TESINA PER IL CORSO DI RETI DI CALCOLATORI

Panoramica sulle reti wireless

e

Standard 802.11

Docente: Concettina Guerra

Studente: **Marco Benvegnù** (436367/IF)
Gruppo: Error404

Università di Padova
Anno Accademico 2002/2003

Panoramica sulle reti wireless

Sin dagli anni 1970, per necessità o per comodità, la possibilità di collegare computer fra loro senza l'uso di fili, ha attirato l'attenzione di ricercatori ed imprenditori (in cerca di qualcosa di nuovo da vendere).
Negli anni 1970, fu la "necessità" di collegare fra loro le isole Hawaii a guidare un insieme di ricercatori allo sviluppo di *AlohaNet.*
Nel 1994, fu la "comodità" di una connessione senza cavo fra cellulari e palmari a spingere Ericsson, IBM, Intel, Nokia e Toshiba verso *Bluetooth.*

PAN Wireless

I cavi sono scomodi: intralciano i movimenti del mouse, sono soggetti ad usura e quelli che collegano il cellulare al PDA vengono spesso lasciati o dimenticati a casa.
Tecnologie ad infrarossi e radio rendono notevolmente più pratiche le operazioni quotidiane di sincronizzazione fra portatile, desktop e palmare, ma anche il download delle immagini dalla macchina fotografica digitale, l'upload di musiche nel riproduttore di MP3, ecc.
A volte si esagera in questa direzione, rendendo wireless anche tastiere e stampanti…
Bluetooth consente collegamenti radio a 721 Kbps su brevi distanze (10 m), ed è progettato per essere economico, semplice da usare, facilmente integrabile e sopratutto a basso consumo.
IrDA (Infrared Device Application) consente collegamenti ad infrarosso a 4 Mbps tra dispositivi posti in visibilità reciproca e ad una distanza di 1 o 2 metri.

LAN Wireless

Una delle applicazioni wireless di maggior rilievo, in questi giorni, è quella cha va sotto il nome di "Mobile Internet", ossia la possibilità di accedere ad Internet, con il proprio portatile o palmare, senza dover dipendere da cavi di collegamento.
Scenario tipico è quello di un'Università o di un ufficio che abbia installato uno o più **punti di accesso** (**AP**) wireless: è sufficiente entrare nel raggio d'azione di uno di questi AP, per vedere il proprio portatile collegato alla rete dipartimentale; diventa così possibile spedire un'e-mail o accedere al Web mentre si è in aula o in cortile, ed anche mentre si passeggia lungo i corridoi del dipartimento.
In questo senso, la tecnologia wireless è orientata ad offrire connettività ad una LAN cablata preesistente. In altri ambiti, è intesa a sostituire completamente l'uso di cavi di collegamento, anche per le postazioni fisse, qualora il cablaggio tradizionale risultasse troppo costoso o scomodo.

È interessante notare come sempre più aeroporti, hotel, fiere ed anche negozi stiano installando AP atti ad offrire accessibilità Internet alla propria clientela. Spesso, in occasione di convegni e presentazioni, viene temporaneamente attivato un AP per intrattenere i presenti durante le pause.
Il fenomeno è esplosivo: con l'aumentare della copertura, sempre più utenti saranno interessati ad acquistare interfacce wireless per i propri portatili, e con l'aumentare dell'utenza, sempre più locali pubblici saranno interessati a fornire copertura.
All'inizio di questo fenomeno, a causa dell'eterogeneità delle tecnologie proposte, sorsero grossi problemi di compatibilità, e subito apparve chiara la necessità di uno standard. Nel 1997 il comitato IEEE approvò lo standard **802.11**, la cui variante 802.11b ad 11 Mbps, nota anche come

WiFi, ha riscontrato un grandissimo successo. Tale standard verrà analizzato nella seconda parte di questo documento.

Altro scenario importante è quello rappresentato da ospedali, magazzini o ristoranti che vogliano offrire accesso ad un database centrale ai propri dipendenti (dotati di palmare): un magazziniere potrà aggiornare l'inventario ed effettuare un nuovo ordine direttamente dal magazzino, ed un cameriere potrà trasmettere le ordinazioni in cucina.

