

5주차 3차시 무선 LAN의 보안 및 미래

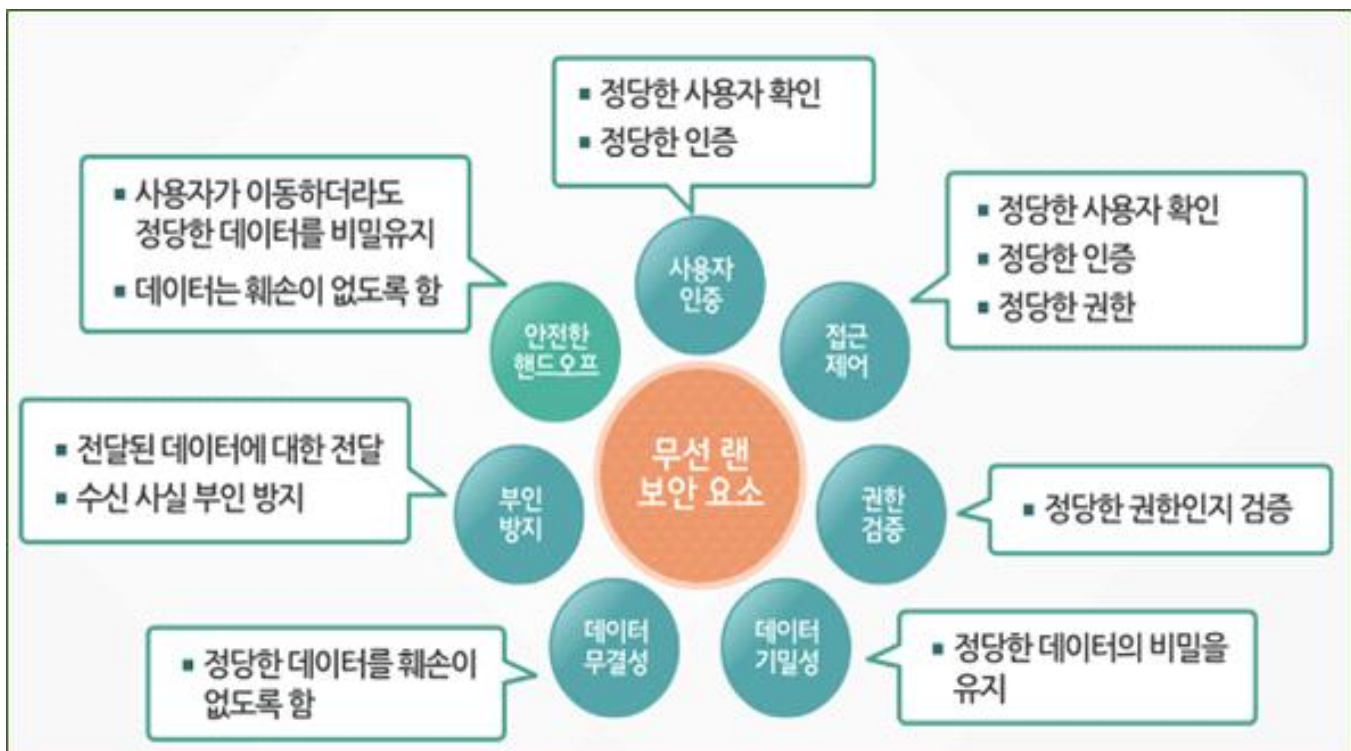
【학습목표】

1. CSMA/CA 및 DSSS의 원리를 설명할 수 있다.
2. OFDM 및 MIMO의 원리를 설명할 수 있다.

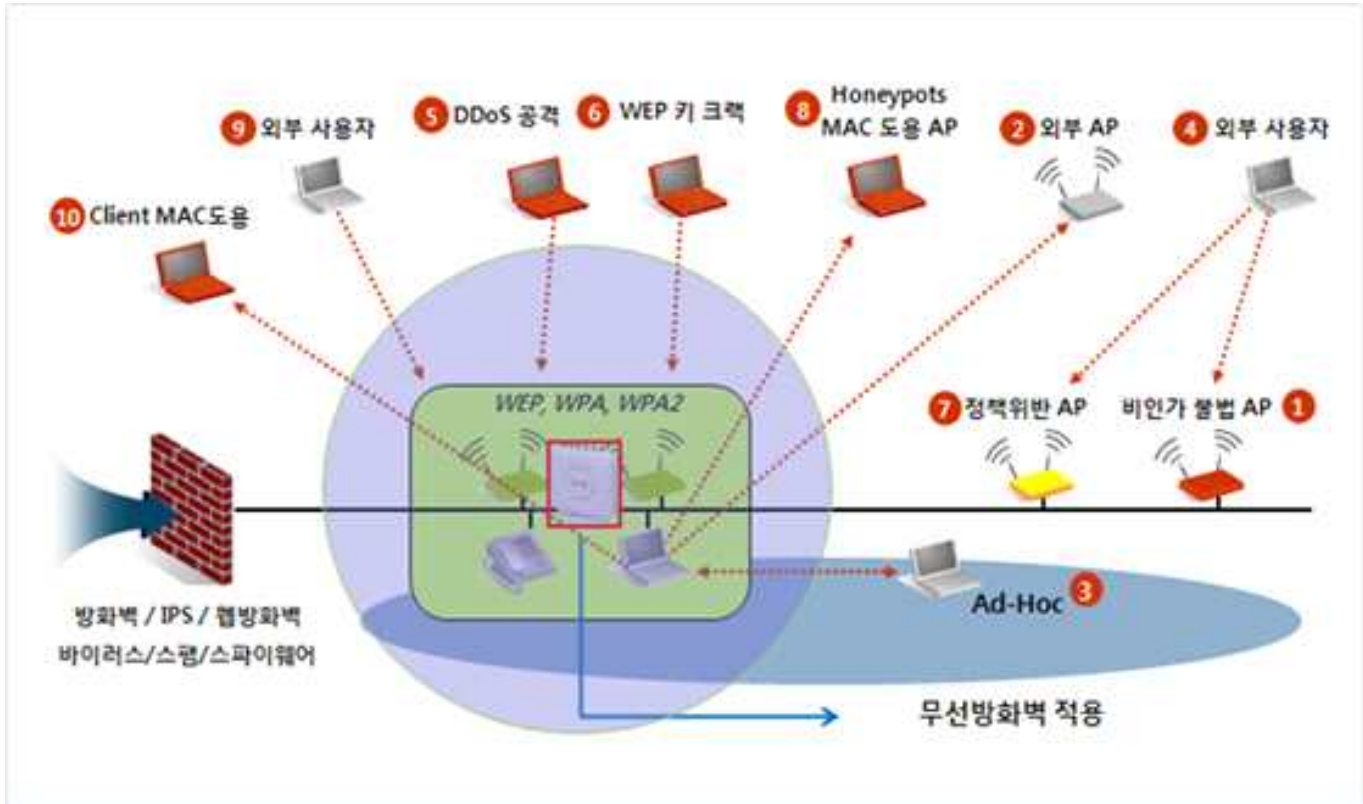
학습내용1 : 무선 LAN의 보안

