TRABAJO ESPECIAL DE GRADO

COMPARACIÓN ENTRE LOS ESTÁNDARES 802.11 E HIPERLAN2

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Rangel C., Johnny.
para optar al título de
Ingeniero Electricista

Caracas, 2008

TRABAJO ESPECIAL DE GRADO

COMPARACIÓN ENTRE LOS ESTÁNDARES 802.11 E HIPERLAN2

Tutor Académico: Aldo Roveri

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Rangel C., Johnny.
para optar al título de
Ingeniero Electricista

Caracas, 2008

DEDICATORIA

Dedico este trabajo a los que me han dado sus bendiciones:

"A Dios y a mis padres: María Eva e Ismael"

AGRADECIMIENTOS

Para empezar quiero agradecer a Dios por ser mi guía espiritual en todos los momentos de mi vida y mandarme a este mundo de la mano, de mis padres: Eva e Ismael, a quienes agradezco sus orientaciones y cuidados. Agradezco también a mis hermanos Juan Carlos, Ismael Dario y María de los Ángeles, por toda la colaboración, comprensión y afecto incondicionado en todos estos años. También agradezco a mis amigos más cercanos en los últimos años de la carrera Irene Salas, Hector Nuñez, Ambar Azocar, Manuel Martinez y Freddy Da Silva.

Agradezco a la Universidad Central de Venezuela, en particular a la Escuela de Ingeniería Eléctrica, donde he seguido los primeros pasos de la carrera de ingeniería. Igualmente, agradezco a la Università di Roma La Sapienza, en particular a la Facoltà d'Ingegneria, por permitirme participar en el convenio de doble titulación, con lo cual he alcanzado el título de la Laurea Specialistica in Ingegneria delle Telecomunicazioni, convirtiéndome en Doctor en Ingeniería de las Telecomunicaciones.

Rangel C., Johnny.

COMPARACIÓN ENTRE LOS ESTÁNDARES 802.11 E HIPERLAN2.

Tutor Académico: Aldo Roveri. Tesi. Università degli studi di Roma La Sapienza. INFOCOM. Ingegneria delle Telecomunicazioni. Tesis. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. 156 h. + anexos.

Palabras Claves: Estudio comparativo, comparación, Estándares, Estándar IEEE 802.11, Estándar Hiperlan2 (HIgh PErfomance Radio Local Area Network), IEEE (Institute for Electric and Electronic Engineering), ETSI (European Telecommunications Standards Institute), MAC (Medium Acces Control), QoS (Quality of Service), OFDM (Orthogonal Frequency-Division Multiplexing), DSSS (Direct Sequence Spread Spectrum), FHSS (Frequency Hopping Spread Spectrum).

Resumen. Se plantea el estudio del estandar 802.11 e Hiperlan2. Ambos estándares están relacionados en la tecnología de redes inalámbricas donde el estándard 802.11 es desarrollada por la IEEE y el estándar Hiperlan2 es desarrollada por la ETSI. Se realiza la comparación de los estándares en la parte técnica como es la frecuencia de operación, throughput, la topologias de redes, la tecnología de acceso y en la QoS, también en la parte económica y en el consumo de potencia, para esto se desarrollo el estudio en dos productos que son el Atheros para el Hiperlan2 y Broadcom para el 802.11g específicamente.

INDICE GENERALE

INDICE DELLE FIGURE

INDICE DELLE TABELLE

INTRODUZIONE

Scopo del presente lavoro di tesi è stato lo studio ed il confronto tra alcuni standard di comunicazione wireless nell'ambito della realizzazione di reti locali di computer (Wireless LAN). Il confronto è stato effettuato a livello di protocollo e particolare attenzione è stata rivolta al sottolivello MAC (Media Access Control).

Le comunicazioni wireless, ed in particolare il Wireless Networking, rappresentano una tecnologia in rapida espansione che consente all'utente un accesso a reti e servizi senza necessità di cablaggi. Possiamo pensare, ad esempio,ad un utente provvisto di una serie di dispositivi, generalmente indipendenti l'uno dall'altro, quali il telefono cellulare, il computer portatile, il PDA e cosi via ed immaginare una situazione in cui questi dispositivi possano interagire fra di loro, ad esempio per condividere documenti presenti sul proprio computer portatile durante una riunione oppure per ricevere la posta elettronica sul PDA invece che sul computer fisso e tutto ciò senza necessità di alcun cablaggio.

Possiamo pensare ad operazioni più "quotidiane" come entrare in un centro commerciale e veder comparire sul nostro PDA le ultime novità e le offerte del giorno oppure scaricare sul computer portatile mappe ed informazioni turistiche mentre si passa un casello autostradale o si sosta in una stazione di servizio. Tutto questo oggi è già possibile dal punto di vista tecnologico e le sperimentazioni sono già state avviate con successo in molte parti del mondo, Italia compresa. Le reti locali wireless sono senza dubbio uno dei possibili fulcri dell'attuale e futura innovazione tecnologica.

Ovviamente l'approccio wireless nella realizzazione di reti di computer presenta dei vantaggi ma anche degli svantaggi rispetto al classico approccio cablato .Questi aspetti saranno illustrati nel Capitolo1 di questa tesi, insieme ad una panoramica sui vari "tipi" di comunicazione wireless, distinti sia in relazione ai vari campi di applicazione che in relazione ai vari mezzi trasmissivi che si possono usare per eliminare la presenza dei cavi.

In seguito, nel Capitolo 2 e Capitolo 3, vedremo una panoramica generale sugli standard wireless attualmente disponibili per la realizzazione di Wireless LAN, specificamente lo standard 802.11 e Hiperlan2 rispettivamente, mentre nel Capitolo 4 e Capitolo 5 analizzeremo in dettaglio le caratteristiche dei protocolli scelti come obiettivo della tesi, cioè 802.11 e Hiperlan2.

CAPITOLO I

WIRELESS

1.1 Vantaggi e svantaggi dell'approccio Wireless

In via teorica, gli utenti di una rete locale wireless vogliono usufruire degli stessi servizi e vorranno disporre delle stesse potenzialità a cui una rete cablata li ha abituati. In pratica, l'equivalenza tra i due approcci wireless e wired, è una sfida aperta. In particolare l'approccio wireless, a fronte di innegabili vantaggi, è soggetto ad alcuni limiti non presenti nell'approccio cablato. Osserviamo i punti chiave del confronto tra i due approcci.

1.1.1 Mobilità

La libertà di movimento è uno dei vantaggi maggiori dei terminali wireless nei confronti di quelli cablati, che sono statici quando connessi alla rete locale. La mobilità impone peró la necessità di considerare, a livello di sviluppo di sistemi, il problema dell' "handoff". In una wireless LAN ogni terminale ha un'area di copertura chiamato "cella", sfruttando un paradigma delle reti di telefonia cellulare; in teoria, le celle di una stessa rete si sovrappongono e quindi, per la maggior parte del tempo, un terminale si trova all'interno della cella di uno o più terminali. Se i terminali sono mobili, essi devono poter passare da una cella ad un'altra in maniera "trasparente" e senza perdere la connessione alla rete. Questo processo di passaggio è detto appunto handoff.

Grazie alla mobilità dei terminali è più facile la gestione della loro posizione ovvero è agevolata la scalabilità delle reti. Di solito in fase di progetto di nuovi edifici, si potrebbe considerare la possibilità di cablare gli ambienti dedicati alla presenza di nodi di una rete locale (uffici, centri di calcolo e cosi via). È ovvio che tutto diventa più difficile per edifici già esistenti e per cui non è stata prevista la suddetta possibilità. Quest'ultima situazione è invece facilmente gestibile con le reti locali wireless. È notevolmente più semplice inoltre l'installazione di una rete locale

laddove limiti ambientali e strutturali impedirebbero l'installazione e la gestione di una rete locale cablata standard (ad esempio strutture culturali quali musei ed edifici storici da salvaguardare).

1.1.2 Allocazione delle frequenze

Tutti gli utenti di una stessa rete locale wireless devono operare su una banda di frequenza comune, a prescindere dal mezzo trasmissivo scelto. Le bande di frequenza dedicate a particolari applicazioni devono ,di solito, essere approvate e necessitano di una licenza. Inoltre questa regolamentazione può variare da paese a paese. Questo problema è stato risolto dagli odierni standard per wireless LAN, i quali usano delle particolari bande di frequenza accessibili nella maggior parte dei paesi senza bisogno di alcuna licenza. La tabella 1.1 riassume le bande di frequenza che non hanno bisogno di licenza:

Banda	Mezzo Trasmissivo	Limiti	Normativa
ISM	Onde Radio in Spread Spectrum	2.400 - 2.4835 GHz	FCC CFR47 Part 15 in USA e Canada, E.T.S. 300-328 in Europa, Giappone ed altri paesi aderenti.
U-NII	Onde Radio	5.725 - 5.850 GHz	FCC CFR47 Part 15 in USA e Canada, E.T.S. 300-328 in Europa, Giappone ed altri paesi aderenti.
N/A	Infrarosso	Spettro visibile, circa 850nm	Tutto lo spettro e' liberamente utilizzabile in tutti i paesi.

Tabella 1.1: Bande tipicamente utilizzate per applicazioni WLAN

1.1.3 Interferenza e Affidabilità

L'interferenza nelle comunicazioni wireless può essere causata dalle cosiddette collisioni, ovvero trasmissioni simultanee da parte di due o più terminali wireless nella stessa banda di frequenza. In realtà il problema dell'interferenza e' più ampio e coinvolge anche dispositivi di uso comune che non hanno nulla a che vedere con le wireless LAN ma che possono causare non pochi problemi al funzionamento di queste ultime (ad esempio, un comune forno a microonde che opera nella banda 2.4-

2.5 GHz). L'affidabilità del canale di comunicazione è misurata in BER (Bit Error Rate). Questo valore indica il numero di bit che hanno presentato un errore relativamente al numero totale di bit ricevuti per una trasmissione. Di solito viene espresso con una potenza negativa del dieci e dà un'indicazione di quante volte un pacchetto (o un'altra unità informativa) dev'essere ritrasmessa a causa di un errore.

1.1.4 Riservatezza dei dati

In una rete cablata il mezzo di trasmissione può essere reso sicuro fisicamente e l'accesso alla rete può essere controllato facilmente. In una wireless LAN, invece il mezzo trasmissivo è aperto a tutti i terminali wireless che si trovano nel raggio d'azione di un trasmettitore ed è perciò più difficile gestire la sicurezza sia delle trasmissioni che dell'accesso alle varie reti. La riservatezza dei dati e la protezione degli accessi sono di solito realizzati tramite crittografia a vari livelli. Alcune conseguenze dell'adozione di un certo grado di sicurezza indurranno probabilmente una certa riduzione delle prestazioni insieme ad un aumento dei costi dei dispositivi.

1.1.5 Consumo di potenza

I dispositivi di una rete cablata standard di solito sono alimentati dalla tensione di rete. I dispositivi wireless invece, dovendo essere portatili nonché mobili, sono di solito alimentati a batteria. Essi devono perciò essere progettati con la massima attenzione per quanto riguarda l'efficienza energetica.

1.1.6 Sicurezza degli utenti

Sono in corso da diverso tempo molteplici studi sui problemi che le emissioni RF (Radio Frequenza) potrebbero causare alla salute dell'utente. Le reti devono perciò essere progettate per minimizzare la potenza trasmessa dai dispositivi di rete. Per quel che riguarda i dispositivi wireless che utilizzano la tecnologia IR (Infra Red) i trasmettitori ottici devono essere progettati, ed in seguito installati, in modo da evitare danni alla vista.

1.1.7 Throughput

Dal punto di vista del throughput le wireless LAN, a causa di limiti sia fisici che di banda disponibile, partono svantaggiate rispetto alle reti cablate ma, nel corso degli anni le tecnologie che consentono la realizzazioni di wireless LAN sono migliorate, fino a poter disporre oggi di terminali wireless che possono comunicare ad una velocità di circa 54 Mbit/s.

1.2 Strutture tipiche e tecnologie per Wireless LAN

Le Wireless LAN forniscono tutte le funzionalità delle LAN cablate ma senza richiedere alcun cablaggio fisico. Possiamo distinguere sostanzialmente due tipi di configurazione per le WLAN ovvero

Reti Ad Hoc

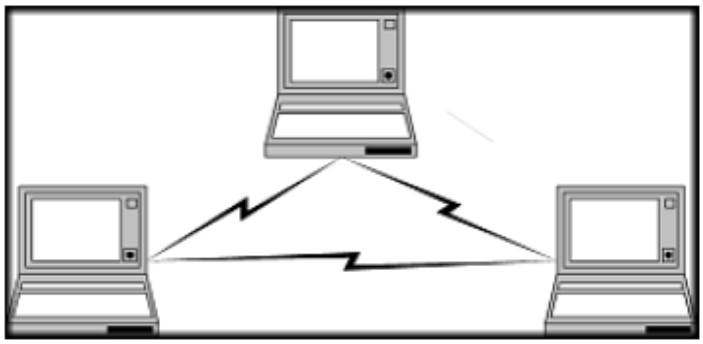


Figura 1.1: WLAN Ad Hoc

Reti con Infrastruttura

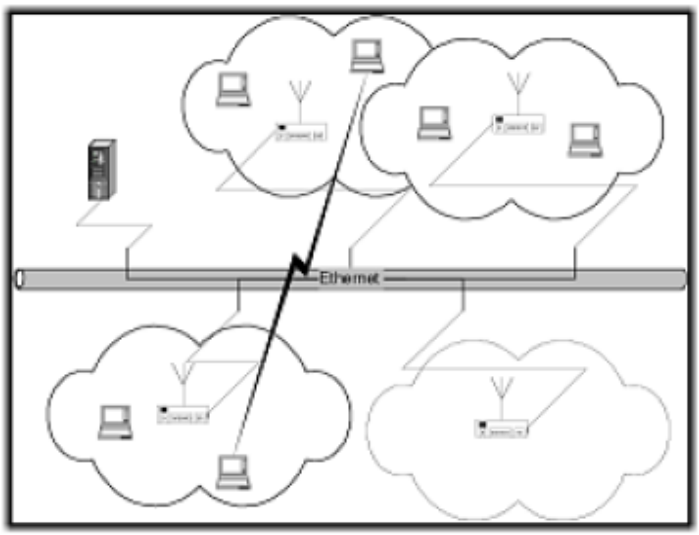


Figura 1.2: WLAN con Infrastruttura

La topologia "Ad Hoc" consiste nell'associazione spontanea di un gruppo di terminali con lo scopo di realizzare delle comunicazioni senza il sostegno di un'infrastruttura di rete ovvero di un coordinamento da parte di un particolare terminale. La comunicazione avviene quindi direttamente tra i terminali e l'area di copertura è limitata dal range dei singoli terminali. Questa struttura non prevede la connessione con una rete cablata ed è quindi costituita soltanto da terminali di tipo wireless.

La topologia "Infrastructured", al contrario, viene realizzata per fornire agli utenti dei servizi particolari (ad esempio la connessione con una rete LAN cablata preesistente o con reti WAN come Internet), oppure per aumentare l'area di copertura della rete WLAN. La comunicazione tra i terminali viene coordinata da un terminale particolare che gestisce anche i suddetti servizi aggiuntivi.

1.3 Tecniche Trasmissive

Dal punto di vista tecnologico, rispetto al mezzo trasmissivo utilizzato i dispositivi si dividono in 3 categorie principali:

IR WLAN

Le comunicazioni wireless che utilizzano la porzione dello spettro denominata "infrarosso", sono comunemente utilizzate per una vasta gamma di dispositivi di controllo remoto. Di recente, le suddette comunicazioni ottiche sono state oggetto di studio anche per quel che riguarda le applicazioni nel campo delle reti di computer. Come per qualsiasi soluzione tecnica, anche questa presenta vantaggi e svantaggi. Innanzitutto, come visto anche in tabella 1.1, lo spettro infrarosso è virtualmente illimitato e questo può permettere il raggiungimento di un'elevata capacità trasmissiva. Inoltre lo spettro infrarosso è immune da problemi di licenze. La radiazione infrarossa ha delle particolari caratteristiche che la rendono interessante per alcuni tipi di configurazione WLAN. Ovviamente tale radiazione non può oltrepassare muri o altre superfici opache, ma, grazie alle sue proprietà di riflessione, può essere riflessa diffusamente da oggetti colorati. Perciò si può realizzare una WLAN che copra un'intera stanza usando la riflessione del soffitto o delle pareti. Operando in questo modo, ad esempio, sono nulle le interferenze tra due WLAN operanti in ambienti adiacenti. Infine, il costo delle apparecchiature IR è relativamente basso cosi come la loro complessità. Questo mezzo trasmissivo presenta anche degli svantaggi : essendo una radiazione luminosa, è soggetta ad interferenza da parte di tutte le altre sorgenti luminose quali luce solare o luce artificiale. Per acquisire maggiore robustezza nei confronti di queste interferenze si potrebbe pensare di aumentare la potenza dei trasmettitori ma quest'ultima è comunque limitata da problemi di consumo di potenza e dai pericoli derivanti dall'uso dei raggi infrarossi.

Spread Spectrum WLAN

Il mezzo trasmissivo utilizzato è la Radio Frequenza. Attualmente la tecnica dello spread spectrum è quella più usata per la realizzazione di WLAN. Questa tecnica è stata inizialmente sviluppata per usi militari, proprio perchè l'idea che sta alla base dello spread spectrum è quella di "espandere" il contenuto informativo di un segnale su una banda maggiore di quella richiesta per rendere l'intercettazione più difficile.

Questa non è l'unica ragione del successo della tecnica dello spread spectrum: i trasmettitori spread spectrum utilizzano gli stessi livelli di potenza dei trasmettitori narrowband ma, poichè lo spettro dei segnali è molto più ampio, la loro densità spettrale di potenza è notevolmente più bassa di quella dei trasmettitori narrowband. Dunque, i segnali spread spectrum e quelli narrowband possono occupare la stessa banda con bassissima interferenza.

Come tutti i dispositivi che utilizzano un mezzo trasmissivo RF, anche i dispositivi spread spectrum WLAN sono soggetti al problema cosiddetto "multi-path fading". Questo termine indica la situazione nella quale un segnale RF arriva ad un ricevitore da una serie di singoli percorsi di propagazione a causa delle riflessioni del segnale trasmesso su oggetti stazionari o in movimento. La lunghezza dei suddetti percorsi di propagazione è generalmente diversa e perciò i vari segnali arrivano al ricevitore con diversi ritardi. Questi ritardi si traducono in differenze di fase sui segnali. Il segnale risultante al ricevitore è la somma vettoriale dei segnali componenti e quindi tipicamente si hanno delle variazioni di ampiezza che hanno dato origine al termine "fading" poichè è molto probabile che l'ampiezza del segnale risultante sia più bassa di quella del segnale trasmesso.

La tecnica di spread spectrum può essere implementata in vari modi. Cronologicamente la prima implementazione è stata il cosiddetto frequency hopping spread spectrum mentre attualmente si preferisce usare la tecnica direct sequence spread spectrum. In generale si usa il modello mostrato in figura 1.3:

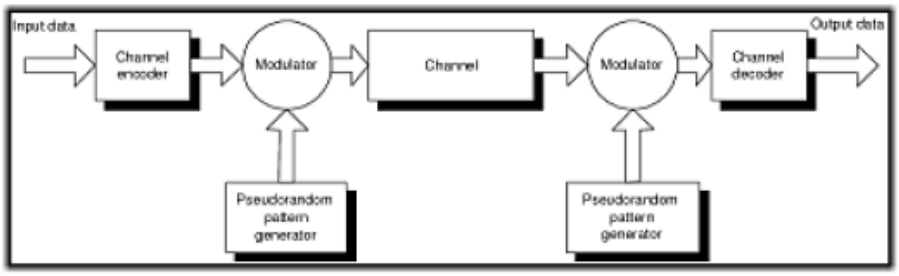


Figura 1.3: Modello generico di un sistema di comunicazioni Spread Spectrum

I dati vengono inviati ad un channel encoder che produce un segnale analogico con una banda relativamente stretta attorno ad una frequenza centrale.

Questo segnale viene poi modulato usando una sequenza casuale di cifre detta pseudorandom sequence ed è proprio questa modulazione che incrementa significativamente la banda del segnale che dev'essere trasmesso.

Dal lato del ricevitore, si usa la stessa pseudorandom sequence per demodulare il segnale spread spectrum. Infine il segnale viene inviato al channel decoder per recuperare il contenuto informativo. Osserviamo ora più in dettaglio le tecniche che implementano lo spread spectrum.

**Frequency Hopping Spread Spectrum*

Questa implementazione consiste nel trasmettere il segnale usando una sequenza pseudo casuale di frequenze radio, "saltando" di frequenza in frequenza ad intervalli di tempo fissati (ovvero con uno specifico "hop rate"). Dall'altro lato del canale, solo i ricevitori che conoscono la particolare sequenza di hopping del trasmettitore possono ricevere correttamente l'informazione.

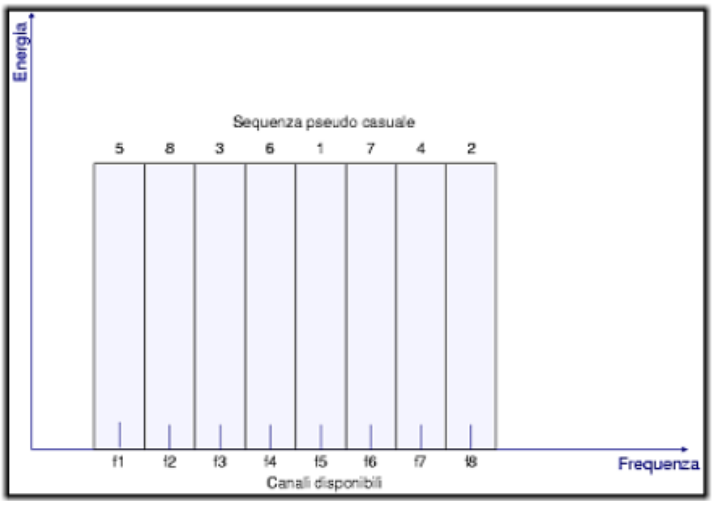


Figura 1.4: Allocazione dei canali e sequenza pseudocasuale

La figura 1.4 mostra come vengano allocati un certo numero di "canali" per il segnale FH.

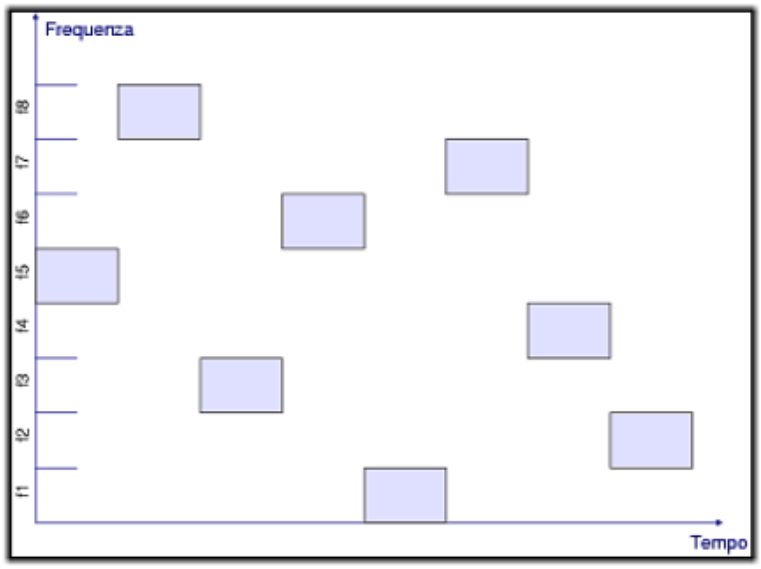


Figura 1.5: FHSS: uso del canale nel dominio del tempo

Come si vede dalla figura 1.5, il trasmettitore opera su una frequenza alla volta per un periodo di tempo prefissato, durante il quale uno o più bit vengono trasmessi; dopodiché esso continua a trasmettere ma "saltando" alla frequenza che viene immediatamente dopo nella sequenza di hopping prestabilita in maniera "pseudo casuale".

**Direct Sequence Spread Spectrum*

Ogni singolo bit d'informazione del segnale originale viene codificato con un codice rappresentato da una sequenza di bit detta "chipping code". Questo processo detto "spreading" espande il segnale su una banda più ampia di quella richiesta per la trasmissione e tale espansione è direttamente proporzionale al numero di bit che compongono il chipping code. La sequenza di spreading è generata ad una velocità più alta rispetto al data rate del segnale informativo originale. Nel trasmettitore, il segnale informativo viene combinato in qualche modo con il chipping code (di solito si compie una operazione di OR Esclusivo (XOR) tra i due segnali). In seguito questa combinazione viene convertita in un simbolo che viene modulato e trasmesso. Dal lato del ricevitore si effettua l'operazione inversa (detta "De-spreading") per ottenere il segnale originario. Osserviamo le seguenti figure :

Figura 1.6: DSSS: spettro dei segnali trasmesso e ricevuto

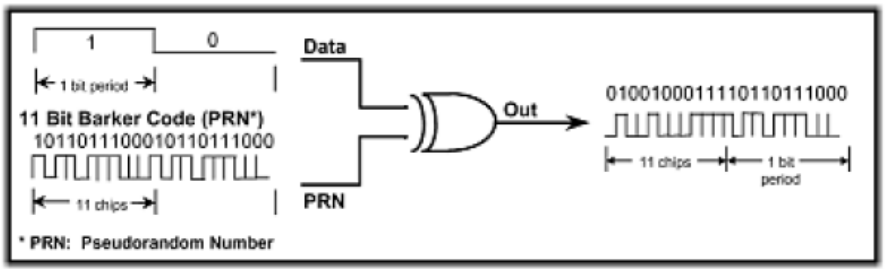


Figura 1.7: DSSS: spreading dei dati

La figura 1.7 si riferisce in particolare all'operazione di spreading mediante sequenza di Barker, che analizzeremo in dettaglio nel capitolo dedicato allo standard IEEE 802.11.

Volendo fare un confronto tra le due tecniche possiamo osservare che :

- I sistemi FH sono suscettibili al rumore durante un singolo "slot" ma a lungo termine possono realizzare una comunicazione quasi senza errori poichè la comunicazione si sposta lungo tutta la banda. I sistemi FH sono più semplici di quelli DS nel senso che gli schemi di modulazione utilizzati sono più semplici e quindi richiedono una minore complessità dal lato del ricevitore. A fronte di questi aspetti positivi dei sistemi FH, osserviamo che il loro data rate massimo è condizionato dall'ampiezza dei canali e, sfruttando tutta la banda a loro disposizione, tendono a causare maggiori interferenze su altri sistemi.
- Il vantaggio principale dei sistemi DS è la possibilità di ottenere data rate più alti rispetto ai sistemi DS usando schemi di modulazione più complicati.

Comunque, in generale, i metodi di modulazione usati nei dispositivi DS complicano la circuiteria dal lato del ricevitore.

- La situazione attuale del mercato WLAN basati su Spread Spectrum vede una quasi completa predominanza dei sistemi DS sui sistemi FH.

OFDM

Un'altra tecnica trasmissiva, è Orthogonal Frequency-Division Multiplexing(OFDM), un tipo di modulazione multi - portante, dove il flusso di dati è suddiviso in diverse sottoportanti, uniformemente spaziate e ortogonali tra di loro. Questa tecnica l'analizzeremo in dettaglio nel capitolo dedicato allo standard Hiperlan2.

Il vantaggio primario dell'OFDM rispetto agli schemi a singola portante è la robustezza fronte alle variazioni del segnale e alle condizioni di propagazione, a parità di diminuzione della velocità di trasmissione.

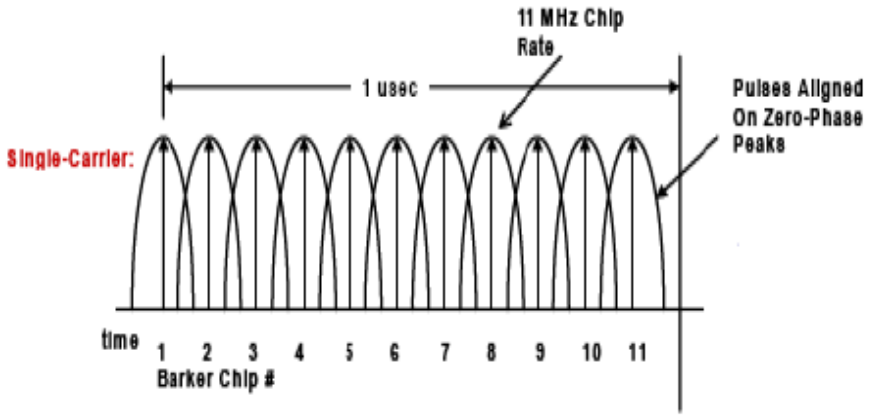


Figura 1.8: Spettro di una singola portante OFDM

CAPITOLO II

STANDARD 802.11

Lo scopo dello standard IEEE 802.11 è quello di "fornire connettività wireless a dispositivi o stazioni che richiedono un'istallazione rapida, siano essi portatili o palmari o ancora montati su veicoli mobili all'interno di una "local area" [1]. Il suddetto standard definisce le funzioni e i servizi richiesti ai dispositivi compatibili con esso per operare all'interno delle reti ad hoc e con infrastruttura, anch'esse compatibili con lo standard.

Esso definisce delle procedure MAC e tecniche di trasmissione dei segnali attraverso un livello fisico (PHY) che potrà essere la radio frequenza (RF) o la radiazione infrarossa (IR). La comunicazione è "orientata al pacchetto". Vengono descritte anche delle procedure per fornire un certo livello di riservatezza delle informazioni.

Una caratteristica molto importante del protocollo definito dallo standard IEEE 802.11 è che un dispositivo mobile può comunicare con altri dispositivi, fissi o mobili, in maniera trasparente, ovvero, al di sopra del livello MAC, un dispositivo IEEE 802.11 viene visto come un qualsiasi dispositivo appartenente ad una LAN IEEE 802.x e offre dei servizi comparabili con quelli offerti da un dispositivo 802.x appunto. In altre parole la mobilità dei dispositivi viene gestita a livello MAC.

2.1 Gli standard IEEE 802.11

Nel 1997 l'istituto IEEE (*Institute for Electric and Electronic Engineering*), approvò uno standard per wireless LAN denominato "802.11", che specificava la realizzazione di dispositivi capaci di ottenere 1 o 2 Mbps in termini di velocità di trasferimento. Lo standard specifica il livello MAC e il livello PHY per la

trasmissione nella banda ISM 2.4 GHz. La banda utilizzata si estende da 2.4 GHz fino a 2.4835 GHz in Nord America e Europa, mentre in Giappone le normative vigenti impongono una banda da 2.471 GHz a 2.497GHz. Due anni più tardi, in seguito agli ottimi risultati ottenuti da produttori quali Lucent Technologies e Harris Semiconductor (ora Intersil Corp.), l'istituto IEEE ratificò un nuovo standard, con prestazioni migliori, denominato IEEE 802.11b; esso permetteva di ottenere 11 Mbps in termini di velocità di trasferimento ed è lo standard su cui sono basati la maggior parte dei dispositivi attualmente disponibili sul mercato. In realtà IEEE 802.11b non è uno standard "ex novo", bensì specifica delle modifiche alle tecniche di modulazione (e quindi al livello PHY) che permettono di elevare la velocità di trasferimento e mantengono comunque la compatibilità all'indietro verso i dispositivi IEEE 802.11.

Il nome IEEE 802.11(b) risulta un pò troppo ostico per il mercato dell'utente finale e quindi sempre più spesso sui dispositivi attualmente sul mercato si trova la sigla Wi-Fi, contrazione di Wireless Fidelity; Wi-Fi è un marchio di qualità poichè attesta la certificazione del dispositivo da parte della Wi-Fi Alliance. Sempre nel 1999 l'istituto IEEE ratificò le specifiche di un altro standard della famiglia 802.11, la variante denominata 802.11a. Le specifiche riguardano sempre il livello MAC e il livello PHY, ma la banda utilizzata è la U-NII (*Unlicensed National Information Infrastructure*) 5 GHz e, mediante la tecnica di modulazione OFDM (*orthogonal frequency division multiplexing*), i dispositivi realizzati in conformità allo standard IEEE 802.11a possono ottenere fino a 54 Mbps in termini di velocità di trsferimento. Anche in questo caso si usa sempre più spesso la denominazione Wi-Fi5 per indicare i dispositivi compatibili con lo standard IEEE 802.11a.

Attualmente lo stato delle specifiche 802.11 può essere riassunto così:

- IEEE 802.11: opera nella banda di 2.4 GHz, impiegando tecniche di modulazione di tipo DSSS e FHSS, che li permettono di arrivare ad una velocità di circa 2 Mbps.
- IEEE 802.11a: opera nella banda di 5 GHz, impiega uno schema di modulazione di tipo OFDM, che le permette di arrivare ad una velocità di

circa 54 Mbps. Non è interoperabile con la versione successiva IEEE 802.11b. Sono a disposizione 12 canali.

- IEEE 802.11b: anche conosciuto come Wi-Fi (Wireless-Fidelity). Opera nella banda di 2.4 GHz, impiega tecniche di modulazione di tipo DSSS e CCK. Queste le permettono di raggiungere un'alta velocità di trasmissione con un ampio raggio di copertura con lo stesso AP (100 metri @ 11 Mbps). Sono a disposizione 14 canali. A differenza della versione IEEE 802.11a, richiede poche stazioni base per avere un maggiore raggio di copertura.
- IEEE 802.11g: opera nella banda di 2.4 GHz. Complessivamente arriva ad una velocità di trasmissione di circa 54 Mbps. Utilizza lo schema di modulazione OFDM quando la velocità di trasmissione è sopra dei 20Mbps, altrimenti utilizza le tecniche DSSS e CCK. E' più robusto in quanto a sicurezza dalla versione iniziale IEEE 802.11. E' compatibile con la versione IEEE 802.11b. Sono a disposizione 14 canali. Ha un raggio di copertura simile a la versione IEEE 802.11b. E' quello più impiegato attualmente in combinazione con IEEE 802.11b.
- IEEE 802.11e: è il primo standard orientato a soddisfare una Qualità di Servizio, a seconda del tipo di utenza (residenziale o affare). Sono aggiunte caratteristiche di supporto multimediali per farli interoperabili con le versioni IEEE 802.11b e IEEE 802.11a . Può essere implementata in applicazioni di tipo Video on Demand, Audio on Demand, Voice overIP (VoIP) ed accesso Internet ad alta velocità.
- IEEE 802.11i: questa versione aggiunge il meccanismo di cifratura Advanced Encryption Standard (AES), il quale è più robusto dal tradizionale meccanismo di sicurezza Wi-Fi.

In IEEE 802.11, le stazioni base sono chiamate *Access Point* (AP), e la zona di copertura di un access point è denominata *Basic Service Area* (BSA). L'insieme di tutti i terminali serviti dallo stesso AP è chiamato *Basic Service Set* (BSS).Diversi BSS, a loro volta, possono essere interconnessi attraverso un'infrastruttura cablata per formare un *Extended Service Set* (ESS). L'infrastruttura appena descritta è necessaria

per il funzionamento di IEEE 802.11 nella cosiddetta modalità infrastruttura. In alternativa, IEEE 802.11, consente la comunicazione diretta tra i terminali senza infrastruttura nella modalità ad hoc.

2.2 La normativa italiana

Come già accennato, la banda di 2,4GHz non è soggetta a licenze in molti paesi del mondo tra cui l'Italia e può essere utilizzata da chiunque nell'ambito però di severi limiti di emissione di potenza; il limite di emissione in Italia per apparati a "bassa potenza" è pari a 0,1W/mq per la potenza dell'onda piana equivalente61 (più diffusamente noto come limite di 100mW), come stabilito dal decreto ministeriale 381/98 all'articolo 4, comma 2.

La regolamentazione applicata alle attività di telecomunicazioni è quella prevista nel decreto del Presidente della Repubblica num. 447 del 5 ottobre 2001, entrato in vigore dal 1 gennaio 2002, regolamento recante disposizioni in materia di licenze individuali e di autorizzazioni generali per i servizi di telecomunicazioni ad uso privato (supplemento ordinario n.282 alla Gazzetta Ufficiale – Serie Generale n. 300 del 28 dicembre 2001) vengono operate delle modifiche sostanziali in direzione di una liberalizzazione del settore. I termini principali della legge prevedono:

- *Applicazioni indoor* non è necessaria alcuna autorizzazione per l'uso di prodotti radioLan nell'ambito del proprio fondo di proprietà. In questo caso non occorre fare alcuna domanda di autorizzazione e non si pagano tasse. (Si intende fondo di proprietà il singolo sito o più siti contigui appartenenti allo stesso proprietario, soggetto fisico o giuridico, parti dello stesso fondo o più fondi dello stesso proprietario si considerano contigui, anche se separati, purché collegati da opere ermanenti che consentono il passaggio pedonale, il proprio fondo può contenere edifici, piazzati, spazi aperti, ecc... Non è possibile includere nel proprio fondo i collegamenti wireless insistenti sul territorio pubblico come attraversamento di strade, ferrovie fiumi, collegamenti terra-mare e collegamenti tra piattaforme in mare).

- *Applicazioni outdoor* al di fuori del proprio fondo di proprietà è invece necessaria un'autorizzazione generale che si ottiene tramite domanda al Ministero delle Comunicazioni e pagamento di una tassa annuale minima; il sistema potrà comunque essere già installato nel momento in cui l'utente spedisce, via raccomandata A/R, al Ministero la richiesta per ottenere l'autorizzazione; questa richiesta è soggetta al silenzio/assenso da parte del Ministero stesso decorse le quattro settimane stabilite.

Ciò significa che l'utilizzo di reti locali basate su tecnologie wireless, radio o ponti ottici è totalmente di libero uso all'interno del proprio fondo, non è necessario richiedere alcuna autorizzazione e non sono previste imposte.

Per i network che esulano dal fondo di proprietà occorre l'autorizzazione generale soggetta al silenzio assenso.

2.3 L'architettura di una WLAN IEEE 802.11

Una WLAN 802.11 è basata su una architettura cellulare, ovvero l'area in cui deve essere distribuito il servizio viene suddivisa in celle proprio come accade nei sistemi di distribuzione per servizi di telefonia cellulare. Ciascuna cella viene chiamata BSS (*basic service set*). Una BSS è un'insieme di "stazioni" (STA) ovvero dispositivi fissi o mobili compatibili IEEE 802.11. Le STA vengono controllate tramite una coordination function (CF) e lo standard 802.11 ne prevede due:

- **Distributed Coordination Function (DCF)**:
  che è obbligatoria per ogni BSS;
- **Point Coordination Function (PCF)**:
  che invece è opzionale.

Una "coordination function" è in pratica un insieme di regole per l'accesso al mezzo trasmissivo e la realizzazione dei vari servizi offerti dal protocollo e quindi dalle diverse STA. L'attributo "distributed" assegnato al DCF indica l'assenza di un coordinamento centralizzato al funzionamento delle STA di una BSS, ovvero l'accesso al mezzo trasmissivo e il trasferimento dei dati è totalmente distribuito tra le STA di quella BSS. Al contrario, quando in una BSS è attiva la funzione PCF

(ricordiamo che la sua implementazione è opzionale), allora esiste una particolare STA che regola l'accesso al mezzo trasmissivo e la realizzazione dei servizi, e le altre STA devono seguire le regole dettate dalla STA che controlla la BSS.

La configurazione di rete più semplice realizzabile con dispositivi 802.11 è la cosiddetta IBSS (indipendent BSS), che è una rete "ad hoc" formata da almeno 2 STA. Una BSS può a sua volta essere parte integrante di una rete più ampia, la cosiddetta extended service set (ESS). Una ESS è formata da una serie di BSS interconnesse tra di loro tramite un distribution system (DS). Tipicamente il DS potrebbe essere una rete cablata (ethernet o altra). Dal punto di vista logico, la BSS e il DS utilizzano dei mezzi trasmissivi diversi: la BSS utilizza il wireless medium (WM) mentre il DS utilizza il distribution system medium (DSM).

L'architettura IEEE 802.11 è indipendente da un mezzo trasmissivo specifico e quindi il WM e il DSM possono essere uguali ma possono anche non esserlo. In ogni caso le specifiche IEEE 802.11 coprono solo il WM. Le STA connesse al DS vengono dette access point (AP). Lo standard IEEE 802.11 divide i servizi offerti dalle STA in due categorie:

- **Station services (SS)**
- **Distribution system services (DSS)**

I servizi DSS vengono realizzati tramite gli access point e sono dei servizi che permettono al MAC il trasporto dei pacchetti tra due STA che non possono comunicare direttamente poichè non sono nell'area di copertura radio l'una dell'altra. Lo standard definisce anche il concetto di portal. Un portal è un dispositivo che permette l'interconnessione tra una rete LAN 802.11 e un'altra rete 802.x. Questo concetto rappresenta una descrizione astratta di una parte delle funzionalità di un bridge. Anche se lo standard non lo richiede espressamente, la maggior parte delle installazioni riuniscono l'access point e il portal in un'unica entità fisica.