Anche quando non è possibile installare un AP, permane la possibilità di instaurare una LAN wireless fra le stazioni presenti; in questo caso si parla di reti **ad hoc** o di **MANET** (**Mobile Ad hoc NETwork**). Alcuni esempi:

- Raduno di persone con un portatile (nel caso di un gruppo di lavoro, la rapidità e la semplicità con cui la rete può essere installata va a tutto beneficio della produttività)
- Operazioni di acquisizione dati su terreno inospitale
- Flotta di navi in mezzo all'oceano
- Interventi militari in territorio nemico

Assieme ad 802.11, altre tecnologie hanno ricevuto grande approvazione:

- **HomeRF** - sfrutta il protocollo SWAP ed è orientato all'uso domestico a basso costo
- **HiperLAN/2** - standard Europeo a 54 Mbps

802.11b è lo standard attualmente più diffuso, e per Giugno 2003 sarà disponibile la nuova variante **802.11g** (**WiFi 5**), che, grazie alle elevate prestazioni (54 Mbps) ed alla compatibilità con il consolidato 802.11b, sembra destinata ad un futuro roseo.

MAN Wireless

Un altro dominio di applicazione è quello delle MAN wireless (**broadband wireless** o **wireless local loop**), che consente di distribuire dati (Internet, telefonia, on-demand cinema…) su di un agglomerato di case tramite una potente antenna. Questa soluzione fornisce un'alternativa al costoso cablaggio dell'*ultimo miglio*.
Il gruppo di lavoro IEEE **802.16** si occupa di questa architettura.

WAN Wireless

La telefonia di terza generazione (**3G**) si propone di fornire gli stessi servizi visti per le LAN e le MAN wireless, ma con una copertura totale, anziché localizzata in prossimità degli AP, fornendo fino a 384 Kbps alle stazioni mobili e 2 Mbps a quelle fisse in casa.
Tecnologie di punta, in questo movimentato settore, sono **UMTS** e **CDMA2000**, ma quelle dominanti, per ora, sono quelle di transizione (**2.5G**), come **EDGE** (un'evoluzione di **GSM**) e **GPRS**. Sul lato applicativo emergono **WAP** e **I-Mode**; quest'ultimo, in particolare, ha conquistato il mercato Giapponese, grazie ad un'offerta di servizi davvero vantaggiosa.
Potrebbe anche accadere che la larga diffusione di 802.11 renda superfluo 3G, almeno negli ambienti urbani.

NOTA: La precedente classificazione in PAN, LAN, MAN e WAN non è netta, ma solo indicativa dei principali ambiti d'applicazione delle varie tecnologie.

Standard 802.11

Lo standard 802.11 è un documento costituito da più di 500 pagine (v. [1]). Quella che segue vuole essere una breve e chiara introduzione agli aspetti più importanti di tale standard. Particolare attenzione è stata dedicata al protocollo di controllo degli accessi al mezzo.

Problematiche

Le reti wireless sono caratterizzate da una serie di problematiche non presenti nei sistemi cablati:

- Scelta di una banda radio disponibile a livello mondiale
- Problema della stazione nascosta/esposta (discusso in seguito)
- Le trasmissioni radio sono soggette ad un'elevata rumorosità
- I segnali radio ad alta frequenza sono soggetti alla riflessione e quindi vengono ricevuto più volte con sfasamenti temporali dipendenti dalla lunghezza del percorso compiuto. Questo tipo d'interferenza viene chiamata **multipath fading**.
- Minimizzare il consumo delle batterie
- Le microonde sono ionizzanti ed è quindi necessario limitarne la potenza
- La mobilità dei computer impone l'uso di tecniche di routing specializzate
- Molte implementazioni di TCP e UDP sono ottimizzate per sole reti affidabili
- I dati trasmessi via radio sono facilmente intercettabili e quindi vanno crittografati
- Vulnerabilità alle interferenze dovute a dispositivi che lavorano alle stesse frequenze (o ad attacchi di "Denial of Service")

Terminologia

Lo standard 802.11 gestisce sia reti **ad hoc** che reti ad **infrastruttura**; queste ultime sono costituite da una o più **celle** indipendenti, ognuna delle quali è controllata da una **stazione base**, chiamata **Access Point** o **AP**. I vari AP sono connessi tra loro da una rete, tipicamente cablata, chiamata **Distribution System**.

