



IEEE 802.11&WLAN

Ing. Daniele Tarchi
email: tarchi@lart.det.unifi.it
<http://lart.det.unifi.it>



Evoluzione LAN → WLAN

- 1990: IEEE 802.11: accesso condiviso CSMA/CA, fino a 2 Mbit/s
- IEEE 802.11b: fino a 11 Mbit/s - WiFi
- IEEE 802.11a: fino a 54 Mbit/s
- Minore complessità di implementazione
- Secondo Analysys Consulting (Sept 02): 1 Mbyte su WLAN: 0.3 €cent, su GPRS: fino a 38 €cent.
- Creazione di "ambienti" interconnessi per accesso ai servizi
- Evoluzione dei terminali PDA, con schede WLAN

IEEE 802.11

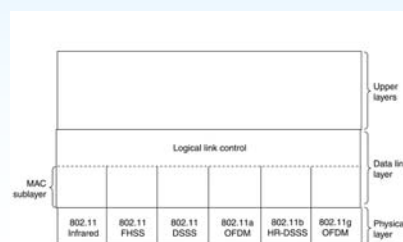


- IEEE 802.11, più noto come Wi-Fi, denota un insieme di standard per WLAN sviluppati dal WG 11 del comitato IEEE802. Il termine 802.11x è anche usato per identificare questo insieme di standard e non deve essere confuso con uno dei suoi elementi. Il termine IEEE 802.11 è usato anche per riferirsi alla versione originale, detta anche legacy 802.11.
- La famiglia 802.11 include 6 tipi di modulazioni che usano lo stesso protocollo MAC. Le più popolari tecniche sono quelle definite dagli amendments a, b, g. La sicurezza è definita dall'amendment i, mentre l'n definisce nuove tecniche per aumentare il throughput. Gli altri standard della famiglia (corrispondenti alle altre lettere) sono estensioni o correzioni ai precedenti standard.
- 802.11b and 802.11g standards lavorano sulla banda dei 2.4 GHz. A causa di questa scelta tali apparati possono spesso interferire con forni a microonde, telefoni cordless, apparecchi bluetooth. Lo standard 802.11a utilizza la banda dei 5 GHz, ed è pertanto non affetta dai prodotti che operano sulla banda dei 2.4 GHz.

IEEE 802.11



- Primo standard IEEE 802.11 pubblicato nel 1997
- Nuova versione rilasciata nel 1999, riconosciuta anche da ANSI e ISO
- Definisce livello MAC e livello fisico
- Capacità trasmissive fino a 2 Mbit/s



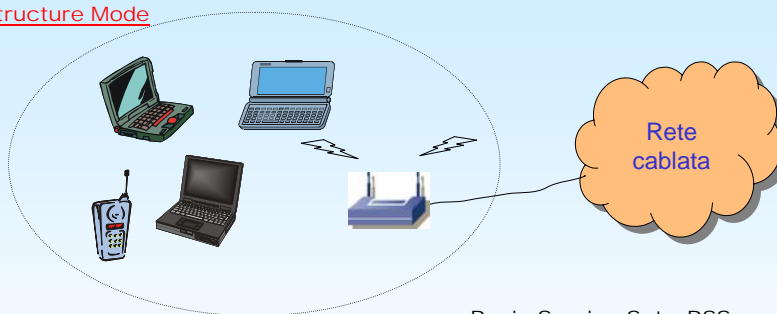
IEEE 802.11

- La versione originale dello standard fu rilasciata nel 1997, e specifica due rate pari a 1 e 2 Mbit/s via collegamenti infrarossi o onde radio sulla banda ISM a 2.4 GHz. La modalità IR rimane parte dello standard ma non è mai stata utilizzata.
- La tecnologia di accesso è la cosiddetta Carrier Sense Multiple Access con Collision Avoidance (CSMA/CA). Una parte significativa del data rate è sacrificata dal meccanismo CSMA/CA per migliorare l'affidabilità del collegamento sotto diverse condizioni.
- Un punto debole dello standard originario era dovuta al fatto che, essendo molti punti lasciati aperti, spesso l'interoperabilità non funzionava perfettamente.
- Le specifiche 802.11 sono state rapidamente soppiantate dall'802.11b, tant'è che la rapida evoluzione di tale tecnologia è avvenuta solo dopo lo sviluppo di 802.11b.