La seguente figura riassume tutti i componenti tipici di un'architettura di rete 802.11:

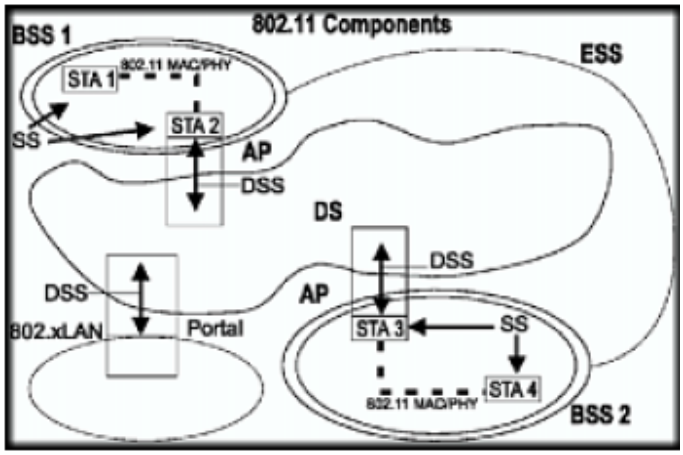


Figura 2.1: L'architettura completa IEEE 802.11

2.4 Servizi offerti dalle reti IEEE 802.11

Abbiamo visto la divisione fatta dallo standard tra station services e distribution system services. Ora analizziamo meglio i singoli servizi e osserviamo innanzitutto la seguente tabella che li riassume mantenendo la distinzione suddetta:

Station Services	**Distribution System Services**
Authentication	Association
Deauthentication	Disassociation
Privacy	Distribution
MSDU delivery	Integration
	Reassociation

Tabella 2.1: IEEE 802.11: servizi disponibili

In tutto vi sono 9 servizi, di cui 6 sono collegati al trasporto dei pacchetti tra le STA (MSDU (MAC *service data unit*) delivery) e 3 vengono usati per controllare l'accesso e la riservatezza delle WLAN 802.11. I servizi sono realizzati tramite uno o più tipi di MAC frame: alcuni saranno realizzati utilizzando dei frame di tipo management, altri da frame di tipo data. In una IBSS (ad hoc network), sono disponibili solo i servizi denominati "station services" (SS).

Authentication

Tramite questo servizio, viene condivisa la reciproca identità tra due STA che vorranno comunicare. Se non verrà stabilito un livello di autenticazione accettabile da entrambe le parti, il processo di autenticazione fallirà. IEEE 802.11 supporta diversi processi di autenticazione: si tratta tuttavia di un'autenticazione a "livello di collegamento" (*link level)*, mentre un'autenticazione ad esempio di tipo "utente-utente" (*user level*) è supportata ma non viene specificata nello standard. Un esempio di schema di autenticazione supportato è lo schema "a chiave condivisa" (*shared key*), ma questo implica che sia implementata l'opzione WEP (*wired equivalent privacy*) di cui parleremo in seguito.

Deauthentication

Questo servizio viene invocato quando dev'essere cancellata un'autenticazione. In un ESS, come vedremo, l'autenticazione è un prerequisito per un altro servizio, l'associazione; dunque al momento della deautenticazione, viene a mancare anche l'associazione. La deautenticazione è una notifica, non una richiesta e quindi non può essere rifiutata da nessuna delle due parti.

Privacy

Per raggiungere un livello di riservatezza dei dati paragonabile a quello di una rete cablata, in cui solo i dispositivi fisicamente connessi alla rete possono ascoltare il traffico, lo standard IEEE 802.11 fornisce la possibilità di cifrare il contenuto dei messaggi trasmessi dalle STA. Questa funzionalità viene ottenuta tramite il servizio privacy. IEEE 802.11 specifica inoltre come opzionale il meccanismo WEP (wired equivalent privacy) per la cifratura dei dati. Il servizio di privacy può essere invocato solo per i frame di tipo data e per alcuni frame che controllano l'autenticazione. Tutte le STA iniziano a funzionare "in chiaro" (senza cifratura), per realizzare i servizi di

autenticazione e privacy. Se il servizio privacy non viene invocato, tutti i messaggi verranno trasmessi non cifrati.

I "*distribution system services*" (DSS) vengono usati per distribuire i messaggi all'interno del "*distribution system*" (DS) e per supportare il concetto di "mobilità".

Distribution

Questo è il servizio principale usato dalla STA 802.11. Viene invocato da ciascun messaggio da o per una STA 802.11 operante in una ESS. Con riferimento alla figura 2.1, consideriamo un messaggio mandato dalla STA1 verso la STA4. Il messaggio viene prima ricevuto dalla STA2 che è l'AP della BSS cui la STA1 appartiene. L'AP invia il messaggio al servizio di distribuzione implementato nel DS, il quale si occupa di distribuirlo alla STA3 (un altro AP) la quale accede al WM per trasferire finalmente il messaggio al destinatario STA4. Come il messaggio verrà trasmesso all'interno del DS non viene specificato da IEEE 802.11: lo standard specifica delle informazioni da fornire al DS per determinare l'AP di "uscita" del suddetto messaggio. Tali informazioni vengono fornite attraverso i 3 servizi: *association, reassociation e disassociation*.

Integration

Questo servizio permette il trasporto delle MSDU tra una WLAN 802.11 e il DS attraverso un portal. Quindi i messaggi inviati da una STA 802.11 che devono essere ricevuti da una LAN preesistente attraverso un portal, invocheranno il servizio di integration prima della distribuzione tramite il DS. Anche questo servizio non viene coperto dallo standard.

Come abbiamo visto, vi sono altri servizi che supportano il servizio di distribuzione (distribution): le informazioni necessarie al corretto funzionamento del servizio distribution vengono fornite dai servizi di "associazione"; cioè prima che un dato possa essere gestito dal servizio distribution, una STA dev'essere "associata".

Per capire il concetto di associazione, è necessario prima capire il concetto di "mobilità".

Vi sono 3 tipi di transizioni che definiscono il concetto di mobilità di un dispositivo IEEE 802.11:

No-transition

Questo tipo di mobilità prevede 2 sottoclassi che sono in genere indistinguibili:

1. Static ovvero nessun movimento.
2. Local movement ovvero movimento nell'area di copertura delle STA con cui stiamo comunicando.

BSS-transition

Questo tipo di mobilità riguarda i movimenti di una STA da una BSS ad un'altra ma sempre all'interno della stessa ESS.

ESS-transition

Questo tipo di mobilità riguarda i movimenti di una STA da una BSS appartenente ad una ESS in una BSS appartenente ad un'altra ESS. In realtà questa possibilità è supportata solo in teoria, poichè IEEE 802.11 non garantisce il mantenimento delle connessioni a più alto livello.

Queste categorie di mobilità sono supportate dai servizi di associazione.

Association

Tramite questo servizio, una STA comunica la propria presenza all'AP della propria BSS. Viene sempre invocato da una STA. Una STA non può associarsi con più di un AP in uno stesso momento, questo per assicurare che il servizio di distribuzione trovi un AP unico per trasportare i messaggi del DS. L'association è sufficiente a gestire la mobilità di tipo "No-transition" ed è necessaria ma non sufficiente a gestire la mobilità "BSS-transition".

Disassociation

Tramite questo servizio viene cancellata un'associazione attualmente in corso. Il DS viene informato della disassociazione dall'AP corrispondente. Può essere invocato sia dalla STA che dall'AP. E' unanotifica, non una richiesta e quindi non può essere rifiutata da nessuna delle due parti.

Reassociation

Per supportare la transizione di tipo "BSS-transition" è necessario invocare il servizio di riassociazione. Tramite questo servizio, viene spostata un'associazione corrente da un AP ad un altro. Questo tiene informato il DS della mappa tra AP e STA quando quest'ultima si sposta da una BSS ad un'altra. La riassociazione permette inoltre di cambiare i parametri di una associazione corrente mentre la STA rimane associata all'AP. La riassociazione viene sempre invocata dalla STA.

La seguente figura illustra le relazioni tra i vari servizi:

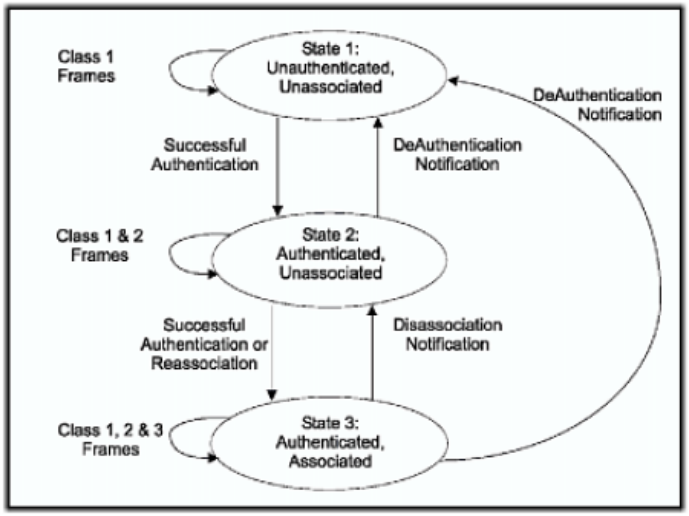


Figura 2.2: Relazioni tra i servizi IEEE 802.11

2.5 Livello MAC dello standard IEEE 802.11

Lo standard IEEE 802.11 specifica un protocollo MAC che comprende una serie di funzioni che realizzano tutte le possibili operazioni di una WLAN 802.11. In

generale, il livello MAC gestisce e mantiene le comunicazioni tra le STA, coordinando l'accesso al mezzo trasmissivo condiviso. Il livello MAC è in pratica il "cuore" di una WLAN 802.11: esso si serve del livello fisico (PHY) per le funzioni di rilevamento della portante (*carrier sensing*), trasmissione e ricezione dei frame 802.11.

2.5.1 Architettura del MAC

L'architettura del MAC IEEE 802.11 può essere descritta dalla figura 2.3:

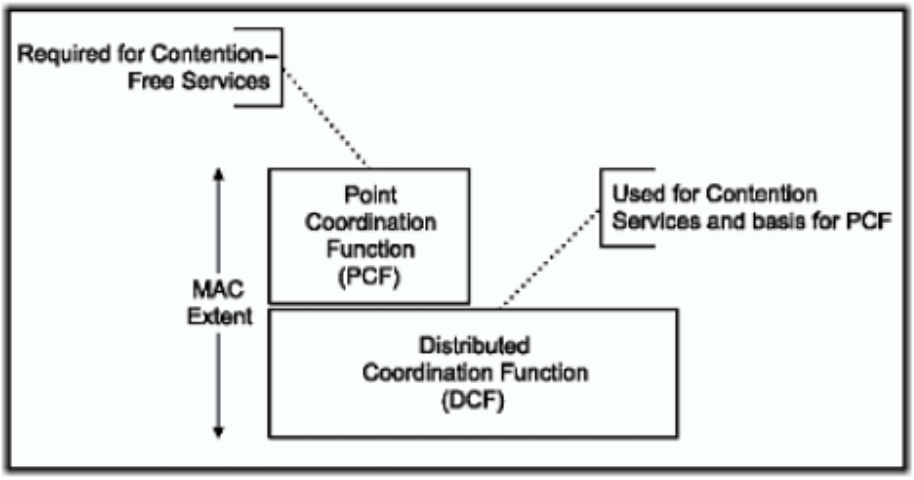


Figura 2.3: Architettura del MAC IEEE 802.11

2.5.2 Distributed Cooordination Function(DCF)

Il meccanismo di accesso base è denominato *Distributed Coordination Function* (DCF), basato sul meccanismo di "accesso multiplo con rilevamento della portante e prevenzione delle collisioni" (*Carrier Sense Multiple Access with Collision Avoidance-CSMA/CA*). Il DCF dev'essere implementato in tutte le STA e viene utilizzato sia nelle reti ad hoc (IBSS) che nelle configurazioni con infrastruttura (AP). Una STA, prima di trasmettere, deve "sentire" il mezzo trasmissivo per controllare che un'altra STA non stia trasmettendo. Se in base alle regole del carrier sensing la STA stabilisce che il mezzo non è occupato, può trasmettere un frame. Se il frame trasmesso era direttamente indirizzato ad un'altra STA (unicast), quest'ultima usa un

immediato positive acknowledgment (*frame ACK*) per indicare la corretta ricezione del frame. Se quest'ultimo frame ACK non viene ricevuto, perchè il mittente non lo riceve oppure perchè il destinatario non è riuscito a ricevere correttamente il dato inviatogli, il mittente programma la ritrasmissione del dato. Si noti che le due situazioni appena descritte, ovvero non ricezione del frame ACK oppure mancata trasmissione dello stesso da parte del destinatario, sono indistinguibili da parte del mittente.

Il protocollo CSMA/CA impone che vi sia un intervallo di tempo specificato tra le trasmissioni di due frame successivi. Questo intervallo viene genericamente chiamato IFS (*Inter Frame Space*). Una STA che vuole trasmettere dovrà assicurarsi che il mezzo trasmissivo risulti libero per l'adeguato IFS prima di provare a trasmettere. Se al contrario il mezzo viene rilevato come "occupato" , la STA deve rimandare la trasmissione fino al termine di quella in corso. Dopo questo ritardo e anche immediatamente dopo una qualsiasi trasmissione avvenuta con successo, una STA deve compiere la cosiddetta procedura di backoff. Questa procedura consiste nel selezionare un ritardo casuale (*random backoff interval*) e rimandare la trasmissione decrementando un contatore (*random backoff interval counter*) ogni volta che il mezzo trasmissivo viene rilevato libero. Quanto appena descritto rappresenta l'accesso base secondo le regole del DCF. E' tuttavia prevista dallo standard una modifica al meccanismo di accesso base, che prevede lo scambio di due piccoli frame di controllo RTS e CTS prima di ogni trasmissione dati, essenzialmente pensata per ridurre ulteriormente le collisioni e ridurre i problemi derivanti dalle situazioni di tipo "nodi nascosti". Questa tecnica è opzionale.

Meccanismo carrier-sense

Per determinare lo stato del mezzo trasmissivo viene usato un meccanismo di carrier-sense (controllo della portante), realizzato dal livello fisico (PHY) a beneficio del MAC; il MAC stesso inoltre, realizza un meccanismo di virtual carrier-sense. Se una STA opera con il metodo di accesso base sommariamente descritto in 2.5.2, allora può avere delle informazioni relative ad una trasmissione in corso da parte di

un'altra STA dal campo "Duration/ID" (vedi 2.8) incluso nell'header dei frame. Tramite questo campo la STA conosce il tempo per il quale il mezzo trasmissivo risulterà ancora occupato, anche in caso di messaggi frammentati su più frame.

Anche nel caso sia abilitato il meccanismo RTS/CTS, viene realizzato il virtual carrier-sense, per mezzo di un contatore denominato NAV (*Network Allocation Vector*), che viene impostato opportunamente tramite le informazioni contenute nei frame RTS e CTS.

Interframe space (IFS)

L'intervallo di tempo tra due frame consecutivi è detto IFS. Lo standard definisce quattro diversi IFS, che definiscono 3 diversi livelli di priorità nella procedura di accesso al mezzo trasmissivo. Più piccolo è il tempo IFS, maggiore sarà la priorità dell'operazione che si basa su quell'IFS. Gli IFS sono definiti come intervalli di tempo sul mezzo trasmissivo e sono indipendenti dalla velocità di trasferimento del canale. Gli IFS saranno differenti per le 3 implementazioni del livello fisico previste dallo standard (*radiazione infrarossa, direct sequence spread spectrum e frequency hopping spread spectrum*).

Short IFS (SIFS)

Questo IFS viene usato per l'acknowledgement (ACK) immediato di un frame, per la risposta di tipo CTS (*clear to send*) and un frame RTS (*request to send*), per delimitare le trasmissioni delle varie MPDU (*MAC protocol data unit*) ovvero le parti in cui vengono frammentate le già citate MSDU se le loro dimensioni eccedono un limite prefissato; viene usato inoltre nella risposta ad un polling del PCF e infine nelle risposte a qualsiasi frame inviato dall'AP durante il *contention-free period* (CFP).

Point coordination function IFS (PIFS)

Questo IFS viene usato dalle STA che operano in PCF per ottenere l'accesso al mezzo trasmissivo all'inizio del CFP.

Distributed coordination function IFS (DIFS)

Questo IFS viene usato dalle STA che operano in DCF per ottenere l'accesso al mezzo e trasmettere frame contenenti dati oppure frame di controllo.

Extended IFS (PIFS)

È il più lungo IFS ed è usato da una stazione che ha ricevuto un pacchetto di cui non è stata in grado di comprendere il contenuto. Questo è necessario per proteggere la stazione (la quale non comprende l'informazione di durata necessaria per il virtual carrier sense) da collisioni con i futuri pacchetti appartenenti al messaggio corrente.

Alcuni IFS sono stabiliti dallo standard in modo assoluto. Altri vengono definiti relativamente ad altre grandezze quali lo slot-time. Lo slot-time è una grandezza molto importante proprio perché è usato come unità di misura di intervalli di tempo quali gli IFS ma anche come unità di misura nel meccanismo del random backoff. L'intervallo di backoff infatti risulta suddiviso in quanti di durata pari al valore slot-time. Si veda a proposito il paragrafo successivo.

Osserviamo dunque alcuni valori derivati dallo standard[2]:

Intervallo	FHSS(frequency hopping spread spectrum)	DSSS(direct sequence spread spectrum)	Hi-rate DSSS	IR(radiazione infrarossa)
SIFS	28μs	10μs	10μs	10μs
Slot Time	50μs	20μs	20μs	8μs

Tabella 2.2: IEEE 802.11: valori degli IFS per i vari PHY

Gli altri IFS possono essere ottenuti con le seguenti formule:

$$\mathbf{PIFS=SIFS\times SlotTime} \quad \mathbf{DIFS=SIFS+2\times SlotTime} \quad (2.1)$$

Random Backoff

Abbiamo visto che il meccanismo carrier-sense dev'essere invocato ogni volta che una STA vuole trasmettere un frame. Se il mezzo trasmissivo è occupato, la trasmissione dev'essere ritardata fino a quando non si trova il mezzo libero per un periodo di tempo continuato maggiore o uguale al DIFS o al EIFS se l'ultimo frame non era stato ricevuto correttamente. Dopo questo intervallo (DIFS o EIFS), e se il contatore di back off (*backoff timer*) non è già pari a 0, la STA genera un periodo di ritardo casuale (*random backoff*), che ritarda ulteriormente la trasmissione. Questo processo è stato previsto per minimizzare le collisioni derivanti dai tentativi di accesso al mezzo da parte di più STA che avevano ritardato la propria trasmissione a causa di uno stesso evento.

La durata del random backoff può essere espressa da:

$$\textbf{BackoffTime=Random()}\times\textbf{SlotTime} \quad (2.2)$$

ove "Random" è un intero pseudocasuale uniformemente distribuito nell'intervallo [0,CW]. CW indica il parametro detto Contention Window, che rappresenta in pratica un'unità di misura per il random backoff. CW è compreso nell'intervallo [CWmin,CWmax], e la sua gestione può essere descritta così:

- CW inizialmente assumerà il valore CWmin. Questo valore, come anche CWmax dipendono dallo specifico PHY.
- I valori che CW può assumere in sequenza sono dati dalle potenze crescenti di 2, meno 1, fino ad arrivare al valore CWmax.
- Ogni STA ha un contatore (retry counter) che viene incrementato ogni volta che un frame non viene trasmessa con successo. Un incremento del retry counter provoca un incremento di CW.
- Se CW raggiunge il valore CWmax, ulteriori tentativi di trasmissione falliti non modificheranno il suo valore.
- CW verrà resettato a CWmin dopo ogni tentativo di trasmissione concluso con successo

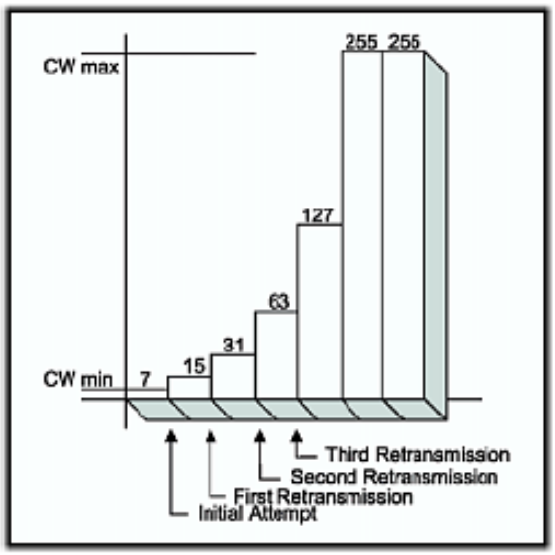


Figura 2.4: Valori e limiti del parametro CW

Alcuni valori dallo standard:

Parametro	FHSS	DSSS	Hi-rate DSSS	IR
CW_{min}	15	31	31	63
CW_{max}	1023	1023	1023	1023

Tabella 2.3: IEEE 802.11: valori dei limiti del CW per i vari PHY

Nella figura 2.5, possiamo vedere una possibile situazione relativa alla procedura di backoff appena descritta.

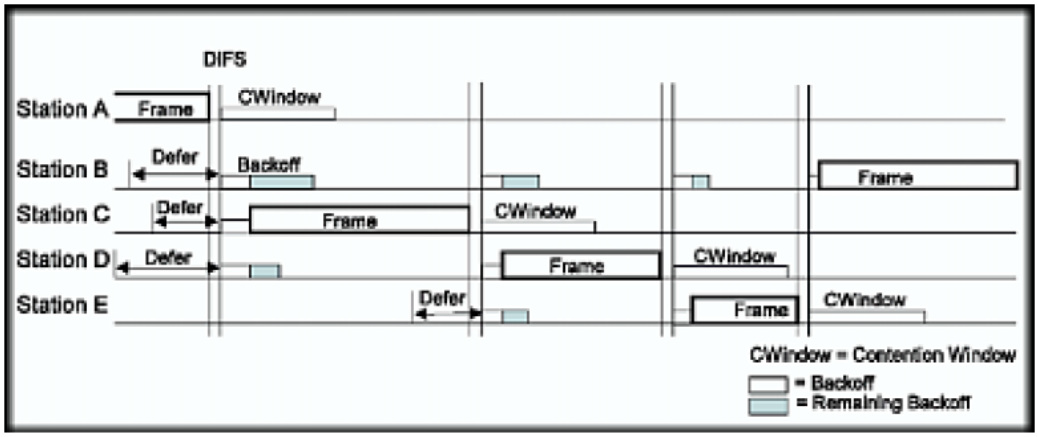


Figura 2.5: Procedura di back off

La STA "A" trasmette un frame mentre le altre STA ritardano a causa di questa trasmissione. Alla fine di quest'ultima, tutte le STA controllano il mezzo trasmissivo per un tempo pari a DIFS, dopo di chè tutte le STA eseguono la procedura di random backoff. Risulta "vincente" la STA "C", che possedeva un random back off minore rispetto alle altre STA concorrenti. Come si vede dalla figura 2.5, il timer di backoff delle STA viene decrementato solo se quando il mezzo risulta libero. Infatti, nel momento in cui la STA "C" vince la contesa per l'accesso al mezzo, il timer di backoff delle STA concorrenti "B" e "D" viene fermato e il suo valore mantenuto. Al termine della trasmissione della STA "C" viene osservato da tutte le STA un ritardo pari a DIFS; successivamente la contesa per l'accesso al canale viene risolta in favore della STA "D", che aveva un valore residuo del random backoff timer minore rispetto alla concorrente STA "B" (si notino le differenze tra le aree più scure in figura).

Procedura di accesso standard

La figura 2.6 illustra il meccanismo di accesso base del DCF:

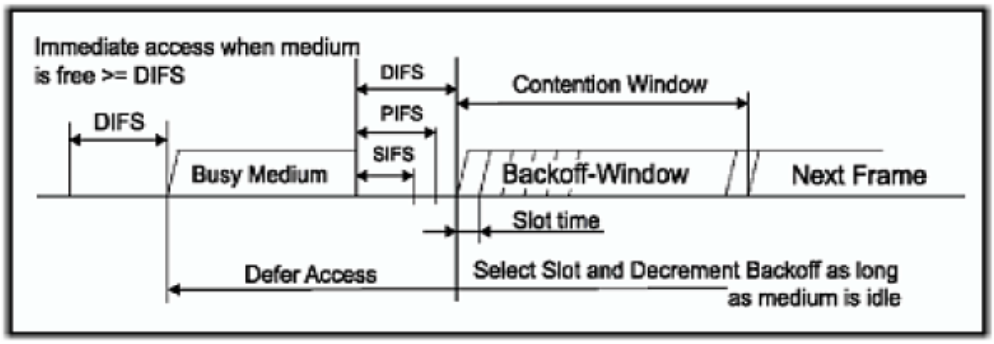


Figura 2.6: Procedura di accesso base

Riassumendo:

- In generale una STA che opera secondo le regole del DCF, trasmette un frame quando rileva il mezzo libero continuamente e per un tempo pari a DIFS (o EIFS).
- Se il mezzo viene invece rilevato come occupato, viene seguita la procedura di back off.

Una caratteristica importante del MAC IEEE802.11 consiste nella cosiddetta capacità di frammentazione/deframmentazione delle unità informative che vengono trasmesse e ricevute dalle STA. Si possono dunque frammentare le MSDU (*MAC Service Data Unit*) e le MMPDU (*MAC Management Protocol Data Unit*), in unità più piccole, che abbiamo finora chiamato frame e che lo standard IEEE 802.11 indica anche con l'acronimo MPDU (*MAC Protocol Data Unit*).

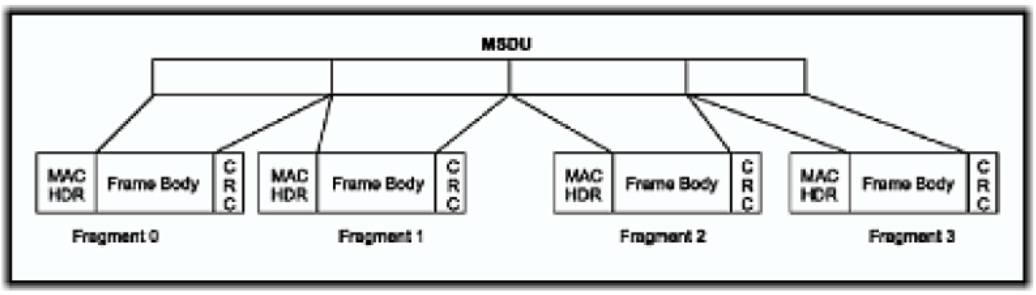


Figura 2.7: IEEE 802.11: frammentazione

La frammentazione delle MSDU e delle MMPDU è prevista per aumentare l'efficienza delle trasmissioni, poichè unità informative più piccole sono più

facilmente trasferibili, anche nel caso che le condizioni del canale siano sfavorevoli (interferenze, traffico elevato etc.).

L'operazione di ricomposizione di una MSDU (o MMPDU) frammentata viene chiamata deframmentazione. Solo le unità informative unicast possono essere frammentate, mentre non è prevista questa possibilità per i messaggi multicast o broadcast.

La frammentazione è gestita tramite il parametro "*FragmentationThreshold*", che definisce la dimensione dei frame nei quali viene frammentata una MSDU.

Possiamo vedere dalla figura 2.8 come una STA che abbia avuto accesso al mezzo trasmissivo, possa usare il SIFS, cioè il più breve degli intervalli di attesa, per trasmettere i vari frammenti di una MSDU, senza quindi dover ricontendere l'accesso al mezzo per ogni singolo frammento:

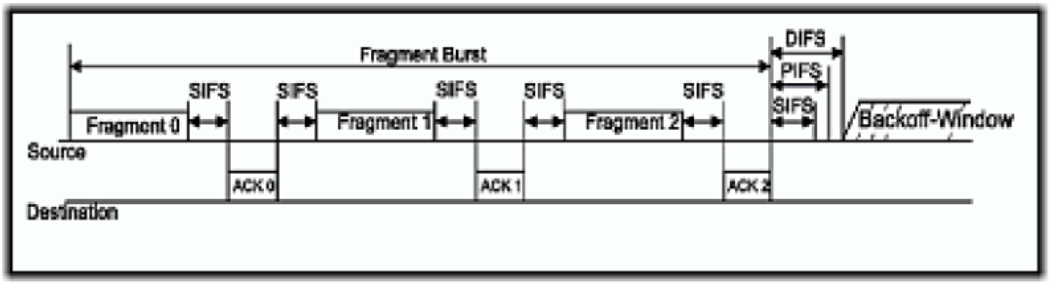


Figura 2.8: Trasmissione fragment-burst

In questo modo, una STA che ha accesso al mezzo continua a trasmettere, ad intervalli di SIFS, le MPDU in cui ha frammentato una MSDU, fino a che queste ultime MPDU non sono finite oppure finchè viene mancato un ACK.

Procedura di accesso con meccanismo RTS/CTS

Nella figura 2.9, osserviamo la procedura di accesso con meccanismo RTS/CTS:

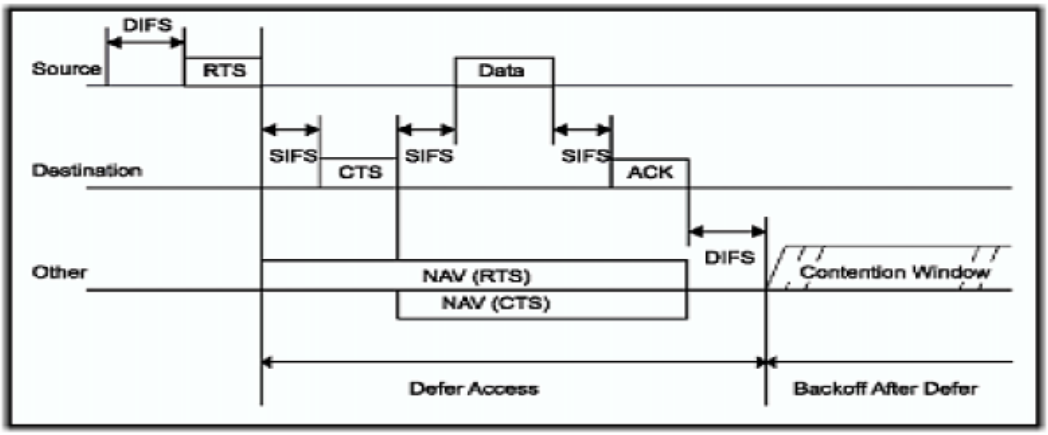


Figura 2.9: Procedura di accesso con meccanismo RTS/CTS

Nodi Nascosti

Si dice che un nodo (STA) A è nascosto ad un nodo B appartenente alla stessa BSS, quando i due nodi sono fuori dalla reciproca portata radio, cioè non possono comunicare direttamente.

Possiamo visualizzare, tramite la figura 2.10, un possibile problema legato alla presenza di nodi nascosti:

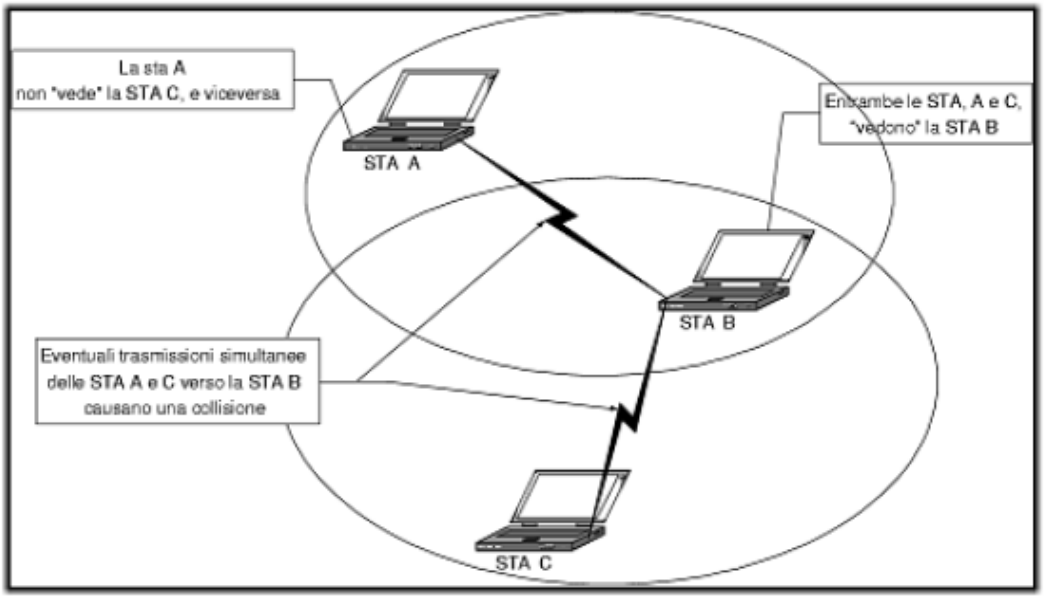


Figura 2.10: Problema dei nodi nascosti

Le STA A e C non sentono le reciproche trasmissioni e, quindi, può capitare che entrambe portino avanti due trasmissioni contemporanee verso la STA B che si trova nel raggio di copertura di entrambe. Ovviamente questo causa una serie di collisioni e la STA B non riceverà correttamente i pacchetti che le altre STA tentano di inviargli. Per ovviare a questo problema si usa il meccanismo RTS/CTS:

- Una STA che volesse trasmettere una MPDU verso un'altra STA (ad esempio in figura 2.10 la STA A vorrebbe trasmettere un dato alla STA B), dovrà prima inviare un frame di tipo RTS diretto alla STA B. Le STA che possono ricevere correttamente tale frame RTS, grazie al campo "Duration/ID" contenuto nell'header di tale frame, aggiusteranno di conseguenza il proprio NAV in modo da deferire l'accesso al mezzo poichè un'altra STA ha iniziato una trasmissione. Nel caso visualizzato in figura 2.10, la STA C non riceve le informazioni contenute nel frame RTS inviato dalla STA A.
- La STA B, ricevuto il frame RTS, risponde con il frame CTS (dopo un intervallo SIFS), comunicando di essere pronta ad accettare dei dati. Il frame CTS verrà stavolta ricevuto dalla STA C, la quale aggiusterà il proprio NAV in base a quanto contenuto nell'header del suddetto frame CTS. Dunque, la STA C, pur non sentendo l'inizio della trasmissione della STA A poichè fuori dal raggio di copertura di quest'ultima, sente comunque la trasmissione della STA B, e, ritarda l'accesso al mezzo trasmissivo fino alla fine della trasmissione in corso.
- Il frame di dati veri e propri sarà inviato esattamente un SIFS dopo la trasmissione del frame CTS, senza controllare il mezzo.

L'uso di questo meccanismo è opzionale, e, poichè provoca un leggero overhead dovuto alla presenza dei 2 frame RTS/CTS, si può configurare in modo che venga attivato solo per le trasmissioni di frame di dimensioni significative. Tutti i frame di dimensione maggiore del parametro RTSThreshold, saranno soggetti al meccanismo RTS/CTS. Se il valore di RTSThreshold è 0, vuol dire che tutti i frame saranno inviati col meccanismo RTS/CTS. Se il valore di RTSThreshold è maggiore della massima

dimensione consentita per le MSDU, allora nessun frame sarà inviato col meccanismo RTS/CTS. Il meccanismo RTS/CTS può essere usato anche in caso di frammentazione delle MSDU.

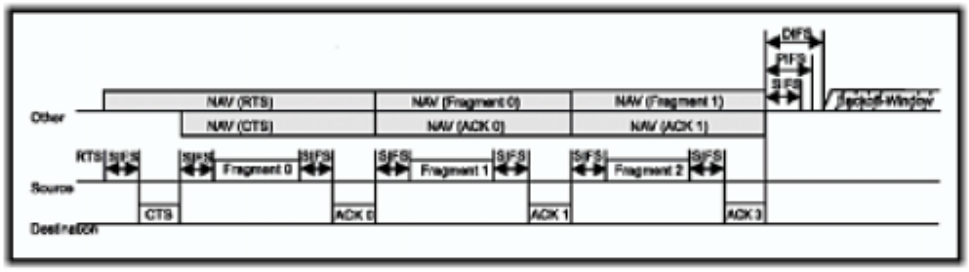


Figura 2.11: Meccanismo RTS/CTS e frammentazione

Come si vede dalla figura 2.11, i frame RTS/CTS vengono scambiati solo per il primo frammento, e, in seguito, viene usato ai fini del settaggio NAV, il campo "Duration/ID" dei frame dati e dei frame ACK che li seguono.

Broadcast e multicast

La trasmissione broadcast (o multicast) di frame dati, in generale non è soggetta al meccanismo RTS/CTS. Questo è vero però solo per i frame in cui il bit ToDS (vedi 2.8) è pari a 0, nel qual caso viene usata la procedura di accesso base e non viene inviato alcun frame ACK. Nel caso in cui un frame broadcast (o multicast) abbia invece il bit ToDS pari a 1, tale frame segue le regole della procedura di accesso con RTS/CTS, questo perchè il suddetto frame è diretto verso l'AP.

La suddetta distinzione in base al valore del bit ToDS si riflette anche sulla ritrasmissione dei frame: solo nel caso in cui ToDS sia pari a 1 è previsto il meccanismo di recupero dei dati non ricevuti correttamente (ovvero la ritrasmissione dei frame).

Trasmissione degli ACK

Tutti i frame unicast di tipo dati richiedono espressamente una "conferma di ricezione", effettuata dal destinatario tramite la trasmissione del frame ACK

(acknowledgment), come abbiamo già accennato. Tale frame dev'essere inviato, a prescindere dallo stato del mezzo trasmissivo, esattamente un SIFS dopo un frame dati. Nel caso in cui il suddetto frame dati abbia il bit ToDS pari a 1, è l'AP che deve inviare il frame ACK. Come abbiamo già visto, non viene inviato alcun ACK per i frame broadcast (o multicast).

La STA che invia un frame dati con richieste di ACK stabilisce che la propria trasmissione è fallita se non riceve un ACK entro il tempo definito dal parametro ACKTimeout.

Procedure di recupero

Il recupero degli errori, ovvero dei frame non ricevuti correttamente, è gestito dalla STA mittente, tramite ritrasmissione dei suddetti frame finchè gli stessi non vengono ricevuti correttamente oppure finchè non viene raggiunto un certo limite (retry limit).

Ogni STA possiede due contatori detti STA short retry count (SSRC) e STA long retry count (SLRC).

Il contatore SSRC viene incrementato ogni volta che fallisce la trasmissione di un frame MAC appartenente ad una MSDU o ad una MMPDU la cui dimensione è minore o uguale al valore RTSThreshold, mentre tale contatore viene resettato quando la suddetta trasmissione avviene con successo.

Il contatore SLRC viene incrementato ogni volta che fallisce la trasmissione di un frame MAC appartenente ad una MSDU o ad una MMPDU la cui dimensione è maggiore al valore RTSThreshold, mentre tale contatore viene resettato quando la suddetta trasmissione avviene con successo. I frame ritrasmessi sono contraddistinti dal valore 1 nel campo Retry.

I tentativi di ritrasmissione di una MSDU o MMPDU finiscono quando il contatore SSRC raggiunge il limite imposto dal parametro ShortRetryLimit, o quando il contatore SLRC raggiunge il limite imposto dal parametro LongRetryLimit. Quando viene raggiunto almeno uno di questi limiti, la MSDU o la MMPDU in questione viene scartata. Lo standard IEEE 802.11 fissa a 7 il valore dei limiti ShortRetryLimit e LongRetryLimit.

Rilevamento dei frame duplicati

Una STA dev'essere in grado di rilevare, a livello MAC, la ricezione di frame già ricevuti. Questo processo è facilitato dal campo Sequence Control che è composto da un numero di sequenza e da un numero di frammento e che è incluso in ogni frame di tipo dati e management. Dunque, le MPDU che fanno parte di una stessa MSDU avranno lo stesso numero di sequenza e le diverse MSDU avranno (con elevata probabilità) un numero di sequenza differente. Il numero di sequenza è generato dalla STA trasmittente ed è parte di una sequenza crescente di interi. La STA ricevente mantiene una cache dei dati <Address 2 - numero di sequenza - numero di frammento> più recenti. La stessa STA scaricherà dunque tutti quei frame che hanno il bit Retry settato e i cui valori <Address 2 - numero di sequenza - numero di frammento> corrispondono ad un record della cache. La STA effettuerà comunque la procedura di ACK (se il frame lo richiede) anche se poi scarterà il frame a causa della duplicazione.