Bande ISM

Molti governi hanno mantenuto libere alcune bande di frequenze, note come **bande ISM** (Industriale, Scientifica, Medica). Esse possono essere usate liberamente da chiunque, senza dover richiedere licenze, a patto di rispettare precisi limiti di potenza e di utilizzare tecniche di **spread spectrum** atte a limitare le interferenze fra i diversi dispositivi.

Molti apparecchi sfruttano le bande ISM:

- telefoni cordless
- forni a microonde
- radiocomandi per cancelli automatici, sistemi d'allarme e giocattoli
- apparati radar
- Bluetooth

ed interferiscono con il normale funzionamento delle LAN wireless.

Negli USA sono disponibili le seguenti bande:

Frequenza iniziale	Larghezza di banda
902 MHz	26 MHz
2.4 GHz	83.5 MHz
5.725 GHz	125 MHz

ma in Europa e Giappone, solo la banda a 2.4 GHz è disponibile.
Inoltre, all'aumentare della frequenza, aumentano gli effetti di riflessione ed assorbimento delle onde elettromagnetiche, e di conseguenza diminuiscono le distanze raggiungibili. In particolare, a 2.4 GHz è possibile coprire una distanza 4 volte superiore che a 5 GHz.
Per questi ed altri motivi, la maggioranza degli standard utilizza la banda ISM a 2.4 GHz.

Strato fisico

Lo standard 802.11 del 1997, specificava tre tecniche di trasmissione, tutte ad 1 o 2 Mbps. A detta di molti, le prestazioni fornite erano insufficienti. Il comitato si mise di nuovo al lavoro, e nel 1999 furono approvati 2 nuovi standard:

- **802.11b**, compatibile con 802.11, aggiungeva a quest'ultimo due nuove velocità: 5.5 Mbps e 11 Mbps
- **802.11a**, che, sfruttando una delle più versatili tecniche di modulazione (QAM-64), poteva raggiungere i 54 Mbps

802.11a usava però la banda a 5 GHz, e quindi, 2 anni dopo, il comitato propose una sua variante, **802.11g**, consentendo di raggiungere i 54 Mbps nella banda ISM tradizionale a 2.4 GHz, e mantenendo la compatibilità verso il basso con i dispositivi 802.11b (l'approvazione di quest'ultimo standard è prevista per Giugno 2003).

La seguente tabella riassume le caratteristiche fisiche delle varianti 802.11 proposte:

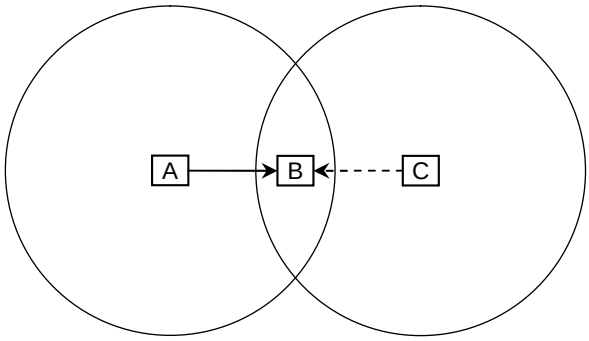
Protocollo	Modulazione	Velocità	Banda utilizzata
802.11	Infrarosso diffuso	1 o 2 Mbps	-
	FHSS	1 o 2 Mbps	2.4 GHz ISM
	DSSS	1 o 2 Mbps	2.4 GHz ISM
802.11a	OFDM	54 Mbps (max)	5.2 GHz UNII
802.11b	HR-DSSS	11 Mbps (max)	2.4 GHz ISM
802.11g	OFDM	54 Mbps (max)	2.4 GHz ISM

La velocità viene adattata dinamicamente sulla base del rapporto segnale/disturbo.
Per una discussione dettagliata sulle tecniche di modulazione vedere [3]. In questa sede ci si limita a notare che, al fine di evitare interferenze fra dispositivi radio che sfruttano la stessa banda, si ricorre a tecniche di **spread spectrum**, che consistono nel distribuire il segnale su una banda molto più larga del necessario, in modo che esso appaia come rumore ai dispositivi non interessati. Ad es. FHSS (Frequency Hopping Spread Spectrum) ottiene lo scopo saltando ad intervalli regolari da una frequenza portante all'altra in modo pseudocasuale; solo i dispositivi *sintonizzati* sullo stesso seme e intervallo (**dwell time**) rilevano un segnale netto. Ciò incrementa anche la sicurezza e la reiezione al *multipath fading*.

