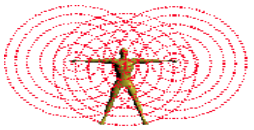


Protocollo 802.11

Ing. Cristian Randieri

Università degli Studi di Catania

Istituto Nazionale di Fisica Nucleare (INFN)

Introduzione

- Una 802.11 LAN è basata su una architettura cellulare in cui l'area in cui deve essere distribuito il servizio viene suddivisa in celle proprio come accade nei sistemi di distribuzione per servizi di telefonia GSM.

- Ciascuna cella (chiamata ***Basic Service Set*** o *BSS* nella nomenclatura) è controllata da una stazione base denominata ***Access Point*** o più semplicemente *AP*.

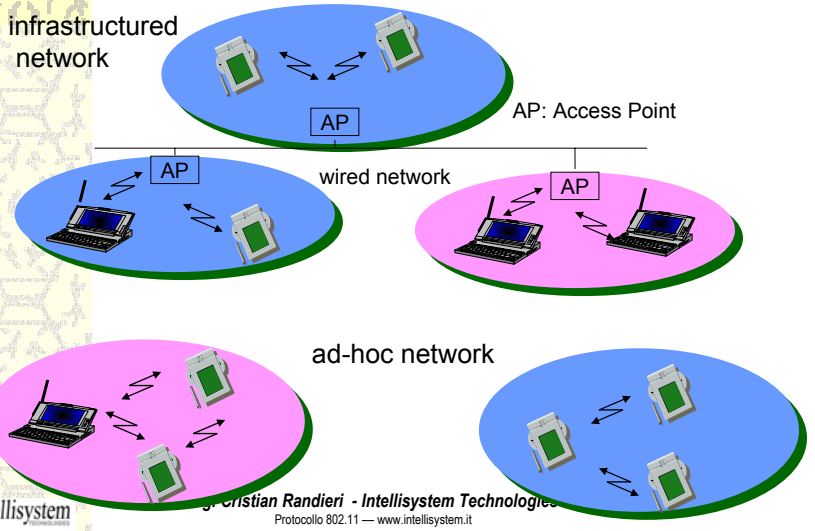
Access Point

- Sebbene una wireless LAN possa essere formata da una singola cella, con un singolo ***Access Point,*** la maggior parte delle installazioni sarà formata da una molteplicità di celle dove i singoli Access Point sono interconnessi attraverso un qualche tipo di rete di distribuzione (che normalmente viene definita ***Distribution System* o *DS***);

Ad-Hoc network

- A volte per motivi di costi, di logistica ecc.. non è possibile usufruire di un'infrastruttura.
- Pertanto esiste un modo di funzionamento privo di Access Point denominato ***ad-Hoc*** che permette il collegamento diretto di calcolatori.
- Tale soluzione è adottata negli ambienti militari, ambienti ad alto rischio, nella home automation.

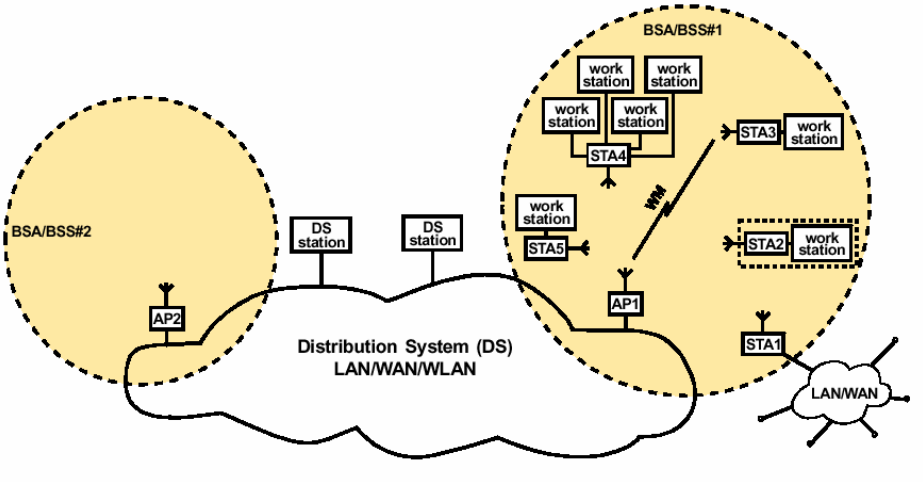
Tipologia ad Hoc



Infrastuctured WLan

- La rete di distribuzione è normalmente costituita da una dorsale Ethernet e in certi casi è wireless essa stessa.
- Il complesso delle diverse wireless LAN interconnesse, comprendenti differenti celle, i relativi Access Point e il sistema di distribuzione, viene visto come una singola rete 802 dai livelli superiori del modello OSI ed è noto nello standard come ***Extended Service Set (ESS).***

Schema di una tipica rete LAN basata sul protocollo 802.11

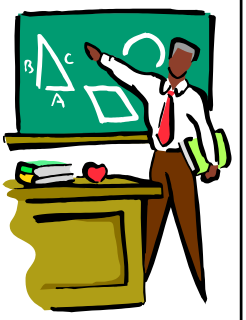


Concetto di Portal

- 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. Questo concetto rappresenta una descrizione astratta di una parte delle funzionalità di un ***translation 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.

Descrizione degli strati dell'IEEE 802.11

Come tutti gli altri protocolli 802.x, anche il protocollo 802.11 prende in considerazione i due livelli di MAC e livello fisico.



Lo standard attualmente disponibile definisce un singolo livello MAC che può interagire con i seguenti tre livelli fisici, operanti a velocità variabili tra 1 e 3 Mbit/s:

- ***Frequency Hopping Spread Spectrum (FHSS) nella banda ISM 2,4 GHz.***
- ***Direct Sequence Spread Spectrum (DSSS) nella banda ISM 2,4 GHz.***
- ***Trasmissione infrarossa***

Descrizione degli strati dell'IEEE 802.11

- Oltre alle funzionalità standard usualmente fornite dai livelli MAC dei protocolli 802.x, il MAC 802.11 supporta delle funzionalità aggiuntive, tipiche dei livelli superiori dello stack protocollare, come gestione della frammentazione, la ritrasmissione dei pacchetti e gestione dell'acknowledgements.
- Il livello di MAC definisce due differenti metodi di accesso che verranno di seguito descritti:
  - *Distributed Coordination Function e Point*
  - *Coordination Function.*

802.2			Data Link Layer
802.11 MAC			
FH	DS	IR	PHY Layer

Livello Fisico

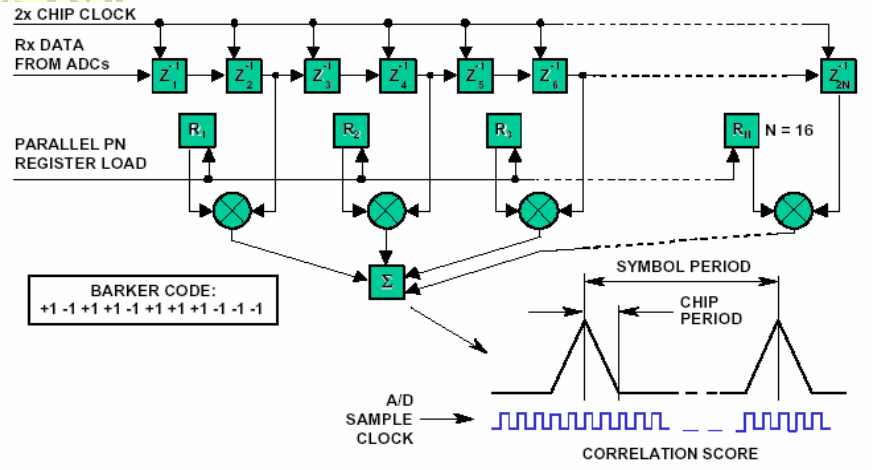
- Come detto in precedenza lo strato fisico include due tecnologie basate su RF la Direct Sequence Spread Spectrum (DSSS) e la Frequency Hpped Spread Spectrum (FHSS).
- Entrambe sono state definite conformemente alla FCC 15.247 per operare nella banda ISM 2.4 GHz.