2.5.3 Point Coordination Function (PCF)

Il MAC IEEE 802.11 prevede un metodo di accesso opzionale chiamato *Point Coordination Function* (PCF), che può essere usato però solo nelle reti con infrastruttura. Questo metodo di accesso prevede che un'entità logica detta *Point Coordinator* (PC), che risiede nell'AP della BSS, stabilisca istante per istante mediante un'operazione di polling quale STA sia autorizzata a trasmettere. Questo tipo di accesso potrebbe richiedere un coordinamento ulteriore nel caso in cui, nella stessa area e sullo stesso canale, si trovassero ad operare due BSS in PCF. Quest'ultima situazione non è specificata dallo standard.

Il PCF utilizza un meccanismo *virtual carrier-sense* insieme ad un meccanismo d'accesso basato su priorità. Il metodo d'accesso fornito dal PCF può dunque essere utilizzato per realizzare un accesso di tipo *contention-free* (CF), ovvero il PC controlla integralmente la trasmissione delle STA cosicchè si elimina la contesa di queste ultime per il mezzo trasmissivo.

E' previsto dallo standard che i metodi DCF e PCF debbano coesistere: quando in una BSS è presente un PC, i due metodi di accesso si alternano creando un *Contention-free Period* (CFP) cui segue un *Contention Period* (CP).

Tutte le STA di una BSS in cui è presente un PC attivo, possono operare correttamente e, se associate con l'AP in cui risiede appunto l'entità PC, possono ricevere frame in accordo alle regole del PCF. Così come è opzionale per un AP agire da PC, allo stesso modo è opzionale per una STA implementare la possibilità di rispondere alle richieste del PC durante il CFP. Le STA che implementano tale possibilità sono riferite nello standard come STA CF-Pollable.

Struttura e temporizzazione del CFP.

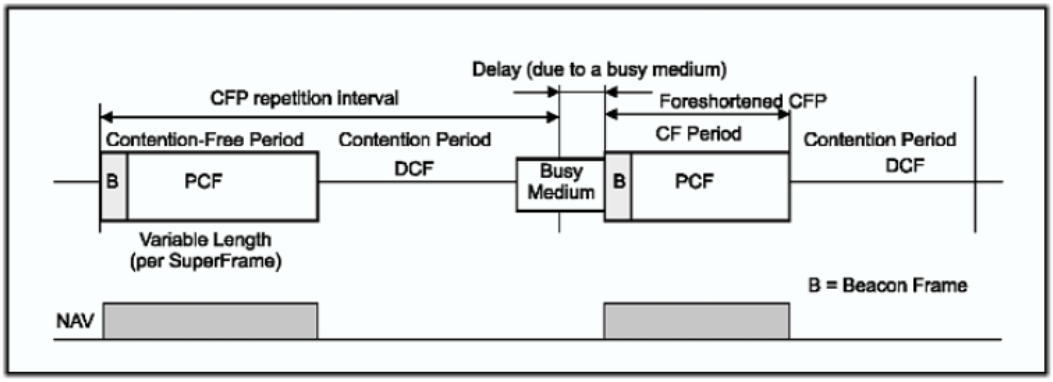


Figura 2.12: Alternanza tra CFP e CP

Il metodo PCF è usato per il trasferimento dei frame durante il CFP. Il CFP si alterna nel tempo con il CP, durante il quale è il metodo DCF a controllare il trasferimento dei frame. Lo standard IEEE 802.11 impone che sia comunque sempre presente un CP di durata sufficiente a trasmettere almeno una sequenza completa di frame. Questa possibilità viene imposta dallo standard per permettere la trasmissione dei frame di tipo Management. Ciascun CFP comincia con un frame speciale detto beacon, che contiene delle informazioni importanti sul CFP, tra le quali un elemento di tipo DTIM (*Delivery Traffic Indication Map*), che è a sua volta un particolare pacchetto TIM (*Traffic Indication Map*).

Ordine	Elemento informativo
1	Timestamp
2	Beacon Interval
3	Capability Information
4	SSID
5	Supported Rates
6	FH Parameter Set
7	DS Parameter Set
8	CF Parameter Set
9	IBSS Parameter Set
10	TIM

Tabella 2.4. Composizione del payload dei frame Beacon

Il campo CF Parameter Set è così strutturato:

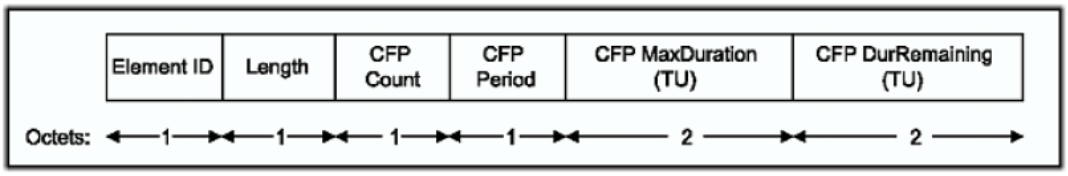


Figura 2.13: Formato dell'elemento CF parameter Set

Il beacon che segna l'inizio del CFP ha il campo CFPCount pari a 0, altrimenti tale campo indica quanti DTIM (incluso il frame attuale) verranno trasmessi prima dell'inizio del prossimo CFP. Il PC genera dei periodi CFP ad intervalli pari al valore del parametro CFPRate, espresso in termini di intervalli DTIM e comunicato alle STA della BSS tramite il campo CFPPeriod del CF Parameter Set visto in figura 2.13.

Possiamo vedere un esempio nella figura seguente:

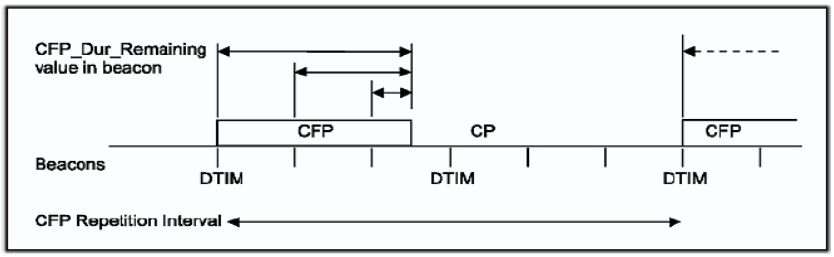


Figura 2.14: Beacon e CFP

In questo esempio, il CFP si ripete ogni 2 intervalli DTIM e l'intervallo DTIM a sua volta è pari a 3 intervalli beacon.

Il PC può terminare un CFP prima della sua fine prevista. Tale fine è specificata dal parametro CFP-MaxDuration anch'esso incluso nel CF Parameter Set. Il termine prematuro del CFP potrebbe essere dovuto, ad esempio, alla mancanza di traffico da gestire. Come si vede dalla figura 2.12, il traffico contention che segue il periodo CFP, potrebbe causare un ritardo nella trasmissione del beacon che inizia il prossimo CFP. In questa situazione, la durata del successivo periodo CFP risulta diminuita proprio del suddetto ritardo. Lo standard prevede che in caso di mezzo trasmissivo occupato dalla trasmissione DCF di un frame, la trasmissione del beacon debba essere ritardata fino al completamento del frame DCF. Quindi, nell'alternanza tra i due metodi di accesso, viene garantita una durata minima per il CP, ma non viene garantita una durata minima per il CFP, anzi ne viene definita una durata massima. Questo significa che il CFP non garantisce alcuna banda minima di trasmissione.

Procedura di accesso base

Il metodo di accesso contention-free è basato su uno schema di tipo polling (interrogazione) controllato dall'entità logica detta PC che risiede nell'AP di una BSS con topologia infrastrutturata. Il PC acquisisce il controllo del mezzo trasmissivo all'inizio di ogni CFP, e tenta di mantenere questo controllo per tutta la durata del CFP usando un IFS minore di quello usato dalle STA che operano secondo le regole del DCF. Abbiamo già accennato al suddetto IFS (PIFS ovvero Point Coordination Function IFS), e dalla tabella possiamo effettivamente vedere come il suo valore sia

inferiore al DIFS, che è il tempo IFS che viene usato dalle STA che operano secondo le regole dal DCF per intercalare le trasmissioni consecutive dei frame.

Quindi, all'inizio di un CFP, il PC controlla il mezzo trasmissivo, e, se risulta libero per un tempo maggiore o uguale a PIFS, il PC trasmette un beacon con il CF Parameter set e l'elemento DTIM. Tutte le altre STA settano il proprio NAV proprio in base all'informazione CFP-MaxDuration, in modo da evitare possibili trasmissioni non causate da poll del PC, sia da parte di STA CF-Pollable che da parte di tutte le altre STA. Le STA CF-Pollable e il PC non usano il meccanismo RTS/CTS durante il CFP. Quando una STA CF-Pollable viene interrogata dal PC, essa può trasmettere soltanto una MPDU, diretta verso il PC o verso una qualsiasi altra STA, e può effettuare un cosiddetto piggyback dell'ACK per un frame ricevuto dal PC, usando un particolare sottotipo di frame dati. La ricezione del frame appena inviato dalla STA che è stata interrogata dev'essere confermata con l'invio di un frame ACK dopo un SIFS, proprio come col metodo DCF, a conferma del fatto che il metodo PCF non è un'entità logica a se stante ma dipende strettamente dal DCF. Se tale conferma non avviene (o la STA mittente non la riceve), la STA che è stata autorizzata a trasmettere dal PC non può ritrasmettere il frame fino a quando non viene interrogata nuovamente dal PC, oppure può decidere di ritrasmetterlo durante il CP. Il PC può invece ritentare la trasmissione di un frame di cui non ha avuto l'ACK, dopo un tempo PIFS.

Le figure 2.15 e 2.16, illustrano i casi appena descritti, ovvero una trasmissione PC-STA e una trasmissione STA-STA, entrambe durante il CFP.

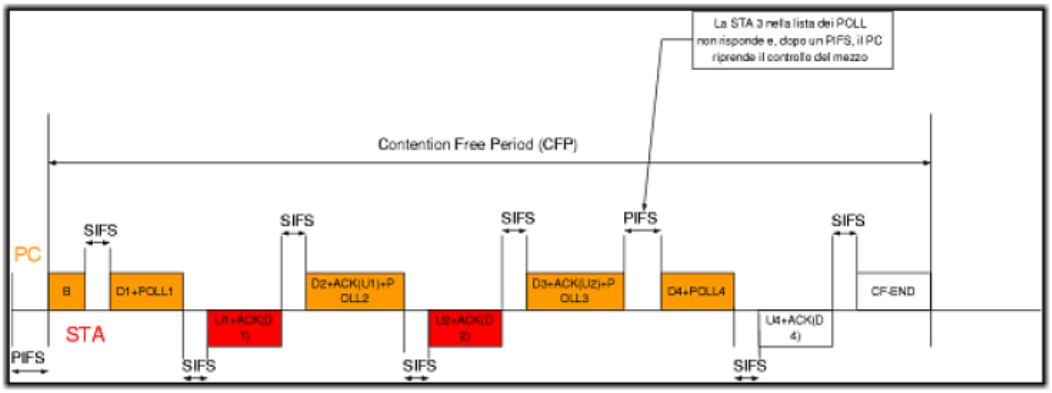


Figura 2.15: PCF: trasmissione PC verso STA

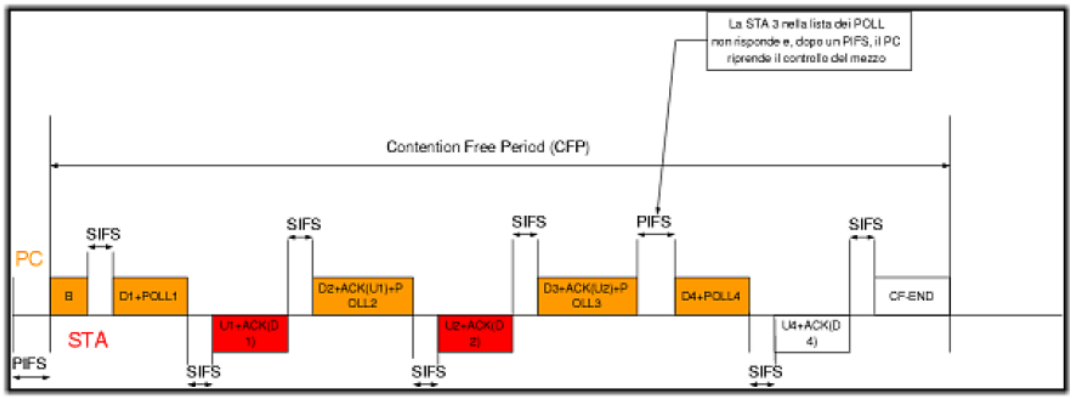


Figura 2.16: PCF: trasmissione STA verso STA

La presenza e la gestione del NAV durante il CFP sono utili per facilitare l'operatività delle reti nella situazione di sovrapposizione dei rispettivi periodi CFP e delle rispettive aree di copertura. Tuttavia, come abbiamo già detto, il modo in cui tali BSS in questa situazione, coordinano i rispettivi CFP, non è coperto dallo standard IEEE 802.11.

Definiamo gli istanti in cui, nominalmente, dovrebbe iniziare la trasmissione del beacon che segna l'inizio del CFP come TBTT (*Target Beacon Trasmission Time*). In questi istanti tutte le STA, eccetto l'AP, inizializzeranno il proprio NAV al valore CFP-MaxDuration. Questo evento ha 2 effetti:

- Impedisce alle STA diverse dall'AP di prendere il controllo del mezzo durante il CFP.
- Risolve il problema dei nodi nascosti, così come faceva il meccanismo RTS/CTS per il DCF.

Una STA che vuole unirsi ad una BSS in cui opera un PC, usa le informazioni contenute in elemento del CF Parameter Set, il CFPDurRemaining, presente nei beacon e nei frame di tipo Probe Response, il cui uso verrà descritto in seguito. Usando tali informazioni, le nuove STA aggiornano il proprio NAV in modo da non interferire con un eventuale CFP in corso.

Il PC può concludere anzitempo il CFP trasmettendo un frame di tipo *CF-End* (o CF-End+ACK): una STA che riceva uno di questi due frame, a qualsiasi BSS essa appartenga, è autorizzata a resettare il proprio NAV.

Riepilogo delle regole del metodo PCF

E' opportuno riepilogare le regole che definiscono il metodo d' accesso PCF:

- Il PC può inviare dei frame di tipo unicast, broadcast o multicast ad ogni STA attiva ed anche ad eventuali STA CF-Pollable ma in Power Save (in seguito vedremo le modalità definite power save).
- Durante il periodo CFP, ogni STA CF-Pollable deve operare dopo un SIFS nel seguente modo:
    1. se ha ricevuto un frame di tipo Data+CF-Poll oppure Data+CF-ACK+CF-Poll, deve rispondere conun frame di tipo Data+CF-ACK oppure semplicemente con un frame CF-ACK se non ha dati da inviare.
    2. se ha ricevuto un frame di tipo CF-Poll deve rispondere con un frame di tipo Data oppure Null
    3. se ha ricevuto un frame di qualsiasi altro tipo (dati o management), deve rispondere con un frame di tipo ACK

- Le STA non CF-Pollable si comportano praticamente seguendo le regole del metodo DCF, e quindi rispondono alla ricezione di un frame di qualsiasi tipo (dati o management) usando un frame ACK dopo un SIFS.
- Quando una STA CF-Pollable viene interrogata dal PC con un Poll (frame Data+CF-Poll, Data+CF-ACK+CF-Poll, CF-Poll o CF-ACK+CF-Poll), può mandare un frame verso una STA qualsiasi. Se tale frame è diretto al PC, o deve passare attraverso il PC perchè diretto al DS, il PC stesso deve confermare la ricezione del frame usando l' indicazione CF-ACK (frame Data+CF-ACK, CF-ACK, Data+CF-ACK+CF-Poll, CF-ACK+CF-Poll o CF-End+CF-ACK) dopo un SIFS. Se invece il frame è diretto verso una STA (che sia CF-Pollable oppure no), la STA destinataria confermerà con un frame ACK dopo un SIFS.

Polling list

Il PC può realizzare 2 diverse forme del servizio contention-free: con o senza interrogazioni. Queste due modalità sono comunicate tramite l' elemento *Capability Information* che si trova nei *frame beacon, probe response, association response, reassociation response* che vengono inviati dall'AP.

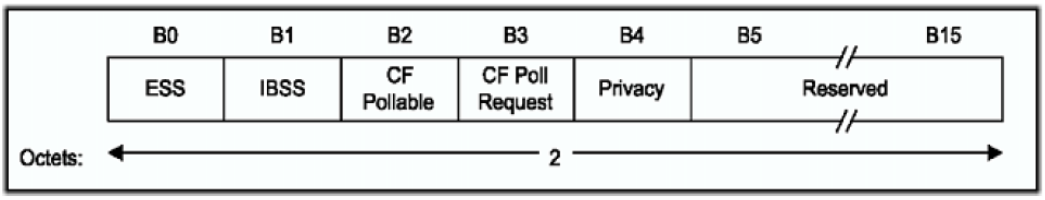


Figura 2.17: Struttura del campo Capability Information

In particolare, i campi CF-Pollable e CF-Poll Request vengono così interpretati quando i frame in cui sono contenuti provengono da un AP/PC:

CF-Pollable	CF-Poll Request	Significato
0	0	Nessuna funzione Point Coordination presso l'AP
0	1	Point Coordination presso l'AP solo per il trasporto dei pacchetti da e verso il DS (nessun polling)
1	0	Point Coordination presso l'AP sia per il trasporto dei pacchetti verso il DS che per il polling
1	1	Riservato

Tabella 2.5: Uso dei campi CF-Pollable e CF-Poll Request da parte dell'AP

Se il PC realizza un CFP soltanto per il trasporto di frame verso il DS, così come può fare durante il funzionamento DCF, esso non ha bisogno di creare e gestire una polling list e non genererà quindi mai dei frame contenenti l'indicazione CF-Poll. Se al contrario, il PC prevede di usare le interrogazioni (poll) per le STA che lo richiedono (*CF-Pollable*), esso genera e mantiene una polling list e la usa per generare dei frame con l'indicazione CF-Poll, ovvero per generare le interrogazioni alle STA incluse nella lista stessa. La polling list è solo un costrutto logico e non viene resa disponibile all'esterno del PC.

Analizziamo ora le procedure minime di gestione della polling list, osservando che un AP/PC può implementare varie tecniche per la suddetta gestione ma queste sono fuori dalla copertura dello standard IEEE 802.11:

- Quando la polling list è popolata, durante il CFP il PC deve mandare almeno un frame di tipo CF-Poll ad una STA inclusa nella polling list.
- Le STA nella polling list sono interrogate in ordine di AID (Association Identifier) crescente. Il valore AID è un identificativo di 16 bit, di valore compreso tra 1 e 2007, che viene assegnato alla STA dall'AP appunto in fase di associazione (Association), durante la quale la STA stessa comunica il suo futuro comportamento in base alla seguente tabella (i campi CF-Pollable e CF-Poll request sono compresi nell'elemento *Capability Information* presente nei frame di tipo *Association* e *Reassociation Request)*:

CF-Pollable	CF-Poll Request	Significato
0	0	La STA non è CF-Pollable
0	1	La STA è CF-Pollable ma non richiede di essere messa nella polling list
1	0	La STA è CF-Pollable e richiede di essere messa nella polling list
1	1	La STA è CF-Pollable e richiede di non essere mai interrogata

Tabella 2.6: Uso dei campi CF-Pollable e CF-Poll Request da parte delle STA

- Se rimane tempo durante il CFP, tutti i frame CF sono stati inviati e tutte le STA della polling list sono state interrogate, il PC può decidere di:
    1. generare uno o più frame CF-Polls verso una o più STA della polling list
    2. mandare frame di tipo dati o management a una o più STA (anche non appartenenti alla polling list).
    3. Se il CFP termina prima che tutte le STA della polling list vengano interrogate, la polling list riprenderà dal punto in cui si è interrotta nel successivo periodo CFP.

Come abbiamo visto nella tabella 2.5, una STA comunica la propria posizione nei confronti della polling list al momento dell'associazione o riassociazione. Tale posizione può essere modificata tramite il servizio di riassociazione. Sempre dalla stessa tabella, possiamo notare che c'è anche la possibilità per una STA di essere CF-Pollable ma di non voler essere mai interrogata. Questa possibilità che può sembrare inutile, sarà esaminata meglio nella sezione dedicata al *Power Save*.

2.5.4 Sincronizzazione

Illustriamo ora le procedure che consentono a tutte le STA di una BSS di rimanere sincronizzate con un clock comune. La sincronizzazione è basata su una funzione, gestita da ogni singola STA, detta TSF (*Timing Synchronization Function*) e su un timer, il TSF Timer.

Sincronizzazione nelle WLAN IEEE 802.11 con infrastruttura

In una WLAN IEEE 802.11 con infrastruttura, l'AP provvederà a realizzare la funzione TSF e controllerà il clock comune. L'AP trasmetterà periodicamente dei frame di tipo beacon, contenenti una copia (timestamp, vedi descrizione del frame beacon) del proprio TSF Timer, per consentire alle altre STA della BSS di sincronizzarsi con quest'ultimo. Una STA che riceve questo beacon, deve accettare senza condizioni le informazioni relative al timestamp dell'AP e aggiustare il proprio TSF Timer in base al timestamp stesso.

Generazione e trasmissione dei beacon

L'AP dunque genera dei beacon ad intervalli pari al valore *BeaconPeriod*, stabilendo perciò la temporizzazione della BSS. Abbiamo già definito col termine TBTT gli istanti in cui l'AP nominalmente, ovvero in mancanza di traffico in corso e quindi con il mezzo trasmissivo libero, dovrebbe iniziare la trasmissione di un frame di tipo beacon. Possiamo osservare un esempio nella figura 2.18:

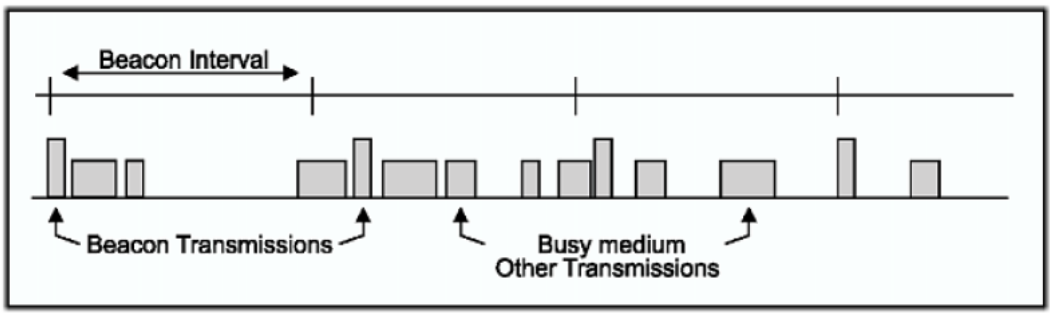


Figura 2.18: Trasmissione dei beacon in una BSS

Ricezione dei beacon

Una STA appartenente ad una WLAN IEEE 802.11 con infrastruttura, deve usare le informazioni contenute nei beacon solo se il campo BSSID coincide con l'indirizzo

MAC dell'AP che gestisce la BSS di cui la STA fa parte. Se il suddetto confronto è positivo, la STA modifica il proprio timer TSF con il valore del timestamp ricevuto col beacon, altrimenti significa che ha ricevuto il beacon di un'altra BSS, che deve ignorare.

Sincronizzazione nelle WLAN IEEE 802.11 ad hoc

La funzione TSF in una WLAN ad hoc, o IBSS, è implementata con un algoritmo distribuito cui prendono parte tutte le STA della IBSS. Una qualsiasi STA è in grado di generare e trasmettere beacon, in accordo alla procedura che vedremo, e le altre STA devono operare le modifiche, al proprio timer TSF, solo se il valore timestamp, ricevuto tramite il beacon o frame di tipo probe response, è in ritardo rispetto al proprio.

Generazione dei beacon

La generazione dei beacon è distribuita. Il periodo di trasmissione dei beacon (beacon period) è incluso nei frame di tipo beacon o probe response, e tutte le STA devono adottare questo parametro al momento in cui si uniscono alla IBSS. Il parametro beacon period è stabilito dalla STA che inizializza la IBSS. Il beacon period a sua volta definisce gli istanti TBTT. Ad ogni TBTT ogni STA deve:

1. Sospendere qualsiasi eventuale procedura di backoff in corso.
2. Calcolare un ritardo casuale, uniformemente distribuito nell'intervallo [0; 2×CWmin×SlotTime].
3. Aspettare questo ritardo casuale, come nella procedura di backoff.
4. Se durante quest'attesa viene ricevuto un beacon generato da un'altra STA, viene cancellato il ritardo casuale calcolato e viene abbandonata la procedura di trasmissione del beacon, riprendendo eventuali backoff sospesi.
5. Se invece non viene ricevuto alcun beacon durante l'attesa, allora la STA invia il beacon con il proprio timestamp.

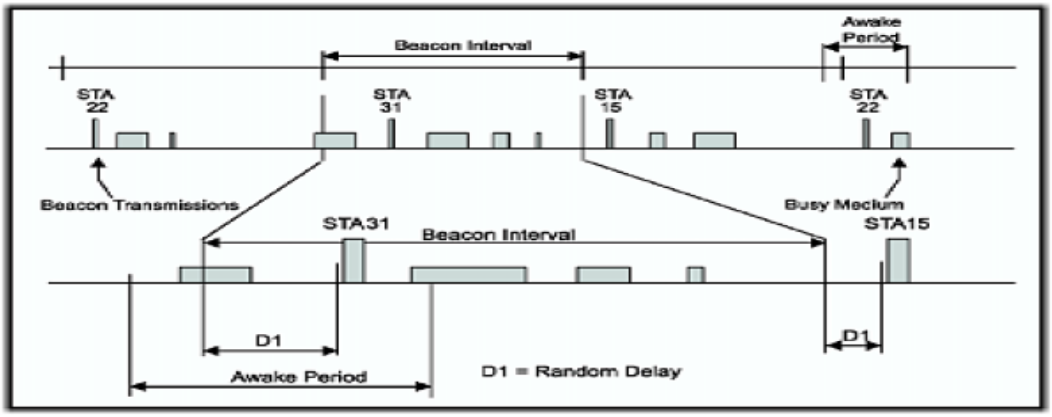


Figura 2.19: Trasmissione dei beacon in una IBSS

Si noti che è possibile che più di una STA in una IBSS generi e invii un beacon subito dopo il TBTT, o a causa di una non corretta ricezione di un beacon inviato da un'altra STA, o a causa di collisione tra le trasmissioni dei beacon stessi.

Ricezione dei beacon

Una STA appartenente ad una IBSS accetta le informazioni contenute in ogni beacon ricevuto solo se il sottocampo IBSS dell'elemento Capability Information è posto ad 1 ed il contenuto del campo SSID del beacon è uguale all'indirizzo MAC della IBSS. In questo caso, la STA modificherà il proprio timer TSF con il valore ricevuto con il beacon solo se quest'ultimo è in ritardo rispetto al proprio TSF .

2.6 Power management e modalità Power Save

2.6.1 Power management in una WLAN con infrastruttura

Relativamente al consumo di potenza, una STA può trovarsi in uno dei seguenti 2 stati:

Awake

la STA funziona a pieno regime.

Doze

la STA non riceve nè trasmette e perciò consuma pochissima potenza.

Una STA si sposta da uno stato all'altro in base ai cosiddetti *Power Management Modes* (modalità di gestione della potenza). Queste modalità sono riassunte nella tabella 2.6.

Una STA che voglia cambiare modalità di funzionamento deve comunicarlo all'AP tramite il bit *Power Management* contenuto nel Frame *Control Field* dei pacchetti. Il valore di questo bit indicherà all'AP quale sarà, a conclusione dello scambio di frame in corso durante il quale non può ovviamente cambiare nulla, la modalità di funzionamento scelta dalla STA. Se la modalità scelta è la modalità PS (*Power Save*) l'AP non deve trasmettere alcuna MSDU alla STA in PS, bensì deve conservare tutto il traffico relativo alla STA e trasmetterglielo in momenti prestabiliti.

La STA in PS ascolterà il canale periodicamente per ricevere dei frame di tipo beacon nei quali trova l'elemento TIM (*Traffic Indication Map*). La ricezione dei beacon, relativamente alla procedura di gestione degli elementi TIM, è regolata dai parametri ListenInterval e ReceiveDTIMs.

In particolare, il parametro ListenInterval viene comunicato dalla STA all'AP al momento dell'associazione e indica all'AP in quali beacon la STA sarà in ascolto. Il parametro ReceiveDTIMs, invece, è comunicato dalla STA all'AP al momento del cambio di modalità operativa (da AM a PS), ed indica se la STA in questione riceverà ed interpreterà o meno i beacon con elemento DTIM.

In pratica, l'AP costruisce l'elemento TIM come una mappa virtuale del traffico che esso mantiene in memoria per tutte le STA che si trovano in PS. Quest'ultime, ricevendo e analizzando il TIM contenuto nei beacon, possono sapere se l'AP ha del traffico in attesa destinato ad esse, ed agire di conseguenza ovvero:

- In una BSS operante col metodo DCF, o durante il CP che segue il CFP se la BSS opera col metodo PCF, la STA in PS trasmette un frame di tipo PS-Poll (Power Save Poll) all'AP per segnalare che è pronta a ricevere il traffico bufferizzato nell'AP stesso. L'AP risponde subito con la MSDU bufferizzata

oppure può confermare (ACK) la ricezione del frame PS-Poll e rispondere più tardi.

- Se il TIM indica che il frame bufferizzato verrà inviato durante il CFP, la STA (che sarà dunque una STA CF-Pollable), non manderà alcun frame PS-Poll, ma aspetterà il proprio turno all'interno del CFP per ricevere il traffico bufferizzato nell'AP, rimanendo in AM per tutta la durata del CFP stesso.

Nel caso in cui almeno una STA della BSS sia in PS, l'AP deve bufferizzare tutto il traffico broadcast e multicast e trasmetterlo alla STA (o alle STA) immediatamente dopo la trasmissione del primo beacon che contiene un'indicazione di tipo DTIM

Active Mode (AM)	La STA può ricevere frame in qualsiasi momento. In AM la STA si trova nello stato Awake. Se la STA è presente nella polling list dell'AP, essa deve rimanere in AM per tutta la durata del CFP
Power Save Mode (PS)	La STA si trova nello stato Doze e passa in Awake solo per ascoltare dei beacon prestabiliti (in base al ListenInterval), per ricevere traffico broadcast o multicast bufferizzato dall'AP (in base al ReceiveDTIMs), per trasmettere dei frame di tipo PS-Poll ed aspettare risposta agli stessi oppure per ricevere, durante il CFP se si tratta di una STA CF-Pollable, il traffico bufferizzato

Tabella 2.7: Modalità Power Management

Una STA che ritorna dallo stato *Doze* allo stato *Awake* deve compiere una procedura di *Clear Channel Assesment* (CCA), con la quale può riconoscere correttamente una sequenza di frame in corso e impostare il proprio NAV.

Definizione dei TIM

Un elemento TIM contiene una mappa virtuale delle STA in PS per le quali l'AP mantiene del traffico bufferizzato. In aggiunta, il TIM indica anche la presenza di traffico bufferizzato di tipo broadcast o multicast. Ad ogni STA in una WLAN con infrastruttura viene assegnato, in fase di associazione, un identificativo AID. E'

proprio tramite questo AID che l'AP costruisce il TIM. L'AID=0 è riservato al traffico broadcast o multicast bufferizzato.

Possiamo distinguere due tipi di TIM:

* TIM

E' un elemento TIM standard che viene incluso in ogni frame di tipo beacon.

* DTIM

E' un elemento TIM trasmesso al posto di un TIM normale, ad intervalli pari al valore del parametro DTIMPeriod. Immediatamente dopo la trasmissione di un beacon con un elemento DTIM, l'AP deve mandare tutto il traffico bufferizzato di tipo broadcast e multicast, prima di cominciare ad inviare quello unicast.

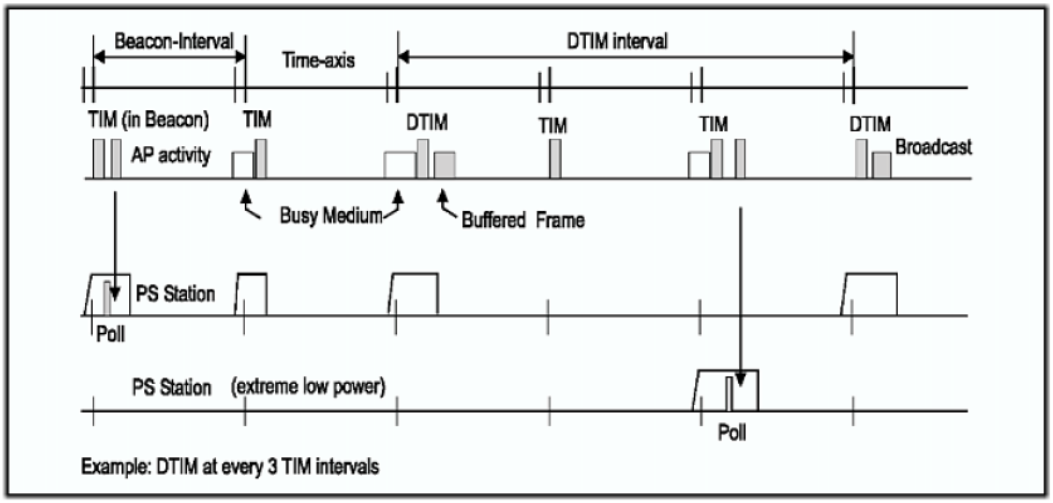


Figura 2.20: Power management nelle BSS con infrastruttura

La figura 2.20 illustra una situazione possibile, con l'ipotesi che venga trasmesso un elemento DTIM ogni 3 elementi TIM. La linea più in alto rappresenta l'asse dei tempi. La linea immediatamente sotto illustra l'attività dell'AP.

Quest'ultimo programma la trasmissione di un beacon affinché avvenga ad ogni istante TBTT (ovvero ad intervalli *Beacon Interval*). Siccome il mezzo può essere occupato nell'istante TBTT, quindi la trasmissione del beacon può essere ritardata. Notiamo che:

- subito dopo un beacon contenente un elemento DTIM, l'AP trasmette tutto il traffico broadcast bufferizzato.
- la STA in PS la cui attività nel tempo è descritta dalla terza linea.

Funzione Aging

L'AP implementa una funzione cosiddetta di aging, che serve a cancellare il traffico che ha bufferizzato per un periodo di tempo troppo lungo. Questa funzione dev'essere basata sul parametro ListenInterval di ciascuna STA, ovvero la funzione dev'essere tale da non cancellare il traffico prima che sia passato un intervallo pari a ListenInterval. La definizione di una tale funzione è comunque fuori dalla trattazione dello standard IEEE 802.11.

2.6.2 Power management in una WLAN ad hoc (IBSS)

La gestione della modalità *power save* nelle WLAN IEEE 802.11 ad hoc è simile a quella vista per le WLAN che hanno una topologia con infrastruttura, ovvero le STA conservano in un buffer il traffico unicast e multicast destinato a STA che si trovano in modalità PS, e tale traffico viene annunciato, prima di essere inviato, in periodi prestabiliti nei quali tutte le STA, anche quelle in PS appunto, sono in ascolto. Il suddetto annuncio viene fatto tramite un frame dedicato alle WLAN ad hoc, il cosiddetto ATIM (*Ad hoc Traffic Indication Map*)

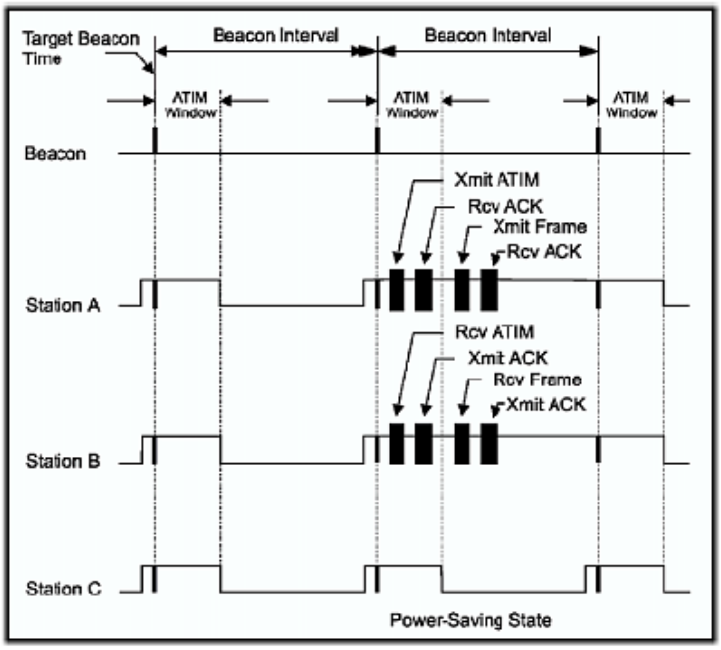


Figura 2.21: Power management in una IBSS

Facendo riferimento alla figura 2.21, si definisce ATIM Window l'intervallo di tempo in cui tutte le STA, incluso quelle in PS, sono nello stato Awake. La durata della ATIM Window è specificata dal parametro *ATIMWindow* (che si trova nell'elemento IBSS Parameter Set dei frame di tipo beacon e probe response).

Essa inizia subito dopo l'istante TBTT e durante questa finestra temporale possono essere trasmessi solo frame di tipo beacon o ATIM. Quando una STA deve inviare una o più MSDU ad un'altra STA che si trova in modalità PS, essa deve innanzitutto inviare verso la STA in PS un frame ATIM durante l'ATIM Window.

Sempre nella figura 2.21, osserviamo come la STA A abbia la necessità di inviare un frame alla STA B che si trova in PS. Allora, durante l'ATIM Window, la STA A invia un frame ATIM direttamente indirizzato alla STA B, che si trova nello stato *Awake* per tutta la durata dell'ATIM Window. La ricezione di un ATIM di tipo diretto (unicast) dev'essere confermata dalla STA ricevente (con un frame di tipo ACK); in caso contrario, la STA trasmittente tenta la ritrasmissione effettuando una procedura di backoff, sempre all'interno della ATIM Window. I frame di tipo ATIM di tipo multicast non prevedono alcuna conferma. La STA B, ricevendo un ATIM ad essa

indirizzato, innanzitutto conferma tale ricezione con un frame ACK diretto alla STA A, e poi rimane nello stato *Awake* per tutta la durata del beacon interval corrente, in attesa di ricevere la (o le) MSDU che la STA A deve inviarle. Se una STA in PS non riceve alcun frame ATIM durante l'ATIM Window, può tornare nello stato Doze alla fine della ATIM Window, fino al prossimo istante TBTT ovvero all'inizio della successiva ATIM Window.

Quindi, alla fine della ATIM Window, possono iniziare le trasmissioni di tutti i frame unicast che sono stati annunciati con successo (ovvero quelli i cui relativi ATIM sono stati confermati con l'ACK) durante l'ATIM Window, e possono iniziare le trasmissioni di tutti i frame multicast e broadcast annunciati durante l'ATIM Window. La trasmissione di questi frame segue le regole del metodo d'accesso DCF.

Nella IBSS, a causa della mancanza di un'entità quale un AP che coordini la WLAN, una STA può soltanto stimare lo stato (AM o PS) di una qualsiasi altra STA nella IBSS. Il modo in cui una STA compie questa stima è fuori dalle specifiche dello standard IEEE 802.11, anche se viene consigliato di basarsi sulle informazioni relative al power management (bit *Power Management* nel Frame *Control Field*) trasmesse dalle altre STA, oppure anche su informazioni quali una cronologia delle trasmissioni riuscite e fallite verso le altre STA. In quest'ultimo caso, l'uso del meccanismo RTS/CTS in una IBSS può facilitare le stima dello stato PS delle STA: se un frame RTS viene inviato ma non viene ricevuto un frame CTS, la STA mittente può dedurre che la STA destinataria sia in modalità PS.

2.7 Procedure di Scan e Join

Le procedure di scan e join sono realizzate da una serie di funzioni o primitive.

