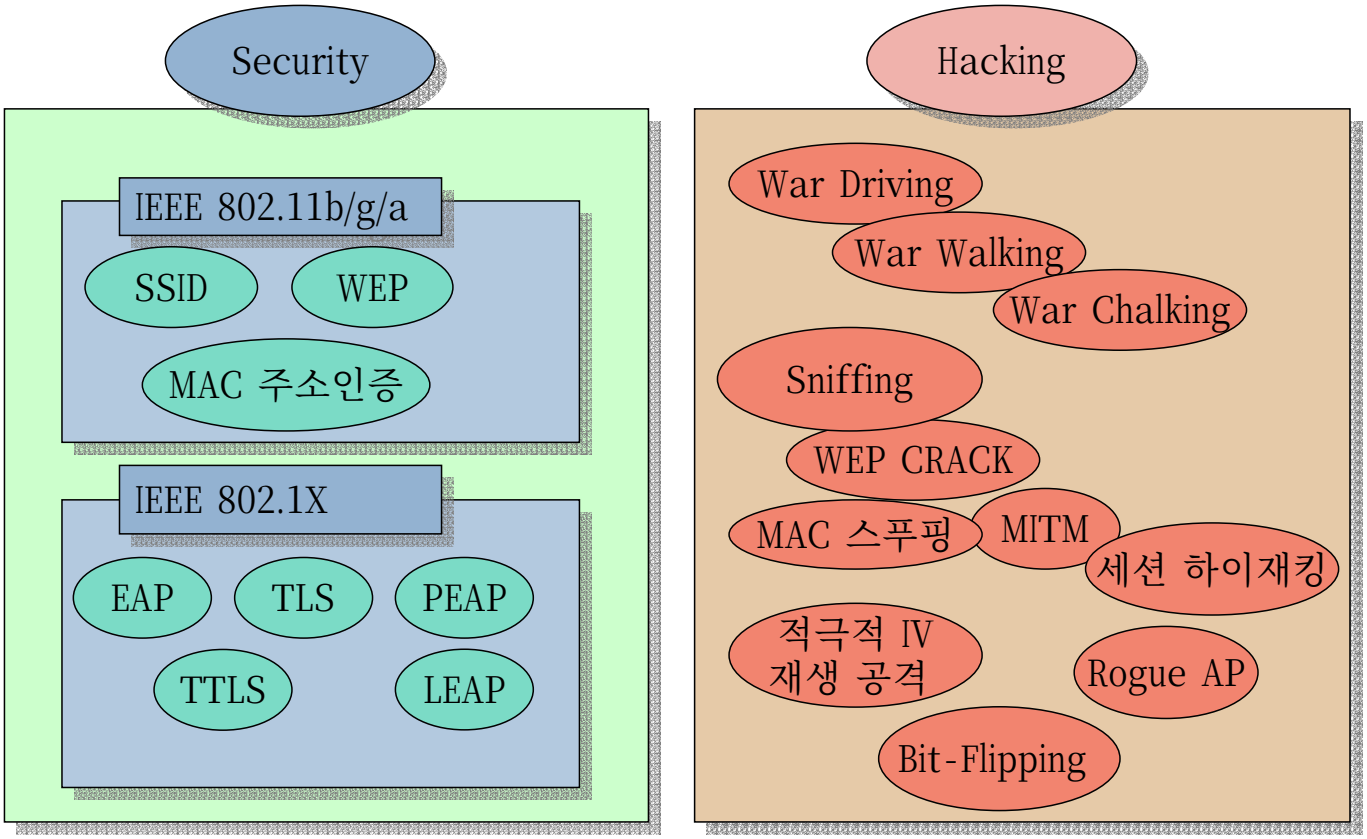
WLAN Security & Hacking
And
Next Generation Wireless

2005. 1. 18

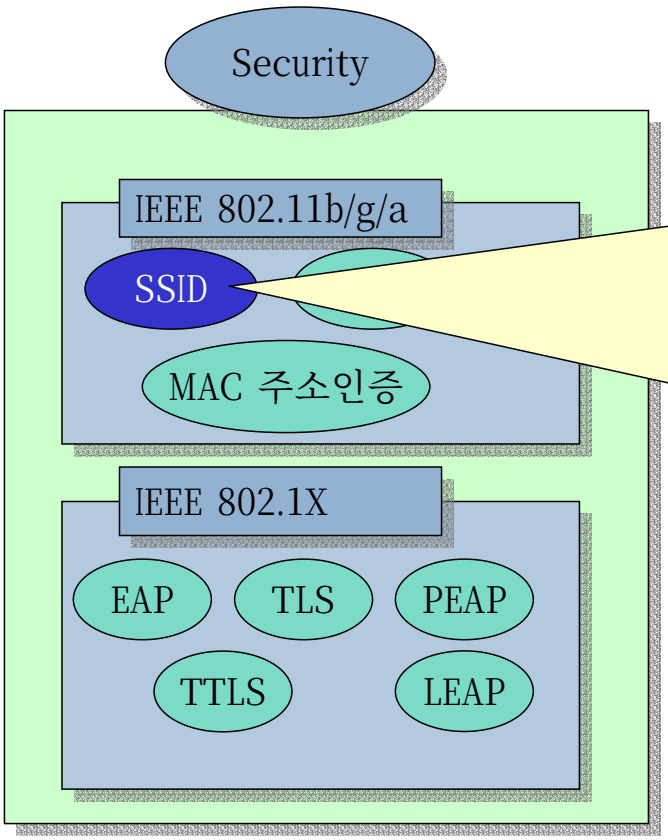
김 경 곤 (A.K.A. Anesra)

목 차

1. 무선 LAN 보안/해킹 레이아웃



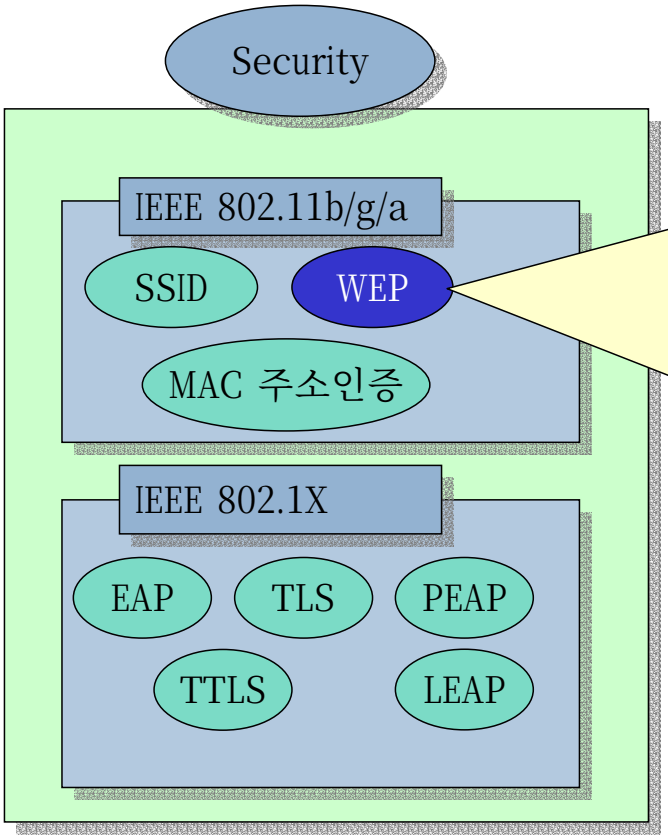
2. 무선 LAN 보안 기술들



SSID
-Service Set Identifier
-WLAN을 논리적으로 구분할 수 있는 구조 제공
-AP의 SSID값과 단말기의 SSID값이 일치해야지 통신 가능
-데이터 암호화 하지 않음

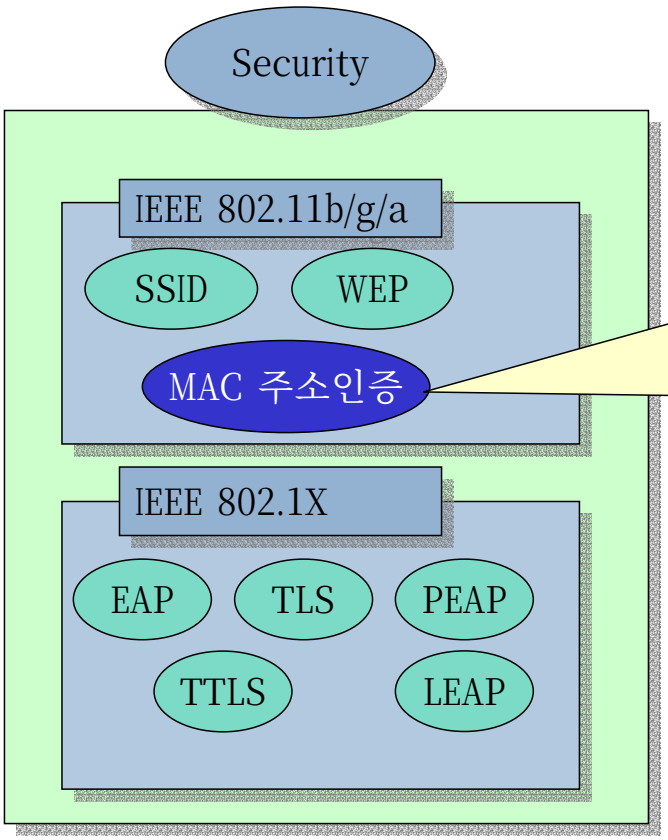
Sniffing을 통해 SSID값을 쉽게 추출할 수 있음.

2. 무선 LAN 보안 기술들



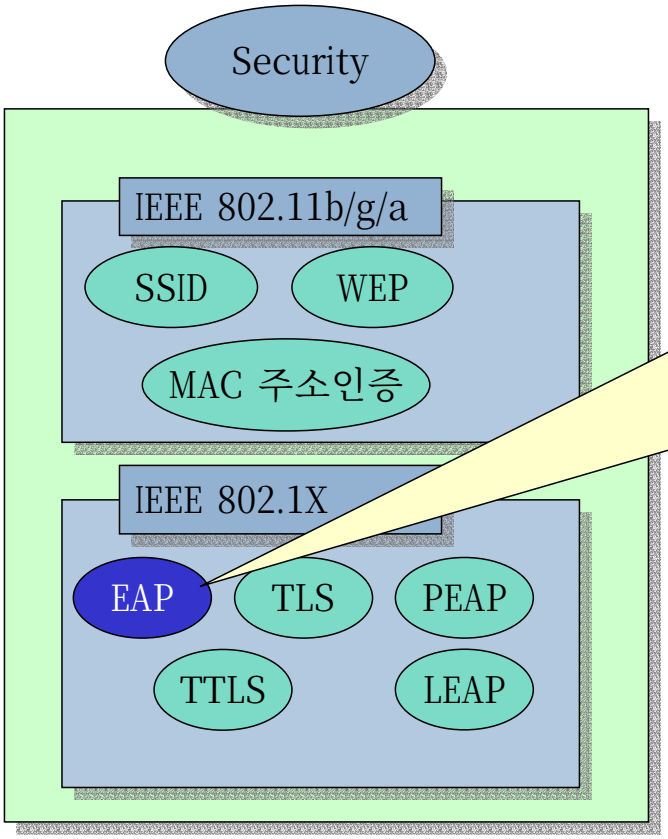
WEP
-Wired Equivalent Privacy
-AP가 단말을 인증하기 위해 사용
-AP에 WEP키를 등록한 후 단말에도 WEP키 등록
-인증원리:
1. 단말이 AP에 공유키 요청
2. AP가 WEP키로 평문을 단말에 전송
3. 단말은 평문을 자신의 WEP키로 암호화해서 전송
4. AP가 복호화 가능하면 통신

2. 무선 LAN 보안 기술들



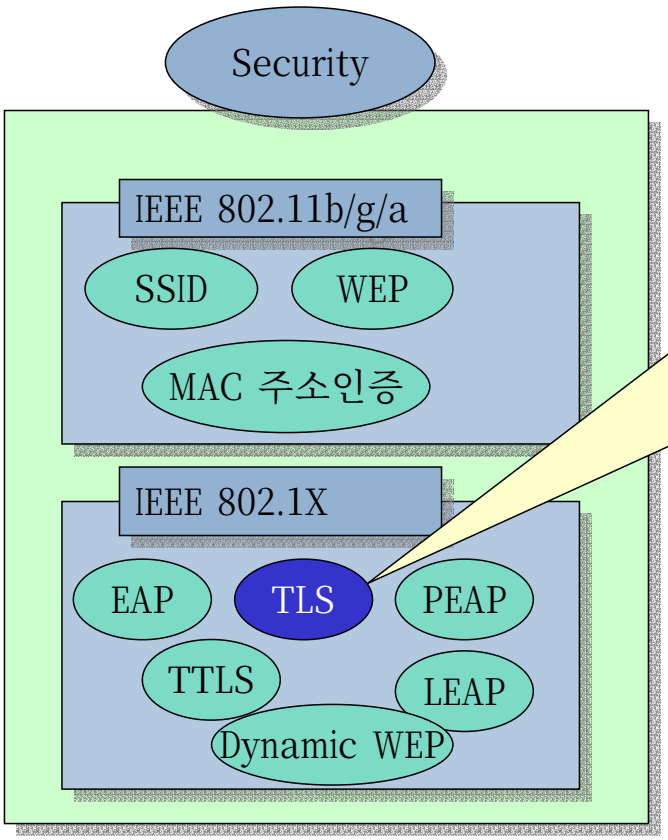
MAC 주소 인증
-AP 또는 Radius(인증 서버)에 단말의 MAC주소를 등록 후 접속 단말의 MAC주소를 확인하여 접속 인가