Region	Allocated Spectrum
US	2.4000 – 2.4835 GHz
Europe	2.4000 – 2.4835 GHz
Japan	2.471 - 2.497 GHz
France	2.4465 - 2.4835 GHz
Spain	2.445 - 2.475 GHz

Livello Fisico

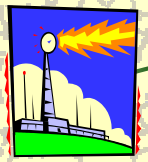
- Entrambe le FHSS e DSSS supportano trasmissioni a 1 e 2 Mbit/s.
- Le trasmissioni a 11 Mbyte/s sono correntemente supportate dallo standard DSSS.
- I sistemi DSSS sono simili a quelli adoperati per i satelliti GPS e per alcuni tipi di telefoni cellulari.
- Ogni bit di informazione viene combinato mediante una funzione XOR con una sequenza numerica Pseudo Random (PN).
- Il risultato è uno stream digitale modulato ad alta velocità mediante tecniche Differential Phase Shift Keying (DPSK).

Matched Filter Correlator Used for Reception of DSSS Signal



Livello Fisico

- Quando viene ricevuto un segnale di tipo DSSS viene adoperato un matched filter al fine di rimuovere la sequenza PN al fine di ricostruire lo stream originale.
- L'alto troughput di 5.5 e 11 Mbit/s implica che i ricevitori DSSS debbano adoperare differenti codici PN associati ad altrettanti banchi di filtri correlatori.
- Il metodo di modulazione ad alta velocità adoperato prende il nome di Complimentary Code Keying (CCK).



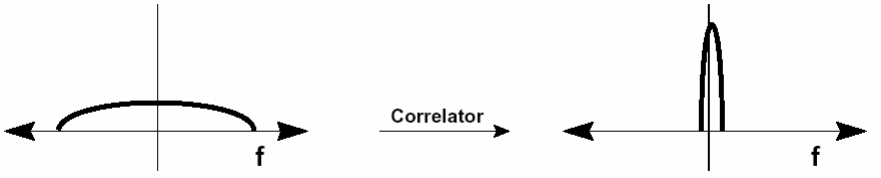
Segnale trasmesso

- Modifica dello spettro usando codici PN per generare il segnale spread spectrum.

•LA sequenza PN provoca un'allargamento (spread) della banda passante del segnale risultante (da cui il termine spread spectrum) con una conseguente riduzione del picco di potenza.

Segnale ricevuto

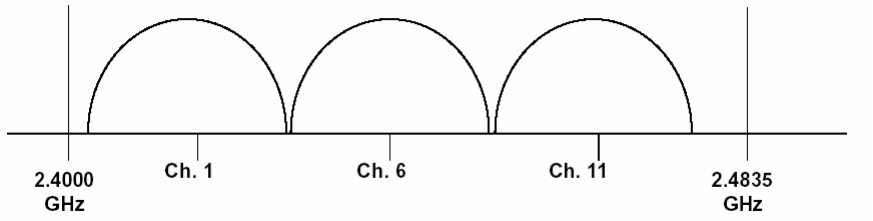
- Il segnale ricevuto è correlato alla sequenza PN al fine di ricostruire i dati originari e di filtrare eventuali interferenze.



Canali DSSS non sovrapposti all'interno della banda ISN

Diversamente dal data rate dei dati che è di 1, 2, 5.5, o 11 Mbit/s, la larghezza di banda del canale per i sistemi DSSS è di circa 20 MHz.

Di conseguenza la banda ISM verrà distribuita lungo tre canali non sovrapposti (not overlapping channels).

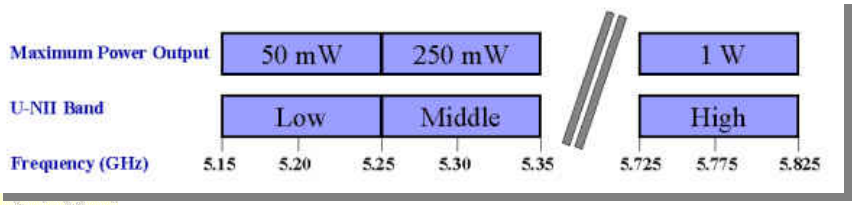


Standard IEEE 802.11a

- Lo standard sino adesso discusso è definito dalla IEEE come standard 802.11b.
- Lo standard 802.11a rappresenta la prossima generazione delle tecnologie wireless.
- Permetterà di raggiungere velocità di 54 Mbit/s lungo tutto il raggio di copertura del segnale.
- Sarà facilmente interfacciabile con lo standard 802.11b.

Livello fisico 802.11a

- Viene adoperata una banda passante di 300 MHz all'interno della banda dei 5 GHz U-NII (Unlicensed National Information Infrastructure band).
- La banda dei 300 MHz viene suddivisa in tre distinti domini da 100 MHz ciascuno dei quali ha una potenza d'uscita diversa.



Livello fisico 802.11a

- A causa del livello alto di potenza in uscita la band più alta sarà utilizzata nei prodotti building-to-building.
- Le altre due bande sono più adatte ai dispositivi che adoperano antenne integrate.

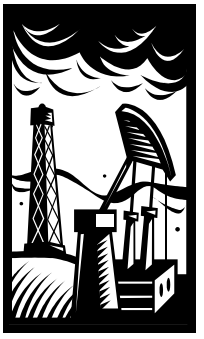
Livello fisico 802.11a

Una delle prime problematiche che ci si pone riguarda la gestione della banda 5 GHz nelle varie parti del mondo.

- Negli ***USA*** l'FCC ha allocato le tre bande tutte all'interno della U-NII.
- In ***Europa*** solamente le bande basse e e medie sono libere. Di conseguenza è in atto una collaborazione tra l' IEEE e l'ETSI (European Telecomunications Standars Institute) al fine di allocare la terza banda.
- In ***Giappone*** solamente la banda bassa è libera.

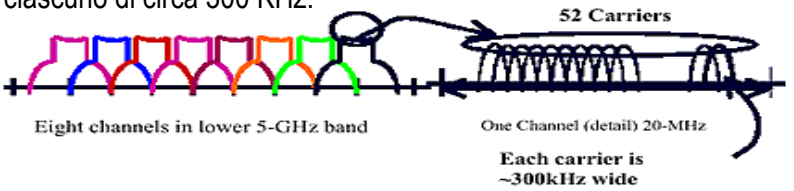
Un confronto

- Nel caso della 802.11b si lavora nei 2.4 GHz della banda ISM (Industrial Scientific & Medical band).
- Questa banda è molto popolata e offre 83 MHz di spettro per tutto il traffico wireless, incluso quello dei telefoni cordless, le trasmissioni building-to-building e dei microonde.
- A confronto la banda dei 300 MHz all'interno della banda U-NII oltre ad avere una banda più larga è scarsamente popolata.



Modulazione OFDM

- Lo standard 802.11a adopera una modulazione di tipo OFDM (Orthogonal Frequency Division Multiplexing) che mediante un nuovo schema di codifica migliora le prestazioni dello spread spectrum in termini di disponibilità dei canali e velocità di trasmissione.
- Adoperando la OFDM si definiscono 8 canali non sovrapposti da 20 MHz all'interno delle 2 lower band.
- Ciascuno di questi canali è a sua volta suddiviso in 52 subcarriers ciascuno di circa 300 KHz.



Subcarriers

- La trasmissione dati relativa ai 52 subcarriers avviene in parallelo.
- I dispositivi di ricezione pertanto saranno capaci di processare parallelamente altrettanti canali, ciascuno dei quali rappresenta una frazione dell'informazione trasmessa.

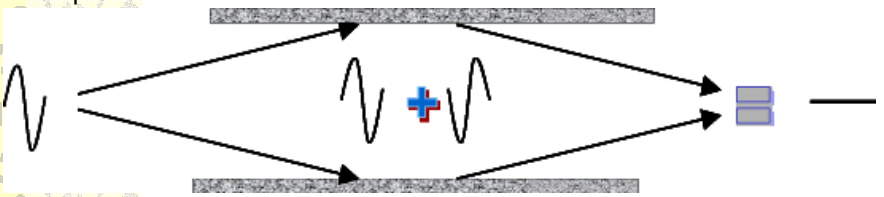
- All'interno della 802.11a è definito un meccanismo per controllare e prevenire la perdita dei dati (meccanismo non presente nella 802.11b).
- La tecnica adoperata è la FEC (Forward Error Correction).