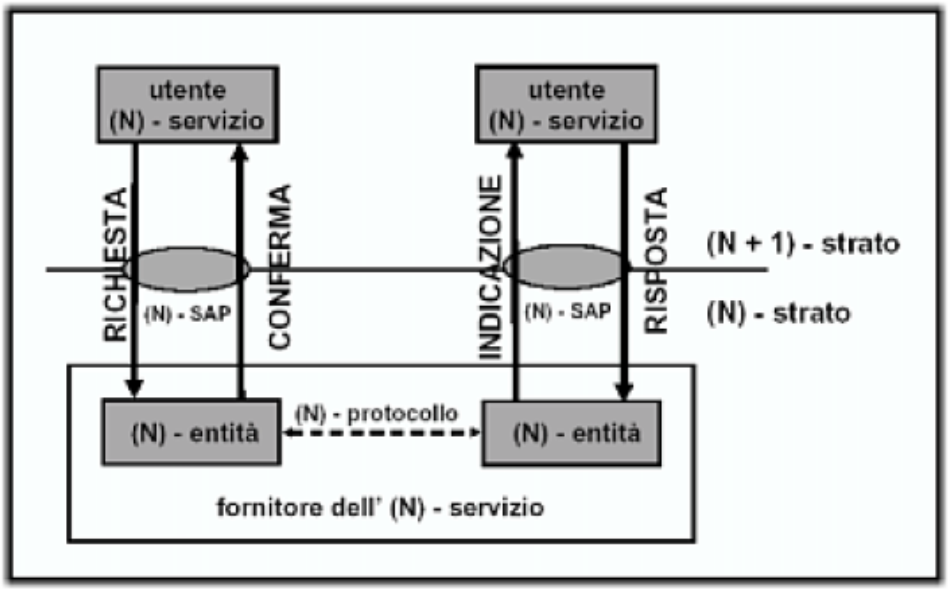


Figura 2.22: Primitive

Una primitiva (in figura rappresentate come frecce) è una procedura che permette di attivare ed usufruire dei servizi forniti dal livello inferiore di un certo protocollo organizzato a livelli. In particolare le primitive usate per le procedure di scan sono:

- MLME-SCAN.Request
- MLME-SCAN.Confirm

Lo standard IEEE 802.11 prevede 2 tipi di scan:

1. Active (attivo)
2. Passive (passivo)

Lo scan può essere utilizzato dunque per:

- trovare una rete ed connettersi ad essa
- trovare un nuovo AP (Roaming)
- inizializzare una IBSS (ad hoc network)

Successivamente alla procedura di scan, tramite la quale si ricercano le BSS e si acquisiscono i loro parametri, una STA può decidere di effettuare una procedura di join, per richiedere di entrare a far parte di una specifica BSS fra quelle trovate. Le primitive usate per le procedure di scan sono:

- MLME-JOIN.Request
- MLME-JOIN.Confirm

2.7.1 Scan passivo

Se si sceglie questo tipo di scan, la STA si mette in ascolto su ciascun canale specificato nella ChannelList della primitiva MLME-SCAN.Request (vedi 2.7.2), per il tempo specificato sempre nella suddetta primitiva, aspettando di riconoscere dei frame di tipo Beacon contenenti il particolare SSID scelto, oppure aspettando di riconoscere un Beacon con l'SSID broadcast, a seconda di quanto specificato nella primitiva MLME-SCAN.Request. Alla fine dello scan, ovvero quando tutti i canali scelti sono stati esaminati, viene usata la primitiva MLME-SCAN.Confirm per conservare tutte le informazioni raccolte, a beneficio di un'eventuale successiva procedura di join.

2.7.2 Scan Attivo

Questa modalità di scan implica la generazione di frame di tipo Probe e la successiva elaborazione dei frame *Probe Response*. Al momento della ricezione della primitiva MLME-SCAN.Request con il parametro *ScanType* che indica uno scan attivo, una STA deve compiere la seguente procedura:

- Per ciascun canale da esaminare, aspetta che trascorra il tempo indicato dal parametro ProbeDelay;
- ottiene l'accesso al mezzo secondo le regole del metodo DCF; invia un frame di tipo Probe Request con l'indirizzo broadcast , il SSID e il BSSID broadcast;
- resetta e fa partire un ProbeTimer
- la STA continua a mandare frame di tipo Probe finchè rileva il mezzo libero e il ProbeTimer risulta inferiore al valore MinChannelTime, dopodichè la STA resetta il proprio NAV e passa ad esaminare il successivo canale. Può capitare che la STA rilevi il mezzo occupato quando tenta di mandare frame

di tipo Probe Request, quindi ritarda la trasmissione dei suddetti frame ma rimane su quel canale al massimo fino a che il ProbeTimer raggiunge il valore MaxChannelTime, dopodichè raccoglie tutte le risposte ottenute e passa ad esaminare il canale successivo.

- resetta il proprio NAV e passa ad esaminare il canale successivo.

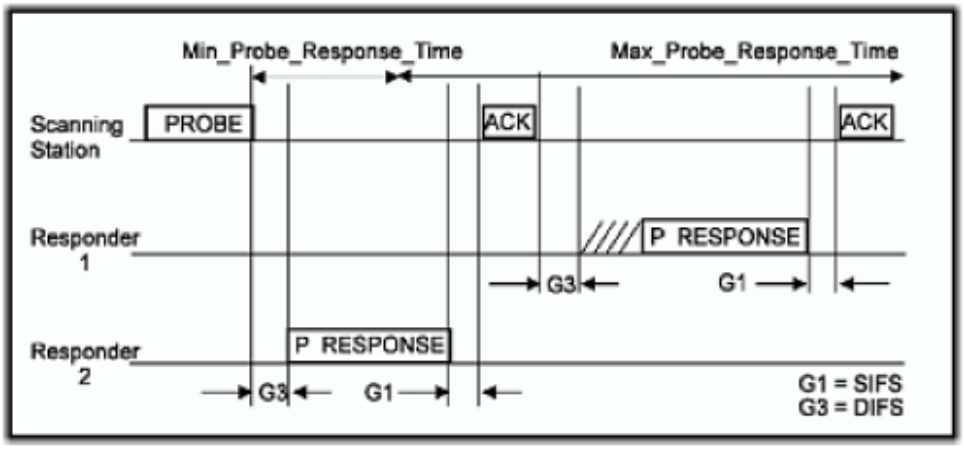


Figura 2.23: Scan Attivo

Regole per l'invio dei frame Probe Response

Una STA che riceve un frame di tipo Probe Request deve rispondere con un frame di tipo Probe Response solo se il valore SSID nel probe request è il SSID di tipo broadcast oppure se coincide esattamente con il proprio SSID.

I frame di tipo probe response vanno indirizzati direttamente alla STA che ha inviato i frame probe request, e vanno inviati secondo le regole del metodo DCF. Anche un AP deve rispondere ad un probe response secondo le regole appena descritte. In una IBSS invece, è la STA che ha generato l'ultimo beacon che ha il compito di rispondere ai frame probe response. In questa situazione, vi è la possibilità che più di una STA in una IBSS risponda ai probe request, poichè è possibile che più di una STA nella IBSS invii un beacon.

In ogni BSS, in un dato momento, dev'esserci almeno una STA nello stato Awake (ovvero in modalità AM), per rispondere ai probe request. Una STA che invia un beacon, deve rimanere nello stato Awake e rispondere ai probe request fino a che non

riceve un altro beacon con il valore BSSID corrente. Nel caso in cui la STA che invia un beacon sia un AP, esso deve sempre rimanere nello stato Awake per rispondere ai probe request.

**Primitiva MLME-SCAN.Request*

Questa primitiva supporta il processo di scan per la ricerca di BSS nel raggio di copertura di una STA. Tale primitiva viene invocata con i seguenti parametri:

Nome	Tipo	Valori possibili	Descrizione
BSSType	Enumeration	INFRASTRUCTURE, INDIPENDENT, ANY_BSS	Specifica che tipo di BSS si vuole cercare
BSSID	MACAddress	Qualsiasi valido indirizzo MAC , individuale o di gruppo	Identifica uno specifico BSSID o lo scan usa il BSSID di tipo broadcast
SSID	Stringa di ottetti	0-32 ottetti	Identifica uno specifico SSID oppure lo scan usa il SSID di tipo broadcast
ScanType	Enumeration	ACTIVE, PASSIVE	Specifica il tipo di scan, attivo o passivo
ProbeDelay	Intero	N/D	Ritardo (in μs) da usare prima di trasmettere un frame Probe in caso di scanning attivo
ChannelList	Insieme ordinato di interi	Ciascun canale sarà scelto in base alla lista dei canali disponibili per uno specifico PHY	Specifica la lista dei canali che saranno esaminati nello scan
MinChannelTime	Intero	≥ ProbeDelay	Il tempo minimo speso ad esaminare un singolo canale
MaxChannelTime	Intero	≥ MinChannelTime	Il tempo massimo speso ad esaminare un singolo canale

Tabella 2.8: Parametri della primitiva MLME-SCAN.Request

**Primitiva MLME-SCAN.confirm*

Questa primitiva restituisce la descrizione dell'insieme delle BSS rilevate durante il processo di scan. Tale primitiva viene invocata con i seguenti parametri:

Nome	Tipo	Valori possibili	Descrizione
BSSDescriptionSet	Insieme di elementi di tipo BSSDescription	N/D	E' un insieme, anche nullo, di istanze del tipo BSSDescription
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS	Indica il risultato della primitiva MLME-SCAN.Confirm

Tabella 2.9: Parametri della primitiva MLME-SCAN.Confirm

* *Primitiva MLME-JOIN.Request*

Questa primitiva serve a richiedere la sincronizzazione e quindi l'ingresso in una BSS da parte di una nuova STA. I parametri di questa primitiva sono:

Nome	Tipo	Valori possibili	Descrizione
BSSDescription	BSSDescription	N/D	La descrizione della BSS cui la STA si vuole aggiungere. Quest'elemento deriva direttamente dall'insieme ottenuto dalla primitiva MLME-SCAN.Request
JoinFailureTimeout	Intero	≥ 1	Il limite, in termini di beacon interval, dopo il quale la procedura di join viene interrotta senza successo
ProbeDelay	Intero	N/D	Ritardo (in μs) da usare prima di trasmettere un frame Probe in caso di scanning attivo
OperationalRateSet	Insieme di interi	2-127 (∀intero dell'insieme)	L'insieme dei *data rate* (in unità da 500 kb/s) che la STA può usare all'interno della BSS. La STA dev'essere in grado di ricevere usando ciascuno dei data rate elencati nella lista. Questo elemento è un sottoinsieme del BSSBasicRateSet

Tabella 2.10: Parametri della primitiva MLME-JOIN.Request

Nome	Tipo	Valori possibili	Descrizione
BSSID	MACAddress	N/D	Il BSSID della BSS trovata
SSID	Stringa di ottetti	1-32 ottetti	Il SSID della BSS trovata
BSSType	Enumeration	INFRASTRUCTURE, INDIPENDENT	Il tipo della BSS trovata
BeaconPeriod	Intero	N/D	Il periodo di trasmissione dei beacon della BSS trovata
DTIMPeriod	Intero	Come definito nel formato dei frame	Il periodo (espresso in numero di beacon period) dei beacon contenenti un elemento DTIM
Timestamp	Intero	N/D	Il timestamp del frame appena ricevuto (probe response o beacon) dalla BSS trovata
Localtime	Intero	N/D	Il valore del TSF della STA al momento della ricezione del primo ottetto del campo Timestamp del frame ricevuto (probe response/beacon) dalla BSS trovata
PHY Parameter Set	Come definito nel formato del frame	Come definito nel formato del frame	L'insieme dei parametri che caratterizza il PHY
CF Parameter Set	Come definito nel formato del frame	Come definito nel formato del frame	L'insieme dei parametri per i periodi CF, se la BSS trovata supporta questa modalità
IBSS Parameter Set	Come definito nel formato del frame	Come definito nel formato del frame	L'insieme dei parametri per la IBSS, se la BSS trovata è una WLAN ad hoc
Capability Information	Come definito nel formato del frame	Come definito nel formato del frame	Le capacità della BSS
BSSBasicRateSet	Insieme di interi	2-127 (∀intero dell'insieme)	L'insieme dei *data rate* (in unità da 500 kb/s) che devono essere supportati da tutte le STA che vogliono aggiungersi a questa BSS. La STA dev'essere in grado di ricevere usando ciascuno dei data rate elencati nella lista

Tabella 2.11: Elemento BSSDescription

** Primitiva MLME-JOIN.Confirm*

Questa primitiva conferma l'avvenuta sincronizzazione con una BSS. Questa primitiva richiede i seguenti parametri:

Nome	Tipo	Valori possibili	Descrizione
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS	Indica il risultato della primitiva MLME-JOIN.Request

Tabella 2.12: Parametri della primitiva MLME-JOIN.Confirm

2.7.3 Roaming

La topologia con infrastruttura consente l'implementazione di un sistema per la gestione delle transizioni delle stazioni mobili da una BSS ad un altra (roaming). Lo standard fornisce come supporto la procedura di *Riassociazione*. Quando un terminale mobile IEEE 802.11 decide di spostarsi da una BSS ad un'altra nelle vicinanze, tipicamente per migliorare le condizioni di ricezione come avviene nelle reti cellulari, compie una procedura di *scan* alla fine della quale possiede una lista di AP che può ordinare ad esempio in base alla qualità del segnale. Una volta scelto l'AP verso cui ha deciso di spostarsi, invia una richiesta (un frame *Reassociation Request*) verso questo AP. Il frame *Reassociation Request* contiene anche l'indirizzo MAC dell'AP cui la stazione è correntemente associata. Successivamente, l'AP prescelto invia alla stazione un frame *Reassociation Response*, comunicandole l'esito della procedura.

Possiamo osservare che:

- lo standard specifica che l'AP verso cui una stazione si è spostata, riassociandosi, deve comunicare al sistema di distribuzione l'avvenuta riassociazione, cosicchè il sistema di distribuzione può sempre univocamente determinare un AP che serve la stazione che si è spostata da una BSS ad un'altra. In pratica deve avvenire uno scambio d'informazioni tra i due AP coinvolti nell'operazione di roaming. Tutto questo non fa comunque parte dello standard, cosicchè sono stati sviluppate molte soluzioni proprietarie. Vi è comunque un particolare Task Group (IEEE 802.11f) all'interno dell'organizzazione IEEE che sta studiando un protocollo, al momento in fase di bozza, detto IAPP (inter access point protocol) per standardizzare questa procedura.

2.8 Formato dei pacchetti

Ciascun pacchetto MAC (o frame come lo abbiamo chiamato finora), è composto dai seguenti componenti base:

1.*MAC Header*: che comprende informazioni di controllo, informazioni sugli indirizzi mittente e destinatario, etc.

2.*Frame Body*: di lunghezza variabile, contiene informazioni relative al tipo di frame specificato nell'header (ad esempio, se il frame è di tipo dati il frame body conterrà i dati stessi, ovvero il payload).

3.*Frame Check Sequence* (FCS): è il CRC a 32 bit usato per rilevare gli errori di ricezione.

2.8.1 Formato generale dei frame

La figura 2.24 illustra il formato dei frame MAC del protocollo IEEE 802.11:

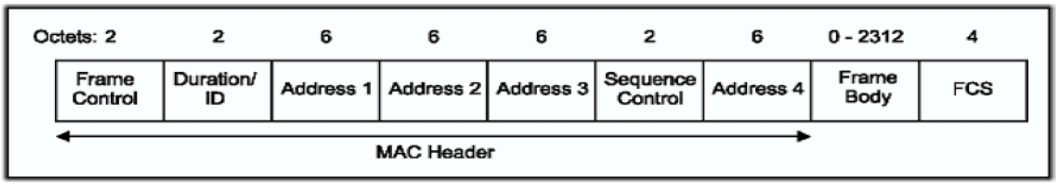


Figura 2.24: Formato generale del frame MAC

I campi: *Address 1, Address 2, Address 3, Sequence Control, Address 4* e *Frame Body* sono presenti solo in alcuni tipi di frame.

2.8.2 Descrizione dei campi

Frame control

La figura 2.25, mostra il contenuto del campo frame control incluso nell'header:

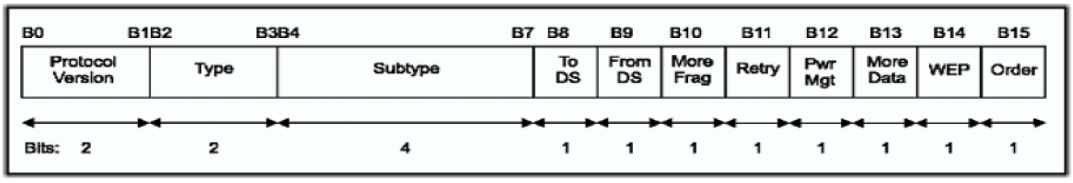


Figura 2.25: Formato del Frame Control Field

E' opportuno analizzare alcuni campi di maggiore importanza:

Campi Type e Subtype

Lo standard prevede 3 tipi di frame: data, control e management. Ciascuno dei tipi ha a sua volta molti sottotipi e questi possono essere riassunti nelle tabelle 2.13 e 2.14:

Type (b3,b2)	Descrizione type	Subtype (b7,b6,b5,b4)	Descrizione subtype
00	management	0000	association request
00	management	0001	association response
00	management	0010	reassociation request
00	management	0011	reassociation response
00	management	0100	probe request
00	management	0101	probe response
00	management	0110-0111	riservati
00	management	1000	beacon
00	management	1001	ATIM
00	management	1010	disassociation
00	management	1100	deauthentication
00	management	1101-1111	riservati

Tabella 2.13: Valori possibili dei campi Type e Subtype del frame control field

Type (b3,b2)	Descrizione type	Subtype (b7,b6,b5,b4)	Descrizione subtype
01	control	0000-0001	riservati
01	control	1010	PS-Poll
01	control	1011	RTS
01	control	1100	CTS
01	control	1101	ACK
01	control	1110	CF-End
01	control	1111	CF-End+CF-ACK
10	data	0000	data
10	data	0001	data+CF-ACK
10	data	0010	data+CF-Poll
10	data	0011	data+CF-ACK+CF-Poll
10	data	0100	Null
10	data	0101	CF-ACK
10	data	0110	CF-Poll
10	data	0111	CF-ACK+CF-Poll
10	data	1000-1111	riservati

Tabella 2.14: Valori possibili dei campi Type e Subtype del frame control field (continua)

Campi ToDS e FromDS

Le diverse combinazioni dei campi ToDS e FromDS e i loro significati possono essere riassunti nella seguente tabella:

ToDS	FromDS	Significato
0	0	E' presente in un frame di tipo dati che va da una STA ad un'altra nella stessa IBSS, ed è presente in tutti i frame di tipo control e management
0	1	E' presente nei frame di tipo dati destinati al DS
1	0	E' presente nei frame di tipo dati provenienti dal DS
1	1	E' presente nei frame che transitano da un AP ad un altro Ap tramite il Wireless DS (WDS)

Tabella 2.15: Combinazioni dei campi To/From DS nei frame di tipo dati

Campo More Fragments

Questo bit, se posto ad 1, indica che il frame corrente è una parte (MPDU) di un messaggio (MSDU) che è stato frammentato a livello MAC, e quindi seguiranno altri frammenti dello stesso messaggio. Il suo valore è 0 in tutti gli altri casi.

Campo Retry

Il bit retry è posto a 1 se il frame corrente rappresenta una ritrasmissione di un frame precedente. Questo è utile nella rilevazione dei frame duplicati.

Campo WEP

Il bit WEP, se settato a 1, indica che il *Frame Body* (ovvero il payload) contiene delle informazioni che sono state cifrate con l'algoritmo WEP. Solo i frame del tipo Data e del tipo Management, sottotipo Authentication, possono avere il bit WEP settato a 1, tutti gli altri frame hanno tale bit settato a 0. Se il bit WEP è settato a 1, il frame body aumenta di dimensione come si vede dalla figura 2.26:

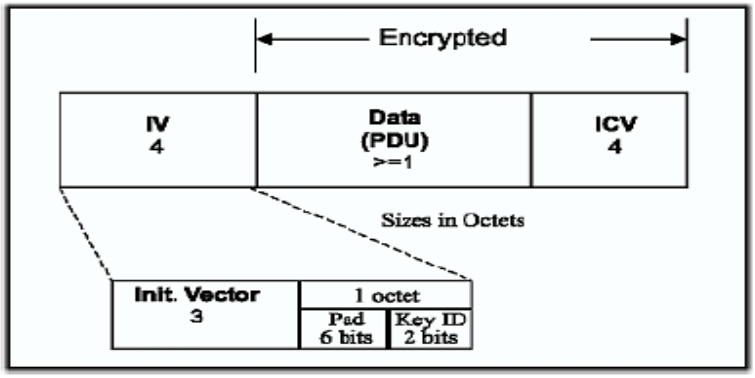


Figura 2.26: WEP

Il processo di cifratura espande il frame body di 8 bytes.

Campo Duration/ID

Le dimensioni di questo campo sono 16 bit e il suo contenuto può essere riassunto dalla tabella seguente:

Bit 15	Bit 14	Bit 13-0	Uso
0	0-32767		Durata
1	0	0	Valore fisso tra i frame trasmessi durante il CFP
1	0	1-16383	Riservato
1	1	0	Riservato
1	1	1-2007	AID per i frame di tipo PS-Poll
1	1	2008-16383	Riservato

Tabella 2.16: Codifica dei bit del campo Duration/ID

Come già visto, il campo Duration/ID è usato per aggiornare il NAV delle STA che accedono al mezzo secondo le regole del metodo DCF.

Campi di tipo Address

Nell'header dei pacchetti MAC IEEE 802.11 vi sono 4 campi dedicati agli indirizzi, ciascuno dei quali contiene un indirizzo a 48 bit conforme allo standard IEEE Std 802-1990. Un indirizzo MAC può essere di 2 tipi:

1. Indirizzo individuale. L'indirizzo associato ad una particolare STA nella rete.
2. Indirizzo di gruppo. Un indirizzo relativo a destinazioni multiple. Anche qui abbiamo 2 sottotipi:
   - Multicast. Un indirizzo associato, a livello superiore al MAC, ad un gruppo di STA della rete.
   - Broadcast. Un particolare indirizzo multicast che indirizza tutte le STA appartenenti ad una specifica LAN. Quando i bit del campo Destination Address sono tutti pari a 1, questa situazione viene interpretata come un trasferimento broadcast.

I suddetti 4 campi dedicati agli indirizzi possono contenere una delle seguenti indicazioni: BSSID (BSS *Identifier*), *Destination Address* (DA), *Source Address*

(SA), *Trasmitter Address* (TA) e *Receiver Address* (RA), sebbene alcuni frame possano non contenere alcuni dei campi d'indirizzo.

In alcuni casi, l'uso di un particolare campo d' indirizzo è direttamente collegato alla sua posizione (1-4) all'interno dell'header del frame MAC. Ad esempio, quando una STA vuole confrontare il proprio indirizzo con l'indirizzo destinazione di un frame, controlla sempre il contenuto del campo Address 1, oppure l'indirizzo del ricevente (ovvero della STA destinataria immediatamente successiva) dei frame CTS e ACK è sempre ottenuta dal campo Address 2 nel corrispondente frame RTS o nel frame che si sta confermando con l'ACK.

BSSID

Questo campo rappresenta un indirizzo a 48 bit avente lo stesso formato degli indirizzi MAC IEEE 802, che identifica univocamente ciascuna BSS. Se quest'ultima possiede un'infrastruttura, ovvero è presente l'AP, il campo BSSID rappresenta l'indirizzo MAC della STA in cui risiede l'AP.

In una IBSS, quest'indirizzo viene generato casualmente.

Il valore pari a tutti 1 del campo BSSID, rappresenta una situazione di broadcast per tutte le BSS. Può essere usato solo nei frame di tipo probe request (vedi 2.7).

Destination address (DA)

Il campo DA contiene un indirizzo MAC (individuale o di gruppo) che identifica la (o le) entità MAC intese come destinataria (o destinatarie) finale della MSDU (o del singolo frammento MPDU) contenuto nel frame body.

Source Address (SA)

Il campo SA contiene un indirizzo MAC individuale che identifica l'entità MAC dalla quale ha avuto origine la trsmissione della MSDU (o MPDU).

Receiver Address (RA)

Il campo RA contiene un indirizzo MAC (individuale o di gruppo) che identifica l'entità (o le entità) MAC che, relativamente al WM (*Wireless Medium*), sarà l'immediata destinataria del frame body corrente.

Trasmitter Address (TA)

Il campo TA contiene un indirizzo MAC individuale che identifica la STA che ha trasmesso, relativamente al WM, la MPDU contenuta nel frame body.

Campo Sequence control

Il campo Sequence Control è costituito da 16 bit: 12 bit di Sequence Number e 4 bit di Fragment Number. Il campo sequence number contiene il numero di sequenza di una MSDU o di una MMPDU. Ad ogni MSDU o MMPDU trasmessa da una STA viene assegnato un sequence number, tramite un contatore modulo 4096, che parte da 1 e viene incrementato di uno per ogni MSDU o MMPDU. Ciascun frammento della stessa MSDU o MMPDU contiene lo stesso sequence number che è stato assegnato a quella MSDU o MMPDU. Il sequence number rimane invariato per tutte le ritrasmissioni della MSDU o MMPDU oppure di uno dei loro frammenti.

Il campo fragment number indica il singolo frammento di una MSDU o MMPDU. Tale campo è 0 per il primo frammento di una MSDU o MMPDU e viene incrementato di uno per ogni frammento trasmesso.

Rimane tuttavia costante durante le ritrasmissioni di uno stesso frammento.

Campo FCS

Questo campo contiene un codice CRC (*Cyclic Redundancy Check*) a 32 bit, calcolato su tutti i campi dell'header e del frame body. Il polinomio generatore del FCS è:

$$G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

2.8.3 Descrizione di alcuni frame importanti

E' utile, a titolo di esempio, riportare la composizione di alcuni frame che abbiamo visto essere importanti per il corretto funzionamento di una WLAN IEEE 802.11

Composizione dei frame di tipo dati

La composizione di un frame di tipo dati non dipende non varia a seconda dei sottotipi, ed è definito dalla figura 2.27:

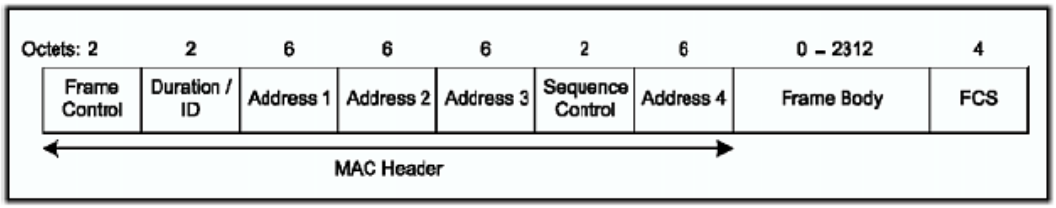


Figura 2.27: Composizione del frame di tipo dati

Il contenuto dei campi d'indirizzo dipende dai valori dei campi ToDS e FromDS, come si vede dalla tabella 2.17, e ricordando che i valori ToDS e FromDS possono essere interpretati come da tabella 2.15:

ToDs	FromDS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Tabella 2.17: Relazione tra To/From DS e i campi Address in un frame dati

Quando il contenuto del campo è N/A, il campo stesso è omesso. Il campo Address 1 contiene sempre l'indirizzo MAC del destinatario del frame, mentre il campo Address 2 contiene sempre l'indirizzo MAC della STA che sta trasmettendo il frame.

Una STA usa in contenuto del campo Address 1 per capire se il frame è ad essa indirizzato. Nel caso in cui il campo Address 1 contenga un indirizzo di gruppo (multicast o broadcast), viene esaminato anche il valore BSSID per capire se il frame multicast o broadcast ha avuto origine nella stessa BSS della STA ricevente.

Una STA usa il contenuto del campo Address 2 per indirizzare il frame ACK, quando richiesto.

RA è l'indirizzo MAC del'AP che nel sistema di distribuzione wireless è l'immediato destinatario del frame, o del frammento. TA invece è l'indirizzo MAC dell'AP che, sempre nel sistema di distribuzione wireless, è l'immediato mittente del frame o del frammento.

Il valore BSSID viene così interpretato:

- se la WLAN è di tipo ``con infrastruttura", il BSSID coincide con l'indirizzo MAC della STA IEEE 802.11 che funziona da AP;
- se la WLAN è una rete ad hoc (IBSS), il BSSID è l'identificativo della IBSS (scelto casualmente).

Il frame body consiste nell'MSDU (o in un suo frammento MPDU) più i campi aggiunti dal WEP nel caso sia stata attivata quest'opzione. Il frame body è nullo nei frame Null, CF-ACK, CF-Poll, e CF-ACK+CF-Poll.

Il campo *Duration* viene inizializzato come segue:

- Per tutti i frame inviati durante il CFP, viene impostato al valore 32768
- Per i frame inviati durante il CP:

1. Se il campo *Address 1* contiene un indirizzo di gruppo, il campo *Duration* viene azzerato.
2. Se il campo *More Fragments* è 0 nel Frame *Control Field* e il campo *Address 1* contiene un indirizzo individuale, nel campo *Duration* viene scritta la durata, in microsecondi, necessaria per trasmettere un frame ACK più un intervallo SIFS.
3. Se il campo *More Fragments* è settato a 1 nel Frame *Control Field* (dunque si tratta di un frammento di MSDU) e il campo Address 1 contiene un indirizzo individuale, nel campo Duration viene scritta la durata, in microsecondi,

necessaria a trasmettere il successivo frammenti delle MSDU in questione più 2 frame ACK più 3 intervalli SIFS.

Composizione generale dei frame di tipo Management

Anche la composizione dei frame di tipo Management non varia a seconda dei diversi sottotipi. Possiamo osservare tale composizione in figura 2.28:

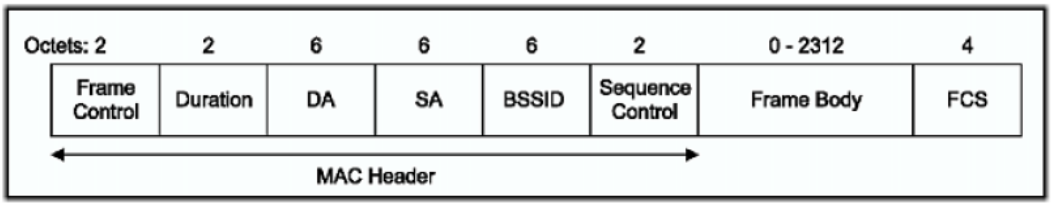


Figura 2.28: Composizione dei frame di tipo management

Il frame body è composto in parte da campi di dimensione fissata, ed in parte da elementi informativi, ovvero raggruppamenti di più dati che possono avere dimensione variabile. Alcuni campi o elementi informativi sono obbligatori ed è obbligatorio anche l'ordine in cui devono comparire all'interno del frame body.

2.9 Livello fisico (PHY)

Lo standard IEEE 802.11, prevede 3 diverse implementazioni del livello fisico che consente il trasporto delle informazioni tra le STA di una WLAN compatibili:

- *IR Infrarosso*
- *FHSS Frequency Hopping Spread Spectrum* (Radiofrequenza)
- *DSSS Direct Sequence Spread Spectrum* (Radiofrequenza)

Il livello PHY è costituito dalle seguenti 2 funzioni:

- PLCP (*Physical Layer Convergence Function*) che, grazie alla procedura PLCP (*Physical Layer Convergence Procedure*), mappa le MPDU IEEE 802.11 (*Mac Protocol Data Unit*) in frame dal formato compatibile con il sistema PMD (vedi a seguito) ed in generale semplifica l'interfaccia tra il MAC ed il livello PHY.

- PMD (*Physical Medium Dependent*) è un sistema che definisce le caratteristiche di un mezzo trasmissivo wireless (WM) e definisce i metodi per trasmettere e ricevere dati attraverso tale mezzo trasmissivo, oltre a fornire funzioni CCA (*Clear Channel Assessment*).

Nelle sezioni successive analizziamo le implementazioni FHSS e DSSS, poichè sono le più usate nei dispositivi commerciali.

2.9.1 IEEE 802.11 FHSS

Abbiamo già visto nell'Introduzione i principi generali di un sistema di trasmissione a RF (Radiofrequenza) che adotti la tecnica denominata *Frequency Hopping*. Le caratteristiche del PHY FHSS specificato dallo standard IEEE 802.11 sono esaminate di seguito.

Bande operative

Il PHY IEEE 802.11 FHSS è stato definito per operare nella banda ISM 2.4 GHz. Per le normative europee si veda la tabella 2.18.

L'intervallo di frequenze utilizzabile dai dispositivi che usano questo PHY è specificato, relativamente alla posizione geografica, nella seguente tabella:

Limite inferiore (GHz)	Limite superiore (GHz)	Intervallo (GHz)	Area geografica	# di canali
2.402	2.480	2.400-2.4835	Nord America	79
2.402	2.480	2.400-2.4835	Europa (tranne Francia e Spagna)	79
2.473	2.495	2.471-2.497	Giappone	23
2.447	2.473	2.445-2.475	Spagna	27
2.448	2.482	2.4465-2.4835	Francia	35

Tabella 2.18: Bande operative IEEE 802.11 FHSS

Come si vede dalla tabella 2.18, in Europa (escluse Francia e Spagna) sono definite canali di hop, non sovrapposti e spaziati di 1 MHz.

Livelli di potenza di emissione

In Europa, il limite imposto alla potenza di trasmissione dei dispositivi IEEE 802.11 è 100 mW EIRP. Lo standard impone inoltre che tutti i dispositivi realizzati in conformità con esso debbano supportare almeno un livello di potenza trasmessa pari a 10 mw EIRP.

Nel caso in cui si realizzasse un dispositivo conforme allo standard, ma con la capacità di trasmettere segnali di potenza maggiore di 100 mW EIRP, dev'essere implementato un meccanismo di controllo della potenza di trasmissione che operi in modo da ridurre la potenza del segnale trasmesso ad un livello minore o uguale a 100 mW, quando necessario.

Modulazione del segnale

La trasmissione del segnale avviene usando la modulazione GFSK (*Gaussian Frequency Shift Keying*) con un prodotto BT (*bandwitdh-time*) pari a 0.5; in particolare:

** 2-GFSK*

Questa modulazione prevede che il simbolo 1 venga codificato con una deviazione positiva (+fd), rispetto alla portante Fc, mentre prevede che il simbolo 0 venga codificato con una deviazione negativa (−fd), rispetto alla portante. La velocità di segnalazione (Fclk) è pari ad 1 Msimbolo/s, cosicchè otteniamo una velocità di trasferimento (data-rate) pari a 1 Mbit/s. Il fattore di deviazione h2 (definito come la differenza tra le frequenze al centro delle sequenze 0000 e 1111 diviso per 1 MHz), è 0.32. Quindi si ha:

1 Mbit/s, 2GFSK	
Simbolo	**Deviazione dalla portante**
1	$[1/2]\cdot h_2\cdot F_{clk}$=160 *KHz*
0	$-[1/2]\cdot h_2\cdot F_{clk}$

Tabella 2.19: Codifica dei simboli 2GFSK

** 4-GFSK*

Questa modulazione prevede la seguente codifica:

2 Mbit/s, 4GFSK	
Simbolo	**Deviazione dalla portante**
10	$[3/2]\cdot h_4 \cdot F_{clk}$=216 *KHz*
11	$[1/2]\cdot h_4 \cdot F_{clk}$=72 *KHz*
01	$-[1/2]\cdot h_4 \cdot F_{clk}$
00	$-[3/2]\cdot h_4 \cdot F_{clk}$

Tabella 2.20: Codifica dei simboli 4GFSK

Ove $h_4=0.45\times h_2=0.144$. Questa codifica consente di raddoppiare il data rate: la velocità di segnalazione è sempre 1 Msimbolo/s , ma ogni simbolo codifica 2 bit di informazione e quindi otteniamo un data rate di 2Mbit/s.

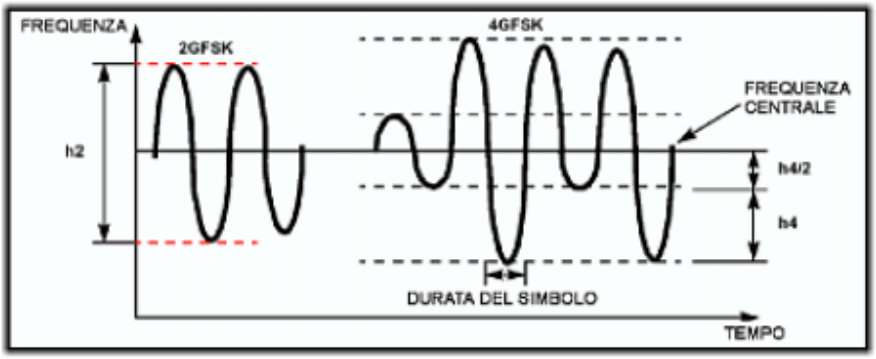


Figura 2.29: Modulazioni usate dal livello fisico FHSS

Generazione delle sequenze di hopping

Facciamo in seguito riferimento a sistemi che possiedono 79 canali di hop (USA e Europa tranne Francia e Spagna). Ogni singola entità PMD (ovvero ogni STA) genera una sequenza pseudocasuale composta da 79 hop. Sono previste 78 diverse sequenze, organizzate in 3 insiemi da 26 sequenze ciascuno. L'algoritmo di generazione assicura una distanza minima di 6 canali tra due hop consecutivi. I 3 insiemi da 26 sequenze

sono stati pensati per facilitare l'allocazione di più reti nella stessa area; il rischio di collisioni tra pacchetti trasmessi da STA che operano in reti WLAN che usano sequenze di hopping appartenenti a insiemi diversi è minimo, e alcuni test indicano che il throughput non degrada sensibilmente anche se si collocano fino a 15 diverse reti nella stessa area.

Definiamo Fx lo schema composto dalle 79 frequenze di hop per una specifica WLAN (o BSS, ovviamente tutte le STA della WLAN adottano lo stesso schema Fx).

$$Fx=\{f_x(1),f_x(2),\ldots,f_x(p)\}$$

ove:

- fx(i) è il numero del canale per la i-esima frequenza dell'x-esimo schema di hopping.
- p è il numero dei canali disponibili (nel nostro caso p=79).

La frequenza fx(i) viene calcolata così:

$$f_x(i)=[b(i)+x] mod\ (79)+2$$

dove b(i) rappresenta l'i-esimo elemento della cosiddetta base hopping sequence, definita, sempre nel caso dei sistemi con 79 hop, dalla seguente tabella:

i	*b(i)*	*i*	*b(i)*	*i*	*b(i)*	*i*	*b(i)*	*i*	*b(i)*	*i*	*b(i)*	*i*	*b(i)*	*i*	*b(i)*
1	0	11	76	21	18	31	34	41	14	51	20	61	48	71	55
2	23	12	29	22	11	32	66	42	57	52	73	62	15	72	35
3	62	13	59	23	36	33	7	43	41	53	64	63	5	73	53
4	8	14	22	24	71	34	68	44	74	54	39	64	17	74	24
5	43	15	52	25	54	35	75	45	32	55	13	65	6	75	44
6	16	16	63	26	69	36	4	46	70	56	33	66	67	76	51
7	71	17	26	27	21	37	60	47	9	57	65	67	49	77	38
8	47	18	77	28	3	38	27	48	58	58	50	68	40	78	30
9	19	19	31	29	37	39	12	49	78	59	56	69	1	79	46
10	61	20	2	30	10	40	25	50	45	60	42	70	28	—	—

Figura 2.30: Base hopping sequence per USA e Europa (tranne Francia e Spagna)

Come abbiamo già detto, sono definiti nello standard 78 schemi (o sequenze) di hopping, ovvero 78 permutazioni delle 79 frequenze disponibili, organizzati in 3 insiemi da 26 schemi ciascuno. Questi insiemi sono:

1.x={0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}

2.x={1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}

3.x={2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}

Facciamo un esempio per chiarire meglio: supponiamo che una STA operi in una WLAN che adotta lo schema 33 che appartiene al set 1, mentre un altra STA operi in un'altra WLAN collocata nella stessa area della prima WLAN ma adottando lo schema 71, che appartiene al set 3. Allora gli hop della prima STA saranno definiti dalla relazione:

$$F_{33}=\{f_{33}(1),f_{33}(2),\ldots,f_{33}(79)\}$$

e

$$f_{33}(1)=[b(1)+33]mod\ (79)+2=0+33+2=35\Rightarrow 2.435\ GHz$$

$$f_{33}(2)=[b(2)+33]mod\ (79)+2=23+33+2=58\Rightarrow 2.458\ GHz$$

e cosi via. Come si vede, tra gli hop 1 e 2 vi è una distanza di 23 MHz, e questo è utile per ridurre la possibilità di collisioni successive: se il canale 1 (f=2.435 GHz) risultasse disturbato ed il pacchetto trasmesso utilizzando quella frequenza non venisse inviato o ricevuto correttamente, la successiva ritrasmissione avvererebbe sul canale 2 (f=2.458 GHz) che dista dal primo 23 MHz e, presumibilmente, non è coinvolto nei disturbi che agivano sul canale 1. Allo stesso tempo, osserviamo la sequenza generata per la seconda WLAN, sovrapposta geograficamente alla prima, ma che utilizza lo schema 71 del set 3:

$$F_{71}=\{f_{71}(1),f_{71}(2),\ldots,f_{71}(79)\}$$

e

$$f_{71}(1)=[b(1)+71]mod\ (79)+2=0+71+2=73\Rightarrow 2.473\ GHz$$

$$f_{71}(2)=[b(2)+71]mod\ (79)+2=15+2=17\Rightarrow 2.417\ GHz$$

e cosi via. Come si vede, vale lo stesso discorso fatto per la prima WLAN per quel che riguarda le interferenze sui singoli canali; inoltre le frequenze che fanno parte dello schema scelto dalla seconda WLAN saranno per la maggior parte differenti da quelle che fanno parte dello schema scelto dalla prima WLAN, cosicchè si minimizza il rischio di collisione tra i pacchetti delle diverse WLAN.

