Reti wireless: IEEE 802

Fulvio Babich (babich@units.it)

DIA – Università di Trieste

Generalità

- IEEE 802 LAN/MAN Standards Committee (LMSC) è una commissione dell'IEEE preposta a sviluppare standard per le reti locali (LAN) e per le reti metropolitane (MAN).

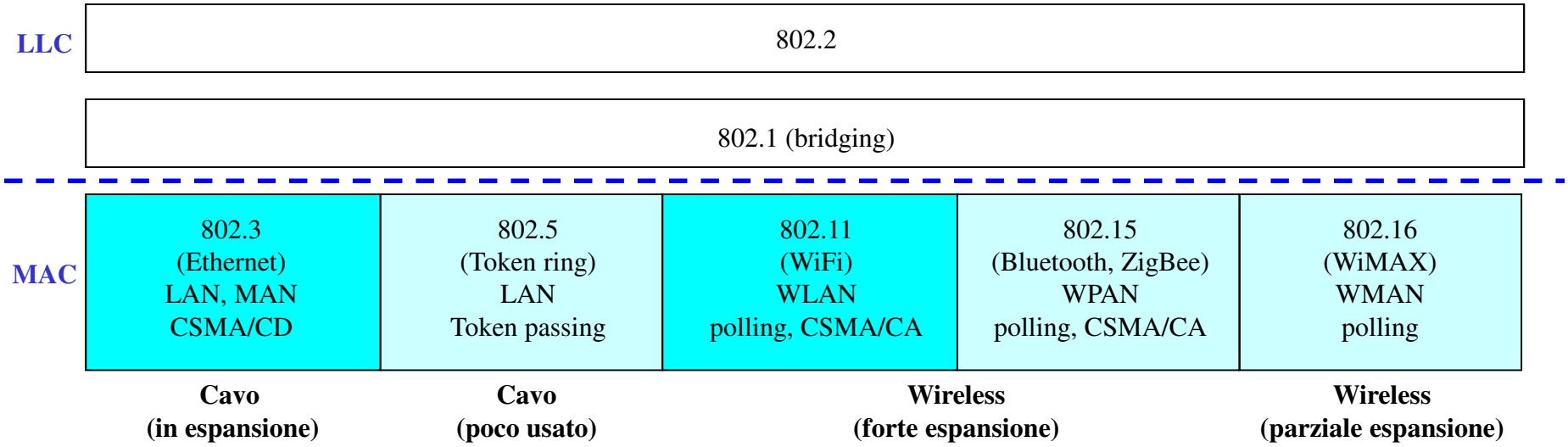
- I protocolli e i servizi specificati negli standard 802 si situano nei due livelli più bassi (fisico e Data Link) nel modello di riferimento a sette strati espresso dallo standard ISO-OSI. I protocolli 802 suddividono lo strato OSI DLL in due sottostrati, chiamati Logical link control (LLC) e Media Access Control (MAC), in modo tale che gli strati 802 possono essere indicati in questo modo:

  - Data link layer
  - Sottostrato LLC
  - Sottostrato MAC

  - Strato fisico (Phy)

Progetto IEEE 802

- Obiettivo: sviluppare una serie di standard per i livelli OSI 1 e 2 delle reti PAN, LAN e MAN con pacchetti di lunghezza variabile.
- Livello 2 suddiviso in due sottolivelli:
  - Logical Link Control (LLC): sottolivello comune indipendente dal mezzo trasmissivo (IEEE 802.2).
  - Medium Access Control (MAC): standard di accesso diversi in base al mezzo trasmissivo ed al tipo di rete (IEEE 802.3-IEEE 802.24).
- Alcuni standard sono continuamente aggiornati ed estesi (nuovi task group), altri sono stati abbandonati.



Radio - Tecnologie

- Tabella comparativa

	802.11 (WiFi)	802.15 (Bluetooth-802.15.1, MAC/PHY ZigBee-802.15.4)	802.16 (WiMAX)
Banda	2.4, 5.8, 60 GHz	2.4 GHz	2-66 GHz
Bit rate massima	7 Gbit/s	24 Mbit/s (802.15.1) 250 kbit/s (802.15.4)	70 Mbit/s
Raggio di copertura	100 m	10 m	50 km
Tipologia di rete	WLAN	WPAN (802.15.1) reti di sensori (802.15.4)	WMAN
Traffico	multimediale	multimediale (802.15.1) limitato (802.15.4)	multimediale
Accesso	centralizzato e distribuito	centralizzato (802.15.1) centralizzato e distribuito (802.15.4)	centralizzato

802.11 - Tabella comparativa

Standard	802.11	802.11a	802.11b	802.11g	802.11n	802.11ac
Frequenza		5 GHz	2.4 GHz	2.4 GHz	2.4 GHz 5 GHz	5 GHz
Velocità massima	2 Mbit/s	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s	6.9 Gbit/s
Tecnica	FH/DSSS	OFDM	DSSS	OFDM	OFDM	OFDM
Banda	22 MHz	20 MHz	22 MHz	20 MHz	40 MHz	160 MHz
Modul.	DQPSK	64 QAM	DQPSK	64 QAM	64 QAM	256 QAM
Note	Barker Legacy		Barker CCK		MIMO	MIMO Beamform.

Wireless LAN 802.11

- Una W-LAN è una rete che fornisce servizi di comunicazione agli utenti garantendo la mobilità delle stazioni in modo trasparente agli strati più alti dello stack di protocolli.
- Il componente di base della WLAN 802.11 è la **stazione**
  - È una qualsiasi unità che contiene le funzionalità del protocollo 802.11
- Le stazioni 802.11 possono essere
  - mobili
  - stazionarie (Access Point)
- Un insieme di stazioni costituisce un **Basic Service Set** (BSS)
- Esistono due topologie base:
  - Independent Basic Service Set (IBSS) o Ad Hoc Network
  - Infrastructure Basic Service Set o Infrastructure Mode

IEEE 802.11

- Vantaggi
  - Supporto alla mobilità dei nodi e degli utenti.
  - Bit rate superiori rispetto alle reti cellulari, ma inferiori rispetto alle LAN cablate.
  - Bassi costi di installazione e di riposizionamento dei nodi (assenza di cavi).

- Stazioni
  - Elementi della rete. Possono essere mobili, oppure fissi (Access Point).
  - Un insieme di stazioni costituisce un Basic Service Set (BSS).

- Tipologie di reti supportate
  - *Mobile Ad-hoc NETwork* – MANET.
  - *Vehicular Ad-hoc NETwork* – VANET.
  - *Wireless Mesh Network* – WMN.

Struttura della rete

- Independent Basic Service Set (IBSS - rete P2P o Ad-Hoc)
  - Una WLAN IBSS rende possibile collegare in modo indipendente più postazioni wireless tra loro senza nessun dispositivo centrale che funga da tramite. Modalità semplice ed economica, ma non adatta a una rete numerosa, per l'eccesso di conflitti.
- Infrastructure Basic Service Set (BSS o Infrastruttura)
  - Gestita da un Access Point centrale collegato a una rete esterno che funge da unico tramite per il traffico dei dispositivi wireless che si trovano nel suo range di copertura. Una singola WLAN BSS rappresenta una cella, chiamata Basic Service Area (BSA). Un Access Point pubblico, è detto hotspot.
- Extended Service Set (ESS)
  - Composta da due o più WLAN BSS collegate tra loro mediante un Distribution System al fine di generare un'area di copertura di maggiore, con funzione di roaming per gestire la mobilità. Le celle wireless in configurazione ESS si sovrappongano almeno del 10% per garantire questa funzionalità.

Distribution System (DS)

- Livello presente in ciascun AP che funge da dorsale della WLAN, attraverso il quale un AP comunica con un altro AP per:
  - Scambiare pacchetti destinati alle stazioni nei rispettivi BSS.
  - Trasmettere pacchetti in modalità roaming (cambio di cella dovuto alla mobilità).
  - Interagire con la rete esterna a cui la WLAN è collegata.

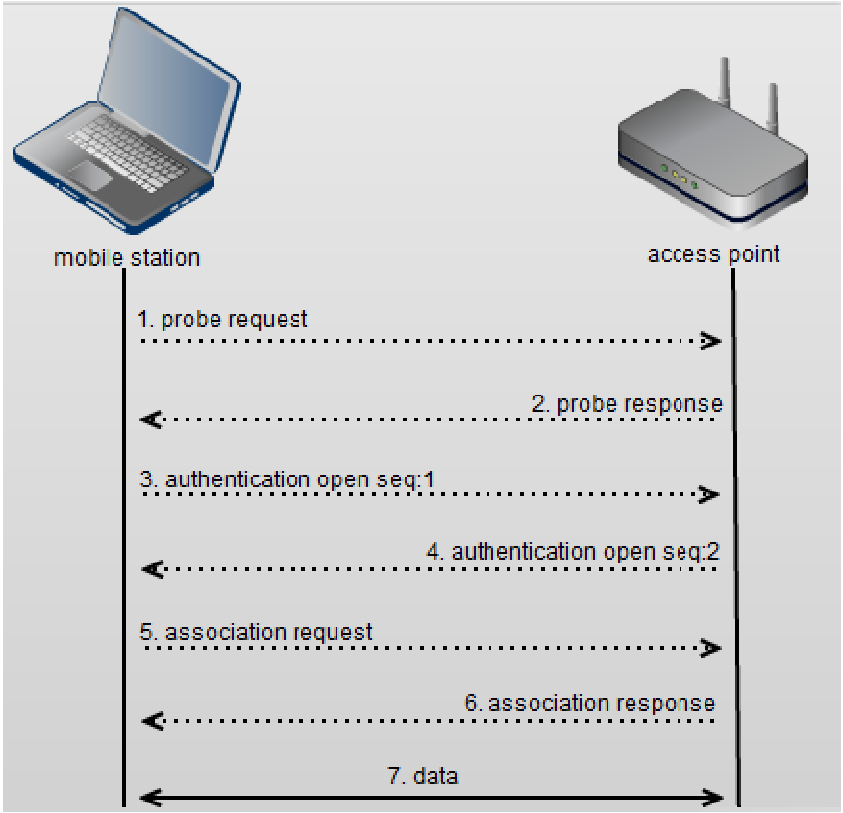
- Lo standard 802.11 lascia libertà di scelta sulla tecnologia utilizzabile per l'implementazione del DS, e stabilisce i servizi che esso deve fornire.

- 802.11f standardizza il protocollo Inter-Access Point Protocol (IAPP)
  - Registrazione degli AP in una rete
  - Scambio di informazioni tra AP quando una stazione si muove tra aree di copertura supportate da AP di diversi produttori

Servizi 802.11

- Servizi di distribuzione (forniti dall'Access Point)
  - Association: quando entra nel raggio d'azione di un AP, una stazione utilizza il servizio di associazione per informare l'AP della sua presenza e delle sue esigenze.
  - Dissociation: può avvenire sia su iniziativa dell'AP che della stazione.
  - Re-association: una stazione in movimento può trasferire il controllo da un AP ad un altro.
  - Distribution: l'AP invia i frame ricevuti verso le stazioni della propria cella (via radio) o verso gli altri AP attraverso il sistema di distribuzione.
  - Integration: gestisce la conversione di un frame 802.11 in altri formati.
- Servizi di stazione (forniti da tutte le stazioni)
  - Authentication: verifica che la stazione sia autorizzata ad usufruire del servizio di trasmissione.
  - De-authentication: quando la stazione esce dalla rete.
  - Privacy: cifratura dati trasmessi.
  - Data delivery.