1. 개요

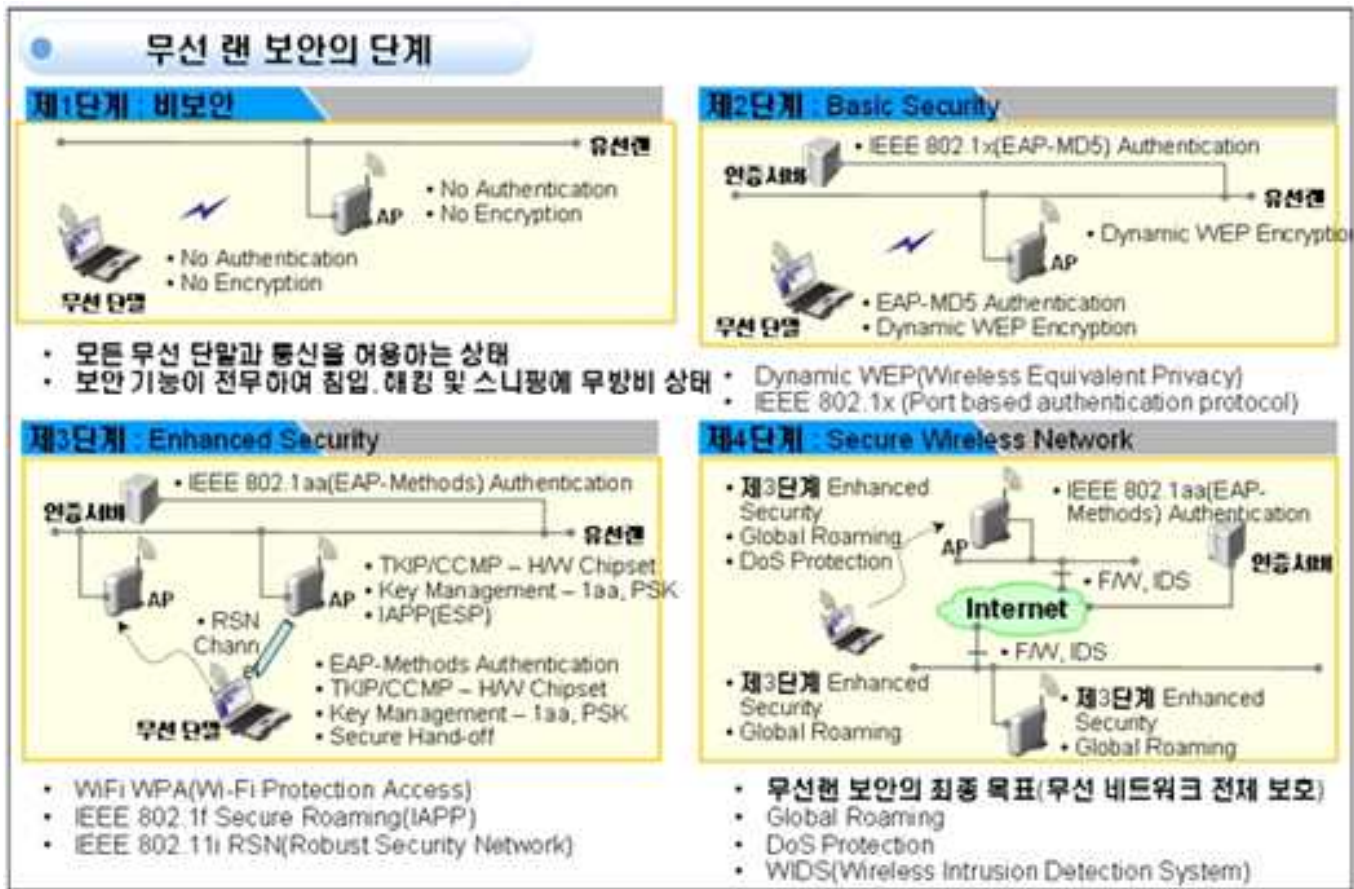
- 이동성, 확장성 그리고 편리성으로 확산되는 무선랜의 안정성 확보



- 무선 LAN의 안정성을 위협하는 요소들



- IEEE + Wi-Fi Alliance 의 인증과 암호화 기술을 정의한 보안 표준 기술 규격 제정

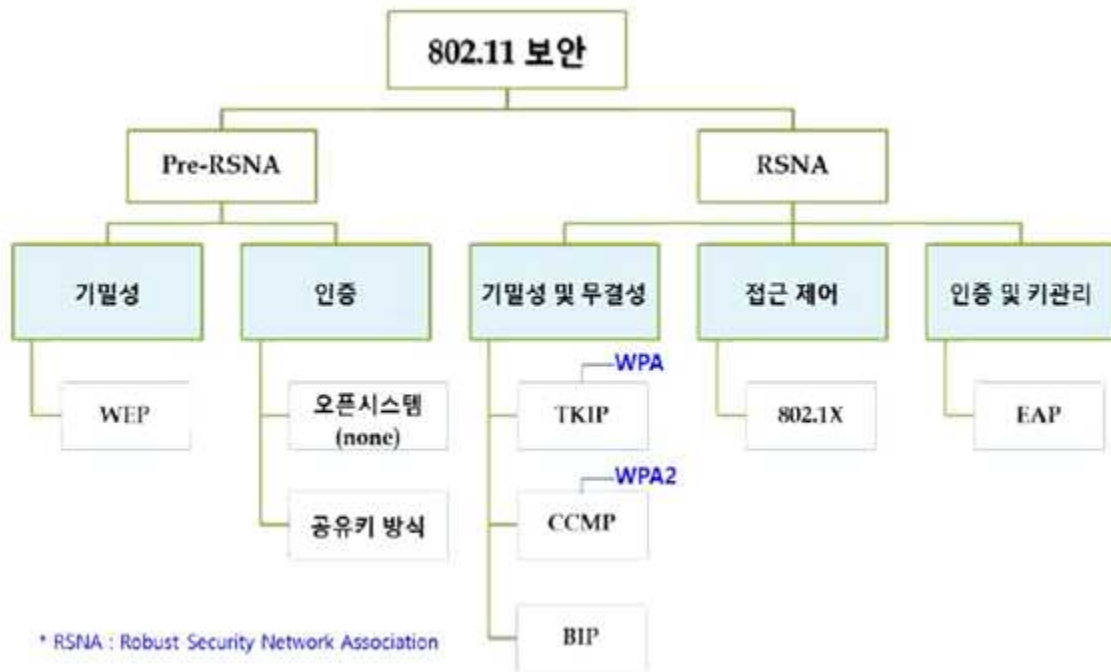