2. 무선 LAN 보안 기술들



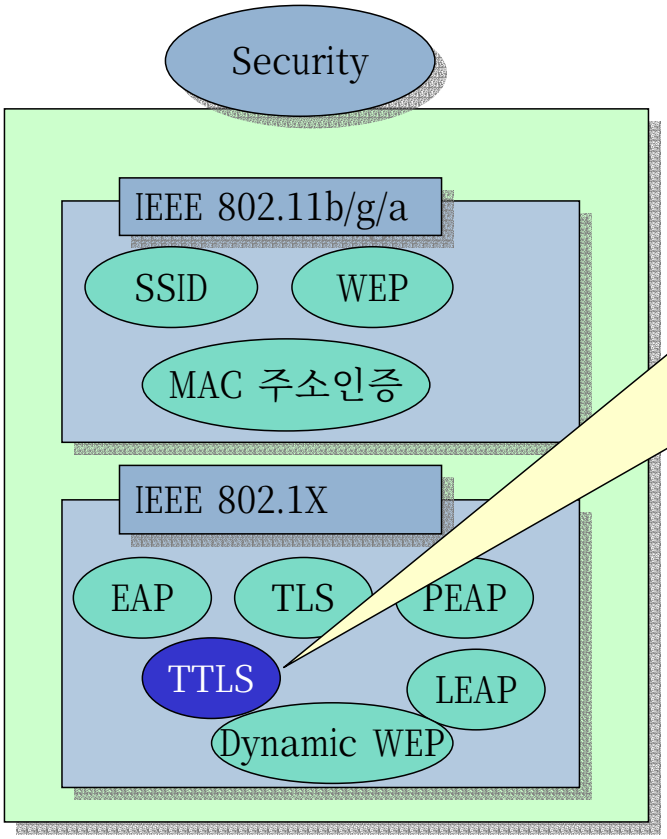
EAP
-Extensible Authentication Protocol
-인증을 통해 네트워크를 보호하는 포트 Access 프로토콜
-EAP유형:MD5, PEAP, LEAP, TLS, TTLS

2. 무선 LAN 보안 기술들



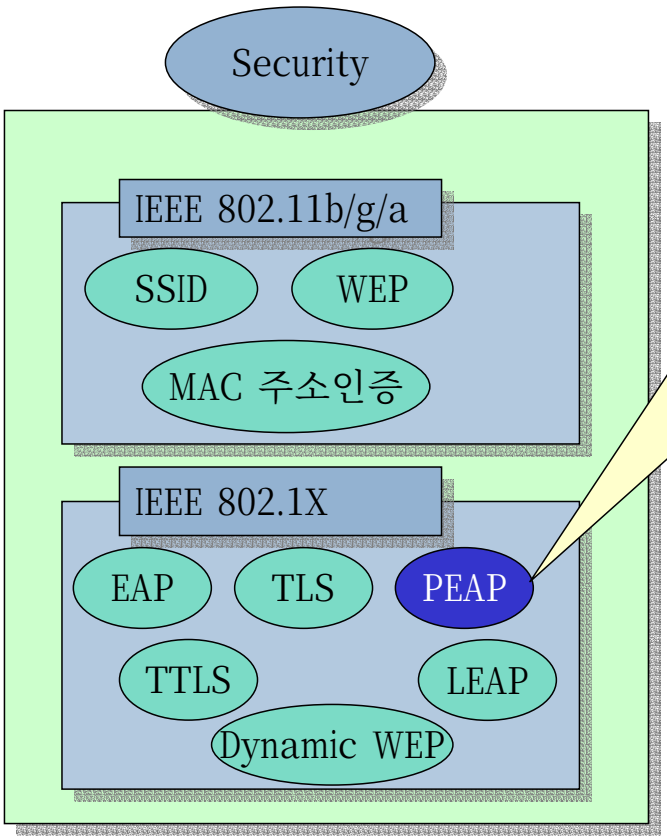
EAP-TLS
-Transport Layer Security
-단말기와 서버 양쪽 다 인증함
-사용자 WEP키 및 세션 기반 WEP키를 동적으로 생성
-단점:단말기와 서버 모두 인증서를 관리해야 함

2. 무선 LAN 보안 기술들



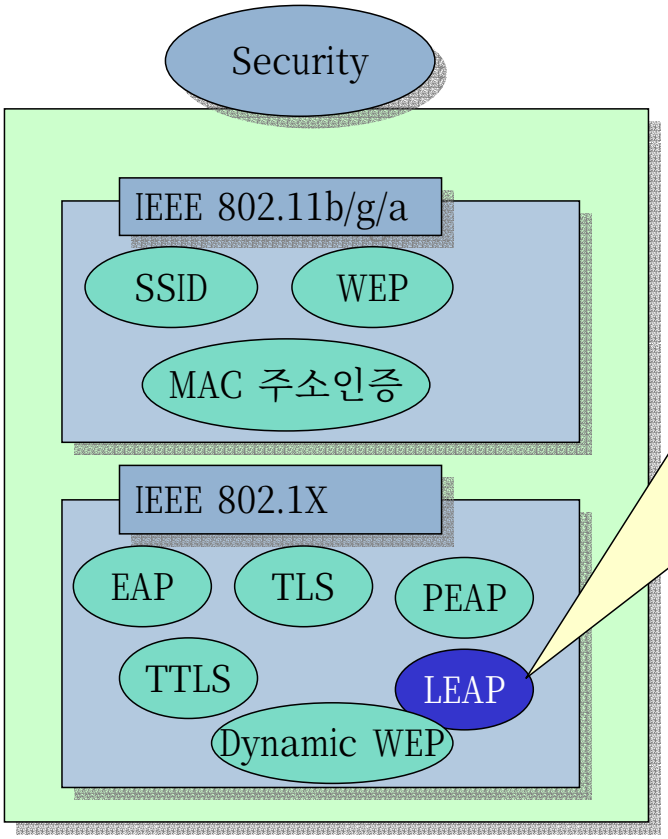
EAP-TTLS
-(Tunneled TLS)
-Funk Software와 Certicom이 TLS를 보강하여 개발한 방법
-암호화된 터널을 사용
-TLS와 달리 서버 측 인증서만 사용

2. 무선 LAN 보안 기술들



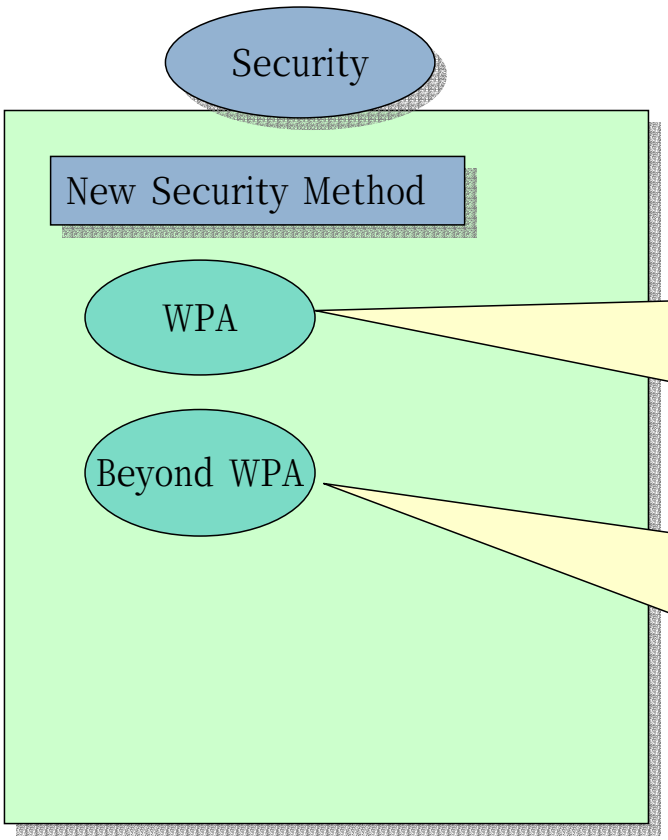
PEAP
-Protected Extensible Authentication Protocol
-단말기와 서버간 터널을 구성
-서버측 인증서만 사용
-MS, Cisco, RSA Security에서 개발한 방법

2. 무선 LAN 보안 기술들



LEAP
-Lightweight EAP
-주로 Cisco Aironet WLAN에서 사용하는 EAP인증 유형
-Dynamic WEP키 사용하여 전송 데이터 암호화 하여 상호인증
-Cisco에서 독점 행사하였으나, 지금은 다른 어댑터에서도 사용 가능

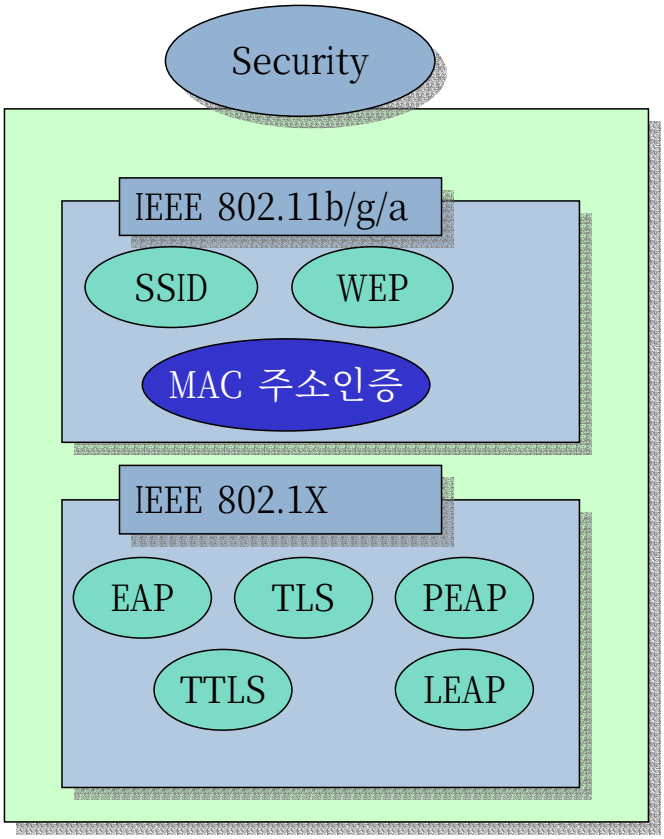
2. 무선 LAN 보안 기술들



WPA
-(Wi-Fi Protected Access)
-IEEE 표준 기반 새로운 보안 솔루션
-802.1x인증 및 TKIP암호화 기법을 포함

Beyond WPA
-TGi(IEEE Task Force i)는 무선 LAN 보안을 심층적으로 다룸
-2004년 내 차세대 AP 제품에 AES암호화와 802.1x인증 방법 선보임

2. 무선 LAN 보안 기술들



TKIP
-Temporal Key Integrity Protocol

2. 무선 LAN 보안 기술들

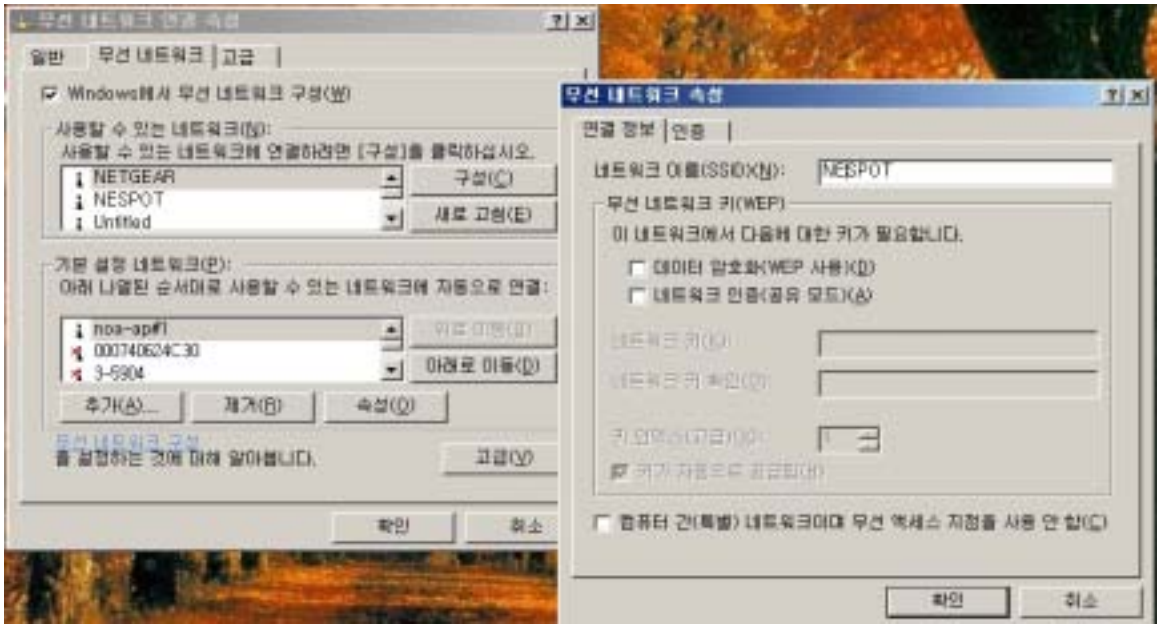
802.1x EAP 유형, 기능 / 이점	MD5 --- Message Digest 5	TLS --- Transport Level Security	TTLS --- Tunneled Transport Level Security	PEAP --- Protected Transport Level Security	LEAP --- Lightweight Extensible Authentication Protocol
클라이언트측 인증서 필요	아니오	예	아니오	아니오	아니오
서버측 인증서 필요	아니오	예	예	예	예
WEP 키 관리	아니오	예	예	예	예
Rouge AP 감지	아니오	아니오	아니오	아니오	예
제공업체	MS	MS	Funk	MS	Cisco
인증 속성	일방	쌍방	쌍방	쌍방	쌍방
구축 난이도	용이	난해	중간	중간	중간
무선 보안	불량	최고	고급	고급	고급