Association



- Stati di connessione 802.11
  - Not authenticated
  - Authenticated but not yet associated
  - Authenticated and associated
- 1. Probe request
  - Broadcast. Versione supportata.
- 2. Probe response
  - Versione e cifratura supportata.
- 3. Authentication open
  - Numero di sequenza 1
- 4. Authentication open
  - Nr. 2; stato: Authenticated but not yet associated
- 5. Association request
  - Inviata all'AP prescelto, con le prestazioni richieste.
- 6. Association confirm: se le prestazioni sono compatibili, crea un Association ID

Re-association

- Consente ad una stazione di cambiare la sua attuale associazione con un altro AP
- È usato quando una stazione mobile esce dal BSS, perde il contatto con l'AP a cui è associata e ha bisogno di associarsi ad un nuovo AP di un altro BSS
- Tale servizio è simile a quello di associazione. Include l'informazione sull'AP precedente, per dare modo al DS di gestire la mobilità
- Il nuovo AP può contattare il precedente AP per ricevere frame in eventuale attesa per l'invio alla stazione mobile
- Combinato con l'association, è sufficiente per il supporto della BSS transition

Disassociation

- Utilizzato dalla stazione per informare l'AP che non intende più utilizzare i suoi servizi.
- Utilizzato da un AP, in caso di risorse non sufficienti o di shut-down
- Deve essere accettato
- La stazione mobile deve effettuare un Association con un altro AP per riprendere a comunicare.

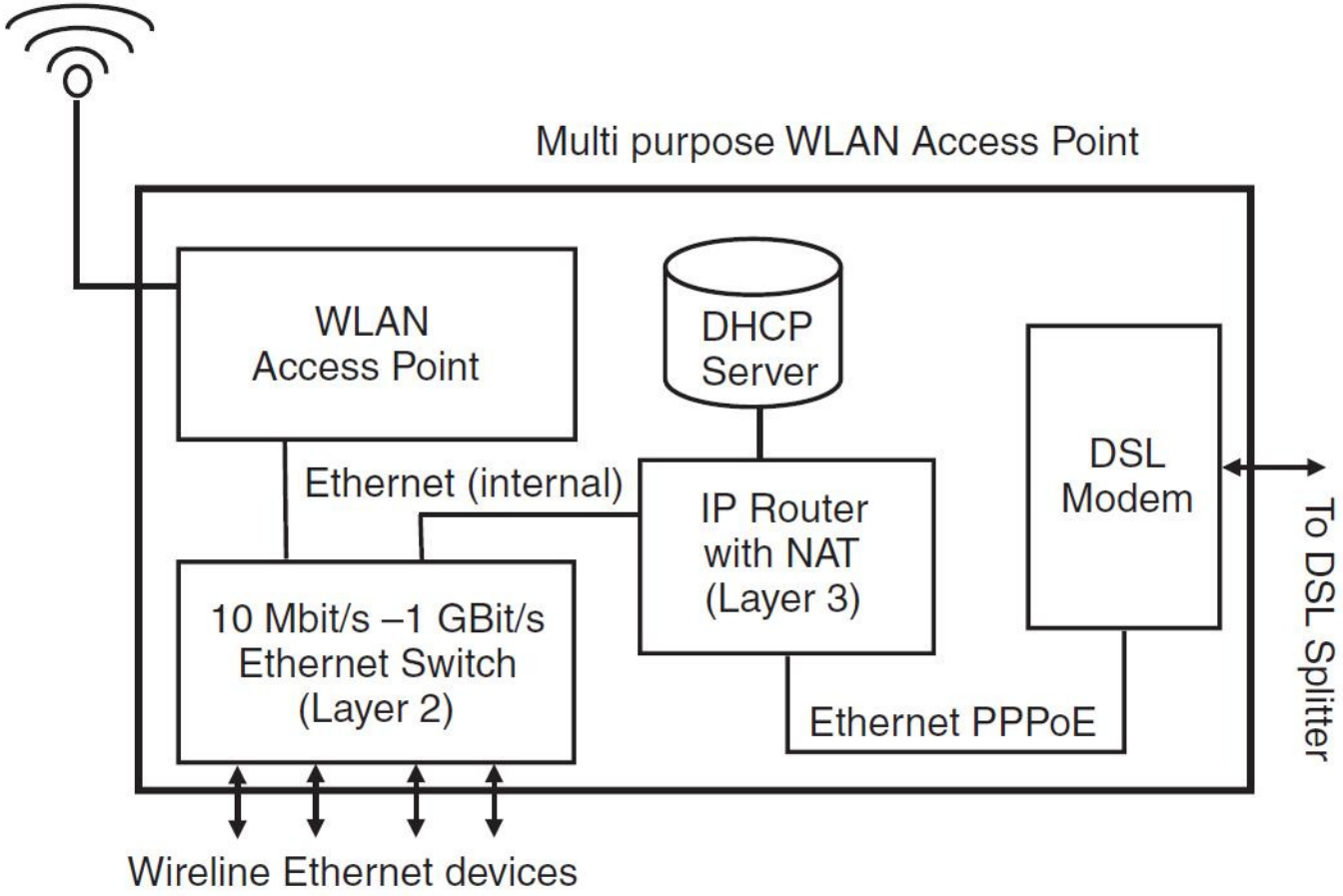
Pre-Shared Key (PSK) Authentication

- Basata su password o su chiave condivisa da stazione e AP. Ne esistono di diversi tipi.
- Wired Equivalent Privacy (WEP): non sicura. Gli hacker sono in grado di catturare la versione cifrata dell'authentication response e di derivare la chiave di cifratura.
- Wi-Fi Protected Access (WPA): due modalità di funzionamento
  - Personale: basata su chiave segreta condivisa.
  - Aziendale: utilizza un server di autenticazione.
  - Utilizza l'algoritmo di cifratura RC4 (Rivest Cipher 4), un vettore di inizializzazione di 48 bit (contro i 24 bit del WEP), e chiavi a 256 bit. La chiave viene aggiornata continuamente mediante il protocollo Temporal Key Integrity Protocol (TKIP).
- WPA 2: Sostituisce gi algoritmi RC4 e TKIP con gli algoritmi CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) e AES (Advanced Encryption Standard) per incrementare la robustezza.

802.1x Framework

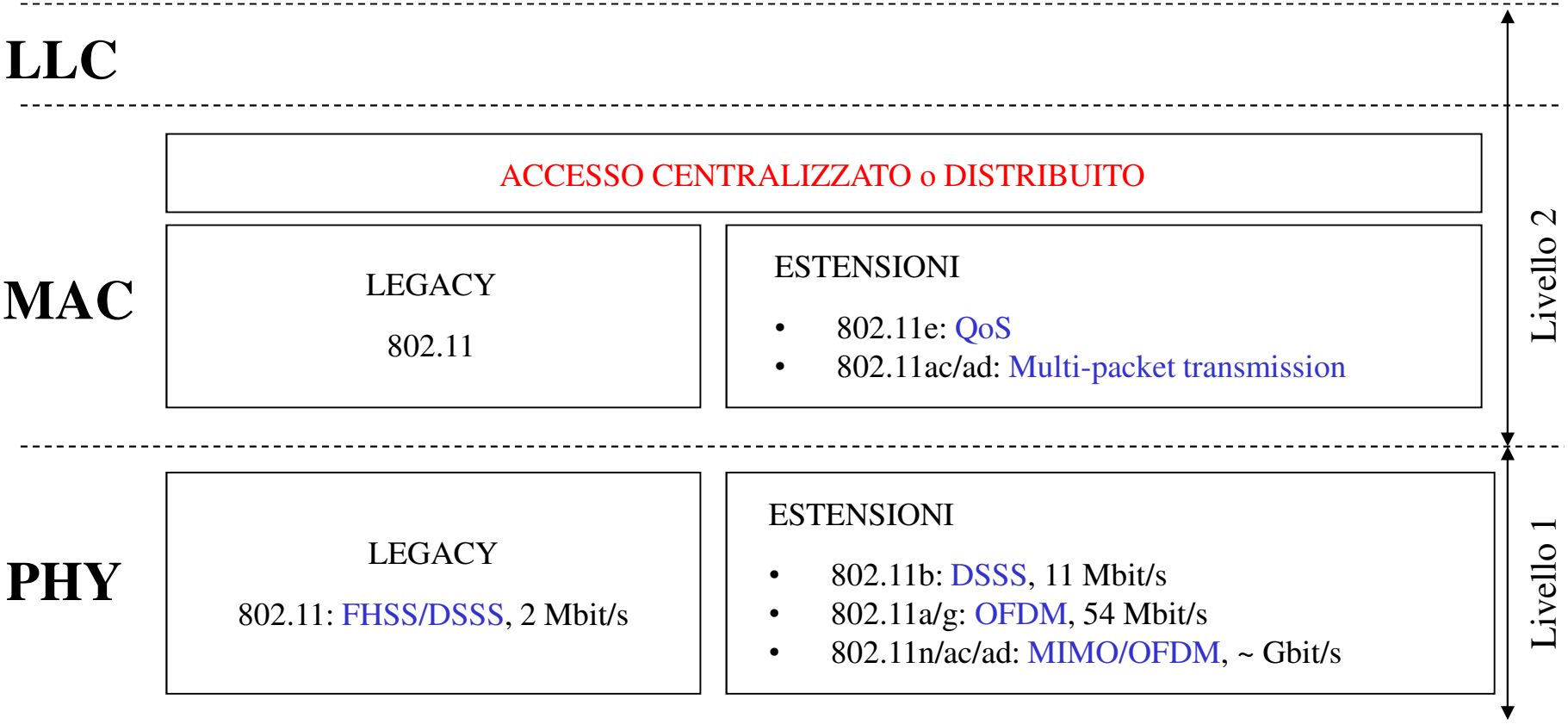
- Usato da WPA 2 Enterprise
- Si basa su EAP, (Extensible Authentication Protocol RFC 2284): denominato “EAP over LAN” o EAPOL. Coinvolge tre elementi: il supplicant, l’authenticator (un AP) e l’authentification server.
- Sequenza di autenticazione
  - Initialization. Nuovo supplicant. Solo il traffico 802.1X è consentito. Altro traffico basato su protocolli Internet (TCP e UDP) è respinto.
  - Initiation. L'authenticator trasmette periodicamente “EAP-Request Identity” frames ad uno specifico indirizzo MAC sulla rete locale. Il supplicant in ascolto invia un “EAP-Response Identity” frame, contenente un User ID. L'authenticator in seguito incapsula questo ID in un pacchetto “RADIUS Access-Request” e lo inoltra all'authentication server.
  - Negotiation (“EAP Negotiation”) L'authentication server risponde specificando il tipo di authentication EAP che il supplicant dovrebbe utilizzare. Tale risposta è trasmessa dall’authenticator al supplicant.
  - Authentication . Se l'authentication server e il supplicant concordano l'EAP method, si scambiano EAP Request e EAP Response concluse con “EAP-Success” o “EAP-Failure”. In caso positivo il traffico può iniziare.

Modem DSL con interfaccia Wi-Fi



- Communication Systems for the Mobile Information Society, Martin Sauter, 2006, John Wiley & Sons,

IEEE 802.11 – Struttura



802.11a

- Multiplazione: OFDM
- Frequenza: 5 GHz
- Bit rate: fino a 54 Mbit/s
- Note
  - L'intervallo di frequenze adottato non era libero in molti paesi (in Europa era usato da Hiperlan, poi abbandonato).
  - La propagazione a 5 GHz è meno efficacie, e limita la diffusione del segnale.
  - Molto meno diffuso dell'802.11b, definito contemporaneamente e realizzato per primo, che usa una banda non licenziata (Banda ISM - Industrial, Scientific and Medical), a frequenze inferiori (2.45 Ghz) e quindi con minori problemi di propagazione.

Struttura di trama (802.11 a/g)

- Preambolo (SYNC): 10+2 (short/long) simboli OFDM (8 µs, 12 subcarrier/ 8 µs 52 subcarrier): 16 µs
- Signal: 1 simbolo (4 µs): BPSK, Informazioni su modalità di trasmissione e lunghezza pacchetto.
- Payload: simboli OFDM (4 µs) su 52 portanti (48 dati, nei formati previsti e 4 pilot, BPSK); max 4096 per frame.