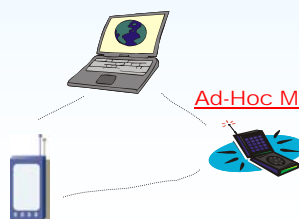
IEEE 802.11: Topologia

Infrastructure Mode



Basic Service Set – BSS:
insieme di stazioni controllate
dalla stessa Coordination Function

Ad-Hoc Mode



IEEE 802.11 Physical Layer



- Livello fisico: diviso in tre sottolivelli:
 - Physical Layer Convergence Protocol (PLCP): adatta il livello MAC al particolare livello fisico (PMD)
 - Physical Medium Dependent: descrive come inviare e ricevere informazioni sul mezzo wireless
 - Layer Management
- Tre tipi di livello fisico supportati:
 - Direct Sequence Spread Spectrum (DS-SS)
 - Frequency Hopping Spread Spectrum (FH-SS)
 - Infrarosso (900 nm, PPM, no Line of Sight, max 20m, non attraversa le strutture murarie)
- Operano sui 2.4 Ghz: frequenze ISM - Industrial Scientific Medical Band, unlicensed

DS-SS PHY



- Frequenza operativa: 2.4 GHz
- DBPSK: 1 Mbit/s
- DQPSK: 2 Mbit/s
- SS code: 11chip/bit
- 11 MHz di banda occupata dopo lo spreading
- $P_{max} =$
 - 1W USA,
 - 100 mW EU,
- $P_{min} = 10\text{mW}$

FH-SS PHY

- L'SS code viene usato per scegliere su quali frequenze "saltare" (hopping).
- Hopping su 79 canali di 1 MHz ciascuno
- Nel complesso si ottiene un segnale che spazia in un ampio range di frequenze, da cui "Spread Spectrum"
- Usa modulazione Gaussian Frequency Shift Keying - GFSK, a 1 e 2 Mbit/s



IEEE 802.11 MAC Layer

Servizi Real-Time

Servizi Dati, Non Real-Time

MAC Layer

Point Coordination
Function (PCF)

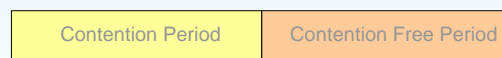
Distributed Coordination
Function (DCF)

Physical Layer



CP e CFP

- La DCF gestisce il Contention Period (CP)
- La PCF gestisce il Contention Free Period (CFP)
- CP e CFP formano un superframe
- Durante CFP l'AP fa polling sulle WSTA e decide chi far parlare
- Durante CP c'è contesa fra le WSTA senza controllo centralizzato



Superframe (durata variabile)

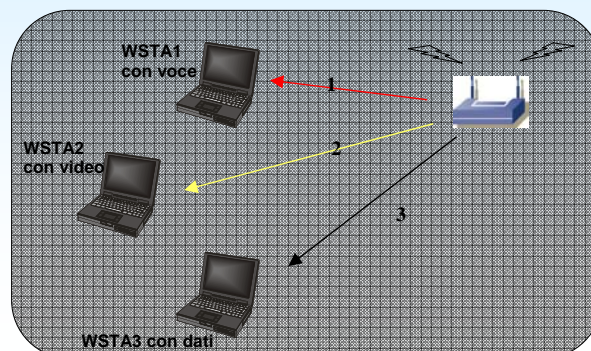
Qui non c'è controllo centrale, accesso regolato su contesa distribuita fra le stazioni

Qui c'è controllo centrale dell'AP, che decide quali stazioni far parlare e quando (poll)



IEEE 802.11 PCF

- L'accesso al canale wireless è regolato dall'Access Point
- L'AP decide chi e quando deve trasmettere e in base a questo "chiama" le stazioni relative (polling)
- La PCF viene utilizzata per supportare servizi che hanno specifici requisiti in termini di ritardo massimo sopportabile (voce, video)



