+ 최홍석 · 무선랜 전문 엔지니어

무선 네트워크의 이해와 발전 방향

IEEE 802.16e의 표준인 Wibro가 시장에 나올 때 이런 얘기가 있었다. Wibro가 나오면 무선랜 시장은 없어질 것이다. 하지만, 현재 무선 시장은 여러 가지 방식이 Convergence 되고 있다. 이동통신의 2G, 3G, 앞으로의 4G와 Wibro와 WiMax, Wi-Fi 등이 공존하고 있으며, 모든 통신 방식을 지원하는 One-Chip 개발과 각각의 칩을 따로 생산하는 방식으로 진행되고 있다.

무선 네트워크의 이해

무선 네트워크는 기기들에게 선에서의 자유, 우리 생활에는 편리함을 제공한다.
구리선을 사용하던 전화에서 무선 전화기, 휴대 전화기가 나왔고, 트위스트 패어 케이블을 이용하여 사용하던 인터넷이 Wi-Fi라는 무선 네트워크가 되었다. 기업은 무선 네트워크를 사용하여 직원들이 책상의 굴레에서 벗어나 보다 넓은 생각을 하게 한다. 그만큼 속도와 보안이 상당한 발전을 이루었기 때문에 가능한 일이다.

무선 네트워크 표준

국제 표준화는 1990년 10월부터 위원회에 IEEE 802.11에 의해 무선 매체 접근제어 물리 계층 규격에 대한 표준화가 OSI참조모델에 준하여 진행되고 있다.

	802.11b	802.11a	802.11g	802.11n
Standard Approved	1999년 09월	1999년 09월	2003년 06월	2009년 09월
Available Bandwidth	83.5MHz	580MHz	83.5MHz	83.5/580MHz
Frequency Band of Operation	2.4GHz	5GHz	2.4GHz	2.4/5GHz
Non-Overlapping Channels	3~4	21	3~4	3~4/21
Data Rate per Channel	1~11Mbps	6~54Mbps	6~54Mbps	1~600Mbps
Modulation Type	DSSS, CCK	OFDM	DSSS, CCK, OFDM	DSSS, CCK, OFDM, MIMO

무선의 표준에서 802.11b는 11Mbps의 전송 속도가 나오고, 802.11a/g는 54Mbps의 전송 속도가 나온다. 그런데, 실제 속도는 802.11b가 약 5.5Mbps, 802.11a/g가 약 25/18Mbps로 대략 1/2 정도가 되는 이유는
첫 번째로 SISO(Single Input Single Output) 안테나에 있다. 유선 네트워크로 말하면 Half Duflex 방식으로 보낼 때는 보내는 것만 하고 받을 때는 받는 것만 하기 때문이다.
두 번째로 무선랜의 특성상 데이터의 신뢰성을 위하여 무선 패킷이 한 개가 전송될 때마다 잘 받았다는 답변으로 Acknowledge를 패킷 단위로 각각 발생하기 때문에 실제 전송 속도에 몇 %를 Acknowledge가 가져간다.

현재 802.11n TG(Task Group)에서는 SISO를 MIMO(Multiple Input Multiple Output) 방식인 다중 송수신 안테나 기술을 채택하여 송수신 데이터 효율을 높였으며, MIMO 방식의 스마트 안테나는 노이즈를 최소화하여 원활한 데이터 전송경로를 조정한다.
802.11n에서는 Acknowledge도 프레임 집속(Focusing) 기능으로 Ack를 최소화 시키고, 효율성을 최대화 한다.그리고 기존 하나의 채널당 20MHz를 사용하던 것을 40MHz로 확장시키는 기술을 사용하여 속도를 향상시켰다. 802.11a/g 상용 당시에도 비슷한 기술(turbo mode)이 있었으나, 당시에 국내 전파법의 점유 주파수 대역의 규정을 위배하였기 때문에 사용하지 못하였다. 현재는 802.11n 표준 때문에 수정되었고 802.11n Draft 2.0 이상에서는 40MHz로 확장시 300Mbps의 무선 Bandwidth를 사용할 수 있다.
전송 속도를 위한 기본 표준 외에도 로밍을 위한 표준, 무선 QoS를 위한 표준, 동적 주파수 선택 기능 등 다양한 무선의 기술 표준들이 만들어 졌고, 현재 만들어 지고 있으나 AP에서 지원할 수 있는 기술의 한계 때문에 무선랜 컨트롤러 제품들이 출시되고 있다.

