Appunti del corso di
Sistemi di elaborazione: Reti I

PROF. G. BONGIOVANNI

4) Il sottolivello MAC (Medium Access Control)

Come già chiarito, le reti sono divise in due categorie: ***punto a punto*** e ***broadcast***.

Nelle reti broadcast il problema principale è decidere quale elaboratore (detto anche ***stazione***) ha diritto di usare il mezzo trasmissivo quando c'è competizione (qui non si può alzare la mano per chiedere la parola!). Si deve evitare che molte stazioni trasmettano contemporaneamente, perché i relativi segnali si disturberebbero a vicenda.

I protocolli per decidere chi è il prossimo a trasmettere su un canale broadcast (detto anche ***multiaccess channel*** o ***random access channel***) appartengono ad un sottolivello del livello data link, detto ***sottolivello MAC***.

Essi sono usati sopratutto nelle LAN, ma anche nelle parti di WAN basate su satelliti.

Il problema principale è come allocare il canale ai vari utenti in competizione. Ci sono due meccanismi fondamentali:

- ***allocazione statica***, che viene decisa in anticipo;
- ***allocazione dinamica***, che si adatta alle esigenze di ogni momento.

L'allocazione statica prevede la suddivisione del canale fra gli N utenti, ciascuno dei quali riceve di conseguenza una frazione della banda totale. Si può fare, ad esempio, con tecniche quali FDM, allocando a ciascun utente una banda di frequenze distinta da quella degli altri utenti. Ciò va bene se il numero di utenti non varia rapidamente e se tutti trasmettono con un data rate più o meno costante, però in genere comporta vari problemi:

- si verifica uno spreco di banda quando uno o più utenti non trasmettono;
- poiché il traffico è in generale molto ***bursty***, i picchi che si verificano non possono essere gestiti solamente con la sottobanda allocata.

Viceversa, l'allocazione dinamica cerca di adeguarsi alle esigenze trasmissive, in modo da soddisfarle al meglio. Ci sono alcune assunzioni da fare:

1. ***modello a stazioni***: ci sono N stazioni indipendenti, ognuna delle quali genera nuovi frame per la trasmissione. La probabilità di generare un frame in un intervallo di tempo T è uguale a pT, dove p è una costante e rappresenta il tasso d'arrivo dei nuovi frame. Quando un frame è generato, la stazione si blocca finché esso non è trasmesso;
2. ***singolo canale***: un singolo canale, e null'altro, è disponibile per le comunicazioni; tutte le stazioni vi possono trasmettere e da esso possono ricevere, e tutte sono ad uguale livello;

3. ***collisioni***: se due frame vengono trasmessi contemporaneamente, si sovrappongono ed il segnale risultante è rovinato (si verifica collisione):
    - tutte le stazioni possono rilevare la collisione;
    - i frame devono essere ritrasmessi;
    - non ci sono altri tipi di errori;
4. ***tempo***: può essere gestito in due modi:
    - ***continuous time***: la trasmissione di un frame può iniziare in un qualunque istante;
    - ***slotted time***: il tempo è diviso in intervalli discreti (***slot***). Uno slot può contenere 0, 1 oppure più di un frame. Ciò corrisponde ad uno slot vuoto, ad uno slot con un frame e ad uno slot in cui si verifica una collisione. La trasmissione può iniziare solo all'inizio di uno slot;
5. ***ascolto del canale***: ci sono due possibilità,
    - ***carrier sense*** (tipico delle LAN): le stazioni, prima di trasmettere, ascoltano il canale; se è occupato non cercano di trasmettere;
    - ***no carrier sense*** (tipico dei canali via satellite, nei quali vi è un elevato round trip time): le stazioni non ascoltano, trasmettono senz'altro; si preoccuperanno dopo di vedere se c'è stata una collisione.

4.1) Protocollo ALOHA

Nacque negli anni '70 per collegare tra loro, tramite radio al suolo, gli elaboratori sparsi nelle isole Hawaii.

Esistono due versioni, ***Pure Aloha*** e ***Slotted Aloha***.

Nel ***Pure Aloha*** le stazioni trasmettono quando vogliono, però durante la trasmissione ascoltano il canale e confrontano ciò che ricevono con ciò che hanno spedito.

Dunque, se si verifica una collisione se ne accorgono, e in tal caso, dopo aver lasciato passare una quantità di tempo casuale, ritrasmettono il frame. La scelta di attendere per una quantità di tempo casuale discende dal fatto che altrimenti una collisione ne ricrea infinite altre.

Qual'è l'efficenza dello schema Aloha puro, in queste circostanze caotiche?

Definiamo come ***frame time*** il tempo necessario alla trasmissione di un frame, che ha lunghezza fissa. Supponiamo che vengano complessivamente generati dei frame con una distribuzione di Poisson avente media di S frame per frame time.

Ovviamente, se S >= 1, ci saranno quasi sempre collisioni. Per un throughput ragionevole ci aspettiamo 0 < S < 1. Purtroppo, oltre ai frame nuovi, ci sono anche quelli relativi alla ritrasmissione causata da collisioni precedenti.

Supponiamo che la distribuzione di tutti i frame (vecchi e nuovi) sia anch'essa di Poisson, con valor medio pari a G frame per frame time.