Short Training	Long Training	Signal	Dati
10 simboli brevi	2 simboli normali	1 simbolo	Max 4096 simboli per frame
8 µs	8 µs	4 µs	Max 16.384 ms

Campi Signal e Dati 802.11 a/g

PLCP - Header

Rate 4 bit	Res. 1 bit	Length 12 bit	Parity 1 bit	Tail 6 bit	Service 16 bit	PSDU 8·Length	Tail 6 bit	Pad
OFDM, BPSK Rate 1/2					OFDM Specified Rate			
Signal (1 OFDM symbol)					Data			

Rate (Mbit/s)	R1-R4
6	1101
9	1111
12	0101
18	0111
24	1001
36	1011
48	0001
54	0011

N_{SYM}= num. dei simboli in OFDM

N_{DBPS}= num. dei bit dati per simbolo OFDM

N_{DATA}= num. dei bit dati

N_{PAD}= num. dei bit pad

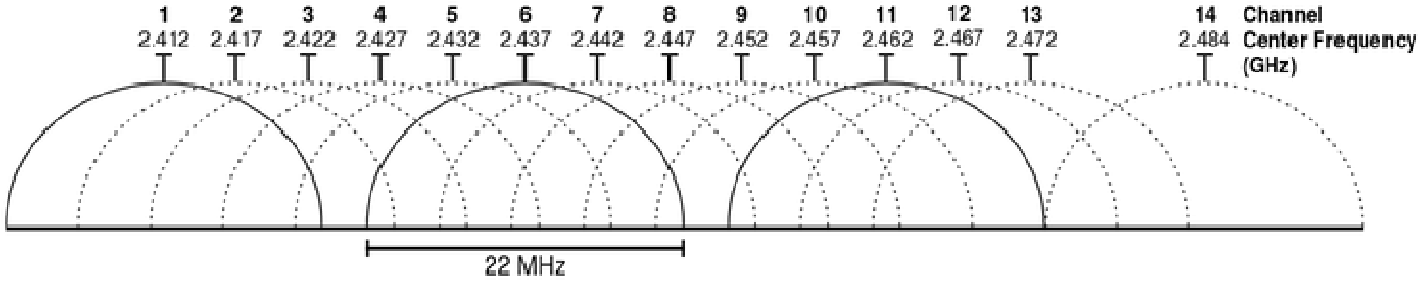
$$N_{SYM} = \left\lceil \frac{16+8\cdot Length+6}{N_{DBPS}} \right\rceil$$

$$N_{DATA} = N_{SYM} \cdot N_{DBPS}$$

$$N_{PAD} = N_{DATA} - (16 + 8 \cdot Length + 6)$$

802.11b

- DSSS
- 14 canali sovrapposti di banda pari a 22 MHz, nell'intervallo di frequenze ISM (2.4-2.5 GHz).



- Chip rate: 11 Mchip/s
- Bit rate: 1, 2, 5.5, 11 Mbit/s
  I vari tassi si ottengono associando in modo opportuno i bit ai chip.
- Per le bit rate pari a 1, 2 Mbit/s, la sequenza di espansione è una sequenza di Barker a 11 chip, con ottime proprietà di autocorrelazione:
  +1 +1 +1 −1 −1 −1 +1 −1 −1 +1 −1 (legacy)
- Per ottenere i tassi superiori, si adottano i codici CCK (Complementary Code Keying), basati sulle sequenze di Hadamard-Walsh.

Struttura di trama (802.11 b)

- Preambolo (HR/DSSS): SYNC (128 bit, 01 alternati)+SFD (Start Frame Delimiter, 1111001110100000, 16 bit) 144 µs

- Header: Signal (tasso di trasmissione espresso in 100 kbit/s, 8 bit), Service (8 bit), Length (lunghezza dati in µs,16 bit), CRC (Cyclic Redundancy Check, $g(x)=x^{16}+x^{12}+x^5+1$, 16 bit): 48 µs.

- Payload:
  - 1 Mbps DSSH DBPSK
  - 2 Mbps DSSH DQPSK
  - 5.5/11 Mbps CCK

Sync 128 bit	SFD 16 bit	Signal 8 bit	Service 8 bit	Length 16 bit	CRC 16 bit	Data
1 Mbit/s						1,2,5.5,11 Mbit/s

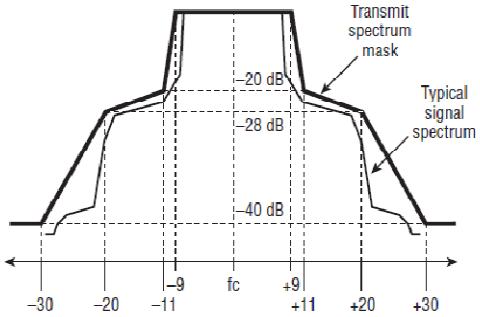
Struttura di trama (802.11 b) preambolo breve

- Preambolo (HR/DSSS): SYNC (56 bit, 01 alternati)+SFD (Start Frame Delimiter, 1111001110100000, 16 bit), 1 Mbit/s: 72 µs
- Header: 48 bit, 2 Mbit/s: 24 µs.
- Payload:
  - 2 Mbps DSSH DQPSK
  - 5.5/11 Mbps CCK

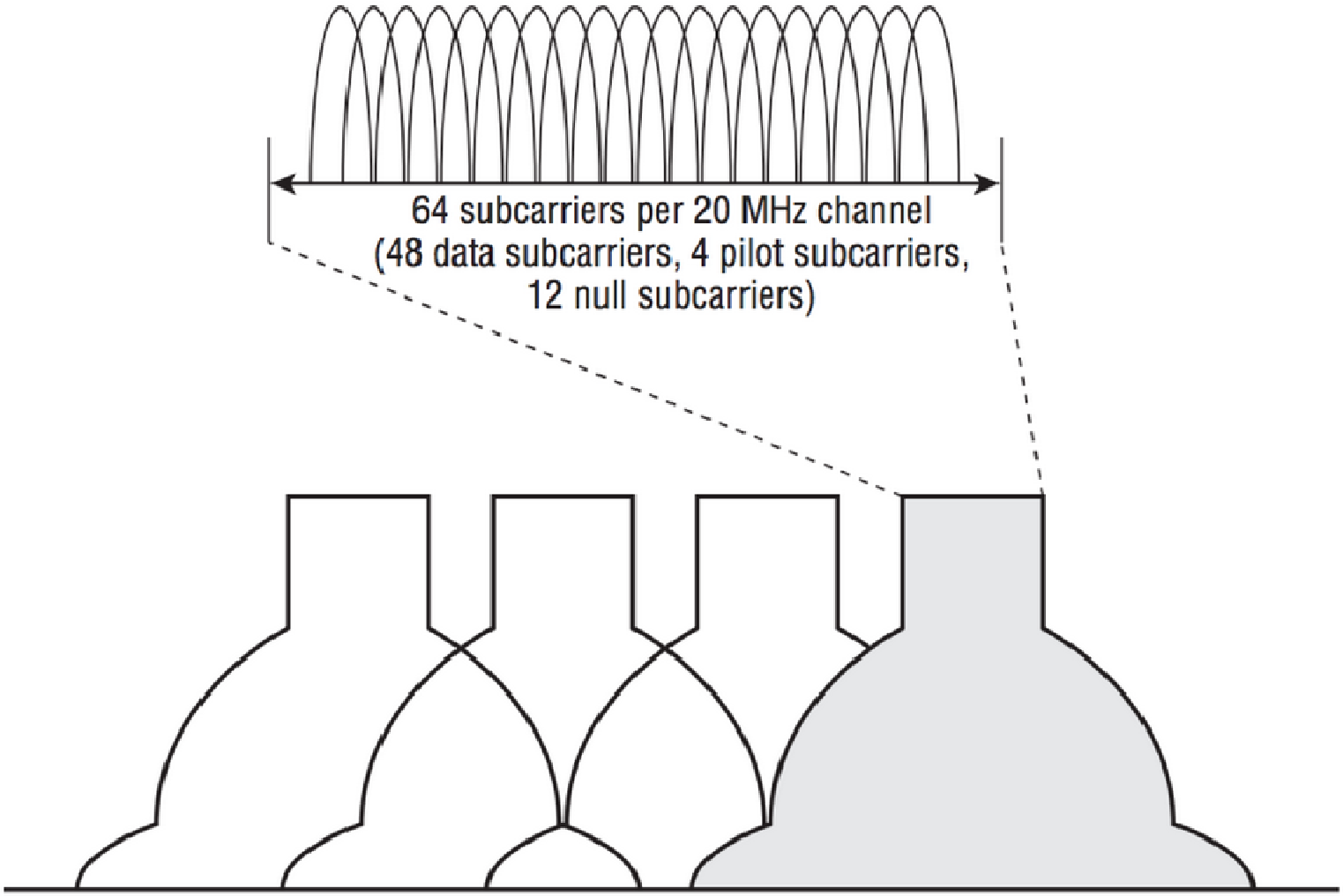
Sync 56 bit	SFD 16 bit	Signal 8 bit	Service 8 bit	Length 16 bit	CRC 16 bit	Data
1 Mbit/s		2 Mbit/s				2,5.5,11 Mbit/s

802.11a/g

- OFDM
- Banda: W=20 MHz (separazione canali).
- Sottoportanti per canale: N_{FFT}=64
- Sottoportanti usate: 52 (non usata la frequenza centrale)
- $\Delta_f = W/N_{FFT}$=312.5 kHz; durata utile simbolo: $T=1/\Delta_f$=3.2 µs.
- Margine 0.8 µs. Durata complessiva: 4 µs.
- Banda occupata (inclusa la frequenza centrale): 16.56 MHz.
- Filtraggio canale:
  - Banda passante: f_c±9 MHz
  - Transizione fuori banda (-20 dB): f_c±11 MHz
  - Fine transizione fuori banda: (-28 dB): f_c±20 MHz
  - Background: (-40 dB): f_c±40 MHz



