# 무선랜 취약점분석

작성자 : silverhwak

# 목 차

# 1. 무선 랜의 정의

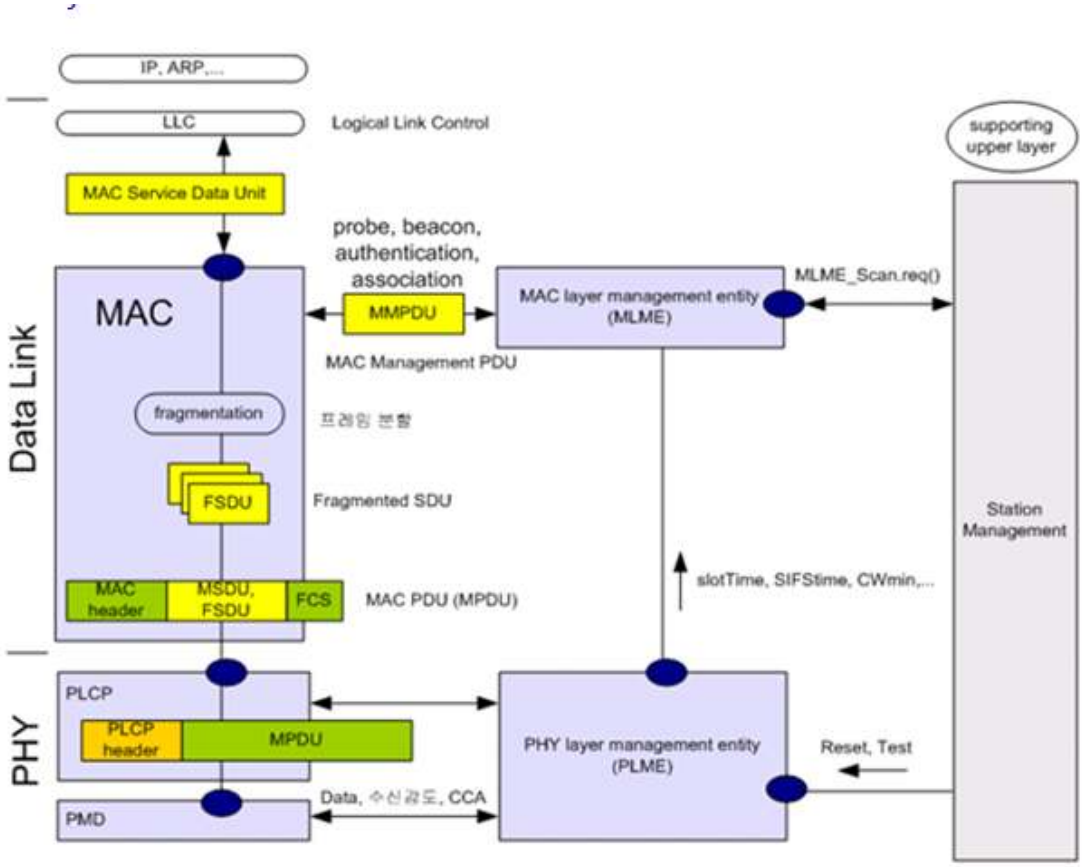
-두 대 이상의 컴퓨터가 선 없이 연결한 상태로, 무선으로 된 로컬 영역 네트워크을 일컬음. 무선 랜은 스프레드 분광이나 전자기파 기반의 OFDM 변조 기술을 사용하여 제한된 지역 안에 있는 기기끼리 서로 통신할 수 있게 해 줌. 이로써 사용자가 무선 랜 지원 지역을 돌아다니며 네트워크에 접속 가능하게 함.

무선 랜의 장점
편의성: 가정이나 사무실에서 무선 네트워크 장비가 있는 곳이라면 무선 네트워크를 쉽게 사용.
휴대성: 일반 노동 환경 밖에서도 인터넷에 접근. 커피숍과 같은 공공 장소에서 무선 인터넷 접속에 비용을(얼마) 내지 않고 사용.
생산성: 장소를 옮겨 다니며 원하는 네트워크의 접속을 유지.
배치: 무선 네트워크를 처음 설치할 때에는 하나 이상의 액세스 포인트를 요구. 한편 유선 네트워크는 수많은 장소에 케이블선을 깔아야 하므로 비용이 늘어나는 문제점이 존재.
확장성: 무선 네트워크는 기존의 장비를 사용하여 수많은 고객을 받아들일 수 있음.

단점
보안: 무선랜은 라디오 주파수를 사용하여 컴퓨터에 네트워크를 제공. 공간과 비용을 위해 최종 컴퓨터에 설치되어 있는 무선 랜카드의 성능은 대체적으로 좋지 않음. 신호를 어느 정도 잡기 위해, 무선랜 수신 장치는 상당히 많은 양의 전력을 사용. 다시 말해, 무선랜 성능이 좋지 않은 주변 컴퓨터가 무선 패킷을 가로챌 수 있을 뿐 아니라, 좋은 품질에 적은 돈을 소비하려는 사용자가 눈에 잘 띄는 곳에서 패킷을 가져갈 수 있음.
지원 범위의 한정: 일반적으로 쓰이는 802.11g 네트워크는 수십 미터의 거리를 지원. 일반 가정의 규모가 큰 경우 이러한 거리는 충분하지 못할 수 있음. 범위를 넓히려면 리피터나 추가적인 액세스 포인트 구매가 필요.
신뢰성: 다른 라디오 주파수 비슷하게, 무선 네트워크 신호는 다양한 통신 간섭에 노출.
속도: 대부분의 무선 네트워크는 일반적인 유선 네트워크에 비해 느린 편.

# 2. 802.11 Layer의 구조

802.11은 흔히 무선 랜, wi-fi라고 부르는 local area를 위한 컴퓨터 무선 네트워크에 사용되는 기술.