A basso carico ci aspettiamo poche collisioni, quindi G è circa uguale ad S. Ad alto carico invece avremo più collisioni, per cui G sarà maggiore di S.

In ogni caso, sotto qualunque condizione di carico il ***throughput*** (cioé la ***quantità di pacchetti che arrivano a destinazione***) è uguale al carico offerto moltiplicato per la probabilità che la trasmissione abbia successo, ossia:

Throughput = G*P(0)

dove P(0) è la probabilità che un frame non soffra collisioni.

Per calcolare il throughput effettivo, e quindi l'efficienza, ottenibile col protocollo Pure Aloha, si devono fare due considerazioni.

La prima è che la probabilità di generare k frame durante un intervallo di tempo pari ad un frame time è data, per la distribuzione di Poisson sopra definita (avente, si ricordi, valor medio pari a G frame per frame time) dalla relazione:

$$P(k) = \frac{G^k e^{-G}}{k!}$$

Dunque, la probabilità che si generino zero frame in un intervallo di tempo pari ad un frame time è pari a

$P(0) = e^{-G}$.

La seconda considerazione è che il ***periodo di vulnerabilità*** di un frame, cioé l'intervallo di tempo nel quale esso è a rischio di collisioni, è lungo 2 volte il frame time.

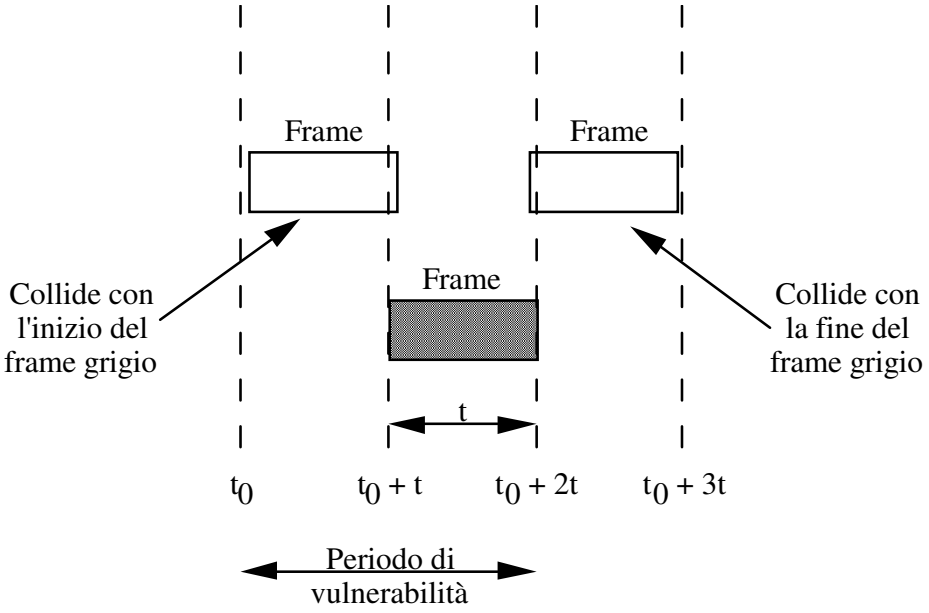

Figura 4-1: Il periodo di vulnerabilità

In tale periodo vengono generati mediamente 2G frame. Di conseguenza, la probabilità che non si generino nuovi frame per tutto il periodo di vulnerabilità di un frame è:

$$\mathbf{P(0) = e^{-2G}}$$

Utilizzando tale probabilità nella relazione vista sopra per il throughput, otteniamo la stima del throughput ragggiungibile col protocollo Pure Aloha, che è

$$\mathbf{Throughput = Ge^{-2G}}$$

ed ha la seguente forma:

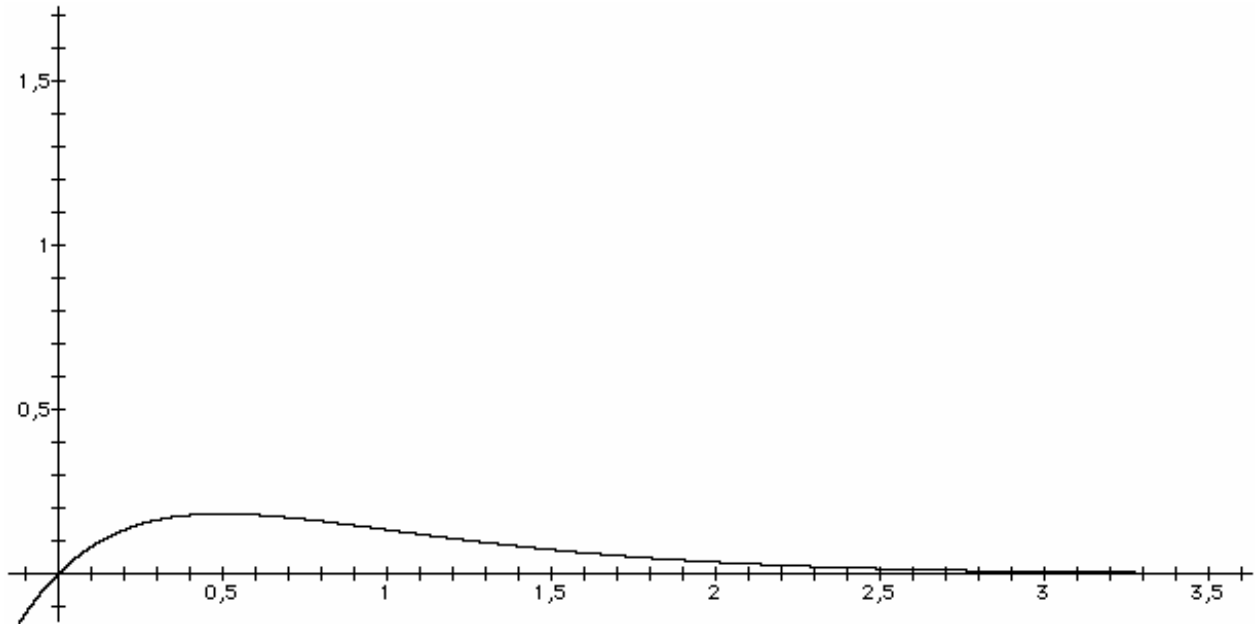

Figura 4-2: Throughput del protocollo Pure Aloha

Il massimo throughput è 0,184, cioé meno del 20% (due frame su 10 slot) in corrispondenza di un carico G pari a 0,5 frame per frame time.

Un modo per aumentare l'efficienza di Aloha (Roberts, 1972) consiste nel dividere il tempo in intervalli discreti, ciascuno corrispondente ad un frame time. Ovviamente gli utenti devono essere d'accordo nel confine fra gli intervalli, e ciò può essere fatto facendo emettere da una attrezzatura speciale un breve segnale all'inizio di ogni intervallo.

Le stazioni non possono iniziare a trasmettere quando vogliono, ma solo all'inizio dell'intervallo. Questo protocollo, che prende il nome di Slotted Aloha, dimezza il periodo di vulnerabilità che diviene uguale ad un solo frame time.

In tale periodo vengono generati mediamente G frame, per cui la probabilità che non si generino nuovi frame per tutto il periodo di vulnerabilità di un frame è:

$$\mathbf{P(0) = e^{-G}}$$

Utilizzando tale probabilità nella relazione vista precedentemente per il throughput, otteniamo la stima del throughput ragggiungibile col protocollo Slotted Aloha, che è:

$$\mathbf{Throughput = Ge^{-G}}$$

ed ha la seguente forma:

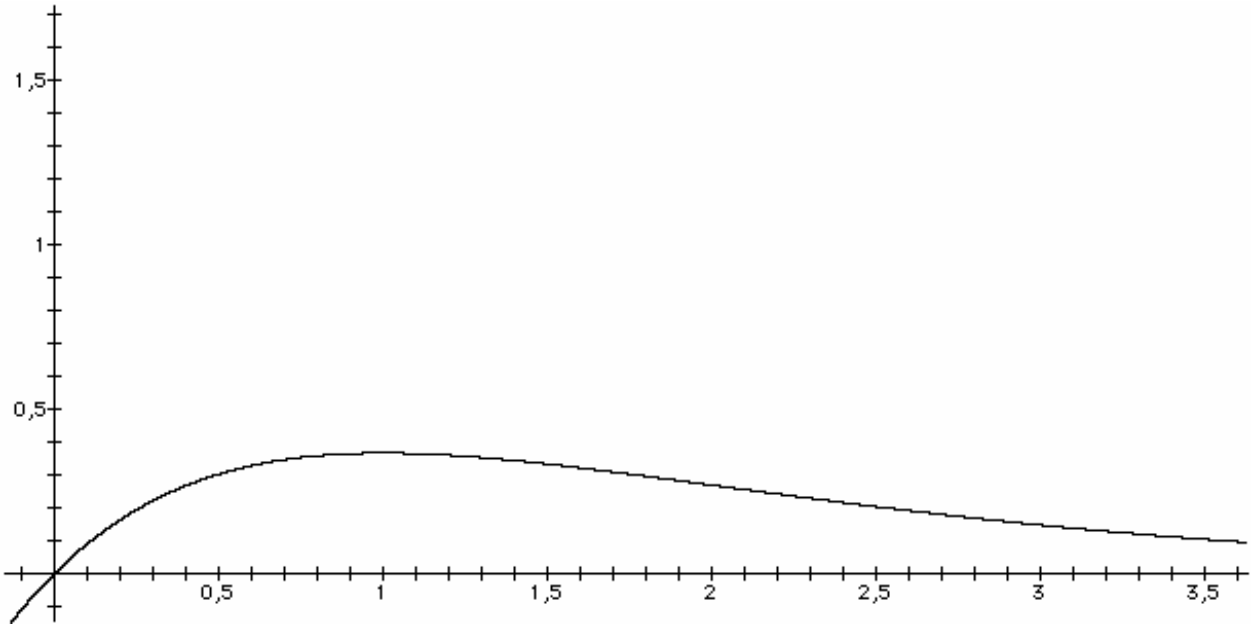

Figura 4-3: Throughput del protocollo Slotted Aloha

Il massimo throughput è 0,368, in corrispondenza di un carico G pari a 1 frame per frame time.

4.2) Protocolli CSMA (Carrier Sense Multiple Access)

Anche Slotted Aloha ha una bassa efficienza, il che d'altronde è comprensibile visto che le stazioni trasmettono senza preoccuparsi se il canale è libero.