IEEE 802.11 DCF

- Distributed Coordination Function:
 - L'accesso al mezzo wireless è coordinato in modo distribuito.
 - Non c'è un controllo centrale dell'accesso al canale.
 - Sono possibili collisioni
 - Per ridurre/evitare collisioni ciascuna stazione usa un tempo casuale durante il quale aspetta a trasmettere (backoff)

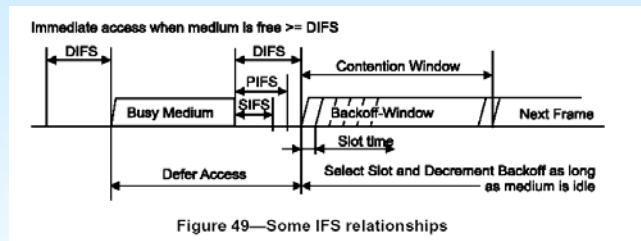


CSMA/CD vs CSMA/CA

- Nelle LAN il Carrier Sensing Multiple Access with Collision Detection (CSMA/CD) si basa su due fondamentali assunzioni:
 1. In una LAN tutti possono sentire tutti
 2. Un transceiver può trasmettere e ricevere allo stesso tempo
- Sulle WLAN le due assunzioni non sono valide
- CSMA with Collision Avoidance (CSMA/CA)
 - anziché rilevarla si cerca di evitare la collisione



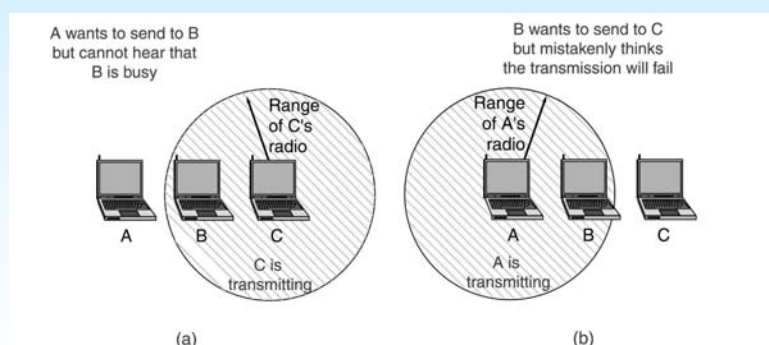
Processo di Backoff



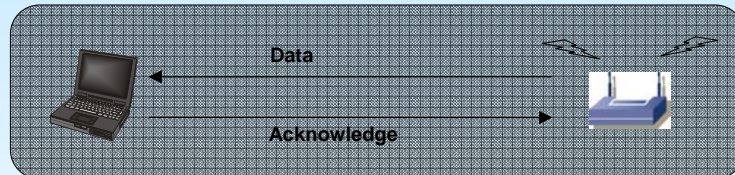
- SIFS = Short Inter Frame Space
- PIFS = PCF Inter Frame Space
- DIFS = DCF Inter Frame Space

- Backoff Time = $\text{random}(0, \text{Contention Window})$
- Contention Window $\in [CW_{\min}, CW_{\max}]$

