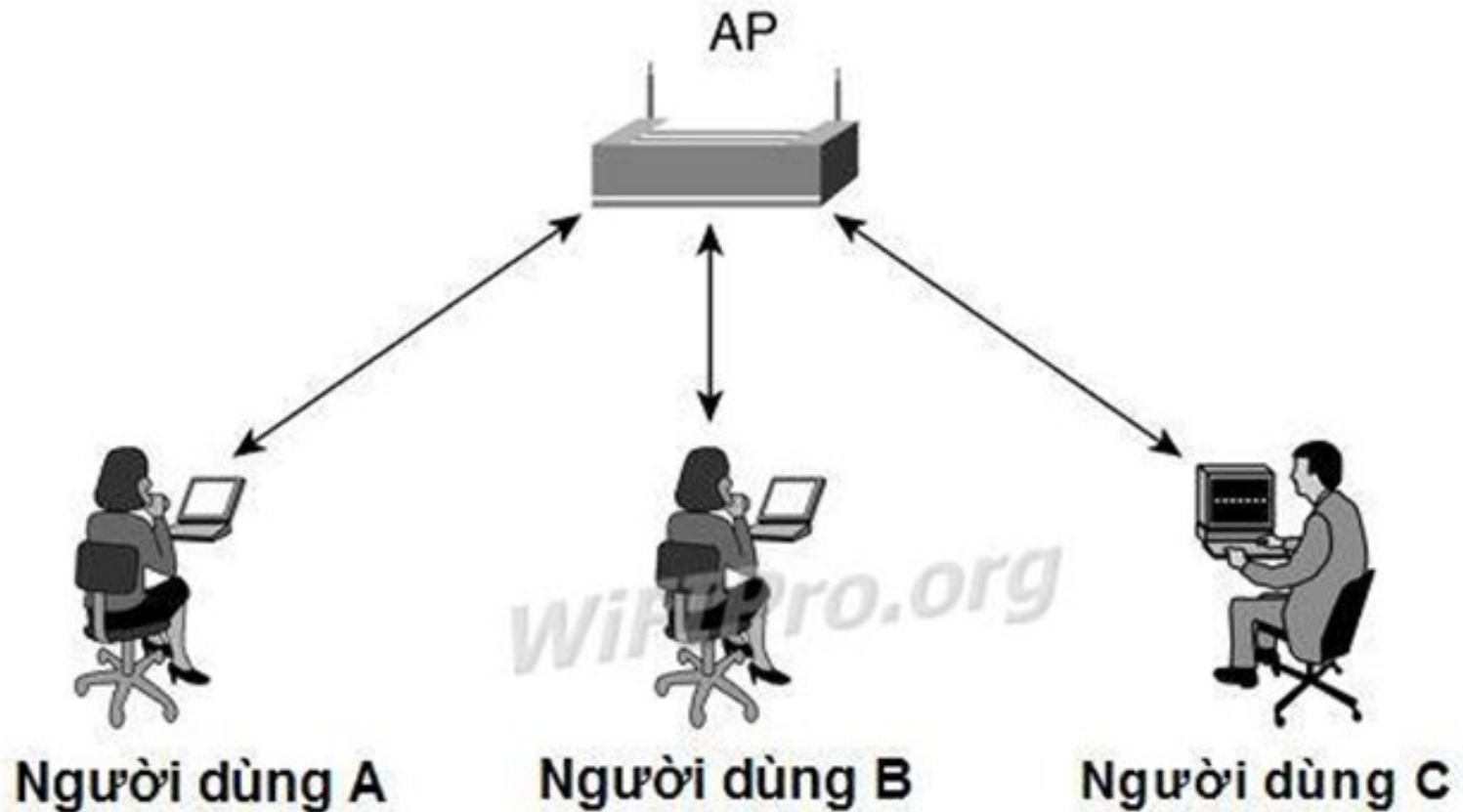
■ Cấu hình:

- ☐ Các Station phải cùng SSID: Service set identifier

3.2 Mạng BSS

- Bao gồm các điểm truy nhập AP
- AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng.
- Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP.