Nelle reti locali invece le stazioni possono ascoltare il canale e regolarsi di conseguenza, ottenendo un'efficienza molto più alta. I protocolli nei quali le stazioni ascoltano il canale prima di iniziare a trasmettere si dicono ***carrier sense***.

Ci sono vari tipi di protocolli carrier sense:

- ***1-persistent***
  - Quando una stazione deve trasmettere, ascolta il canale:
    - se è occupato, aspetta finché si libera e quindi trasmette;
    - se è libero, trasmette (con probabilità 1, da cui il nome).

    - Se avviene una collisione, la stazione aspetta un tempo random e riprova tutto da capo.
    - Problemi:
        - una stazione A trasmette, e prima che il suo segnale arrivi a B anche B inizia a trasmette, dunque si verifica una collisione. Più alto è il tempo di propagazione fra A e B e più grave è il fenomeno;
        - A e B ascoltano contemporaneamente durante la trasmissione di C, e non appena quest'ultima termina iniziano entrambe a trasmettere: anche in questo caso si verifica una collisione.
- ***Nonpersistent***
    - Quando una stazione deve trasmettere, ascolta il canale:
        - se è occupato, invece di trasmettere non appena si libera come in 1-persistent la stazione aspetta comunque un tempo random e ripete tutto il procedimento da capo;
        - se è libero, si comporta come in 1-persistent.
    - Intuitivamente, ci si aspettano maggiori ritardi prima di riuscire a trasmettere un frame e meno collisioni rispetto a 1-persistent.
- ***P-persistent*** (si applica a canali slotted)
    - Quando una stazione deve trasmettere, ascolta il canale:
        - se è occupato, aspetta il prossimo slot e ricomincia da capo;
        - se è libero:
            - con probabilità p trasmette subito;
            - con probabilità 1 - p aspetta il prossimo slot; se anch'esso è libero, riapplica tale procedimento;
    - Il processo si ripete finché:
        - il frame è trasmesso, oppure
        - qualcun altro ha iniziato a trasmettere. In questo caso la stazione si comporta come in una collisione: aspetta un tempo random e ricomincia da capo.
    - Intuitivamente, al diminuire di p ci si aspettano crescenti ritardi prima di riuscire a trasmettere un frame ed una progressiva diminuzione delle collisioni.

4.3) Protocolli CSMA/CD (CSMA with Collision Detection)

Un ulteriore miglioramento si ha se le stazioni interrompono la loro trasmissione non appena rilevano una collisione, invece di portarla a termine.

Rilevare la collisione è un processo analogico: si ascolta il canale durante la propria trasmissione, e se la potenza del segnale ricevuto è superiore a quella trasmessa si scopre la collisione.

Quando si verifica una collisione, la stazione aspetta una quantità casuale di tempo e riprova a trasmettere.

Posto uguale a T il tempo di propagazione del segnale da un capo all'altro della rete, è necessario che trascorra un tempo pari a 2T perché una stazione possa essere sicura di rilevare una collisione.

Infatti, se una stazione A posta ad una estremità della rete inizia a trasmettere al tempo t_0, il suo segnale arriva a B (posta all'altra estremità della rete) dopo al tempo $t_0 + T$; se un attimo prima di tale istante anche B inizia a trasmettere, la collisione conseguente viene rilevata da B quasi immediatamente, ma impiega una ulteriore quantità T di tempo per giungere ad A, che la può quindi rilevare solo un attimo prima dell'istante $t_0 + 2T$.

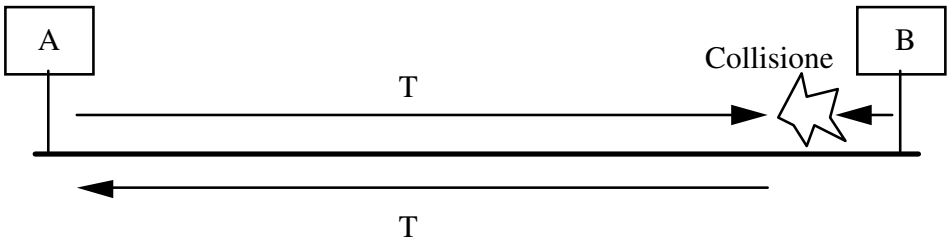

Figura 4-4: Rilevazione di una collisione

Il modello concettuale che si utilizza è il seguente:

- vi è un'alternanza di periodi di ***contesa***, di ***trasmissione*** e di ***inattività***;
- il periodo di contesa è modellato come uno Slotted Aloha con slot di durata 2T: a titolo di esempio, per un cavo di 1 km T vale circa 5 microsecondi.