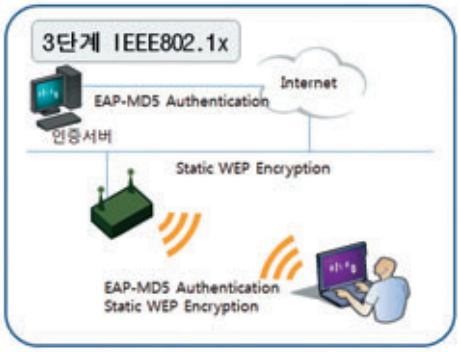
무선랜 보안 기술 동향

1단계는 초기의 무선랜을 보안 설정이나 암호화 없이 사용하였으나, 기업이나 개인의 정보 보호 때문에 최근에는 사용하지 않는다. ESSID의 숨김 기능은 고급 사용자들에게는 확인이 가능하여 특별한 보안은 되지 않으나, 일반적인 사용자의 무분별한 접근은 막을 수 있으므로 현재도 많이 사용되고 있다.

* 참고사항
- SSID : Service Set IDentifier
- ESSID : Extended SSID
- BSSID : Basic SSIC

2단계는 AP와 단말 사이에 RC4 Encryption Algorithm을 사용하여 암호화 한다. 하지만, Shared Key를 이용하는 문제로 Key의 유출이나, 해킹 프로그램으로 Key의 Scan이 가능하기 때문에 대기업 및 공공기관에서는 사용하지 않는 것을 권고한다.

* 참고사항
- WEP : (Wired Equivalent Privacy) 무선 데이터의 보안성을 제공하기 위하여 1997년 IEEE802.11 표준에 정의된, 데이터의 암호화에 동일키를 사용하는 대칭형 구조임

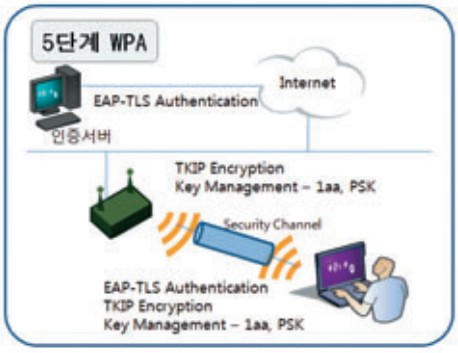


3단계는 2단계 보안을 보완하는 방법으로 인증과 보안을 같이 사용하는 방식이지만, 보안은 2단계와 같은 Shared(or Static) WEP을 사용하여 데이터 보호가 완전하게 되지 않는다.

* 참고사항
- EAP(Extensible Authentication Protocol) : RFC2284에 정의된 PPP 프로토콜의 확장판 EAP는 전통적인 인증방식, 토큰카드, 커버로스 등 여러 인증방식을 지원하는 전반적 인증 프로토콜이다.
- MD5(Message Digest 5) : ID/PW, 단방향 인증 방식

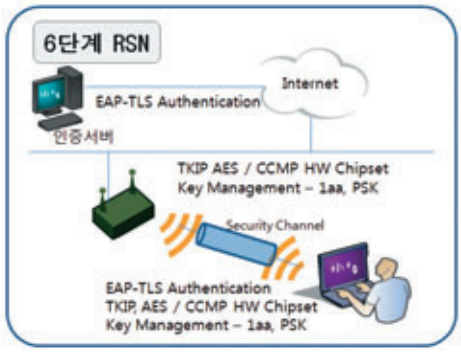
4단계는 3단계의 보안 및 암호화의 보완, 상호인증 방식인 인증서 기반의 인증 및 동적인 WEP을 적용하여 암호화키의 유출 문제를 해결한다.