3.2 Mạng BSS



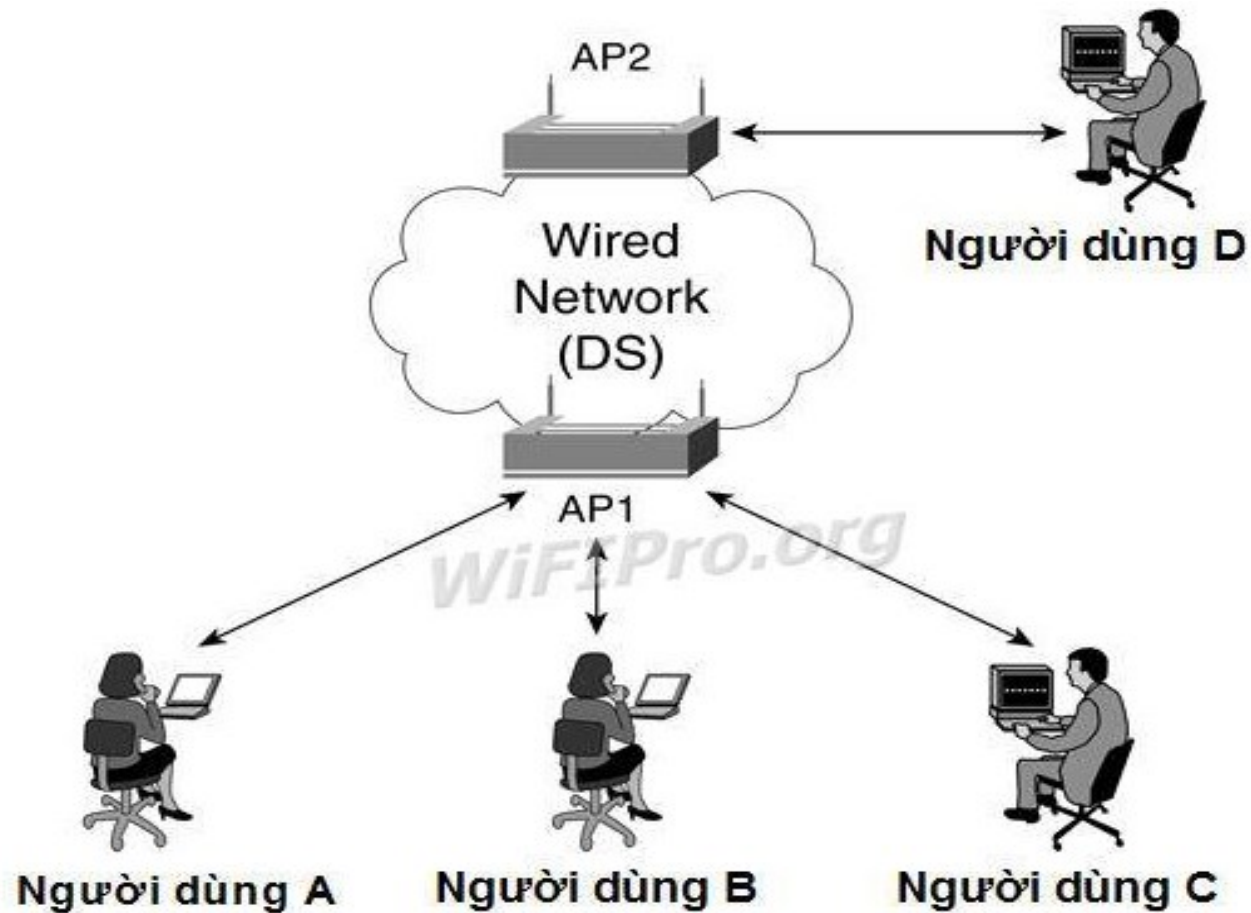
3.2 Mạng BSS

- Thiết bị AP có thể sẽ yêu cầu một trong những điều kiện sau, trước khi cho phép một máy trạm tham gia vào:
 - SSID phải giống nhau.
 - Một tốc độ truyền dữ liệu tương thích.
 - Hoàn tất vấn đề xác thực.

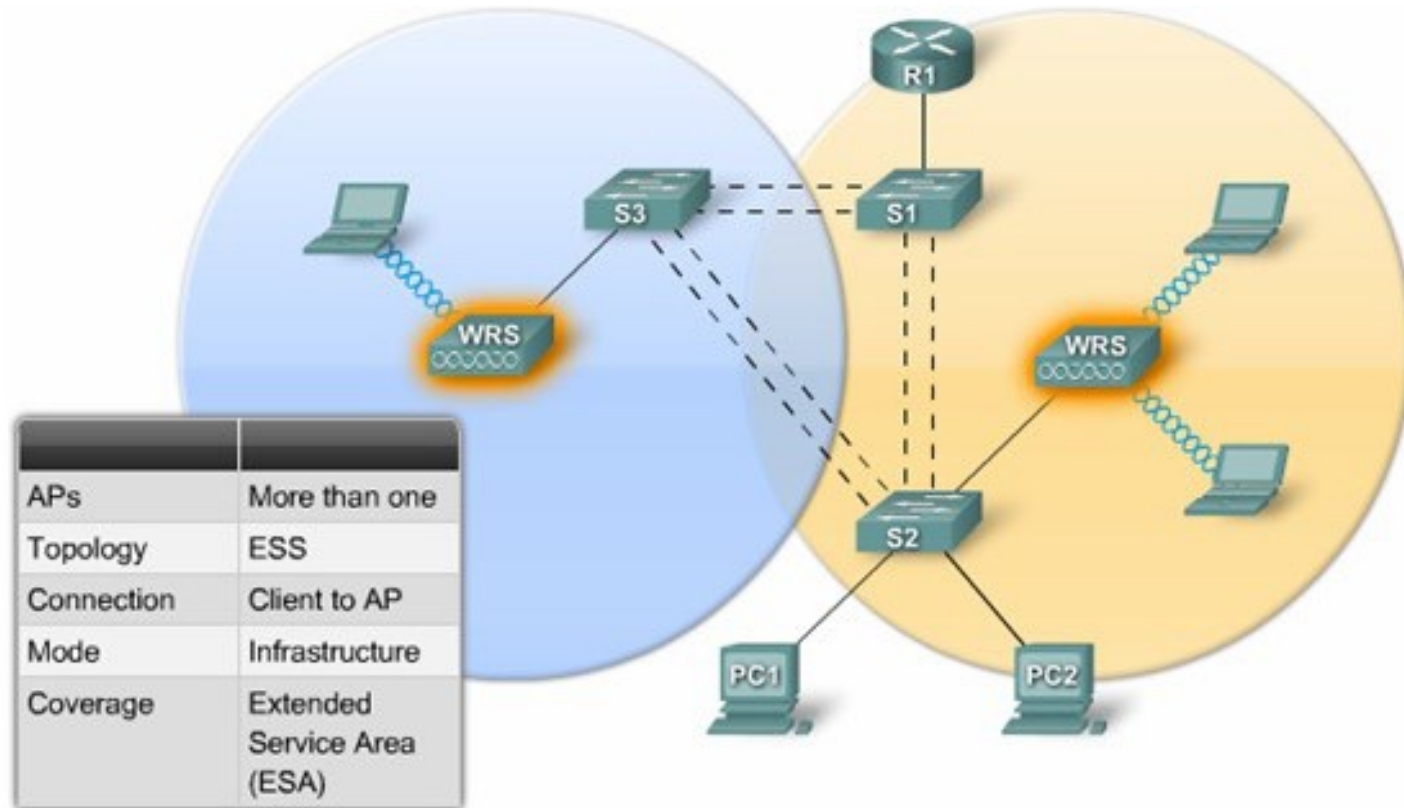
3.2 Mạng ESS

- Mạng ESS thiết lập 2 hay nhiều AP với nhau nhằm mục đích mở rộng phạm vi phủ sóng.
- Một ESS là 1 phân vùng mạng logic.
- Tên mạng của 1 ESS được gọi là ESSID
- Các Cell phải chồng lên nhau 10-15% để đạt được thành công trong quá trình chuyển vùng

3.2 Mạng ESS




3.2 Mạng ESS



3.2 Mạng ESS

Phân biệt: SSID, BSSID, ESSID ???



4. Các chuẩn của mạng WLAN

4. Các chuẩn trọng mạng WLAN

- Mạng WLANs hoạt động dựa trên bộ chuẩn 802.11
- 802.11 được phát triển từ năm 1997 bởi tổ chức IEEE
- Chuẩn này được xem là chuẩn dùng cho các thiết bị di động có hỗ trợ Wireless, phục vụ cho các thiết bị có phạm vi hoạt động tầm trung bình.

4. Các chuẩn trọng mạng WLAN

IEEE 802.11a: Là chuẩn mở rộng của 802.11

- Được đưa vào sử dụng năm 1999
- Hoạt động ở băng tần 5Ghz
- Tốc độ 54 Mbps: 30m:11Mbps, 90m:1Mbps
- Vì hoạt động ở tần số cao hơn nên hiệu suất tốt hơn.

4. Các chuẩn trọng mạng WLAN

IEEE 802.11b: Là chuẩn mở rộng của 802.11

- Được đưa vào sử dụng năm 1999
- Cung cấp truyền dữ liệu trong dải tần 2.4Ghz, tốc độ truyền 1-11Mbps.
- Được sử dụng phổ biến cho các đối tượng doanh nghiệp, gia đình, văn phòng nhỏ.
- Nhược điểm: băng tần dễ bị nghẽn, hệ thống dễ bị nhiễu với các hệ thống khác: lò viba, Bluetooth.
- Không cung cấp dịch vụ QoS.