- 인증 및 암호화 기술

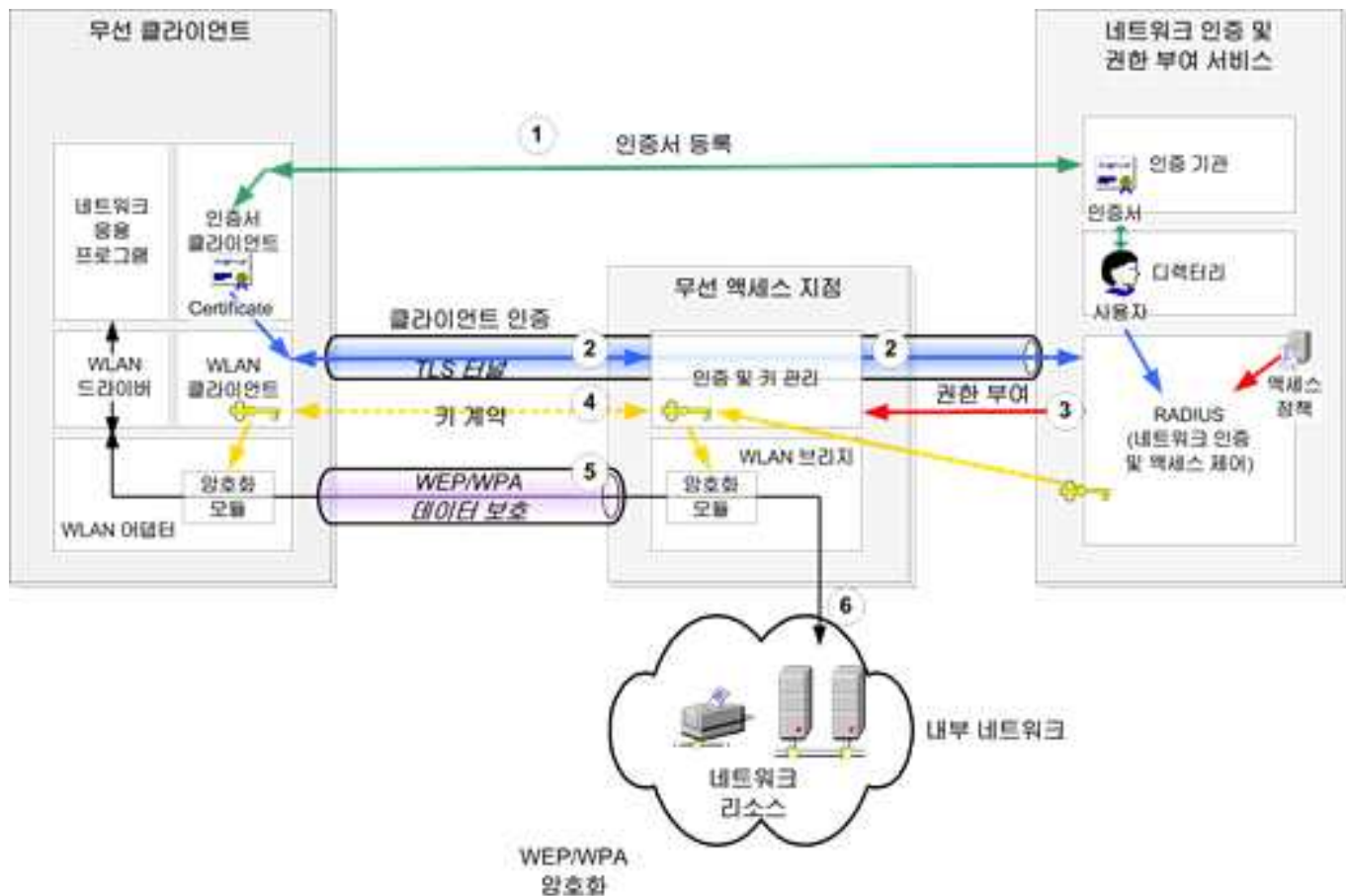
구분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access 2)
인증	사전 공유된 비밀키 사용 (64비트, 128비트)	사전에 공유된 비밀키를 사용하거나 별도의 인증서버를 이용	사전에 공유된 비밀키를 사용하거나, 별도의 인증서버 이용
암호방법	고정 암호키 사용 RC4 알고리즘 사용	암호키 동적 변경(TKIP) RC4 알고리즘 사용	암호키 동적 변경 AES 등 강력한 암호 알고리즘 사용
보안성	가장 취약하여 널리 사용되지 않음	WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	강력한 보안기능 제공