FEC (Forward Error Correction)

- Consiste nell'inviare una copia secondaria assieme all'informazione primaria.
- Se parte dell'informazione primaria è danneggiata mediante algoritmi sofisticati è possibile recuperare l'informazione corretta a partire dalla copia secondaria. In questo modo si elimina la ritrasmissione dell'informazione.
- Ovviamente ciò implica un overhead che ha scarso impatto sulle performance grazie all'elevata velocità di trasmissione.
- Un altro meccanismo per garantire l'integrità della trasmissione è il Delay Spread.

Delay Spread

- Quando un segnale radio lascia l'antenna trasmittente, e quindi viene irradiato, può capitare che incontri una superficie riflettente che lo riflette all'antenna stessa causando il cosiddetto fenomeno di riflessione che di fatto provoca una degradazione delle prestazioni.

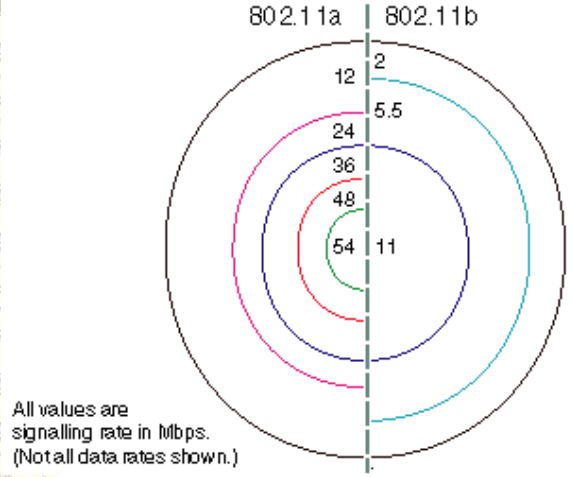


- Mediante il Delay Spread viene introdotto un delay tra due trasmissioni successive, in questo modo vengono ridotte le interferenze multipath.

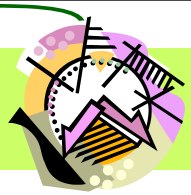
Data Rates & Ranges

- I dispositivi che utilizzano la 802.11a supporteranno velocità di 6, 12, e 24 Bbit/s.
- Velocità opzionali potranno raggiungere i 54 Mbit/s e dovranno comunque includere velocità di 48, 36, 18, e 9 Mbit/s.
- Queste differenze sono il risultato di differenti tecniche di modulazione.
- In particolare per arrivare ai 54 Mbit/s si adopererà un meccanismo chiamato 64QUAM (64-level Quadrature Amplitude Modulation) che provvederà ad allocare la massima quantità d'informazione all'interno di ogni subcarrier.

Differenze tra 802.11a e 802.11b



Hiperlan/2



- L'Hiperlan/2 è una specifica wireless sviluppata dall'ETSI che presenta alcune similarità a livello fisico con la 802.11a.
- Adopera la tecnologia OFDM e lavora nella banda dei 5 GHz.
- Come detto in precedenza la banda 5 GHz U-NII non è certificata in Europa per superare questa limitazione si è proposto di inserire una specifica che mediante le tecniche di DCS (***Dynamic Channel Selection***) e TCP (***Trasmit Power Control***) permetterà ai client di ricercare i canali più liberi e di usare la minima potenza d'uscita nel caso sia possibile avere interferenze.

Considerazioni sullo strato MAC

- Entrambi gli standard 8021.11a e 802.11b adopereranno lo stesso Media Acces Control (MAC) basato su CSMA-CA.

- Le differenze sono per l'Hiperlan/2 che utilizza il TDMA (Time Division Multiple Access).

Livello MAC 802.x

- Il livello MAC definisce come metodo di accesso il **Distributed Coordination Function.**
- Questo è un meccanismo di tipo **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** che lavora in questo modo:
  - una stazione che vuole trasmettere, ascolta il mezzo;
  - se il mezzo è occupato, allora sposta la trasmissione ad un altro momento mentre, se il mezzo è libero, trasmette subito.
- Questo tipo di protocollo è abbastanza efficiente quando il mezzo non è molto utilizzato, permettendo alle stazioni di trasmettere con piccoli ritardi; nonostante ciò, la probabilità che due o più stazioni decidano di trasmettere contemporaneamente, generando una collisione, non è nulla.

Livello MAC 802.x

- Queste collisioni devono essere identificate in modo tale che lo strato MAC possa ritrasmettere il pacchetto da solo senza nessun intervento da parte degli strati superiori, cosa che evita ritardi inutili.
- Mentre questi meccanismi di Collision Detection sono facilmente implementabili per reti cablate, per reti wireless non possono essere usati per due motivi:

Limitazioni del livello MAC 802.x

1. L'implementazione di un meccanismo di collision detection richiederebbe la progettazione di ricetrasmettitori full duplex, capaci cioè di trasmettere e di ricevere contemporaneamente, facendo lievitare i costi di produzione.
2. In un ambiente wireless, non si può fare l'ipotesi che tutte le stazioni si ascoltino tra loro (cosa che invece è richiesta nel meccanismo di collision detection), perché anche se il trasmettitore sente libero il mezzo intorno a sé, non è detto che intorno al ricevitore il mezzo sia altrettanto libero.

Collision Avoidance

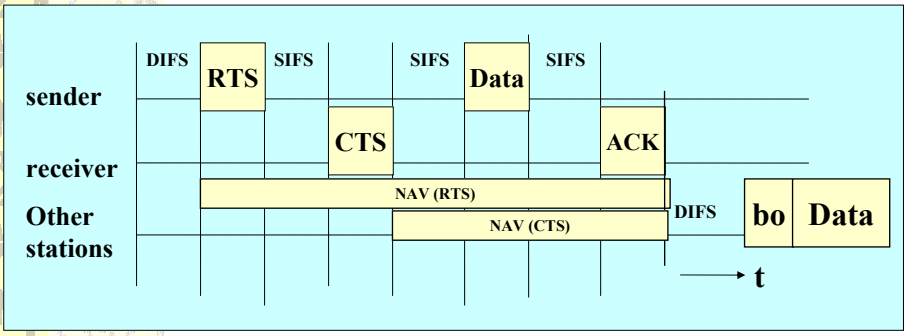
Per prevenire questi problemi, lo standard usa un meccanismo di **Collision Avoidance:**

- Una stazione che vuole trasmettere ascolta il mezzo. Se il mezzo è occupato, allora sposta la trasmissione ad un altro momento. Se in un certo istante di tempo (chiamato **Distributed Inter Frame Space (DIFS))** il mezzo è libero, la stazione può trasmettere.
- La stazione destinataria controlla il CRC del pacchetto ricevuto e manda un ACK. La ricezione dell'ACK indica che non è avvenuta nessuna collisione in trasmissione.
- Se il mittente non riceve l'ACK allora ritrasmette il frammento fino a quando non riceve l'ACK o fino a quando non ha esaurito i tentativi a sua disposizione.

Virtual Carrier Sense

- Per ridurre la probabilità che due stazioni collidano, lo standard definisce un meccanismo di ***Virtual Carrier Sense***.
- La stazione che vuole trasmettere, prima invia un piccolo pacchetto broadcast, chiamato ***RTS (Request To Send),*** che include informazioni sulla sorgente, sulla destinazione e sulla durata della transazione seguente (ad esempio la durata della trasmissione del pacchetto e dell'ACK conseguente); la stazione che deve ricevere risponde (se il mezzo è libero) con un pacchetto broadcast di controllo chiamato ***CTS (Clear To Send)*** che include la stessa informazione circa la durata della trasmissione.
- Tutte le stazioni che ricevono i pacchetti RTS e CTS modificano un indicatore Virtual Carrier Sense (chiamato Network ***Allocation Vector (NAV)***) per la durata indicata ed utilizzano questa informazione insieme con il Phisical Carrier Sense al momento in cui vanno a effettuare la rilevazione di occupazione del mezzo.