802.11 a/g Canali OFDM



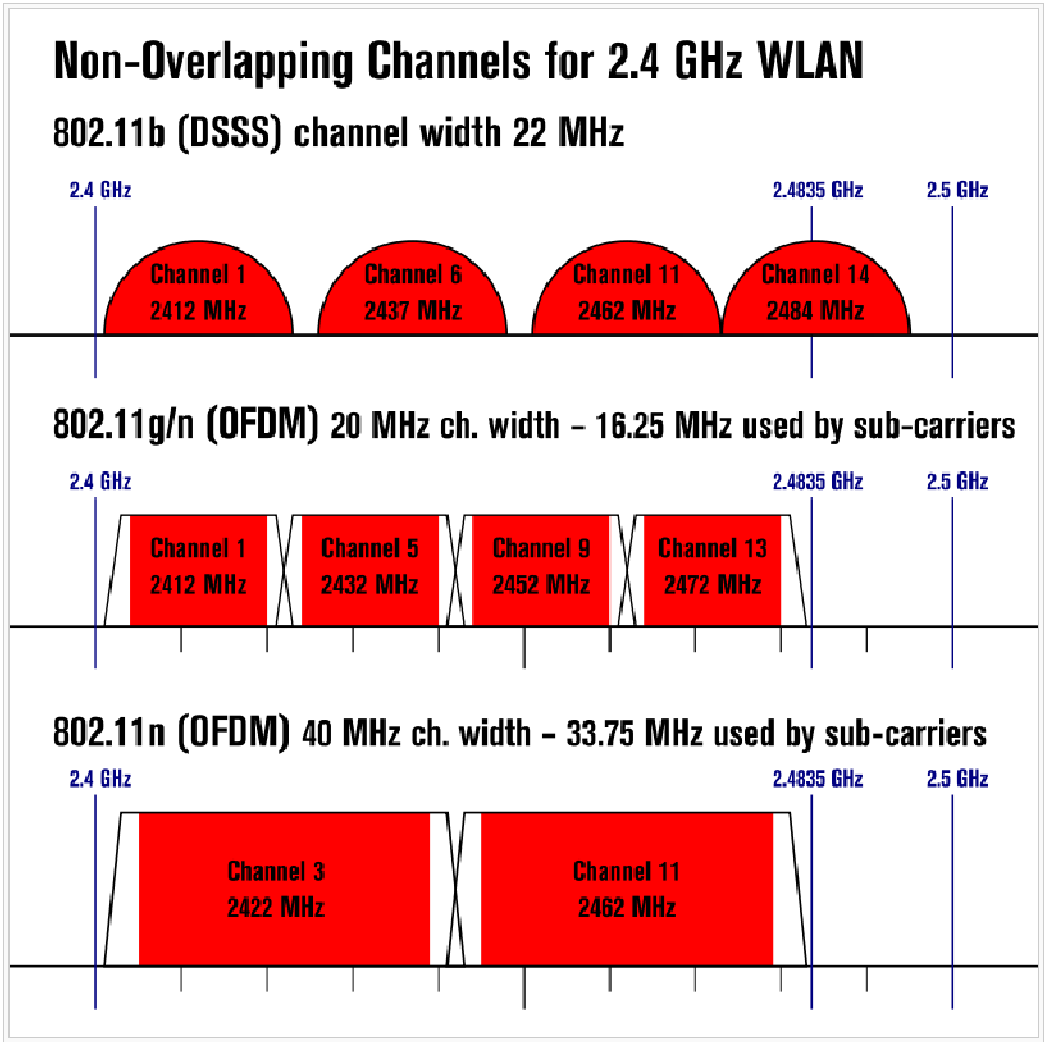
Tasso di trasmissione

Data rate [Mbit/s]	Modulazione	Tasso codice	Bit per portante	Bit per simbolo	Bit utili per simbolo
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16 QAM	1/2	4	192	96
36	16 QAM	3/4	4	192	144
48	64 QAM	2/3	6	288	192
54	64 QAM	3/4	6	288	216

802.11n

- Viene introdotto il MIMO 4x4 (multiplazione).
- Opera sia a 2.4 GHz che a 5 GHz.
- Viene incrementato leggermente il numero di portanti utilizzabili (da 48 a 52 nella banda di 20 MHz).
- Accanto al margine (CP) di 800 ns, viene previsto un margine di 400 ns. Nei due casi l'intervallo di simbolo è pari, rispettivamente a 4 µs e 3.6 µs.
- Vengono previsti canali da 40 MHz, con 108 portanti utilizzabili.
- Parametri:
  - b: bit per simbolo (da 1, BPSK, a 6, 64 QAM)
  - R_c: tasso codice (da 1/2 a 5/6).
  - M: portanti dati per simbolo.
  - T_s: intervallo di simbolo.
  - S: numero di flussi in parallelo (da 1 a 4).
  - Bit rate: $b \cdot R_c \cdot M \cdot S / T_s$ Mbit/s
    Valor massimo (b=6, R_c=5/6, M=108, T_s=3.6 µs, S=4): 600 Mbit/s

Multiplazione: un confronto



Canali (Europa)

- Intervallo 2.4-2.4835 GHz
  - 4 canali da 20 MHz
  - 2 canali da 40 MHz
- Intervallo 5.17-5.33 GHz
  - 8 canali da 20 MHz
  - 4 canali da 40 MHz
- Intervallo 5.49-5.725 GHz
  - 11 canali da 20 MHz
  - 5 canali da 40 MHz

Modi di trasmissione

Mode	Modul.	Rc	S	Mbit/s 20 MHz 400 ns	Mbit/s 20 MHz 800 ns	Mbit/s 40 MHz 400 ns	Mbit/s 40 MHz 800 ns
0	BPSK	1/2	1	7.2	6.5	15.0	13.5
1	QPSK	1/2	1	14.4	13.0	30.0	27.0
2	QPSK	3/4	1	21.7	19.5	45.0	40.5
3	16 QAM	1/2	1	28.9	26.0	60.0	54.0
4	16 QAM	3/4	1	43.3	39.0	90.0	81.0
5	64 QAM	2/3	1	57.8	52.0	120.0	108.0
6	64 QAM	3/4	1	65.0	58.5	135.0	121.5
7	64 QAM	5/6	1	72.2	65.0	150.0	135.0
…							
15	64 QAM	5/6	2	144.4	130.0	300.0	270.0
…							
23	64 QAM	5/6	3	216.7	195.0	450.0	405.0
…							
31	64 QAM	5/6	4	288.9	260.0	600.0	540.0

Struttura di trama (802.11 n)

- Viene introdotto un nuovo preambolo, utilizzato per beamforming e MIMO, e non utilizzabile dai dispositivi a/g.
- Tre modi di trasmissione
  - Legacy
  - HT-MM (High Throughput – Mixed Mode): terminali n in rete mista
  - HT-GF (HT – GreenField): terminali in rete n pura (non usato)
- Preambolo HT-MM.

L-STF	L-LTF	L-SIG	HT-SIG	HT-STF	HT-LTF	…	HT-LTF	Dati
8 µs	8 µs	4 µs	8 µs	4 µs	4 µs		4 µs	

- Il campo HT-SIG è usato per fornire informazioni su modulazione, codifica, lunghezza in byte (in realtà tale *lunghezza* serve a determinare il tempo di trasmissione, ipotizzando che la trasmissione avvenga a 6 Mbit/s)

802.11n HT-SIG

- Campi di HT-SIG
  - Modulazione e codifica (7 bit).
  - Banda utilizzata (0: 20 MHz; 1: 40 MHz).
  - Lunghezza (16 bit): fino a 65535.
  - Not sounding (1 bit): per distinguere pacchetti di stima del canale.
  - Aggregazione (1 bit): 1 per indicare pacchetti MAC aggregati.
  - Space Time Block Coding (2 bit): diversità in trasmissione.
  - Forward Error Correction (1 bit): 1 se LDPC.
  - Short Guard Interval (1 bit).
  - CRC (8 bit)
  - Tail (6 bit)

Aggregation

- Un pacchetto MAC può essere composto dall'aggregazione di più pacchetti provenienti dai livelli superiori.
- Consente di risparmiare sui tempi di accesso.
- Il singolo frammento (A-MPDU) ha il seguente formato.

M-PDU Delimiter	MAC-Header	MAC-Payload	FCS	PAD

- Dimensione A-MPDU: $2^{13+\text{Exponent}}$-1 byte, Exponent=0:3 (8, 16, 32, 64 kbyte)

Riepilogo caratteristiche livello fisico 802.11 n

- Obbligatorie
  - HT Mixed Mode
  - Intervallo di guardia di 800 ns
  - Canali a 20 MHz
  - Modi da 0 a 7, singolo flusso
  - Per gli AP modi da 8 a 15, doppio flusso

- Opzionali
  - HT GreenField
  - Intervallo di guardia di 400 ns
  - Canali a 40 MHz
  - Modi da 16 a 31, fino a quattro flussi
  - Low Density Parity Check Codes
  - Space Time Block Coding

802.11 ac

- Aumentano le prestazioni e la scalabilità
- Incremento delle prestazioni mediante:
  - incremento della banda, dai 40 MHz di 802.11n a 80 MHz (234 portanti) e 160 MHz (468 portanti);
  - modulazioni più complesse (256 QAM);
  - incremento del numero di flussi MIMO, fino a un massimo di 8.
- Opera a 5 GHz, per evitare l'affollamento della banda inferiore.
- Introduce il Multi User MIMO, mediante beamforming.
- Mantenuta la compatibilità con gli standard precedenti, dato che i canali pilota mantengono il formato del 402.11a.
- Il meccanismo RTS/CTS è usato per evitare le collisioni e risolvere il problema del terminale nascosto.

Modi di trasmissione

Modo	Modulazione	Tasso codice	Tasso	SNR Soglia Shannon [dB]
0	BPSK	1/2	1/2	-2.8
1	QPSK	1/2	1	0.2
2	QPSK	3/4	3/2	3.4
3	16 QAM	1/2	2	5.1
4	16 QAM	3/4	3	9.3
5	64 QAM	2/3	4	12.6
6	64 QAM	3/4	9/2	14.4
7	64 QAM	5/6	5	16.2
8	256 QAM	3/4	6	19.2
9	256 QAM	5/6	20/3	21.4

Velocità massima di trasmissione

Modul.	Rc	S	Mbit/s 80 MHz 800 ns	Mbit/s 80 MHz 400 ns	Mbit/s 160 MHz 800 ns	Mbit/s 160 MHz 400 ns
256 QAM	5/6	1	390	433	780	867
256 QAM	5/6	2	780	867	1560	1733
256 QAM	5/6	3	1170	1300	2340	2600
256 QAM	5/6	4	1560	1733	3120	3467
256 QAM	5/6	5	1950	2167	3900	4333
256 QAM	5/6	6	2340	2600	4680	5200
256 QAM	3/4	7	2730	3033	5460	6067
256 QAM	5/6	8	3120	3467	6240	6933

802.11 a/g/n/ac: OFDM

Standard	Subcarrier range	Pilot subcarrier	Subcarrier totali (data/pilot)	Capacità rispetto 802.11a/g	Capacità rispetto 802.11ac 20 MHz
802.11 a/g	-26:-1 1:26	±7, ±21	52 (48/4)	1	-
802.11n 802.11ac 20 MHz	-28:-1 1:28	±7, ±21	56 (52/4)	1.1	1
802.11n 802.11ac 40 MHz	-58:-2 2:58	±11, ±25 ±53	114 (108/6)	2.3	2.1
802.11ac 80 MHz	-122:-2 2:122	±11, ±39 ±75, ±103	242 (234/8)	4.9	4.5
802.11ac 160 MHz	-250:-130 -126:-6 6:126 130:250	±25, ±53 ±89, ±117 ±139, ±167 ±203, ±231	484 (468/16)	9.75	9

Canali (Europa)

- Intervallo 5.17-5.33 GHz
  - 8 canali da 20 MHz
  - 4 canali da 40 MHz
  - 2 canali da 80 MHz
  - 1 canale da 160 MHz

- Intervallo 5.49-5.725 GHz
  - 11 canali da 20 MHz
  - 5 canali da 40 MHz
  - 2 canali da 80 MHz
  - 1 canale da 160 MHz

Struttura di trama (802.11 ac)

- Viene introdotto un nuovo preambolo, utilizzato per beamforming e MIMO, e non utilizzabile dai dispositivi a/g/n.
- Modi di trasmissione
  - Legacy
  - VHT-MM (Very High Throughput – Mixed Mode): terminali ac in rete mista
- Preambolo VHT-MM.

L-STF	L-LTF	L-SIG	VHT-SIG A	VHT-STF	VHT-LTF	VHT-SIG B	Dati
8 µs	8 µs	4 µs	8 µs	4 µs	4 µs	4 µs	

- VHT-SIG A: per tutti i destinatari
- VHT-STF, VHT-LTF, VHT-SIG B: per ciascun destinatario nella modalità Multi User.

802.11ac VHT-SIG A

- Campi di VHT-SIG A
  - Banda utilizzata (2 bit) (00: 20 MHz; 11: 160 MHz).
  - Riservato (1 bit): usi futuri.
  - Space Time Block Coding (1 bit): diversità.
  - Group ID (6 bit): 63 per stazione singola, 0 per AP singolo.
  - Numero di flussi (3 bit): a base 0 (0 significa 1 flusso).
  - Partial AID (9 bit): identifica l'AP.
  - Transmit power save forbidden (1 bit): vietato spegnere il ricevitore.
  - Riservato (1 bit): usi futuri.
  - Short Guard Interval (1 bit). Short GI disambiguation (1 bit).
  - LDPC (1 bit), LDPC Extra Symbol (1 bit).
  - Mode (4 bit): modulazione e codifica.
  - Beamforming (1 bit).
  - CRC (8 bit).
  - Tail (6 bit): 6 zeri.