<802.11 Layer의 구조>

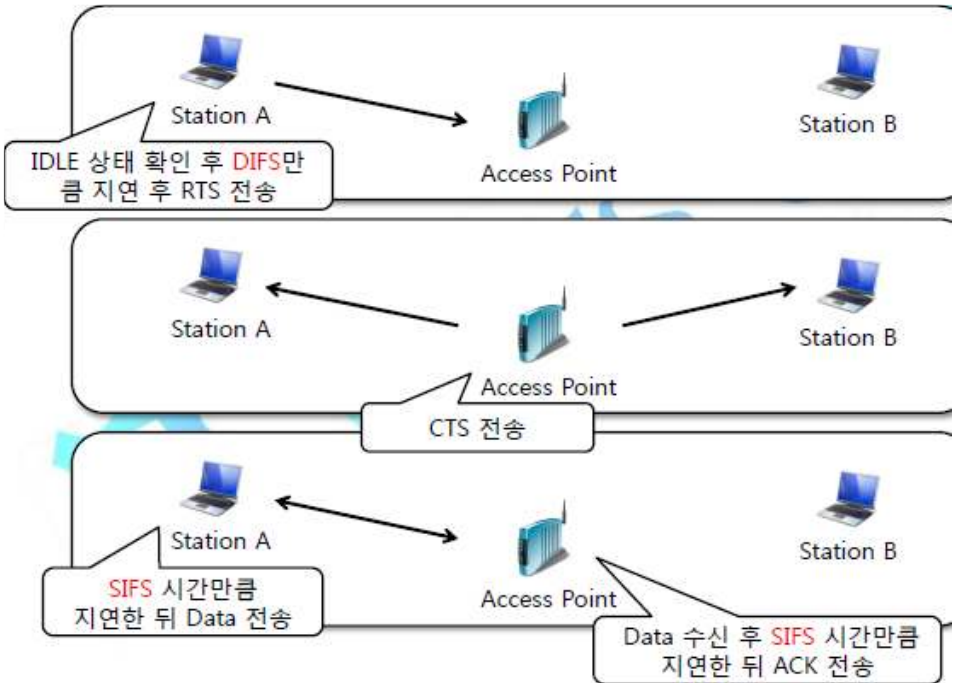
각 블록의 설명

| | |
|---|---|
| Physical Medium Dependent | 변복조를 하는 무선 모뎀 기능을 수행. |

| | |
|---|---|
| | 적외선, RF등의 전송매체의 종류 마다 변복조 방식이 다르기 때문에 물리 매체 종속 계층이라 함. |
| Physical Layer Convergence Protocol | 하부에 다양한 종류의 PMD가 있고, 상위에는 PMD 종류와 무관한 MAC계층이 있으므로, 이들 간의 동작을 정합시키는 역할을 수행.<br>MAC계층으로부터 전달된 MAC_PDU( MPDU )에 Preamble과 PLCP헤더를 추가한 후, 모뎀기능을 수행하는 PMD에 비트열로 전달하여, 송수신 동작을 수행한다. |
| MAC 계층 | 상위 계층 패킷(MAC Service Data Unit - MSDU)나 probe, becacon등의 MAC Management PDU(MMPDU)를 MPDU에 수납 한 후 전송<br>-필요에 따라 MSDU나 MMPDU를 여러 개의 Fragemented SDU(FSDU)로 분할 한 후, 각각을 MPDU로 전송, 헤더의 탈/부착, 신호의 세기 조졸, 데이터 도착 유무확인<br>종류는 Management Frame, control Frame, Data Frame이 존재 |
| MAC Layer Management Entity | 전원관리, 탐색, join, 인증, 결합, 리셋, 시간동기 등의 MAC 계층의 운영에 필요한 관리기능인 MMPDU(probe, beacon, association, authentication)를 수행. |
| PHY Layer Management Entity | 물리계층부에 대한 리셋, 모뎀의 동작값(Slot Time, 송수신 절환 지연시간, Preamble의 길이 등)을 설정하거나 설정 값을 읽음. |

# 3. 802.11 MAC

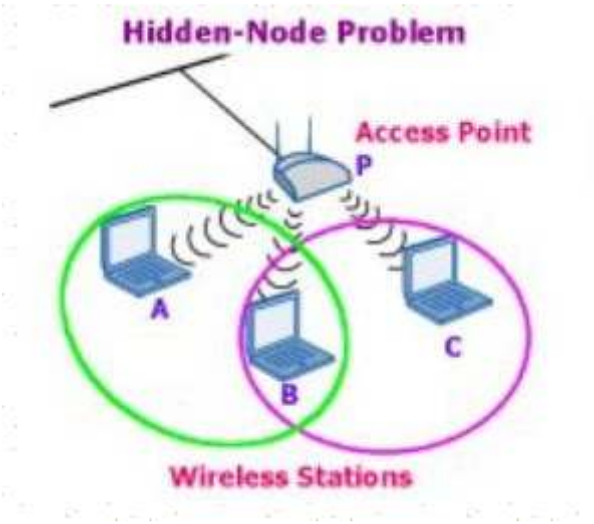
DCF ( Distributed Coordination Fuction )
데이터를 송신 하기전 다른 station이 데이터를 송신중인지 확인하고 일정시간동안 대기하는 방식 ( 경쟁방식 )
CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance )(충돌을 사전에 회피)




<DCF ( Distributed Coordination Fuction )>

PCF ( Point Coordination Fuction )
AP ( Access Point ) 가 단말에게 전송할 데이터가 있는지 확인한후 , 전송할 데이터가 있는 단말에게 전송권한을 줌 (Token Ring과 유사 )
그러나 CSMA/CA의 경쟁방식과는 달리 무경쟁 방식이고 현재는 쓰이지 않음.

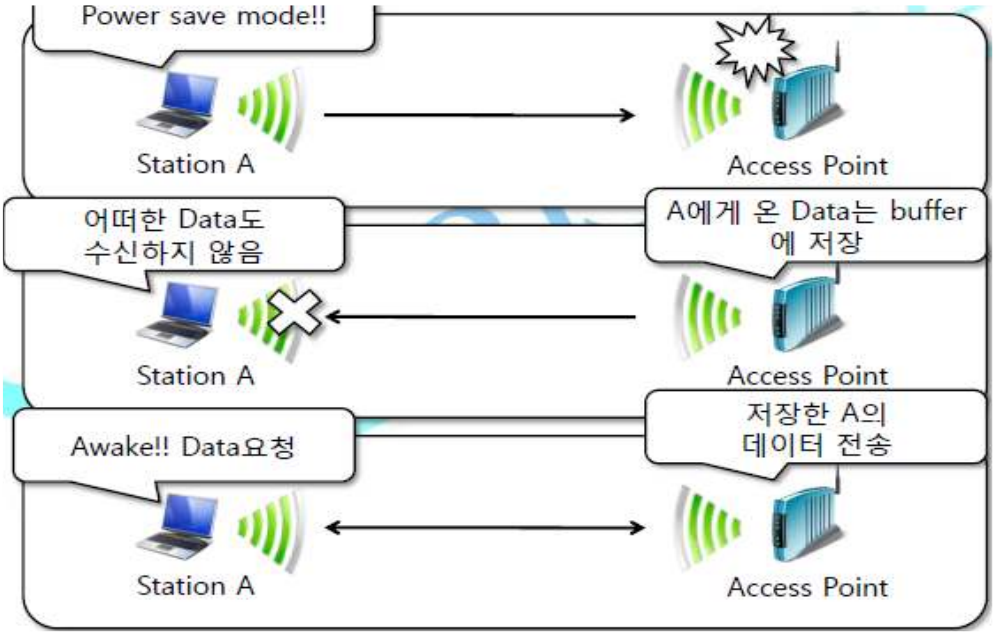
802.11 MAC 의 특징
1. MAC 계층에서의 ACK Frame 사용과 Frame 분할 기능 (TCP/IP Layer의 4계층의 ACK + 3계층의 Fragment)
   TCP Flag(4계층) + IP Fragment offset(3계층)
   -Frame 을 전달받은 수신 측 MAC은 반드시 이에 대한 명시적인 확인을 해주기 위해 ACK Frame으로 응답
2. 긴 Frame 전송 시 무선구간 품질을 위해 여러 개의 짧은 Frame으로 조각내어 전송
3. Hidden-Node 문제
   -AP를 중심으로 통신하는 각 Station 들의 시야를 기준으로 보았을 때 자신의 Carrier 감지 범위를 벗어난 다른 Station은 Hidden-Node가 됨




<hidden node 발생>

4. 전원 공급 문제를 줄이기 위한 Power Saving Mode

-무선은 신호감지에 많은 power가 필요해서 내가 굳이 보낼 데이터가 없을 때는 자는것, 어떠한 일도 처리 하지 않는다. 심지어 Broadcast도 처리를 하지 않는다.