Hop Rate

L'hop rate, ovvero la frequenza con la quale viene cambiato il canale di hop è 2.5 hop/s (quindi la frequenza operativa cambia ogni 400 ms).

Formato dei pacchetti PLCP

Il formato dei pacchetti PLCP è descritto dalla figura seguente:

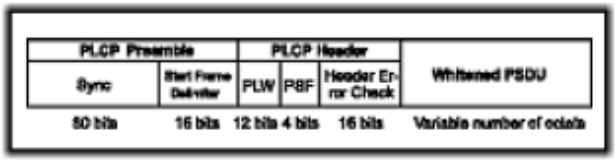


Figura 2.31: FHSS: formato dei pacchetti PLCP

Il PLCP Preamble viene trasmesso sempre a 1Mbps e dev'essere completato in 96μs. Contiene delle informazioni utili per la compensazione dell'offset di frequenza, l'aggiustamento del guadagno, selezione dell'antenna. Il campo SFD (*start frame delimiter*) è una sequenza prefissata di bit che segnala l'inizio vero e proprio del frame. Il PLCP Header viene trasmesso sempre a 1 Mbps e dev'essere completato in 32μs. PLW specifica il numero di byte contenuti nella PSDU, mentre PSF specifica il data rate utilizzato per trasmettere la PSDU.

2.9.2 IEEE 802.11 DSSS

Ancora una volta, possiamo far riferimento a quanto visto nell'Introduzione per quello che riguarda l'implementazione *Direct Sequence* della tecnica *Spread Spectrum*. Le caratteristiche del PHY DSSS dello standard IEEE 802.11 sono esaminate nel seguito.

Bande operative

Il PHY IEEE 802.11 DSSS è stato definito per operare nella banda ISM 2.4 GHz. Per le normative europee si veda la tabella. La tabella seguente riporta le frequenze centrali e gli identificativi (CHNL_ID) dei canali disponibili:

		Normative					
CHNL_ID	Frequenza	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412 MHz	X	X	X	—	—	—
2	2417 MHz	X	X	X	—	—	—
3	2422 MHz	X	X	X	—	—	—
4	2427 MHz	X	X	X	—	—	—
5	2432 MHz	X	X	X	—	—	—
6	2437 MHz	X	X	X	—	—	—
7	2442 MHz	X	X	X	—	—	—
8	2447 MHz	X	X	X	—	—	—
9	2452 MHz	X	X	X	—	—	—
10	2457 MHz	X	X	X	X	X	—
11	2462 MHz	X	X	X	X	X	—
12	2467 MHz	—	—	X	—	X	—
13	2472 MHz	—	—	X	—	X	—
14	2484 MHz	—	—	—	—	—	X

Figura 2.32: Canali disponibili IEEE 802.11 DSSS

Ogni canale ha un'ampiezza di 22 MHz. Nel caso in cui si vogliano allocare nella stessa area più WLAN, per limitare l'interferenza reciproca, è necessario che le frequenze centrali dei canali di ogni WLAN siano spaziate di almeno 25 MHz.

Codifica

Il PHY DSSS dello standard IEEE 802.11 usa, per codificare il flusso informativo, una particolare sequenza di Barker composta da 11 simboli (cosiddetti chip). La sequenza scelta è:

+1,−1,+1,+1,−1,+1,+1,+1,−1,−1,−1

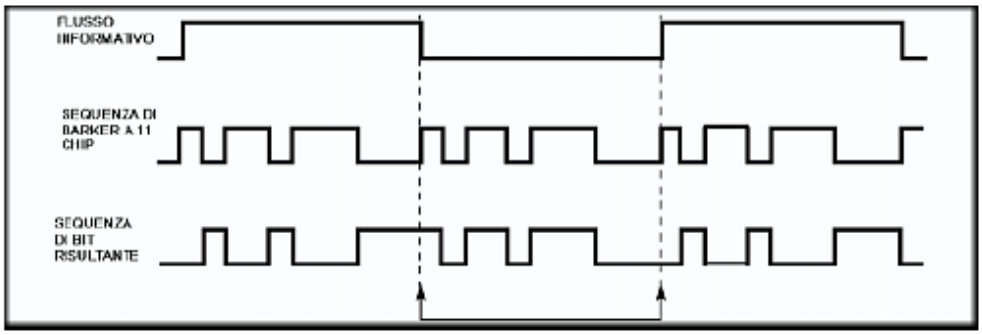


Figura 2.33: Sequenza di Barker per IEEE 802.11 DSSS

Le sequenze di Barker possiedono buone proprietà di correlazione aperiodica, che significa semplicemente che, a causa del comportamento non ripetitivo del codice di Barker, un filtro a comparazione può facilmente riconoscere il codice di Barker in una sequenza di bit.

Modulazioni e data rate

Lo standard specifica 2 modulazioni e 2 data rate associati alle modulazioni stesse, per il PHY DSSS: un basic access rate, basato sulla modulazione DBPSK (*Differential Binary Phase Shift Keying*), ed un enhanced access rate, basato sulla modulazione QBPSK (*Quadrature Binary Phase Shift Keying*).

Bit in ingresso	Modifica alla fase (+$j\omega$)
0	0
1	π

Tabella 2.21: Modulazione DBPSK

Sequenza di 2 bit d0, d1 (d0 primo nel tempo)	Modifica alla fase (+$j\omega$)
00	0
01	[π/2]
11	π
10	[3/2]·π

Tabella 2.22: Modulazione QBPSK

La velocità di modulazione è pari a 1Msimbolo/s. Un simbolo è composto dagli 11 chips della sequenza di Barker vista. Se si sceglie la modulazione DBPSK, si ottiene un data rate pari a 1 Mb/s, poichè ogni simbolo codifica 1 bit d'informazione. Se invece si sceglie la modulazione QBPSK, si ottiene un data rate di 2 Mb/s, poiché ogni simbolo codifica 2 bit d'informazione.

Spettro del segnale modulato

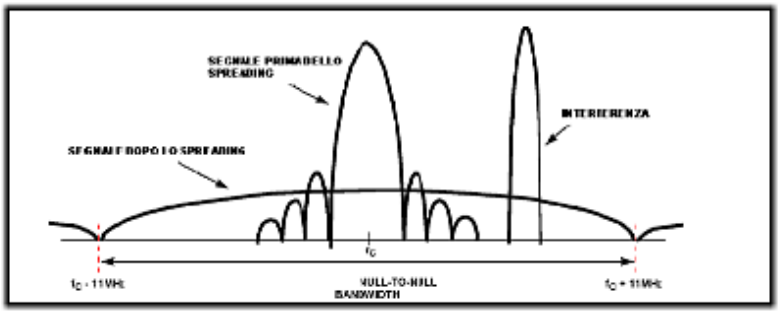


Figura 2.34: DSSS: spettro del segnale modulato

La figura 2.34 mostra lo spettro del segnale DSSS prima e dopo lo spreading. Si noti che lo spettro ha la forma di un inviluppo dall'espressione:

$$\left(\frac{\sin x}{x}\right)^2$$

La modulazione (ovvero la somma modulo 2 del segnale in banda base e della sequenza di barker), effettivamente espande il segnale su una banda più ampia. Il lobo principale della figura 2.34 è una funzione della forma d'onda modulante e della velocità di chipping. Una regola comunemente usata nei sistemi DSSS consiste nel fissare la banda null to null al doppio del valore della velocità di chipping. Usando quindi una sequenza di Barker a 11 chip, con un chip rate di 11 Mcps (mega chip per second), la banda null to null del segnale espanso risulta 22MHz. Questo consente di allocare nella banda ISM 2.4 GHz fino a 3 canali DSSS non sovrapposti.

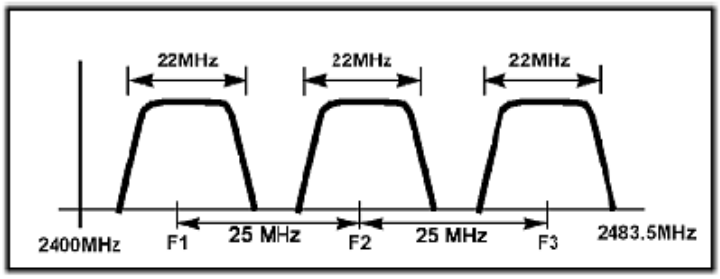


Figura 2.35: DSSS: canali non sovrapposti nella banda ISM

Formato dei pacchetti PLCP

Il formato dei pacchetti PLCP è descritto dalla figura seguente:

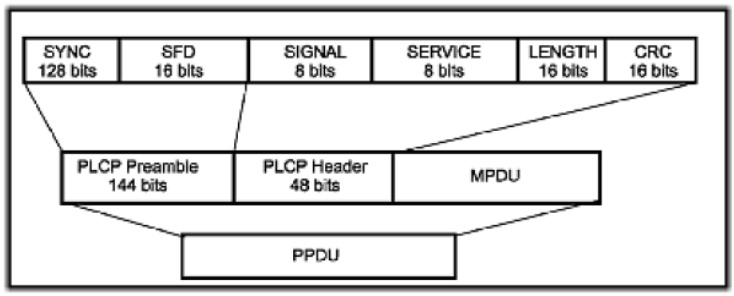


Figura 2.36: DSSS: formato dei pacchetti PLCP

Sia il PLCP Preamble che il PLCP Header devono essere trasmessi a 1Mbps.

2.9.3 IEEE 802.11 Hi-Rate DSSS

Nel 1998, Lucent Technologies e Harris Semiconductor (ora parte della Intersil Corp.) proposero all'istituto IEEE l'inserimento nello standard della tecnica di codifica CCK (*Complementary Code Keying*), la quale, utilizzata per effettuare lo spreading dei segnali nell'implementazione PHY DSSS al posto della sequenza di Barker, consentiva di raggiungere velocità di trasferimento dei dati di 5.5 Mbps e 11 Mbps. L'istituto IEEE accettò tale proposta e, nel 1999, venne rilasciata la specifica IEEE 802.11b, che non prevede modifiche al livello MAC, ma introduce sostanziali novità per l'implementazione DSSS del livello PHY.

CCK

I codici CCK usati nello standard IEEE 802.11b per effettuare lo spreading dei segnali per il PHY DSSS, appartengono alla classe dei polyphase complementary codes, hanno una lunghezza di 8 chip e un chipping rate di 11Mchip/s. Quindi un simbolo è rappresentato da 8 chip complessi. Usando una velocità di segnalazione di 1.375 MSimboli/s (contro gli 1 MSimboli/s dello standard IEEE 802.11), il segnale a 11Mbps ottenuto occuperà la stessa banda del segnale a 2Mbps dello standard IEEE 802.11, consentendo quindi l'allocazione di 3 canali non sovrapposti nella banda ISM.

La code word CCK da 8 chip viene ottenuta dalla formula seguente:

$$c=\{\, e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)},$$
$$-e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_1}\}$$

Con questa formula quindi si generano i codici CCK usati per ottenere data rate di 11Mbps e 5.5Mbps. Scegliendo il data rate 11Mbps, gli 8 codici generati (un simbolo quindi) codificano 8 bit d'informazione, mentre per il data rate 5.5Mbps vengono trasmessi 4 bit per simbolo e quindi gli 8 codici generati codificano 4 bit d'informazione. Facciamo un esempi o riferendoci al data rate 11Mbps. Il flusso informativo viene partizionato in byte (d7,d6,d5, ...,d0), ove d0 è il LSB ed il primo bit in ordine di tempo. Questi 8 bit vengono usati per generare i parametri di fase $\Phi_1-\Phi_4$, come si può vedere dalla tabella seguente:

DIBIT	Parametro di fase
(d0,d1)	φ_1
(d3,d2)	φ_2
(d5,d4)	φ_3
(d7,d6)	φ_4

Tabella 2.23: Schema per la generazione dei parametri di fase

La codifica si basa sulla modulazione DQPSK (*differential quadrature phase shift keying*), che può essere visualizzata nella seguente tabella:

DIBIT (d_{i+i},d_i,)	Fase
00	0
01	π
10	[π/2]
11	−[π/2]

Tabella 2.24: Modulazione QPSK dei parametri di fase

Ad esempio, se il flusso dei dati fosse d7,d6,d5, ...,d0=10110101, dalle tabelle 1.26 e 1.27, si ha che:

d1,d0=01 e così Φ 1=π, d3,d3=01 e così $\Phi_2=\pi$, d5,d4=11 e così $\Phi_3=-\pi/2$ ed infine d7,d6=10 e così $\Phi_4=\pi/2$.

Riportando tali valori nella formula di c si ha:

$$c=\{\ 1,-1,j,j,-j,j,-1,-1\}$$

avendo applicato anche la formula di Eulero $e^{j\theta}=\cos\theta+j\cdot\sin\theta$.

Nonostante queste modifiche, lo standard IEEE 802.11b prevede comunque l'utilizzo della tecnica di spreading DSSS che utilizza la sequenza di Barker a 11 chip che abbiamo già visto in 2.9.2, cosicché i dispositivi realizzati secondo lo standard IEEE 802.11b sono compatibili e quindi possono comunicare con quelli realizzati secondo lo standard IEEE 802.11.

Bande operative

Non sono state specificate modifiche alle frequenze centrali che caratterizzano i canali disponibili per la realizzazione di WLAN IEEE 802.11b. Nello standard IEEE 802.11b tuttavia, è stata aumentata a 30 MHz (contro i 25 MHz dello standard IEEE 802.11) la distanza minima tra due canali consecutivi qualora si dovesse utilizzare tali canali per allocare due diverse WLAN nella stessa area. Questo permette ancora di

allocare fino a 3 WLAN con canali operativi non sovrapposti nella banda ISM 2.4GHz.

In Europa (tranne per Francia e Spagna) abbiamo le seguenti possibilità:

Set	Numero di canali	Numero del canale
1	3	1,7,13
2	7	1,3,5,7,9,11,13

Tabella 2.25: IEEE802.11: canali operativi in Europa (tranne Francia e Spagna)

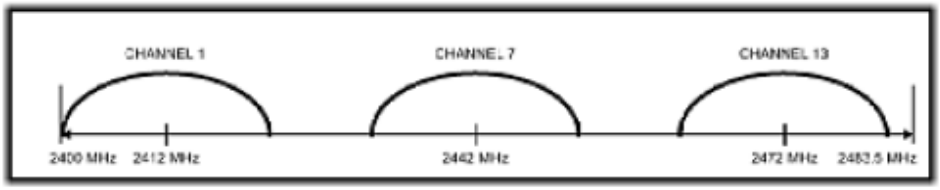


Figura 2.37: IEEE802.11: canali non sovrapposti

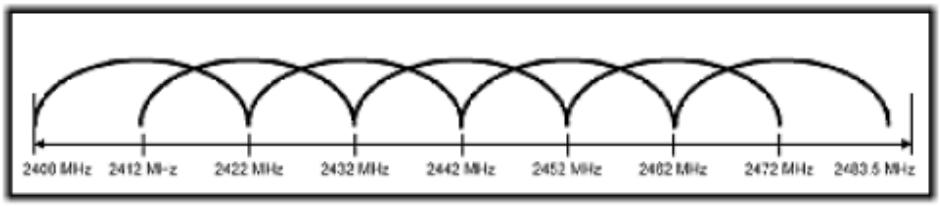


Figura 2.38: IEEE802.11: canali sovrapposti

Formato dei pacchetti PLCP

Lo standard specifica due diversi tipi di PLCP Preamble e PLCP Header:

- *Long Preamble e Long Header*, obbligatori e necessari per l'interoperabilità con i dispositivi realizzati secondo lo standard IEEE 802.11
- *Short Preamble e Short Header*, opzionali.

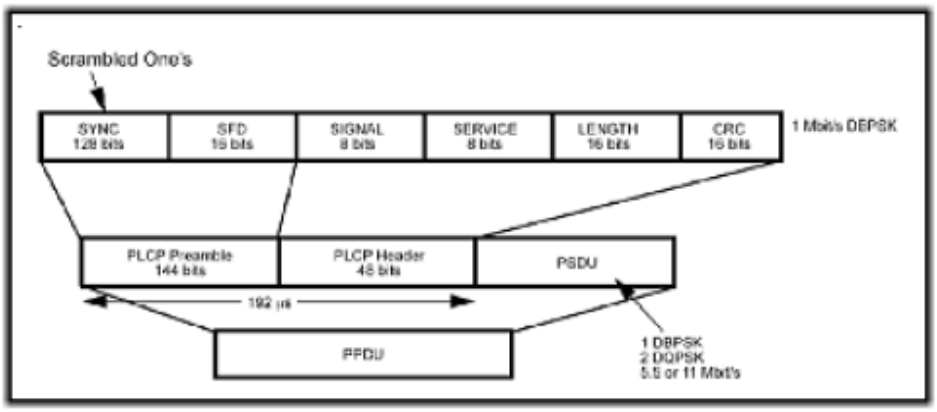


Figura 2.39: IEEE802.11: formato dei pacchetti PLCP con Long Preamble e Header

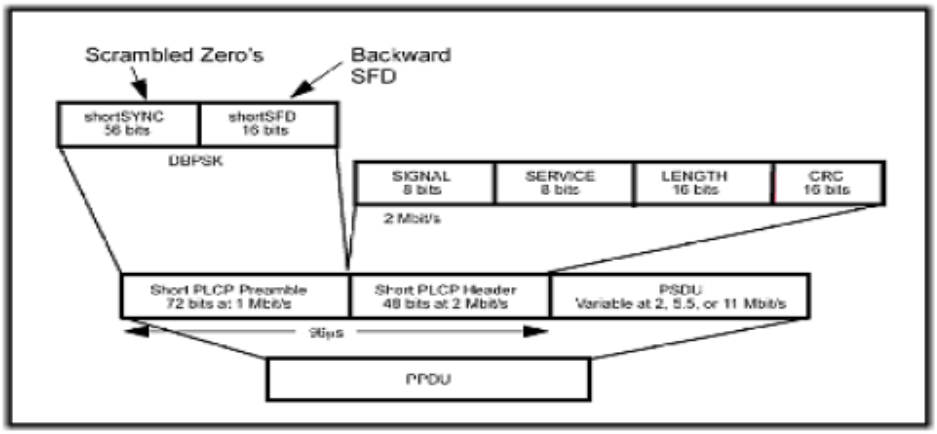


Figura 2.40: IEEE802.11: formato dei pacchetti PLCP con Short Preamble e Header

L'utilizzo dello *Short Preamble* e dello *Short Header* è utile per ridurre l'overhead e quindi migliorare il *throughput* totale della rete. Lo *Short Preamble* viene trasmesso usando la modulazione DBPSK e la solita sequenza di Barker per lo spreading a 1Mbps. Lo *Short Header* viene trasmesso usando la modulazione DQPSK e la solita sequenza di Barker a 2Mbps. La PSDU viene trasmessa a 2, 5.5 oppure 11 Mbps.

CAPITOLO III

HIPERLAN/2

L' HIPERLAN[3] (*HIgh PErfomance Radio Local Area Network*) è una famiglia di standard per la comunicazione digitale ad alta velocità nella banda 5.15-5.13 GHz e 17.1-17.3 Ghz sviluppati dall' ETSI (*European Telecomunications Standards Institute*) nel quadro di uno sforzo chiamato BRAN (*Broad Radio Area Networks*) ed è stato promossa da un gruppo industriale chiamato HiperLAN2 Global Forum, che conta tra i suoi componenti alcuni grosso calibri come BOSH, Dell Computer, Ericsson, Nokia, Telia e Xircom. La funzionalità più attraente dello schema è:

- L'elevata velocità di trasmissione con un throughput continuo per le applicazioni di 20 Mbps.
- Un' altra caratteristica chiave è il supporto per la QoS, particolarmente indispensabile per trasmissioni video e voce.
- Lo schema opera come un'estensione omogenea di altre reti, i nodi di una rete cablata vedono i nodi HIPERLAN come altri nodi della rete.
- Tutti i comuni protocolli di networking layer 3 (IP, IPX, Apple Talk) possono funzionare consentendo l'uso delle applicazioni basate sulla rete.

L'architettura della rete infatti è stata concepita per connessioni con vari tipi di infrastrutture, supporta frame Ethernet, celle ATM e pacchetti IP e PPP. Tutto questo grazie alla definizione di un Convergenze layer, che parleremo più avanti, capace di accettare pacchetti o celle dai sistemi networking già esistenti formattandoli per la distribuzione sul medium wireless.

Opera nella banda di frequenza intorno ai 5.2 GHz (da 5.15 a 5.35 GHz e da 5.470 a 5.725 GHz) con spettro di 455 MHz. La struttura tipica di HIPERLAN/2 prevede dei terminali mobili (*MT-mobile terminal*) che comunicano via radio con un solo punto di accesso(*AP, Access point*) della rete fissa ed, in caso di movimento, il passaggio a punti di accesso adiacenti (handover) avviene in maniera automatica, è

possibile anche la comunicazione diretta tra terminali mobili per mezzo di connessioni ‘ad hoc’(create al momento, con una durata strettamente necessaria allo scambio di dati).

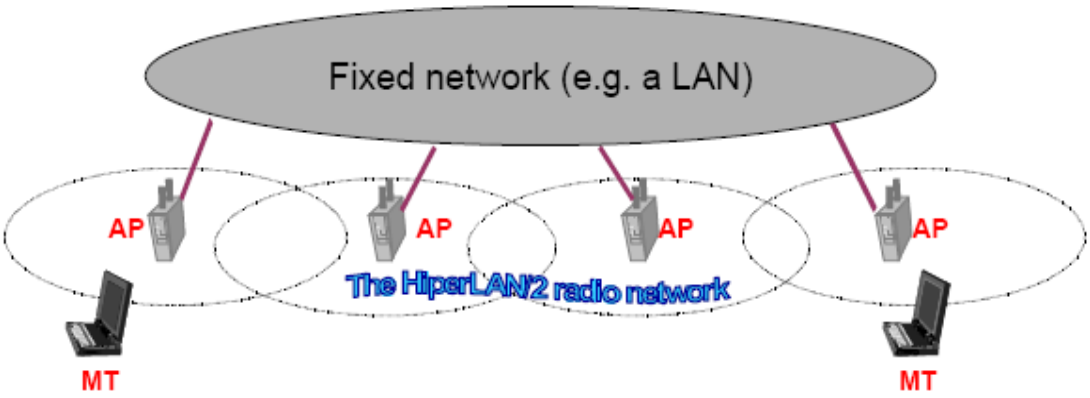


Figura 3.1: rete HIPERLAN/2

L'HIPERLAN2 prevede due modalità di funzionamento:

Centralized mode: ogni AP si connette alla network core che serve le MT a lui associate. Tutto il traffico dei terminali mobili passa attraverso l'AP, sia che appartengano allo stesso AP, sia che appartengano a due core network differenti. Questo è obbligatorio per tutte le MT e gli AP.

Direct mode: l’accesso ai canali di trasmissione è ancora gestito in maniera centralizzata da parte dell’AP, ma il traffico dati avviene direttamente tra i terminali senza passare dell’AP. Questo modo viene usato in ambiente particolarmente piccoli (ad esempio le abitazioni) in cui si aspetta che la maggior parte del traffico avvenga tra terminale associati allo stesso AP. La comunicazione da MT a MT è definita Direct Link (DL). Il medium access è gestito in maniera centralizzata con un CC (central Controller), ma il traffico è scambiato tra i terminali e non passa dal CC. Questo modo è caratteristico di ambienti tipo "home" con un elevato numero di utilizzatori associati allo stesso CC.

3.1 Caratteristica della tecnologia

3.1.1 Trasmissione ad alta velocità

Lo standard HIPERLAN/2 consente di raggiungere data rate molto elevati fino a 54Mbit/s a livello fisico e fino a 25Mbits/s al 3^o livello. A tal fine HIPELAN/2 usa la tecnica di trasmissione OFDM (*Orthogonal Frequency Digital Multiplexing*) che è molto efficiente in ambiente tempo-dispersivi (ad es. gli uffici) in cui il segnale radio trasmesso può essere riflesso molte volte da punti diversi facendo sì che i tempi di propagazione fino al ricevitore possano essere molto diversi da cammino a cammino. Questa variabilità dei ritardi, in corrispondenza di una'alta velocità di trasmissione, può raggiungere una proporzione significativa del simbolo trasmesso (una forma d'onda modulata) portando tale simbolo ad interferire con il successivo (fenomeno noto come "*interferenza intersimbolo*").

Lo schema OFDM combatte questa eventualità dividendo il canale radio in vari subcarrier e trasmettendo i dati in parallelo su di essi. Il *throughput* aggregato finisce per essere identico, ma la velocità dei dati da ogni subcarrier è molto più bassa, rendendo ciascun simbolo piu lungo e quindi in pratica eliminando l'effetto dei ritardi variabili.

L'OFDM richiede tuttavia l'uso di amplificatori di potenza estremamente lineari, che fanno salire il costo degli apparati radio. Come conseguenza, i prodotti hiperlan2 costeranno probabilmente di più rispetto alle alternative caratterizzate da una velocità inferiore.

Le connessioni vengono stabilite tra i terminali mobili (MT) ed i punti di accesso (AP) tramite funzioni di segnalazione tipiche del protocollo. L'accesso è di tipo TDM (*Time Division Multiplexing*). Le connessioni possono essere di due tipi:

- Point-to-poin: bidirezionali
- Point-to-multipoint: sono unidirezionali verso i terminali mobili

Esiste inoltre una canale broadcast che viene usato per raggiungere tutti i terminali da ogni punto di accesso.

3.1.2 Supporto Del QoS(Quality of Service) e della sicurezza

L'approccio di HIEPERLAN2, tipicamente orientato alla connessione, lo rende particolarmente adatto a supportare l'assegnazione di parametri specifici ad ogni connessione (larghezza di banda, ritardo, bit error rate, etc), in base alla qualità del servizio da essa richiesta e quindi al tipo di dati che devono essere trasmessi. È inoltre possibile, seguendo un approccio più semplice, stabilire un livello di priorità tra le varie connessione. Tali caratteristiche, combinate con le alte velocità raggiungibili, consentono la trasmissioni simultanea di diversi tipi di dati (voce, video, dati).

Sicurezza

Per quanto concerne gli aspetti di sicurezza HIPERLAN2 supporta sia l'autenticazione che al codifica : sia gli AP che i MT possono autenticarsi l'una l'altro in modo da garantire l'accesso alla rete solo a chi è autorizzato (dal punto di vista dell'AP). La codifica viene usata, una volta stabilita la connessione, per proteggere i dati trasmessi da intercettazioni indesiderate.

Hiperlan2 introduce per la prima volta meccanismi più completi per la sicurezza nelle reti wireless. Quando una MT lo richiede, l'AP risponde indicando un sottoinsieme di modalità previste per lo strato fisico, un livello di convergenza ed una procedura di crittografia ed autenticazione selezionata.

Se la MT accetta la procedura con crittografia inizia l'algoritmo di Diffie-Hellman con lo scambio di chiavi per negoziare la chiave della sessione segreta per il traffico segreto unicast tra la MT e l'AP.

Algoritmo Diffie-Hellman (DH)

$$K_{pubA} = \alpha^a \bmod p$$

$$K_{pubB} = \alpha^b \bmod p$$

Entrambi valutano:

$$k_x = k_{pubB}{}^a \bmod p = \alpha^{ab} \bmod p$$

$$k_s = k_{pubA}{}^{b} \bmod p = \alpha^{ab} \bmod p$$

Quindi hanno ora una chiave in comune

Hiperlan2 supporta sia DES (data security standard) che il 3DES. AES (Advanced Encryption Standard) è in fase di standardizzazione.

Anche il traffico broadcasting e multicasting può essere protetto attraverso l'uso di chiavi comuni distribuite in maniera cifrata utilizzando chiavi cifrate unicast.

Autenticazione

Per l'autenticazione possono essere utilizzate algoritmi a chiave segreta e pubblica. L'autenticazione è realizzata utilizzando codici di autenticazione di messaggi basata su MD5, HMAC e firma digitale basata su RSA. Meccanismi di risposta a sfide sono anche previsti per realizzare identificazioni.

3.1.3 Selezione Dinamica della Frequenza (Dynamic Frequency Selection, DFS)

Uno degli obiettivi delle specifiche tecniche di HIPERLAN2 è quello di far sì che il sistema operi in modalità Plug-and-Play e senza necessità di pianificazione frequenziale ed è a questo fine che le specifiche prevedono un meccanismo di DFS(*Dynamic Frequency Selection*). Lo scopo è quello di evitare le interferenze da parte di altri apparti, sia dello stesso tipo, sia di tipo diverso, che utilizzano lo stesso spettro di frequenze favorendone un uso il più possibile uniforme.

La funzione di DFS deve essere basata su misure di potenza di segnale sia all'AP sia al terminale associato , e in entrambi i casi sia sul proprio canale operativo, sia su altri canali. Infatti, se è vero che la selezione automatica del canale di frequenza da parte dell'AP rappresenta il primo passo all'accensione dell'apparato, è anche vero che nel tempo, per sopraggiunti motivi di interferenza, L'AP sia costretto a spostarsi dal canale inizialmente selezionato. Analogamente, possono esserci terminali che, trovandosi in particolari situazioni di interferenza, non siamo più in grado di comunicare con l'AP in modo efficiente.

Nel meccanismo di DFS specificato in Hiperlan2, sia l'AP sia il terminale devono quindi essere in grado di effettuare misure di potenze di segnale ricevuto a una data frequenza; inoltre , per quanto detto sopra, l'attivazione della misura può avvenire sia su richiesta dell'AP, sia su iniziativa del terminale. L'algoritmo con cui l'AP effettua la scelta di cambiare non è invece specificato dallo standard, per cui ogni manifatturiera ha facoltà do realizzarne uno proprio.

3.1.4 Supporto della mobilità

Ogni terminale mobile (MT) o comunica con il punto di accesso (AP) che garantisce il miglior segnale radio misurato in termini di rapporto segnale/rumore; perciò, muovendosi, è in grado di riconoscere se c'è un altro AP il cui segnale è migliore. In tale caso il MT ordina all'AP con cui è connesso di effettuare un'operazione di passaggio (handover) verso il nuovo AP. Tutte le connessioni in atto saranno quindi trasferite ed il MT rimarrà connesso con le rete HIPERLAN2 senza interruzioni nella comunicazione. È possibile che durante l'handover si verifichi qualche perdita di pacchetti. Se infine il MT giunge all'esterno dell'area di copertura della rete HIPERLAN2 e vi rimane per un certo tempo, perderà il contatto con la rete ed la connessione verrà interrotta.

Rispetto ad altri sistemi cellulari la mobilità in esterni di hiperlan2 è limitata, in virtù di questo, il contesto di utilizzo ideale per questa tipologia di rete è rappresentato da uffici, abitazioni, aeroporti e stazioni. Tuttavia il supporto per la mobilita è garantito anche nel passaggio tra reti di tipo diverso (ad esempio quando il MT si muove da un LAN a WAN o da una rete aziendale privata ad una rete pubblica). Per offrire una copertura continua i punti di accesso devono avere aree di copertura che si sovrappongano e tali aree hanno un raggio di circa 30 m in ambienti chiusi e di 150 m in ambienti all'aperto privi di ostacoli. Lo standard supporta la mobilita dei MT fino a velocità di 10 m/s.

3.1.5 Indipendenza da reti ed applicazioni esistenti

Hiperlan2 possiede un'architettura flessibile che le permette una semplice integrazione con un gran numero di reti fisse già esistenti. Ad esempio una rete Hiperlan2 può esser impiegata come ultimo tratto wireless di una rete Ethernet, oppure come porta di accesso a reti cellulari di terza generazione. Tutte le applicazioni che oggi vengono impiegate su infrastrutture fisse potranno continuare ad essere usate su una rete Hiperlan2.

3.1.6 Risparmio Energetico

Hiperlan2 implementa un meccanismo per il controllo della potenza di trasmissione (*transmit Power Control*-TPC) sia da parte del MT (in uplink e direct-link) che da parte dell'AP (in downlink).Tutto ciò al fine di raggiungere due obbiettivi:

- Semplificare il progetti del ricevitore nell'AP, non necessitando più di un sistema per il controllo automatico del guadagno (AGC-*Automatic Gain Control*).
- Ridurre le interferenze, ad esempio, con sistemi satellitari.

Il livello di potenza di trasmissione viene adatto in base alle capacita di decodifica del ricevitore più lontano; nei casi in cui sia richiesta una maggiore potenza pur essendo già stato raggiunto il limite massimo o, viceversa, sia richiesta una minore potenza pur essendo già stato raggiunto il limite minimo, il trasmettitore può inoltre una richiesta di passaggio ad un modo PHY più appropriati.

Lo standard prevede un meccanismo per il risparmio energetico basato sulla gestione dei periodi di inattività dei MT (*sleep*). Il MT può, in ogni istante, richiede all'AP di entrare in uno dei sedici stati di basso consumo (specifico per ogni MT) e richiede uno specifico periodo di sleep. Alla fine di tale periodo concordato il MT si mette in ricerca di un segnale di risveglio (wake-up) da parte di un AP sul canale broadcast, in mancanza di questo toma in stato di basso consumo per il successivo periodo e così via (al contrario, quando il MT è in uno stato attivo, controlla il canale

broadcast in ogni frame). Il MT cambierà il suo stato da sleep ad attivo quando identificherà sul canale di controllo del frame un MAC-ID corrispondente al proprio. Ogni AP rimanderà la trasmissione di dati ad un certo MT finché il corrispondente periodo di sleep non sarà giunto al termine. Anche nella trasmissione di tipo DL (da MT a MT) è compito dell'AP svegliare un MT quando si accorge che un altro MT ha dei dati da trasmettergli . Vengono supportati periodi di slepp di diversa durata per permettere di soddisfare i requisiti di breve latenza o di basso consumo (tipicamente si richiede breve latenza per trasmissioni *time critical* come voce e video)

Lo standard definisce inoltre un secondo tipo di approccio per il controllo della potenza di trasmissione ad anello aperto sull'RCH (*Open loop Tansmit Power Control*, **TPC**):

- Ogni AP informa i MT circa la propria potenza di trasmissione ed indica a quale livello di potenza si aspetta di ricevere (questo vale per tutti i MT). Questo meccanismo viene usato quando i terminali si contendono l'accesso all'AP secondo lo schema Slotted Aloha su un canale ad accesso casuale, per garantire un basso ritardo di accesso, L'AP alloca un maggior numero di slot per questo canale nel MAC frame riducendo cosi la probabilità di collisioni.

Lo standard definisce i seguenti limiti di potenza di trasmissione:

- 200 mW EIRP media (Equivalent Isotropic Radiated Power) nella banda 5.15-5.35 MHz, con uso esclusivamente in interni ed implementazione di DFS e TPC.
- 1W EIRP media nella banda 5.47-5.725 MHz, con uso in interni ed in esterni ed implementazione di DFS e TPC.

3.1.7 Struttura e livelli di HIPERLAN2

Lo standard Hiperland2 definisce un livello fisico (*Physical Layer*, **PHY**), un livello di controllo del collegamento dati (*Data link Control Layer,* **DLC**) e, al di sopra di questi, un set di livelli convergenza (*Convergence Layer*, **CL**), che accettano pacchetti o celle dai sistemi di networking già esistenti e li formattano per la trasmissione via radio.

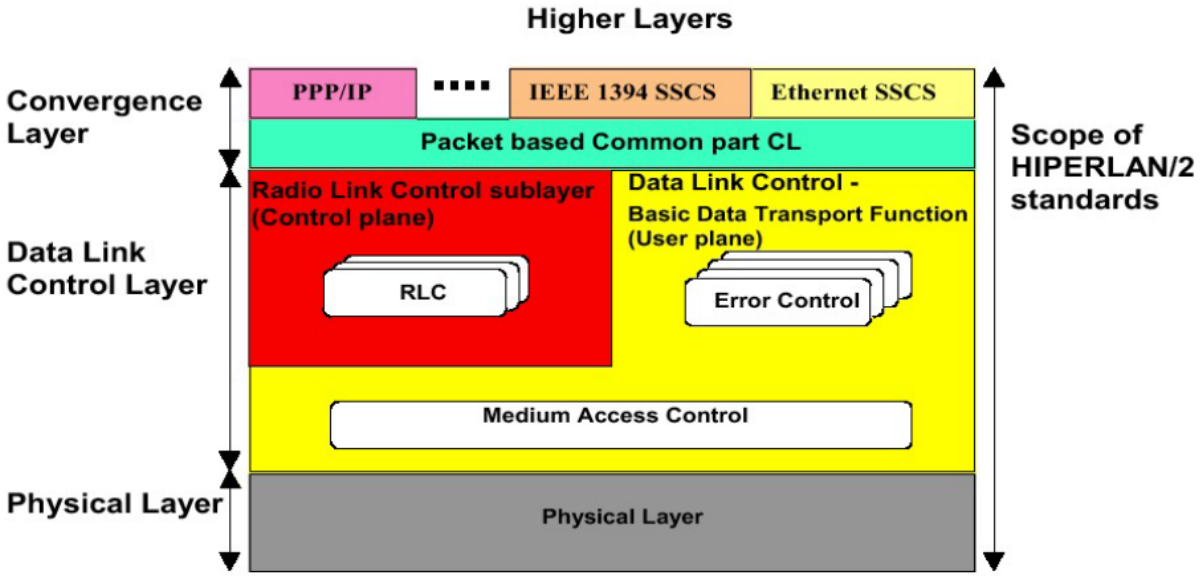


Figura 3.2: Struttura a livelli di Hiperlan2

Le relative principali funzioni sono descritte di seguito:

- Il *physical layer* mantiene le funzioni di trasporto dati con significato di modem dalla banda base alla parte RF. UN aspetto univoco dell' HIPERLAN2 è costituito dal multiplexing OFDM. Estremamente efficace in ambiente dispersivo nei confronti del tempo, come nei casi di canale multipath, combatte l'ISI dividendo il canale in varie subcarrier trasmettendo i dati in parallelo. Nella parte in banda base inoltre ci sono funzioni che riguardano la codifica dei dati (FEC) e il tipo di modulazione usata che variano in funzione del bit rate utilizzato.
- Il *Data Link Control* (**DLC**) consiste nelle funzioni di *Error Controll* (**EC**), di **MAC** ed di *Radio Link Control* (**RLC**). Risulta diviso nelle parti di trasporto dati e controllo, rispettivamente a destra e sinistra della figura 3.2. Inoltre, differenza delle altre WLAN, è Connection Oriented, ovvero prima che un MT inizi la trasmissione, comunica con il punto di accesso attraverso il "piano di segnalazione", time slot ad accesso casuale, ed imposta una

connessione temporanea. Ciò consente di negoziare i parametri di QoS, requisiti di ritardo, jitter e larghezza di banda , e di non interferire reciprocamente con altri terminali nelle trasmissioni successive.

- Il *Convergenze layer* risponde alle richieste di servizio da parte di layer più elevati e formatta i dati come richiesto dal sistema con cui si interfaccia che può essere anche di tipoEthernet, Firewire, ATM o UMTS (*Universal Mobile Telecomunication Sistem*). Provvede inoltre al trasporto dati per il DLC *Connectin Controll* (**DCC**), il *Radio Resurce Control* (**RRC**) e l' *Association Control Function* (**ACF**) relative al DLC.