Hidden and Exposed Nodes

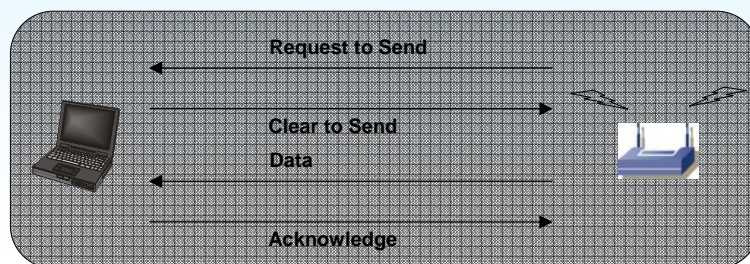


RTS/CTS



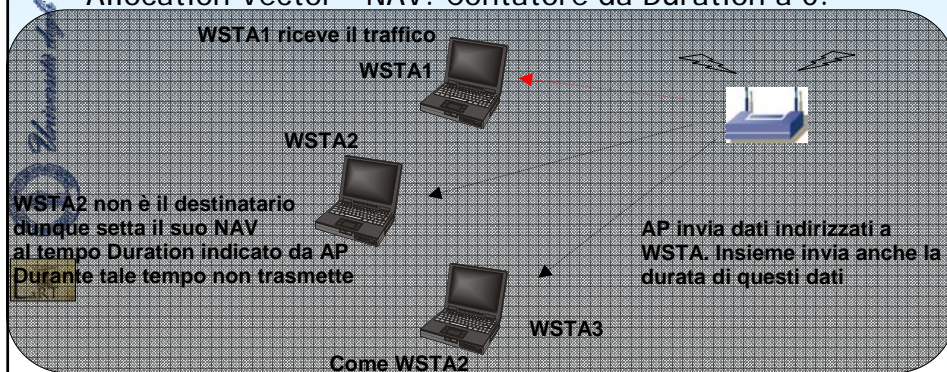
RTS: Request to Send: "Chiedo il permesso di trasmettere"

CTS: Clear to Send: "Permesso accordato! Puoi trasmettere!"

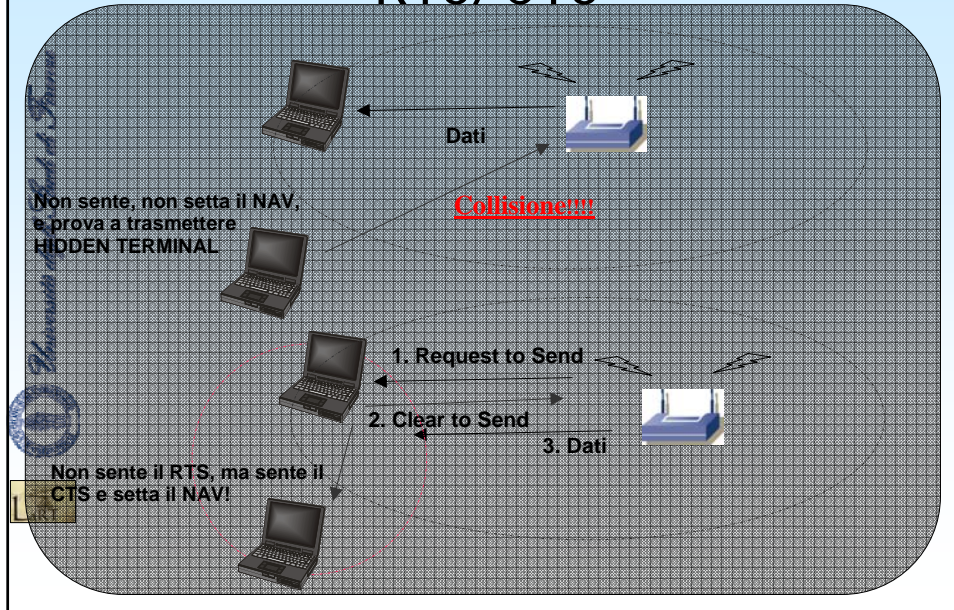


NAV

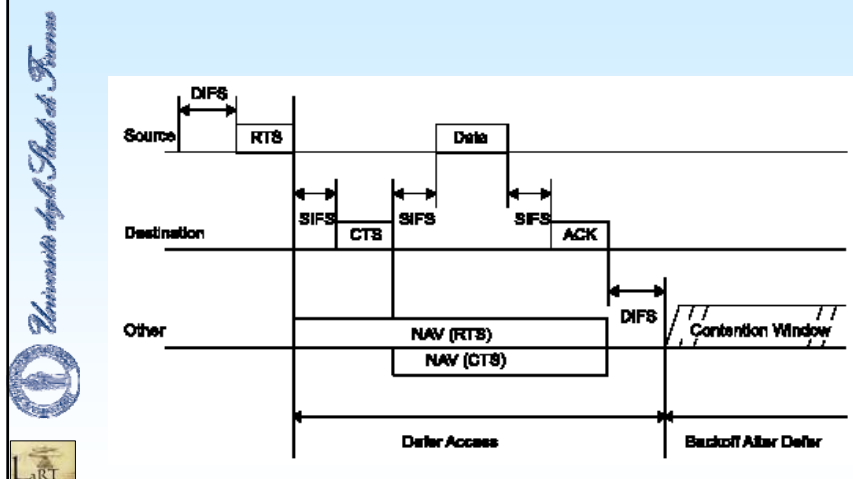
- Carrier Sensing Multiple Access with Collision Avoidance CSMA/CA
- Carrier Sensing a livello fisico : Clear Channel Assessment (CCA): con transceiver su RX si "cerca" la presenza di segnale sul canale wireless
- Carrier Sensing virtuale a livello MAC: Network Allocation Vector - NAV. Contatore da Duration a 0.