<Power Saving Mode>

가. Power Saving Mode를 AP에게 알려줌

나. 신호가 들어오면 AP가 버퍼에 쌓아둠

다. 전원이 들어오면 버퍼에 쌓아둔 패킷을 보내줌

# 4. Lan card mode

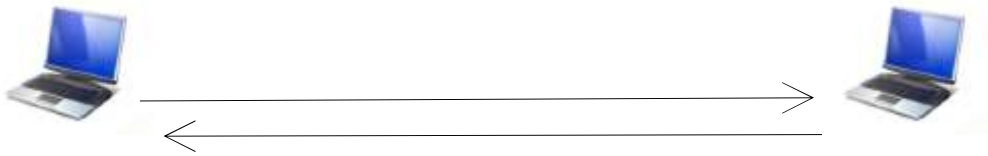
managed mode

-무선 클라이언트( Station )가 Wireless AP 로 바로 연결할때 사용
모든 통신진행을 Wireless AP에게 맡김

station A Access point station B

Ad-Hoc

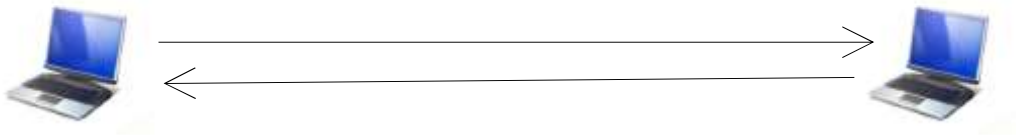
-컴퓨터들 서로가 직접 연결하기 위해 사용하는 모드
각 클라이언트가 통신에 관한 모든 책임을 지게 됨



station A station B

master mode

-무선 네트워크 인터페이스 카드( NIC )가 다른 드라이버 소프트웨어와도 결합해서 작동할수 있게 한다.이를통해 다른 컴퓨터는 이것을 Wireless AP 로 인식하기도 한다.

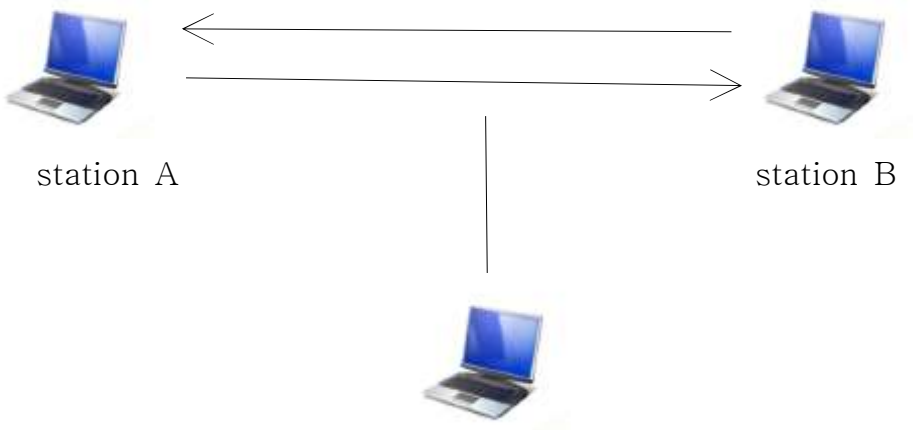


station A station B

Monitor mode

-RFMON( Radio Frequence Monitoring ) 모드

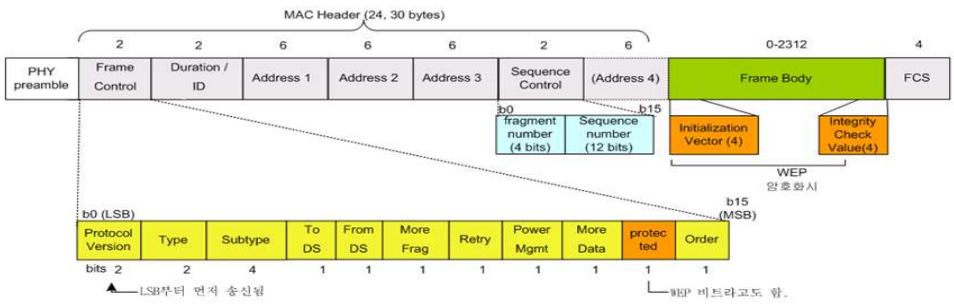
무선 클라이언트에게 데이터를 전송하거나 받지는 못하는 대신 오가는 패킷을 볼수는 있다.




# 5. mac frame

-LAN 상에서 MAC계층의 기능은 상위계층(LLC)으로부터 전달되는 패킷을 접속되어 있는 물리적인 네트워크의 Frame Format에 맞추어 주는 역할을 한다.

## 가.구조



# header 설명

| | |
|---|---|
| MAC Header | MAC header의 길이는 Address 4영역의 유무에 따라 30또는 24 바이트이며, 프레임 바디의 최대길이는 2312바이트.<br>또한, WEP암호화가 사용된 경우, 8바이트가 추가. 참고로 이더넷과 마찬가지로 각 바이트의 비트들은 LSB부터 전송. |
| Frame Control | Protocol Version<br>Type : 해당 프레임이 control( RTS, CTS, ACK ), management( authentication, association ), data Frame인지를 구분하는 2비트<br>00 = Management Frame<br>01 = Control Frame<br>10 = Data Frame<br>11 = Unused<br>Subtype : 각 type의 frame에 대한 세부적인 정보. 각 type과 subtype의 비트들은 MSB부터 기술.<br>-이것은 실제 Frame의 송신 및 수신시 식별하기가 용이하도록 한 것일 뿐, 실제 전송은 각 바이트 별로 LSB가 먼저 송신.<br>To DS 와 From DS : AP를 경유하여 DS(Distribution System)으로 향하는 Data Frame인지 DS로부터의 Data Frame인지를 표시.<br>More Fragment<br>Retry<br>Power management<br>-Station이 곧 전원절약 모드로 들어가는 경우 = 1<br>-Station이 곧 활성 모드로 들어가는 경우 = 0<br>More data : 전원절약모드에서 AP가 단말에게 전달해야 할 frame이 더 있음을 표시.<br>Protect( WEP ) : 해당 프레임이 WEP, TKIP, CCMP등의 무선 구간 암호방식에 의한 암호화가 되어 있음을 표시.<br>Order : 1인 경우, 분할된 프레임들을 재조립할 때, 순서를 지켜서 처리하도록 요구. |
| Duration/ID | Duration : 이 시간 동안 다른 단말들의 채널 사용이 연기되도록 무선 링크의 사용을 예약하는 시간 값인 Net Allocation Vector(NAV)값이 수납.<br>-최상위 비트의 값은 0이고 나머지 15비트 값은 usec단위의 NAV값.<br>Association ID : 전원절약 모드에 있는 단말이 주기적으로 깨어나면서, 그 동안 자신에게 전달되어야 할 프레임을 AP가 보 |