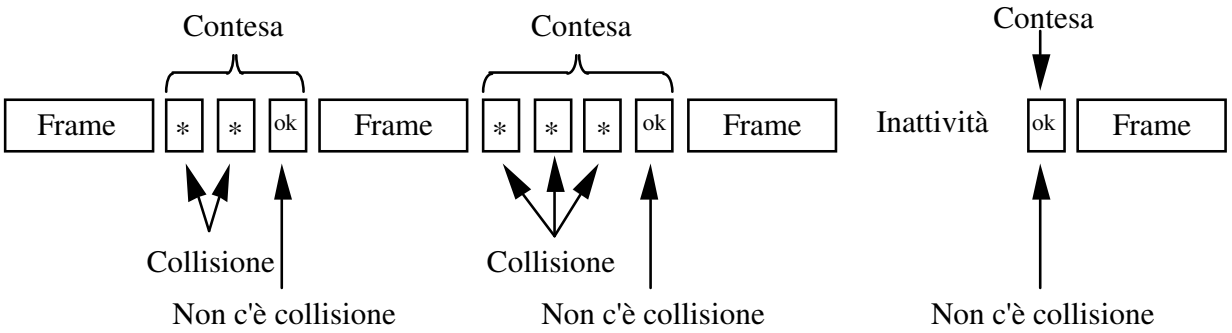

Figura 4-5: Modello concettuale per CSMA/CD

4.4) Le reti ad anello

Una ***rete ad anello*** consiste di una collezione di interfacce di rete, collegate a coppie da linee punto a punto:

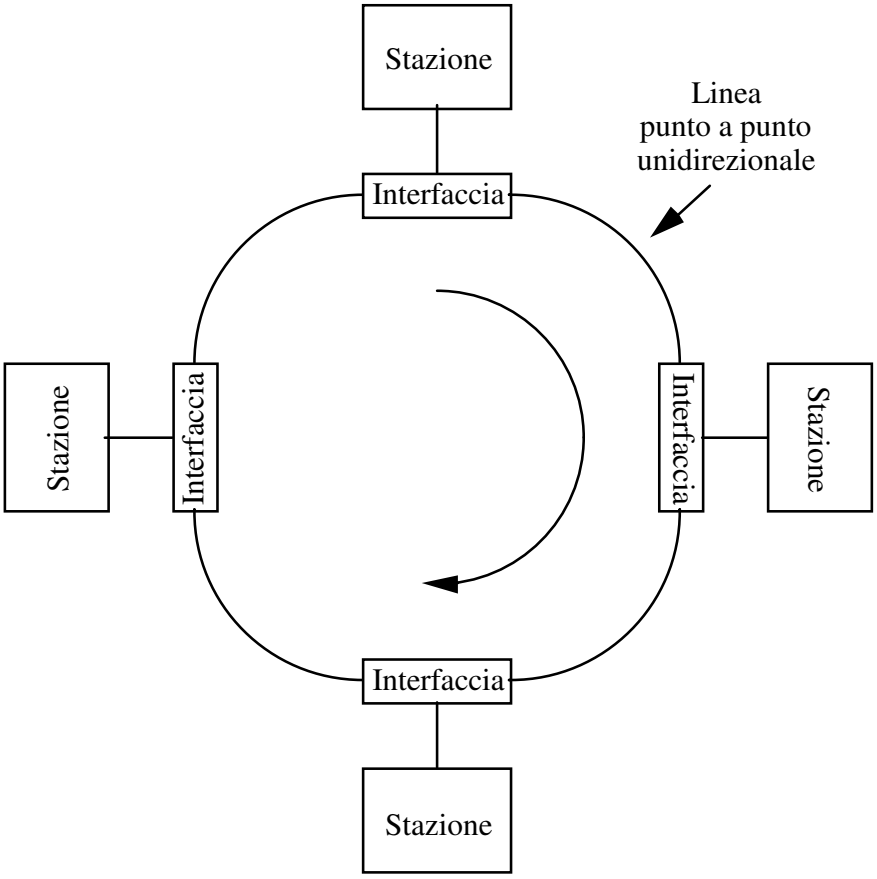

Figura 4-6: Struttura di una rete ad anello

Le reti ad anello hanno diverse attrattive:

- non sono reti basate su un mezzo trasmissivo broadcast;
- non c'è una significativa componente analogica per la rilevazione delle collisioni (che non possono verificarsi);
- l'anello è intrinsecamente equo.

Ogni bit che arriva all'interfaccia è copiato in un buffer interno, poi rigenerato e ritrasmesso sul ring. Può essere modificato prima di essere ritrasmesso.

L'interfaccia di rete può operare in due diverse modalità, ***listen mode*** e ***transmit mode***:

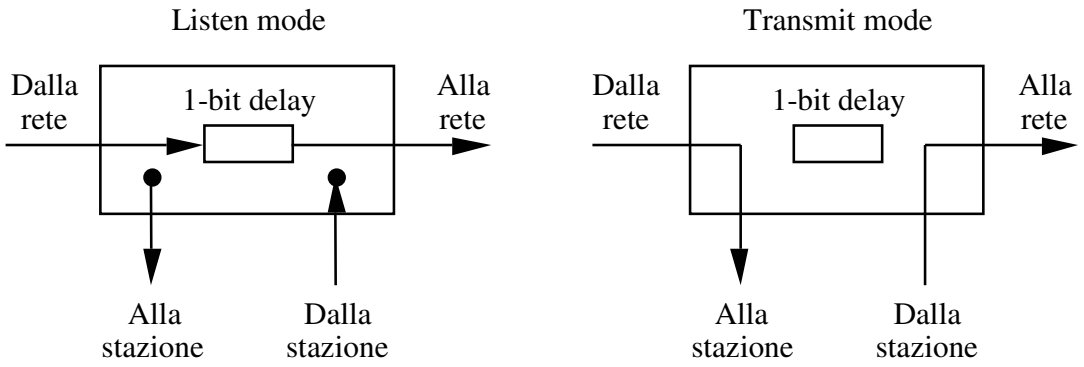

Figura 4-7: Modalità di funzionamento dell'interfaccia di rete

In listen mode i bit in ingresso vengono copiati nel buffer interno (dove possono essere anche modificati) e quindi ritrasmessi con un ritardo di un bit (***1-bit delay***).