4. Các chuẩn trọng mạng WLAN

IEEE 802.11g:

- Được đưa vào sử dụng năm 2003.
- Hoạt động ở băng tần 2.4Ghz, tốc độ 54Mbps
- 15m: 54Mbps
- 45m: 11Mbps

IEEE 802.11n:

- Được đưa vào sử dụng năm 2009.
- Hoạt động ở băng tần 2.4Ghz, hoặc 5Ghz.
- Tốc độ 600Mbps
- Được sử dụng phổ biến nhất hiện nay

4. Các chuẩn trọng mạng WLAN

IEEE 802.11ac – wifi thế hệ thứ 5

- Sử dụng năm 2013
- Tốc độ cao gấp 3 lần so với 802.11n (tối đa 1730Mbps)
- Hoạt động tại băng tần 5Ghz

5. Thiết bị sử dụng WLAN

1, Điểm truy cập AP – Access Point:

- Cung cấp cho các máy khách (client) một điểm truy cập vào mạng (nội bộ công ty hoặc phòng học)
- AP là 1 thiết bị song công (Full duplex)



5. Thiết bị sử dụng WLAN

2, Thiết bị dùng cho máy khách:

a, Card PCI Wireless:

- Dùng để kết nối các máy khách vào hệ thống mạng không dây.
- Được cắm vào khe PCI trên máy tính.
- Loại này được sử dụng phổ biến cho các máy tính để bàn (desktop) kết nối vào mạng không dây.



5. Thiết bị sử dụng WLAN

2, Thiết bị dùng cho máy khách:

b, Card PCMCIA Wireless:

- Trước đây được sử dụng trong các máy tính xách tay (laptop) và các thiết bị hỗ trợ cá nhân số PDA.
- Hiện nay các thiết bị này đều được tích hợp sẵn card wireless bên trong thiết bị.



5. Thiết bị sử dụng WLAN

2, Thiết bị dùng cho máy khách:

c, Card USB Wireless:

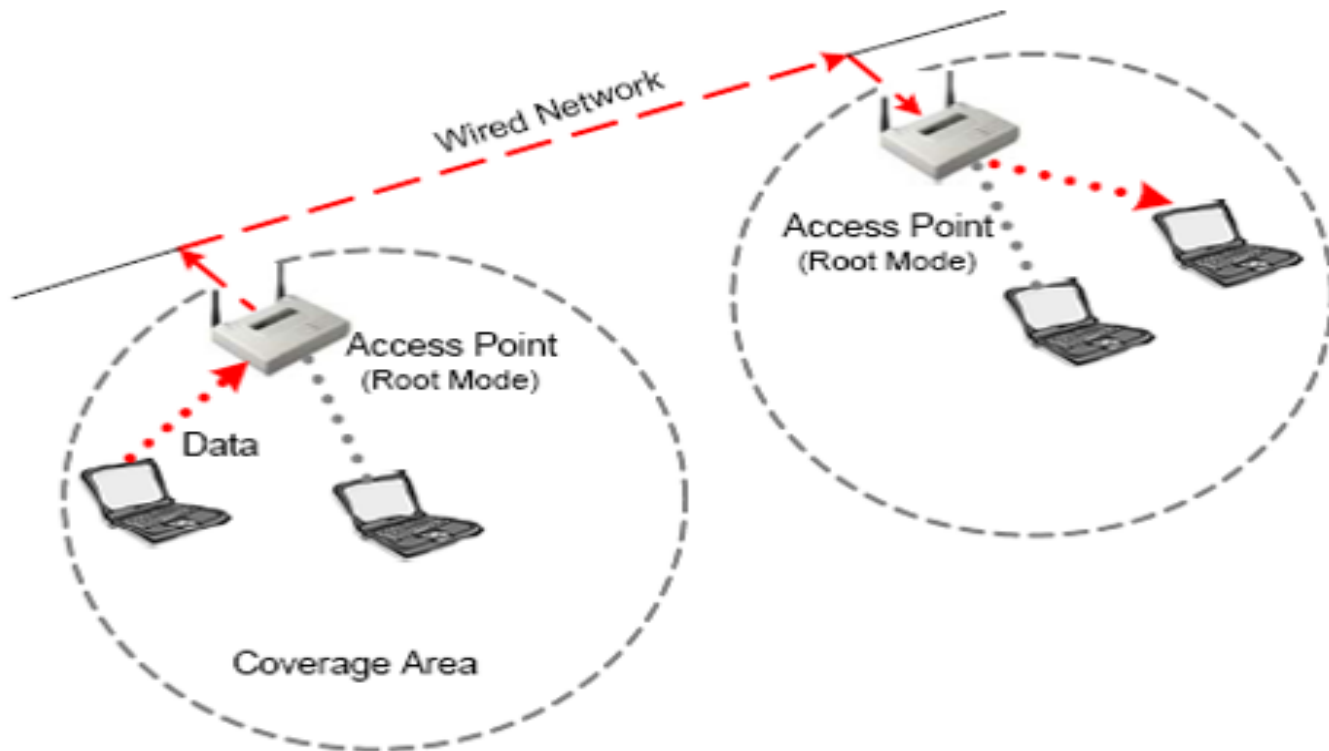
- Loại này rất được ưu chuộng hiện nay dành cho các thiết bị kết nối vào mạng không dây vì tính năng di động và nhỏ gọn.
- Có chức năng tương tự như Card PCI Wireless, nhưng hỗ trợ chuẩn cắm là USB