<table>
<tr><td></td><td>관하고 있는지 질의하는 PS-Poll 메시지를 송신할 때, 자신이 결합된 AP로부터 부여 받은 결합번호(AID)를 Duration/AID 영역에 수납하여 전송.<br>AP는 버퍼를 검사하여, 이 AID에 해당되는 단말에게 전달되어야 할 프레임을 선택하여, 이것을 단말에게 전달.</td></tr>
<tr><td>Address 1,2,3,4</td><td>DA와 SA등 2개의 주소만 사용하는 이더넷과 달리, 무선 LAN에서는 4개의 6바이트 길이의 주소가 사용.<br>-하지만, 한 frame에 A4가 없을 수도 있음.<br>-이러한 4개의 주소 영역의 의미는 ToDS, FromDS 비트에 의해 결정.<br>-일반적으로, A1은 수신측 주소이고, A2는 송신측 주소.<br>Destination Address (DA) : 최종목적지 주소<br>Source Address (SA) : Frame의 최초 송신지 주소<br>Receiver Address (RA)와 Transmitter Address (TA) : 서로 다른 AP를 경유하는 경우, 즉, DA와 SA간에 경유하는 수신측 AP와 송신측 AP의 이더넷 주소이다.<br>BSSID : AP의 MAC Address<br><br><table><tr><td></td><td>ToDS</td><td>FromDS</td><td>Address1</td><td>Address2</td><td>Address3</td><td>Address4</td></tr><tr><td>ToAP</td><td>1</td><td>0</td><td>BSSID</td><td>SA</td><td>DA</td><td>unused</td></tr><tr><td>FromAP</td><td>0</td><td>1</td><td>DA</td><td>BSSID</td><td>SA</td><td>unused</td></tr><tr><td>Within Wireless AP</td><td>1</td><td>1</td><td>RA</td><td>TA</td><td>DA</td><td>SA</td></tr><tr><td>Ad-hoc</td><td>0</td><td>0</td><td>DA</td><td>SA</td><td>BSSID</td><td>unused</td></tr></table></td></tr>
<tr><td>Sequence Control</td><td>2바이트의 이 영역은 매 frame당 할당되는 순서번호와 분할 frame의 순서번호이다.<br>-이들은 모두 ACK의 손실에 의한 재전송 검사와 재조립할 때 사용.<br>Fragment Number(4비트) : 한 Frame이 여러 개의 Frame으</td></tr>
</table>

| | |
|---|---|
| | 로 분할되어 전송되는 경우, 이들간의 순서를 구분하도록 하는 번호.<br>Sequence Number(12비트) : 순서번호는 매 Frame 전송 시마다 1씩 증가된다. 물론 재전송되는 Frame의 경우, 순서번호는 증가하지 않음. |
| Frame Body | 제어 및 관리용 정보나 LLC와 같은 상위계층 메시지 즉, MSDU가 수납.<br>이 영역의 최대 사이즈는 2304바이트.<br>Frame body영역이 Wired Equivalent Privacy( WEP )으로 암호화될 경우 Frame Body는 각각 4바이트 길이의 Initialization Vector( IV )와 Integrity Check Value( ICV ) 등이 추가.<br>분할 될 경우, 최소 길이는 256바이트.<br>ARP나 IP같은 상위 계층 패킷들은 항상 LLC에 수납되어 전송. |
| FCS | 4바이트의 오류검사 코드 |

## 나.설명

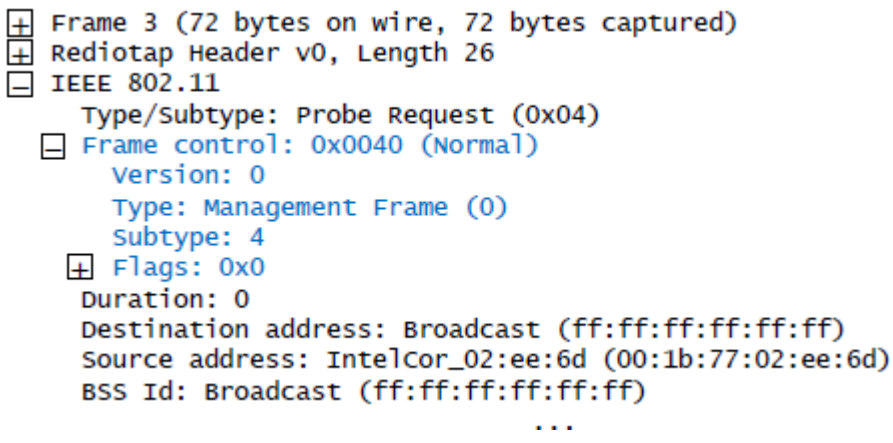
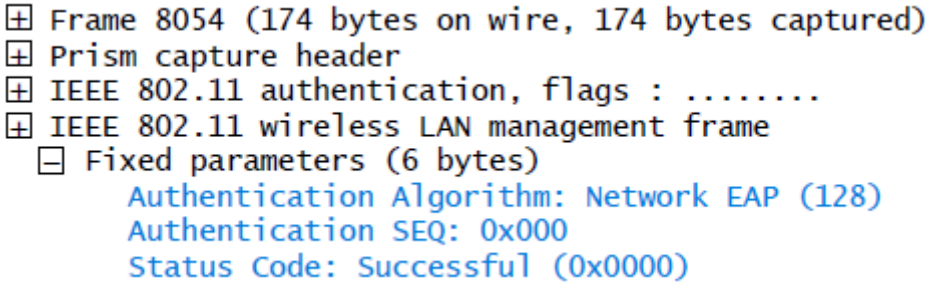
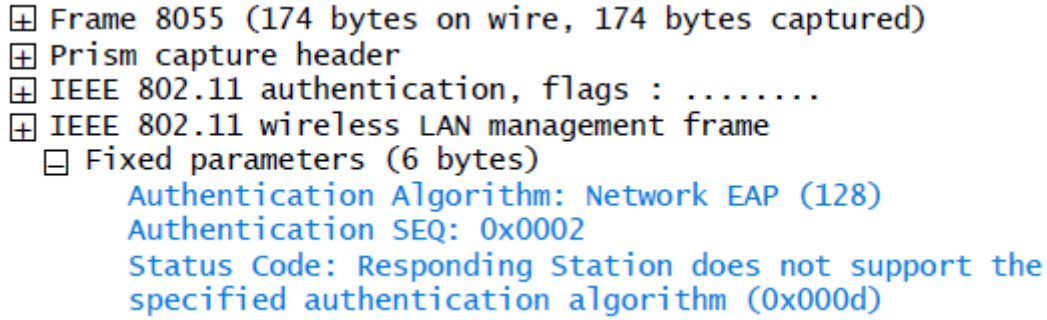
### 1.802.11 Management Frames ( 관리 용도 )