In transmit mode l'anello è aperto, e i bit in arrivo vengono rimossi; nuovi bit vengono trasmessi sull'anello.

Una speciale configurazione binaria, detta ***token*** (***gettone***) circola in continuazione se nessuno vuole trasmettere.

Quando una stazione vuole trasmettere, deve:
1. aspettare che arrivi il token (in listen mode);
2. rimuoverlo dal ring (in listen mode, vedremo come);
3. trasmettere i dati (in transmit mode);
4. rigenerare il token (in transmit mode);
5. rimettersi in listen mode.

Poiché c'è un solo token, questo meccanismo risolve senza conflitti il problema dell'accesso al mezzo.

Alcune considerazioni sono degne di nota:
- il token deve essere contenuto per intero sull'anello, il che non è così ovvio come sembra (qual'è la lunghezza di un bit?);
- un frame, invece, non è necessario che ci stia tutto sull'anello (che in trasmissione è aperto), quindi non ci sono limiti alla dimensione dei frame;
- in genere esiste un tempo massimo entro il quale, una volta preso il token, si deve completare la trasmissione; ciò permette di ottenere una schedulazione round-robin delle trasmissioni;

- quando tutte le stazioni hanno qualcosa da trasmettere, l'efficienza si avvicina al 100%;
- viceversa, quando non c'è traffico, una stazione deve attendere un pò più che in CSMA/CD per trasmettere (mediamente dovrà attendere un tempo pari a quello di attraversamento di mezzo anello, per ricevere il token).

La velocità di propagazione del segnale nel rame è circa 200 metri per microsecondo. Con un data rate (ad esempio) di 1 Mbps, si genera un bit al microsecondo. Dunque, un bit è lungo in tal caso circa 200 metri, per cui per contenere 10 bit un anello dovrebbe essere lungo almeno 2 km.

In realtà sul ring trovano posto:
- x bit sull'anello, in funzione della sua lunghezza totale;
- y bit nei buffer delle interfacce delle y stazioni presenti (1 bit delay).

In definitiva, è necessario che x + y sia maggiore del numero di bit del token. Ciò significa che, a seconda delle caratteristiche dimensionali della rete in questione, può essere necessario ricavare un ritardo addizionale, sotto forma di buffer aggiuntivi, in una stazione (che ha un ruolo particolare, quello di ***monitor dell'anello***).

4.5) Le reti senza fili

Al crescere della diffusione di apparecchiature di calcolo mobili (ad es. elaboratori portatili) è aumentata anche la richiesta di collegare tali dispositivi al mondo esterno, senza però fare uso di cavi che ne impedirebbero di fatto la mobilità. La risposta a tale esigenza viene dalla comunicazione senza fili, basata sull'uso di onde elettromagnetiche.

Un sistema di stazioni mobili capaci di comunicare via radio costituisce una ***LAN senza fili*** (***wireless LAN*** o ***WLAN***).

Una LAN senza fili può essere costituita in due modi diversi, a seconda che sia disponibile oppure no una (o più di una) apparecchiatura detta ***stazione base*** (***base station***).

Se presente, la stazione base è l'apparecchiatura alle quale si collegano le stazioni mobili. A sua volta, la stazione base è collegate ad una rete fissa attraverso la quale si realizza la comunicazione col mondo esterno. L'insieme di una stazione base e dei servizi da essa offerti alle stazioni mobili viene detto ***cella***.

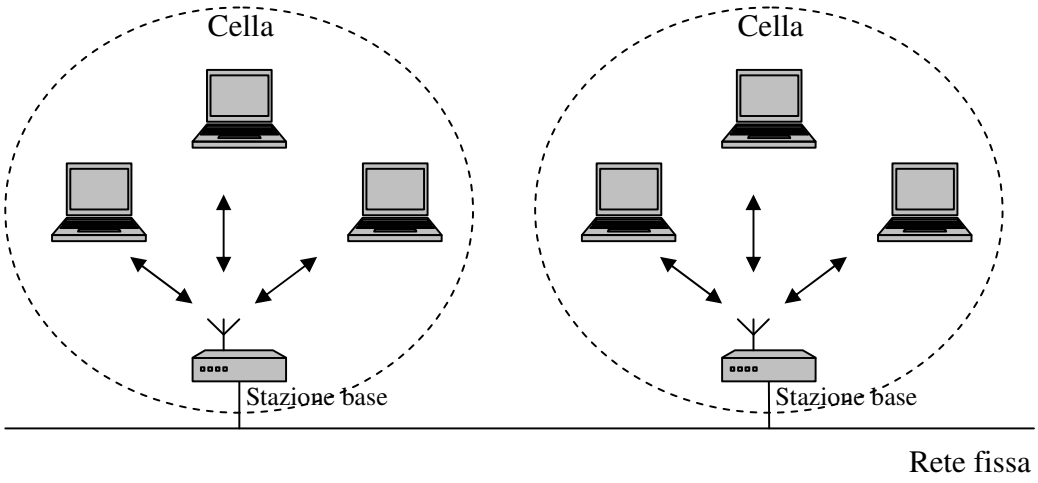

Figura 4-8: LAN senza fili con stazioni base

Nel caso in cui non sia disponibile una stazione base, le stazioni mobili comunicano esclusivamente fra di loro, senza collegamenti con una rete esterna. In questo caso si parla di ***rete ad-hoc*** (***ad-hoc network***).