802.11ac VHT-SIG B

- Campi di VHT-SIG B
  - Lunghezza (17 bit a 20 MHz, 19 bit a 40 MHz, 21 bit negli altri casi). Unità di misura: 4 byte.
  - Riservato (3 bit a 20 MHz, 2 bit altrimenti): usi futuri.
  - Tail (6 bit): 6 zeri.

- Lunghezza massima
  - Il frame 802.11 ac ha un tempo di trasmissione massimo pari a 5.848 ms.
  - Dimensione A-MPDU: $2^{13+\text{Exponent}}$-1 byte, Exponent=0:7.
  - Dimensione massima frame (payload data in bytes): 4.69248 Mbyte.

Riepilogo caratteristiche livello fisico 802.11 ac

- Obbligatorie
  - VHT Mixed Mode
  - Intervallo di guardia di 800 ns
  - Canali a 20, 40, 80 MHz
  - Modi da 0 a 7, singolo flusso
- Opzionali
  - Intervallo di guardia di 400 ns
  - Canali a 160 MHz
  - Modi da 8, 9, singolo flusso
  - 2-8 flussi
  - Low Density Parity Check Codes
  - Space Time Block Coding

802.11 Pacchetti

- Struttura generale pacchetto

PHY		DLL		Higher	Trailer	
PLCP Preamble	header	MAC header	LLC (opt)	Data	FCS	End delimiter

- PLCP (Physical Layer Convergence Protocol), (802.11/a, preamble= training, header=signal).
- MAC header: dipende dal tipo di pacchetto (data packet, network management packet, control packet).
- FCS (Frame Check Sequence): per la rivelazione d'errori.

802.11 Data MAC Header

Frame Control	Duration ID (μs)	Address 1	Address 2	Address 3	Sequence Control	Address 4
2 byte	2 byte	6 byte	6 byte	6 byte	2 byte	6 byte

Frame control (QoS field in DLL: QoS bit in Sub type=1; HT field: order=1)

Protocol Version	Type	Sub-type	To DS	From DS	More frag	Retry	Power Mgmt	More Data	WEP	order
2 bit	2 bit	4 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Indirizzi (SA:source; DA: destination; TA: transmitter; RA:receiver)

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA=DA	TA=SA	BSSID	N/A
0	1	RA=DA	TA=BSSID	SA	N/A
1	0	RA=BSSID	TA=SA	DA	N/A
1	1	RA	TA	DA	SA

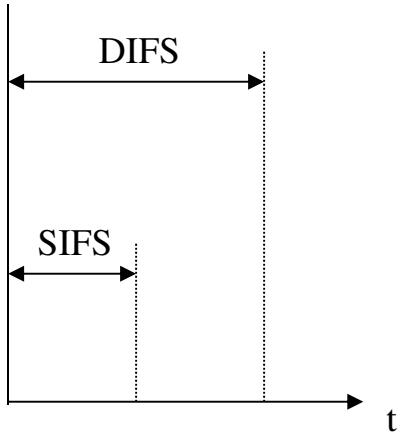
IEEE 802.11 Distributed Coordination Function-DCF (I)

- Due modalità di trasmissione:
  - Accesso Base (Basic Access - BA) - DATA/ACK: dopo la trasmissione del pacchetto dati da parte della sorgente, il destinatario, in caso di corretta ricezione, invia l'ACK.
  - Accesso RTS/CTS (RTS/CTS Access - RCA) - RTS/CTS/DATA/ACK (Request To Send/Clear To Send/DATA/ACK): lo scambio DATA/ACK è preceduto da una fase in cui la sorgente invia una richiesta di trasmissione (RTS) ed il destinatario risponde con un pacchetto di conferma (CTS).

- Uno scambio (handshake a 2 o 4 fasi) è considerato come un'operazione unica, che non deve essere interrotta, per cui la trasmissione dei pacchetti successivi a quello che ha dato inizio all'handshake deve avere priorità rispetto alle trasmissioni degli altri nodi e deve avvenire nel tempo più breve possibile.

IEEE 802.11 DCF (II)

- Short InterFrame Space (SIFS): separa la ricezione/trasmissione di pacchetti appartenenti allo stesso dialogo (DATA/ACK o RTS/CTS/DATA/ACK).
- Distributed InterFrame Space (DIFS): tempo minimo che una stazione deve attendere prima di accedere al canale o generare il backoff: DIFS = SIFS + 2σ (σ: durata di uno slot - slot time).



Essendo il SIFS minore del DIFS, viene garantita una priorità intrinseca alle trasmissioni in corso.

IEEE 802.11 DCF – BA (I)

Oltre al CS fisico, i nodi 802.11 implementano un meccanismo di CS virtuale, detto Network Allocation Vector (NAV). Ogni pacchetto contiene un campo, detto duration field, che specifica la durata dell'intero handshake. Un nodo in ascolto è in grado di sapere per quanto tempo sarà occupato il canale. Può così staccare la parte radio, evitando di fare il CS fisico, ed entrare in modalità sleeping (risparmio energetico).

Procedura di accesso.

1. Quando un nodo ha un pacchetto da trasmettere, il nodo verifica che il NAV sia 0 ed esegue il CS fisico del canale per un tempo pari a DIFS.
2. Se il canale è libero il pacchetto viene immediatamente trasmesso, altrimenti il CS fisico continua e, non appena il canale risulta libero per un DIFS, viene generato il tempo di backoff k (controllo del flusso), dove k è un intero casuale uniformemente distribuito tra 0 e $W_{min} - 1$ (W_{min}: finestra di contenzione minima).

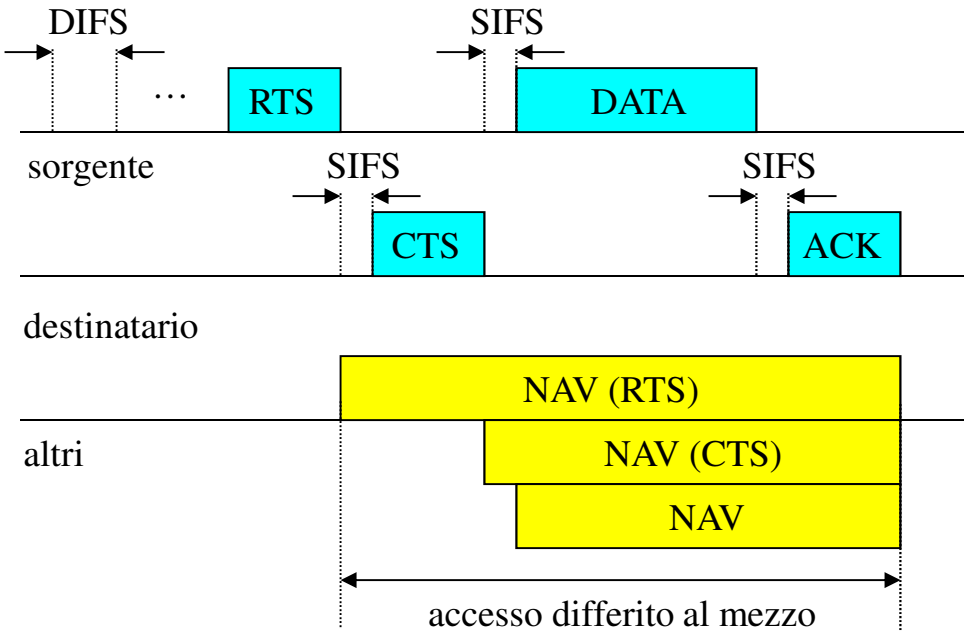
IEEE 802.11 DCF – BA (II)

3. Il backoff viene inserito in un contatore all'indietro, mentre il nodo continua ad eseguire il CS fisico.
   - Se il canale è libero, il conteggio all'indietro prosegue normalmente.
   - Se il canale è occupato, il conteggio viene bloccato e viene ripreso soltanto dopo che il canale risulta nuovamente libero per un tempo pari a DIFS.

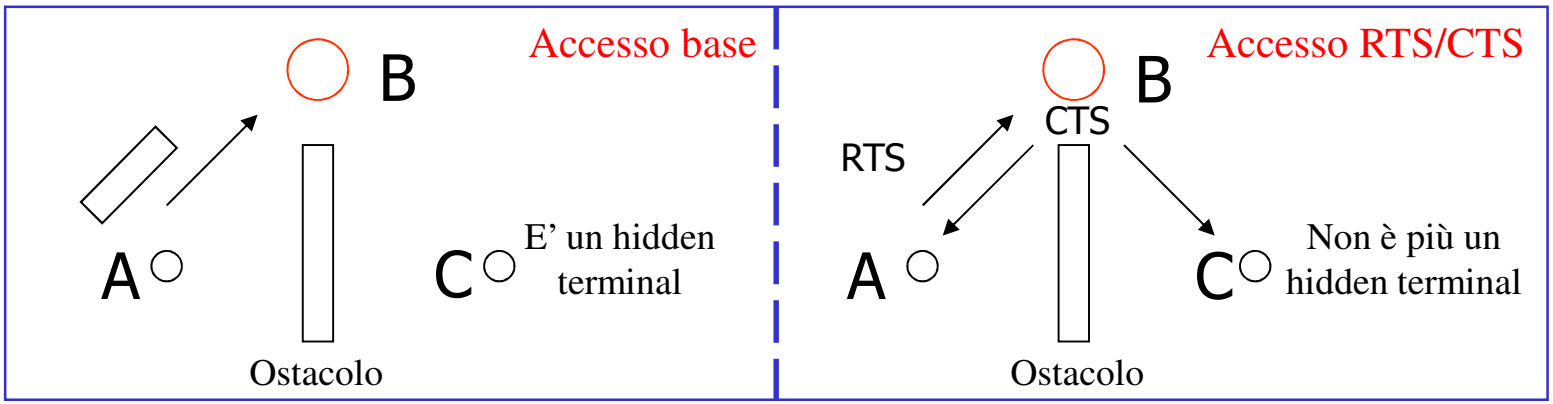
4. Quando il contatore arriva a 0 il pacchetto DATA viene trasmesso. Se il destinatario riceve correttamente DATA, invia l'ACK entro un SIFS.

5. Se il nodo sorgente non riceve l'ACK entro un timeout, schedula la ritrasmissione del pacchetto. Dopo ogni tentativo i, viene incrementato il contatore delle ritrasmissioni ($i = i + 1$). Se $i = m$, dove m è il numero massimo di ritrasmissioni (Retry limit), il pacchetto viene scartato. Altrimenti:
   - viene modificata la finestra di contenzione $W_i = \min(2W_{i-1}, W_{max})$, dove $W_{max} = 2^{m'} \cdot W_{min}$ è la finestra di contenzione massima ed m' è il backoff stage massimo.
     Es.: $m' = 5$, $m = 7$, $W_{min} = 32$
     $W_{max} = 2^5 \cdot 32 = 1024$, $W_i \in \{32,64,128,256,512,1024,1024,1024\}$.
   - viene generato un nuovo backoff k, con k uniformemente distribuito tra 0 e $W_i - 1$.

IEEE 802.11 DCF – RCA



- Analogo all'accesso base, ma come primo pacchetto viene inviato un RTS.
- Vantaggioso per pacchetti DATA di grandi dimensioni (in caso di collisione il tempo perso è inferiore), non utile per pacchetti piccoli.
- Mitigazione degli effetti dovuti all' hidden terminal.