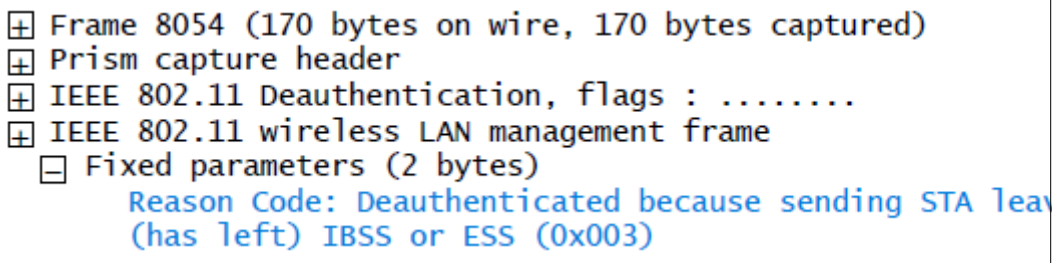
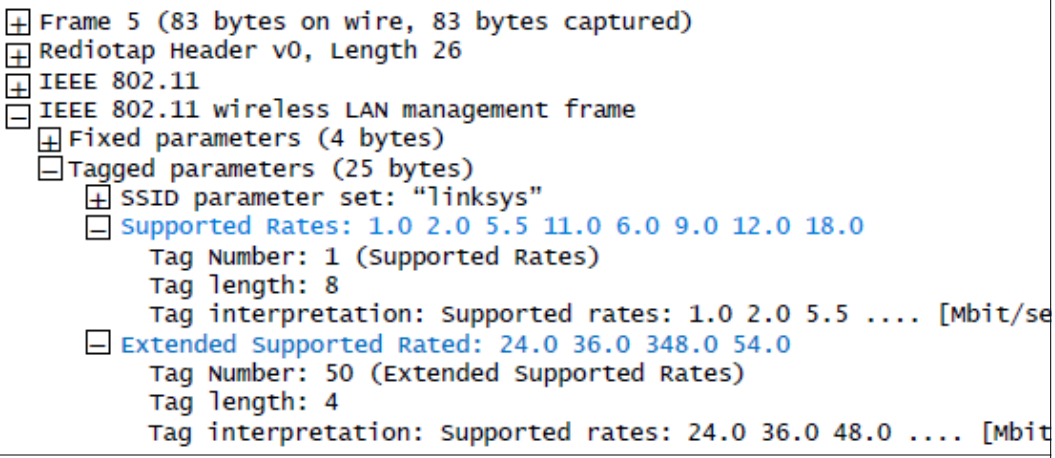
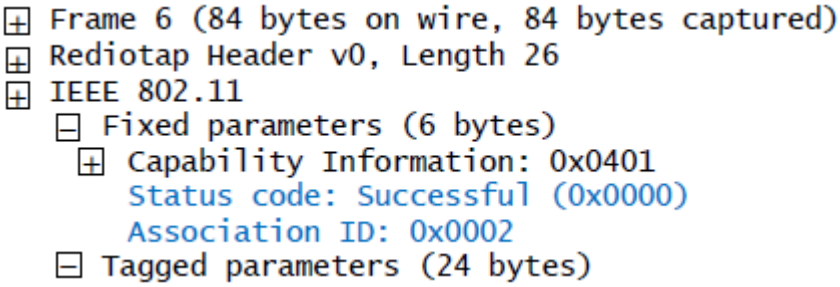
Management Frame은 탐색, 인증, 결합등 다양한 링크 계층에서의 관리 절차에 사용

- BSS안쪽에서의 동작들을 관리하기 위한 management

| Type | | Subtype | Description |
|---|---|---|---|
| 00 | Management | 0000 | Association request |
| | Management | 0001 | Association Response |
| | Management | 0010 | Reassociation request |
| | Management | 0011 | Reassociation response |
| | Management | 0100 | Probe request |
| | Management | 0101 | Probe response |
| | Management | 1000 | Beacon |
| | Management | 1010 | Disassociation |
| | Management | 1011 | Authentication |
| | Management | 1100 | Deauthentication |

## 패킷 분석

<table>
<tr><td>Probe</td><td>Request = 접속 요청 패킷 , Response = 접속 응답 패킷<br>  <br></td></tr>
<tr><td>Beacon</td><td>AP가 자기자신을 광고하기 위한 패킷</td></tr>
<tr><td>Authentication</td><td>Request, Response 둘다 Authentication Algorithm, Authentication SEQ, Status Code 등이 들어있음.<br>Request<br>  <br><br>Response<br>  <br></td></tr>
<tr><td>Disassociation</td><td>연결 해지( RST와 같은 역할 )</td></tr>
<tr><td>Deauthentication</td><td>AP에서 접속을 끊는 역할, 인증 해지( 연결을 끊게 됨 )</td></tr>
</table>

| | |
|---|---|
| | Reason Code 하나로 간단히 구성.<br>  |
| Association Request | Station이 지원가능한 속도 등이 수납됨<br>  |
| Association Response | Status Code와 Power saving을 위한 Association ID( AID )등이 수납됨<br>AID는 AP가 Station 을 관리해주는 번호<br>-bit_map으로 관리하고 사용하면 1 않하면 0 으로 관리.<br>-순차적, 배열순으로 해당 station에게 계속 부여.<br>  |

※ 모든 무선 패킷( wireless frame )은 암호화 되지 않고 평문으로 전송.

언제든지 내가 전달하면 Station과 AP가 받아들일수 있게 Stateless (상태정보 누락) -> 공격자 공격하고싶은 시점에 언제든지 가능

인증 mechanism이 없어서 내가 AP인척, Station 인척 할 수 있음.