출처: http://support.intel.com/support/kr/wireless/wlan/sb/cs-008413.htm

3. 무선 LAN 설정

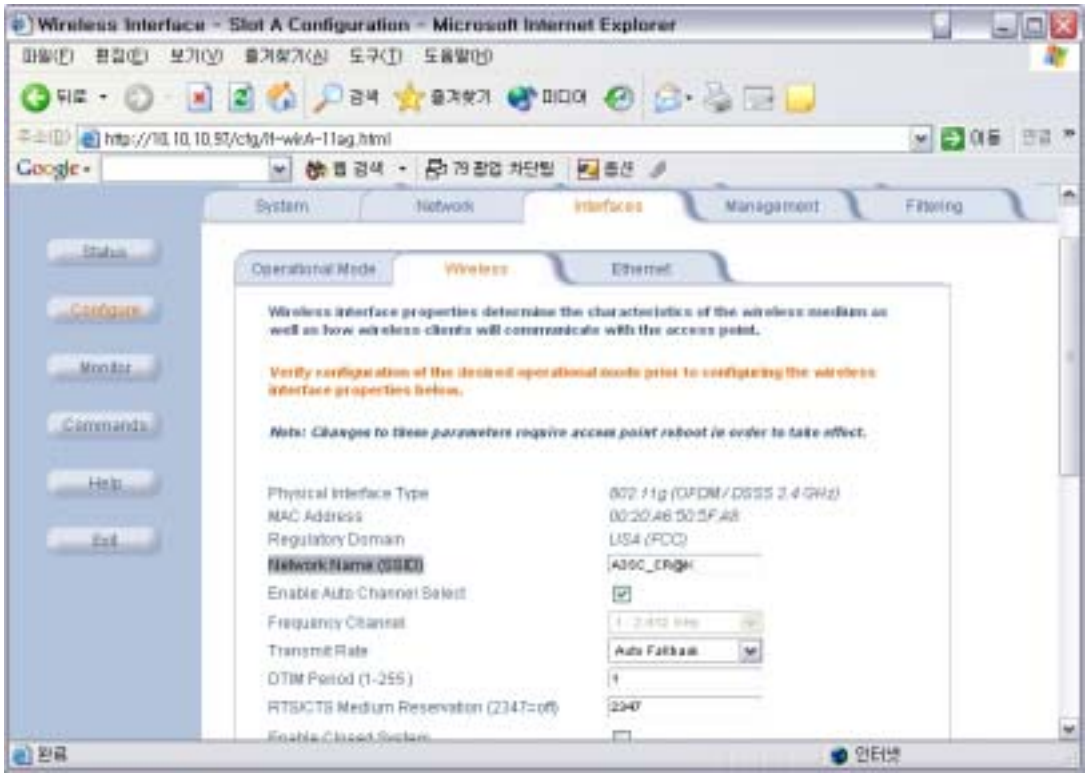
1. SSID 설정 - 클라이언트

• Winxp 에서는 네트워크 연결 속성->무선 네트워크->구성을 선택 후 SSID를 입력할 수 있다.



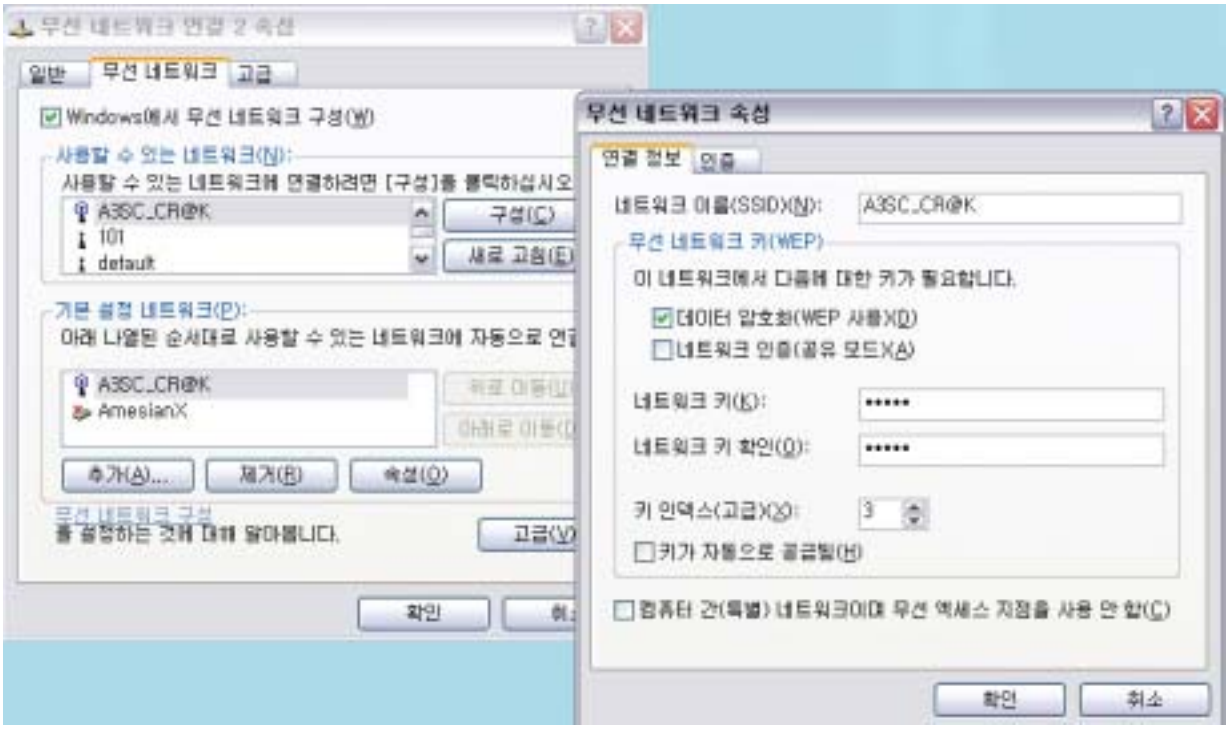
3. 무선 LAN 설정

1. SSID 설정 – AP(Orinoco proxim)



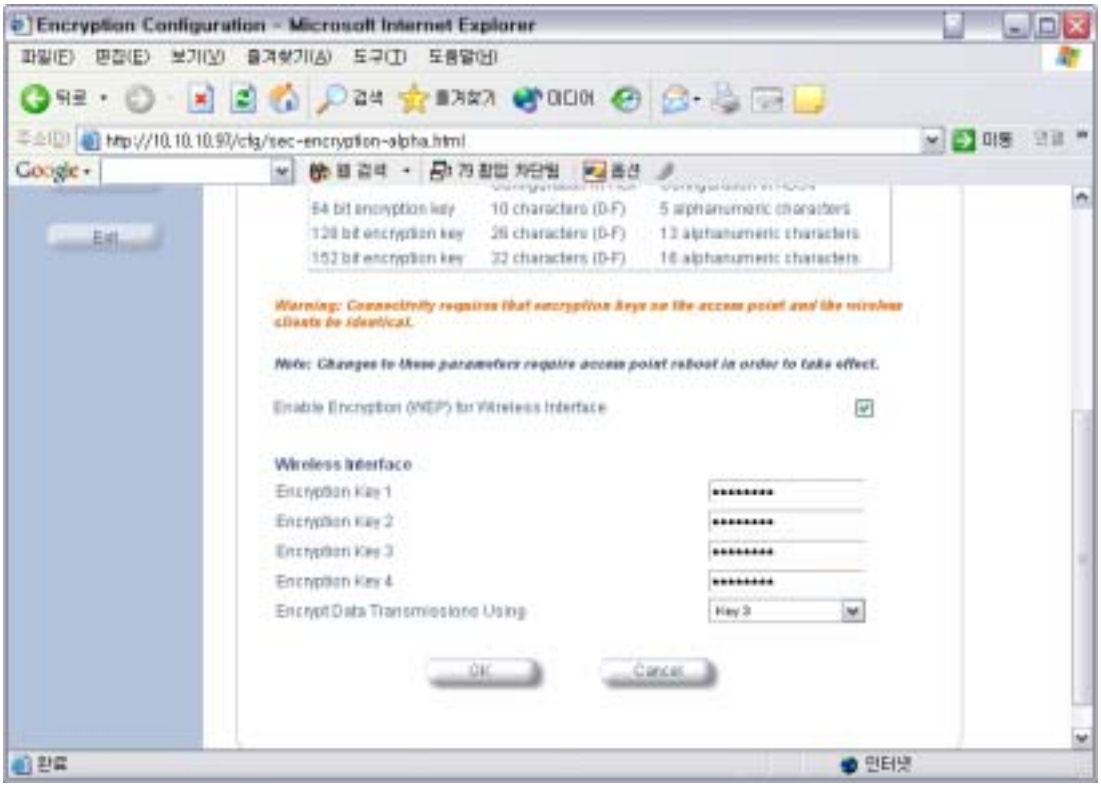
3. 무선 LAN 설정

2. WEP키 설정 – 클라이언트



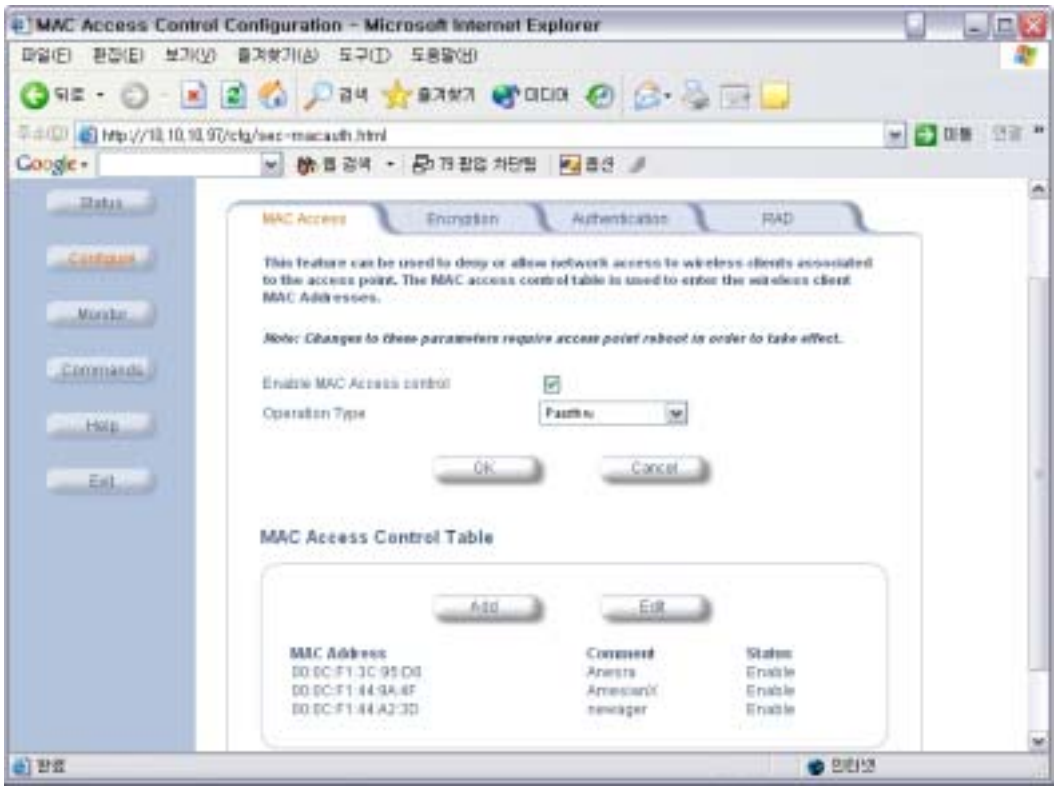
3. 무선 LAN 설정

2. WEP키 설정 – AP



3. 무선 LAN 설정

3. MAC 인증 설정 (AP)



3. 무선 LAN 설정

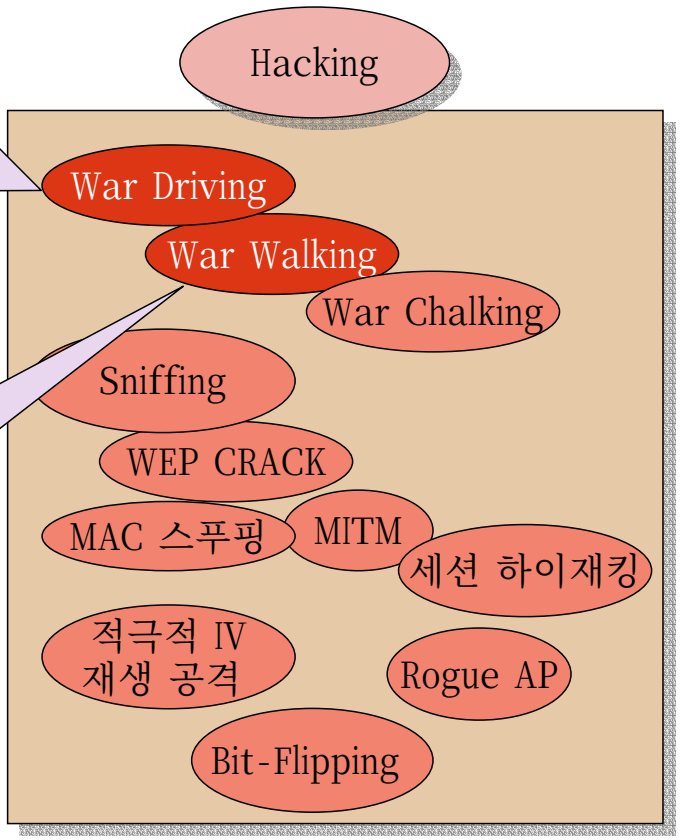
SSID & WEP키 설정 Demo (or 동영상)

Wireless LAN
Hacking Methods

4. 무선 LAN 해킹 기술들

War Driving
-공격자들이 이동수단을 타고 주위 인증을 거치지 않는 AP를 찾아 다니는 행위
-도구: 야기안테나, Boingo, Netstumbler, 차량