RTS/CTS

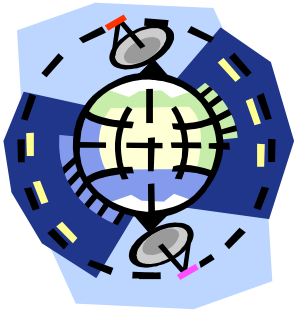


Virtual Carrier Sense

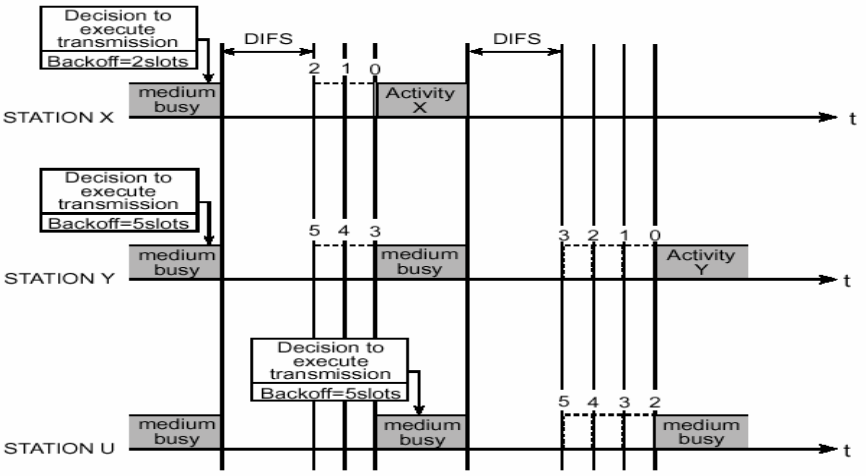
- Questo meccanismo riduce la probabilità di collisione nell'area del ricevitore, che è nascosta al trasmettitore, perché la stazione ascolta il CTS e riserva il mezzo fino alla fine della trasmissione.
- L'informazione di durata nel RTS protegge anche l'area del trasmettitore dalle collisioni che possono avvenire durante l'ACK da parte di quelle stazioni che sono fuori dall'area di visibilità della stazione che deve fornire l'acknowledge. .
- È anche opportuno notare che tale meccanismo, vista la breve durata delle frames RTS e CTS, riduce l'overhead delle collisioni, poiché queste sono identificate molto più velocemente rispetto all'uso di pacchetti di dimensione standard. Questo è vero se il pacchetto dati è significativamente maggiore rispetto all'RTS.

Virtual Carrier Sense

- Per questo motivo lo standard prevede una variante in cui se il pacchetto è breve può essere ritrasmesso senza la transazione RTS/CTS.
- Tutto ciò è controllato in ogni stazione da un parametro detto *RTS Threshold*.



Transazione tra due stazioni A e B con relativo settaggio del NAV nelle stazioni vicine



Acknowledgment a livello di MAC

- Il livello di MAC realizza il rilevamento della collisione aspettando la ricezione di un acknowledge per ogni frammento trasmesso.
- I pacchetti che hanno più di una destinazione, come i pacchetti multicast, non sono soggetti al meccanismo di acknowledge.

Fragmentation e Reassembly

Tipicamente i protocolli per reti locali utilizzano pacchetti aventi dimensioni di diverse centinaia di bytes. Ci sono però molte ragioni che spingono all'utilizzo di pacchetti di dimensioni minori in un contesto wireless LAN:

- A causa della elevata Bit Error Rate di un collegamento radio, la probabilità che un pacchetto sia corrotto durante la fase di trasmissione aumenta all'aumentare della dimensione del pacchetto.
- Nel caso in cui un pacchetto ricevuto debba essere ritrasmesso, l'overhead introdotto dal processo di trasmissione decresce con la dimensione del pacchetto.
- In un sistema Frequency Hopping non è garantita la continuità del mezzo trasmissivo a causa dei salti di frequenza (nel nostro caso questi salti avvengono ogni 20 ms.). Riducendo la dimensione del pacchetto diminuisce la probabilità che la trasmissione sia posticipata dopo il tempo di pausa (dwell time).

Fragmentation e Reassembly

- Di conseguenza è impensabile introdurre un nuovo protocollo che non possa trattare pacchetti di dimensione di 1518 bytes come quelli utilizzati nell'Ethernet, così l'organismo di standardizzazione ha deciso di aggiungere un semplice meccanismo di frammentazione e riassemblaggio al livello di MAC.
- Il meccanismo è costituito da un semplice algoritmo Send-and-Wait che non consente ad una stazione di trasmettere un nuovo frammento finché non sia verificata una delle seguenti situazioni:
  - *Ricezione di un ACK per il frammento precedentemente trasmesso.*
  - *Decide che il frammento è stato ritrasmesso troppe volte ed elimina tutto il frame.*

Intellisystem
Ing. Cristian Randieri - Intellisystem Technologies
Protocollo 802.11 — www.intellisystem.it

Fragmentation e Reassembly

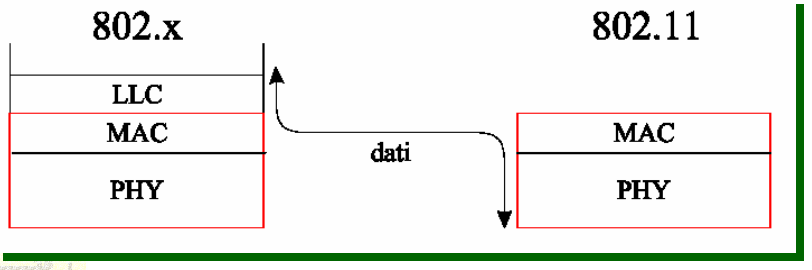
Bisogna notare che lo standard permette alla stazione di trasmettere a un differente indirizzo tra la ritrasmissione di un dato frammento.

Questo è particolarmente utile quando un AP ha parecchi pacchetti arretrati riferiti a differenti destinazioni e uno di questi non risponde.

Nel caso che comunque si verifichi una collisione, allora si utilizza l'algoritmo di **Exponential Backoff**, già utilizzato in Ethernet.

Osservazioni

- È da notare esplicitamente che allo strato MAC 802.11 non viene passata una frame del livello LLC ad esso superiore, bensì una frame 802.x "strappata" al livello PHY 802.x.

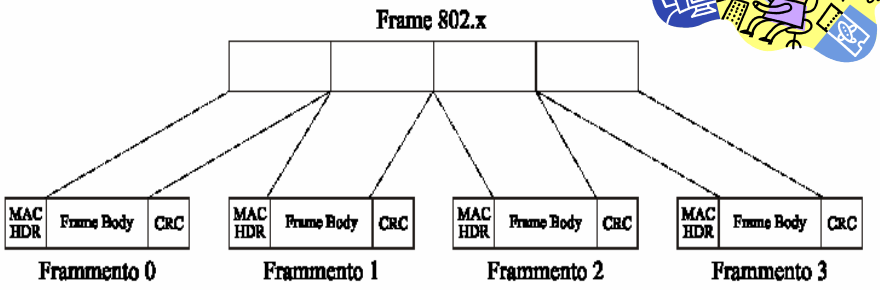


Osservazioni

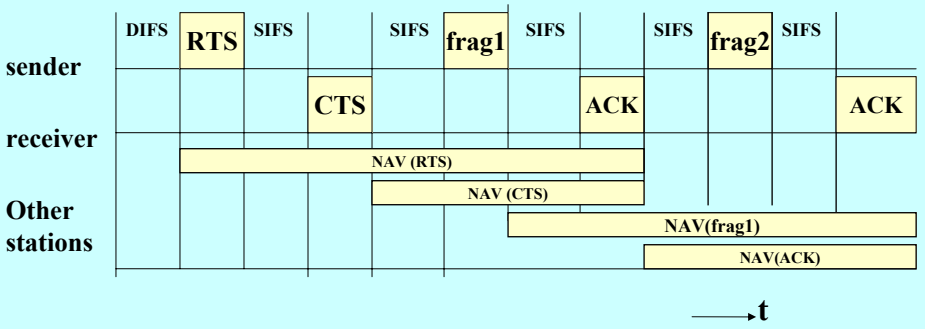
- Tale frame è frammentata ed ogni frammento così ottenuto è completato con un header ed un trailer, creando così delle “microframes” che verranno poi passate al livello PHY 802.11 per essere trasmesse.

- Questo porta a concludere che lo standard 802.11 non può esistere senza gli standard 802.x e che, inoltre, non è collocabile al di sotto di essi, bensì opera su un livello “parallelo”.

Diagramma che mostra una frame (di livello 802.x) da inviare, divisa in vari frammenti dal livello MAC.