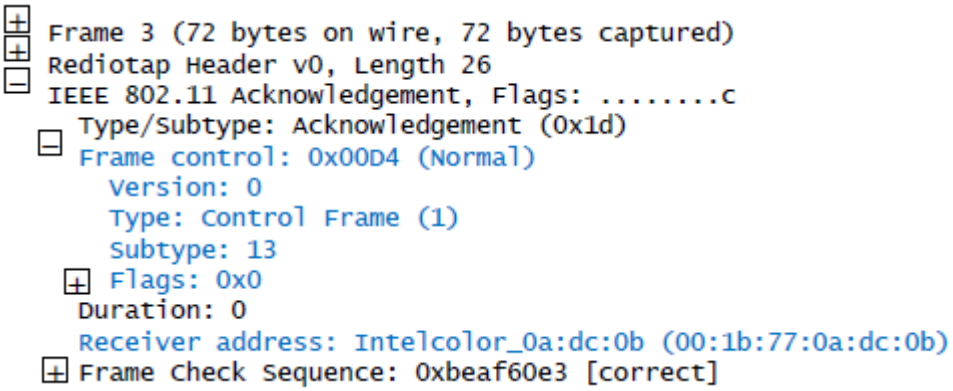
-> Spoofing 가능

2. 802.11 Control Frames ( CSMA / CA MAC의 동작을 지원함 )

| Type | | Subtype | Description |
|---|---|---|---|
| 01 | Control | 1010 | Power Save(PS)-Poll |
| | Control | 1011 | Request To Send (RTS) |
| | Control | 1100 | Clear To Send(CTS) |
| | Control | 1101 | Acknowledgement(ACK) |
| | Control | 1110 | Contention-Free(CF)-End |
| | Control | 1111 | CD-End + CF-Ack |

802.11 Control Frames ( CSMA / CA MAC의 동작을 지원함 )

패킷




3. 802.11 Data Frames

Data Frame은 총 8개의 서브타입으로 구성되어 있고 , 대부분이 사용되지 않으며 non-Qos 네트워크에서의 Data Frame Subtype은 두 가지이다.

| Type | | Subtype | Description |
|---|---|---|---|
| 10 | Data | 0 | 데이터 |
| | Data | 4 | Null Function(no data) |

Null function : 실제 데이터영역은 존재하지만 유효한 패킷이 안에 있지는 않음.

패킷

```
⊞ Frame 3 (72 bytes on wire, 72 bytes captured)
⊞ Rediotap Header v0, Length 26
⊟ IEEE 802.11
    Type/Subtype: Probe Request (0x04)
  ⊟ Frame control: 0x1148 (Normal)
      Version: 0
      Type: Data Frame (2)
      Subtype: 4
    ⊞ Flags: 0x11
    Duration: 314
    BSS Id: Cisco-Li_ab:86:95 (00:1a:70:ab:86:95)
    Source address: IntelCor_02:ee:6d (00:1b:77:02:ee:6d)
    Destination address: Cisco-Li_ab:86:95 (00:1a:70:ab:86:95)
```

# 6. Discovery

- AP의 정보를 찾아내는 것이 주목적

  ESSID, BSSID, Channel, Bit Rate, Encryption Algorithm 등

- Wireless는 자신이 접속할 수 있는 AP를 찾아야 함.

- Active Scanning

  Scan에 필요한 데이터를 Station이 AP에 직접 요청하는 방법 이용

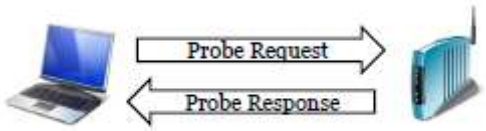
- Passive Scanning

  동일 주파수 대역을 사용하는 패킷을 모니터링 하는 방법을 이용해 Scan을 수행 (X) -> 동일 주파수 대역이 아니라도 Hopping 기법을 사용해서 가능. (우리나라 채널 13개:3~4개)

AP를 찾는 2가지 방법

a. BECON 방식 - AP에게 내가 여기 있다고 광고하는 방식

b. probe Request & Response(Active) - 직접 자기가 접속요청패킷을 보내고 접속응답패킷을 받아서 AP와 연결 하는 방식




# 7. Scanning

a. Active Scanning

Scan에 필요한 데이터를 Station이 AP에 직접 요청하는 방법 이용

-Station이 Probe Request 패킷을 전송하면 AP는 응답으로 Probe Response를 전달.

-Station 은 이 패킷을 받아 AP의 정보를 확인하고, 방식으로는 Directed와 Broadcast가 있음.

-Directed Probe Request

찾고자 하는 AP의 SSID를 미리 알고 있는 경우에 사용됨

Probe request 패킷의 BSSID 필드에 특정값을 입력 후 전송

-Broadcast Probe Request

가장 흔하게 사용되며 주변에 있는 모든 AP를 대상으로 한다.

Probe request 패킷의 BSSID필드에 NULL값을 입력 후 전송

b.Passive Scanning

-Station과 AP가 주고받는 패킷 중 인증 과정을 거치지 않고 ,동일 주파수 대역을 사용하는 패킷을 모니터링 하는 방법

-네트워크 트래픽을 Sniffing 하는 형태로 스캔을 수행한다.

-NIC에서 " monitor mode "를 지원해야 사용가능하다.

-Channel Hopping을 통해 모든 채널의 트래픽을 Sniffing 할 수 있음.

-Active Scanning 보다 더 좋은 결과가 나옴.

-Monitoring Mode는 기본적으로 활성화가 되어있지 않기 때문에 default로 passive scanning 을 제공하는 os는 없다.
-Monitoring Mode는 접속은 안 되고 패킷 지나가는것 만 본다.

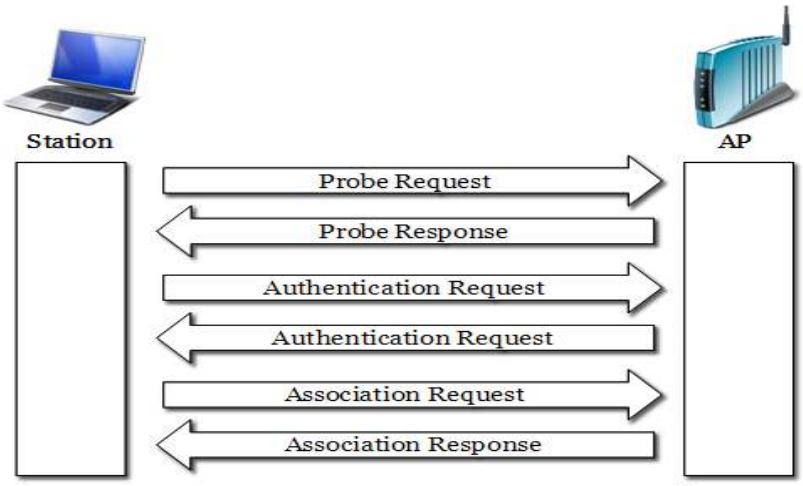
※BSSID, SSID, Encryption Algorithm, Channel, Frequency등이 일반 평문으로 전송되기 때문에 다 알 수 있음.