RTS/CTS



Network Allocation Vector - NAV



IEEE 802.11x



- 802.11: MAC e PHY, 2.4GHz, max 2 Mbit/s
 - 802.11a: PHY, OFDM, 5 GHz, max 54 Mbit/s
 - 802.11b: PHY, DS-SS, 2.4 GHz, max 11 Mbit/s
 - 802.11e: MAC: QoS
 - 802.11g: PHY, OFDM, 2.4 GHz, max 54 Mbit/s
 - 802.11i: sicurezza su WLAN
 - 802.11k: Radio resource measurement enhancements
 - 802.11n: Higher throughput improvements
 - 802.11p: WAVE - Wireless Access for the Vehicular Environment
 - 802.11s: ESS Mesh Networking

IEEE 802.11b



- La revisione 802.11b è stata ratificata nel 1999.
- 802.11b ha un data rate massimo di 11Mbit/s e usa CSMA/CA, che limita il data rate effettivo a circa 5.9 Mbit/s per connessioni TCP e 7.1 Mbit/s per connessioni UDP.
- 802.11b è solitamente usato in configurazioni point-to-multipoint, dove un access point comunica con un'antenna omni-direzionale con uno o più client disposti nelle vicinanze.
- Tipicamente il raggio di copertura indoor è 30 m a 11 Mbit/s e 90 m a 1 Mbit/s. Con antenne esterne a alto guadagno in configurazioni fisse punto-punto è possibile raggiungere anche estensioni fino a 8 Km circa. In questi casi si deve porre molta attenzione ai limiti di legge in termini di potenza emessa.
- Gli adattatori 802.11b possono operare a 11 Mbit/s, ma possono diminuire il rate a 5.5, 2, e 1 Mbit/s (Adaptive Rate Selection), se la qualità del segnale diventa un problema.
- Sono state fatte estensioni proprietarie al protocollo 802.11 per poter aumentare il rate a 22, 33, e 44 Mbit/s.
- Molte compagnie hanno annunciato una versione estesa chiamata "802.11b+", evitata dall'introduzione di 802.11g, che consente trasmissioni fino a 54 Mbit/s ed è compatibile con 802.11b.

IEEE 802.11b PHY

- Standard IEEE 802.11b: 1999
- Allegato all'IEEE 802.11, lo complementa, non lo sostituisce!!
- Specifica solo il Physical Layer
- Suddivide anch'esso PLCP e PMD
- Opera sempre nella frequenza 2.4 - 2.4835 Ghz (EU) ISM
- Mantiene sempre 1 Mbit/s (DBPSK) e 2 Mbit/s (DQPSK) di 802.11 PHY
- Utilizza DS-SS/CCK (Complementary Code Keying) + DQPSK per Data rates a 5.5 e 11 Mbit/s
- DS-SS code: 11 chip per bit, CCK code = 8 chip per bit
- Banda occupata dopo lo spreading = 11 Mhz, (come .11 PHY)
- Pmax= 1 W (USA), 100 mW (EU)



Wi-Fi Alliance

- Wireless Fidelity, marchio detenuto dalla Wireless Ethernet Compatibility Alliance - WECA
- Creata nel 1999
- Organizzazione "no-profit": 3com, Apple, AT&T, Cisco, Intel, HP, IBM, Microsoft, Nokia, Ericsson
- Nata per la promozione della "libertà" di accesso alla Rete con WLAN
- Un dispositivo, anche se conforme alle specifiche 802.11x, non può utilizzare il logo ufficiale Wi-Fi a meno di aver superato le procedure di certificazione stabilite dal consorzio Wi-Fi Alliance; pertanto la presenza del marchio Wi-Fi su di un dispositivo dovrebbe garantirne l'interoperabilità con gli altri dispositivi certificati, anche se prodotti da aziende differenti.