* 참고사항
- TLS(Transport Layer Security) : 단말과 인증서버가 인증서를 이용하여 상호인증하고, 세션기반의 동적 WEP키를 생성 분배하는 방식
- TTLS(Tunneled TLS) : 구현의 편리를 위해 유연한 단말 인증 방법을 채택한 방식으로 단말 인증은 ID/PW로 하고 서버 인증은 인증서 방식으로 인증하는 방식



5단계는 WEP 보안의 취약점을 개선한 방식으로 48bit의 IV를 사용한다. WPA-TKIP은 WEP을 확장한 방식을 사용하여 기존 단말의 하드웨어 교체 없이 보다 발전된 암호화 방식을 사용할 수 있도록 설계되었다. TKIP은 WEP을 이용한 암호화 이전에 별도의 Key 생성 후 WEP에 적용되는 Key가 각 프레임마다 변경되도록 하였다. 그리고, 메시지 무결성 코드인 MIC를 프레임에 포함시켜 WEP 알고리즘의 취약점을 해결하였다.

* 참고사항
- WPA(WiFi Protected Access) : EAP와 TKIP, 802.1x의 세 가지 기술을 조합하여 만든 무선 통신 데이터를 암호화하는 기술로 마스터 킷값을 이용해 사용자 인증 및 전송데이터를 암호화 하는 방식이다.
- WPA는 TKIP(Temporal Key Integrity Protocol)를 기반으로 기존 무선에서 사용 중인 WEP의 문제점을 개선했다. 즉, 무선 네트워크를 통해 데이터를 보낼 때 암호화된 정보의 키를 공유해 보안성이 낮았던 기존 WEP와 달리 이미 한번 개선된 알고리즘을 활용해 훼손이 없도록 키를 보호해 준다.



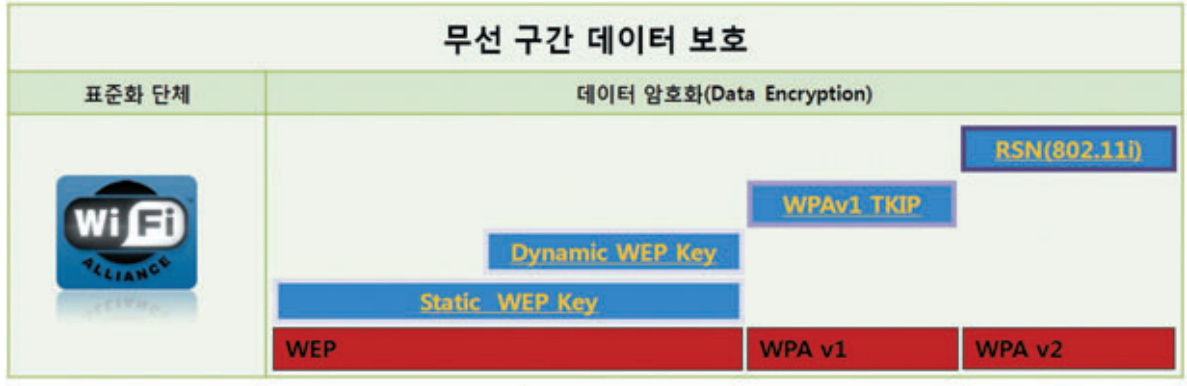
6단계는 5단계 보다 더 강력한 알고리즘인 CCMP를 기본 알고리즘으로 정의하고 있고 암호알고리즘 모듈은 하드웨어 칩셋으로 한다. 패킷 번호는 계속 증가하여 동일한 임시키에 중복되지 않도록 하여 재시도 공격을 방지하며, MAC 헤더 정보의 일부인 추가 인증 데이터를 CCM 암호화 과정에 포함시켜 위조를 방지한다.