Beacon Frame 수집
AP가 주기적으로 발생시키는 패킷 (기본적으로 1초당 10회의 발생주기를 가짐)
-패킷에 대한 암호화를 수행하지않음
-SSID, Address, 지원속도 등의 정보 포함
-특성상 Passive Scanning에 가깝지만 Active Scanning에서도 Beacon Frame 수집을 통한 방법 사용
-보안상취약한데 현재까지 모든 장비는 beacon Frame을 발생하지 않게 한다는 설정은 불가.(발생주기를 늦게 할 수는 있음.)

## Scanning 대응책

| | |
|---|---|
| Active Scanning | Beacon Frame 과 Probe response 패킷을 이용하므로 두 패킷을 차단하는 방법으로 회피<br>Beacon Frame의 경우 통신에 필수적이므로 Beacon Frame의 정보중 BSSID필드를 NULL로 대체 |
| Passive Scanning | 확실한 대응책이 없으므로 위험성을 낮추는 방법을 주로사용<br>-무선 AP의 출력신호를 감소시켜 물리적으로 근접한 위치에만 접근가능하도록 설정(출력신호 감소는 보안 3요소인 기밀 , 무결 , 가용성중 기밀성을 보호하기위해 가용성을 해치는 행위.) |

# 8. 연결 과정




연결 방식

1. Open system
   1) 네트워크 상에서 인증이 이루어 지지 않고 그냥 접속이 이루어짐.
   2) Shared key보다 더 안전하다. -> WEP(5, 13글자(40, 104bit))Key를 사용하기 때문에 -> 대칭키를 사용.
   3) 대부분 이 방식을 사용하는데 WEP Crack에는 취약.
2. Shared key
   1) Key 값에 대한 challenge를 만들어서 전달하는데 그 challenge가 그대로 노출.

# 9. 공격 시연

가. 시나리오

-모든 통신은 연결 과정(key 동기화 과정 등)에서가 보안이 가장 취약

-AP의 WPA key를 알기 위해서 Attcker는 사용자의 연결을 임의적으로 끊어서 다시 연결하는 과정에서 오고 가는 Key를 Sniffing.

-Deauthenticating Users

1. Wireless Network의 SSID를 쉽게 확인할 수 있는 공격 방법
2. Legitimate User에게 Deauthentication 프레임을 전달하여 Network와 연결이끊어지게 한 후, Legitimate User의 reassociation Request를 탐지하여 SSID를 확인 함

3. AP의 보안설정과는 관계없이 Management Frame은 암호화 되지 않고 인증되어진다는 취약점을 이용

-Deauthenticate을 보내면 클라이언트는 다시 접속 하려고 노력. 그때 만약 계속 Deauthenticate 패킷을 보내면 DOS 공격을 시작

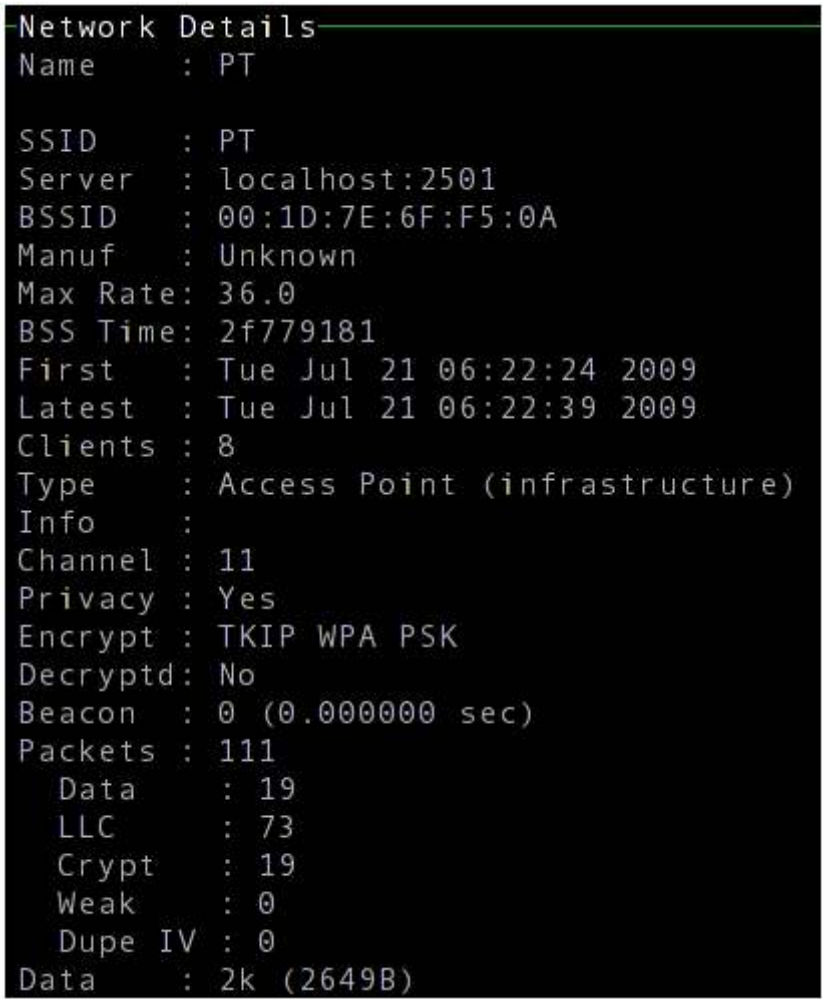
나. 시연

- 준비사항
    1. AP
    2. Backtrack
    3. Victim

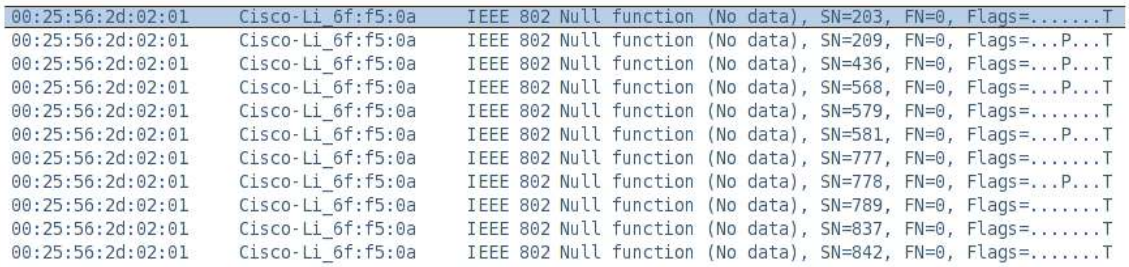
1. Victim은 PT라는 AP의 접속 후 통신 중.
    - Victim의 MAC 정보


2. Attacker은 먼저 kismet를 구동시켜서 공격을 원하는 AP를 선택

후 SSID, BSSID, Channel, Encrypt 정보 등을 획득.