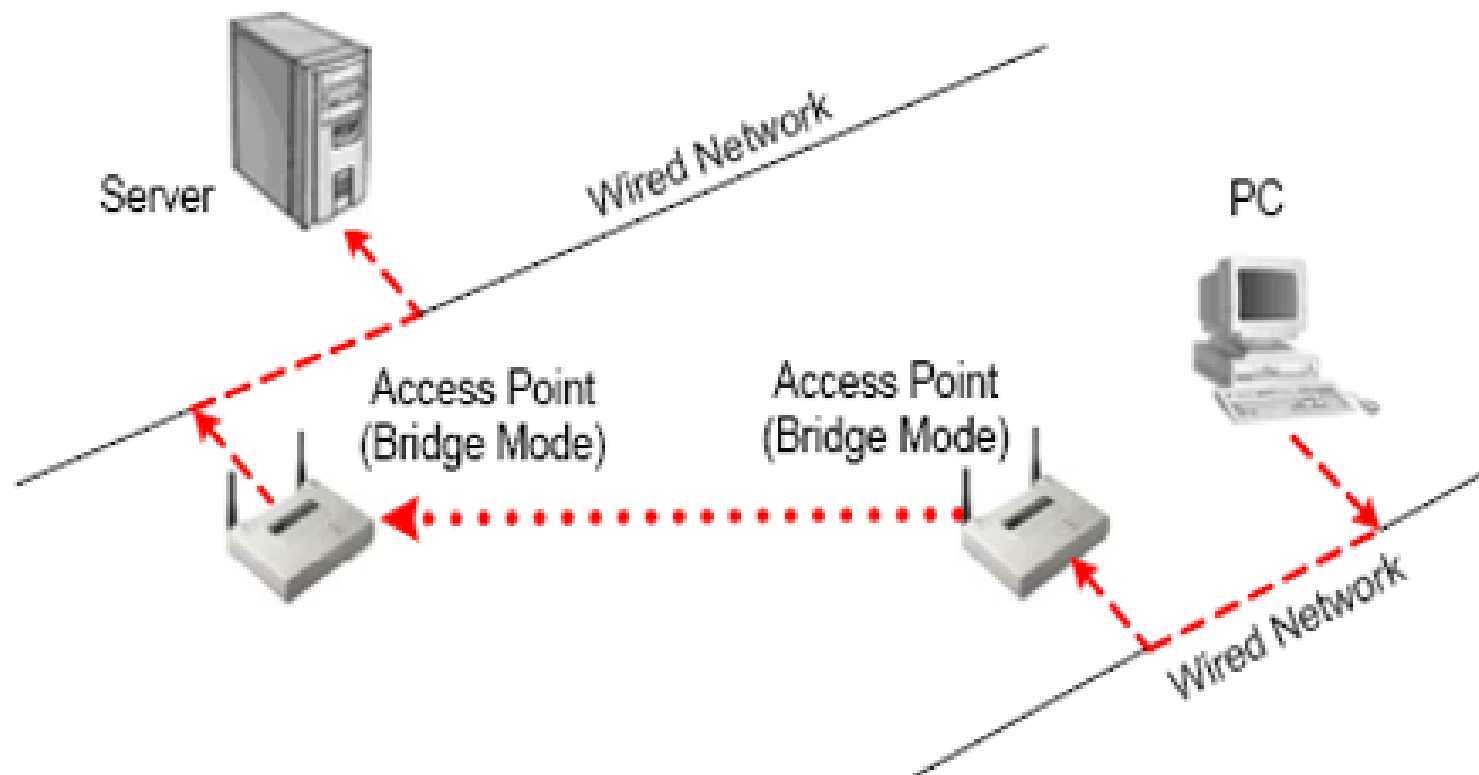
6. Các chế độ hoạt động

- Chế độ gốc (Root mode)
- Chế độ cầu nối (bridge Mode)
- Chế độ lặp (repeater mode)

6.1 Chế độ gốc



6.2 Chế độ cầu nối



6.2 Chế độ lặp

Repeater Mode

Wireless Router
or Access Point



IP: 192.168.0.1

Repeater
(Range Extender/Expander)



TL-WA501G/
TL-WA601G

IP: 192.168.0.10

Mode: Repeater

Desktop/
Laptop



IP: 192.168.0.X



7. Một số hình thức tấn công WLAN

7. Một số hình thức tấn công WLAN

- Tấn công bị động
- Tấn công chủ động
- Tấn công dò tìm mật khẩu
- Tấn công từ chối dịch vụ

7. Một số hình thức tấn công WLAN

■ Tấn công bị động:

- ☐ Kẻ tấn công chỉ lắng nghe trên mạng mà không làm ảnh hưởng tới bất kỳ tài nguyên nào trên mạng.

■ Tấn công chủ động:

- ☐ Kẻ tấn công sử dụng các kỹ thuật làm ảnh hưởng tới mạng

7. Một số hình thức tấn công WLAN

■ Tấn công bị động:

- ☐ Không tác động trực tiếp vào thiết bị nào trên mạng
- ☐ Không làm cho các thiết bị mạng biết được hoạt động của nó
 - **Phát hiện mạng:** Phát hiện Access Point, phát hiện máy trạm kết nối, phát hiện địa chỉ MAC của các thiết bị tham gia, kênh....
 - **Nghe trộm:** Chặn bắt lưu lượng, phân tích giao thức, nguồn và đích kết nối.