War Walking
-공격자들이 걸어 다니면서 인증을 거치지 않는 AP를 찾아 다니는 행위



4. 무선 LAN 해킹 기술들

War Chalking
-공격자들이 WLAN을 탐지한 지역에 그 WLAN에 대한 인증상태를 벽이나 바닥에 표시하는 행위

4. 무선 LAN 해킹 기술들

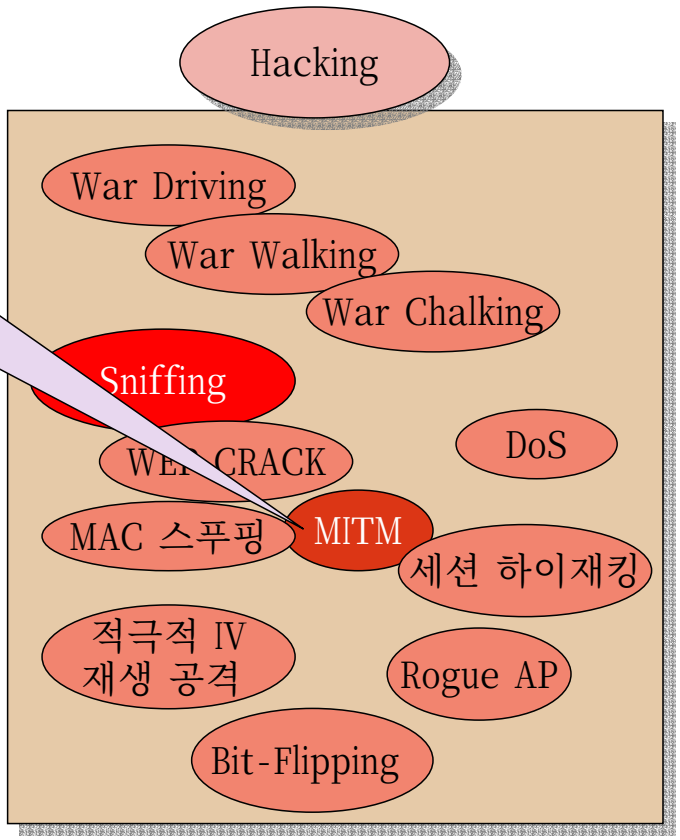
Sniffing을 통해 수집한 프레임을 모아서 WEP키 Crack이 가능함. – 단, 엄청나게 많은 프레임을 모아야지만 WEP키 Crack 가능
-WEP키 Crack : Aironet
-Sniffing : Airopeek(Win), Sniffer Pro (win2k용), Kismet(Linux)

4. 무선 LAN 해킹 기술들

Sniffing을 통해 정상적 사용자의 MAC주소를 추출 한 후 자신의 MAC주소를 정상적 사용자의 MAC주소로 변경 후 접속.
-MAC주소 변경 도구:
윈도우용 : SMAC
리눅스용 : macchanger

4. 무선 LAN 해킹 기술들

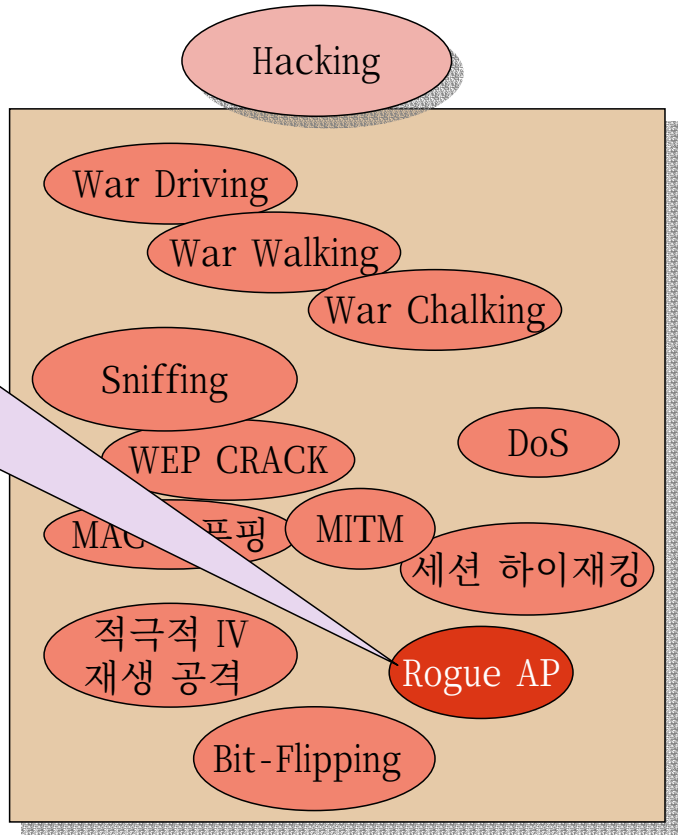
MITM
- 중간에 세션을 훔쳐서 정상적인 사용자로 위장하여 접속하는 공격 방식



4. 무선 LAN 해킹 기술들

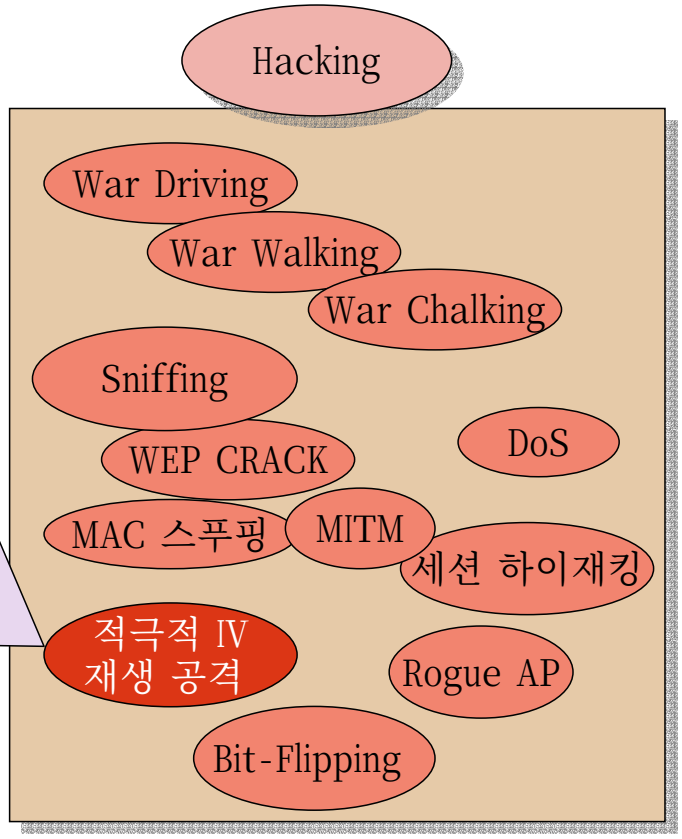
Rogue AP
-공격자가 AP를 가져와서 정상적인 AP보다 강한 신호를 쏘아서 일반사용자가 정상적인 AP가 아닌 공격자가 설치한 AP로 접근하여 사용자의 정보를 추출하는 공격 방식

Hsd에서 사용한 연장들
-Linux Kernel 2.4.22
-pcmcia-cs 3.2.5
-Net DNS 0.42
-Airsnarf 0.2
-Hostap-driver 0.1.0
-Hostap-utils 0.1.0

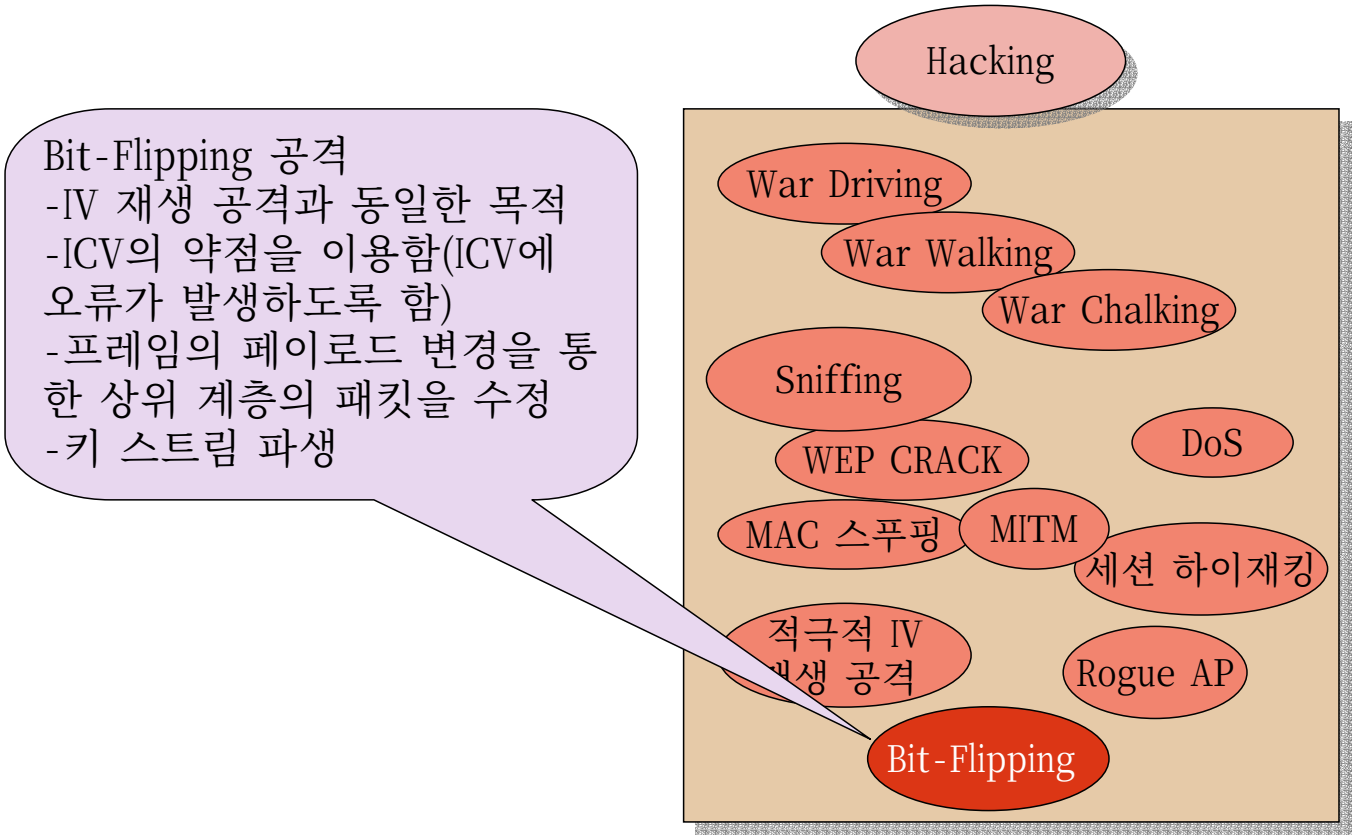


4. 무선 LAN 해킹 기술들

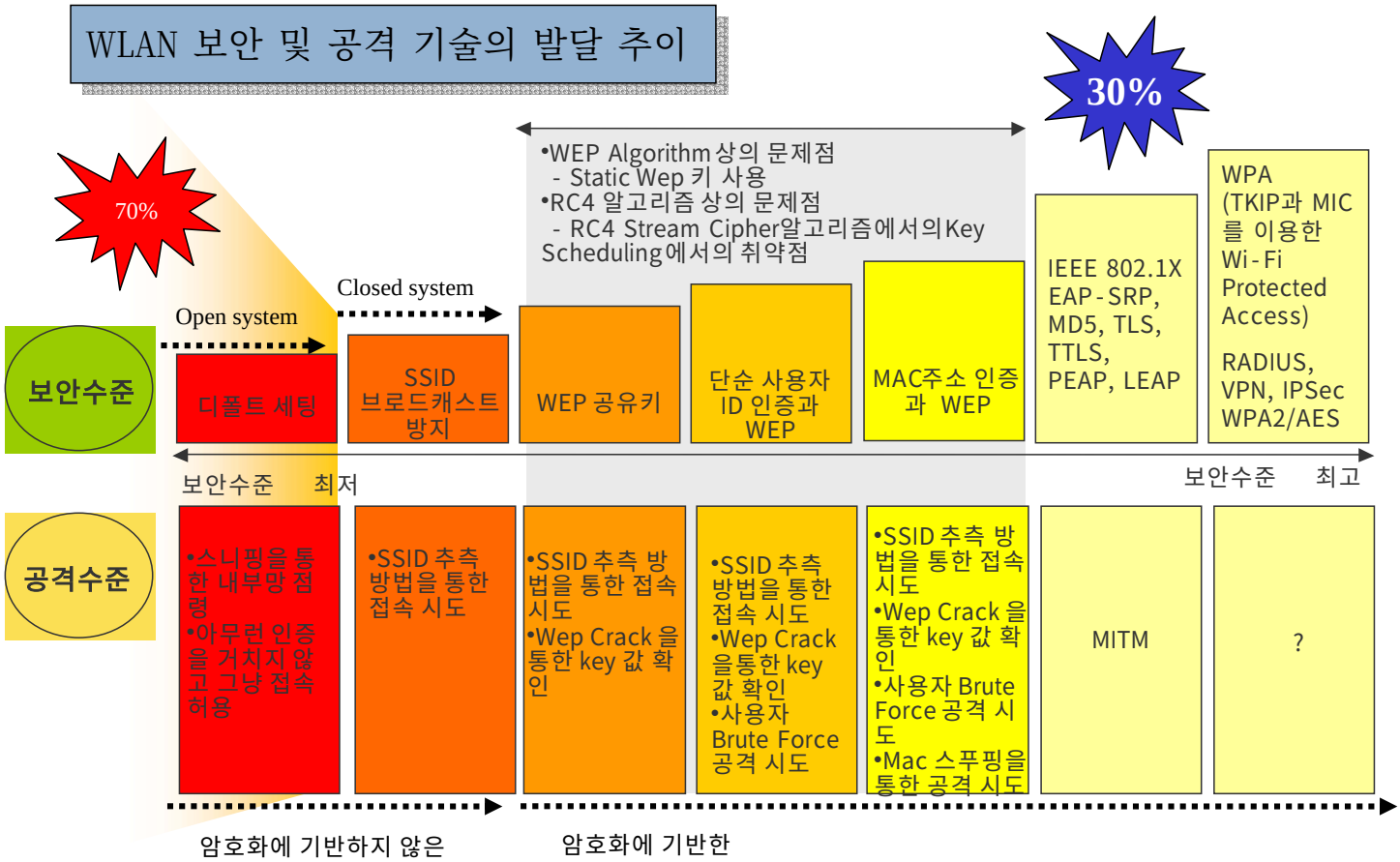
적극적 IV 재생 공격
-메시지 무결성 검사를 위해 제공되는 ICV (Integrity Check Value)는 CRC32 체크 기능을 이용
-CRC32 값은 MITM공격에 취약(IV 재생공격, Bit-Flipping)
-IV와 기본 WEP키를 반복적 사용 및 재생함으로써 네트워크를 파괴하기에 충분한 큰 키 스트림을 생성할 수 있다는 원리를 이용한 공격