Problema della stazione nascosta / esposta

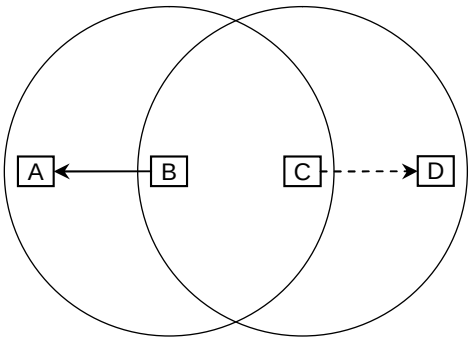
Una delle principali caratteristiche delle LAN wireless è data dall'inefficacia delle tecniche di **Carrier Sensing** nel determinare se il mezzo è accessibile.

Siano date tre stazioni *A, B, C* con i raggi d'azione raffigurati, ed *A* stia trasmettendo a *B*:



Se ora *C* ascolta il mezzo, lo troverà libero e sarà convinta di poter trasmettere a *B*; cominciando a trasmettere disturberà la trasmissione di *A*, impedendo a *B* di riceverla; sia *A* che *C* saranno costrette a ritrasmettere.
Questo è noto come il **problema della stazione nascosta**.

Esiste anche il problema inverso: si supponga che *B* stia trasmettendo ad *A* e che *C* voglia trasmettere a *D*:



Ascoltando il mezzo, *C* sentirà la trasmissione di *B* e concluderà erroneamente di non poter trasmettere; invece, essendo *D* fuori della portata di *B*, ed A fuori della portata di *C*, le due trasmissioni potrebbero avvenire parallelamente senza interferenze.
Questo è noto come il **problema della stazione esposta**.

Ragionamenti analoghi valgono per le tecniche di **Collision Detection** (ad ogni modo non applicabili alle trasmissioni radio, tipicamente half-duplex). Se ne conclude che non è possibile utilizzare lo stesso protocollo usato da Ethernet, ossia CSMA/CD, per il controllo dell'accesso al mezzo.

Carrier Sensing Virtuale

In risposta al problema della stazione nascosta, sono state elaborate delle eleganti tecniche di **Collision Avoidance**: l'idea di base consiste nello stimolare il destinatario nell'emettere un breve frame, in modo da informare le stazioni ad esso vicine di non interferire per l'intera durata della trasmissione che sta per avvenire. Il protocollo è il seguente:

Quando *A* vuole trasmettere un frame a *B*, prima invia un frame **RTS** (**Request To Send**), al quale *B* risponde con un frame **CTS** (**Clear To Send**). Alla ricezione di CTS, *A* può cominciare a trasmettere.
Entrambi i frame RTS e CTS contengono il tempo mancante prima della fine della trasmissione. Ogni stazione nel raggio d'azione di *A* o *B* riceverà uno o entrambi i frame, ed imposterà il proprio indicatore di **Carrier Sensing Virtuale**, chiamato **NAV** (**Network Allocation Vector**), per la durata indicata dal frame.
Il NAV è un contatore che viene decrementato nel tempo, fino a 0; quando NAV è diverso da zero, vuol dire che una trasmissione è in atto nelle vicinanze.