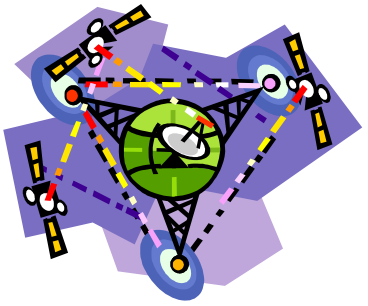


Fragmentation



Inter Frame Spaces

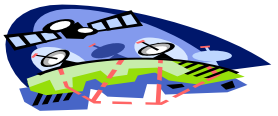
Lo standard definisce quattro tipi di spazi tra i frame (Inter Frame Spaces), che sono utilizzati per fornire differenti priorità:



- ***SIFS – Short Inter Frame Space*;**
- ***PIFS – Point Coordination IF;***
- ***DIFS – Distributed IFS*;**
- ***EIFS – Extended IFS*.**

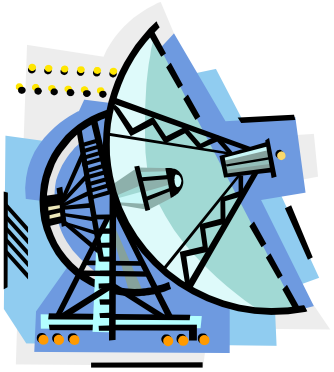
SIFS – Short Inter Frame Space

- E' utilizzato per separare trasmissioni che appartengono ad un singolo dialogo (Fragment-Ack) ed è il più piccolo spazio tra i frame possibile.
- C'è sempre al più una stazione che trasmette ad un dato istante di tempo, prendendosi dunque la priorità sulle altre.
- Questo valore è fissato per il livello fisico ed è calcolato in modo tale che la stazione trasmittente possa essere in grado di commutare il suo modo di funzionamento alla ricezione e decodificare il pacchetto entrante.
- Sul livello fisico dell'802.11 questo valore è settato a 28 ms.



PIFS – Point Coordination IFS

- E' usato dall'Access Point (o dal Point Coordinator, come è chiamato in questo caso) per guadagnare l'accesso al mezzo prima di ogni altra stazione.
- Questo valore è pari al SIFS più uno slot time che vale 78 ms.

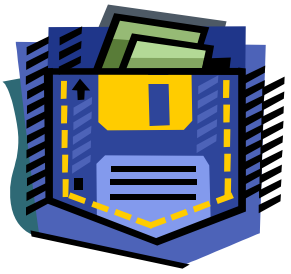


DIFS – Distributed IFS

- E' l'Inter Space Frame utilizzato per una stazione che vuole iniziare una nuova trasmissione.
- E' calcolato come PIFS più uno slot time e vale quindi 128 ms.

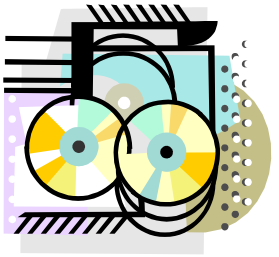
EIFS – Extended IFS

- E' 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 dialogo corrente.



Exponential Backoff Algorithm

- *L'Exponential backoff algotithm* è un metodo ben noto per risolvere il contenzioso tra differenti stazioni che vogliono accedere contemporaneamente al mezzo trasmissivo.
- Il metodo richiede che ciascuna stazione scelga un numero casuale (n) compreso tra 0 e un dato numero e aspetti per questo numero di slot prima di accedere al mezzo, effettuando comunque il controllo sulla portante per vedere se qualche altra stazione ha acceduto al mezzo in precedenza.



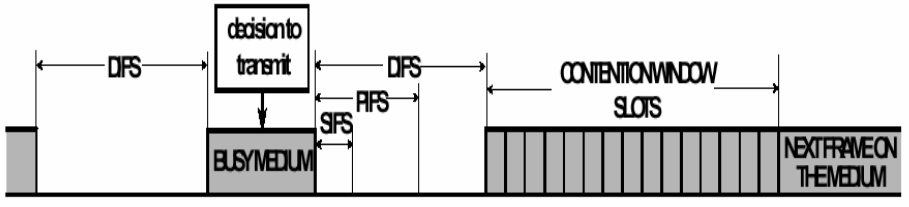
Exponential Backoff Algorithm

- Lo *Slot time* è definito in modo tale che la stazione sia sempre capace di determinare se un'altra stazione ha acceduto al mezzo al inizio del precedente slot. Questo consente di ridurre notevolmente la probabilità di collisione.
- Backoff esponenziale ha il seguente significato: ogni volta che la stazione sceglie uno slot per la trasmissione e si verifica una collisione, sarà esponenzialmente aumentato il massimo valore per la selezione casuale dello slot di trasmissione.

Exponential Backoff Algorithm

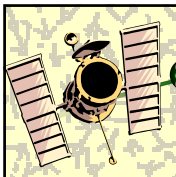
- L'802.11 definisce un *algoritmo di backoff esponenziale* [WLAN1] che deve essere eseguito nei seguenti casi:
  - *Quando la stazione testa il mezzo prima della prima trasmissione del pacchetto e il mezzo è occupato*
  - *Dopo ciascuna ritrasmissione*
  - *Dopo una trasmissione che ha avuto successo.*
- Il solo caso in cui il meccanismo non è utilizzato è quando la stazione decide di trasmettere un nuovo pacchetto e il mezzo viene rilevato libero per un tempo maggiore di DIFS.

Schematizzazione del meccanismo di accesso al mezzo



Metodi di accesso ad una BSS

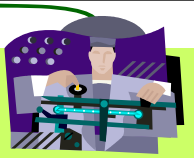
- Quando una stazione vuole accedere ad una esistente BSS (dopo un power-up,sleep mode o entra nell'area di una BSS), la stazione ha bisogno di acquisire la sincronizzazione relativa alle informazioni dall'Access Point.
- La stazione può acquisire questa informazione in uno dei seguenti modi:
  - ***Passive Scanning***: In questo caso la stazione aspetta di ricevere un Beacon Frame dall'Access Point. Il Beacon è un frame periodicamente inviato dall'Access Point contenete l'informazione relativa al sincronismo di trasmissione dei dati.
  - ***Active Scanning***: In questo caso la stazione tenta di localizzare un Access Point attraverso la trasmissione di un Probe Request Frame e attende che un Access Point risponda con frame Probe Response.
- Entrambi i metodi sono validi e la scelta tra uno o l'altro viene effettuata in funzione di esigenze di consumo o di incremento delle prestazioni.



Meccanismi di Autenticazione e Associazione

- Una volta che una stazione ha localizzato un Access Point e ha deciso di unirsi alla corrispondente BSS, viene eseguito il Processo di Autenticazione.
- In questa fase la stazione e l'Access Point effettuano uno scambio di informazioni in modo da verificare la relativa conoscenza di una data Password.
- Non appena le stazioni si sono autenticate inizia il processo di Associazione. In questa fase le informazioni scambiate hanno lo scopo di definire le caratteristiche della stazione e le capacità offerte dalla BSS.
- Tutto ciò consente al DSS, ovvero all'insieme degli AP, di ottenere informazioni circa l'attuale posizione della stazione espressa come appartenenza ad una particolare BSS ovvero come associazione ad un determinato Access Point.
- Osserviamo che una stazione è in grado di trasmettere o ricevere informazioni solo dopo che il processo di associazione si è positivamente concluso.

Roaming



- Il Roaming è il processo che consente lo spostamento di una stazione da una cella (o BSS) ad un'altra senza perdita di connessione.
- Questa funzione è simile a quella che viene realizzata nei sistemi di telefonia cellulare, con due differenze fondamentali:
  - Su un sistema LAN basato su un sistema di trasmissione a pacchetti, la transizione da una cella ad un'altra deve essere realizzata tra la trasmissione di un pacchetto e quella del successivo, al contrario di quanto accade in un sistema per telefonia in cui il processo deve avvenire durante lo svolgimento di una comunicazione. In una LAN quindi il processo risulta sicuramente di più semplice implementazione.
  - Su un sistema per il trasferimento della voce una temporanea disconnessione può non avere un effetto significativo, mentre in un ambiente basato sul pacchetto questa momentanea interruzione della connessione porta ad una significativa riduzione delle prestazioni, in quanto è necessario operare delle ritrasmissioni gestite però dai livelli superiori dello stack protocollare.