3. Attacker은 목적지를 BSSID로 패킷 필터링을 해서 PT라는 AP와 통신하고 있는 사용자가 있는지 확인.
   -wlan.da==00:25:56:2d:02:01로 패킷 필터링을 설정
   -AP에 Ping을 보내고 있는 Victim의 MAC 확인




4. 패킷 Sniffing을 통해서 AP와 통신하고 있는 Victim의 MAC 주소를 얻어

냈으므로 Victim을 공격해 Victim의 연결을 임의적으로 끊는다.

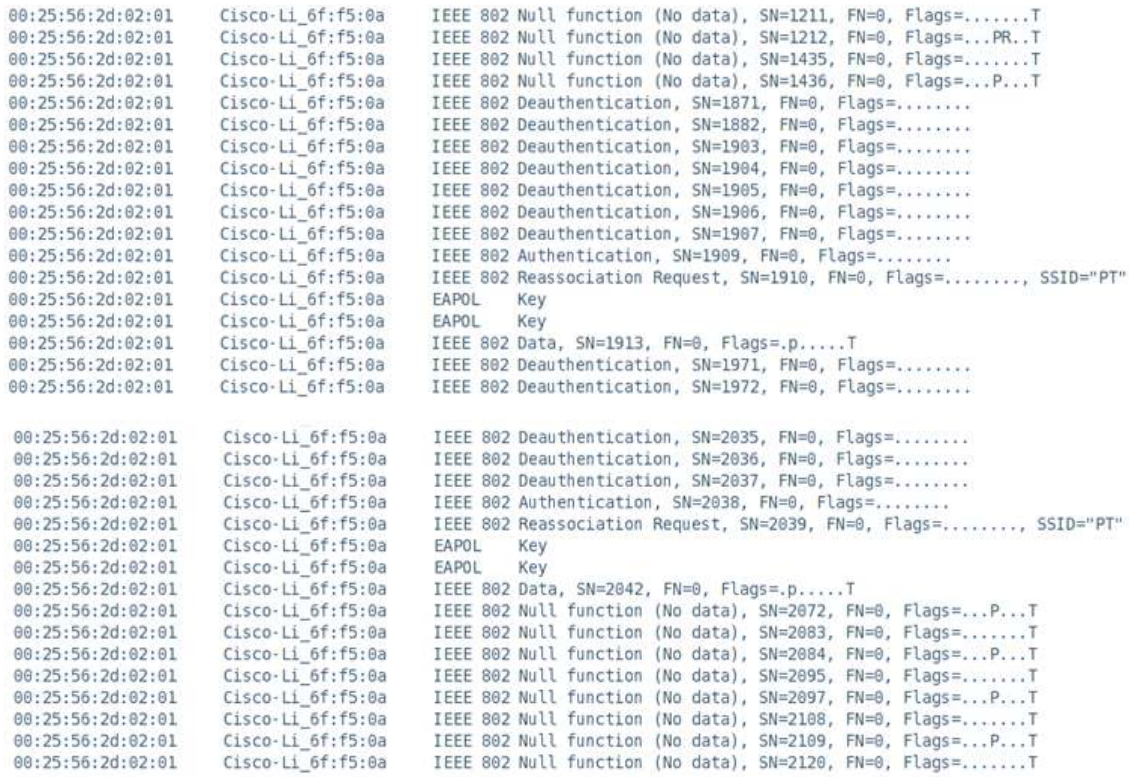
#aireplay-ng rausb -0 10 -a 00:1D:7E:6F:F5:0A -c 00:25:56:2d:02:01

->공격자가 자신의 맥 주소를 victim의 맥 주소로 변환해서 패킷 전송

-Victim의 연결이 잠시 끊기는 것을 확인.


5. Victim이 다시 재접속 하는 과정에서 Key가 오고 가는 것을 확인.

AP에 오던 Ping이 끊어지고 다시 재접속 하는 과정에서 인증과 Key를 주고받는 것을 확인.




- AP가 보내던 응답이 끊어지고 다시 재접속 하는 과정에서 인증과 Key를 주고받는 것을 확인.

```
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=893, FN=0, Flags=....R..., BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=894, FN=0, Flags=........, BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=894, FN=0, Flags=....R..., BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=894, FN=0, Flags=....R..., BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=894, FN=0, Flags=....R..., BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=894, FN=0, Flags=....R..., BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=897, FN=0, Flags=........
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=897, FN=0, Flags=....R...
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=897, FN=0, Flags=....R...
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=897, FN=0, Flags=....R...
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=897, FN=0, Flags=....R...
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=897, FN=0, Flags=....R...
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=903, FN=0, Flags=........, BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=904, FN=0, Flags=........
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=904, FN=0, Flags=....R...
```

```
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=1134, FN=0, Flags=....R...
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Deauthentication, SN=1134, FN=0, Flags=....R...
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Authentication, SN=1151, FN=0, Flags=........
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Reassociation Response, SN=1153, FN=0, Flags=........
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     EAPOL    Key
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     EAPOL    Key
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Data, SN=1156, FN=0, Flags=.p....F.
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=1164, FN=0, Flags=........, BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=1165, FN=0, Flags=........, BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=1166, FN=0, Flags=........, BI=100, SSID="PT"[Malformed Packet]
Cisco-Li_6f:f5:0a     00:25:56:2d:02:01     IEEE 802 Probe Response, SN=1166, FN=0, Flags=....R..., BI=100, SSID="PT"[Malformed Packet]
```

# 10. 취약점 분석 및 대응책

Legitimate User에게 Deauthentication 프레임을 전달하여 Network와 연결이 끊어지게 한 후, Legitimate User의 reassociation Request를 탐지하여 SSID를 확인, 이때 AP의 보안설정과는 관계없이 Management Frame은 암호화 되지 않고 인증되어지지 않는다는 취약점이 노출.

대응책

-Deauthentication packet를 차단하거나 거부할 수 있는 설정은 없기 때문에 기본적인 설정으로는 막을 수 없음. 그러나 일부 제품에서는 패치 된 드라이버를 설치하여 deauthentication packet이나 disassociation packet을 무시 하도록 설정. (Wireless IDS는 공격을 탐지할 수는 있지만 공격을 멈추거나 차단할 수는 없고 다만  관리자에게 탐지여부를 알려줌)

# 11. 결론

현재 무선 랜은 취약점인 키 값의 단순 평문 전송, 키 스트림의 단순성으로 인해 해킹 당하기 쉽다. 현재 WPA라는 기술이 사용 되고 있지만 패스워드의 길이가 짧다면 공격자에의해 키 교환 프레임을 MITM 공격을 통하여 패스워드가 노출 될 수 있다.

현재로써는 사용자가 패스워드의 길이를 길게하고 맥 주소를 확인해서 각자가 예방하는것이 최선으로 생각 됨.