7. Một số hình thức tấn công WLAN

- Ví dụ tấn công dò quét:

```
CH 8 ][ Elapsed: 0 s ][ 2015-06-01 04:46
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
74:D0:2B:83:4A:18	-58	4	0 0	6	54e	WPA2	CCMP	PSK	NgocLinh
E8:DE:27:AD:54:8E	-77	4	0 0	6	54e.	WPA2	CCMP	PSK	tang2
00:50:7F:CF:4B:A0	-82	4	0 0	6	54e	WPA2	CCMP	PSK	CHI
44:33:4C:FB:53:82	-84	2	1 0	1	54e	WPA2	CCMP	PSK	TuanAnh
4C:F2:BF:67:E3:A8	-87	2	0 0	1	54e	WPA2	CCMP	PSK	Huyen Trang
E8:DE:27:2F:5F:2E	-52	5	1 0	1	54e.	WPA2	CCMP	PSK	tang3
30:B5:C2:F1:AB:16	-85	2	0 0	1	54e.	WPA2	CCMP	PSK	khong biet
3C:F8:08:1D:7E:20	-72	3	0 0	11	54e	WPA2	CCMP	PSK	tuyen
F8:1A:67:A7:62:BB	-38	4	0 0	13	54e	WPA2	CCMP	PSK	FPT Telecom
4C:F2:BF:75:F9:14	-49	2	0 0	10	54e	WPA2	CCMP	PSK	NguyenHong

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
E8:DE:27:2F:5F:2E	C0:63:94:50:2D:10	-86	12e-12	0	3	

7. Một số hình thức tấn công WLAN

- Tấn công chủ động:
 - Là hình thức tấn công tác động trực tiếp lên thông tin, dữ liệu của mạng.
 - Dò tìm mật khẩu AP
 - Giả mạo AP
 - Tấn công người đứng giữa
 - Từ chối dịch vụ

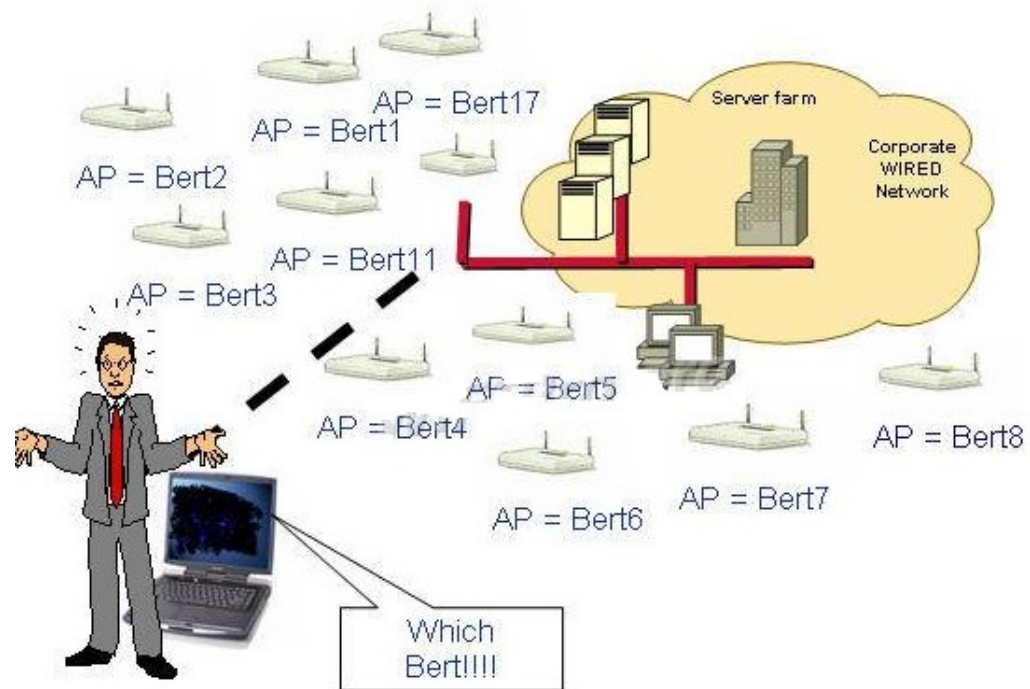
7. Một số hình thức tấn công WLAN

- Tấn công dò tìm mật khẩu:
 - ☐ Vét cạn (WPS - **Wifi** Protected Setup)
 - ☐ Từ điển

7. Một số hình thức tấn công WLAN

■ Tấn công giả mạo AP:

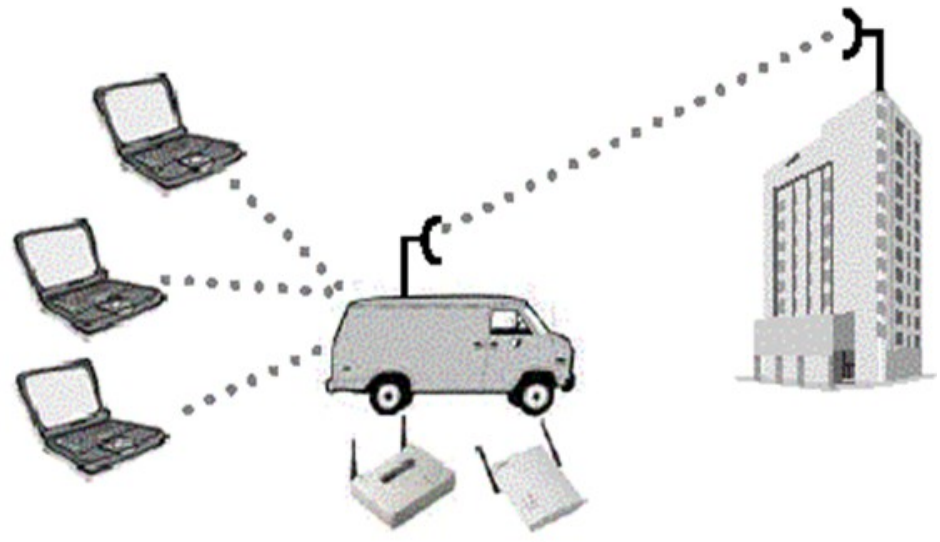
Gửi các gói beacon với địa chỉ vật lý (MAC) giả mạo và SSID giả để tạo ra vô số Access Point giả lập.