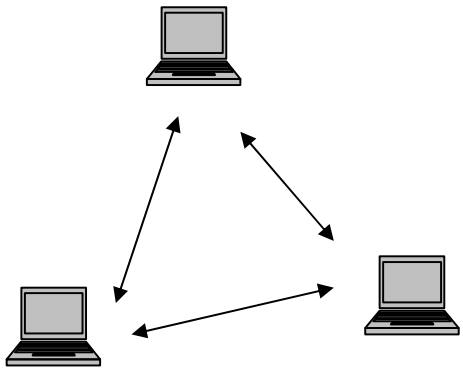

Figura 4-9: Una rete ad-hoc

Indipendentemente dal fatto che una WLAN sia dotata o meno di stazioni base, esistono numerosi problemi da risolvere, legati all'utilizzo della trasmissione senza fili:

- collisioni: devono essere predisposti appositi protocolli per gestirle;

- interferenze e riflessioni: vengono usate tecniche trasmissive a spettro distribuito, che ne minimizzano gli effetti;
- privacy: chiunque può intercettare una trasmissione radio, per cui vanno previsti meccanismi basati sulla crittografia per la protezione dei dati;
- mobilità degli utenti: una stazione mobile può spostarsi da una cella ad un'altra, per cui sono necessari meccanismi per gestire tale situazione (detta ***handover***).

4.5.1) Il problema della stazione nascosta e della stazione esposta

Ogni apparato trasmittente è caratterizzato da una ***portata***, dipendente dalla potenza trasmissiva impiegata, che è la distanza massima alla quale il segnale emesso può essere rilevato. Tutte le apparecchiature entro la portata di un apparato ricevono il segnale trasmesso da tale apparato, mentre quelle al di fuori di tale portata non lo ricevono.

Si consideri la figura seguente, nella quale sono mostrate 4 stazioni con le relative portate.

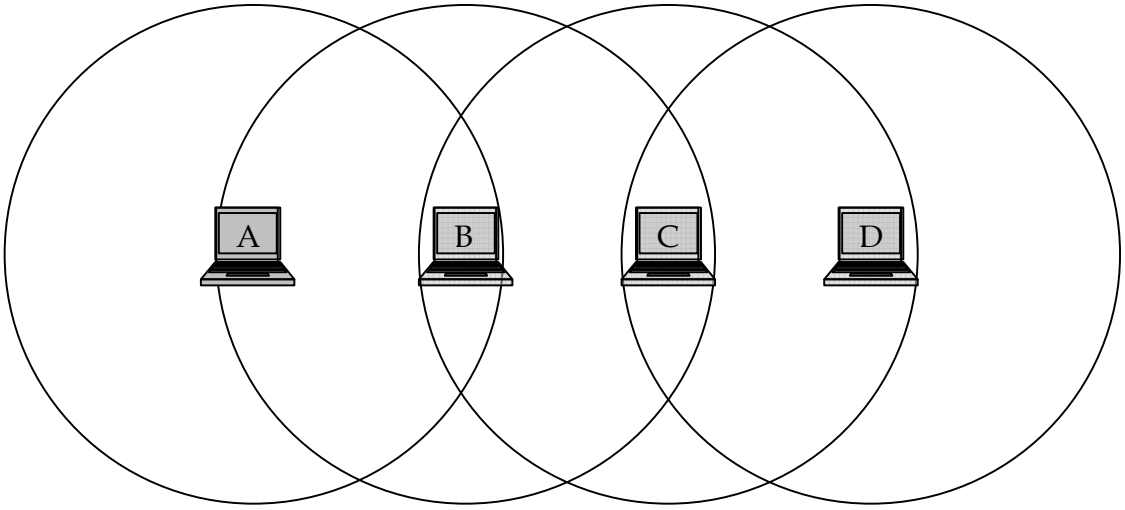

Figura 4-10: Stazioni mobili con le relative portate

Supponiamo ora che la stazione A voglia trasmettere a B. Come può decidere se trasmettere o no? Se A si basa sull'ascolto del canale, e trovandolo libero trasmette, non ha alcuna garanzia di successo, perché potrebbe essere in atto una trasmissione da parte di C. Il che porterebbe ad una collisione in B, raggiunta contemporaneamente dalle trasmissioni di A e C. Questo è il ***problema della stazione nascosta***.

Ora invece consideriamo la situazione in cui B sta trasmettendo ad A, e C desidera trasmettere a D. Ascoltando il canale, C deduce che esso è occupato (C sente la trasmissione

di B) e quindi non inizierà a trasmettere. Invece potrebbe farlo, perché la trasmissione di B non raggiunge D e quindi non provoca una collisione. Questo è il ***problema della stazione esposta***.