Roaming

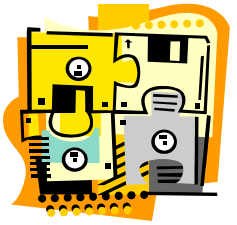
- Lo standard 802.11 non definisce come il roaming debba essere realizzato, ma definisce un modo di funzionamento base.
- La stazione in movimento attraverso il meccanismo di Passive Scanning o quello di Active Scanning rileva quali Access Point sono disponibili per la connessione. In funzione del livello del segnale ricevuto dagli AP decide a quale è più conveniente associarsi e attraverso un meccanismo di riassociazione definito dallo standard può eliminare l'associazione dal vecchio AP e associarsi a quello nuovo.
- Il processo di re-associazione consta di uno scambio di informazioni tra i due AP interessati allo scambio di utente, attraverso il distribution system, quindi senza appesantire la comunicazione attraverso il canale radio.

Mantenimento della sincronizzazione

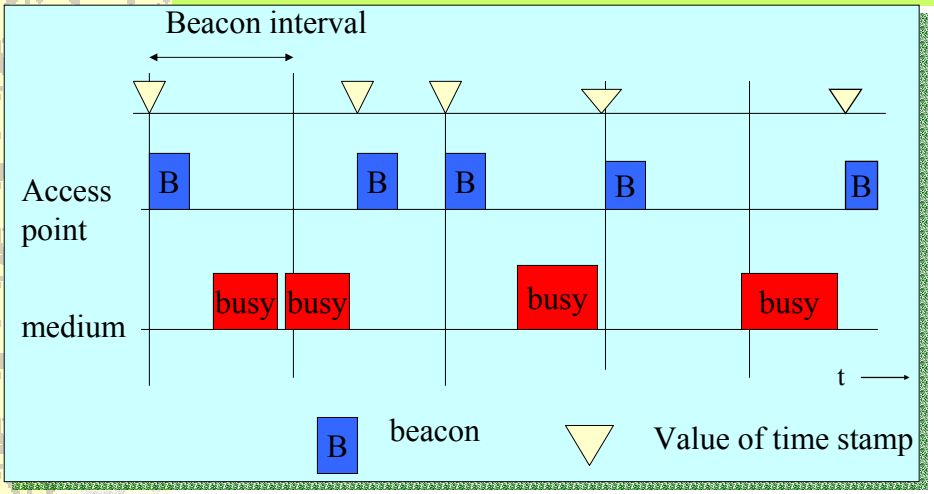
- Le stazioni hanno inoltre la necessità di mantenere la sincronizzazione che è necessaria per mantenere la sincronizzazione nei salti di frequenza e per la realizzazione di altre funzioni come il risparmio energetico.
- In una infrastruttura basata su BSS questo è ottenuto provvedendo all'aggiornamento del clock delle singole stazioni in accordo con il seguente meccanismo:
- L'Access Point trasmette periodicamente un *Beacon Frame contenente* il valore dell'orologio interno dell'Access Point al momento della trasmissione.

Osservazione

- Osserviamo che questo rappresenta il momento in cui la trasmissione viene realizzata e non il momento in cui il frame viene inserito nella coda di trasmissione.
- Poiché anche questo frame viene trasmesso utilizzando la regola CSMA la trasmissione può essere significativamente ritardata.
- La stazione ricevente controlla il valore del proprio orologio al momento della ricezione del segnale e lo corregge mantenendo la sincronizzazione con l'orologio dell'Access Point.
- Questo meccanismo è di fondamentale importanza perché previene lo slittamento del clock che si può verificare dopo alcune ore di funzionamento del sistema.

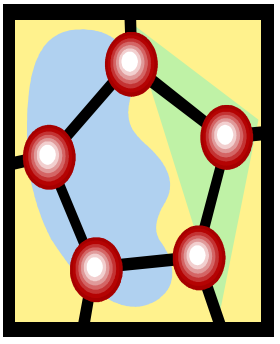


Synchronization



Sicurezza in una rete IEEE 802.11

- La sicurezza è una delle prime preoccupazioni delle persone che realizzano sistemi wireless LAN.
- Il comitato che ha sviluppato lo standard 802.11 ha risposto a questa incessante domanda di sicurezza implementando un meccanismo denominato *WEP* (*Wired Equivalent Privacy*).
- I due scopi fondamentali di questo meccanismo sono:
  - *Prevenire l'accesso alle risorse di rete da parte di apparecchiature Wireless LAN simili.*
  - *Impedire la cattura del traffico wireless LAN da parte di entità esterne.*

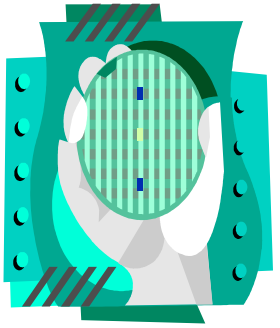


Prevenire l'accesso alle risorse di rete da parte di apparecchiature Wireless LAN simili

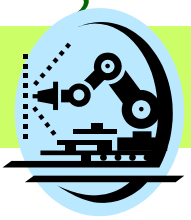
- Questo è realizzato attraverso il meccanismo di autenticazione in base al quale qualunque stazione che voglia comunicare deve dimostrare la conoscenza della chiave di autenticazione correntemente in uso.
- Tale meccanismo è simile a quello attuato nelle wired LAN, nel senso che colui che vuole entrare nel sistema deve immettere i permessi utilizzando la chiave fisica allo scopo di connettere la propria workstation alla LAN.

Impedire la cattura del traffico wireless LAN da parte di entità esterne

- Questa operazione viene realizzata per mezzo dell'algoritmo WEP che è un generatore di numeri pseudo casuali inizializzato per mezzo di una chiave segreta.
- Questo PRNG produce in uscita una sequenza chiave di bits pseudo casuali di lunghezza uguale al più grande pacchetto consentito dal sistema che viene combinata con i pacchetti in uscita o in entrata producendo il pacchetto effettivamente trasferito in aria.



IL WEP

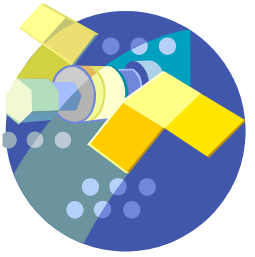


- Il WEP è un semplice algoritmo su RC4 RSA che ha le seguenti proprietà:
  - ***Notevole robustezza***: Un attacco brutale a questo algoritmo è difficoltoso perché ciascun frame è inviato con un vettore di inizializzazione che riavvia il PRNG per ciascun frame.
  - ***Mantenimento della sincronizzazione***: L'algoritmo di re-sincronizzazione è eseguito per ogni messaggio. Questo è necessario per lavorare in un ambiente connection-less dove i pacchetti possono andare persi (questo è tipico di tutte le LAN).

Frame 802.11: Tipi e struttura

Ci sono tre tipi fondamentali di frames

- ***Data Frames*** che sono usati per la trasmissione dei dati;
- ***Control Frames*** che sono usati per il controllo dell'accesso al mezzo (esempio RTS, CTS e ACK);
- ***Menagement Frames*** ovvero frames che vengono trasmessi allo stesso modo dei Data Frames per lo scambio di informazioni di controllo ma non sono passati ai livelli superiori dello stack protocollare (esempio i Beacon Frames).



Frame 802.11: Tipi e struttura

Ci sono tre tipi fondamentali di frames

- ***Data Frames*** che sono usati per la trasmissione dei dati;
- ***Control Frames*** che sono usati per il controllo dell'accesso al mezzo (esempio RTS, CTS e ACK);
- ***Menagement Frames*** ovvero frames che vengono trasmessi allo stesso modo dei Data Frames per lo scambio di informazioni di controllo ma non sono passati ai livelli superiori dello stack protocollare (esempio i Beacon Frames).

Power Saving

- Poiché le WLAN sono tipicamente usate in applicazioni mobili, il limite maggiore è rappresentato dalla durata delle batterie del dispositivo mobile.
- Questa è la ragione per cui lo standard 802.11 gestisce direttamente il Power Saving e definisce un intero meccanismo che consente alle stazioni di entrare in sleep mode per lunghi periodi senza perdere le informazioni trasmesse da altre stazioni.
- L'idea di base per il meccanismo di Power Saving è che l'AP mantiene continuamente in memoria un elenco contenente gli identificativi di tutte le stazioni che si trovano in modalità Power Saving, e bufferizza i pacchetti indirizzati a tali stazioni fino a quando le stesse stazioni non fanno richiesta esplicita di informazioni mediante una **Polling Request**, o fino a quando non cambiano il proprio stato di funzionamento.