IEEE 802.11a



- La revisione 802.11a è stata ratificata nel 1999.
- Lo standard 802.11a usa lo stesso protocollo di 802.11, opera nella banda ISM a 5 GHz band, e usa la tecnica orthogonal frequency-division multiplexing (OFDM) con un massimo data rate di 54 Mbit/s, che permette un rate effettivo di circa 20 Mbit/s. Il data rate può essere ridotto a 48, 36, 24, 18, 12, 9 o 6 Mbit/s.
- Poiché la banda a 2.4 GHz è molto congestionata, l'utilizzo della banda a 5 GHz permette di avere meno interferenza. L'utilizzo di frequenze più alte limita però l'utilizzo solo in caso di Line of Sight e con raggi di copertura minori
- Il suo utilizzo è rimasto confinato a USA e Giappone, poiché in Europa non è stato ancora ratificata la possibilità di usare la banda 5 GHz
- I prodotti 802.11a hanno iniziato ad essere prodotti nel 2001, in ritardo rispetto a 802.11b a causa di componentistica più sofisticata da essere utilizzata a 5 GHz.
- Lo sviluppo in questo momento è orientato su dispositivi dual mode 802.11a e 802.11b (o addirittura tri-mode con 802.11g) poiché non è possibile prescindere da 802.11b che è di gran lunga la tecnologia più utilizzata.

IEEE 802.11a PHY



- Standard IEEE 802.11a: 1999, allegato a 802.11
- Descrive solo Physical Layer
- Usa OFDM al livello fisico, alti data rates, da 6 a 54 Mbit/s
- Durata di un simbolo OFDM=4 μ s
- $P_{tx,max} \approx 30$ mW in Europa
- Frequenza operativa:
 - 5.15-5.35 GHz e 5.725-5.825 GHz in US, UNII - Unlicensed National Information Infrastructure band
 - in Europa 5.15-5.35, ma esistono ancora notevoli limitazioni all'utilizzo (802.11h)

IEEE 802.11g



- Nel giugno 2003 è stata ratificata una nuova modalità chiamata 802.11g.
- Opera nella banda a 2.4 GHz (come 802.11b) ma con un rate massimo di 54 Mbit/s, che consente un rate effettivo di 24.7 Mbit/s come 802.11a.
- L'hardware 802.11g consente di co-operare con l'hardware 802.11b, consentendo di lavorare meglio che non nell'802.11a, soprattutto a causa della banda di frequenza di lavoro
- I prodotti 802.11g sono usciti in commercio prima dell'effettiva standardizzazione, soprattutto in dispositivi tri-mode. Il maggior difetto è posto nel sovraffollamento della banda che oltre a dispositivi 802.11b è usata anche da forni a microonde, terminali Bluetooth e cordless

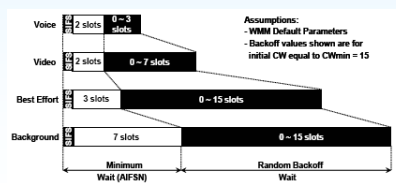
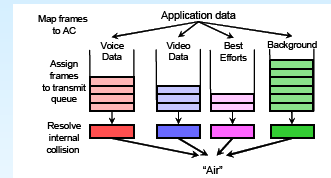
IEEE 802.11g



- IEEE 802.11g: allegato a 802.11
- Dà specifiche sul solo Physical Layer
- High-speed extension del PHY a 2.4 GHz ISM
- Pensato per risolvere problemi di progettazione ai 5 GHz
- Utilizza OFDM come 802.11a
- Data rates: 1, 2, 6, ..., 48, 54 Mbit/s
- RTS/CTS per evitare collisioni da coesistenza con 802.11b
- Slot time = 20 μ s o 9 μ s se solo 802.11g
- Extended Rate PHY - ERP: PHY che lavora su 2.4 GHz ed è un'estensione del PHY DS-SS in 802.11