2. IEEE 802.11 표준 무선 LAN 보안 기술

- 보안 표준 영역
- Pre-RSNA: 오픈 시스템 인증 및 공유키 인증
- RSNA: 보안성을 높인 암호 방식



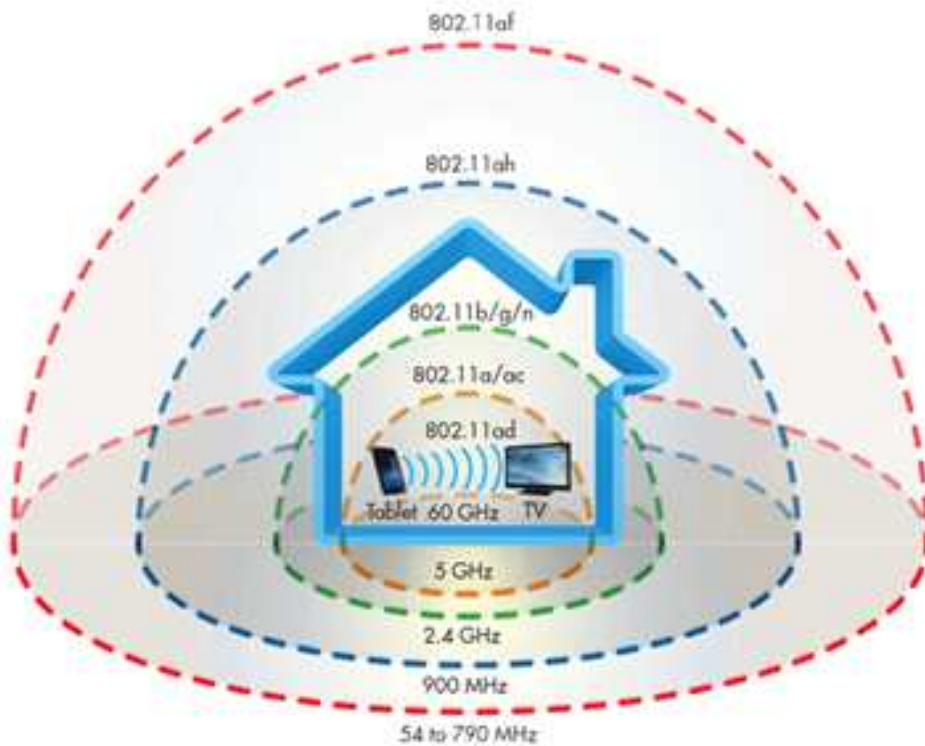
- IEEE 802.1x 인증 및 접근제어 방식



학습내용2 : 무선 LAN의 미래

1. 개요

- * 활용 범위의 확대 및 모바일과의 연동을 통한 새로운 기술의 등장
- 초고화질의 멀티미디어 전송을 가능하게 해주는 Gbps급 이상의 전송 속도를 보장하는 IEEE 802.11ac
- 기존의 제한적인 서비스 영역을 최대 수 Km까지 지원하기위한 광역 IEEE 802.11af 및 802.11ah
- 관련 장비의 셋업 시간을 100ms까지 빠르게 링크시켜주는 IEEE 802.11ai



2. 향후 무선 LAN 기술동향

- * 3가지 진화 방향
- 속도: 지금까지와 마찬가지로 고속을 추구
⇒ (IEEE 802.11ac, IEEE 802.11ad)
- 거리: 기존 기술(2.4 / 5 GHz 대역)에 비해 장거리 전송
⇒ (IEEE 802.11af, IEEE 802.11ah)
- 편의성: 링크 확립 시간의 대폭 단축
⇒ (IEEE 802.11ai)