4. 무선 LAN 해킹 기술들



Wireless LAN Hacking

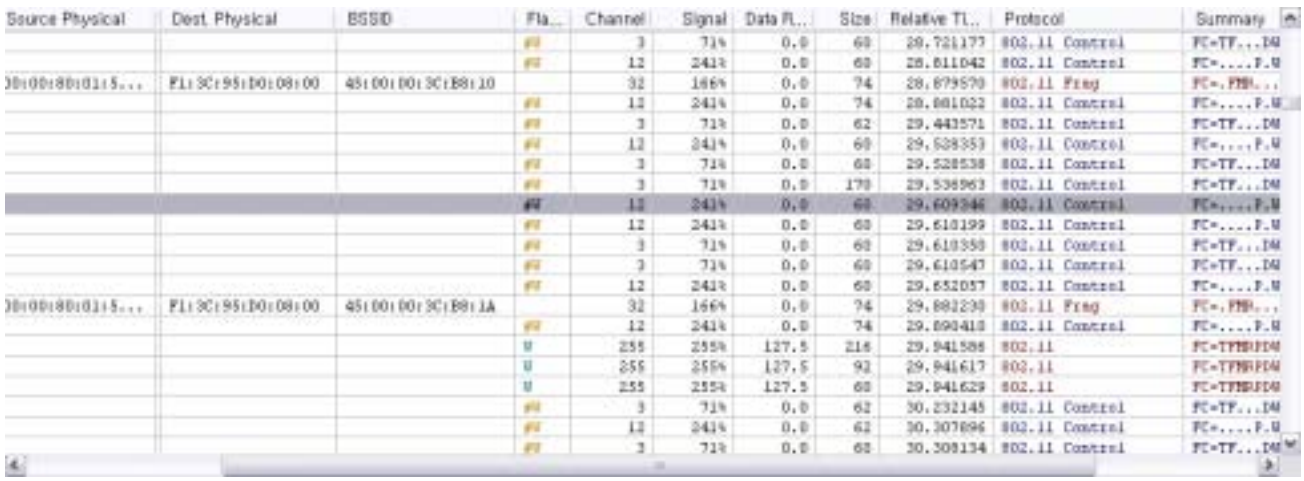


Wireless LAN
Hacking Demonstration

5. 무선 LAN 해킹 기술 상세

0. 무선 LAN 스니핑

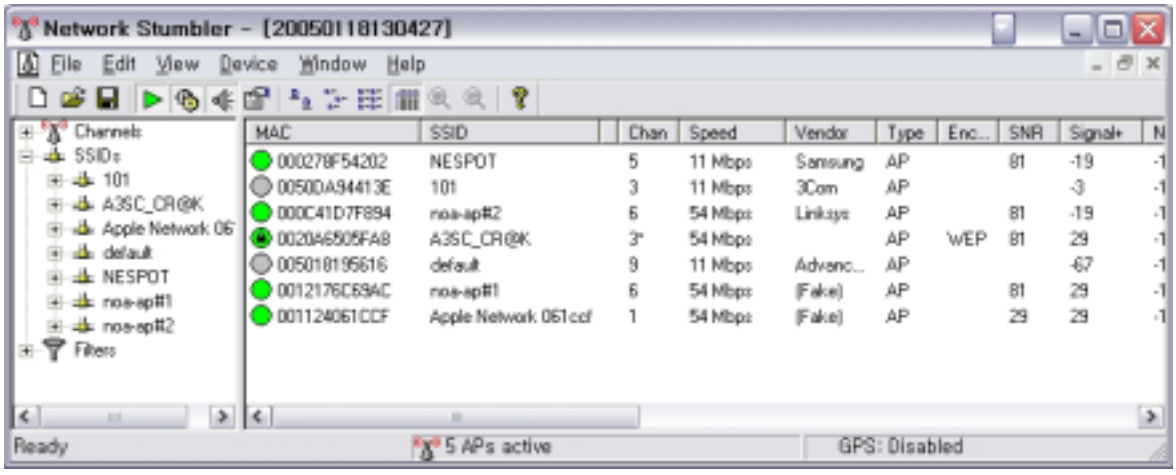
대표적인 도구로써는 AiroPeek 이 있음
AiroPeek은 분석을 조금 이상하게 함.



5. 무선 LAN 해킹 기술 상세

1. War Driving & War Walking

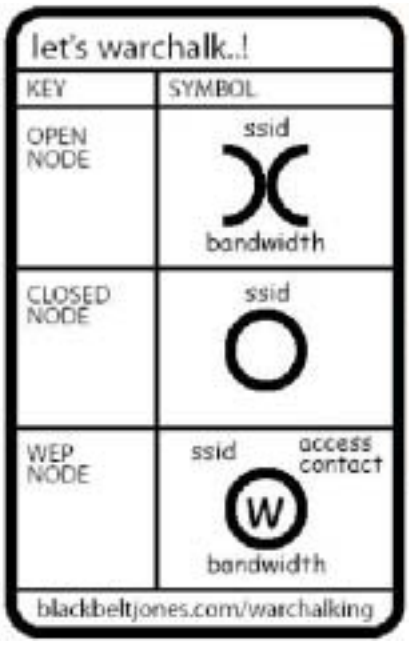
이동하면서 무선 AP를 탐지하는 행위.
특히 Default Setting 된 AP는
Open System이므로 SSID만 알 경우 접근이 가능함
AP탐지 도구 : Netstumbler, Boingo를 많이 사용



5. 무선 LAN 해킹 기술 상세

2. War Chalking

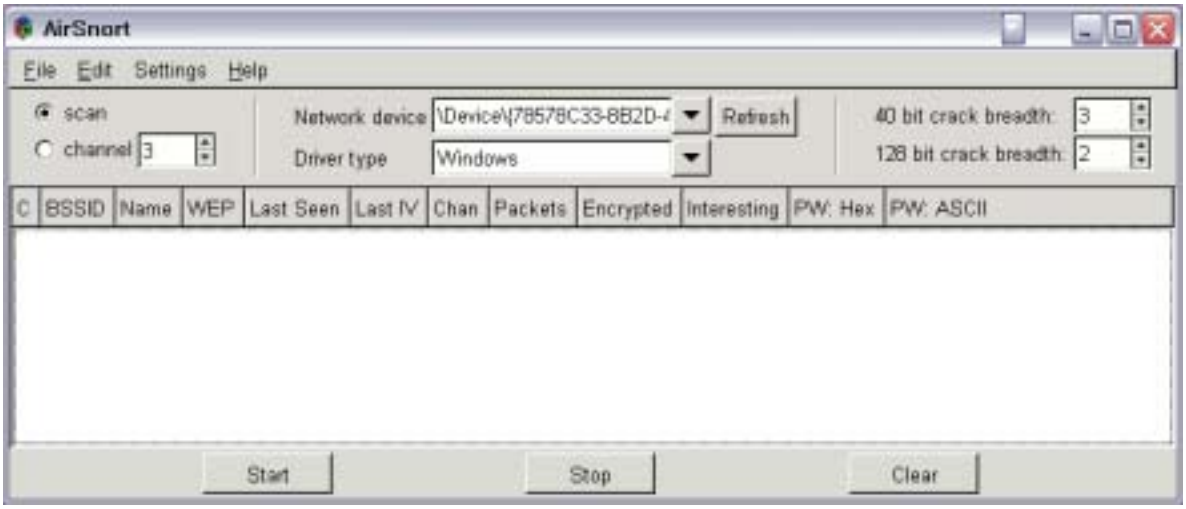
무선 LAN을 탐지한 곳에 AP에 대한 정보를 낙서하는 방법
다른 사람이 사용하거나 Exploit 하기 위해 흔적을 남겨둠



5. 무선 LAN 해킹 기술 상세

3. WEP Crack

WEP키를 수집한 다음에 수집한 프레임을 가지고 WEP키를 복호화 함
도구 : Airsnort

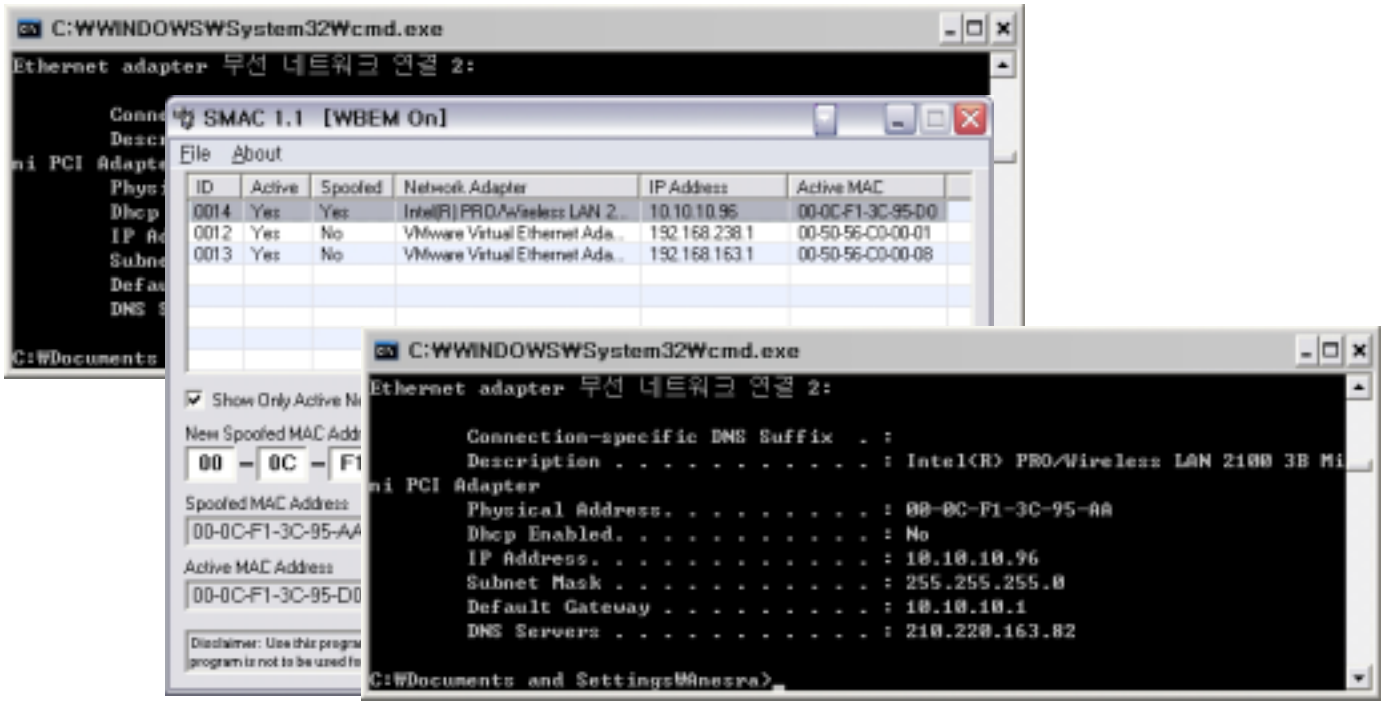


How To Use this?, I can't capture wireless packet as airsnort.