CSMA/CA

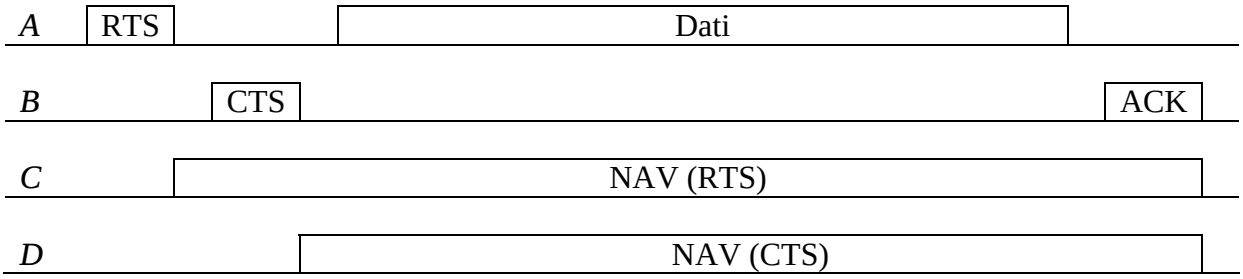
Il precedente protocollo funziona bene solo nel caso teorico in cui le stazioni abbiano tutte lo stesso raggio d'azione e i frame RTS e CTS possano essere scambiati in tempo infinitesimo. In caso contrario, le collisioni possono ancora avvenire, e quindi tale protocollo viene, in genere, affiancato a tecniche di Carrier Sensing tradizionali e di acknowledgement a livello di MAC sublayer.
Il Carrier Sensing riduce la probabilità di collisioni dovute a tentativi di acquisizione contemporanea del mezzo, ed è tanto più efficace quanto più ci si avvicina alla situazione ideale, ma piuttosto frequente, di stazioni tutte comprese nei rispettivi raggi d'azione.
L'acknowledgement a livello di MAC sublayer ha lo scopo di ridurre i tempi di ritrasmissione dei frame danneggiati, anticipando notevolmente un compito normalmente affidato al livello di trasporto.

Il protocollo **CSMA/CA** (**Carrier Sense Medium Access with Collision Avoidance**) funziona nel seguente modo, per una trasmissione da *A* a *B*:

1. La stazione trasmittente *A* cerca di determinare lo stato del mezzo valutando il contenuto di NAV ed ascoltando il mezzo. Il canale è considerato libero, quando sia il *Carrier Sensing Virtuale* che quello *Reale* non rilevano attività. I casi sono due:
    a. Se il canale rimane libero per un intervallo di tempo DIFS[1], salta al punto 3.
    b. Se invece il canale è occupato (o viene occupato durante l'intervallo DIFS), prosegue al punto 2.
2. *A* avvia la **procedura di backoff** (discussa più avanti).
3. *A* emette un RTS.
4. Se entro un intervallo di tempo ben definito, *A* non riceve il CTS da *B*, vuol dire, molto probabilmente, che l'RTS ha colliso con un altro frame; spesso ciò significa che due stazioni hanno scelto lo stesso slot nella finestra di backoff. Per questo motivo, prima di ritentare la trasmissione, *A* raddoppia la dimensione della finestra di backoff (*CW*) e poi ripete dal punto 2. Lo scopo di tale raddoppio è quello di adattare la dimensione della finestra al numero di contendenti, in considerazione del fatto che le collisioni sono indice di "affollamento".
5. Quando *B* riceve l'RTS, risponde con un CTS.
6. Ricevuto il CTS, *A* può cominciare a trasmettere il frame contenente i dati veri e propri.
7. Se entro un intervallo di tempo ben definito, *A* non riceve un ACK da *B*, vuol dire che il frame *Dati* non è stato ricevuto correttamente, e quindi *A* deve ritrasmetterlo ripetendo tutta la procedura.
8. Una volta che *B* ha ricevuto correttamente il frame *Dati*, risponde con un ACK concludendo il protocollo.

[1] Il significato di questa sigla e l'utilità di tale intervallo, saranno chiariti in seguito.

Il seguente esempio mostra il comportamento di 4 stazioni durante la trasmissione da *A* a *B*; la stazione *D* si trova nel raggio d'azione di *B*, ma non in quello di *A*, e quindi aggiorna il proprio NAV solo dopo aver ricevuto il CTS proveniente da *B*.



Procedura di backoff

La procedura di backoff è stata inserita nelle fasi del protocollo CSMA/CA in cui le collisioni sono più frequenti, e consiste nell'attendere per un tempo casuale, ma limitato, secondo l'algoritmo di **binary exponential backoff.** In questo modo si evita che più stazioni, in attesa che il canale si liberi, tentino di acquisire contemporaneamente il canale nell'istante in cui questo viene rilasciato. L'algoritmo è il seguente:

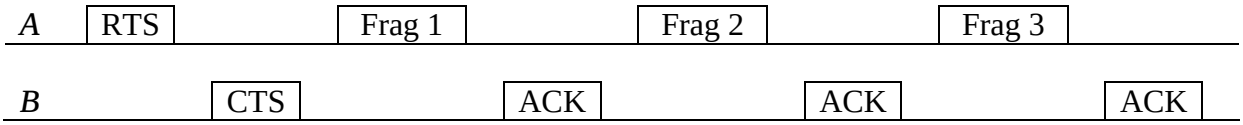
1. *A* aspetta che il canale si liberi, e che rimanga libero per tutto un intervallo DIFS.
2. Solo se il **contatore di backoff** di *A* è a 0, sceglie un numero a caso compreso fra 0 e *CW* (larghezza corrente della finestra di contesa) altrimenti lo lascia al valore attuale (che è il residuo di una procedura di backoff precedentemente interrotta).
3. Per ogni intervallo ***SlotTime*** che il canale rimane libero, il contatore viene decrementato; se il mezzo viene occupato, torna al punto 1.
4. Quanto il contatore giunge a zero, la procedura di backoff termina.

Un esempio in merito alla **dimensione della finestra di backoff** (*CW*): inizialmente *CW* è pari a 7 (*CWmin*); le ritrasmissioni, come visto, implicano un raddoppio del numero di slot, portando *CW* a 15, 31, 63, 127, 255. Arrivata a 255 (*CWmax*), la dimensione non cresce più.
Al corretto completamento di una trasmissione, *CW* viene riportato a 7.

Protocolli MAC

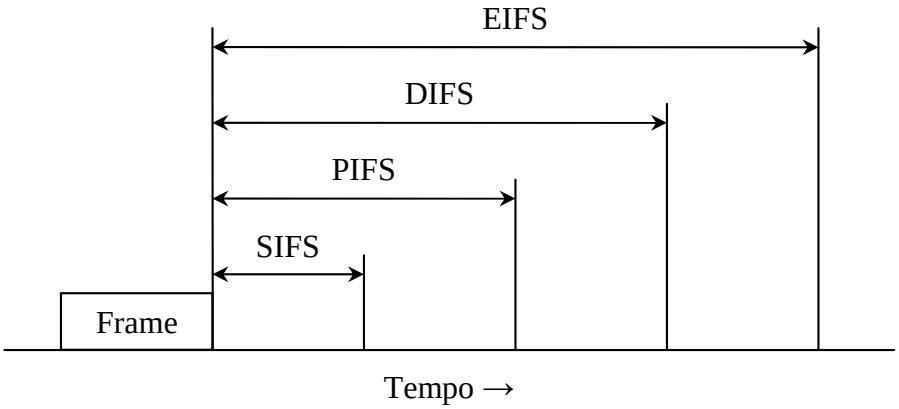
Nello standard 802.11 sono previste due modalità di funzionamento: la prima, chiamata **DCF** (**Distributed Coordination Function**), prevede che siano le stazioni a gestire, in modo distribuito, l'accesso al mezzo, secondo il protocollo CSMA/CA. La seconda, chiamata **PCF** (**Point Coordination Function**) affida all'AP la coordinazione di tutte le stazioni nella sua cella.

In DCF è prevista una tecnica di **frammentazione dei frame**: un frame può essere scomposto in più **frammenti**, ognuno numerato e riscontrato (ACK) separatamente. La motivazione è presto detta: le trasmissioni radio sono affette da un'elevata rumorosità, e se un frame è troppo grande, la probabilità che venga danneggiato diventa elevatissima. La frammentazione consente di restringere le ritrasmissioni ai soli frammenti danneggiati, anziché all'intero frame.
Notare che una volta acquisito il canale con RTS e CTS, più frammenti possono essere inviati in sequenza, dando origine a quello che viene chiamato un **fragment burst**:



In PCF, la stazione base interroga ciclicamente le altre stazioni (**polling**), le quali possono trasmettere solo quando è il loro turno; siccome l'ordine delle trasmissioni è completamente controllato dalla stazione base, non si possono mai verificare collisioni.