3.2 Convergence Layer (CL)[4]

Il livello di convergenza assolve due funzioni principali adatta le richieste di servizio dai layer superiori al servizio offerto dal livello DLC e converte i pacchetti provenienti dai livelli superiori (di lunghezza fissa o variabile) in pacchetti a lunghezza fissa che possono essere gestiti dal livello DLC (*Sevice Data Unite*, **SDU**, di 384 byte cui aggiunge 12 byte di preambolo). In altre parole esso mette in contatto i vari tipi di dato in ingresso con le diverse sezioni del DLC. In realtà è più corretto parlare di un set di Convergence Layer, poiché ve ne possono essere svariati a seconda delle reti con cui verranno connessi. Si possono dividere in due tipi:

- CL basati sulle celle: che si occupano dei livelli superiori con pacchetti di lunghezza fissa (ad es. Le reti basate su ATM).
- CL basati sui datagrammi: che si occupano dei livelli superiori con pacchetti di lunghezza variabile (come Ethernet).

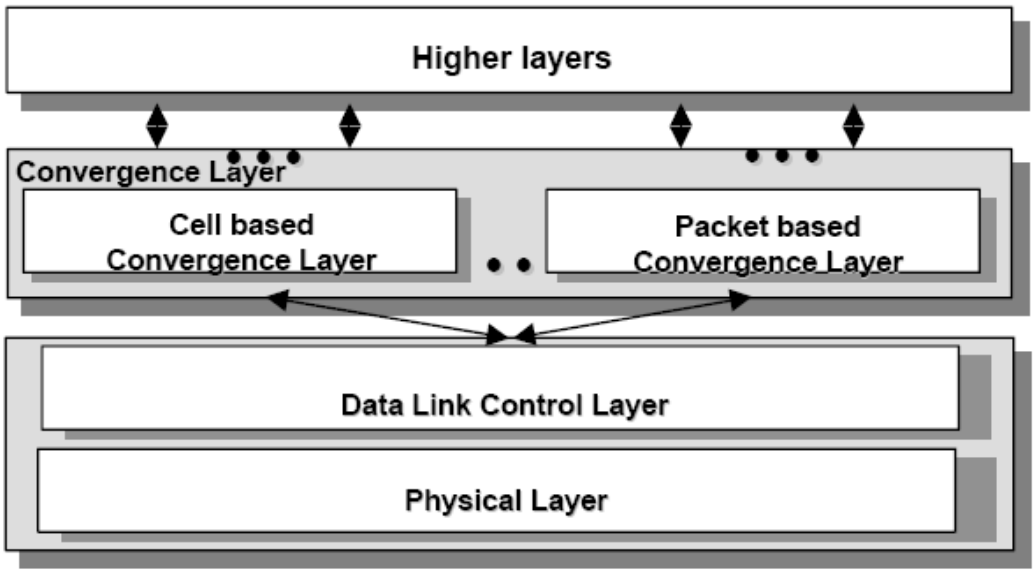


Figura 3.3: Struttura generale del Convergence Layer

Sono inoltre stati definiti dei sottolivelli di convergenza specifici per servizi dedicati (*Service Specific Convergence Sublayer*, **SSCS**) che contengono le funzioni SAR,come è descritta nella figura 3.4, per rendere possibile l'adattamento a Ethernet, IEEE 1394, PPP ed UMTS ed quelli ad essere aperti nel future. Per le celle ATM non ci sono funzioni SAR perché la lunghezza viene già aggiustata nel livello DLC.

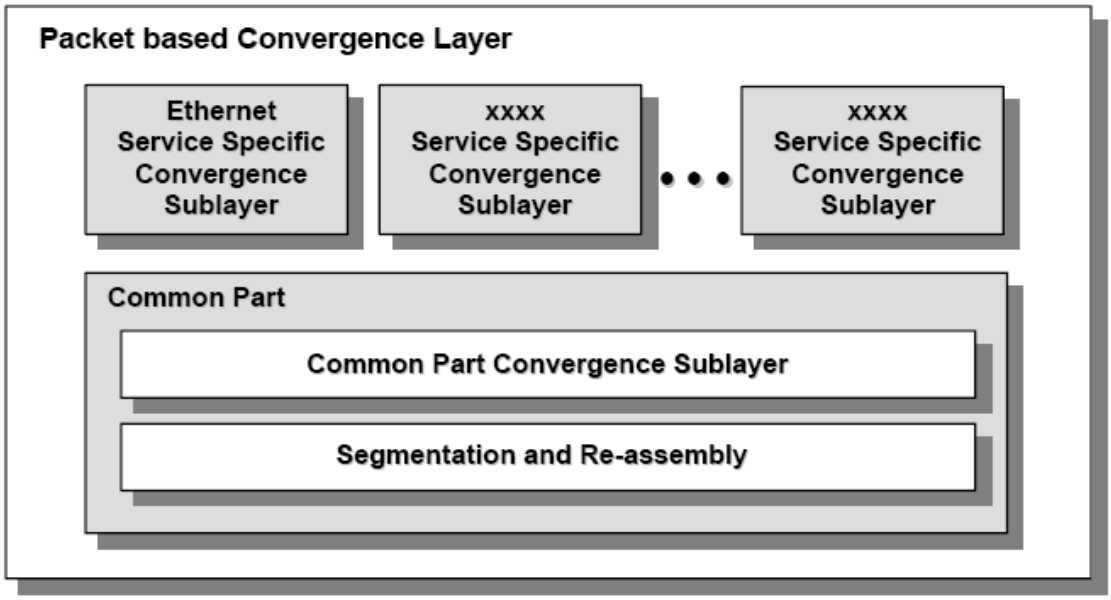


Figura 3.4: Struttura generale del Cl basati sui datagrammi

Common part

La funzione principale di Common Part per il Convergenec layer è segmentare pacchetti ricevuti dal SSCS, e radunare pacchetti segmentati ricevuti dallo strato di DLC prima che loro sono dati su il SSCS.

La funzione di riempimento, segmentazione e riassemblaggio degli SDU a lunghezza fissa per il DLC rende possibile standardizzare ed implementare i livelli DLC e PHY indipendentemente dalla rete cui Hiperlan2 si appoggia.

3.3 Data Link Control Layer (DCL) [5] [6]

Il livello DLC costituisce il collegamento logico tra gli AP ed i MT, assume diverse funzioni per l'accesso al messo trasmissivo, la trasmissione di dati e di segnale di controllo (gestione della connessione). L'AP effettua uno scheduling centralizzato per assegnare dinamicamente le risorse, supportare il QoS e fornire trasmissioni collision-free.

È costituito da un set di sottolivelli:

- MAC (*Medium Access Control*): protocollo per il controllo dell'accesso al mezzo trasmissivo
- EC (*Error Control*): protocollo di correzione dell'errore.
- RLC (*Radio Link Control*): protocollo per il controllo del collegamento radio, che comprende le funzioni di controllo del collegamento DLC (**DCC**, *DLC Connection Control*), delle risorse radio (**RRC**, *Radio Resource Control*) e dell associazioni (**ACF**, *Ascociation Control Function*).

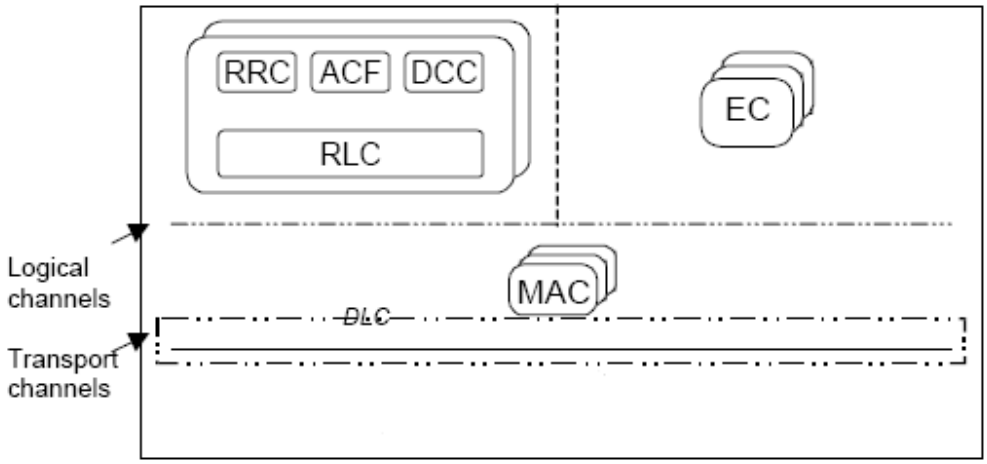


Figura 3.5: Struttura del DLC

Il livello DLC riceve dal livello CL pacchetti di 396 bit (12 bit flag + 384 bit payload); costruisce

una long PDU di 54 ottetti = 432 bit aggiungendo 36 bit (4.5 ottetti) così divisi:

- header: PDU type (2 bit) + sequence number (10 bit)
- footer: CRC-24 (24 bit)

Possiamo osservare la struttura nella figura 3.6:

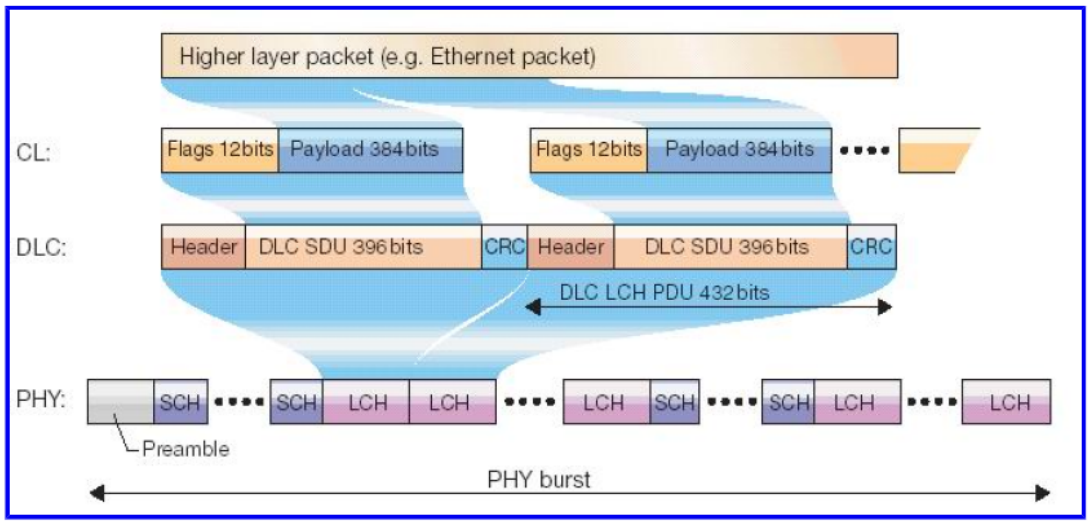


Figura 3.6: Schema generale di tutti i pacchetti per i tre livelli OSI trattati

3.3.1 Medium Access Control (MAC)

Il protocollo MAC viene usato per l'accesso al mezzo trasmissivo (il collegamento radio) e per la trasmissione di dati attraverso di esso. La gestione dei segnale di controllo è centralizzata ogni AP controlla tutte le trasmissioni in up-link, in down-link ed in direct-link; durante l'*associazione* il RLC (Radio link Control) assegna ad ogni terminale un identificatore unico (MAC ID, 8 bit). L'AP informa i MT circa l'istante all'interno del MAC frame in cui questi sono autorizzati a trasmettere i loro dati, in modo tale che possano organizzare opportunamente le richieste di accesso.

L'accesso al mezzo trasmissivo (l'aria) è infatti gestito secondo uno schema di tipo TDMA-TDD (T*ime Division Multiple Access-Time Division Duplex*):

- ogni utente, cioè ogni MT, è autorizzato a trasmettere i propri dati solo in determinati slot temporali all'interno del MAC frame .

Tale struttura permette la comunicazione simultanea sia in up-link che in down-link all'interno dello stesso frame. L'allocazione degli slot temporali per il link nelle due direzioni avviene in maniera dinamica, per meglio soddisfare le necessita delle varie trasmissioni. La struttura base del MAC frame ha una durata fissa di 2ms e comprende vari canali suddivisi in canali logici e canali di trasporto, ognuno dei quali

può essere utilizzato in uplink/downlink/direct-link a seconda della funzione che assolve. Il MAC può essere descritta nella figura 3.7.

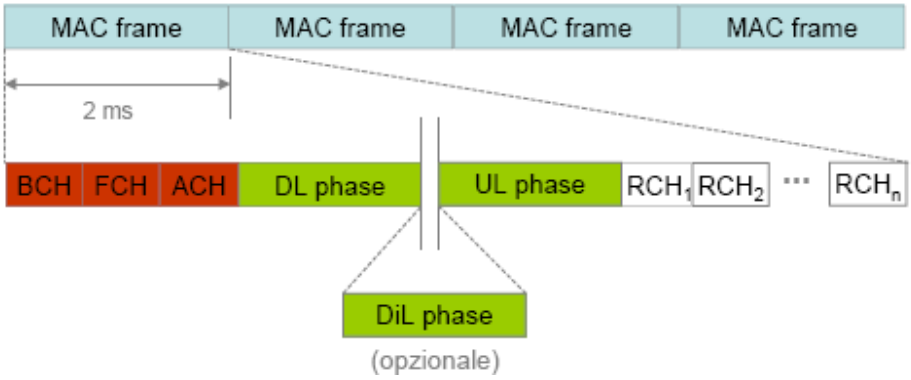


Figura 3.7: Struttura del base del MAC frame (il modo direct link è opzionale)

Canali logici

Si può considerare che i canale logici operino tra terminali di connessione di connessione logica, perciò tra entità logiche. Hiperlan2 definisce un insieme di canali logici per la segnalazione, il controllo ed il trasferimento della informazione. Sono identificati da sigle di quattro lettere.

Semantica dell'informazione trasportata:

- canali di controllo: BCCH, FCCH, RBCH, DCCH, LCCH, ASCH
- canali di accesso: RFCH
- canali di utente: UBCH, UMCH, UDCH

Canale di Controllo Broadcast* (BCCH**, *Broadcast Control CHannel*), solo DL.

Racchiude informazioni di controllo broadcast che riguardano l'intera cella radio, la quantità di tali informazioni è fissa. Tali informazioni vengono trasmesse solo quando l'AP lo ritiene necessario e pssono includere:

- Messaggi RLC broadcast
- Assegnazione di un MAC-ID ad un MT non ancora associato
- Conferma di handover

- Informazioni broadcast dei livelli superiori(livelli di convergenza)
- Chiavi per la codifica.

Tutti i terminali hanno accesso al BCCH e devono perciò essere in grado di interpretarlo, il BCCH deve esser inviato per ogni MAC frame per ogni antenna.

Canale di Controllo del Frame* (FCCH**, *Frame Control CHannel*), solo DL.

Contiene informazioni sulla struttura del MAC frame del punto de vista dell'interfaccia trasmissiva, viene annunciato da messaggi di connessione di risorse (*Resource Grants-RGs*), che indicano il tipo di dati contenuti nel rame e se ci sono delle parti di informazioni. La sua lunghezza è variabile i terminali devono essere in grado di interpretarlo.

Canale di Feedback ad Accesso Casuale* (RFCH**, *Random access Feedback CHannel*), solo DL

Il suo scopo è di informare i terminali che hanno usato l'RCH nel precedente MAC frame circa l'esito dei loro tentativi di accesso. Viene trasmesso una volta per ogni MAC frame per ogni antenna e tutti i terminali devono saperlo interpretare.

Canale Broadcast RLC* (RBCH**, *RLC Broadcast CHannel*), solo DL.in CM e DiL in DM.

Contiene informazioni di controllo broadcast sull'intera cella radio, viene inviato solo quando l'AP (in CM, modo centralizzato) o un MT (in DM, modo diretto) lo ritiene opportuno, ma non più di una volta per frame e per antenna. Può contenere:

- Informazioni su messaggi broadcast RLC
- Trasmissione del MAC ID assegnato ad un terminale non ancora associato
- Informazioni sull'ID del livello di convergenza
- Informazioni sul criptaggio .

Canale di Controllo Dedicato (**DCCH**, D*edicated Control CHannel*),UL, DL e DiL.

Trasporta segnali del sottolivello RLC tra MT ed AP. Tramite tale canale il RLC porta messaggi definiti per il controllo della connessione DLC e funzioni di controllo per l'associazione. Il DCCH costituisce una connessione logica che viene stabilita implicitamente durante l'associazione di un terminale senza alcuna segnalazione esplicita usando parametri predefiniti, viene realizzato come una connessione DLC. Ogni terminale associato ha un DCCH per ogni MAC ID, perciò una volta assegnato il MAC ID al MT, questo userà tale canale per la segnalazioni di controllo. Viene trasmesso nelle sequenze di PDU insieme a UDCH e LCCH.

Canale Broadcast per l'Utente (**UBCH**, *User Broadcast CHannel*), solo DL e DiL.

Viene usato per trasmettere dati dal livello convergenza, se l'AP supporta livelli convergenza multipli possono esistere più UBCH. Viene trasmesso nella sequenza di PDU con o senza canali LCCH.

Canale Multicast per l'Utente (**UMCH**, *User Multicast CHannel*), solo DL e DiL.

Trasporta dati per la comunicazione multi cast, viene trasmesso nella seuqnza di PDU.

Canale Dati per l'Utente (**UDCH**, *User Data CHannel*), UL, DL e DiL.

Si occupa dello scambio di dati (**DLC-PDU**, DLC Packet Data Units) tra AP e MT. Il DLC garantisce la consegna dei pacchetti nella sequenza corretta al livello convergenza. Una connessione DLC, per l'utente su questo canale viene stabilita attraverso segnalazione sul canale DCCH, i parametri caratteristici di tale connessione vengono negoziati durante la fase di associazione e durante la creazione della connessione stessa.

Nella trasmissione uplink il MT inoltra una richiesta di slot di trasmissione per la connessione UDCH, quindi un messaggio di assegnazione delle risorse (*Risource Grant*-RG) viene trasmesso in un successivo FCH. Nella fase downlink, invece, l'AP può allocare risorse per l'UDCH senza che alcun terminale ne faccia richiesta. Per garantire una trasmissione affidabili sull'UDCH viene automaticamente applicato un sistema ARQ, tuttavia una trasmissione ci possono essere connessioni, come quelle per il traffico multicast, che non ne fanno uso.

Canali di controllo del collegamento* (LCCH**, *Link Control CHannel),* UL, DL e DiL.

Porta informazioni (tipicamente messaggi ARQ e di rifiuto) tra le funzioni di controllo degli errori tra l'AP e il MT (o tra due MT in DM) per un determinato UDCH. L'AP determina gli slot di trasmissioni necessari per il LCCH nell'uplink, quindi comunica l'assegnazione delle risorse in un FCH. Viene trasmesso nelle sequenze di PDU con o senza UDCH e UBCH.

Canali di controllo dell'associazione* (ASCH**, *ASsociation Control CHannel),* solo UL.

Trasporta nuove richieste di associazione e messaggi di richiesta di riassociazione, perciò tali messaggi possono essere trasmessi dolo durante l'handover e da parte di MT non associati.

Canali di trasporto

I canali logici vengono mappati su diversi canali di trasporto q questi ultimi costituiscono gli elementi base delle sequenze di PDU. Vengono identificati di sigle di tre lettere. Occupano posizioni ben definite all'interno della frame MAC.

Formato dell'informazione trasportata:

• BCH, FCH, ACH, LCH, SCH, RCH

*_Canale Broadcast_ (**BCH**, _Broadcast Channel_), solo DL

Contiene informazioni di controllo che vengono inviate in ogni MAC frame e raggiungono ogni MT, fornisce:

- Informazioni (non esaustive) sul livello di potenza
- Sulla localizzazione e la lunghezza del FCH e del RCH
- Indicatori di risveglio ed indicatori per l'identificazione sia della rete Hiperlan2 sia dell'AP
- Trasporta tutti i BCCH e deve essere trasmesso in ogni in ogni MAC frame e in ogni antenna.

*_Canale di Controllo del Frame_ (**FCH**, _Frame Channel_), solo DL

Contiene un'esatta descrizione di come le risorse sono state distribuite all'interno del MAC frame, nei canali DL, UL e RCH. Trasporta tutti gli FCCH.

*_Canale di Controllo dell'accesso_ (**ACH**, _Access feedback Channel_), solo DL

Racchiude le informazioni sui precedenti tentativi di accesso al RCH. Viene usato per trasportare gli RFCH in dall'AP agli MT.

Canale per la trasmissione di dati in uplink e downlink (UL e DL phase)

Consistono di sequenze di PDU comprendenti PDU per l'utente (**U-PDU** di 54 byte con 48 byte di informativi) e PDU di controllo (**C-PDU** di 9 byte). C'è una sequenza di PDU per ogni MT, se le risorse gli sono state concesse nel FCH. È convenzione comune riferirsi ai C-PDU come al "canale di trasporto breve" (**SCH**, _Short transport CHannel_) ed ai U-PDU come al "canale di trasporto lungo" (**LCH**, _Long transport Channel_).

*_Canale a "Lungo Trasporto"_ (**LCH**, _Long transport Channel_), UL, DL e DiL.

Trasporta dati per l'utente relativi ai canali UDCH, UBCH e UMCH e messaggi di controllo relative ai canali DCCH e RBCH.

Canale a "Breve Trasporto" (**SCH**, *Short transport CHannel*), UL, DL e DiL.
Trasporta informaizioni di controllo per i canali DCCH, LCCH e RBCH.

Canale per l'accesso casuale (**RCH**, *Random access CHannel*),solo UL.

Viene usato dai MT per richiedere risorse per la trasmissione uplink e nei MAC. Quando aumenta la frequenza di accesso per la richiesta di risorse da parte dei MT, l'AP allocherà maggiori risorse nel RCH. Questo canale è interamente costituto di slot di contessa ai quali tutti gli MT associati a quel particolare AP partecipano, la contesa del canale viene gestita secondo un protocollo Slotted Aloha. Possono perciò verificarsi delle collisioni e le conseguenze degli accessi al RCH verranno riferiti all'AP tramite l'ACH.

La seguente figura riassume i canali logici e trasporto:

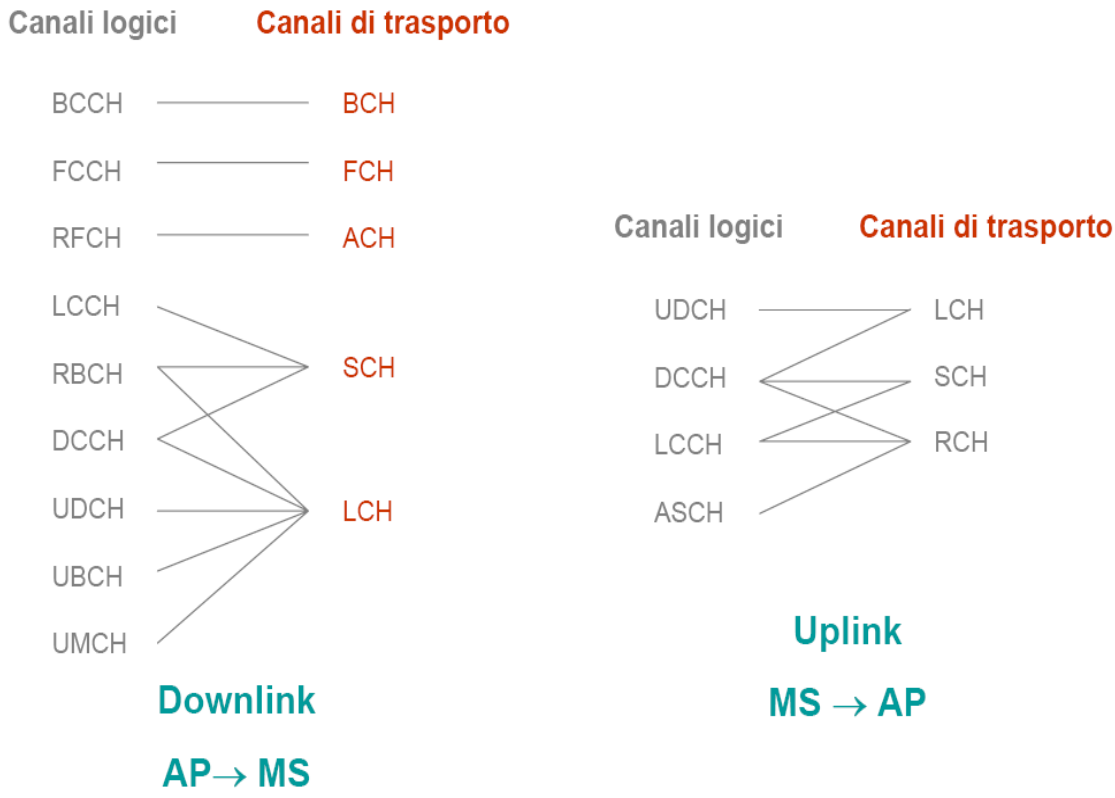


Figura 3.8: Canale logici e trasporto

Nel momento in cui viene stabilita una connessione L'MT riceve un identificatore unico da parte dell'AP (**DLCC-ID**, *DLC Connection IDentifier*) di 6 bit, per ogni connessione DLC stabilita, quando il MT dei dati d trasmettere invia una richiesta di risorse (**RR**, *Resource Request*) all'AP. La RR contiene il numero di U-PDU che il MT ha in attesa per quella particolare connessione DLC e può essere inviato tramite il RCH oppure il SCH. L'AP è in grado di controllare in maniera opportuna il ritardo di accesso semplicemente variando il numero di slot di contesa. Inoltre alcuni slot di contesa sono riservati per il traffico ad alta priorità, cioè messaggi RR, mentre gli slot a bassa priorità vengono principalmente per inizializzare le operazione di handover. Dopo aver inviato la RR, il MT si pone in uno stato libero da contessa, intanto l'AP schedula e connessione per la trasmissione distribuendo in maniera opportuna l'assegnazione delle risorse (***RG,*** *Resource Grand*). Periodicamente l'AP interroga nuovamente il MT per conoscere il numero di U-PDU.

Una connessione DLC può essere usata in maniera unicast, multicast o broadcast ed è definita in maniera univoca dalla combinazione degli identificatori MAC che partecipano e dell'identificatore della connessione DLC, tale combinazione viene chiamata connessione DLC per l'utente (**DUC**, *DLC User Connection*).

- Per la trasmissione unicast ad ogni MT viene assegnato un identificatore MAC (in senso locale, per ogni AP) ed uno o più identificatore di connessione DLC a seconda del numero DUC
- Per la trasmissione multicast Hiperlan2 definisce due modi operativi:

  *N*unicast*

  È considerato esattamente come una trasmissione unicast, con in più, un protocollo ARQ.

  MAC multi cast

  Nel MAC multi cast, invece, viene assegnato un MAC-ID (in senso locale, per ogni AP) per ogni gruppo multicast e non si può usare l'ARQ:

  Ogni U-PDU viene trasmesso una sola volta, tutto il traffico multicast verso quel gruppo viene indirizzato verso la stessa specifica connessione DLC. Hiperlan2 permette l'assegnazione di identificatori

MAC separati per indirizzare fino a 32 gruppi multicast, ma nel caso in cui MT vogliano costituire più di 32 gruppi mutlicast, uno degli identificatori MAC assolverà la funzione di "identificatore MSC di traboccamento", cioè due o più gruppi multicast possono venire indirizzati da questo stesso identificatore.

- È prevista anche la trasmissione broadcast e come nel caso multicast non è previsto alcun ARQ, tuttavia poiché la trasmissione broadcast è molto più critica per la prestazione complessive del sistema, Hiperlan2 definisce uno schema per la ripetizione degli U-PDU broadcast. Ciò significa che lo stesso U-PDU viene ritrasmesso un certo numero di volte (configurabile) nello stesso MAC frame per aumentare la probabilità di riuscita della trasmissione. Da notare che la ricezione di messaggi broadcast non influisce sullo stato di sleep dei MT.

Il livello DLC ha lo scopo principale di schedulare in maniera efficiente il MAC frame. Il MAC frame ed i vari canali di trasporto costituiscono l'interfaccia tra il DLC ad il livello fisico.

3.3.2 Controllo dell'Errore (EC)

Vengono definiti tre modi di correzione dell'errore per supportare diversi tipi di servizi:

1. Il modo "*acknowledged*" (conferma) usa la ritrasmissione per migliorare la qualità del collegamento e viene usato per garantire trasmissioni affidabili, è basato su un meccanismo di controllo a ripetizione selettiva (**SR-ARQ**, *Automatic Repeat Query*) e può soddisfare requisiti di bassa latenza attraverso un meccanismo dei pacchetti.
2. Il modo "*repetition*" (ripetizione) si bassa sulla ripetizione dell'intero DLC-PDU per garantire l'affidabilità della trasmissione. Non è disponibile alcun canale di risposta, ma il trasmettitore può arbitrariamente ritrasmettere i PDU per migliorare la ricezione, il ricevitore accetterà comunque solo i PDU il cui

numero di sequenza rientra in certi criteri di accettabilità. Questo viene usato essenzialmente per la trasmissione broadcast.

3. Il modo "*unacknowledged*" (senza conferma) garantire una trasmissione inaffidabile ma a bassa latenza e senza alcuna ritrasmissione, perciò non vi è alcun canale di risposta.

Il traffico unicast viene trasmesso in modo "*acknowledged*" o "*unacknowledged*", il traffico broadcast in modo "repetittion" o "*unacknowledged*", i servizi multicast possono essere trasmessi in modo "*unacknowledged*" oppure possono essere ripartiti in connessioni unicast esistenti.

Il sottolivello EC serve anche a garantire che gli U-PDU vengano consegnati nella corretta sequenza al livello di convergenza, per fare ciò viene assegnato un numero di sequenza ad ogni U-PDU per ogni connessione. I messaggi di ACK/NACK vengono trasmessi nel LCCH ad ogni pacchetto U-PDU può essere ritrasmesso un certo numero di volte (configurabili). Per supportare in maniera efficiente la QoS in applicazioni real-time in cui il ritardo è un fattore critico (come la voce) viene definito un meccanismo di scarto degli U-PDU che risultano obsoleti (il cui ritardo supera un certo valore), quando ciò avviene il protocollo EC inizia a scartare l'U-PDU in questione e tutti gli U-PDU con numero di sequenze inferiore per i quali non è stato ricevuto l'ACK. Ne risulta che nella trasmissione nel DLC è possibile che si verifichino dei "buchi", cioè delle perdite di dati, mentre la connessione DLC è ancora attiva. Se necessario, è compito dei livelli superiori andare a compensare tali perdite.

La tecnica di rivelazione e correzione degli errori è di tipo FEC (*Foward Error Crrection*) basato su un codice Reed Solomon concatenato con un codice convoluzionale di Viterbi , che permette di raggiungere valori di BER (Bit Error Rate) molto bassi ($\approx 10^{-15}$).

3.3.3 Radio Link Control (RLC)

Il sottolivello RLC fornisce un servizio di trasporti per le funzioni di segnalazione che constituiscono lo schema per lo scambio di segnali di controllo tra AP e MT nel DLC:

- funzione di controllo dell'associazione (**ACF**, *Association Control Function*), funzione di controllo della connessione DLC (**DCC**, *DLC User Connection Control*) e funzione di controllo della risorsa radio (**RRC**, *Radio Resource Control*).

Controllo dell'associazione (ACF)

**Associazione*

Il MT si pone in ascolto sul BCH sei vari AP e seleziona quello con il collegamento radio di migliore qualità (parte dell'informazione portata nel BCH, in questo stadio, ha la funzione di segnale pilota), quindi continua ad ascoltare il broadcast di un identificatore di operatore di rete unico o globale nel BCCH al fine di evitare un'associazione con una rete che non è in grado o non è abilitata a fornire servizi all'utente del terminale. Se il MT decide di continuare l'associazione richiederà e riceverà un MAC-ID dall'AP.

A questo segue uno scambio di informazione sulle capacità di collegamento tramite l'ASCH. L'MT inizia a fornire informazioni (non esaustive) su:

- I modi PHY
- I livelli di convergenza
- Gli algoritmi
- Le procedure di autenticazione e codifica supportati.

L'AP risponderà selezionando un sottoinsieme dei modi PHY che anche'esso supporta, un livello convergenza (solamente uno) ed una procedura di codifica ed autenticazione (in alternativa non verrà usata alcuna codifica e/o autenticazione). Se è stata negoziata con successo una codifica, l'Mt inizia lo scambio della chiave Diffie-Hellman per negoziare la chiave della sessione segreta che verrà usata per

tutto il traffico unicast tra il MT e l'AP, in questo modo anche la successiva autenticazione viene protetta da codifica.

Hiperlan2 supporta entrambi gli algoritmi di codifica DES e 3DES. Anche il traffico broadcast e multicast può essere protetto da codifica tramite l'uso di chiavi comuni (tutti gli MT associati allo stesso AP usano la stessa chiave) che vengono distribuiti agli MT protette dalla chiave di codifica a unicast. Tutte le chiavi di codifica devono essere periodicamente cambiate per evitare problemi di sicurezza.

Esistono due alternative per l'autenticazione:

1. una prevede l'uso di una chiave già condivisa
2. l'atra l'uso si una chiave pubblica.

In questo secondo caso Hiperlan2 supporta una infrastruttura di chiave pubblica (PKI, Public Key Infrastucture) per mezzo della generazione di una firma digitale. Gli algoritmi di autenticazione supportati sono: MD5, HMAC e RSA. È prevista anche l'autenticazione bidirezionale per permettere sia agli MT che agli AP di autenticarsi. Hiperlan2 supporta inoltre una gran numero di identificatori per riconoscere l'utente e/o il MT.

Dopo l'associazione il MT può richiede un canale di controllo dedicato (ciò il DCCH) per inizializzare i proranti (cioè le connessione DLC per l'utente), infatti ogni MT può richiede varie connessione DLC per l'utente, poiché di esse ha un supporto unico per la QoS.

**Diassociazzione*

Un MT può diassociare implicitamente o esplicitamente:

- il primo caso si verifica quando il MT rimane irraggiungibile per un certo periodo di tempo
- nel secondo caso è il MT che avverte l'AP che non intende più comunicare con la rete Hiperlan2.

Controllo della Connessione DLC per l'utente (DCC)

Il MT (cosi come l'AP) fa richiesta di connessione DLC per l'utente trasmettendo messaggi di segnalazione attraverso il DCCH, il quale controlla le risorse per uno specifico livello MAC (identificato del MAC-ID). Non è possibile trasmettere alcun dato a livello di utente finché non c'è almeno una connessione DLC per l'utente attiva tra l'AP e il MT. Tale segnalazione avviene in maniera semplice con una richiesta, contenente le caratteristiche della connessione, seguita da un segnale di ACK.

Stabilita la connessione, l'AP gli assegna un identificatore unico (di connessione DLC). La connessione può quindi essere rilasciata con una procedura del tutto analoga, Hiperlan2 supporta anche la modifica della caratteristiche di una connessione già stabilita.

Controllo della Risorsa Radio (RRC)

**Handover*

Il procedimento di handover inizia con la misurazione della qualità del collegamento radio, la quale può portare ad una richiesta di handover da parte del MT. Hiperlna2 supporta due tipi di handover:

- riassociazione
- handover tramite segnalazione attraverso le rete fissa

La riassociazione consiste nel ristabilire nuovamente un'associazione, cosa che può richiedere del tempo, specialmente in relazione al traffico o in corso, mentre l'atra possibilità prevede che il nuovo AP verso il quale il MT ha richiesto l'handover recuperi le informazione sulla connessione e sull'associazione direttamente dal vecchio AP attraverso la rete fissa. Il MT fornisce al nuovo AP un indirizzo di rete fissa (come un indirizzo IP) per rendere possibili a comunicazione tra il vecchio ed il nuovo AP. Questa soluzione permette un handover veloce minimizzando le perdite di traffico al livello di utente durante la fase di handover.

**Selezione dinamica della frequenza (DFS)*

Il RRC supporta tale funzione permettendo all'AP di istruire il MT associato effettuati della misurazioni sui segnali radio ricevuti dagli AP vicini. A causa di cambiamenti ambientali e della topologia della rete, il RRC include inoltre la segnalazione per informare gli MT associati che l'AP cambierà frequenza.

**MT alive*

L'AP controlla anche gli MT inattivi che non trasmettono traffico in uplink inviando loro un messaggio di 'alive' al quale essi devono rispondere, in alternativa l'AP può stabilire un tempo massimo per il quale un MT può rimanere inattivo. Se non riceve ai messaggi di alive o se il tempo massimo viene superato il Mt viene disassociato.

**Risparmio energetico*

Questa funzione è responsabile per l'entrata o l'uscita dallo stato di basso consumo e per controllare la potenza del trasmettitore. Viene inizializzata dal MT che dopo una negoziazione durante un periodo di sleep (N frame, dove N=2,…216), si pone in stato di sleep. Dopo N frame ci sono quattro scenari possibili:

- AP sveglia MT (l'AP può avere dati in attesa).
- MT si sveglia (MT può avere dei dati in attesa).
- AP comunica a MT di proseguire lo stato di sleep (per N frame ancora).
- MT perde i messaggi di makeup dell'AP ed esegue la sequenza di MT alive.

3.4 Livello fisico (PHY) [7]

Al livello fisico il formato dei dati trasmessi consiste in una coda costituta da un preambolo ed una parte di dati (payload) che può essere generata da ognuno dei canali di trasporto del DLC.

Il preambolo può essere di tre tipi:

- per il canale di controllo broadcast (consente la sincronizzazione di frame, il controllo automatico di guadagno, la sincronizzazione di frequenza e le stima del canale)
- per gli altri canali in down link (solamente per la stima del canale)
- per il canale in uplink e ad accesso casuale (per la stima del canale e della frequenza)

Le prestazione durante la sincronizzazione iniziale (cioè quando MT si sincronizzano sul BCH), sono caratterizzate in termini di probabilità dei errore e probabilità di falso allarme, simulazioni mostrano che anche in condizioni sfavorevoli (rapporto segnale/rumore di 5 dB su un canale ad alta dispersione con 259 ms di ritardo possibile e offset dei frequenza di 40 ppm) le probabilità di successo nella sincronizzazione sono dell'ordine del 96%. Perciò Hiperlan2 fornisce un mezzo per la sincronizzazione veloce, robusto ed efficiente.

È stata scelta modulazione OFDM (O*rthogonal Frequency Division Multiplexing*) per le alte prestazioni che consente di raggiungere in termini di data rate anche in ambienti molto dispersivi e per le limitate richieste hardware necessarie alla sua implementazione. Tale schema di modulazione consente inoltre un uso efficiente della banda disponibile, in quanto le sottoportanti si trovano quanto più vicine possibile:

I dati vengono separati in diversi flussi di dati indipendenti ognuno dei quelli va modulare una diversa sottoportante, ognuno di questi sottocanali viene usato per un collegamento di trasmissione tra un AP e gli MT.

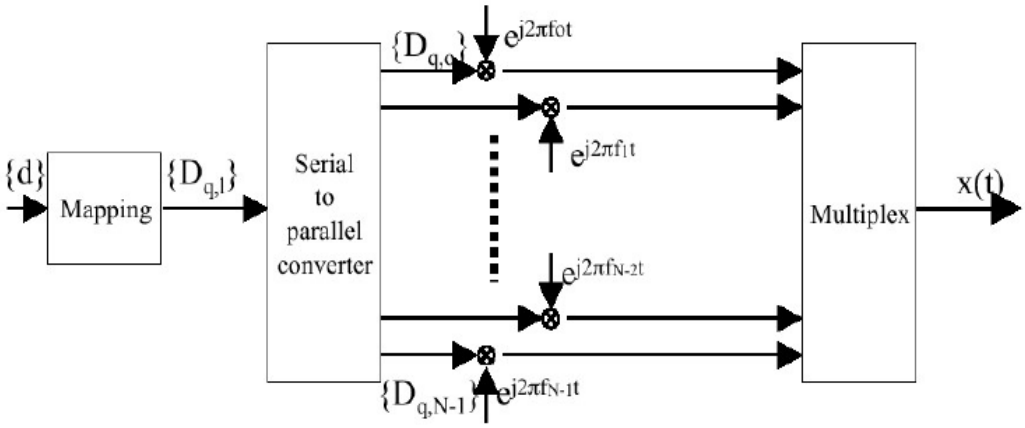


Figura 3.9: Schema del modulatore OFDM

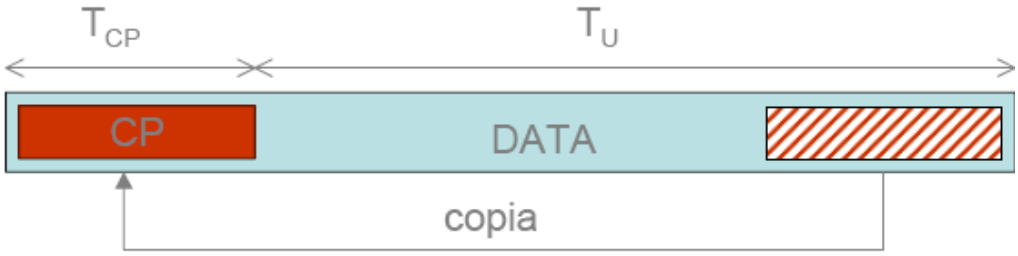


Figura 3.10: Simbolo OFDM

Per minimizzare problemi di interferenza e intersimbolica (**ISI**, *Inter Symbol Interference*) ed interferenza intercanale (**ICI**, *Inter Channel Interference*) ogni simbolo OFDM viene fatti precedere dal cossi detto "prefisso ciclico", che altro non è se non la ripetizione lineare nel canale viene vista come circolare del ricevitore. Tale prefisso viene inserito in trasmissione e rimosso in ricezione, e serve a garantire la perfetta ortogonalità dei sottocanali.