5. 무선 LAN 해킹 기술 상세

4. MAC Changer

MAC 주소를 변경 시켜서 MAC 인증 우회하는 방법



5. 무선 LAN 해킹 기술 상세

5. MITM

More Research & Test & Discussion

5. 무선 LAN 해킹 기술 상세

6. Rogue AP

More Research & Test & Discussion

5. 무선 LAN 해킹 기술 상세

7. DoS

More Research & Test & Discussion

5. 무선 LAN 해킹 기술 상세

8. IV 재생 공격

More Research & Test & Discussion

9. Bit-Flipping 공격

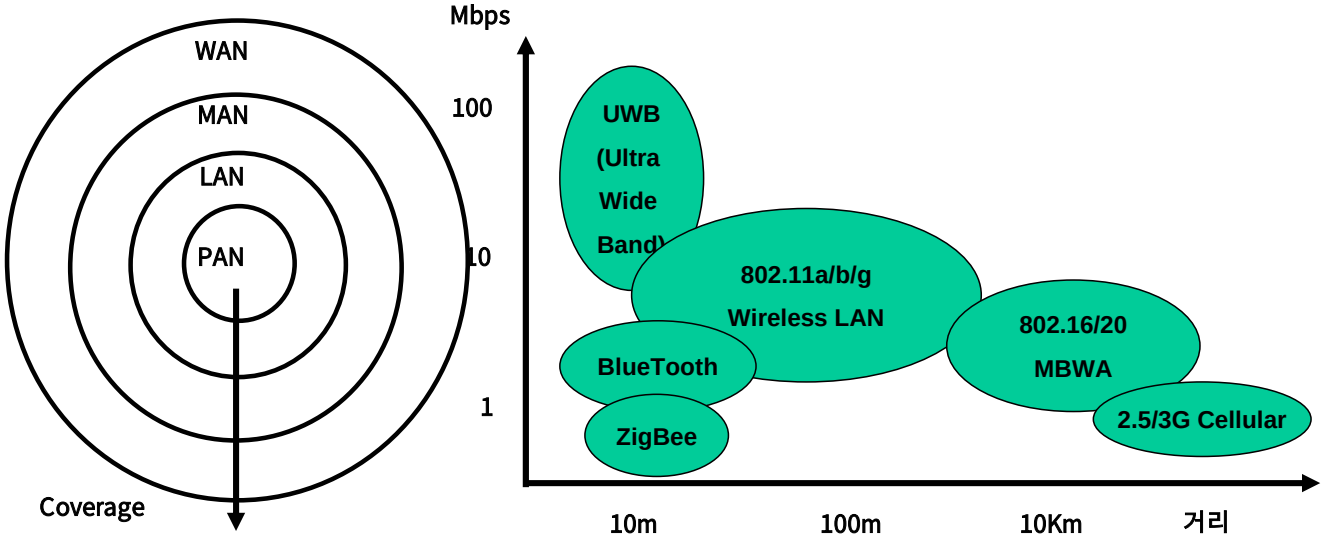
More Research & Test & Discussion

6. Next Generation Wireless

Next Generation Wireless

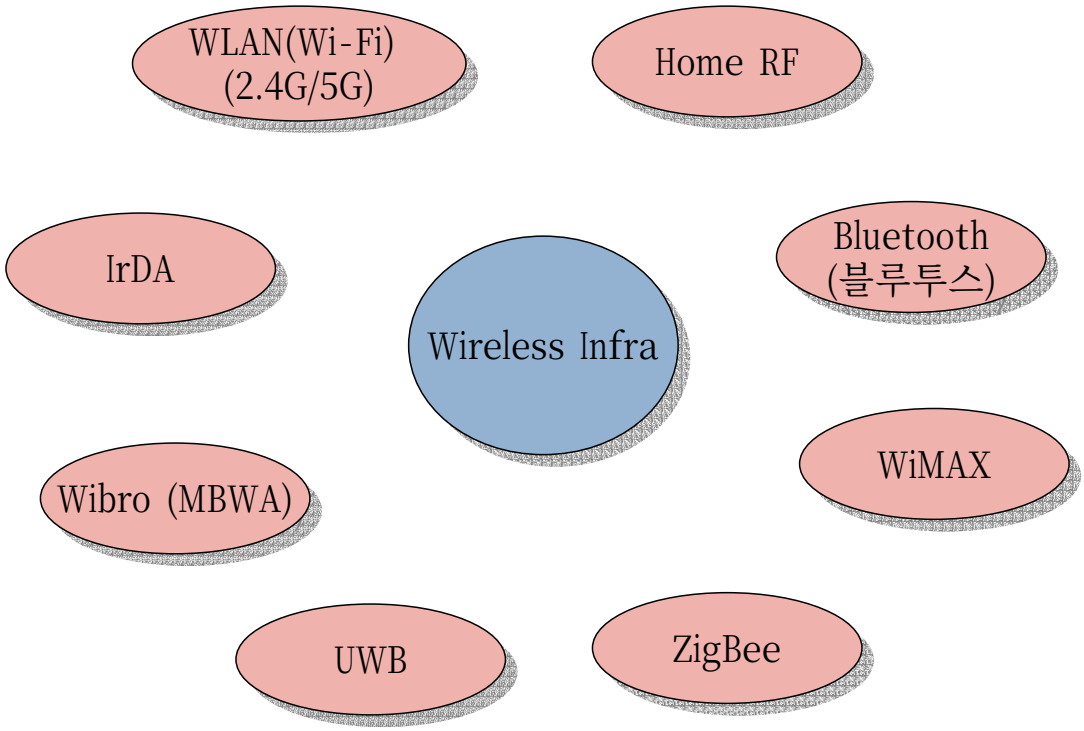
6. Next Generation Wireless

초고속 무선 PAN/LAN 기술 정의

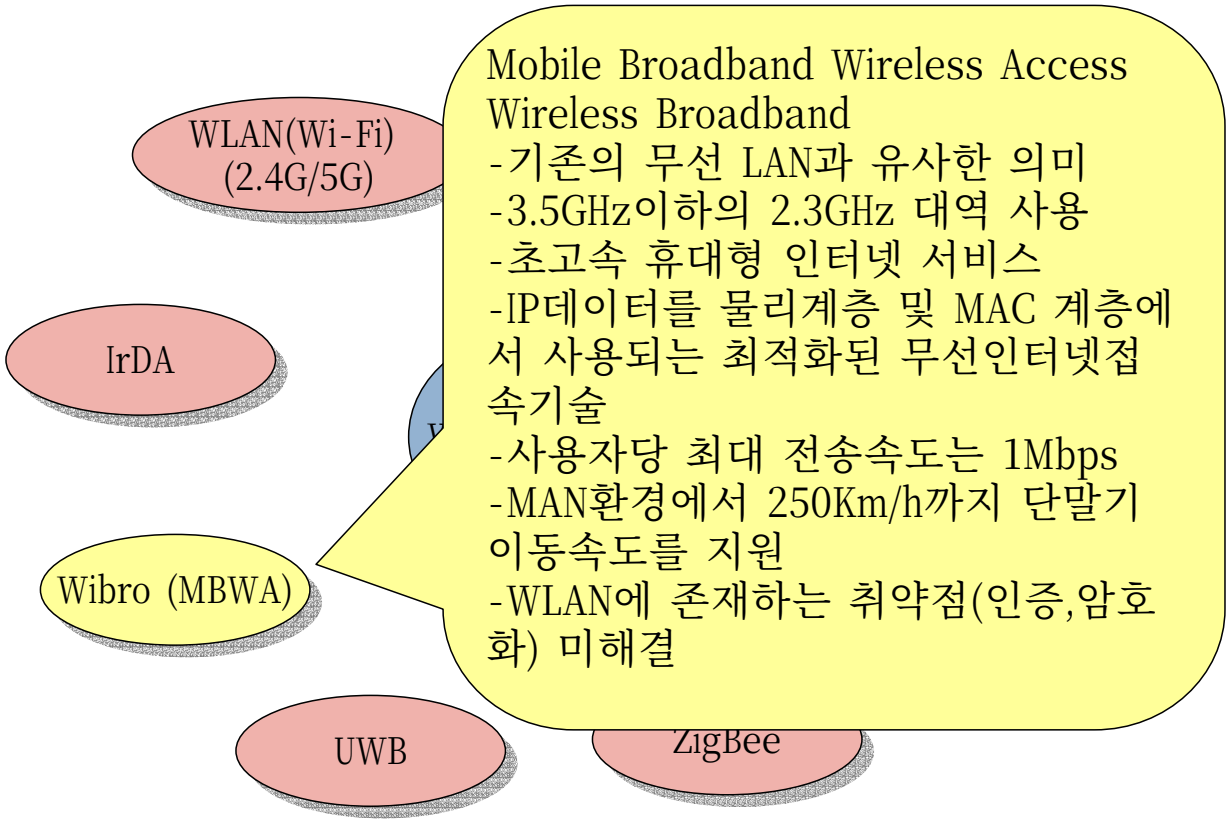


출처: HTI문서

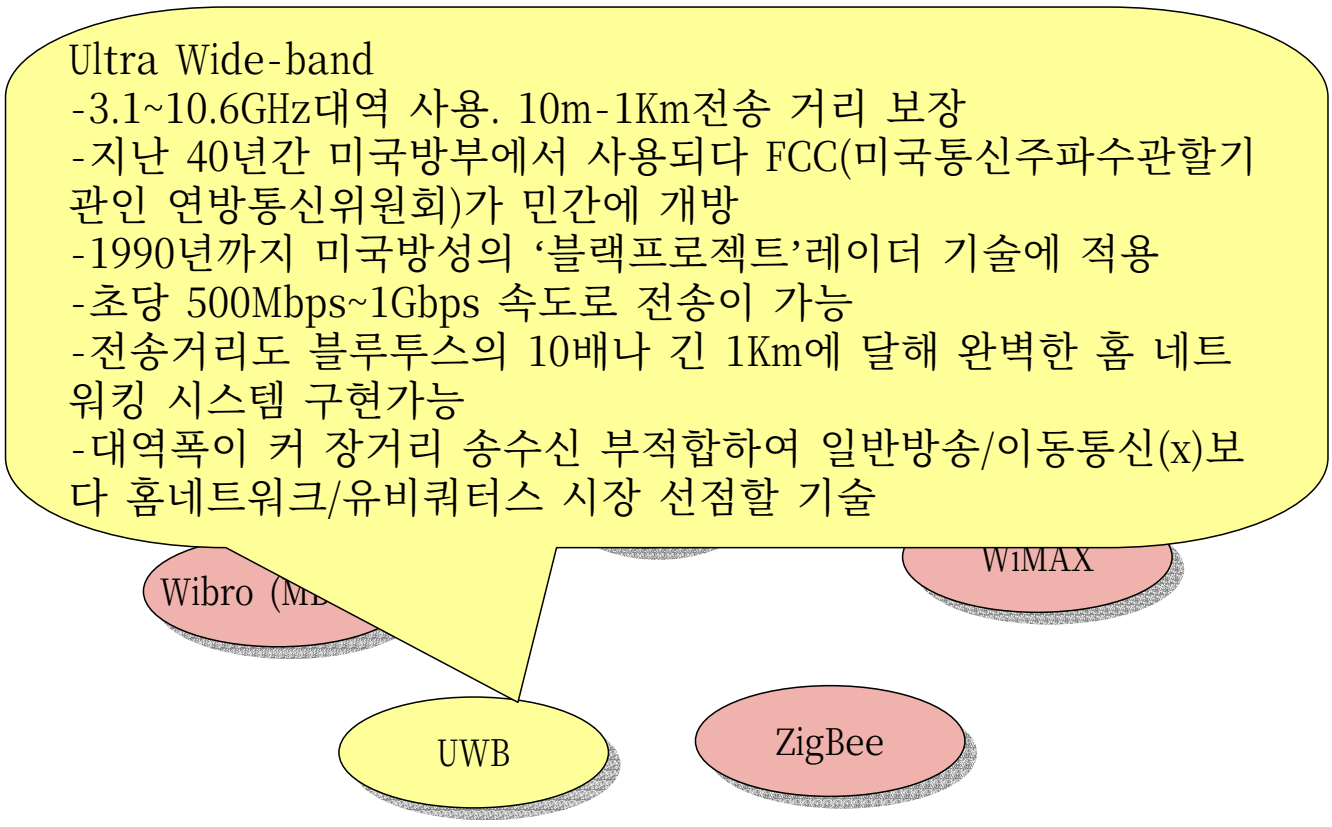
6. Next Generation Wireless



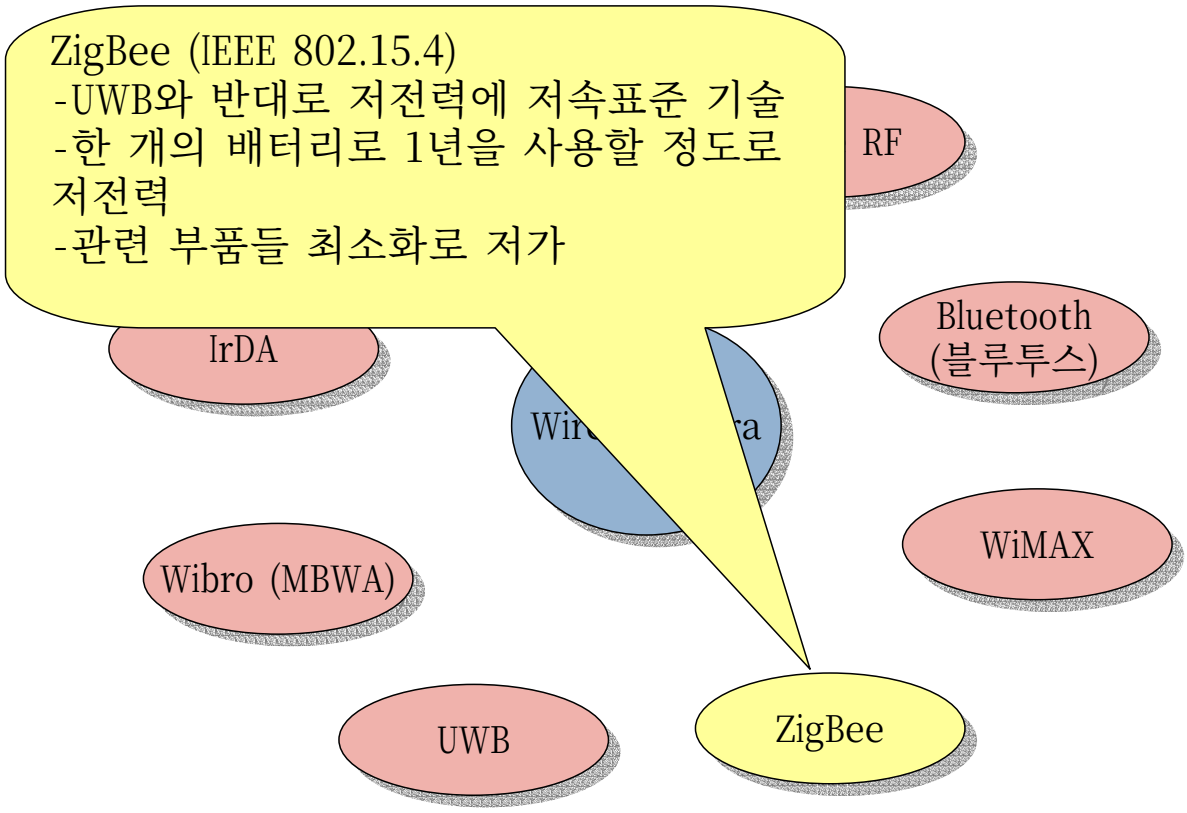