* 참고사항

- CCMP(Counter mode with CBC-MAC Protocol) : CCM 모드를 사용하는 AES(Advanced Encryption Standard) 암호 알고리즘을 사용한다.
- MIC : Message Integrity Code

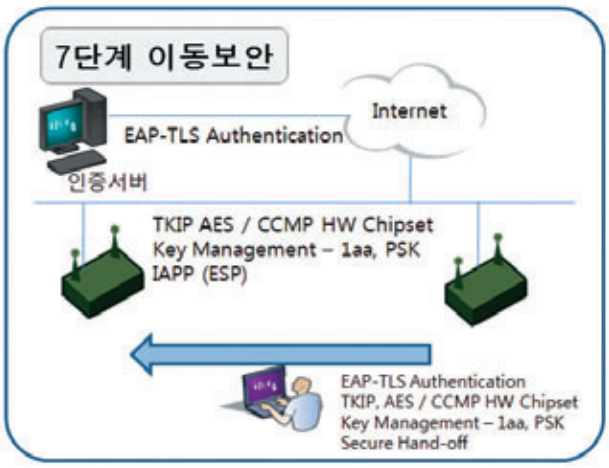
[EAP 인증 타입 비교표]

Topic	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
보안표준	국제표준	국제표준	국제표준	국제표준	Cisco표준
사용자 인증서	N/A	필요	필요 없음	필요 없음	N/A
서버 인증서	N/A	필요	필요	필요	N/A
신용증명	없음	강함	강함	강함	약함
동적 키 지원	지원안함	지원	지원	지원	지원
상호인증	지원안함	지원	지원	지원	지원



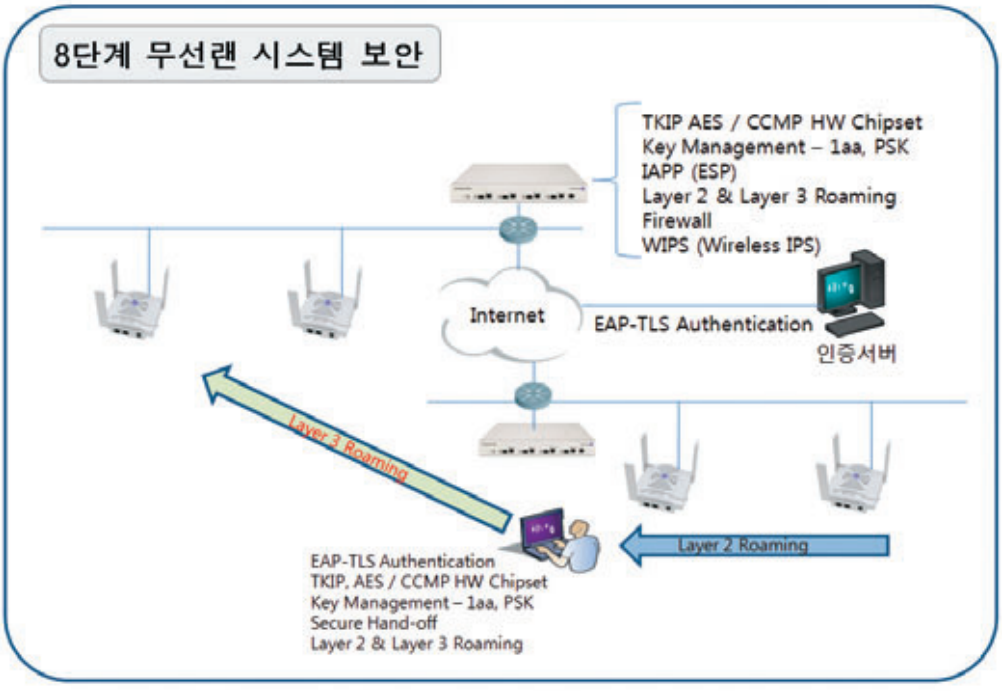
항목	Static WEP Key	Dynamic WEP Key	WPA v1	WPA v2
보안키 적용 방식	WEP(24Bit IV)	WEP(24Bit IV)	TKIP(48Bit IV)	CCMP
암호화 알고리즘	RC4	RC4	RC4	AES
암호 비트	40/128bit	128bit	128bit	128bit
보안 레벨	하(매우 취약)	중/상	상	최상

[무선 데이터 암호화]



7단계는 6단계 이상의 기능을 가진 AP에 IEEE 802.11f 규격인 IAPP(Inter-AP Protocol) 기능을 추가하여 무선랜 사용자의 안전한 이동성을 보장하는 보안 단계이다.