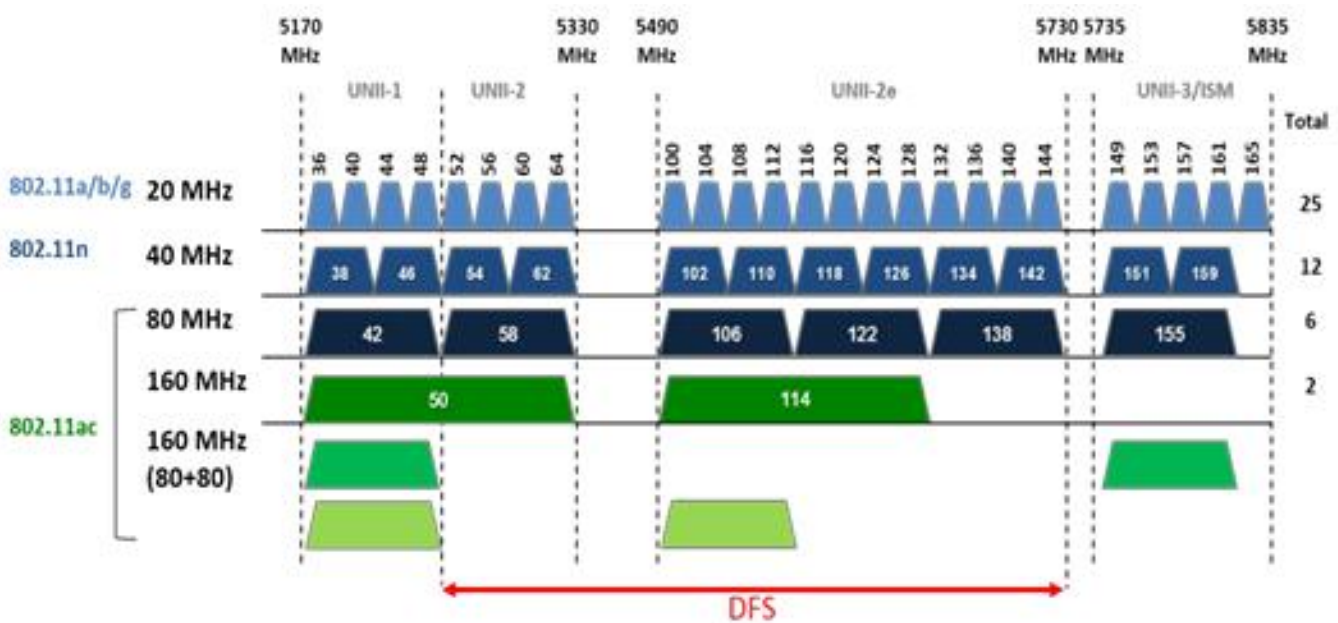


3. IEEE 802.11ac 초고속 무선 LAN



802.11ac

- Gbps 이상의 전송 속도 지원을 위하여 대역폭 확장
- 다수 사용자 동시 접속 기술 적용: Downlink Multi-User MIMO 기술
- 안정적인 전송 속도 지원을 위하여 2.4GHz 대역의 802.11b 및 802.11g와의 호환성 포기



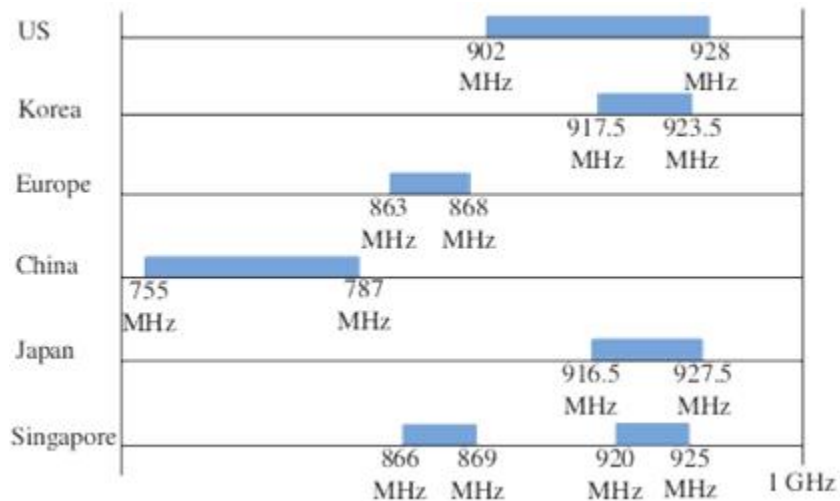
4. IEEE 802.11ah 광역 무선 LAN

IEEE 802.11ah



Wi-Fi HaLow™

- 스마트 그리드, 센서 네트워크, M2M 네트워크, 이동통신 오프-로딩 및 광역 무선 LAN 서비스 지원
- 900MHz 대역 사용 기술
- 1/2/4/8/16MHz 대역폭 지원 및 Single-User MIMO, Multi-User MIMO 동시 지원
- 향후 IoT(Internet of Things) 지원을 위한 소비 전력 최소화 및 광역 Wi-Fi 서비스 기능 포함