7. Một số hình thức tấn công WLAN

■ Tấn công người đứng giữa:

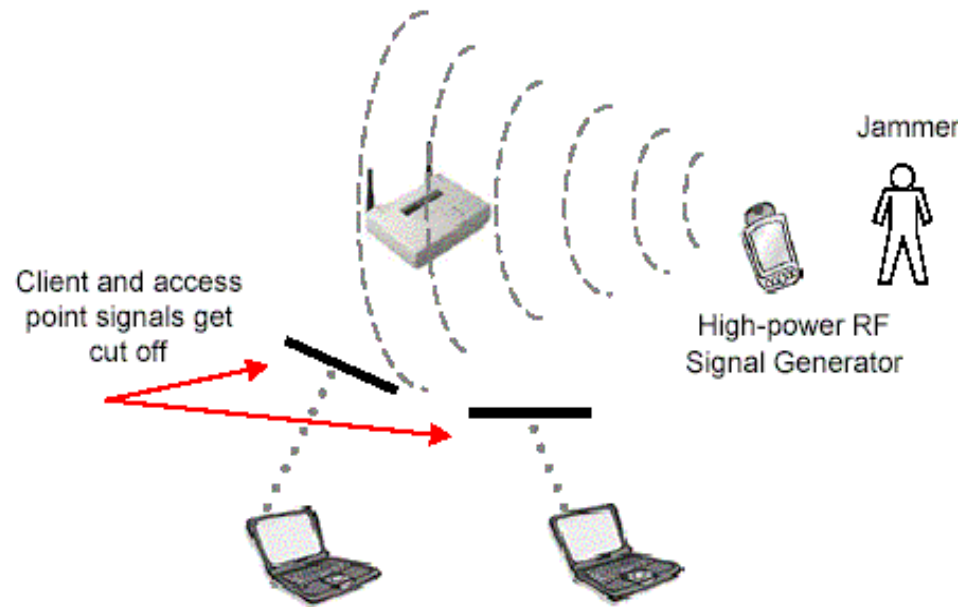
- Kẻ tấn công sử dụng AP giả mạo phát tín hiệu RF tốt hơn
- Thu hút kết nối của máy trạm



7. Một số hình thức tấn công WLAN

■ Tấn công từ chối dịch vụ:

- Sử dụng bộ phát tín hiệu RF (radio frequency) công suất cao
- Làm nhiễu tín hiệu RF





8. An toàn cho WLAN

8. An toàn cho WLAN

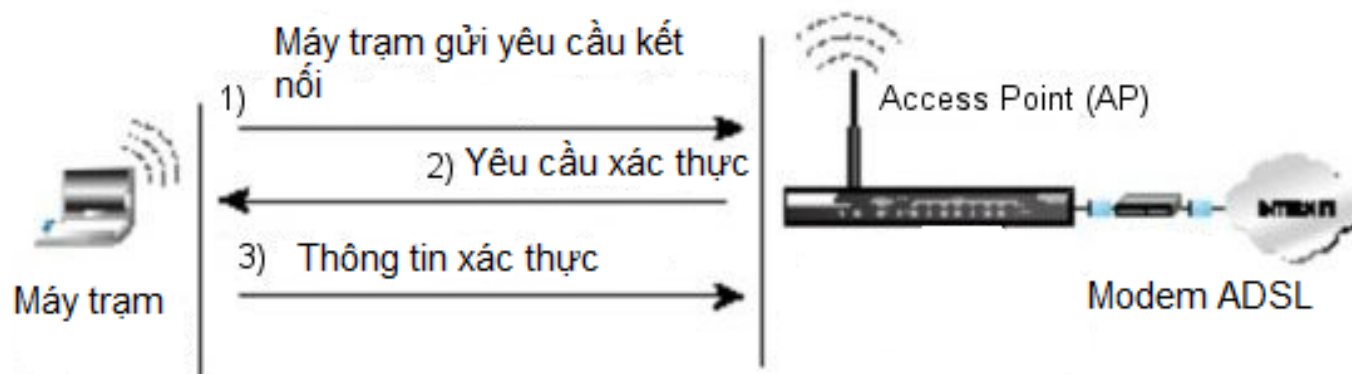
Để cung cấp mức bảo mật tối thiểu cho mạng WLAN thì ta cần hai thành phần sau:

- **Xác thực:** Xác định ai có quyền sử dụng mạng
- **Mã hóa:** Đảm bảo tính riêng tư

8.1 Xác thực

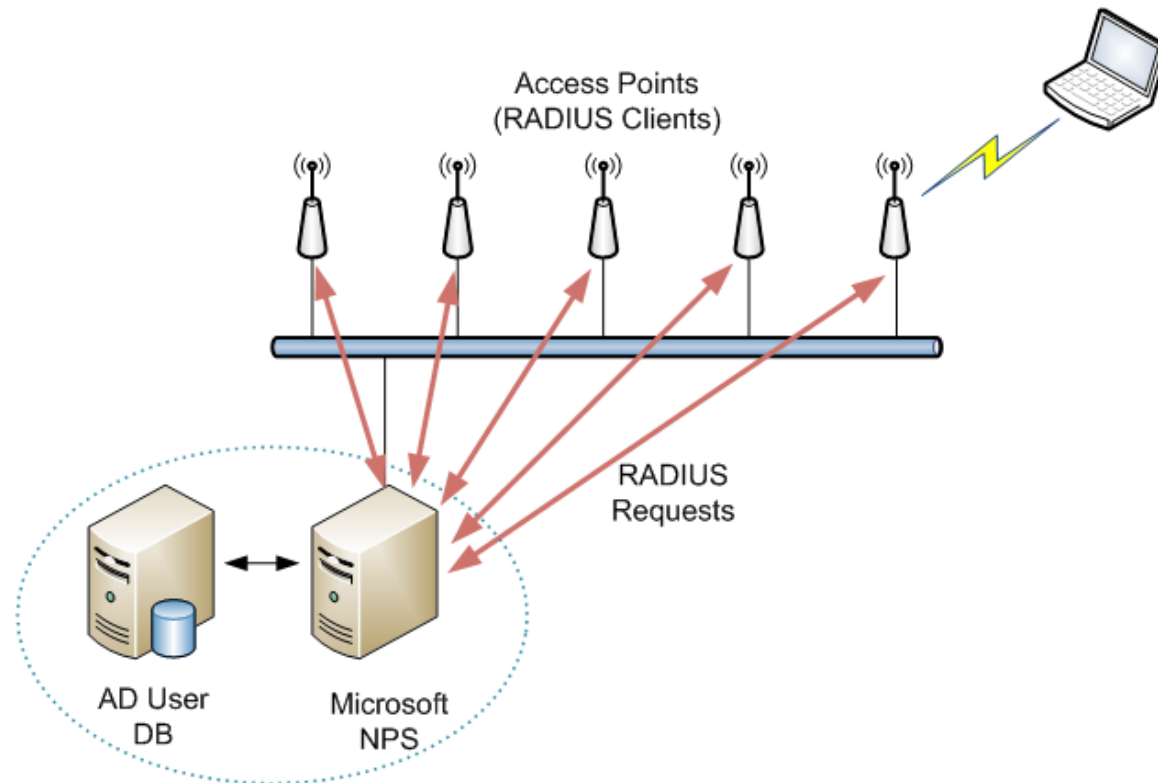
■ Xác thực thông qua SSID và mật khẩu:

- Mỗi mạng không dây đều có định danh duy nhất
- Người dùng muốn gia nhập vào mạng không dây phải biết mật khẩu



8.1 Xác thực

■ Xác thực thông qua máy chủ **RADIUS**:



8.1 Xác thực

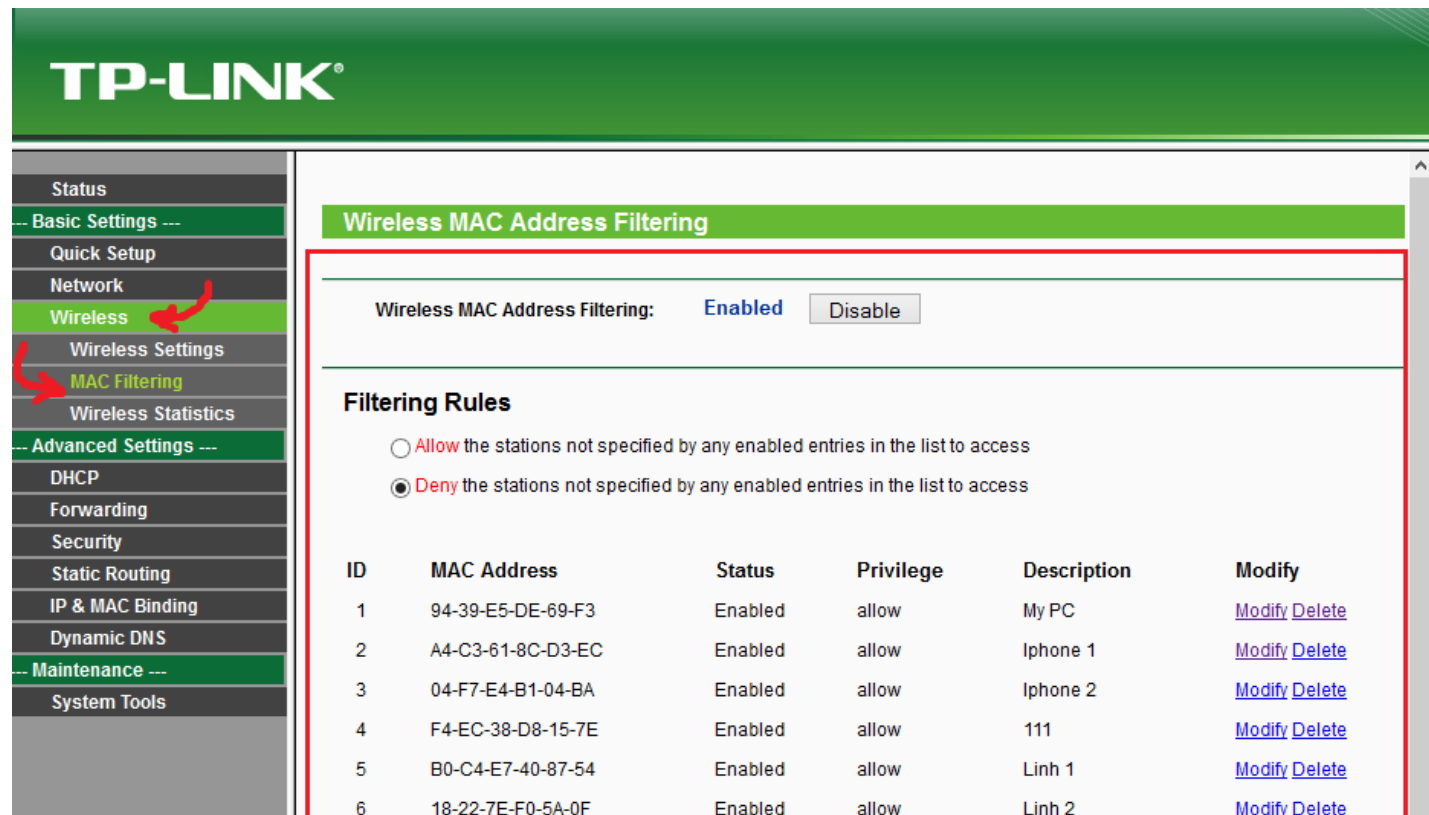
- Sử dụng phương pháp lọc (Filtering)
 - Lọc là phương pháp bảo mật cơ bản sử dụng trong Access Point
 - Mục đích: Cấm những cái không mong muốn, cho phép những cái mong muốn
 - *Lọc thông qua địa chỉ MAC*
 - *Lọc thông qua giao thức*

8.1 Xác thực

- Lọc thông qua địa chỉ MAC
 - Đây là một chức năng có trong hầu hết các Access Point
 - Xây dựng danh sách địa chỉ MAC của máy trạm được phép hoặc không được phép truy cập trong Access Point.