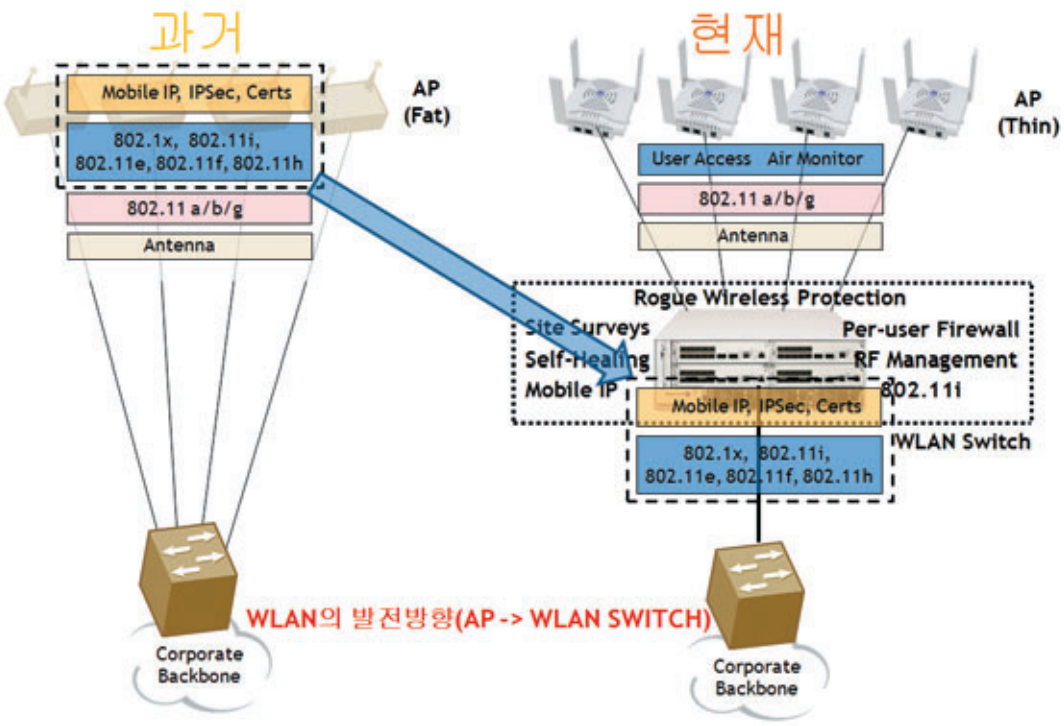
802.11f TG는 무선 단말기가 새로운 AP로 핸드오프 할 때 끊어짐 없는 안전한 서비스를 위하여 서비스 중인 이전 AP로부터 새로운 AP에게 컨텍스트 데이터를 전달하는 IAPP 프로토콜을 제정하고 있다. IEEE 802.11f에서는 무선랜 단말의 핸드오프를 지원하는 AP를 인증하고 AP 사이의 안전한 통신을 위한 정보를 제공하는 IAPP 서버로 RADIUS 서버를 권고한다.