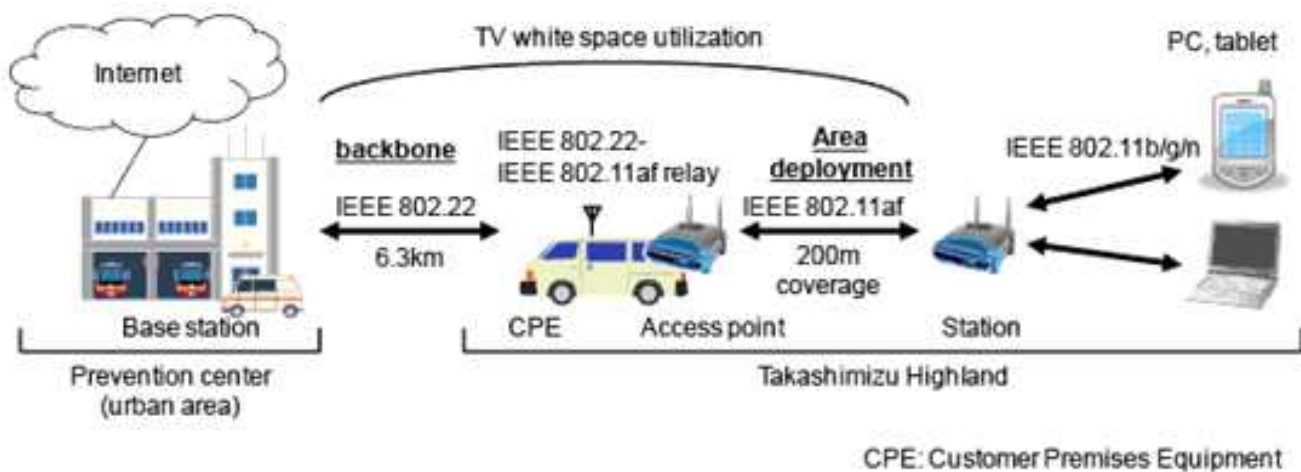
5. IEEE 802.11ah 광역 무선 LAN



현재 TV 사용 주파수 중 유휴대역 (TVWS: TV White Space) 활용 무선 LAN 기술
 국내의 경우 54 ~ 698MHz 대역의 밴드가 해당(TV 채널 번호로는 CH2 ~ CH51)
 1Km 넓은 서비스 범위 및 실내/외 동시 지원을 위한 기술

- Available Spectrum

- VHF(54~72, 76~88, 174~216 MHz), UHF(470~698MHz) in USA, Korea and Canada



6. IEEE 802.11ah 광역 무선 LAN



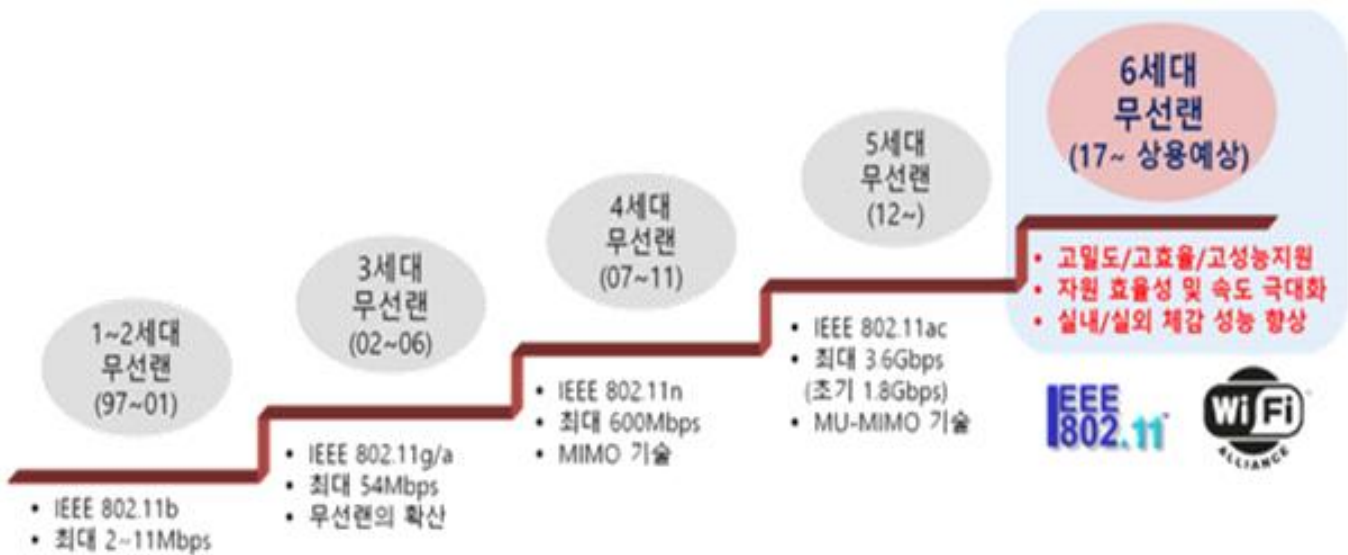
- 무선 LAN 초기 셋업 및 링크 시간의 획기적 단축을 위한 기술
- 보안을 약화시키지 않으면서, AP Discovery, Network Discovery, TSF Synchronization, Authentication & Association, Higher Layer와의 절차 병합 등의 과정들을 간소화하여 신속 접속을 구현

	802.11af	802.11ah	802.11ai
목적	TVWS(TV White Space) 대역에서의 무선랜 활용	900MHz 대역에서의 무선랜 활용	빠른 무선랜 접속
주파수 대역	TV White Space 대역(54~88MHz, 470~806MHz 등)	1GHz 이하에서 TVWS 대역을 제외한 대역(902~928MHz 등)	MAC 표준 기술이므로, 대역에 무관함
채널 대역폭	5.5MHz와 그 배수	1/2/4/8/16MHz	사용하는 PHY 표준 기술의 채널 대역폭
핵심 기술	지오 로케이션 데이터베이스 기반 TV 유휴 대역 활용 기술	<ul style="list-style-type: none"> · 새로운 프리앰블 · 짧은 비콘 (beacon) 신호 · 개층적 TIM(Traffic Indication MAP) · 절전 모드 	<ul style="list-style-type: none"> · 프로브 응답(Probe response) 필터링 기술 · 빠른 무선랜 접속을 위한 새로운 디스커버리 프레임 · 보안 절차 간소화