8.1 Xác thực

- Ví dụ về lọc MAC



TP-LINK®

Wireless MAC Address Filtering

Wireless MAC Address Filtering: **Enabled**

Filtering Rules

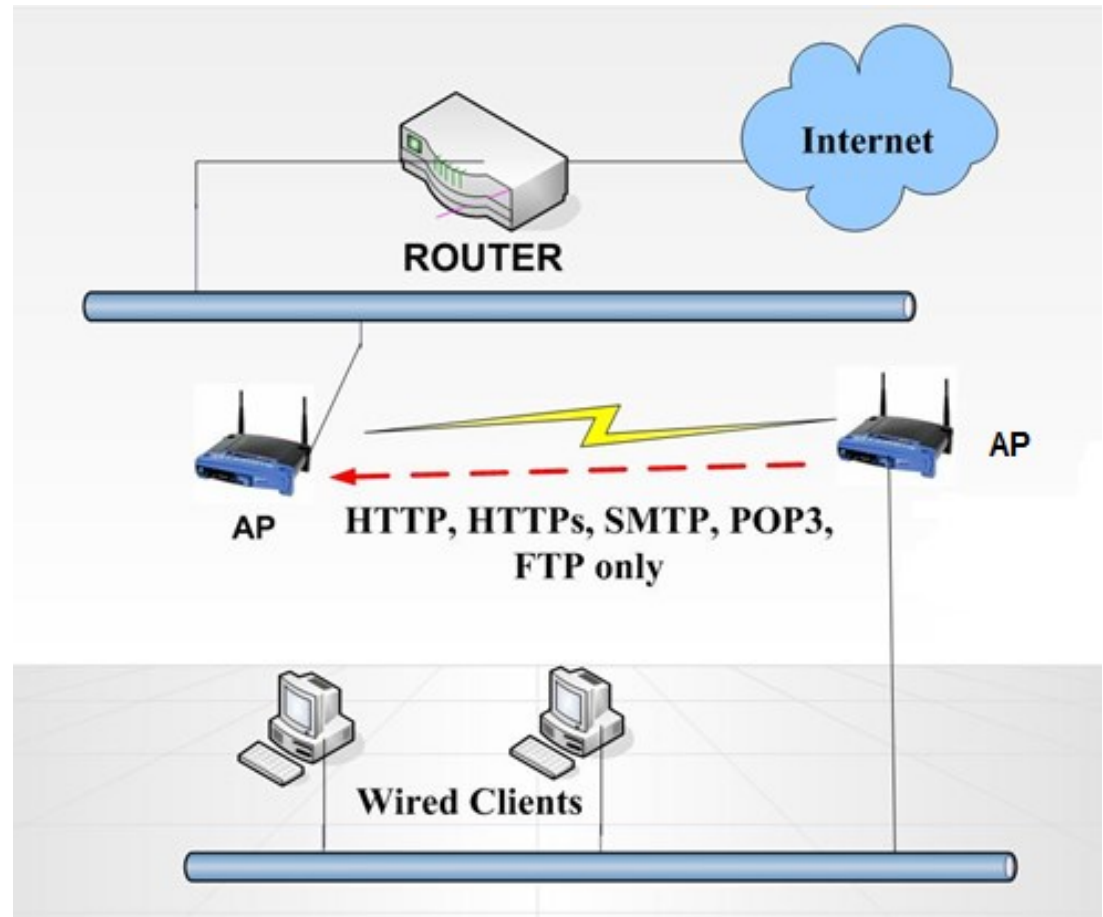
☐ Allow the stations not specified by any enabled entries in the list to access

☒ Deny the stations not specified by any enabled entries in the list to access

ID	MAC Address	Status	Privilege	Description	Modify
1	94-39-E5-DE-69-F3	Enabled	allow	My PC	Modify Delete
2	A4-C3-61-8C-D3-EC	Enabled	allow	Iphone 1	Modify Delete
3	04-F7-E4-B1-04-BA	Enabled	allow	Iphone 2	Modify Delete
4	F4-EC-38-D8-15-7E	Enabled	allow	111	Modify Delete
5	B0-C4-E7-40-87-54	Enabled	allow	Linh 1	Modify Delete
6	18-22-7E-F0-5A-0F	Enabled	allow	Linh 2	Modify Delete

8.1 Xác thực

- Lọc thông qua giao thức:



8.2 Phương pháp mã hóa

- Sử dụng mã hóa để bảo vệ dữ liệu truyền đảm bảo bí mật, toàn vẹn.
- Chính sách an toàn cần xác định rõ thời điểm cần thiết cũng như phương thức thực hiện mã hóa.
- Một số phương pháp mã hóa sử dụng trong mạng không dây: WEP, WPA, WPA2, VPN.

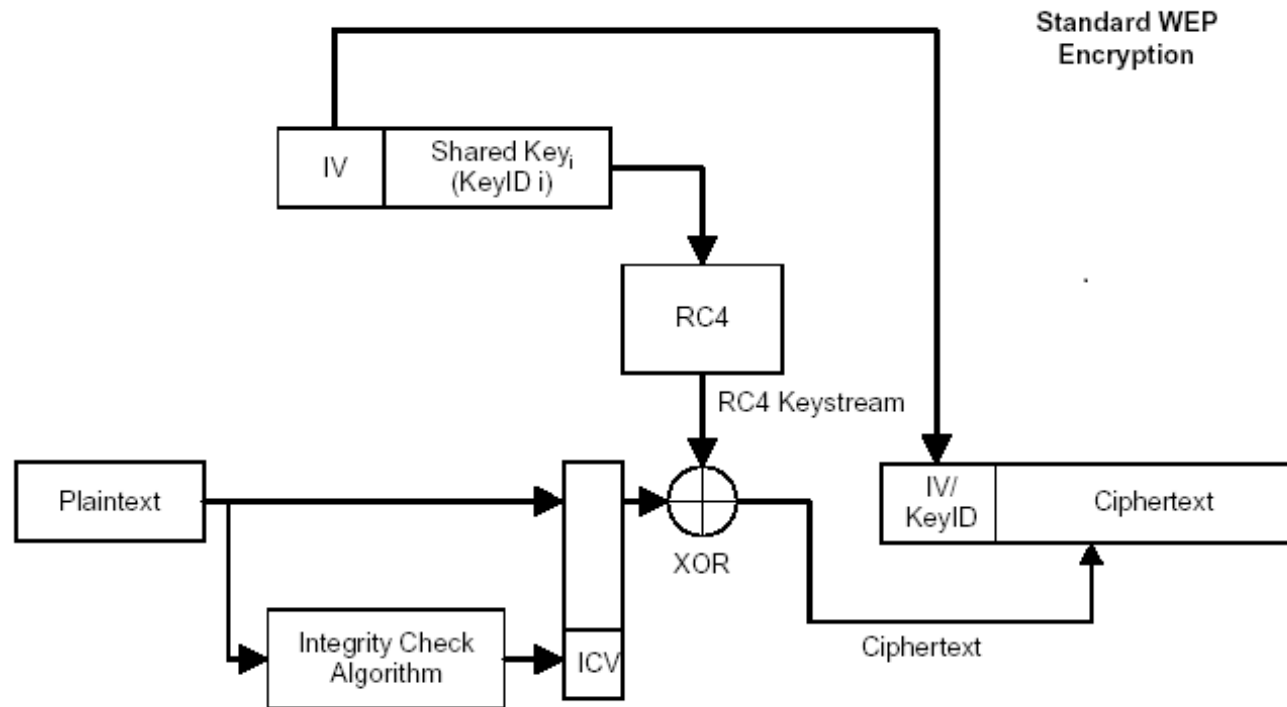
8.2 Phương pháp mã hóa

Mã hóa sử dụng WEP (Wired Equivalent Privacy)

- Được thiết kế để đảm bảo tính riêng tư của dữ liệu trong mạng không dây
- Sử dụng thuật toán mã hóa RC4, mã hóa dữ liệu 40 bit.
- Điều khiển việc truy cập, ngăn chặn sự truy cập của những Client không có khóa phù hợp