Power Saving

- Nelle Beacon Frames, gli AP trasmettono anche informazioni che indicano la presenza di dati bufferizzati per le stazioni in Power Saving, in modo tale che tali stazioni possano risvegliarsi per fare richiesta dei dati a loro indirizzati.

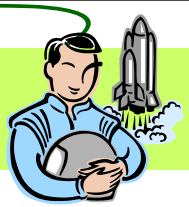
- Le informazioni multicast e broadcast sono conservate negli AP, e trasmesse a tempi prefissati, quando ogni stazione in Power Saving Mode che vuole ricevere questi tipi di frames è sveglia.

Frame 802.11: Tipi e struttura

- Ciascun tipo di frame è poi suddiviso in differenti sottotipi, in base alla specifica funzione.
- I Frame definiti dallo standard 802.11 sono composti dai seguenti componenti:

Preambolo	PLCP Header	MAC Data	CRC

Preambolo



Questo campo è dipendente dal livello fisico e comprende:

- ***Synch***: una sequenza di 80 bit di 1 e 0 alternati che è utilizzata dalla circuiteria del livello fisico per selezionare l'appropriata antenna (se è utilizzata la diversità)
- ***SFD***: è il delimitatore di inizio frame (Start Frame Delimiter) che consiste di una configurazione binaria di 16 bit modello 0000 1100 1011 1101, che è usata per definire la temporizzazione del frame.

PLCP Header

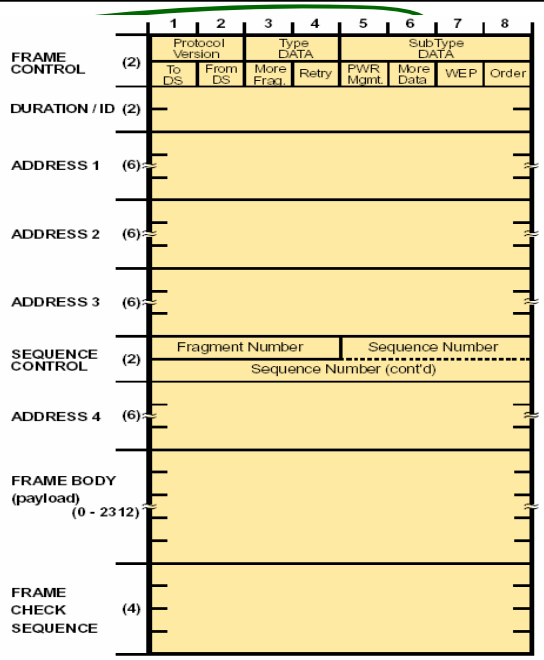
L'Header PLCP è sempre trasmesso a 1Mbit/s e contiene informazioni logiche utilizzate dallo strato fisico per decodificare il frame.

Consiste dei seguenti campi:

- ***PLCP_PDU Length Word***: rappresenta il numero di bytes contenuti nel pacchetto. Questa informazione è essenziale per lo strato fisico allo scopo di rilevare correttamente la fine del pacchetto.
- ***PLCP Signaling Field***: Correntemente contiene solo l'informazione relativa alla velocità di trasmissione codificata in incrementi di 0,5 Mbit/s da un 1 Mbit/s a 4,5 Mbit/s
- ***Header Error check Field***: è un campo di 16 bit che viene utilizzato per la rilevazione d'errore.

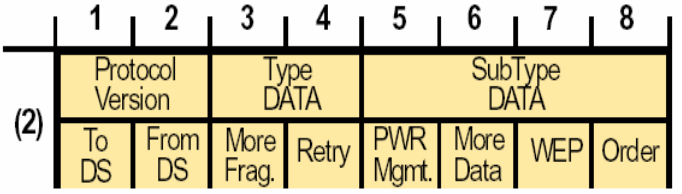
MAC Data

- Tipico formato di un frame di MAC.
- I campi indicati non sono presenti in tutti i frame come di seguito descritto



Campo Frame Control

Il campo Frame Control contiene le seguenti informazioni



Struttura del campo Frame Control

- ***Protocol Version***: Questo campo consiste di 2 bits che sono invarianti sia per dimensione sia per posizionamento nelle successive versioni dello standard 802.11 e saranno utilizzati per riconoscere le future versioni quando queste saranno disponibili. Nella versione attualmente disponibile dello standard questo valore è fissato a 0.
- ***Type e Subtype***: Si compone di 6 bits che definiscono il tipo e il sottotipo del frame secondo la tabella riportata di seguito:

Tabella Type e Subtype

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Association Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-0001	Reserved
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 Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
10	Data	0000-1111	Reserved

Struttura del campo Frame Control

- ***ToDS***: Questo bit è posto al valore 1 quando il frame è indirizzato all'AP allo scopo destinato ad essere trasferito ad una stazione collegata al Distribution System, compresi i casi in cui la stazione di destinazione è nella stessa BSS e l'AP funziona da semplice ripetitore per il frame. In tutti gli altri frame questo bit è posto al valore 0.
- ***FromDS***: Questo bit è posto al valore 1 quando il frame è ricevuto dal Distribution System.
- ***More Fragments***: Questo bit è posto al valore 1 quando più frammenti appartenenti allo stesso frame seguono il frammento corrente.
- ***Retry***: Questo bit indica che il frammento corrente è la ritrasmissione di un frammento precedentemente trasmesso. Questo è utilizzato per riconoscere le trasmissioni duplicate dei frame che si possono verificare quando un pacchetto di Acknowledgment va perso.

Struttura del campo Frame Control

- ***Power Menagement***: Questo bit serve per cambiare lo stato da Power Save a Active e viceversa.
- ***More Data***: Questo bit è utilizzato per il Power Menagement ma viene sfruttato anche dall'Access Point per indicare che ci sono molti frame memorizzati e indirizzati a questa stazione. La stazione può decidere di utilizzare questa informazione per continuare il Polling o anche per commutare il modo di funzionamento in Active.
- ***WEP***: Questo bit indica che il corpo del frame è codificato in accordo con l'algoritmo WEP.
- ***Order***: Questo bit indica che il frame è stato inviato con Stricly-Order service class. Questa classe di funzionamento è definita per utenti che non possono accettare cambi di ordinamento tra frames Unicast e frames Multicast (l'ordinamento dei frames Unicast a uno specifico indirizzo è sempre mantenuto).

Struttura del campo Duration/ID

Questo campo ha due significati diversi in base al tipo di frame:

- In messaggi di Power save Poll questo campo rappresenta l'identificativo della stazione;
- In tutti gli altri frames questo campo rappresenta il valore di durata utilizzato per il calcolo del NAV.

Campo Address Fields

Un frame può contenere al più 4 indirizzi come definito dai campi ToDS e FromDS definiti nel campo Control:

- ***Address-1***: è sempre l'indirizzo del destinatario. Se ToDS è a 1 questo è l'indirizzo dell'AP, mentre se è a 0 questo rappresenta l'indirizzo del destinatario finale.
- ***Address-2***: è sempre l'indirizzo di colui che effettua la trasmissione. Se FronDS è a 1 questo è l'indirizzo dell'AP mentre se è a 0 è l'indirizzo della stazione.

Campo Address Fields

- ***Address-3***: in molti casi è l'indirizzo mancante. Se un frame ha il campo FromDS al valore 1 Address-3 rappresenta l'indirizzo della vera sorgente del frame. Se ToDS i invece a 1 il valore in questo campo identifica l'indirizzo di destinazione.

- ***Address-4***: è usato in casi particolari dove è presente un Distribution System completamente wireless e il frame è stato trasmesso da un AP ad un altro. In questo caso sia ToDS sia FromDS sono a 1 così sia l'indirizzo di destinazione sia l'indirizzo della vera sorgente del frame sono mancanti.

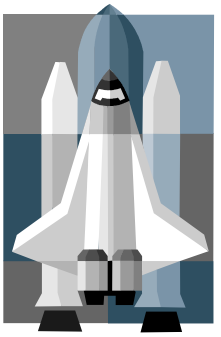
Significato dei campi indirizzo

La seguente tabella riassume l'utilizzo dei vari indirizzi in funzione del valore di ToDS e FromDS.