L'OFDM permette inoltre una grande flessibilità nella scelta e nella realizzazione di diverse alternative di modulazione. Infatti una caratteristica molto importante del livello fisico di Hiperlan2 è che esso è in grado di funzionare in diversi modi, ottenuti applicando diversi schemi di "*puncturing*" ad un codici convoluzionale e combinandoli con diversi schemi di modulazione che vengono gestiti e selezionati dalla funzione di adattamento del collegamento (*link adaption*). Sono supportate le

codifiche BPSK, QPSK, 16QAM obbligatorie, e le codifica 64QAM opzionale. La correzione degli errori viene effettuata tramite l'uso di un codice convoluzionale con rapporto di codifica di ½ e lunghezza di concatenamento pari a 7, ma si possono raggiungere rapporti anche di 9/16, e ¾ per mezzo di puncturing. Vengono definiti sette modi di livello fisico: sei obbligatorio e uno, per il 64QAM, opzionale.

Modo	Modulazione	Rapporto di codifica	Bit rate (PHY)	Bit per simbolo OFDM
1	BPSK	1/2	6 Mbps	24
2	BPSK	3/4	9 Mbps	36
3	QPSK	1/2	12 Mbps	48
4	QPSK	3/4	18 Mbps	72
5	16QAM	9/16	27 Mbps	108
6	16QAM	3/4	36 Mbps	144
7	64QAM	3/4	54 Mbps	216

Tabella 3.1: Mapping codifica e bit-rate supportati

Il canale ha una larghezza di banda di 20 MHz, che consente di ottenere una alta velocità di bit per canale pur mantenendosi una ragionevole numero di canali nello spettro di frequenza allocato (19 canali in Europa). Vengono usate 52 sottoportanti per canale, di cui 48 trasportano dati e 4 assolvono la funzione di pilota per la ricostruzione della fase per la demodulazione coerente. L'intervallo di tempo limite per il prefisso ciclico è fissato ad 800 ns, che consente delle buone prestazioni sul canale anche con ritardi fino 250 ns, è inoltre previsto un intervallo limite opzionale di 400 ns per ambienti interni particolarmente piccoli.

Lo standard definisce solo la parte trasmittente, quella ricevente non è specificata, ma deve rispettare gli stessi requisiti tecnici. Nella tabella 3.2 riassume i parametri del livello fisico.

Massimo RMS delay spread	220 ns
Massima velocità terminali	10 m/s (36 km/h)
Doppler spread/shift tipico	50 Hz @ 5 GHz (velocità 3m/s, circa 11 km/h)
Tempo di coerenza tipico	1/2fd = 10 ms @ 5 GHz (velocità 3 m/s)
Accuratezza oscillatori	20 ppm (offset di frequenza 100 kHz @ 5 GHz);

Tabella 3.2:Parametri del livello fisico in condizioni operative tipiche.

I blocchi funzionali previsti dallo standard per il trasmettitore sono illustrati nella figura 3.11

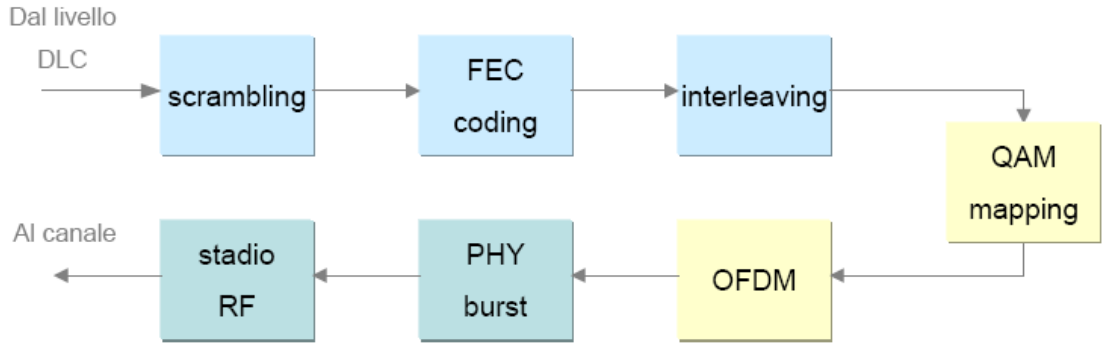


Figura 3.11: Il trasmettitore HIPERLAN/2

Il primo blocco effettua lo *scrambling* su ciascuna PDU train del DLC con una sequenza di lunghezza pari a 127 bits generata dal polinomio questo vale per i dati trasmessi e ricevuti. Tutte le PDU trains appartenenti a frame del MAC sono trasmesse con lo stesso stato iniziale. Il sistema opera nei vari casi come segue:

- Broadcast PDU train con unico settore usato dall'AP: lo scrambling è inizializzato al quinto bit del BCH, al primo bit del FCH e al primo del ACH.
- Broadcast PDU train con più settori usati dall'AP: lo scrambling è inizializzato al quinto bit del BCH; FCH e ACH PDU train sono trasmesse solo nel caso in cui l'AP usa più settori e lo scrambler è inizializzato al primo bit di ciascun campo;
- Nelle downlink PDU train con preambolo corto,

- In tutte le uplink e nelle directlink PDU train lo scrambling è inizializzato al primo bit del PDU train.

Lo stato iniziale, settato come *pseudo random* (PN) non-zero, è determinato dal campo counter del BCH, all'inizio del corrispondente frame del MAC, al quale si aggiunge la sequenza fissa (111) all'inizio come in figura 3.12.

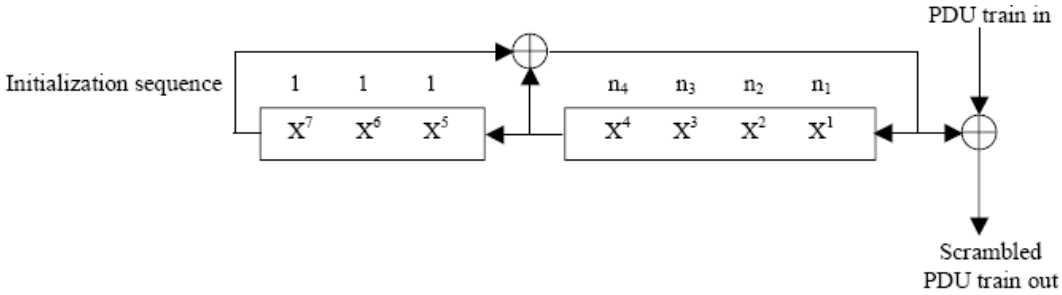


Figura 3.12: Diagramma schematico dello scrambler

Subito dopo è prevista obbligatoriamente la codifica *FEC* sulla sequenza. Questa si svolge in principalmente in quattro step: vengono inseriti sei bits in coda, si codifica con un convoluzionale, si effettua il puncturing P1 indipendente dal code rate ed infine il P2, che invece dipende dal code rate. Nella Figura 3.13 riassume lo Schema delle operazioni di puncturing.

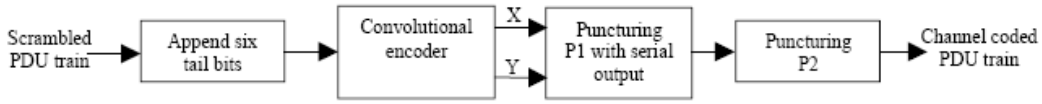


Figura 3.13: Schema delle operazioni di puncuring

Le prime tre operazioni dipendono dal tipo di PDU train come segue:

- Broadcast PDU train con antenna omni-direzionale: i bits di coda e il P1 vengono aggiunti individualmente su BCH, FCH e ACH. Il codificatore viene infine inizializzato con il primo bit di ciascuno di questi ultimi.
- Broadcast PDU train con antenna a settore: i bits di coda e il P1 vengono aggiunti solo sul BCH e il codificatore inizializzato con il suo primo bit.

- FCH e ACH PDU train: i bits di coda e il P1 vengono scelti e aggiunti separatamente per i due. Il codificatore viene inizializzato al primo bit del FCH, al primo dell' ACH prima senza e poi con priorità.
- Nelle downlink PDU train, in tutte le uplink con preambolo corto e nelle direct link PDU train

L'*interleaving* è effettuato su un blocco di dimensioni pari al numero di bit corrispondenti ad un simbolo OFDM, grazie a due operazioni di permutazione nella sequenza già codificata si garantisce prima che due bit consecutivi siano trasmessi su due sub-carrier adiacenti e poi che alternativamente siano mappati sul bit più e meno significativo della costellazione. Lo standard fornisce una rappresentazione matematica ma non una specifica implementazione.

Lo schema di modulazione è di tipo OFDM ed è prevista una funzione di *link adaption* per migliorare le capacità del collegamento radio alle differenti situazioni di interferenza e distanza tra AP ed MT. Il data rate può variare tra 6Mbps e 54Mbps modulando le sotto portanti con diversi alfabeti di segnale e con più livelli di puncturing del codice convoluzionale a rate 1/2. BPSK, QPSK, 16QAM sono formati di modulazione obbligatori, mentre il 64QAM è opzionale sia per AP che per i MT. Come è descritta dalla tabella 2.1.

Le sottoportanti sono numerate da –26 a 26 (quelle esterne non sono utilizzate per garantire la necessaria separazione tra i canali, quella corrispondente alla componente continua non è utilizzata), le sottoportanti pilota sono quelle di indice –21, -7, 7, 21. Il segnale trasmesso su queste è una sequenza PN generata dallo stesso registro a scorrimento utilizzato per lo scrambling.

Numero punti IFFT/FFT	64	
Frequenza di campionamento $f_s=1/T$	20 MHz	
Durata utile simbolo T_U	64*T (3.2 μs)	
Durata prefisso ciclico T_{CP}	16*T (0.8 μs) (obbligatorio)	8*T (0.4 μs) (opzionale)
Intervallo di simbolo T_S ($T_U + T_{CP}$)	80*T (4.0 μs) (obbligatorio)	72*T (3.6 μs) (opzionale)
Numero sottoportanti dati N_{SD}	48	
Numero sottoportanti pilota N_{SP}	4	
Numero totale sottoportanti $N_{ST} = N_{SD} + N_{SP}$	52	
Spaziatura sottoportanti $\Delta f = 1/T_U$	0.3125 MHz	
Spaziatura sottoportanti estreme ($N_{ST} * \Delta f$)	16.25 MHz	

Figura 3.14: Parametri OFDM

Il blocco prima del trasmettitore vero e proprio ha la funzione di formare il *PHY burst*. Lo standard ne definisce cinque tipi diversi di cui l'ultimo è opzionale:

1.broadcast burst;

2.downlink burst;

3.uplink burst with short preamble;

4.uplink burst with long preamble;

5.direct link burst;

Ogni burst è composto da un preambolo e dal payload; la lunghezza del preambolo varia da 8 μs a 16 μs in dipendenza del tipo di burst, e anche la sua struttura è differente in funzione del tipo di burst; la lunghezza del payload è variabile e dipende dalla dimensione del PDU train da trasmettere. La parte iniziale del preambolo (da 0 μs a 8 μs) serve per la sincronizzazione di frame, il controllo automatico di guadagno, la sincronizzazione di frequenza e la stima di canale; la fase finale (8 μs)contiene simboli di training ed è utilizzato esclusivamente per la stima di canale.

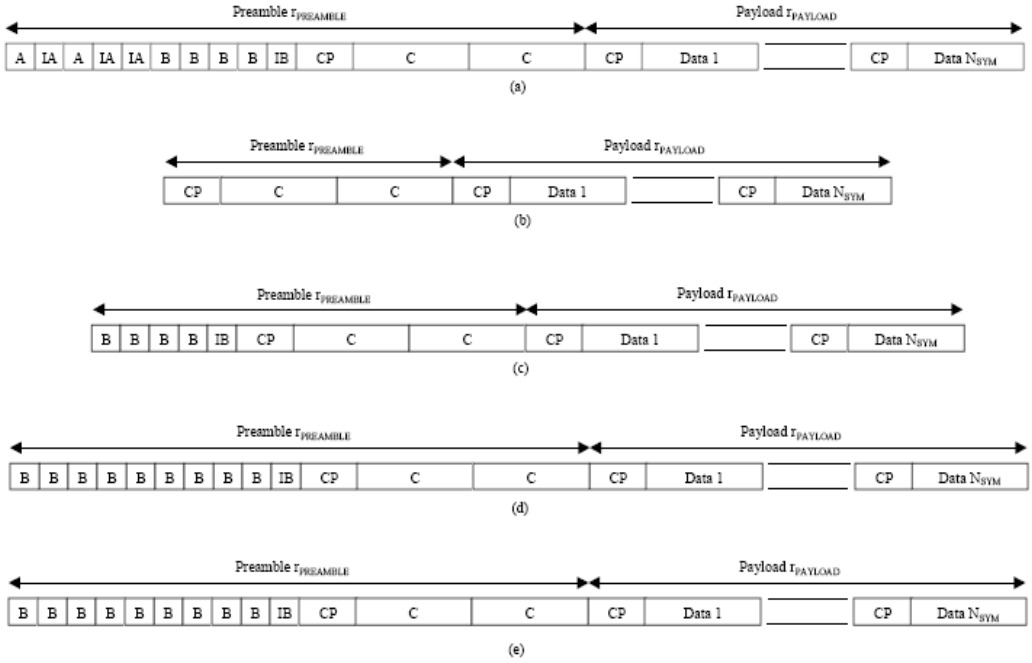


Figura 3.15:Strutture del PHY burst: a)broadcast; b)downlink; c)uplink con preambolo corto; d)uplink con preambolo lungo; e)direct link.

Lo standard prescrive che l'accuratezza dell'oscillatore impiegato sia nell'AP che nell'MT sia di ±20 ppm rispetto alla frequenza nominale, che corrisponde ad un offset di frequenza di ± 100 kHz @5 GHz. Inoltre un solo oscillatore della precisione richiesta deve essere utilizzato sia per la generazione della portante RF, sia come clock per la base dei tempi. Lo standard prescrive inoltre le maschere frequenziali e temporali di trasmissione per la potenza.

CAPITOLO IV

CONFRONTO TRA I PROTOCOLLI A LIVELLO MAC

IEEE 802.11 e Hiperlan2 sono due protocolli che definiscono un livello fisico e un livello MAC (Media Access Control) per comunicazioni wireless a breve raggio (da pochi metri a 100 m) e a basso consumo di potenza (da meno di un mW a 1 W). Hiperlan2 ed IEEE 802.11 sono orientati a connessioni fra computer, come estensione o sostituto delle LAN cablate ovvero altre applicazioni. In questo capitolo si propone di confrontare le caratteristiche principali di questi due protocolli.

4.1 Comunicazione all'interno delle reti

Ci proponiamo in questa sezione un confronto tra gli standard IEEE 802.11 e Hiperland2 riguardo alle caratteristiche delle comunicazioni tra le stazioni appartenenti ad una stessa cella base. In IEEE 802.11 è il Basic Service Set (BSS), in Hiperlan2 è la comunicazione tra l'AP e MT.

4.1.1 Banda radio

Lo standard IEEE 802.11 e hiperlan2 utilizzano diversi banda ISM (Industrial Scientific Medical) a eccezione del 802.11a che usa la stessa banda di Hiperlan2 quella di 5 GHz. La banda che usano le altre tecnologie 802.x è quella di 2.4 GHz ed si estende da 2.4 GHz a 2.4835 GHz.

4.1.2 Utilizzo della banda, tecniche di modulazione e trasmissione RF

*802.11

I dispositivi IEEE 802.11 utilizzano la tecnica DSSS (Direct Sequence Spread Spectrum). La banda disponibile viene suddivisa in 14 canali, parzialmente sovrapposti, ciascuno di ampiezza pari a 22 MHz. Tutti i terminali appartenenti ad

una stessa BSS (con infrastruttura o ad hoc) utilizzano sempre lo stesso canale per le comunicazioni. Per codificare il flusso dei dati trasmessi si usano due tecniche:

- Sequenza di Barker: è la tecnica specificata nello standard IEEE 802.11, il simbolo trasmesso è rappresentato da una sequenza di 11 chip che codifica ogni singolo bit d'informazione. La velocità di modulazione è 1 Msimbolo/s. Le tecniche di modulazione utilizzate sono la BPSK, con la quale ogni simbolo codifica 1 bit d'informazione e quindi si ottiene una velocità di trasferimento pari a 1 Mbps, e la QPSK, con la quale ogni simbolo codifica 2 bit d'informazione e quindi si ottiene una velocità di trasferimento pari a 2 Mbps.
- Lo standard IEEE 802.11b 11g su cui si basano i dispositivi oggi in commercio, usa invece la tecnica CCK (Complementary Code Keying): 16 bit trasmessi sul canale codificano 4 o 8 bit d'informazione. Viene usata una velocità di modulazione pari a 1.375 Msimboli/s con la tecnica QPSK. Quindi, si ottiene una velocità di trasferimento pari a 5.5 Mbps quando il simbolo, o codice CCK, codifica 4 bit d'informazione, mentre si ottiene una velocità di trasferimento pari a 11 Mbps quando il simbolo codifica 8 bit d'informazione può anche raggiungere una velocità massima di 53 Mbps. Tutti i dispositivi conformi allo standard IEEE 802.11g sono interoperabili con i dispositivi IEEE 802.11.

* Hiperlan2

Invece la il standard Hiperlan2 usa la tecnica OFDM con schemi di modulazione e di codifica delle sottoportanti variabili in base alla qualità del collegamento radio, la velocità trasmissiva è compressa tra 6 e 54 Mbps. Le differenze rispetti a quanto prescritto dello standard 801.11 consistono unicamente nel rate del codice impiegato nel modo 5 e nell'assenza del modo 7 (tabella 2.1). Nello standard hiperlan2 inoltre è opzionale solo la modulazione 64QAM.

4.1.3 Potenza di trasmissione

Lo standard IEEE 802.11 prevede che:

- Sia previsto almeno un livello di potenza con EIRP (*Equivalent Isotropic Radiated Power*) pari a 10 mW;
- Per i dispositivi con livelli di potenza massima superiori a 100 mW EIRP, sia previsto almeno un livello di potenza pari a 100 mW EIRP (o ad un livello inferiore).

Hiperlan2 implementa un meccanismo per il controllo della potenza di trasmissione (*transmit Power Control*-**TPC**) sia da parte del MT (in uplink e direct-link) che da parte dell'AP (in downlink).Tutto ciò al fine di raggiungere due obbiettivi:

- Semplificare il progetti del ricevitore nell'AP, non necessitando più di un sistema per il controllo automatico del guadagno (AGC-Automatic Gain Control).
- Ridurre le interferenze, ad esempio, con sistemi satellitari.

Lo standard definisce i seguenti limiti di potenza di trasmissione:

- 200 mW EIRP media (*Equivalent Isotropic Radiated Power*) nella banda 5.15-5.35 MHz, con uso esclusivamente in interni ed implementazione di DFS e TPC.
- 1W EIRP media nella banda 5.47-5.725 MHz, con uso in interni ed in esterni ed implementazione di DFS e TPC.

4.1.4 Pacchettizzazione e throughput

* IEEE 802.11

La dimensione del payload varia da 0 a 2304 byte. L'intero frame IEEE 802.11, header e payload, viene protetto da un CRC32. Non è previsto alcun FEC. Un dispositivo IEEE 802.11g è capace di trasmettere ad una velocità pari a 54 Mbps lordi.

*Hiperlan2

Consistono di sequenze di PDU comprendenti PDU per l'utente (**U-PDU** di 54 byte con 48 byte di payload) e PDU di controllo (**C-PDU** di 9 byte). È convenzione comune riferirsi ai C-PDU come al "canale di trasporto breve" (**SCH**, *Short transport CHannel*) ed ai U-PDU come al "canale di trasporto lungo" (**LCH**, *Long transport Channel*). Lo standard HIPERLAN/2 consente di raggiungere data rate molto elevati fino a 54Mbit/s a livello fisico e fino a 25Mbits/s al 3^{o} livello.

4.1.4 Conclusioni

- Il livello MAC dello standard 802.11 supporta pacchetti a lunghezza variabile, a differenza di quello di Hiperlan2 che gestisce solo pacchetti a lunghezza fissa:
  - Pacchetti di dimensione maggiori comportano prestazioni peggiori nel collegamento radio, ma un miglior throughput per i dati.
  - Pacchetti più piccoli consentono una buona qualità del link a discapito del throughput.

  Questo perché l'accesso al canale non è mai garantito, perciò l'uso di pacchetti piccole dimensione può aumentare il tempo di attesa di un canale libero.

- Il protocollo IEEE 802.11 prevede l'aggiustamento dinamico della velocità di trasferimento dati in base alla qualità del segnale sul canale trasmissivo; la scelta di uno dei 4 data rate possibili viene effettuata dinamicamente dal livello fisico (PHY) e quindi in maniera trasparente ai livelli superiori del protocollo, compreso il MAC.
- Anche lo standard Hiperlan2 prevede l'aggiustamento dinamico della velocità di trasferimento dati in base alla qualità del segnale sul canale trasmissivo dovuto alla modulazione OFDM che è in grado di funzionare in diversi modi, combinandoli con diversi schemi di modulazione che vengono gestiti e selezionati dalla funzione di adattamento del collegamento.

- Lo standard Hiperlan2 offre un throughput maggiore dello standard 802.11in generale.

4.2 Creazione delle reti

4.2.1 Struttura di rete

Entrambi i protocolli prevedono la possibilità di creare una struttura di rete più complessa a partire dai singoli blocchi base:

- ESS (*Extended Service Set*) per 802.11: una ESS è costituita da un certo numero di BSS interconnesse tramite un sistema di distribuzione (DS), che può essere una rete LAN cablata oppure un sistema wireless, anche un altro sistema IEEE 802.11. Le stazioni wireless possono essere mobili e spostarsi da una BSS ad un altra, all'interno della stessa ESS, mantenendo la connessione alla rete. Il sistema di distribuzione si occupa del trasporto dei dati tra BSS diverse. In ogni BSS vi sarà una particolare stazione delegata a tenere i contatti con il DS: se la BSS è di tipo ``con infrastruttura'' tale stazione verrà indicata con il nome di Access Point (AP).
- La struttura tipica di HIPERLAN/2 prevede dei terminali mobili (MT-mobile terminal) che comunicano via radio con un solo punto di accesso(AP-Access point) della rete fissa.

4.2.2 Velocità di creazione delle reti

Un altro parametro significativo per il confronto tra i due protocolli presi in esame è la velocità di creazione delle reti, ovvero la velocità con la quale vengono stabilite le connessioni tra due o più dispositivi.

* 802.11

Prevede le procedure di Scan, Autenticazione e Associazione.

**Procedura di Scan*

La procedura di Scan può essere effettuata in modalità Passiva o Attiva, e serve a conoscere gli indirizzi MAC ed altri parametri relativi alla sincronizzazione corrispondenti a stazioni IEEE 802.11 che si trovano nel raggio d'azione del terminale.

Il tempo medio di scoperta dei dispositivi con la modalità di scan passivo è pari a 50ms moltiplicato per il numero di canali che si intende osservare. Il valore 50ms rappresenta la metà del valore tipicamente assegnato al parametro BeaconPeriod (valore minimo: 1 Time Unit=1024μs). Secondo questa modalità infatti, la stazione si mette in ascolto su un certo numero di canali, tra quelli previsti dalle regolamentazioni nazionali, in attesa di ricevere dei frame di tipo Beacon. Tale frame viene trasmesso periodicamente dall' AP se è presente una rete con infrastruttura, mentre viene trasmesso periodicamente da una stazione eletta con uno schema distribuito se è presente una rete ad hoc (Indipendent Basic Service Set o IBSS).

Usando la procedura di scan attivo invece, la stazione deve prima guadagnare l'accesso al mezzo secondo il metodo CSMA/CA per inviare un frame di tipo Probe Request, dopo diche deve attendere l'accesso al mezzo e l'invio del frame Probe Response dalle stazioni che hanno ricevuto il Probe Request. In questo caso, il tempo di scoperta minimo, in assenza di interferenze esterne alla rete e considerando una rete lontana dalla saturazione, è pari al tempo necessario a trasmettere un frame Probe Request, più un intervallo DIFS (DCF Inter-Frame Space), più il tempo necessario a trasmettere un frame Probe Response, il totale moltiplicato per il numero di canali che si vuole osservare. Possiamo riassumere i suddetti tempi nella tabella seguente

Standard	Tempo (per un singolo canale)
IEEE 802.11 DS 1Mbps	$3ms$
IEEE 802.11b DS 11Mbps	$450\mu s$

Tabella 4.1: Tempi di scoperta dei dispositivi IEEE 802.11 con scan attivo

Se stiamo realizzando una rete ad hoc, la procedura di Scan è sufficiente. Anche l'autenticazione tra due stazioni in modalità ad hoc può essere effettuata ma non è richiesto esplicitamente dallo standard.

Se invece la stazione volesse aggiungersi ad una rete con infrastruttura, una volta scoperto l'Access Point con la procedura di Scan, è richiesta l'Autenticazione tra la stazione e L'Access Point (AP), cui segue l'Associazione della stazione con l'Access Point. Una volta effettuata l'associazione con l'AP, la stazione può comunicare con stazioni in altre BSS di cui l'AP è a conoscenza, può comunicare con il metodo Point Coordination Function (PCF), può comunicare con stazioni fuori dalla sua portata ma visibili all'AP.

**Procedura di Autenticazione*

Può essere effettuata in due modi:

- *Open System Authentication* è il metodo che non prevede alcuna identificazione della stazione. In pratica, una stazione che richiede l'autenticazione con questo metodo, viene autenticata dalla stazione destinataria della richiesta se essa ha scelto lo stesso metodo OSA come metodo d'autenticazione. Questa procedura richiede lo scambio di due frame tra le stazioni coinvolte.
- *Shared Key Authentication* prevede che una stazione venga autenticata da un'altra stazione solo se la prima possiede la stessa chiave segreta della seconda. La chiave segreta comune a più stazioni autenticate tra loro dev'essere distribuita tramite un canale diverso da un canale IEEE 802.11. L'utilizzo di questo metodo è possibile solo se le stazioni implementano il protocollo WEP (*Wired Equivalent Privacy*). Questa procedura prevede lo scambio di quattro frame fra le due stazioni coinvolte.

**Procedura di Associazione*

Prevede l'invio, sempre secondo le regole CSMA/CA, del frame Association Request dalla stazione verso l'Access Point, il quale dovrà rispondere con il frame

Association Response. Ancora una volta, i tempi di questa operazione di associazione sono quelli relativi all'invio di un frame ed alla ricezione di una risposta: pertanto possono essere applicate le stesse considerazioni e gli stessi risultati visti per la procedura di scan attivo.

*Hiperlan2

Prevede il protocollo MAC che viene usato per l'accesso al mezzo trasmissivo (il collegamento radio) e per la trasmissione di dati attraverso di esso. La gestione dei segnale di controllo è centralizzata ogni AP controlla tutte le trasmissioni in up-link, in down-link ed in direct-link; durante l'*associazione* il RLC (*Radio link Control*) assegna ad ogni terminale un identificatore unico. L'AP informa i MT circa l'istante all'interno del MAC frame in cui questi sono autorizzati a trasmettere i loro dati, in modo tale che possano organizzare opportunamente le richieste di accesso.

L'accesso al mezzo trasmissivo (l'aria) è infatti gestito secondo uno schema di tipo TDMA-TDD (T*ime Division Multiple Access-Time Division Duplex*):

- ogni utente, cioè ogni MT, è autorizzato a trasmettere i propri dati solo in determinati slot temporali all'interno del MAC frame .

Tale struttura permette la comunicazione simultanea sia in up-link che in down-link all'interno dello stesso frame. L'allocazione degli slot temporali per il link nelle due direzioni avviene in maniera dinamica, per meglio soddisfare le necessita delle varie trasmissioni. La struttura base del MAC frame ha una durata fissa di 2ms e comprende vari canali suddivisi in canali logici e canali di trasporto, ognuno dei quali può essere utilizzato in uplink/downlink/direct-link a seconda della funzione che assolve.

Anche è previsto in hiperlan2 una processo di Autenticazione e Associazione.

**Autenticazione*

Per l'autenticazione possono essere utilizzate algoritmi a chiave segreta e pubblica. L'autenticazione è realizzata utilizzando codici di autenticazione di messaggi basata su MD5, HMAC e firma digitale basata su RSA. Meccanismi di risposta a sfide sono anche previsti per realizzare identificazioni.

**Associazione*

Il MT si pone in ascolto sei vari AP e seleziona quello con il collegamento radio di migliore qualità, quindi continua ad ascoltare il broadcast di un identificatore di operatore di rete unico o globale al fine di evitare un'associazione con una rete che non è in grado o non è abilitata a fornire servizi all'utente del terminale. Se il MT decide di continuare l'associazione richiederà e riceverà un MAC-ID dall'AP.

4.2.3 Conclusioni

Le due standard hanno una infrastruttura di rete molto simile ma comunque hanno un tempo connessione diverso per la creazione della rete, dove si può stimare che il tempo per creare una rete in Hiperlan2 è minore di quella per il 802.11dovuto che il tempo del frame in 802.11 non è fisso come è successo in Hiperlan2, questo anche per la tecnica di acceso che loro due implementano che sono diversi. Hiperlan2 fornisce anche migliore prestazioni nella sicurezza con la autenticazione e associazione che lo standard 802.11.

4.3 Topologie di rete

* IEEE802.11

Le specifiche IEEE 802.11 rappresentano uno standard per la realizzazione di wireless LAN operanti nella banda ISM 2.4 GHz. Lo standard prevede sia la comunicazione diretta (peer-to-peer) tra i terminali, che la comunicazione tra i terminali e le base station dette Access Point (AP).

* Topologia con infrastruttura

La configurazione tipica di una rete realizzata con dispositivi IEEE 802.11 è quella cosiddetta ``con infrastruttura".

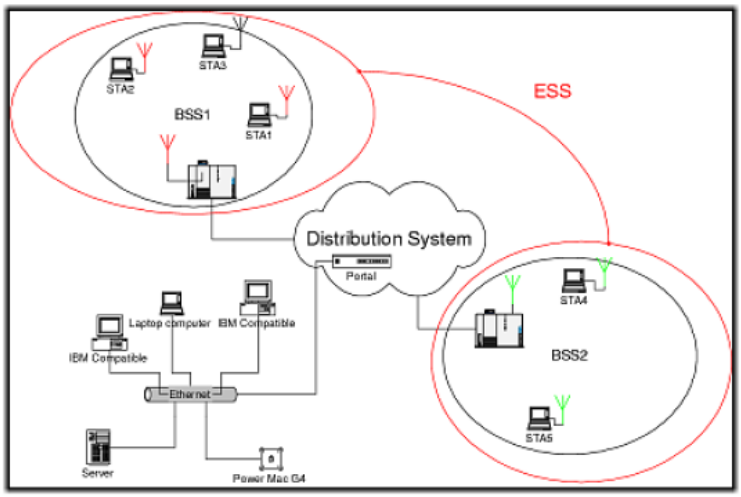


Figura 4.1: Topologia con infrastruttura e definizione di ESS

Si possono identificare delle celle base, dette BSS (Basic Service Set) nelle quali i terminali si associano con un AP ed il traffico tra le stazioni associate fluisce attraverso l'Access Point stesso (i terminali associati con l'Access Point non comunicano direttamente tra di loro). In una BSS può esistere solo un Access Point.

Diverse BSS possono essere interconnesse tramite un Distibution System (DS), a formare un cosiddetto ESS (Extended Service Set). Viene definito inoltre il Portale, ovvero un'entità che collega il Distribution System con altre infrastrutture di rete integrate, ad esempio LAN Ethernet. Si osservi che:

- le BSS possono sovrapporsi parzialmente
- le BSS possono essere disgiunte nello spazio
- possono essere collocate nella stessa area più ESS o anche reti con topologia ad hoc Indipendent BSS (IBSS)

La figura seguente illustra la famiglia degli IEEE 802 e la loro relazione con i livelli dello stack OSI/ISO:

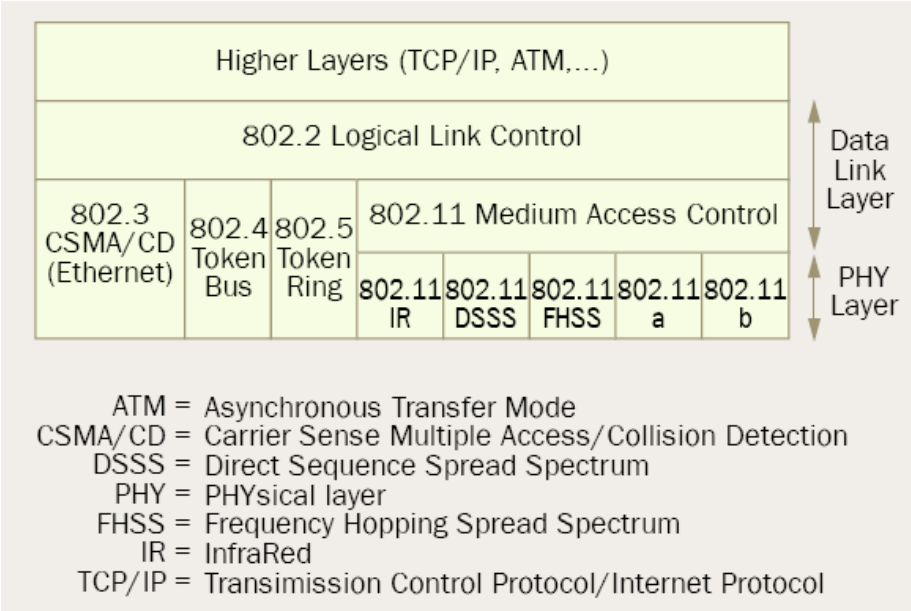


Figura 4.2: La famiglia degli standard IEEE 802

Lo standard IEEE 802.11 contiene le definizioni del livello MAC e del livello fisico, e specifica dei Servizi grazie ai quali si può implementare un sistema di distribuzione e quindi una rete ESS, la quale apparirà come un'unica BSS dal livello LLC (Logical Link Control) dei terminali associati con un AP in una qualunque BSS. I seguenti servizi (Distribution System Services) sono definiti per la realizzazione di una topologia ESS:

Associazione

È il servizio con il quale le stazioni di una BSS si associano ad un Access Point allo scopo di usufruire del Distribution System. Grazie all'associazione, il Distribution System realizza una mappa delle stazioni associate con i vari Access Point della ESS.

Disassociazione

È il servizio invocato per terminare un'associazione.

Riassociazione

È un servizio invocato per spostare l'associazione di una stazione da un Access Point ad un altro, oppure per cambiare dei parametri relativi ad un'associazione.

Distribuzione

È il servizio che si occupa di trasportare i messaggi attraverso l'AP della BSS di appartenenza. Dev'essere usato per ogni comunicazione da parte di una stazione associata con un Access Point.

Integrazione

Se il servizio di Distribuzione suddetto determina che il destinatario finale di un messaggio è un membro di una LAN integrata, allora il punto d'uscita del messaggio dal Distribution System è un Portale anzichè un Access Point e viene invocato il servizio di integrazione dopo il servizio di distribuzione.

Sono definiti inoltre i servizi SS (Station Services):

Autenticazione

È usato da tutte le stazioni per stabilire la propria identità nei confronti delle stazioni con cui si vuole comunicare. Nel caso di topologia con infrastruttura, l'autenticazione è un prerequisito per l'associazione e viene effettuata nei confronti dell'AP.

Deautenticazione

È un servizio invocato per terminare un'autenticazione. Nel caso di topologia con infrastruttura, la deautenticazione comporta la disassociazione.

Privacy

È il servizio che permette la cifratura dei messaggi trasmessi.

Trasporto dei pacchetti

Ogni stazione dev'essere in grado di accedere al mezzo per inviare e ricevere pacchetti. Questo servizio è usato dalle stazioni associate con una Access Point per comunicare con l'Access Point e per comunicare fra stazioni non associate con un Access Point (in modalità ad hoc).

* Topologia ad hoc

Come abbiamo detto, lo standard IEEE 802.11 consente a due o più terminali di comunicare direttamente, senza la presenza di alcuna infrastruttura di rete.

Possiamo osservare che:

- L'unico metodo d'accesso disponibile è quello con acceso al mezzo distribuito (DCF) (Distributed Coordination Function), che segue le regole del protocollo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Non è disponibile l'accesso controllato centralizzato (PCF).
- Non esiste un Distribution System, quindi i servizi di Associazione, Disassociazione, Riassociazione, Distribuzione ed Integrazione non sono disponibili.
- Una IBSS può avere un numero qualsiasi di partecipanti.
- È possibile realizzare delle reti ad hoc di tipo multi hop ma un terminale non può appartenere a più di una IBSS.

*Hiperlan2

Opera nella banda di frequenza intorno ai 5.2 GHz (da 5.15 a 5.35 GHz e da 5.470 a 5.725 GHz) con spettro di 455 MHz. La struttura tipica di HIPERLAN/2 prevede dei terminali mobili (*MT-mobile terminal*) che comunicano via radio con un solo punto di accesso(*AP-Access point*) della rete fissa ed, in caso di movimento, il passaggio a punti di accesso adiacenti (handover) avviene in maniera automatica, è possibile anche la comunicazione diretta tra terminali mobili per mezzo di connessioni ‘ad hoc’(create al momento, con una durata strettamente necessaria allo scambio di dati).

L'Hiperlan2 prevede due modalità di funzionamento:

Centralized mode: ogni AP si connetta alla network core che serve le MT a lui associate. Tutto il traffico dei terminali mobili passa attraverso l'AP, sia che appartengano allo stesso AP, sia che appartengano a due core network differenti. Questo è obbligatorio per tutte le MT e gli AP.

Direct mode: l’accesso ai canali di trasmissione è ancora gestito in maniera centralizzata da parte dell’AP, ma il traffico dati avviene direttamente tra i terminali senza passare dell’AP. Questo modo viene usato in ambiente particolarmente piccoli

(ad esempio le abitazioni) in cui si aspetta che la maggior parte del traffico avvenga tra terminale associati allo stesso AP. La comunicazione da MT a MT è definita *Direct Link* (DL).

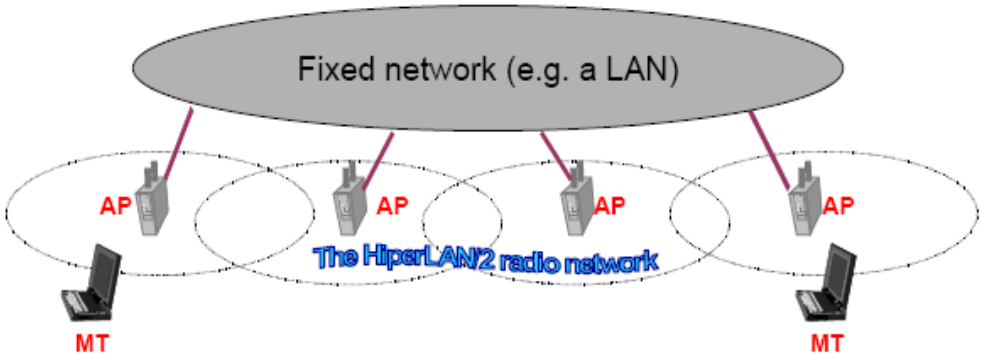


Figura 4.3: Rete Hiperlan/2

Conclusioni

- Le topologie rappresentate dalla BSS con infrastruttura 802.11 e Centralized mode della Hiperlan2 presentano numerose analogie. In entrambi i casi, il traffico è gestito da un'entità centralizzata (Access Point in IEEE 802.11come in Hiperlan2), con la differenza dove in Hiperlan2 le stazioni, durante gli spostamenti , possono effettuare misure su tutte le frequenze disponibili in modo di rivelare il miglior punto di accesso alla rete, questo procedimento è chiamato Handover mentre questa funzione non è presente in un Access Point 802.11. Con questa topologia dunque il routing dei pacchetti all'interno della singola cella base è effettuato attraverso l'Access Point per 802.1 e Hiperlan2 .
- Una rete del tipo Ad-hoc è invece costituta solo da stazioni terminali, in essa lo scambio di pacchetti avviene direttamente tra le stazioni coinvolte. Per queste reti, se realizzate con apparti a standard Hiperlan2 è necessario che una delle stazioni, chiamata CC (*Central Controller*), gestisca l'allocazione

della banda dalle altre. Invece lo standard 802.11consente a due o più terminali di comunicare direttamente.