- Bảo vệ dữ liệu trên truyền bằng mã hóa chúng và chỉ cho những client có khóa WEP đúng giải mã

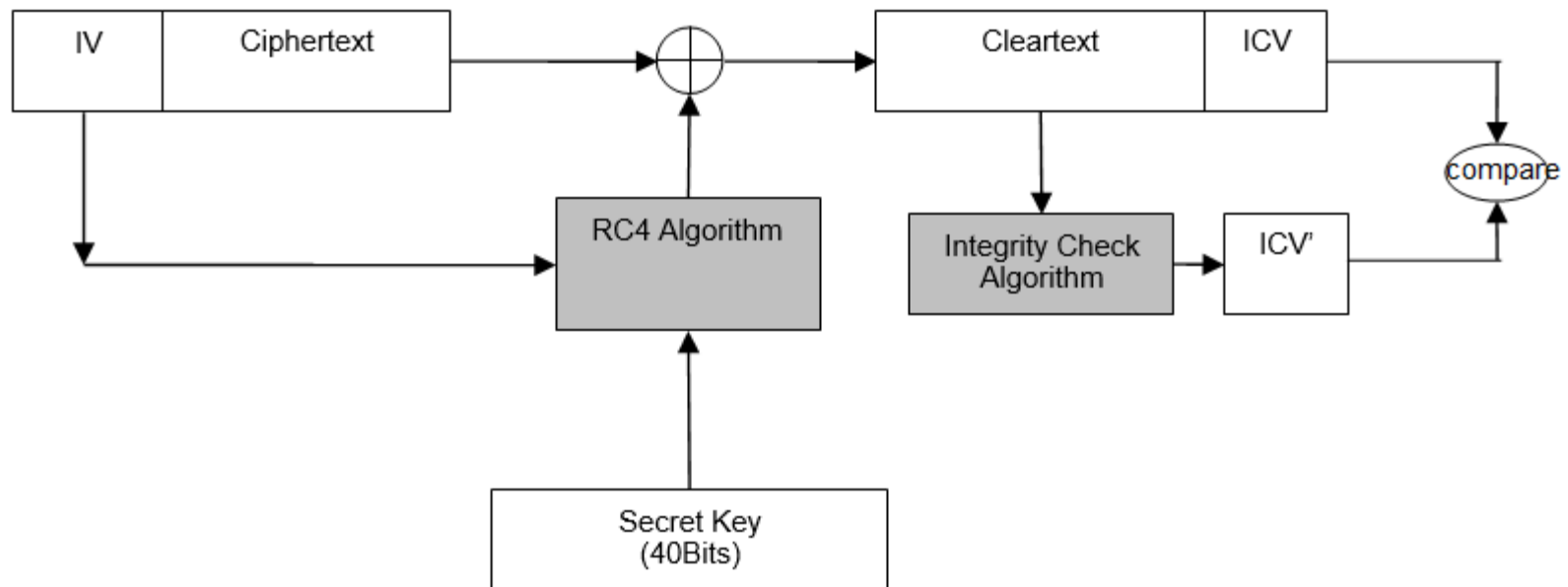
8.2 Phương pháp mã hóa

Tiến trình mã hóa của WEP:



8.2 Phương pháp mã hóa

Tiến trình giải mã của WEP:



8.2 Phương pháp mã hóa

Nhược điểm của WEP (1997):

- WEP sử dụng khóa cố định được chia sẻ giữa một Access Point (AP) và nhiều người dùng (users) cùng với giá trị IV.
- Độ dài khóa ngắn (64 bit): Với 24 bit IV, 40 bit khóa
- Thuật toán mã hóa RC4 là thuật toán yếu.
- Giá trị IV không được mã hóa lúc truyền.

8.2 Phương pháp mã hóa

Mã hóa sử dụng WPA (2003):

- Sử dụng giao thức thay đổi khóa tự động TKIP. Thay đổi khóa mã cho mỗi gói tin.
- Vẫn sử dụng thuật toán RC4, nhưng chiều dài khóa mã hóa 128 bit.
- IV có chiều dài 48 bit.
- Sử dụng thuật toán kiểm tra toàn vẹn thông điệp MIC (Message Integrity Check)

8.2 Phương pháp mã hóa

Mã hóa sử dụng WPA2 còn gọi là 802.11i

- Được sử dụng bắt đầu từ năm 2004
- WPA2 sử dụng thuật toán mã hóa AES (Advance Encryption Standar)
- Mã khóa của AES có kích thước khối 128 bít, độ dài khóa 128, 192 hoặc 256 bit
- Sử dụng kết hợp các thuật toán trao đổi khóa TKIP

Tìm hiểu mở rộng

- Tìm hiểu về hệ thống phát hiện xâm nhập cho mạng WLAN.
- Cài đặt, cấu hình công nghệ VPN cho mạng không dây WLAN
- Tìm giải pháp để phòng chống các loại tấn công vào mạng không dây WLAN