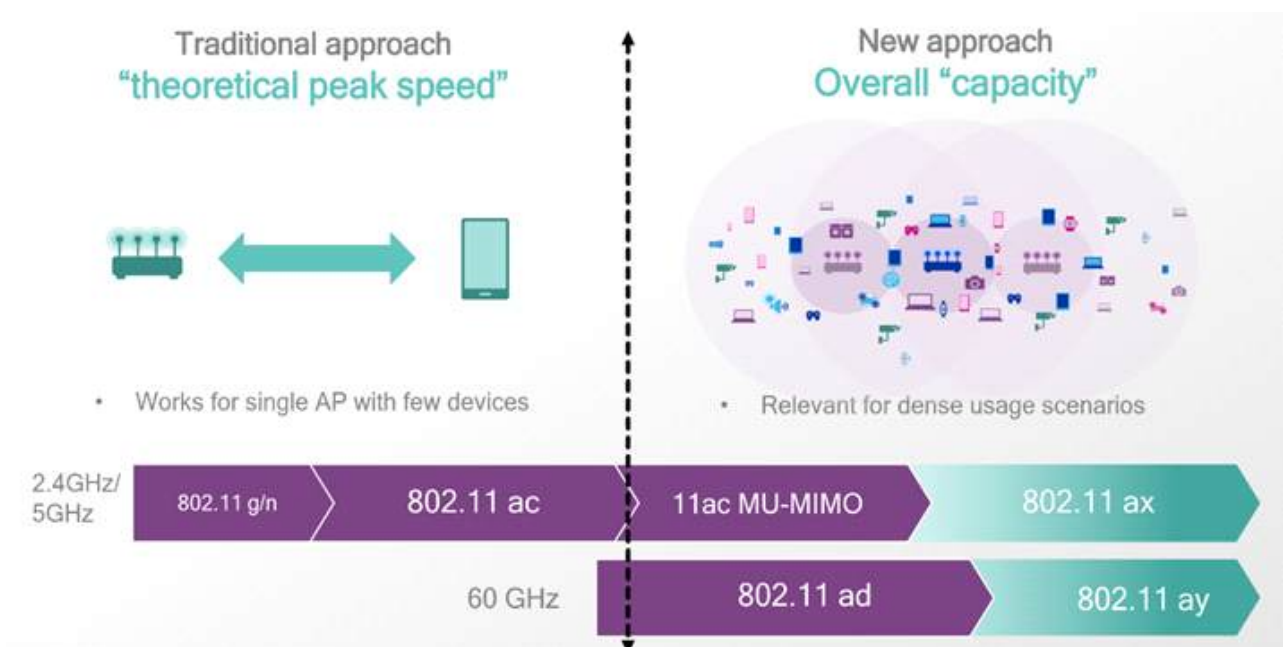
7. IEEE 802.11ax HEW (High Efficiency ELAN)



- 관련 노드들의 기하 급수적 증가 및 이를 위한 AP들의 증가 설치, 운영 등의 환경에서 사용자들에게 향상된 성능과 서비스를 제공하기 위한 기술
- 최소 4배 이상의 체감 성능 향상을 위한 기술



8. 무선 LAN의 발전 방향



* 기타 IEEE 802.11 표준들

- IEEE 802.11d: 지역 간 로밍용 확장 기술 (2001)
- IEEE 802.11e: QoS, 패킷 버스팅 등 기능 확장 기술 (2005)
- IEEE 802.11f: 인터 액세스 포인트 프로토콜
- IEEE 802.11h: 유럽용 5GHz대역 전송 방식 (2004)
- IEEE 802.11i: 보안 확장 (2004)
- IEEE 802.11j: 일본용 전송 방식 (2004)
- IEEE 802.11k: 전파 자원 측정 확장 기술 (2008)
- IEEE 802.11p: 빠르게 움직이는 운송 수단을 위한 무선 접속 기술
- IEEE 802.11r: 빠른 로밍 (2008)
- IEEE 802.11s: ESS 메쉬 네트워킹
- IEEE 802.11t: 무선 성능 예측 (WPP)
- IEEE 802.11u: 802.11 기반이 아닌 네트워크와의 상호 연동 (2011)
- IEEE 802.11v: 무선 네트워크 관리
- IEEE 802.11w: 보호된 관리 프레임 (2009)

【학습정리】

1. 이동성, 확장성 그리고 편리성으로 확산되는 무선랜의 안정성을 확보하기 위해 무선 LAN 보안 기술들이 많이 대두되고 있다.
2. 무선 LAN은 속도는 고속을 추구하고, 거리는 기존에 비해 장거리로 전송시키며, 링크 확립 시간을 대폭 단축시키기 위한 방향으로 진화하고 있다.