IEEE 802.11 DCF – Analisi (I)

Definizioni

- H : tempo di trasmissione del payload (informazione)
- n : numero di nodi
- m : numero massimo di ritrasmissioni
- m' : backoff stage massimo
- k : contatore del backoff
- i : contatore delle ritrasmissioni
- W_i : finestra di contenzione all'i-esima ritrasmissione

$$W_i = 2^{\min(i,m')} W_{\min}$$

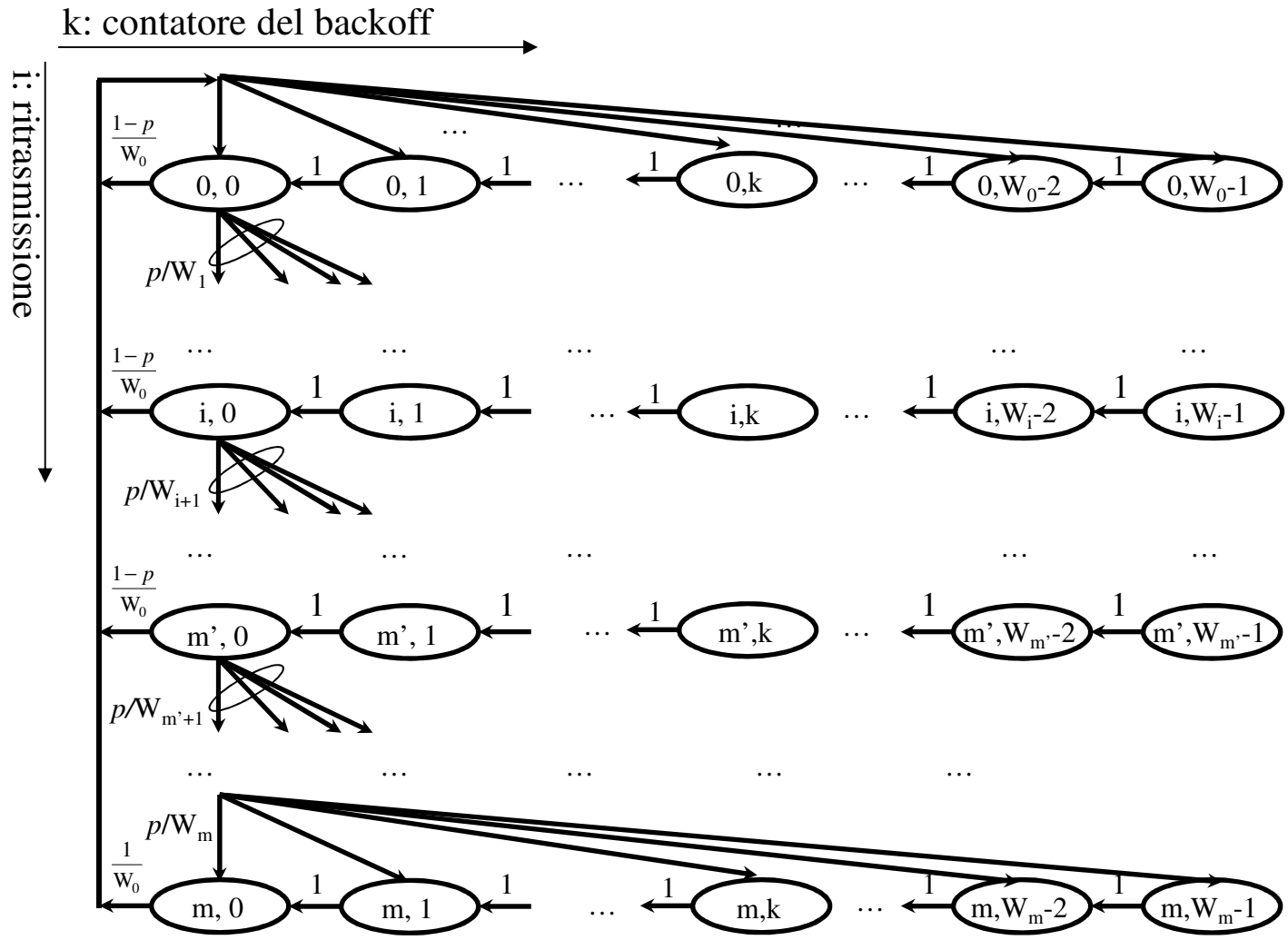
- p: probabilità di collisione

Ipotesi

- Saturazione (c'è sempre un pacchetto in coda da trasmettere).

IEEE 802.11 DCF – Analisi (II)

- Modello della DCF per il singolo nodo: catena di Markov bidimensionale.



IEEE 802.11 DCF – Analisi (III)

Probabilità di transizione:

$$\begin{cases} \Pr\{i,k|i,k+1\}=1 & k\in[0,W_i-2] \quad i\in[0,m] & (1) \\ \Pr\{0,k|i,0\}=\dfrac{1-p}{W_0} & k\in[0,W_0-1] \quad i\in[0,m-1] & (2) \\ \Pr\{i,k|i-1,0\}=\dfrac{p}{W_i} & k\in[0,W_i-1] \quad i\in[1,m] & (3) \\ \Pr\{0,k|m,0\}=\dfrac{1}{W_0} & k\in[0,W_m-1] & (4) \end{cases}$$

(1) All'inizio di uno slot il contatore viene decrementato (sicuramente prima o poi).
(2) Dopo un successo all'i-esimo tentativo, che avviene con probabilità (1 - p), riparto con la finestra di contenzione minima W_0 ed ho un valore k-esimo per il backoff counter che è uniformemente distribuito tra 0 e $W_0 - 1$.
(3) Dopo un fallimento all'(i - 1)-esimo tentativo, che avviene con probabilità p, riparto con la finestra di contenzione W_i ed ho un valore k-esimo per il backoff counter che è uniformemente distribuito tra 0 e $W_i - 1$.
(4) Una volta raggiunto il massimo numero di ritrasmissioni, riparto con un nuovo pacchetto e con la finestra di contenzione minima.

IEEE 802.11 DCF – Analisi (IV)

- Passo I: determinazione delle probabilità di stato $\pi_{i,k}$, $i \in [0,m]$, $k \in [0,W_i-1]$.
  - Espressione delle $\pi_{i,k}$ in funzione di $\pi_{0,0}$:

$$\pi_{i,k} = f_{i,k}(\pi_{0,0})$$

  - Imposizione della condizione di normalizzazione:

$$\sum_{i=0}^{m} \sum_{k=0}^{W_i-1} \pi_{i,k} = 1$$

$$\Downarrow \ldots$$

$$\pi_{0,0} = \pi_{0,0}(p) = \frac{2(1-2p)(1-p)}{W_0\left[1-(2p)^{m'+1}\right](1-p) + (1-2p)\left(1-p^{m+1}\right) + W_0 2^{m'} p^{m'+1}(1-2p)\left(1-p^{m-m'}\right)}$$

$$\Uparrow$$

Problema in più: p è un'incognita

IEEE 802.11 DCF – Analisi (V)

- Espressione della probabilità di trasmissione in funzione della probabilità di collisione (ricordando che il pacchetto viene trasmesso quando il backoff timer arriva a zero):

$$\tau = \sum_{i=0}^{m} \pi_{i,0} = F(p)$$

- Espressione della probabilità di collisione in funzione della probabilità di trasmissione (ricordando che la probabilità di collisione in quello slot è la probabilità che una delle rimanenti n - 1 stazioni trasmetta):

$$p = 1 - (1 - \tau)^{n-1}$$

- Queste formano un sistema non-lineare di due equazioni in due incognite, che può essere risolto numericamente in p e τ :

$$p, \tau \Rightarrow \pi_{0,0} \Rightarrow \pi_{i,k}$$

IEEE 802.11 DCF – Analisi (VI)

- Passo II: determinazione del throughput.

$$S = \frac{\overbrace{P_{tr} P_s \mathrm{H}}^{\text{frazione di slot utile}}}{\underbrace{(1-P_{tr})\sigma}_{\substack{\text{frazione di slot} \\ \text{sprecata per inutilizzo}}} + \underbrace{P_{tr} P_s T_s}_{\substack{\text{frazione di slot} \\ \text{necessaria per un successo}}} + \underbrace{P_{tr}(1-P_s) T_c}_{\substack{\text{frazione di slot} \\ \text{sprecata per collisione}}}}$$

$P_{tr} = 1-(1-\tau)^n$ Probabilità che almeno una (qualunque) stazione trasmetta un pacchetto.

$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}}$ Probabilità di successo (probabilità che esattamente un nodo trasmetta ed i rimanenti n - 1 no, condizionata al fatto che almeno un nodo trasmetta).

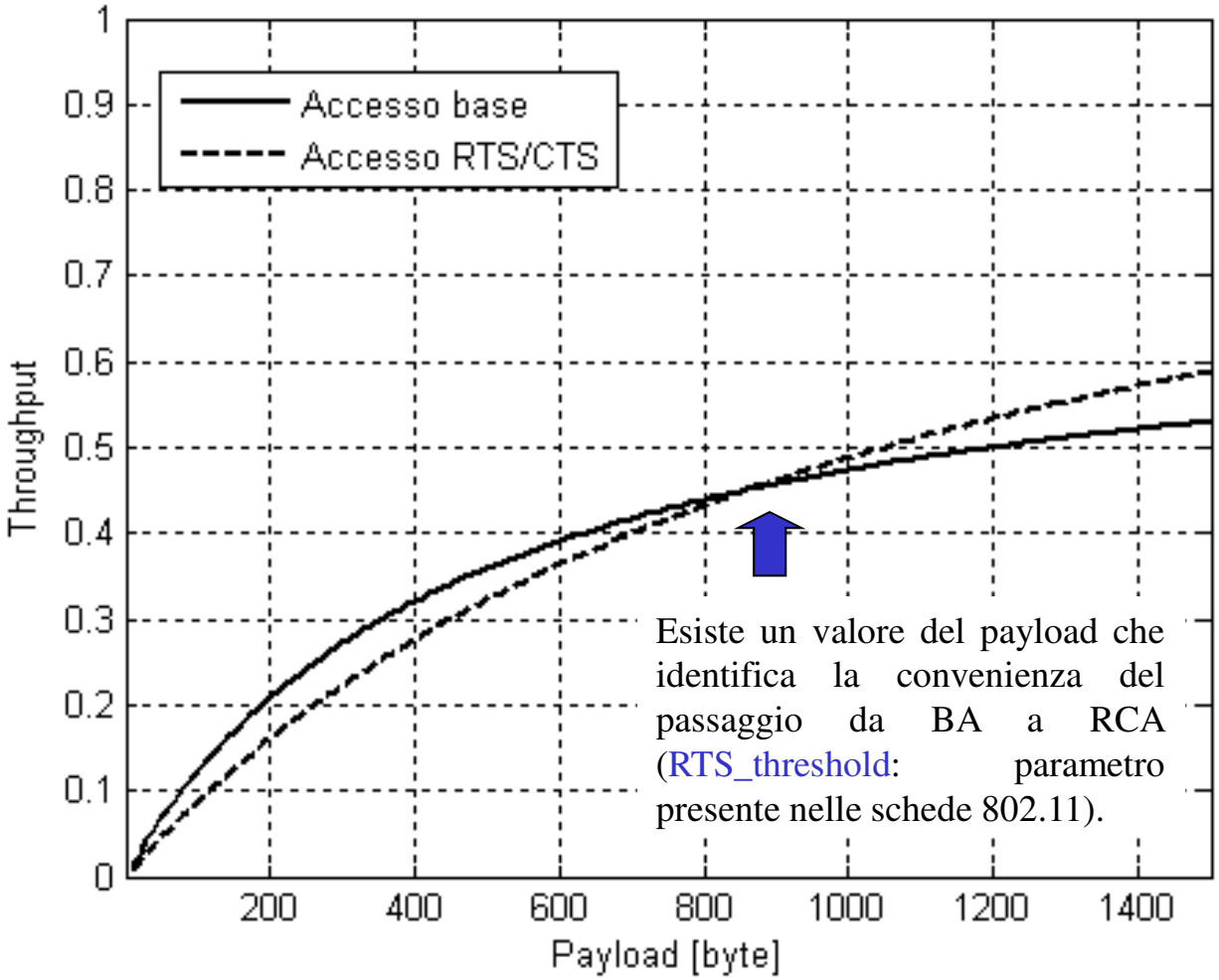
T_c Tempo perso a causa di una collisione.

T_s Tempo richiesto da una trasmissione con successo.