4.4 QoS

* IEEE 802.11

Offre il metodo d'accesso al mezzo detto Point Coordination Function (PCF), alternativo al Distributed Coordination Function (DCF). L'utilizzo di questo metodo d'accesso è limitato alla topologia con infrastruttura e prevede che una stazione detta Point Coordinator (PC), che di solito coincide con l'Access Point, regoli l'accesso al mezzo delle stazioni che richiedono di far parte di una polling list, interrogandole con uno schema round robin e garantendo loro l'accesso al mezzo. In ogni caso, una parte del canale dev'essere comunque dedicata all'accesso con contesa. Viene definito infatti un intervallo temporale detto superframe, composto da un Contention Free Period (CFP) durante il quale vige il metodo PCF, ed un periodo, Contention Period (CP), durante il quale vige il metodo DCF. Il CP deve durare abbastanza da permettere almeno l'invio di un frame.

Il metodo d'accesso PCF presenta le seguenti caratteristiche:

- La dimensione temporale di un periodo CFP può venire ridotta da un residuo di traffico DCF. Dunque, non è garantita un'effettiva allocazione temporale delle risorse del canale, poichè gli istanti di inizio dei periodi CFP non vengono necessariamente preservati.
- Una stazione interrogata dal PC può trasmettere solo un frame, di dimensione variabile tra 0 e 2304 byte. All'inizio di un CFP non è nota la quantità totale dei dati che tutte le stazione della polling list devono inviare. A causa della variabilità dei payload dei frame delle stazioni interrogate e del tempo necessario a trasmettere tali frame, il PC potrebbe non riuscire ad interrogare tutte le stazione della polling list entro il CFP. Le stazioni che rimangono escluse, dovranno ritardare ulteriormente le loro trasmissioni, e

quindi viene introdotto del ritardo che potrebbe non essere accettabile per applicazioni time-bounded.

*Hiperlan2

Lo standard definisce che *Data Link Control* (**DLC**) consiste nelle funzioni di *Error Controll* (**EC**), di **MAC** ed di *Radio Link Control* (**RLC**), è Connection Oriented, dove prima che un MT inizi la trasmissione, comunica con l'Access Point attraverso il "piano di segnalazione", time slot ad accesso casuale, ed imposta una connessione temporanea. Ciò consente di negoziare i parametri di QoS, requisiti di ritardo, jitter e larghezza di banda, e di non interferire reciprocamente con altri terminali nelle trasmissioni successive.

Conclusioni

- Il problema del supporto QoS a livello MAC non è stato affrontato dallo standard IEEE 802.11 fino ad ora. Sono attualmente allo studio del Task Group IEEE 802.11e diverse modifiche al MAC 802.11 che offrano supporto per applicazioni che richiedono un certo QoS.
- Meccanismi di QoS e di gestione di servizi con vincoli temporali o di errore è applicabili in Hiperlan2. A ogni connessione può essere assegnato un particolare valore di QoS, intermini, ad esempio, di banda, jitter, tasso di errore o, più semplicemente, indicando un livello di priorità. Questi meccanismi facilitando lo svolgimento di servizi, quali quello fonico o video in combinazione con quello di trasmissione di dati.

CAPITOLO V

CONFRONTO COSTI E CONSUMI

In questo capitolo ci proponiamo di confrontare due soluzioni wireless attualmente sul mercato, una per realizzare dispositivi IEEE 802.11 ed una per realizzare dispositivi Hiperlan2. Il confronto si focalizzerà principalmente sul consumo di potenza e sul costo dei dispositivi.

5.1 Broadcom per lo standard 802.11

La Broadcom Corp. (http://www.broadcom.com) rappresenta attualmente uno dei più grossi produttori di hardware per la realizzazione di dispositivi 802.11, in tutte le sue versioni da IEEE 802.11a fino IEEE802.11g.

5.1.1 Caratteristiche dell' hardware

Attualmente la Broadcom offre la soluzione **BCM94318**, per la realizzazione di dispositivi compatibili con lo standard IEEE 802.11g. Il chipset BCM94318 realizza sia il livello fisico (RF) che il livello MAC compatibili con lo standard IEEE 802.11a,g.

Nella figura 5.1 possiamo osservare una schematizzazione del sistema BCM94318:

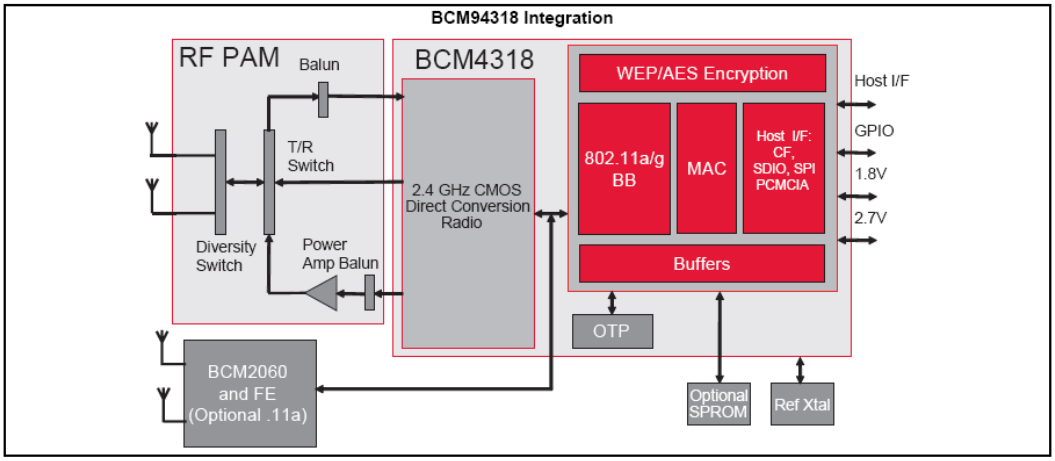


Figura 5.1: Soluzione BCM94318 per Broadcom

Nella tabella 5.1 possiamo osservare come è composto il sistema:

Interface	PCI, SDIO/SPI
System Bus Support	PCI, CardBus, Compact Flash, EBI
Standard	IEEE 802.11g, 802.11a with external radio BCM2060
Data Rate, Mbps	54, 48, 36, 24, 18, 12, 9, 6/11, 5.5, 2, 1
Modulation	PSK/CCK, DQPSK, DBPSK, OFDM
Network Architectures	Infrastructure and ad hoc
Operating Frequencies	2.4 GHz—2.497 GHz, 4.9 GHz —5.85 GHz with 2060 option
Operating Channels	11 for North America; 13 for Europe, and 14 for Japan
RF Output Power	20 dBm maximum
Antenna Connectors	Hardware diversity support - Transmit and Receive
Power Requirements	1.8V (3.3V for ref designs)
Power Consumption	Average Standby < 20 mW
Security	802.1x; WEP; WEP2; WPA, WPA2; TKIP; Weak-key avoidance; CCX, CCX 2.0; 128-bit OCB mode AES, 802.11i
Dimensions	12mm x 12mm 196-pin pkg., 10mm x 10mm 144-pin pkg
Software Support	Microsoft WHQL certified for Windows XP, Windows 2000, Windows Me, and WindowsSE operating systems. Embedded drivers for Linux and VxWorks operating systems
Certifications	IEEE 802.11 compliant; Wi-Fi CERTIFIED; ACPI power management

Tabella 5.1: Specifica del chipset BCM94318

5.1.2 Cosa offre lo standard 802.11 per la riduzione del consumo di potenza

Un dispositivo IEEE 802.11, in un istante qualsiasi, può trovarsi in uno dei seguenti due stati:

- Awake: la stazione è completamente operativa
- Doze: la stazione non riceve né trasmette ed il consumo di potenza è ridotto.

Conseguentemente abbiamo due modalità di Power Management:

- Active Mode (AM)

- Power Save Mode (PS)

La gestione delle stazioni in PS è ovviamente diversa a seconda della topologia della nostra rete IEEE 802.11:

** Topologia con infrastruttura*

Una stazione in AM che vuole entrare in PS, deve effettuare con successo uno scambio di pacchetti con l'Access Point cui è associata (ovvero deve ricevere un *Acknowledgement*), modificando il bit dedicato al Power Management contenuto nell'header dei pacchetti. In questa topologia infatti, l'Access Point si occupa di archiviare tutto il traffico destinato alle stazioni della rete che si trovano in PS.

L'Access Point costruisce la mappa virtuale delle stazioni in PS e del traffico ad esse destinato e comunica tale mappa tramite l'elemento TIM (*Traffic Indication Map*) contenuto in ogni Beacon che esso invia periodicamente. La modalità PS delle stazioni prevede che, ad intervalli regolari e configurabili, le stazioni stesse rientrino nello stato AM per ricevere i Beacon inviati dall'Access Point e quindi sapere se quest'ultimo ha del traffico bufferizzato per loro. Nel caso una stazione non rilevi dal TIM che l'Access Point ha del traffico indirizzato a se stessa, può tornare nello stato PS, fino al prossimo istante prescelto per l'ascolto del beacon. Nel caso contrario invece, la stazione può richiedere l'invio del traffico bufferizzato nell'Access Point, inviandogli un frame di tipo PS-Poll cui l'Access Point risponde appena possibile inviando il traffico bufferizzato per quella stazione.

Una stazione che vuole rientrare in Active Mode dalla modalità *Power Save*, deve effettuare l'operazione detta *Clear Channel Assesment* (CCA) per rilevare la presenza di eventuali trasmissioni in corso sul canale ed, in caso ve ne siano, ritardare il tentativo d'accesso al mezzo con le modalità previste dal MAC.

** Topologia ad hoc*

In questa topologia le stazioni possono comunque utilizzare la modalità Power Save ma, visto che non esiste un Access Point, tutte le stazioni devono occuparsi di bufferizzare il traffico di tutte le stazioni che si trovano in Power Save. Viene definita un finestra temporale (*ATIM Window*), durante la quale tutte le stazioni in Power

Save si portano nello stato Awake per ricevere dei frame particolari, gli ATIM (ad hoc TIM). Le stazioni che hanno del traffico bufferizzato per qualche altra stazione in Power Save, durante l'ATIM Window accedono al mezzo per inviare frame di tipo ATIM direttamente indirizzate alle stazioni che devono ricevere il traffico bufferizzato. Se queste stazioni ricevono correttamente il frame ATIM, rimangono nello stato Awake anche dopo la fine della ATIM Window, per ricevere il traffico ad esse destinate; in caso contrario le stazioni possono tornare nello stato Power Save fino alla prossima finestra ATIM.

Possiamo osservare che:

- Le stazioni che vogliono entrare in Power Save non hanno una stazione referente analoga all'Access Point cui comunicare tale cambiamento di stato. Dunque lo stato istantaneo di una stazione, Awake o Doze, può essere solo stimato da tutte le altre stazioni della rete ad hoc, ad esempio in base alla storia delle precedenti trasmissioni. Lo standard non specifica alcun metodo per la stima dello stato Power Management delle stazioni in una rete con topologia ad hoc;
- L'invio e la ricezione dei frame ATIM durante la finestra ATIM Window avviene secondo le regole del metodo Distributed Coordination Function (DCF), ovvero secondo il metodo d'accesso CSMA/CA. A seconda del traffico presente sul mezzo trasmissivo, potrebbe anche non essere possibile, per una stazione con del traffico bufferizzato per un'altra stazione in Power Save, riuscire a mandare il frame ATIM, oppure potrebbe non essere possibile, per la stazione che deve ricevere il traffico, mandare un frame ACK verso la stazione che ha bufferizzato il traffico, impedendo di fatto la trasmissione del suddetto traffico dopo la finestra ATIM. Quindi, in definitiva, lo standard IEEE 802.11 specifica un solo stato a basso consumo di potenza, lo stato Doze, e dà la possibilità di configurare i tempi in cui una stazione rimarrà nello stato Doze (tramite il parametro ListenInterval, che specifica l'intervallo di tempo che intercorre tra l'ascolto consecutivo di due beacon)

Implementare lo standard con i chipset BCM94318

Abbiamo visto come lo standard IEEE 802.11 prevede una sola modalità Power Save, con la possibilità di configurare quanti beacon ascoltare e quindi quanto effettivamente rimanere nello stato Doze.

- Il dispositivo ha una specificazione che possiamo vedere nella tabella 4.1 che nella modalità di standby (che sarebbe quella di Powe Save) ha una media di minore di 20 mW, la specifica non indica il tempo che fa per entrare in questa modalità.

5.1.3 Costi

Il kit BCM94318 comprende:

- il BCM 4318 (2.4 GHz CMOS Direct Conversion Radio, WEP/AES Encryption, 802.11a/g BB, MAC Host I/F: CF, SDIO, SPI, PCMCIA, Buffers, OTP)
- RF-PAM (Diversity Switch, Balun, T/R switch, Power Amp. Balun)
- BCM2060 and FE (Optional .11a)
- Opzionale SPROM

Con questa chipset nel mercato possiamo trovare queste schede:

- BCM94318 SD (2.4 GHz 802.11b/g Secure Digital Client Production Design), 144-pin BGA package
- BCM94318 MPG 802.11b/g per MiniPCI
- BCM94318 MPAG 802.11a/g per MiniPCI

Dove ognuno costa circa 40$

5.2 Atheros per lo standard Hiperland2

Attualmente la tecnologia non è molto diffusa per la sua complessità e quindi non è ancora supportata da una ampia disponibilità di prodotti ma comunque l'Atheros (http://www.Atheros.com) offre la gamma AR50006XS, specificamente il chipset AR5414, per la tecnologia hiperlan2 insieme a lo standard 802.11a, vista l'estrema somiglianza del PHY layer. Infatti il prodotto no implementa la tecnica d'accesso specificata in hiperlan2, ma può garantire una QoS, ed anche il DFS e il TPC.

5.2.1 Caratteristiche dell' hardware

Le specifiche del AR5414 può essere descritta nella tabella 5.2.

Frequency Band	4.900 to 5.850 GHz and 2.300 to 2.500 GHz
Network Standard	802.11a, 802.11b, 802.11g
Modulation Technology	OFDM with BPSK, QPSK, 16 QAM, 64 QAM; DBPSK, DQPSK, CCK
FEC Coding Rate	1/2, 1/3, 1/4
Hardware Encryption	AES, TKIP, WEP
Quality of Service	802.11e draft
Media Access Technique	CSMA/CA
Host Interface	Mini PCI, CardBus, PCI
Communication Interface	High speed UART
Peripheral Interface	GPIOs, LEDs
Memory Interface	EEPROM
Supported Data Rates	
IEEE 802.11a	6 to 54 Mbps
IEEE 802.11b	1 to 11 Mbps
IEEE 802.11g	1 to 54 Mbps
Atheros Super AG Mode	Up to 108 Mbps
Chip Specifications	AR5414
Operating Voltage	1.8V +/-5% 3.3V +/-10%
Package Dimensions	13mm x 13mm
Package	224 Plastic Ball Grid Array

Tabella 5.2: Specifiche del chipset AR5414

La schematizzazione del chipset può essere vista nella figura 5.2

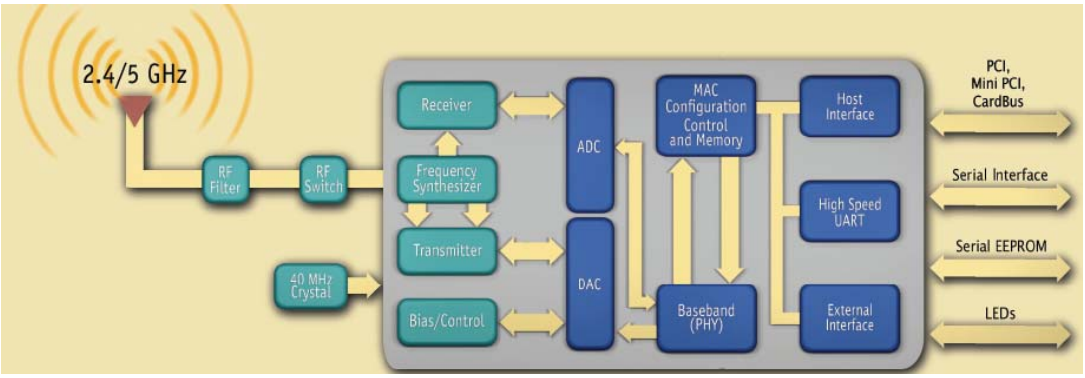


Figura 5.2: Schema del AR5414

5.2.2 Cosa offre Hiperlan2 per la riduzione del consumo di potenza

Hiperlan2 implementa un meccanismo per il controllo della potenza di trasmissione (*transmit Power Control*-TPC) sia da parte del MT (in uplink e direct-link) che da parte dell'AP (in downlink).Tutto ciò al fine di raggiungere due obbiettivi:

- Semplificare il progetti del ricevitore nell'AP, non necessitando più di un sistema per il controllo automatico del guadagno (AGC-*Automatic Gain Control*).
- Ridurre le interferenze, ad esempio, con sistemi satellitari.

Il livello di potenza di trasmissione viene adatto in base alle capacita di decodifica del ricevitore più lontano; nei casi in cui sia richiesta una maggiore potenza pur essendo già stato raggiunto il limite massimo o, viceversa, sia richiesta una minore potenza pur essendo già stato raggiunto il limite minimo, il trasmettitore può inoltre una richiesta di passaggio ad un modo PHY più appropriati.

Lo standard prevede un meccanismo per il risparmio energetico basato sulla gestione dei periodi di inattività dei MT (*sleep*). Il MT può, in ogni istante, richiede all'AP di entrare in uno dei sedici stati di basso consumo (specifico per ogni MT) e richiede uno specifico periodo di sleep. Alla fine di tale periodo concordato il MT si mette in ricerca di un segnale di risveglio (wake-up) da parte di un AP sul canale

broadcast, in mancanza di questo toma in stato di basso consumo per il successivo periodo e così via (al contrario, quando il MT è in uno stato attivo, controlla il canale broadcast in ogni frame). Il MT cambierà il suo stato da sleep ad attivo quando identificherà sul canale di controllo del frame un MAC-ID corrispondente al proprio. Ogni AP rimanderà la trasmissione di dati ad un certo MT finché il corrispondente periodo di sleep non sarà giunto al termine. Anche nella trasmissione di tipo DL (da MT a MT) è compito dell'AP svegliare un MT quando si accorge che un altro MT ha dei dati da trasmettergli . Vengono supportati peridodi di slepp di diversa durata per permettere di soddisfare i requisiti di breve latenza o di basso consumo (tipicamente si richiede breve latenza per trasmissioni *time critical* come voce e video)

Lo standard definisce inoltre un secondo tipo di approccio per il controllo della potenza di trasmissione ad anello aperto sull'RCH (*Open loop Tansmit Power Control*, **TPC**):

- Ogni AP informa i MT circa la propria potenza di trasmissione ed indica a quale livello di potenza si aspetta di ricevere (questo vale per tutti i MT). Questo meccanismo viene usato quando i terminali si contendono l'accesso all'AP secondo lo schema Slotted Aloha su un canale ad accesso casuale, per garantire un basso ritardo di accesso, L'AP alloca un maggior numero di slot per questo canale nel MAC frame riducendo cosi la probabilità di collisioni.

Implementare lo standard con i chipset AR5414

Abbiamo visto come lo standard Hiperlan2 prevede una sola modalità di sleep, con la possibilità di configurare il TPC. Nella figura 5.3 riassume i relativi consumi.

A Mode:	Cont. Tx:	1100mA (typical)~1300mA (max)
	Cont. Rx:	250mA (typical)~270mA (max)
	Stand by:	280mA (typical)~290mA (max)
G Mode:	Cont. Tx:	730mA (typical)~780mA (max)
	Cont. Rx:	240mA (typical)~260mA (max)
	Stand by:	280mA (typical)~290mA (max)
B Mode:	Cont. Tx:	730mA (typical)~780mA (max)
	Cont. Rx:	200mA (typical)~220mA (max)
	Stand by:	230mA (typical)~240mA (max)
Power saving: 40mA (typical)		

Figura 5.3: Consumi del chipset AR5414

La figura 5.4 illustra cosa sono A mode, G mode e B mode

A Mode:
5.15~5.35 & 5.725~ 5.85 GHz for US
5.15~5.35 GHz for Japan
5.15~5.35 & 5.47~5.725 GHz for ETSI
5.725~5.85 GHz for China
4.94~4.989Ghz for US safety band
B/G Mode:
2400~2483.5 MHz (for US, Canada, EU, China and Japan)

Figura 5.4: Bande di frequenze secondo il modo

5.2.3 Costi

Il kit AR5414 comprende:

- Integra un amplificatore LNA
- Convertitori ADC-DAC
- Il blocco MAC Configuration Control and Memory
- Il Blocco PHY, dove lavora da 4.900 a 5.850 e 2.300 a 2.500 GHz

Con questa chipset nel mercato possiamo trovare queste schede:

- AR5006XS 802.11a/b/g CardBus Card
- AR5006XS 802.11a/b/g Mini PCI

Dove ognuno costa circa 60€

5.3 Confronto

Come abbiamo potuto osservare nella tabella 5.2 e nella figura 5.3, il consumo di potenza dei dispositivi compatibili con lo standard 802.11g è decisamente inferiore al consumo di potenza dei dispositivi compatibili con lo standard Hiperlan2/802.11a e questo conferma tra l'altro la diversa posizione dei due standard rispetto alle applicazioni possibili. D'altro canto i dispositivi hiperlan2 hanno un prezzo maggiore in comparazione con i dispositivi 802.11g, dovuto a che il mercato del hiperlan2 è più piccolo de quello dello standard 802.11 e quindi meno diffuso.

CONCLUSIONI

Lo sviluppo delle comunicazioni wireless, dai telefoni cellulari fino alle wireless LAN, è in continua crescita. Molte sono le proposte riguardo gli standard per tali comunicazioni ed ognuna di queste offre dei vantaggi e degli svantaggi. In generale, la scelta di utilizzare un dispositivo conforme ad uno standard piuttosto che ad un altro è correlata alla specifica applicazione che si vuole realizzare: in altre parole è necessario conoscere bene le caratteristiche dei protocolli di comunicazione wireless per capire quali applicazioni è possibile realizzare e quali no, oppure quali prestazioni ci possiamo aspettare da un protocollo o da un altro una volta stabilita l'applicazione.

Nella presente tesi ci siamo concentrati sullo studio approfondito degli standard 802.11 e Hiperlan2, in particolare riguardo il meccanismo di accesso al mezzo (MAC) trasmissivo wireless.

Nel Capitolo 2 e nel Capitolo 3 pertanto, ci siamo occupati di sintetizzare, per quanto possibile, le caratteristiche dei due standard, che possono essere così riassunte:

- IEEE 802.11

  è uno standard per la realizzazione di LAN wireless, sviluppato per estendere o addirittura sostituire LAN cablate poichè i dispositivi conformi possono contare su un raggio d'azione di circa 150-300 m e su un data rate lordo fino a 54Mbps (protocollo IEEE 802.11g); lo standard fornisce solo le definizioni del livello fisico e del metodo d'accesso al mezzo; è stato pensato per realizzare dispositivi con una batteria capace; attualmente sono attivi diversi gruppi all'interno dell'istituto IEEE per lo sviluppo di alcune varianti del protocollo, tra le quali segnaliamo IEEE 802.11a che opera nella banda U-NII 5 GHz e che permette ai dispositivi conformi di realizzare un data rate lordo di 54Mbps.

- Hiperlan2

  è uno standard come il 802.11 per la realizzazione di LAN wireless, ma ha delle tecniche per la gestione della qualità di servizio (cosa che non garantisce il 802.11) e su un data rate lordo fino a 54Mbps; anche lo standard fornisce solo le definizioni del livello fisico e del metodo

d'accesso al mezzo; è stato pensato per realizzare dispositivi con una batteria capace.

In seguito, nel Capitolo 4, ci siamo occupati di confrontare i metodi d'accesso al mezzo (MAC) dei due standard ed in particolare abbiamo affrontato le seguenti problematiche:

- Proprietà di creazione di reti efficienti, con particolare attenzione alla velocità di creazione delle reti e dei link tra i terminali ed infine alle metodologie implementate da entrambi i protocolli per la creazione ed il mantenimento delle reti.
- Proprietà delle topologie di rete realizzabili con i due protocolli, con particolare attenzione alla capacità di estensione delle singole celle base, alle capacità di connessione con altri tipi di rete, alle problematiche di routing dei messaggi ed indirizzamento dei dispositivi quando le topologie realizzate non consentano la connessione completa della rete.
- Proprietà dei link realizzati tra i dispositivi di una singola cella base, con particolare attenzione alle caratteristiche della sezione radio dei dispositivi ed al throughput realizzabile con i singoli link.
- Capacità di offrire un certo livello di Quality of Service (QoS).

Infine, nel Capitolo 5, abbiamo portato il confronto tra i due standard ad un livello più basso, contattando alcuni costruttori di dispositivi compatibili con lo standard 802.11, in particolar 802.11g, e di dispositivi compatibili con lo standard Hiperlan2. Un problema sempre più sentito dagli utenti, così come dai costruttori stessi, è il **consumo di potenza** dei dispositivi, proprio perchè, nella maggior parte dei casi, la comunicazione wireless è implementata su dispositivi mobili e quindi spesso alimentati a batteria. Ci siamo dunque occupati di confrontare innanzitutto i metodi offerti dagli standard 802.11 e Hiperlan2 per ottimizzare il consumo di potenza dei terminali, e, successivamente, abbiamo osservato le implementazioni di tali metodi nei chip di diversi costruttori, andando a confrontarne le prestazioni in alcuni semplici scenari d'uso. Infine, abbiamo cercato di dare un'idea del prezzo dei singoli chipset, sia per Hiperlan2 che per 802.11.

BIBLIOGRAFIA

[1] International Standard ISO/IEC 8802-11: 1999(E) ANSI/IEEE Std 802.11, 1999 Edition, 1999.

[2] International Standard ISO/IEC 8802-11: 1997(E) ANSI/IEEE Std 802.11, 1997 Edition, 1997.

[3] HiperLAN/2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band, 1999.

[4] ETSI TS 101 475, Broadband Radio Access Networks (BRAN);HIPERLAN Type 2; Physical (PHY) layer, 2002.

[5] ETSI TS 101 761-3, Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) Layer; Part 3: Profile for Business Environment, 2006.

[6] ETSI TS 101 761-4, Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) Layer; Part 4: Extension for Home Environment, 2006.

[7] ETSI TS 101 763-1, Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Cell based Convergence Layer Part 1: Common Part, 2004.

GLOSSARIO

IEEE802.11

ACK *Acknowledgment.*

AID *Association identifier*. Identificativo dato dall'Access Point alle stazioni autenticate ed associate.

AP *Access Point*. Una stazione particolare che, oltre ad essere un nodo della rete, si occupa di gestire il traffico e, come opzione, anche l'accesso al mezzo, delle stazioni ad essa associate.

Associazione Servizio usato per effettuare una mappa Access Point/Stazioni e permettere alle stazioni di usufruire dei servizi del DS. Vedi anche DS.

ATIM *Ad-Hoc Traffic Indication Map*. Mappa virtuale del traffico bufferizzato in una certa stazione e destinato alle stazioni in Power Save, utilizzato nelle configurazione topologica Ad-Hoc.

Autenticazione Servizio usato per stabilire l'identità di una stazione.

Beacon Pacchetto speciale trasmesso periodicamente dall' AP, oppure da una stazione scelta con un algoritmo distribuito se la rete ha topologia ad-hoc, usato per la sincronizzazione e la trasmissione di informazioni importanti.

BSS *Basic Service Set*. Cella base dell'architettura IEEE 802.11.

BSSID *BSS Identification.*

CCA *Clear Channel Assessment*.

CF *Contention Free*. Modalità d'accesso al mezzo controllata, ovvero le stazioni non devono contendere l'accesso al mezzo trasmissivo.

CFP *Contention-free period*. Intervallo di tempo durante il quale l'accesso al mezzo delle stazioni che ne hanno fatto espressamente richiesta è controllato dal PC. Vedi anche PC.

CP *Contention Period*. Modalità d'accesso al mezzo distribuita, ovvero le stazioni devono contendere l'accesso al mezzo trasmissivo.

CRC *Cyclic Redundancy Check*. Metodo per il controllo degli errori nei dati trasmessi attraverso un collegamento.

CTS *Clear To Send*. Pacchetto speciale usato insieme al pacchetto RTS, per ridurre la possibilità di collisioni dovute a nodi nascosti. Vedi anche RTS.

CW *Contention Window*. Parametro usato come unità di misura temporale del Random Backoff.

DA *Destination Address.*

DBPSK *Differential Binary Phase Shift Keying.*

DCF *Distributed Coordination Function*. Indica il metodo d'accesso al mezzo applicato durante il CP.

DIFS *distributed* (coordination function) *interframe space.*

DQPSK *differential quadrature phase shift keying.*

DS *distribution system.* Entità, non specificata dallo standard IEEE 802.11, che si occupa della connessione tra le diverse BSS e consente la creazione di una ESS. Vedi anche ESS.

DSM *distribution system medium*. Mezzo trasmissivo con il quale opera il DS.

DSS *distribution system service*. Servizio che dev'essere fornito (implementato) nel DS. I servizi DS sono: Associazione, Riassociazione, Disassociazione, Distribuzione, Integrazione.

DSSS *direct sequence spread spectrum.*

DTIM *delivery traffic indication message*. Indicazione del traffico broadcast per le stazioni in Power Save.

EIFS *extended interframe space.*

EIRP *equivalent isotropically radiated power.*

ESS *extended service set*. Elemento dell'architettura IEEE 802.11 composto dal'interconnessione di diverse BSS attraverso un DS.

FCS *frame check sequence*. E' il campo che, all'interno dei frame IEEE 802.11, contiene il codice CRC per il frame stesso.

FHSS *frequency-hopping spread spectrum.*

GFSK *Gaussian frequency shift keying.*

IBSS *independent basic service set.* Indica una BSS in cui non è presente un access point, ovvero una BSS con topologia ad-hoc.

IFS *interframe space.*

IR *infrared.*

ISM *industrial, scientific, and medical.*

MAC *medium access control.*

MMPDU *MAC management protocol data unit.*

MPDU *MAC protocol data unit.*

MSDU *MAC service data unit.*

NAV *network allocation vector*. Contatore impementato in ciascuna stazione che tiene traccia della durata di una eventuale trasmissione in corso sul mezzo, usato dalla stazione stessa per ritardare il tentativo di accesso al mezzo fino alla fine della trasmissione in atto.

PC *point coordinator*. Entità, di solito localizzata nell'AP, che si occupa di gestire l'accesso al mezzo trasmissivo delle stazioni associate durante il CFP.

PCF *point coordination function*. Indica il metodo d'accesso al mezzo applicato durante il CFP.

PDU *protocol data unit*.

PHY *physical (layer).*

PIFS *point* (coordination function) *interframe space*.

PLCP *physical layer convergence protocol*.

PMD *physical medium dependent.*

PN *pseudo-noise* (code sequence).

PS *power save* (mode).

RA *receiver address.*

RF *radio frequency*.

RSSI *received signal strength indication.*

RTS *request to send*. Pacchetto speciale usato insieme al pacchetto CTS, per ridurre la possibilità di collisioni dovute a nodi nascosti. Vedi anche CTS.

SA *source address.*

SDU *service data unit.*

SIFS *short interframe space.*

SS *station service*. Servizio che dev'essere offerto (implementato) all'interno di una stazione. I servizi SS sono: Autenticazione, Deautenticazione, Privacy, Trasporto dei pacchetti.

SSID *service set identifier.*

STA *station.*

TA *transmitter address.*

TBTT *target beacon transmission time*. Intervallo di tempo nominale tra la trasmissione di due Beacon.

TIM *traffic indication map*. Mappa virtuale del traffico bufferizzato dall'AP e destinato alle stazioni in Power Save.

TSF *timing synchronization function.*

TU *time unit.*

WEP *wired equivalent privacy*. L'algoritmo crittografico opzionale specificato dallo standard IEEE 802.11 per offrire un certo livello di riservatezza dei dati trasmessi.

WM *wireless medium.*

HIPERLAN2

ACF *Association Control Function*

ACH *Access feedback Channel*

AGC *Automatic Gain Control*

AP *Access Point*

ARQ *Automatic Repeat Request*

ASCH *ASsociation control CHannel*

BCH *Broadcast Channel*

CA *Collision Avoidance*

CL *Convergence Layer*

C-SAP *Control Service Access Point*

CSMA *Carrier-Sense Multiple Access*

DCCH *Dedicated Control CHannel*

DFS *Dynamic Frequency Selection*

DLC *Data Link Control*

DLCC *DLC Connection*

DUC *DLC User Connection*

DCC *DLC user Connection Control*

EC *Error Control*

FCH *Frame CHannel*

LCCH *Link Control CHannel*

LCH *Long transport CHannel*

MAC *Medium Access Control*

MAC-ID *MAC identifier*

MT *Mobile Terminal*

PDU *Protocol Data Unit*

PHY *PHYsical layer*

RCH *Random CHannel*

RLC *Radio Link Control*

RRC *Radio Resource Control*

SAP *Service Access Point*

SBCH *Slow Broadcast CHannel*

SCH *Short transport Channel*

SDU *Service Data Unit*

TDD *Time-Division Duplex*

TDMA *Time-Division Multiple Access*

U-SAP *User Service Access Point*

UDCH User Data CHannel

APPENDICE

1. Caratteristiche Tecniche del chipset BCM94318

KEY FEATURES

- Industry's smallest IEEE 802.11b/g solution makes wireless LAN connectivity practical for pocket-sized electronic devices.
- Extreme integration includes radio, baseband, MAC, and all other radio frequency (RF) components found on a typical wireless LAN board—making small mobile devices easier, less expensive and faster to manufacture.
- Innovative power management reduces power consumption by up to 97% in standby mode, providing greatly extended battery life for mobile devices.
- Cost-effective architecture with single-sided, all-CMOS design eliminates over 100 components, providing more affordable wireless connectivity for consumer electronics.
- High-performance features standard across the AirForce product line:
  - OneDriver™
  - SmartRadio™
  - WPA, WPA2
  - Cisco® Compatible Extensions (CCX)
  - AES in hardware
  - WMM for advanced Quality of Service
  - Xpress™ technology
  - 125 High Speed Mode™
- Reference designs include Secure Digital I/O, MiniPCI, CardBus, and Compact Flash.

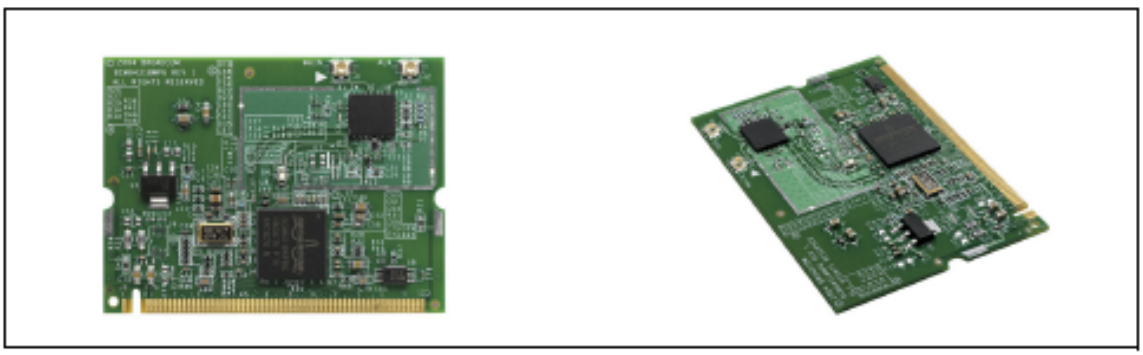
POWER MANAGEMENT

- Innovative power management techniques improve battery life by creating deep sleep state when device is in stand-by mode.
- Designed for low CPU utilization to ensure CPU resources are available for handheld applications.

AIRFORCE FEATURE SET

- SmartRadio: Continuous calibration reduces test time and improves manufacturability.
- Xpress Technology: Standards-based frame bursting improves overall network efficiency.
- 125 High Speed Mode: Standards-plus performance enhancement delivers best real-world performance when both client and AP support High Speed Mode.
- Security:
  - WPA- and WPA2-CERTIFIED for powerful encryption and authentication
  - AES in hardware for faster data encryption and 802.11i compatibility
  - Cisco Compatible Extensions (CCX, CCX 2.0) certified
  - SecureEZSetup™ for simple Wi-Fi setup and WPA security configuration
- Worldwide support: Global products supported with worldwide homologated design.
- OneDriver: Single driver across all platforms—802.11a/b/g—simplifies driver update process and improves customer satisfaction.

BCM94318 MP Reference Design



2. Caratteristiche Tecniche del chipset AR5414

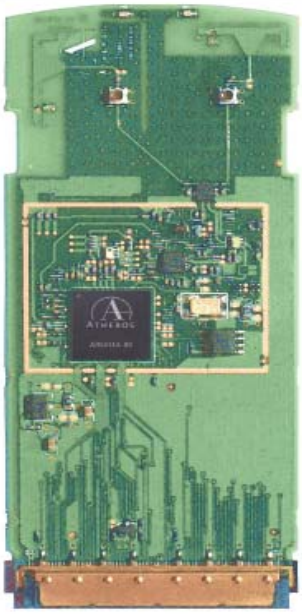
AR5006XS Solution Highlights

- Highly integrated single chip CMOS solution with multiprotocol MAC/baseband processor and 2.4/5 GHz radio
- Uses digital CMOS technology exclusively, minimizing power consumption and cost while maximizing reliability
- Support for IEEE 802.11a, 802.11b, 802.11g
- 802.11e standard compatible bursting
- Super AG™ mode delivers up to 108 Mbps data link rate with typical end user throughput exceeding 60 Mbps
- Super AG utilizes Adaptive Radio to automatically identify clear channels for maximum throughput and standards compatible operation
- Wireless Multimedia Quality of Service support (QoS)
- Hardware encryption for the Wi-Fi Protected Access (WPA) and IEEE 802.11i security specifications, provides Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP) and Wired Equivalent Privacy (WEP) without performance degradation
- Extended tuning range (2.300-2.500 & 4.900-5.850 GHz) for worldwide use
- Dynamic Frequency Selection/Transmit Power Control (DFS/TPC) for international operation
- Support for draft IEEE 802.11e, h, i and j standards
- Atheros XR™ eXtended Range technology to give Wi-Fi products twice the range of existing designs
- Power-saving design improvements reduce system power consumption by 98%

AR5414 Single-Chip CMOS MAC/Baseband/Radio

- Support for IEEE 802.11a, 802.11b, 802.11g
- Operates from 4.900 to 5.850 and 2.300 to 2.500 GHz
- Advanced wideband receiver with best path sequencer for better range and multipath resistance than conventional equalizer-based designs
- Integrated low-noise amplifier (LNA)
- External PA and/or LNA can be used for special applications
- Eliminates all IF filters and most RF filters; no external voltage-controlled oscillators (VCOs) or surface acoustic wave (SAW) filters needed
- Enhanced transmit and receive chains
- Super AG mode includes dynamic 108 Mbps capability, real-time hardware data compression, Fast Frames and standards-compliant bursting
- Atheros XR eXtended Range technology to give Wi-Fi products twice the range of existing designs
- No external FLASH or RAM memory needed
- PCI 2.3 and PC Card 7.1 host interfaces with DMA support
- Integrated analog-to-digital and digital-to-analog converters
- High speed UART with DMA supports data rates up to 1 Mbps
- Serial EEPROM, LEDs, GPIOs peripheral interfaces
- Low power operational and sleep modes

AR5006XS 802.11a/b/g CardBus Card



- Windows® drivers for Windows XP, Windows 2000, Windows ME, Windows 98 SE and Windows NT 4.0
- A single driver and firmware code base supports all Atheros chipsets, and provides both backward and forward compatibility with Atheros previous and next-generation multi-standard designs.
- Integrated WPA suppticant supports Windows XP, Windows 2000, Windows ME, Windows 98 SE and Windows NT 4.0
- Client utility supports configuration profiles, current link status, statistics and diagnostics

AR5006XS 802.11a/b/g Mini PCI