6. Next Generation Wireless



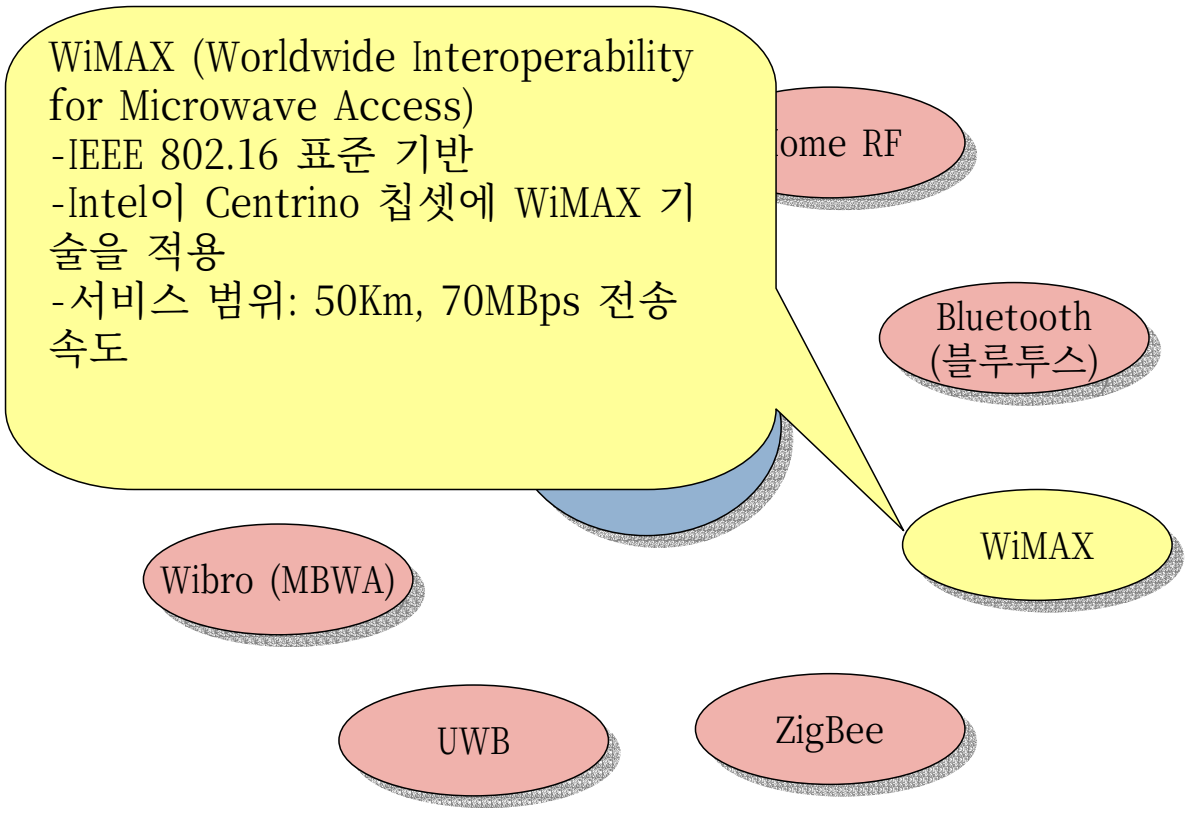
6. Next Generation Wireless



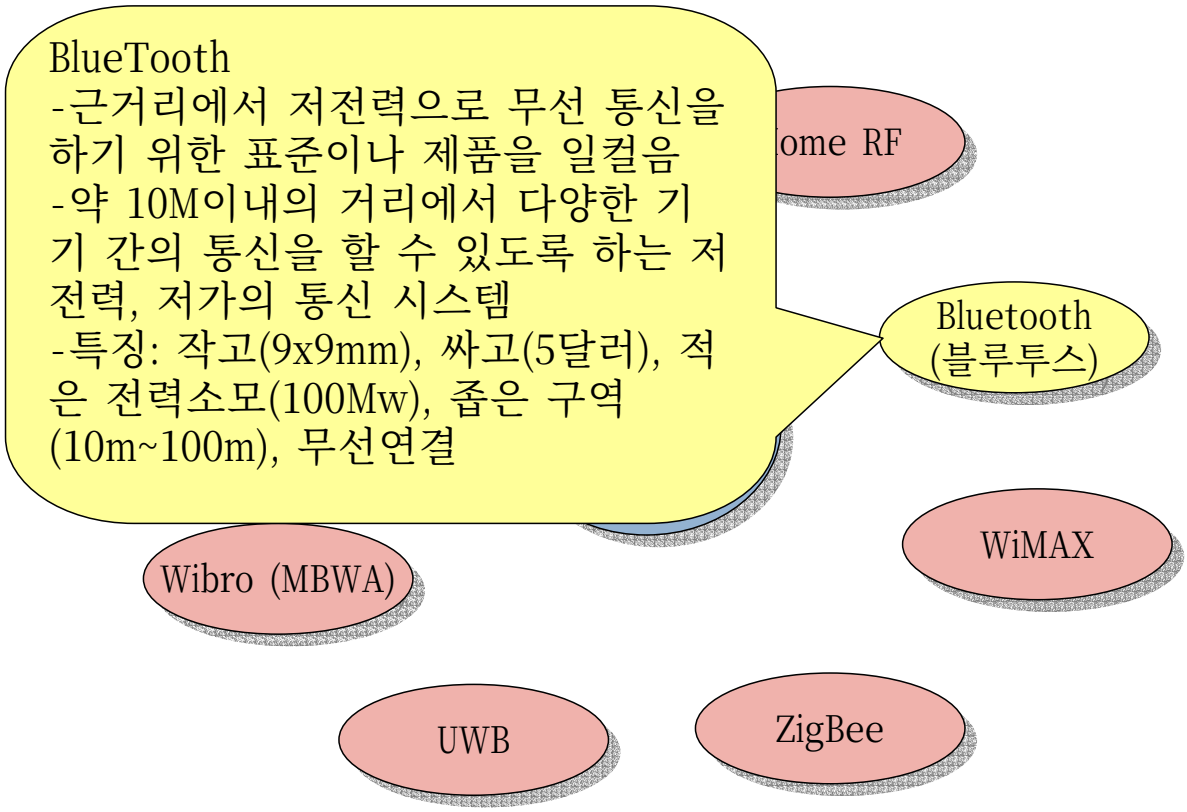
6. Next Generation Wireless



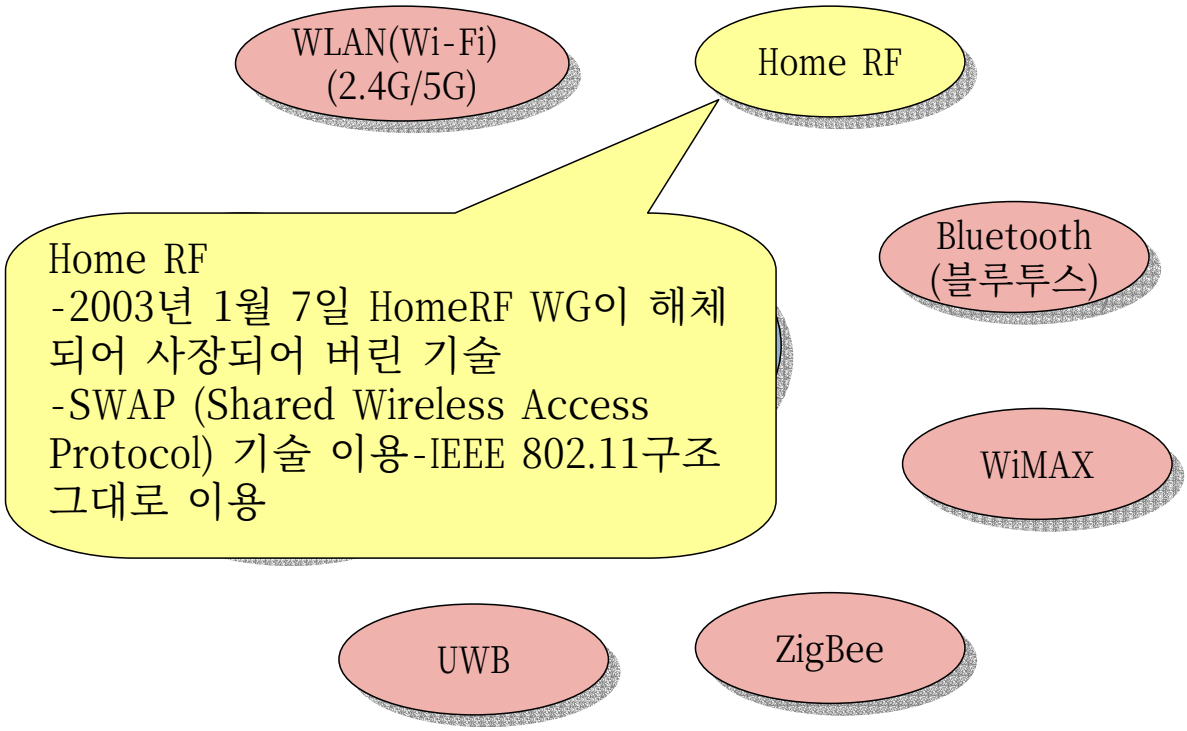
6. Next Generation Wireless



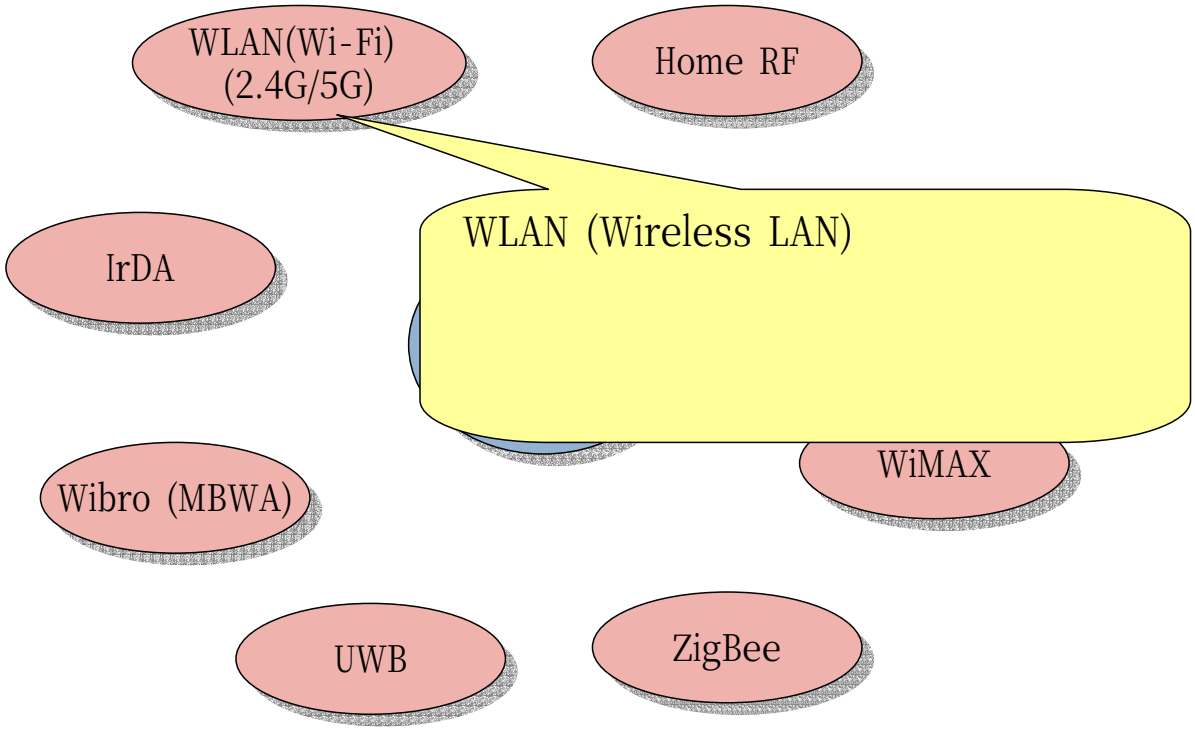
6. Next Generation Wireless



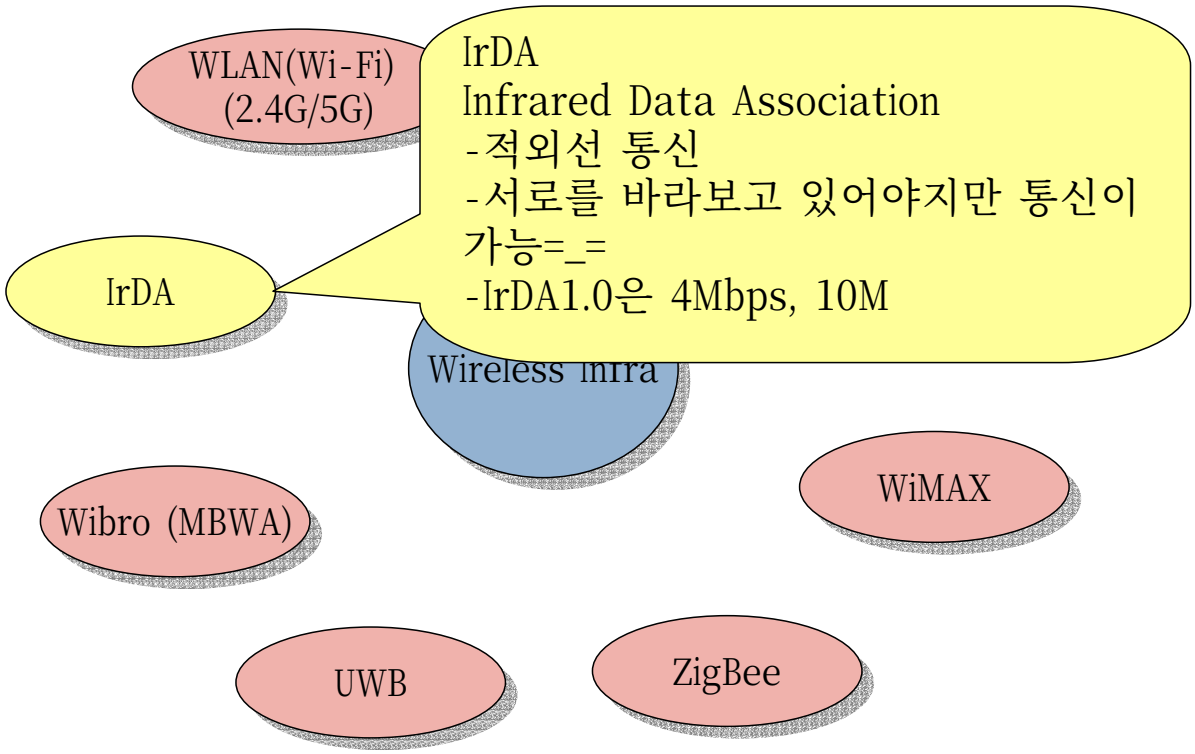
6. Next Generation Wireless



6. Next Generation Wireless

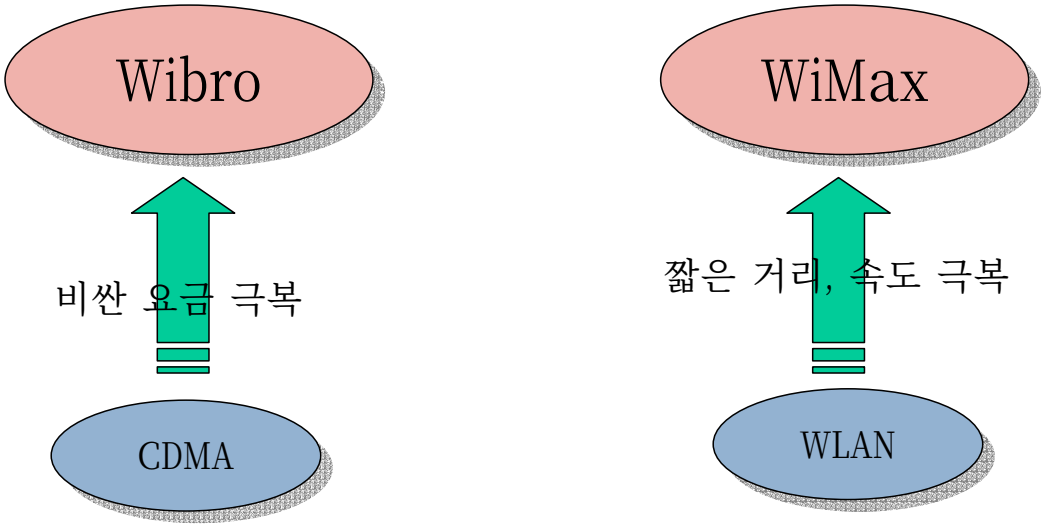


6. Next Generation Wireless

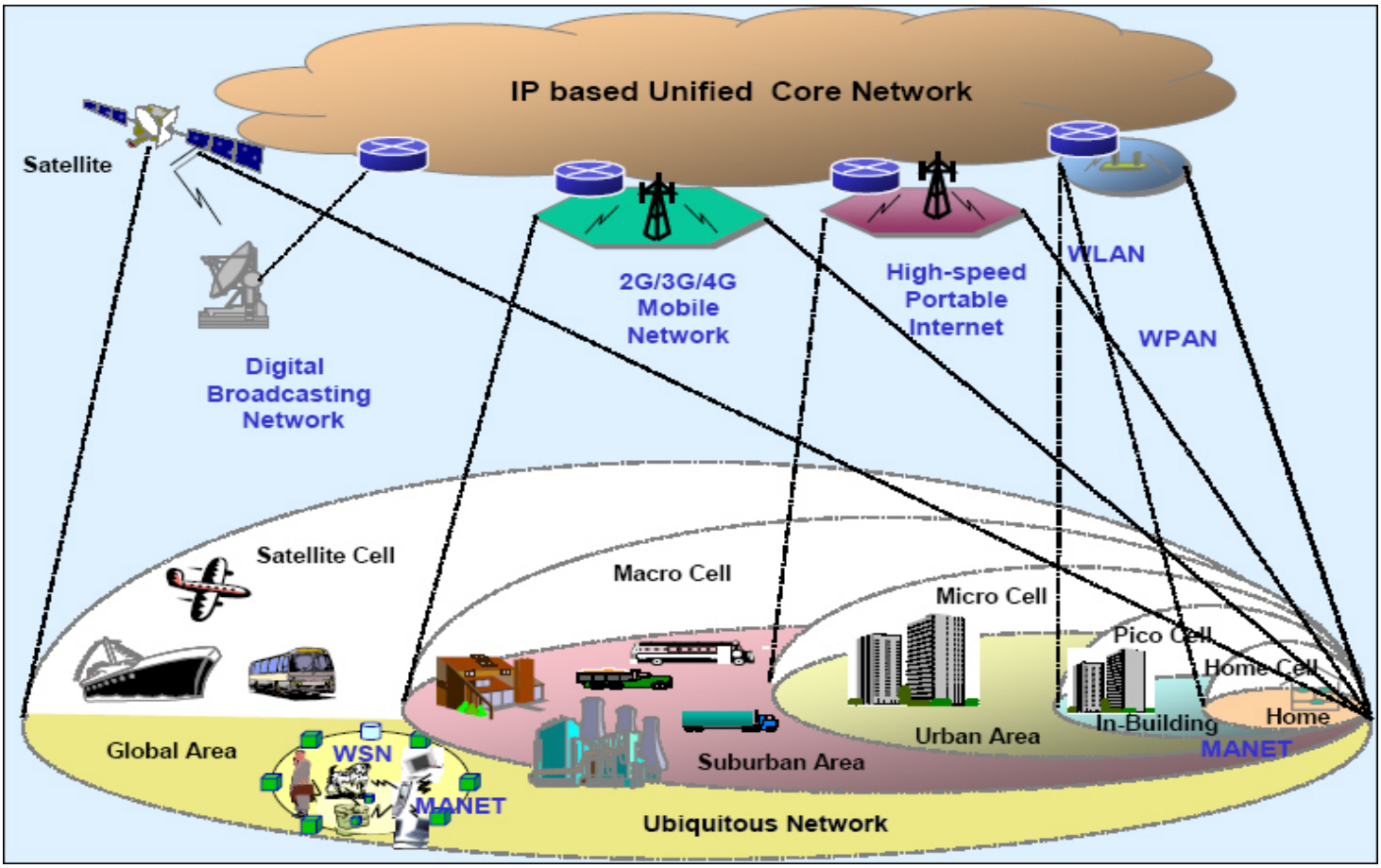


6. Next Generation Wireless

Wibro와 WiMax 비교

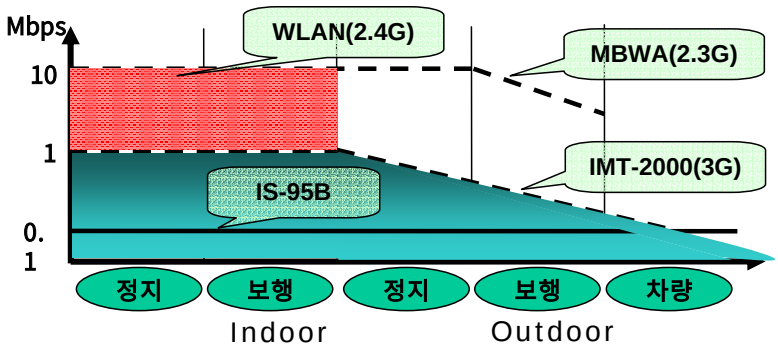


6. Next Generation Wireless



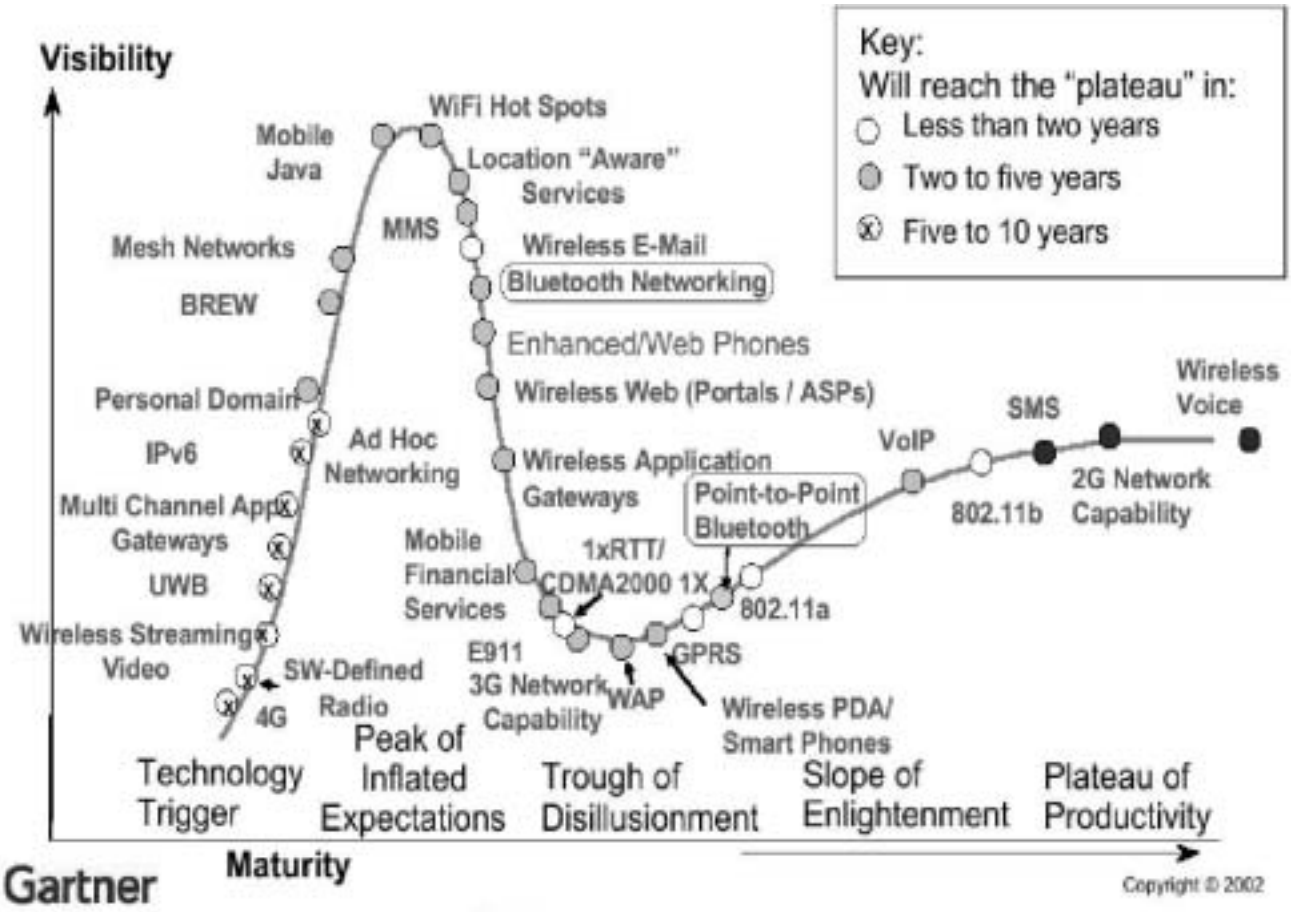
6. Next Generation Wireless

	WLAN (2.4G/5G)	MBWA (2.3G)	1xEV-DO, IMT-2000 (3G)