무선랜 보안 기술의 최종 목표는 무선보안 요소 충족과 무선 네트워크 전체를 보호하는 것이다. 이는 동일 사업자 영역에서 사용자 이동성 지원과 사업자 영역이 상이한 무선 네트워크를 안전하게 사용할 수 있는 글로벌 로밍 서비스를 포함한다.
무선 보안의 8단계는 무선 네트워크를 위한 방화벽, 침입탐지 기능 등의 유선 네트워크에서 사용되던 다양한 보안 기능을 통합하여 무선랜 사용자에게 신뢰성 있는 무선 접속을 보장할 수 있는 무선 시스템이다.
8단계 무선 시스템 보안을 위해서는 하드웨어 적으로 한계가 있는 AP에 모든 기능을 수행하게 하는 것 보다는 무선랜 컨트롤러 시스템을 적용하여 하드웨어의 한계를 극복하고 통합 보안 관리를 하는 것이 바람직한 운영 방법일 것이다.
Layer 2 장비인 Access Point는 한계를 넘기 위한 여러 진화 과정을 거쳤으며, 진화과정의 첫 번째가 단독형 AP, 두 번째가 NMS 정도의 무선랜 Appliance 기능의 시스템, 세 번째가 중앙 집중 처리 및 보안 장비인 무선랜 컨트롤러 시스템, 그리고 현재는 세 번째 시스템에서 모바일 기능을 추가하여 중앙 관리, 보안, 이동성을 보장한다.

현재 무선랜 시장에서는 무선랜 컨트롤을 중앙 집중형식으로 해야 하는지, 아니면 AP 단독으로 처리해야 하는지에 대한 작은 논쟁이 있다. 한 집단은 "중앙 집중식으로 가야한다." 다른 한 집단은 "단독 AP type에 NMS적인 부분만 지원하면 된다."라는 2가지 의견 중 개인적인 생각으로는 중앙 집중식이 더 좋다고 생각한다. 그렇게 생각하는 이유는 Access Point의 하드웨어적인 한계가 가장 큰 이유일 것이다.
AP는 IEEE 802.11 데이터를 IEEE 802.3 데이터로 Bridge 해주는 Layer 2 장비이다. 사용자나 기업에서는 무선랜을 사용하여 이동성과 보안이 완벽하길 기대하고 다양한 Device 연동이 필요하며, Wireless Voice 연동을 위한 Voice Protocol의 QoS도 필요하다.
이동성을 보면 사용자는 같은 건물 내에서의 이동은 물론이고 지방의 지사로 출장시에도 이동성을 필요로 한다. 그런데, Layer 2 장비인 AP가 Layer 3인 IP 기반의 서비스인 장비 간에 이동성을 지원하려면 첫째는 상당히 성능이 좋은 프로세스와 메모리를 사용해야 하고, 둘째는 AP의 크기가 약간 커질 것이며, 셋째는 AP들은 암호화 키 생성을 위한 AP와 사용자 간에 공유한 Master Key를 AP들 간에 공유해야하는 기능과 Layer 3 기반의 이동성을 지원하는 터널링 기능도 필요할 것이다.

AP는 얼마나 커져야 할까?
얼마나 좋은 프로세스를 사용해야 할까?
그리고 그렇게 많은 기능을 하려면 기본적인 기능에 문제가 되지 않을까?
이런 여러 가지의 의문점이 생긴다. 현재 상용되고 있는 무선 컨트롤러 시스템은 이런 AP를 가볍게 하였다. AP는 RF(Radio Frequency)의 기본 기능만 하고, 모든 무겁고 힘겨운 기능들을 컨트롤러로 넘긴다.



무선랜 기술의 방향과 미래

IEEE 802.16e의 표준인 Wibro가 시장에 나올 때 이런 얘기가 있었다. Wibro가 나오면 무선랜 시장은 없어질 것이다. 하지만, 현재 무선 시장은 여러 가지 방식이 Convergence 되고 있다.