Accesso base: $T_c = T_s = \mathrm{DIFS} + \mathrm{DATA} + \mathrm{SIFS} + \mathrm{ACK}$

Accesso RTS/CTS:
$$\begin{cases} T_s = \mathrm{DIFS} + \mathrm{RTS} + \mathrm{SIFS} + \mathrm{CTS} + \mathrm{SIFS} + \mathrm{DATA} + \mathrm{SIFS} + \mathrm{ACK} \\ T_c = \mathrm{DIFS} + \mathrm{RTS} + \mathrm{SIFS} + \mathrm{CTS} \ \ (< T_s) \end{cases}$$

IEEE 802.11 DCF – Analisi (VII)



Esiste un valore del payload che identifica la convenienza del passaggio da BA a RCA (RTS_threshold: parametro presente nelle schede 802.11).

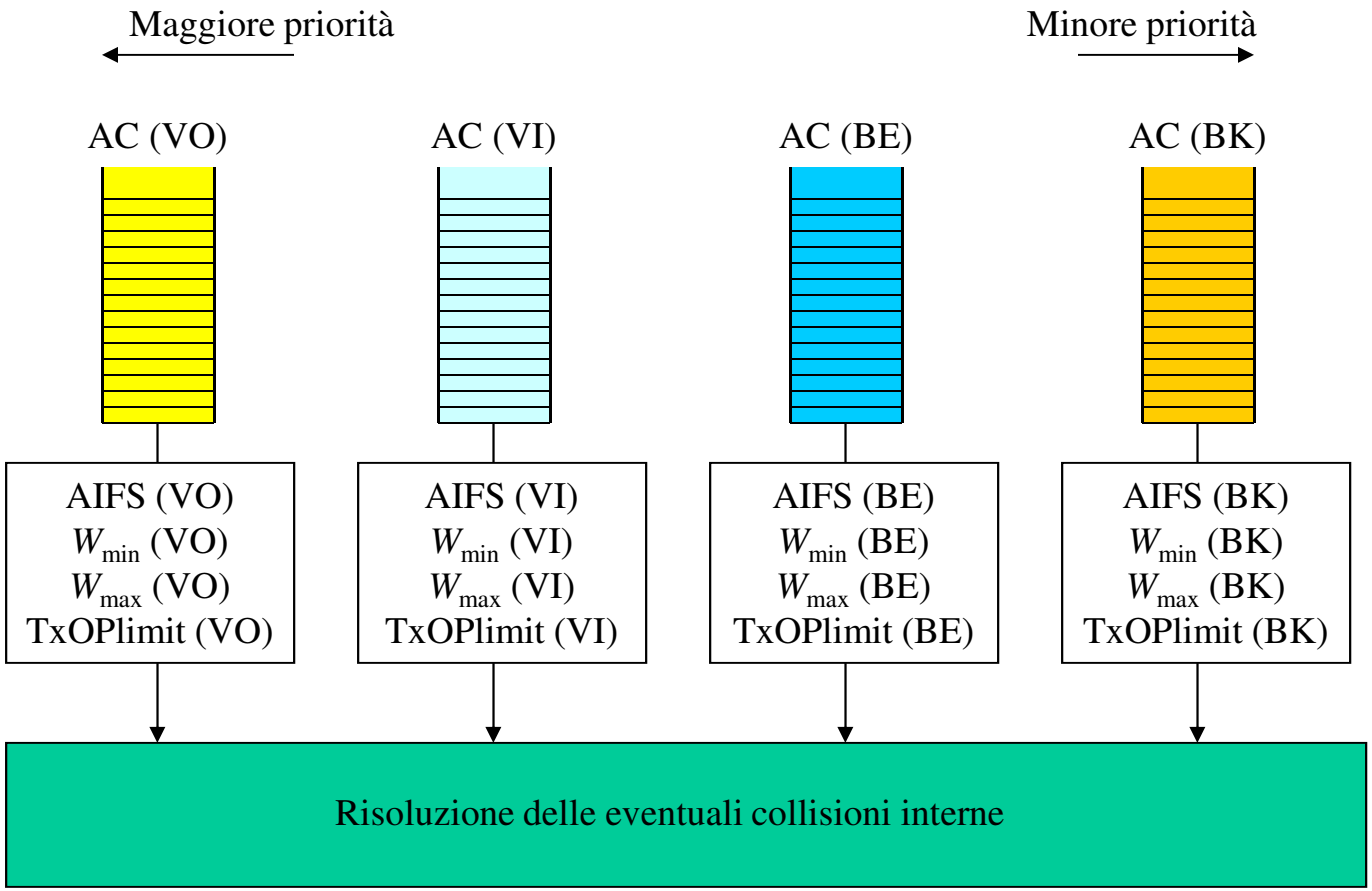
IEEE 802.11e

Estensione nata per soddisfare requisiti di QoS per traffico multimediale tramite l'introduzione di classi di priorità.

- Quattro categorie di accesso (Access Category - AC): VOice (VO), VIdeo (VI), Best Effort (BE), BacKground (BK).
- Estensione della DCF adottando la Enhanced Distributed Channel Access (EDCA).
- Introduzione di un nuovo parametro. Una stazione che ottiene l'accesso non è obbligata ad inviare un solo pacchetto, ma ha una Transmission Opportunity (TxOP), un intervallo di tempo definito da un istante iniziale e da una durata (TxOPlimit) durante il quale può inviare più pacchetti.

IEEE 802.11e – EDCA (I)

Singolo nodo



IEEE 802.11e – EDCA (II)

- Se, ad uno stesso nodo, due pacchetti appartenenti ad AC diverse collidono, la TxOP viene data alla AC a priorità più elevata, mentre l'altra AC si comporta come se avesse colliso (risoluzione delle collisioni interne).

- Le AC sono differenziate in base ai valori dei parametri dell'algoritmo di accesso:

  - Arbitration InterFrame Space AIFS[AC]: basso (alto) per AC a priorità elevata (bassa), è una generalizzazione del DIFS.

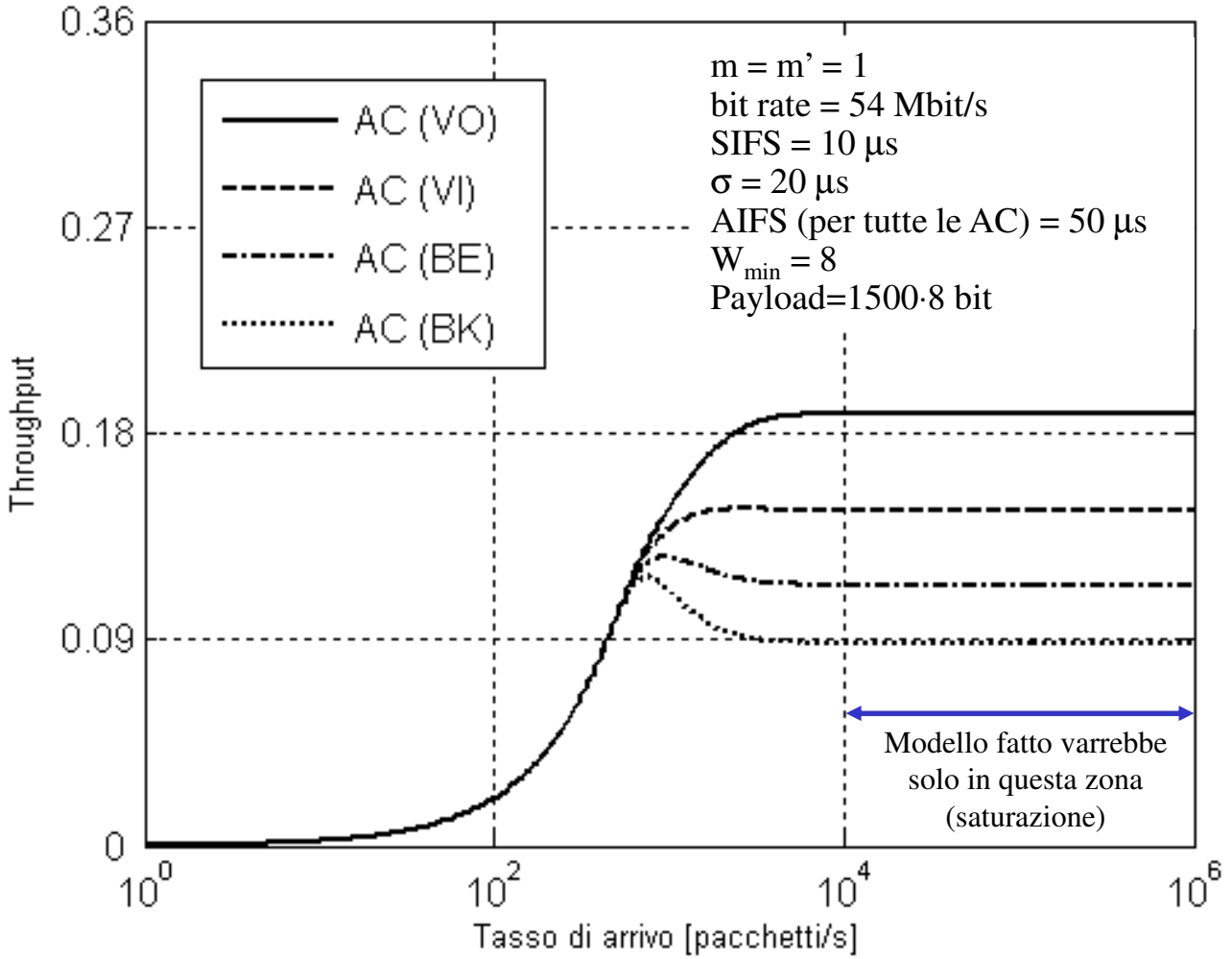
  - CW_{min}[AC]: bassa (alta) per AC a priorità elevata (bassa), backoff bassi (alti) per traffici con (senza) vincoli sul ritardo – VO, VI (BE, BK).

  - CW_{max}[AC]: bassa (alta) per AC a priorità elevata (bassa), poche (molte) ritrasmissioni per traffici con (senza) vincoli sul ritardo – VO, VI (BE, BK).

  - TxOPlimit[AC]: alto (basso) per AC a priorità elevata (bassa).