ToDS	FromDS	Address1	Address2	Address3	Address4
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**

CAMPO Sequence Control

- Questo campo è utilizzato per rappresentare l'ordine di differenti frammenti che appartengono ad uno stesso frame e di controllare la duplicazione dei pacchetti.
- E' in realtà costituito da due sottocampi, Fragment Number e Sequence Number, che definiscono il frame e il numero del frammento nel frame.



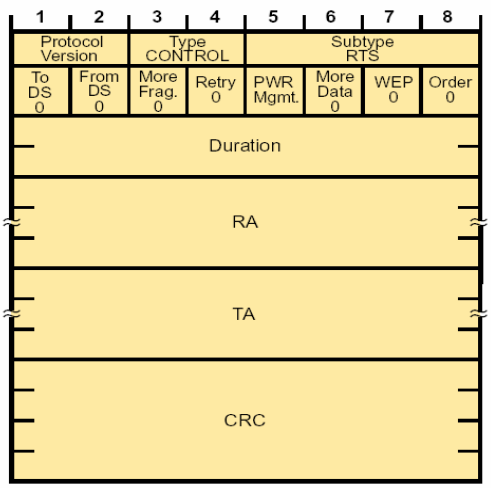
CAMPO CRC

- Il CRC è un campo di 32 bit contenete un Cyclic Redundancy Check (CRC) a 32 bit.

Formato delle Frames più comuni

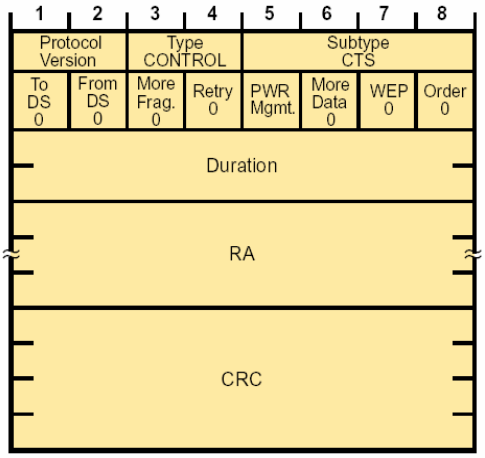
Formato del Frame RTS

- L'RA del frame RTS è l'indirizzo della STA che è designata come immediato destinatario del successivo frame dati o di Menagement.
- Il TA è l'indirizzo della STA che ha trasmesso il frame RTS.
- Il campo Duration contiene il tempo, espresso in microsecondi, richiesto per trasmettere il successivo frame dati o Menagement, più un CTS, più un frame ACK, più tre intervalli SIFS.



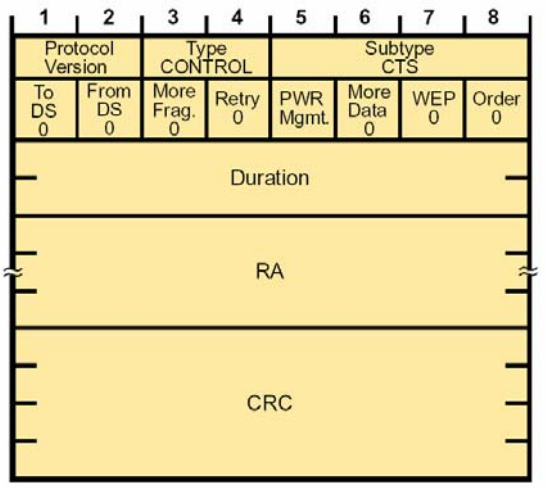
Formato del frame CTS

- Il campo Receiver Address (RA) del CTS è copiato dal campo Transimitter Address (TA) del frame RTS immediatamente precedente del quale il CTS rappresenta la risposta.
- Il valore Duration è il valore ottenuto dal campo Duration del frame RTS immediatamente precedente, meno il tempo, espresso in microsecondi, richiesto per trasmettere il frame CTS e il suo intervallo SIFS.



Formato del frame ACK

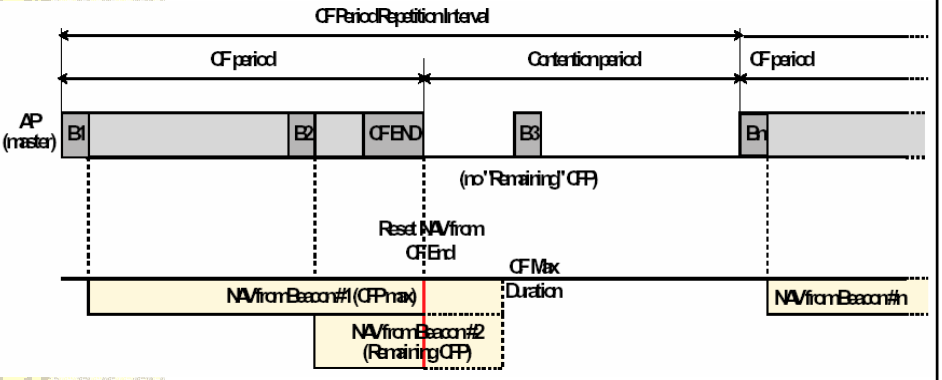
- Il campo Receiver Address del frame ACK è copiato dal campo Address-2 del frame immediatamente precedente.
- Se il bit More Fragment era settato a 0 nel precedente frame, il valore del campo Duration è posto a 0, altrimenti il valore è ottenuto dal campo Duration del precedente frame meno il tempo in microsecondi richiesto per trasmettere il frame ACK e il suo intervallo SIFS.



Point Coordination Function

- Oltre alla funzione base di coordinazione denominata Distributed Coordination, è prevista una *Point Coordination Function*, che può essere usata per implementare servizi che hanno requisiti temporali stringenti, come le trasmissioni audio o video.
- Questa funzione fa uso dell'elevata priorità che l'Access Point può guadagnare attraverso l'utilizzo di un breve Inter Space Frame (PIFS).

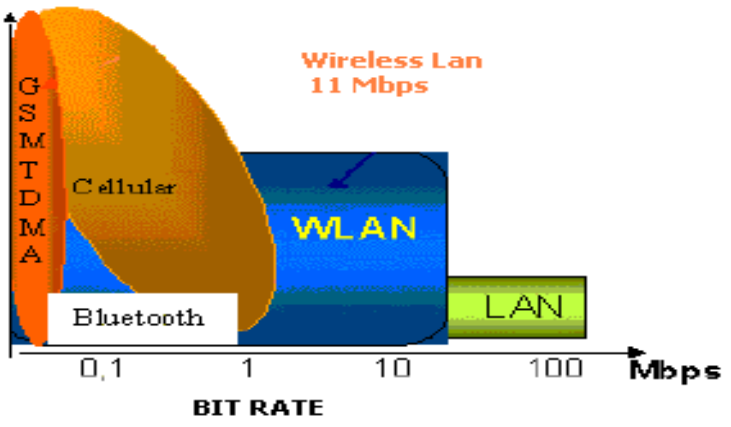
Point Coordination Function



Point Coordination Function

- Utilizzando questa elevata priorità di accesso, l'Access Point emette secondo un meccanismo di polling delle richieste alle stazioni per la trasmissione dati, quindi controlla l'accesso al mezzo.
- Allo scopo di consentire alle stazioni regolari di accedere al mezzo trasmissivo è prevista la norma in base alla quale l'Access Point deve lasciare abbastanza tempo per il Distributed Access all'interno della PCF.

Confronto tra i Bit Rates



Bibliografia

- CISCO ***http://www.cisco.com***
- 3Com Corporation ***http://www.3com.com***
- Aironet Wireless Communication ***http://www.aironet.com***
- Bay Networks ***http://www.netwave-wireless.com***
- Breeze Wireless Communication Ltd. ***http://www.breezecom.com***
- Cabletron Systems, Inc. ***http://www.cabletron.com***
- Institute of Electrical & Electronics Engineers, Inc ***http://www.ieee.org***
- Lucent Technologies ***http://www.wavelan.com***
- Ministero delle Telecomunicazioni ***http://www.comunicazioni.it***
- Proxim Inc. ***http://www.proxim.com***
- The Wireless LAN Alliance ***http://www.wlana.com***

FINE