Tutte le stazioni devono supportare DCF, mentre PCF è opzionale, e raramente implementato. DCF e PCF possono coesistere all'interno di una stessa cella, grazie ad un'intelligente assegnazione dei tempi d'attesa:



Lo standard definisce 4 intervalli di tempo, i quali forniscono diversi livelli di priorità ai vari protocolli:

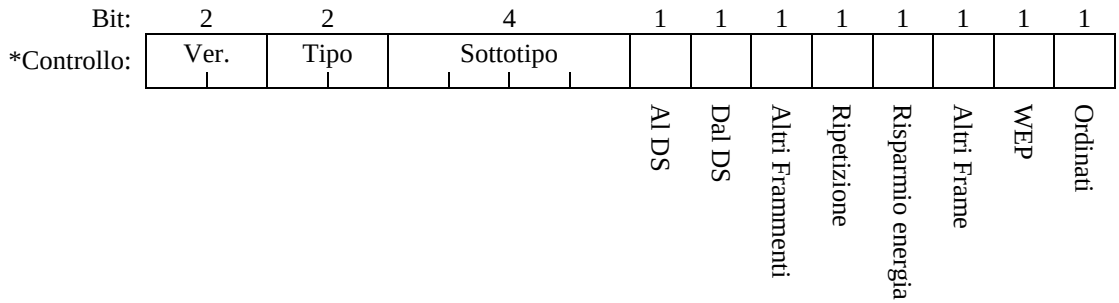
- **SIFS (Short Inter Frame Space)** - è l'intervallo più breve, usato per separare i frame appartenenti ad una singola trasmissione. Ad esempio, gli intervalli tra i frame RTS, CTS, Frag ed ACK di un fragment burst, hanno tutti questa durata. Notare che una sola stazione ha il permesso di rispondere dopo un intervallo SIFS. In questo modo si impedisce alle altre stazioni, le quali devono attendere per un periodo più lungo, di interrompere una trasmissione in corso.
- **PIFS (PCF Inter Frame Space)** - trascorso un intervallo più lungo, PIFS, è il turno dall'AP (chiamato anche Point Coordinator, in questo contesto).
- **DIFS (DCF Inter Frame Space)** - se l'AP non ha nulla da dire, trascorso l'intervallo DIFS, ogni stazione può tentare di acquisire il canale per iniziare una nuova trasmissione; è a questo punto che possono verificarsi le collisioni per accesso contemporaneo, ed infatti la finestra di contesa (**slotted backoff window**) comincia proprio dopo questo intervallo.
- **EIFS (Extended Inter Frame Space)** - usato al posto di DIFS dalle stazioni che hanno ricevuto un frame incomprensibile, dal quale, quindi, non è stato possibile estrarre l'informazione necessaria all'aggiornamento dell'indicatore NAV. Questo intervallo è stato studiato in modo da consentire ad un'altra stazione di rispondere al frame ignoto, risincronizzando anche questa stazione.

Formato dei frame

Esistono 3 tipi di frame: **Dati**, **Controllo** e **Gestione**.
A livello di MAC sublayer[1], i frame di tipo "Dati" hanno la seguente struttura:

Otteti:	2	2	6	6	6	2	6	0÷2312	4
	Controllo*	Durata	Indirizzo 1	Indirizzo 2	Indirizzo 3	Numero	Indirizzo 4	**Dati**	CRC

Gli indirizzi sono 4, in quanto, oltre agli indirizzi delle stazioni di origine e di destinazione, sono presenti anche quelli degli AP di entrata ed uscita nelle comunicazioni fra celle differenti. Gli indirizzi sono tutti nel formato standard IEEE 802 a 48 bit; tramite una procedura di assegnazione globale[2] si garantisce che ogni interfaccia abbia un indirizzo univoco a livello mondiale, consentendo ad una stazione di muoversi da una LAN all'altra senza rischio di collisioni.
Il campo Durata consente, a tutte le stazioni che hanno ricevuto il frame, di prevedere per quanto tempo il mezzo rimarrà occupato.
Il campo Numero consente di numerare i frammenti. Dei 16 bit disponibili, 12 identificano il frame e 4 identificano il frammento.
Il campo Controllo, a sua volta, è suddiviso in 11 sottocampi:



Il primo ottetto è suddiviso in 3 campi con il seguente significato:

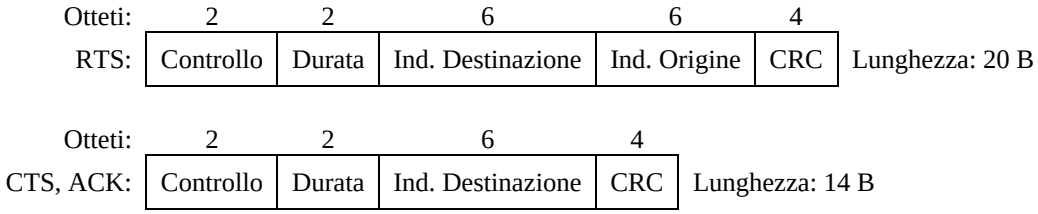
- **Ver.** - Versione dello standard IEEE 802.11
- **Tipo** - Specifica il tipo del frame: Gestione, Controllo o Dati
- **Sottotipo** - RTS, CTS, ACK, ecc.