IEEE 802.11e

- IEEE 802.11e è stato approvato alla fine del 2005 come lo standard che definisce un insieme di miglioramenti alla Quality of Service per applicazioni WiFi. Lo standard è considerato particolarmente strategico per applicazioni delay-sensitive, come Voice over Wireless IP e Streaming Multimedia. Il protocollo migliora il livello MAC di IEEE 802.11.
- L'802.11e migliora DCF e PCF, attraverso una nuova funzione di coordinamento: la Hybrid Coordination Function (HCF). All'interno di HCF, ci sono due metodi di accesso al canale, simili a quelli definiti nell'802.11 legacy: HCF Controlled Channel Access (HCCA) e Enhanced DCF Channel Access (EDCA). Ambedue EDCA e HCCA definiscono Traffic Classes (TC). Per esempio le email possono essere assegnate a una classe a bassa priorità e Voice over Wireless IP (VoWiP) possono essere assegnate a una classe ad alta priorità.



EDCA

- Con EDCA, il traffico ad alta priorità ha una più alta probabilità di essere spedito che non il traffico a bassa priorità: una stazione ad alta priorità aspetta un po' meno in media che una stazione a bassa priorità.
- In aggiunta ogni livello di priorità ha una Transmit Opportunity (TXOP) assegnata. Una TXOP è un intervallo di tempo limitato durante il quale una stazione può inviare più frame possibile (fino a che la durata della trasmissione non si estende oltre la massima durata del TXOP).
- Se un frame è troppo grande per essere trasmesso in un singolo TXOP, può essere frammentato. L'uso di TXOP riduce il problema delle stazioni a basso rate che si prendevano un quantità di tempo molto grande nel legacy 802.11 DCF MAC.
- Gli AP certificati Wi-Fi Multimedia (WMM) devono avere il supporto per EDCA and TXOP. Tutti gli altri miglioramenti sono opzionali.

HCCA



- L'HCCA lavora in maniera simile al PCF: l'intervallo fra due periodi di beacon è diviso in due periodi, il CFP e il CP. Durante il CFP, l'Hybrid Coordinator (HC) - che è anche l'AP - controlla l'accesso al mezzo. Durante il CP, tutte le stazioni funzionano in EDCA.
- La maggior differenza con il PCF è la definizione delle Traffic Classes (TC). Inoltre l'HC può coordinare il traffico nella maniera preferita (non solo round-robin). Inoltre, le stazioni informano sulla lunghezza delle proprie code per ogni Traffic Class (TC). L'HC può usare questa informazione per dare priorità ad una stazione piuttosto che a un'altra. Un'altra differenza è che le stazioni sono associate a un TXOP: possono inviare più pacchetti per un certo intervallo di tempo selezionato dall'HC. Durante la CP, l'HC permette alle stazioni di inviare dati inviando un frame di CF-Poll.
- HCCA è generalmente considerato la più avanzata e complessa funzione di coordinamento. Con HCCA, la QoS può essere configurata con grande precisione. Le QSTA hanno la possibilità di richiedere specifici parametri di trasmissione (rate, jitter, ecc.) che devono essere rispettati per certe applicazioni come VoIP e video streaming per lavorare più efficacemente su reti Wi-Fi.
- Il supporto per HCCA non è obbligatorio in 802.11e. Solo pochi APs prevedono di implementare HCCA.

Wireless Multimedia Extensions (WME)



- Wireless Multimedia Extensions (WME), noto anche come Wi-Fi Multimedia (WMM) è una certificazione della Wi-Fi Alliance basata sullo standard IEEE 802.11e. WMM permette di avere il traffico diviso in 4 AC (Access Categories) - voce, video, best effort, e background. Comunque non prevede un throughput garantito. E' molto interessante per applicazioni semplici come il Wi-Fi Voice over IP (VoIP).
- Power Save Certification
 - La Wi-Fi Alliance ha aggiunto la Power Save Certification alle specifiche WMM. Power Save usa meccanismi dall'802.11e e 802.11 per ridurre il consumo di potenza o comunque regolarlo.
 - La certificazione è pensata soprattutto per prodotti specifici come cordless o dispositivi portatili.