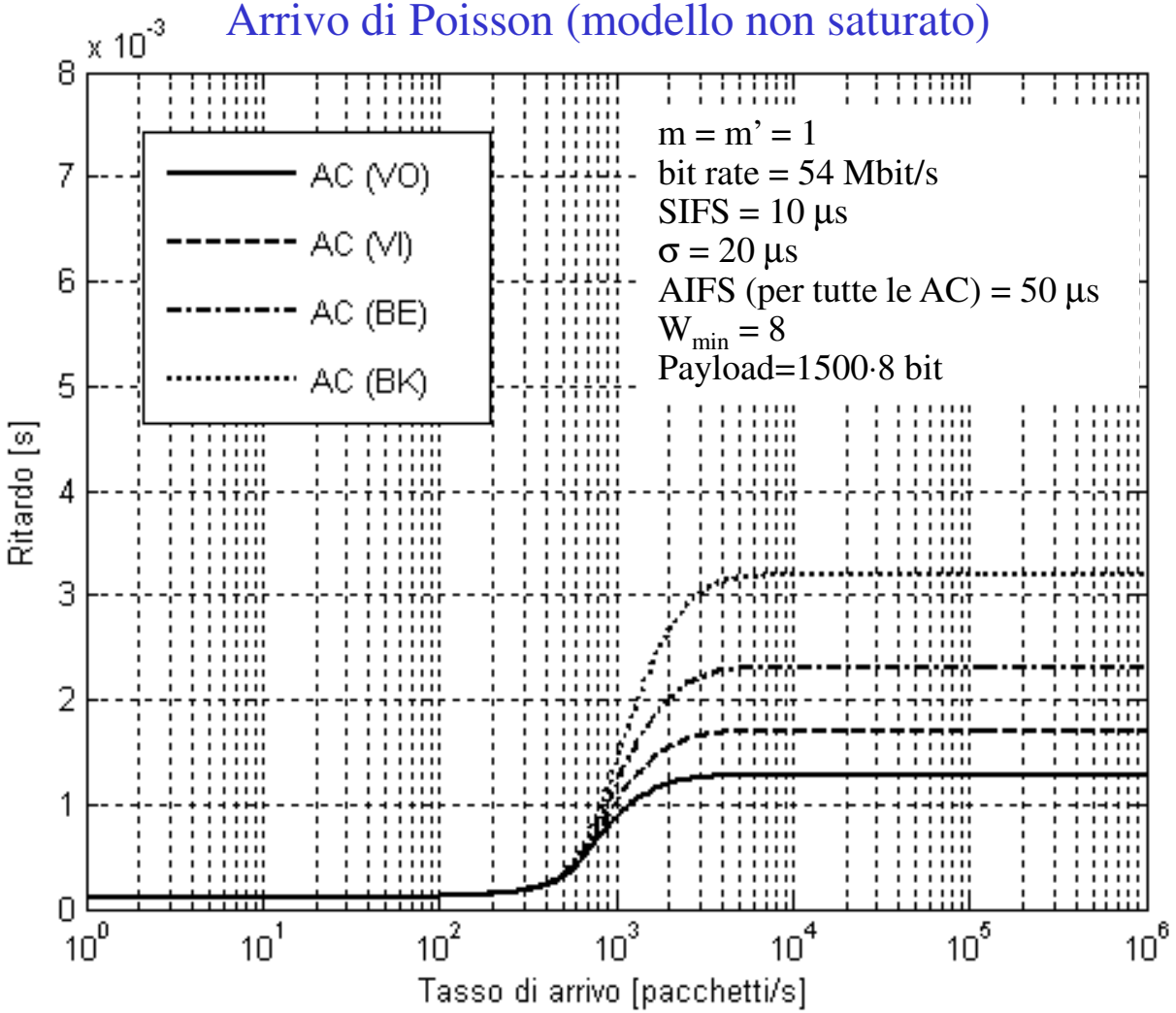
IEEE 802.11e EDCA – Throughput

Arrivo di Poisson (modello non saturato)



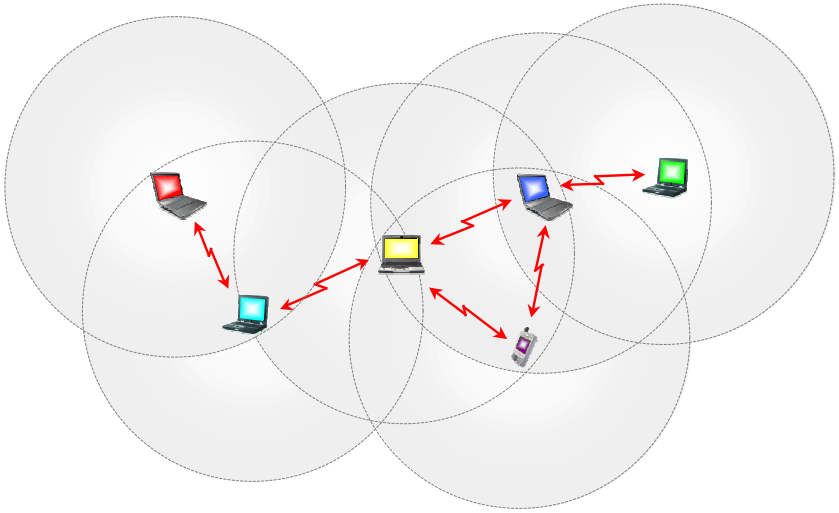
IEEE 802.11e EDCA – Ritardo

Arrivo di Poisson (modello non saturato)

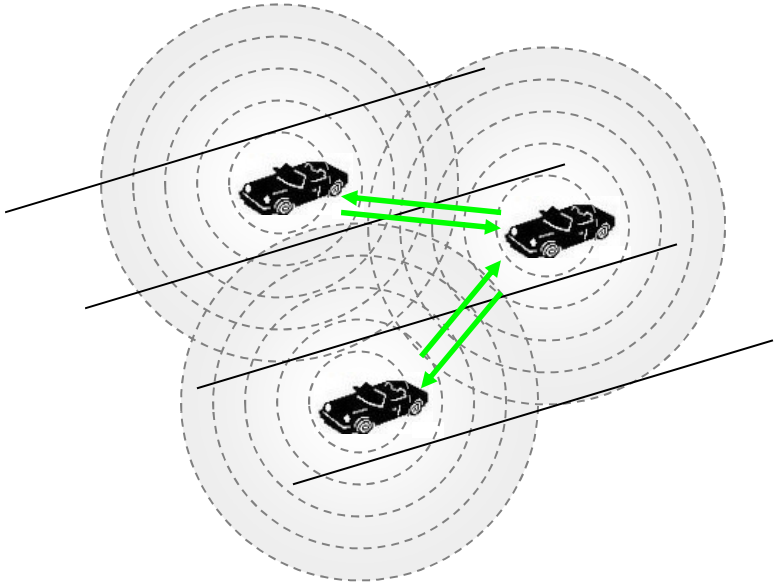


IEEE 802.11 – MANET/VANET

- MANET: nessuna autorità centrale.
  - Accesso completamente distribuito.
  - Ogni nodo può fare da router.
- Mobilità pedestre.
- Obiettivi: throughput e risparmio energetico (i nodi non sono connessi ad una rete di alimentazione fissa).

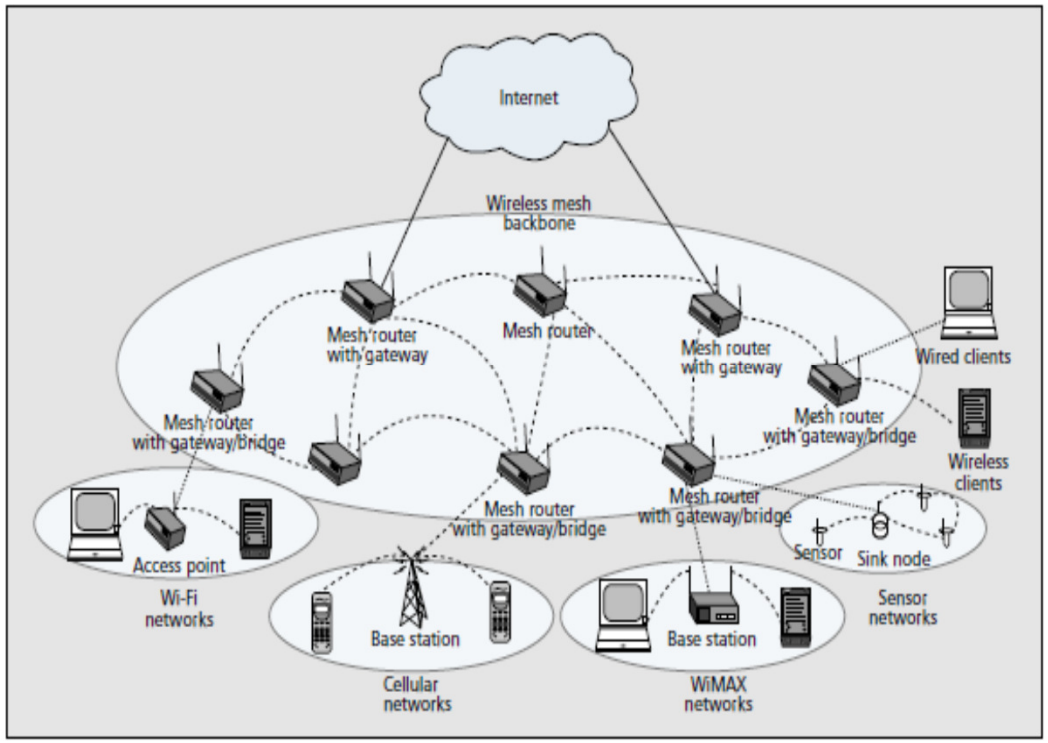


- VANET: gestione della comunicazione interveicolare e della comunicazione tra veicoli e postazioni fisse.
- Elevata mobilità (autostrade intelligenti, treni ad alta velocità: fino a 500km/h).
  - Forte fluttuazione del segnale.
  - Routing (breve durata dei percorsi).
- Obiettivo: affidabilità.



IEEE 802.11 – WMN

- WMN: nodi con interfacce radio multiple.
- Due tipologie di nodi: mesh router (solitamente fissi, formano la backbone) e mesh client (mobili).
- Un mesh router può fare anche da gateway/bridge con altre reti.
- Obiettivo: supporto di traffico multimediale con requisiti di QoS.
- Tecnologia alla base delle wireless community network: reti create e gestite non da operatori, ma da gruppi di tecnici appassionati grazie ai bassi costi dei dispositivi WiFi.



La finalità di una wireless community network, che non è proprietaria, ma rappresenta un bene comune, è la condivisione della connettività ad Internet. Es. SeattleWireless (USA), Freifunk (Germania), Guifi.net (Spagna), Ninux.org (Italia), …

IEEE 802.11af e IEEE 802.11ah

- IEEE 802.11af (White-Fi) e IEEE 802.11ah (HaLow) sono soluzioni proposte per la connettività IoT (Internet of Things). Entrambe utilizzano uno spettro precedentemente concesso in licenza e non interferiscono con i segnali Wi-Fi tradizionali nelle bande da 2.4 GHz e 5 GHz né con reti cellulari.
- White-Fi si avvale delle frequenze liberate dalla televisione in banda UHF (*digital dividend*).
  - L'uso dello spettro *digital dividend* è regolato in modo diverso nei diversi stati (900 MHz negli Stati Uniti, 850 MHz in Europa e 700 MHz in Cina).
- HaLow (*Low Power, Long Range*) estende il Wi-Fi nella banda a 900 MHz, consentendo la connettività a bassa potenza necessaria per le applicazioni IoT, compresi sensori e dispositivi indossabili.
  - HaLow offre diverse funzionalità di risparmio energetico, come *Target Wake Time* (TWT) e *Traffic Indication Map* (TIM), che consentono ai dispositivi di comunicare a intervalli selezionati, risparmiando così la carica della batteria.

802.11ax

- IEEE 802.11ax, commercializzato come Wi-Fi 6 da Wi-Fi Alliance, è uno standard di specifiche IEEE 802.11, in attesa di una distribuzione completa alla fine del 2019 (wireless ad alta efficienza).
- 802.11ax è progettato per funzionare in tutte le bande ISM tra 1 e 6 GHz quando diventano disponibili per l'uso 802.11, oltre alle bande 2.4 e 5 GHz già assegnate.
- Nuovi parametri
  - Δf=78.125 kHz.
  - Banda: 20, 40, 80, 160 MHz.
  - NFFT: (1, 2, 4, 8) · 256.
  - Portanti utili alle diverse bande: (9, 18, 37, 74) · 26.
  - CP: 0.8, 1.6, 3.2 µs. La durata del simbolo è T=12.8 µs.
  - Modulazione/codifica più efficiente: 1024 QAM, R_c=5/6.
  - Bit rate utile massima: 9.4 Gbit/s.

Tabella riassuntiva

Standard	802.11a	802.11g	802.11n	802.11ac	802.11ax	802.11af	802.11ah	802.11ad
Release	9/99	6/03	10/09	12/13	9/19	2/14	12/16	12/12
Frequenza [GHz]	5	2.4	2.4, 5	5	2.4, 5, 6	<1	0.9	60
Bit Rate [Mbit/s]	54	54	600	6933	9431	426.7 (a) 568.9 (b)	346.7	4620
Tecnica	OFDM	OFDM	OFDM	OFDM	OFDM	OFDM	OFDM	SC-FDM
Banda [MHz]	20	20	40	160	160	4x(6,7) (a) 4x8 (b)	1-16	2640
Δf [kHz]	312.5	312.5	312.5	312.5	78.125	41.7 (a) 55.6 (b)	31.25	5156.25
Distanza [m]	100	100	100	50	100	3000	1000	10
Flussi MIMO	-	-	4	8	8.	4 4 canali	4	
					Wi-Fi 6	White-Fi	HaLow	Beam forming