Gli 8 flag che seguono, quando impostati ad 1, hanno il seguente significato:

- **Al DS -** il frame è diretto al sistema di distribuzione
- **Dal DS** - il frame proviene dal sistema di distribuzione
- **Altri Frammenti** - seguono altri frammenti appartenenti allo stesso frame
- **Ripetizione** - questo frammento è la ripetizione di un frammento precedentemente trasmesso
- **Risparmio energia** - al termine del frame l'interfaccia della stazione entrerà nella modalità di basso consumo
- **Altri Frame** - il trasmettitore ha altri frame per il ricevitore
- **WEP** - il campo *Dati* è stato crittografato con l'algoritmo WEP (Wired Equivalent Privacy)
- **Ordinati** - frammento appartenente alla classe di servizio *StrictlyOrdered*

[1] Lo strato fisico prevede altri campi, dipendenti dalla tecnica di modulazione e legati alla sincronizzazione.
[2] Un'impresa che voglia produrre nuove interfacce deve richiedere ad un ente centrale un blocco di indirizzi da assegnare alle proprie schede.

I frame di tipo "Gestione" hanno un formato simile, ma, essendo confinati ad una singola cella, richiedono solo 3 indirizzi. I frame di "Controllo" sono ancora più brevi, richiedendo solo 1 o 2 indirizzi, e non contenendo i campi *Dati* e *Numero*. Quelli più importanti hanno la seguente struttura e lunghezza:



Servizi

Ogni LAN wireless conforme allo standard 802.11 deve fornire i seguenti nove servizi:

1. **Associazione** - Appena una stazione entra nel raggio d'azione di un AP, invoca questo servizio per informare la stazione base della sua presenza e delle sue necessità.
2. **Dissociazione** - Sia le stazioni che gli AP possono terminare una precedente associazione.
3. **Riassociazione** - Una stazione in moto può trasferire il controllo da un AP all'altro.
4. **Distribuzione** - L'AP smista i frame che lo raggiungono verso le stazioni della propria cella (via radio) o verso gli altri AP, attraverso il sistema di distribuzione.
5. **Integrazione** - Questo servizio gestisce la traduzione dei frame 802.11 verso altri formati.
6. **Autenticazione** - Una stazione deve dimostrare di essere autorizzata ad usufruire del servizio di trasmissione.
7. **Deautenticazione** - Una stazione che voglia abbandonare la rete deve "deautenticarsi" e "dissociarsi".
8. **Segretezza** - I dati trasmessi via radio possono essere ascoltati da chiunque si trovi all'interno dell'area di diffusione. Questo servizio gestisce la crittografazione dei frame attraverso l'algoritmo RC4 (concesso dalla RSA).
9. **Trasmissione** - Scambio di frame, fra due stazioni, a livello di MAC sublayer.

I primi 5 sono chiamati "servizi di distribuzione" e sono forniti dall'AP, gli ultimi 4 sono i "servizi di stazione" e devono essere assolti da tutte le stazioni.

Bibliografia

[1] ANSI/IEEE Std 802.11, 1999 Edition; pp. 1-97

[2] A. S. Tanenbaum - *Computer Networks* - Upper Saddle River, NJ: Prentice Hall, 2003; pp. 68-71, pp. 292-304, pp. 100-106, pp. 267-270, pp. 553-555, pp. 166-169

[3] T. S. Rappaport - *Wireless Communications: principles and practice* - Upper Saddle River, NJ: Prentice Hall, 2002; pp. 46-54, pp. 591-593

[4] W. Stallings - *Local and Metropolitan Area Networks* - Upper Saddle River, NJ: Prentice Hall, 1997; pp. 376-382

Marco Benvegnù (hiforce@gmx.it)
http://web.tiscali.it/hiforce/
14 Marzo 2003