전송속도	▪ 초고속	▪ 고속	▪ 중고속
요금	▪ 저가	▪ 중저가	▪ 고가
이동성	▪ 정지/준정지	▪ 정지/보행/중저속이동	▪ 고속이동
제공 서비스	▪ 각종 인터넷 서비스	▪ 각종인터넷 서비스	▪ 간결한 정보서비스 ▪ 중저속 VoD등
강점	▪ 우수한 품질 ▪ 다양한 컨텐츠 이용	▪ 실외인터넷 제공 ▪ 중저속 이동성/고속전송 ▪ 다양한 컨텐츠 이용	▪ 실외인터넷 제공 ▪ 고속이동성/저속전송 ▪ 다양한 컨텐츠



출처: HTI문서

6. Next Generation Wireless

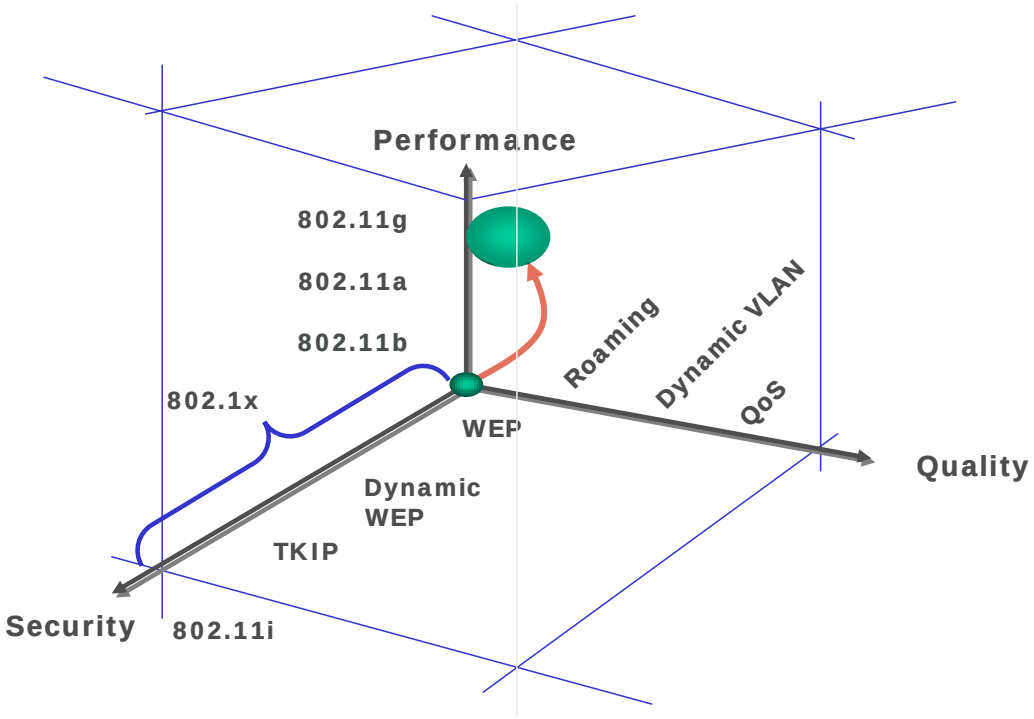


Reference (볼만한 사이트)

CISCO 802.11 무선 LAN 보안 백서
- http://www.cisco.com/global/KR/products/pc/wlp/1200/wswpf_wp.shtml

Discussion

WLAN 주요 표준



IEEE 802.11 무선랜 기본 통신 과정

1단계 : 클라이언트부터 주변 AP 검색 및 연결 대상 선정

1. Probe Request

2. Probe Response

2단계 : IEEE 802.11 무선 LAN 통신 인허가

3. Authentication Request

4. Authentication Response

3단계 : IEEE 802.11 무선 LAN 통신

5. Association Request

6. Association Response

무선랜 Client

AP (Access Point)