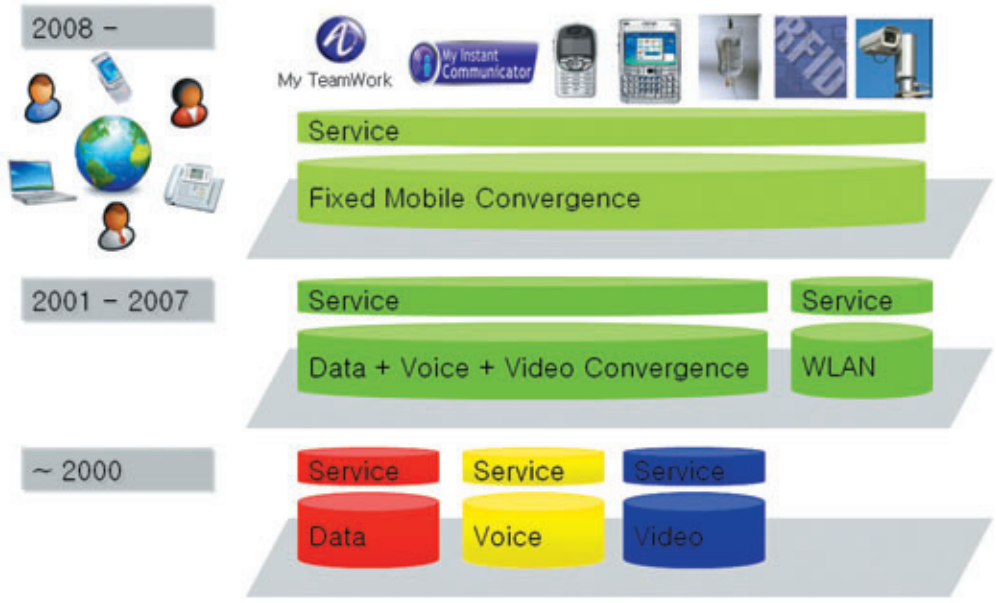
이동통신의 2G, 3G, 앞으로의 4G와 Wibro와 WiMax, Wi-Fi 등이 공존하고 있으며, 모든 통신 방식을 지원하는 One-Chip 개발과 각각의 칩을 따로 생산하는 방식으로 진행되고 있다.

무선의 명칭도 PAN(Personal Area Network) – Bluetooth, LAN(Local Area Network) – 802.11 무선랜, MAN(Metropolitan Area Network) – 802.16 WiBro or WiMax, WAN(Wide Area Network) – GSM, CDMA, 2G~4G 등으로 각각의 서비스마다의 서비스 Area를 구분하고 있다. 그리고, 각각의 서비스별로 고속 무선 표준을 진행 중이며, 무선의 고속 표준은 IEEE802.11n에서 더 나아가 IEEE802.11ac와 IEEE802.11ad 두 개의 TG가 속도 1Gbps 이상의 표준을 연구하고 있다.

[무선 네트워크의 유형별 특징]

	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11	802.16	GSM, GPRS, CDMA, 2.5-4G
Speed	1Mbps 이하 또는 그 이상	11~300+Mbps (450+Mbps)	11~100+Mbps	10~7.2+Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	PDAs, Mobile Phones, Cellular access

무선랜 기술의 활용



무선랜을 통하여 아이들은 게임기의 P2P 게임을 즐기고, 무선랜이 탑재된 PMP에 음악, 영화 , 영어수업 등을 전송받아 시청하고, 사무실 내에서는 VoIP를 무선으로 활용하고, 사무실 외부에서는 이동통신망을 사용하는 FMC(Fixed Mobile Convergence)를 활용하고, 책상에서 인터넷 선과 전원 선이 사라질 것이며, 창고나 공장에서는 물류 및 물자를 무선으로 생산 관리한다. 예를 들어, LCD를 생산하는 공장에서는 LCD 판넬을 이동할 때 무선랜과 같은 주파수 대역을 활용하여 무선으로 자동 조정하여 사용 중이다.

무선랜의 발전 및 활용은 네트워크와 통신, 네트워크와 방송 등 그 외 여러 가지의 통합과 맞물려 더욱 많이 발전하고 활용도가 높아질 것이다. 그러므로 우리는 더 나아질 모바일 환경을 잘 활용하여 조금 더 편리한 생활을 하게 되는 것이다.