802.11n

- Nel gennaio 2004 è stato annunciato la formazione della Task Group n per sviluppare un nuovo miglioramento allo standard 802.11.
- L'obiettivo è di raggiungere un data rate teorico di 540 Mbit/s.
- Dal punto di vista tecnico le migliorie più grandi sono apportate dall'utilizzo delle cosiddette tecniche MIMO (multiple-input multiple-output) che consentono l'utilizzo congiunto e cooperativo di più antenne in trasmissione e ricezione.
- Il processo di standardizzazione è previsto essere completato nella seconda metà del 2006, per essere approvato non prima del luglio 2007.



ETSI HIPERLAN

- Standard ETSI 1996 - High PERFORMANCE LAN
- BRAN (Broadband Radio Access Networks)
- ETSI ha definito 4 tipi di HIPERLAN:
 - type 1 e type 2 (WLAN su 5.2 GHz)
 - HIPERACCESS (WLL su 5.2 GHz)
 - HIPERLINK (p2p su 17 GHz)
- Multihop routing al livello MAC
- Schema di accesso: simile a CSMA ma con segnalazione attiva
- Il MAC usa accesso con priorità, solo i pacchetti con maggiore priorità vengono scelti per la trasmissione dedicata, gli altri devono seguire fase di contesa



La famiglia HIPERLAN

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	



HIPERLAN/1

- Lo sviluppo della prima versione di HIPERLAN, chiamata HIPERLAN/1, iniziò nel 1991, quando lo sviluppo di 802.11 era già in corso. L'obiettivo di HIPERLAN era ottenere una data rate maggiore di 802.11; lo standard fu approvato nel 1996.
- Lo standard copre livello fisico e MAC, analogamente a 802.11, con l'aggiunta di un nuovo sottolivello, Channel Access and Control (CAC), che si occupa dell'accesso delle nuove richieste al canale, dipendentemente da utilizzo del canale e priorità delle richieste.



HIPERLAN/1



- Il livello CAC opera grazie ad un diverso protocollo di livello MAC detto Elimination-Yield Non-Preemptive Multiple Access (EY-NPMA), che si occupa di codificare ogni accesso in un livello di priorità. Questo permette di minimizzare le collisioni e consentire la trasmissione efficiente di flussi multimediali tramite la gestione delle priorità. A livello fisico sono utilizzate le modulazione FSK e GMSK:
- Caratteristiche:
 - range 50 m
 - Bassa mobilità (1.4 m/s)
 - Supporto per traffico sincrono e asincrono
 - Audio a 32 kbit/s, con 10 ns di latenza
 - video a 2 Mbit/s, con 100 ns di latenza
 - Dati a 10 Mbit/s
- HIPERLAN non interferisce con gli apparati elettrici ed elettronici a 2.4GHz.



HIPERLAN/2



- Le specifiche funzionali di HIPERLAN/2 furono terminate nel febbraio 2000. La versione 2 è stata pensata per un collegamento veloce per molte tipologie di rete, dai backbone UMTS alle reti ATM e IP, pur rimanendo la possibilità di essere utilizzata privatamente come HIPERLAN/1. HIPERLAN/2 lavora sulla banda a 5 GHz e fino a Mbit/s.
- I servizi base sono dati, audio e video, con un' enfasi particolare alla gestione della qualità di servizio (QoS - Quality of Service).
- Lo standard copre il vello fisico, Data Link Control and Convergence. Quest'ultimo si occupa delle funzionalità service dependent fra DLC e livello rete. Il Convergence sublayer può essere usato anche sopra il livello fisico per connettere reti IP, ATM o UMTS networks. Questo rende HIPERLAN/2 molto attraente per l'interconnessione di reti diverse.
- A livello fisico utilizza BPSK, QPSK, 16QAM o 64QAM.