I due problemi sopra esposti derivano essenzialmente dal fatto che la stazione trasmittente non ha modo di sapere quale sia la situazione del canale nei pressi della stazione ricevente, e quindi protocolli CSMA/CD (adatti al caso in cui una trasmissione raggiunge *tutte* le stazioni) in questo ambito non funzionano.

4.5.2) Protocolli MACA e MACAW

Una prima soluzione è rappresentata dal protocollo ***MACA*** (***Multiple Access with Collision Avoidance***), nel quale non vi è ascolto del canale (infatti manca CS nella sigla) e si cerca di evitare le collisioni anziché rilevarle.

Non si impiega l'ascolto del canale sulla base delle seguenti considerazioni:
- il canale libero per il trasmettitore non significa che lo sia anche per il ricevitore (e quindi non è detto che la trasmissione abbia successo: problema della stazione nascosta);
- il canale occupato per il trasmettitore non significa che lo sia anche per il ricevitore (e quindi non è detto che la trasmissione non sia possibile: problema della stazione esposta);
- nell'ambito delle trasmissioni radio apparecchiature full duplex, in grado di ricevere e trasmettere contemporaneamente, sono molto costose da realizzare.

L'idea di fondo è semplice: il trasmettitore invia un breve messaggio al ricevitore chiedendogli l'autorizzazione a trasmettere. Il ricevitore, se può accettare la trasmissione, risponde con messaggio di via libera. Solo se riceve tale messaggio il trasmettitore inizia ad inviare i dati.

Il funzionamento è il seguente:
- A invia a B un piccolo frame (30 byte) chiamato ***RTS*** (***Request To Send***), contenente la lunghezza del frame dati vero e proprio che dovrà essere trasmesso;
- B, se non è impegnato nella ricezione di altri dati, risponde ad A con un altro piccolo frame, chiamato ***CTS*** (***Clear to Send***) che lo autorizza a trasmettere. Anche il frame CTS riporta la lunghezza del frame dati che verrà trasmesso da A, ricopiata dal frame RTS.

Le altre stazioni si comportano nel seguente modo:
- Tutte le stazioni che ricevono solo il frame RTS (situate quindi entro la portata di A ma non entro quella di B) devono rimanere in silenzio per un tempo che consenta al frame CTS di raggiungere A, dopodiché possono trasmettere;

- Tutte le stazioni che ricevono solo il frame CTS (situate dunque entro la portata di B ma non entro quella di A) devono rimanere in silenzio per il tempo necessario alla trasmissione del frame dati (la cui lunghezza trovano nel frame CTS);
- Le stazioni che ricevono sia il frame RTS che il CTS (situate entro la portata sia di A che di B) applicano ambedue le regole sopra viste.

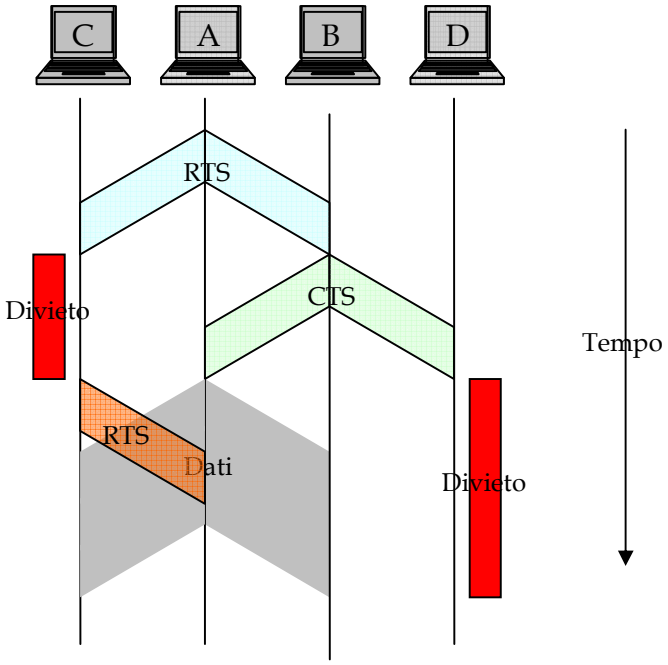

Figura 4-11: MACA: RST – CTS - Dati

Si noti quanto segue: le stazioni fuori dalla portata del ricevitore non ricevono il suo CTS e dunque non sanno se la trasmissione del frame avrà luogo o no; di conseguenza potrebbero inviare ad A degli RTS durante la sua trasmissione (RTS color arancio in figura). Tali RTS non causano collisioni (A è in trasmissione e non in ricezione), ma rimangono senza risposta e quindi fanno crescere il numero di insuccessi e di conseguenza l'intervallo di tempo da attendere prima di riprovare.

Nonostante tutte le precauzioni prese, le collisioni possono ugualmente avvenire: ad esempio due stazioni A e B, che non si sentono a vicenda, inviano un RTS ad una terza stazione C che si trova a portata di entrambe: in C si verifica una collisione. Oppure una stazione A invia un RTS a C mentre esso viene raggiunto da un CTS originato da una stazione (B nella figura) che si trova fuori dalla portata di A. Di nuovo, in C si verifica una collisione.

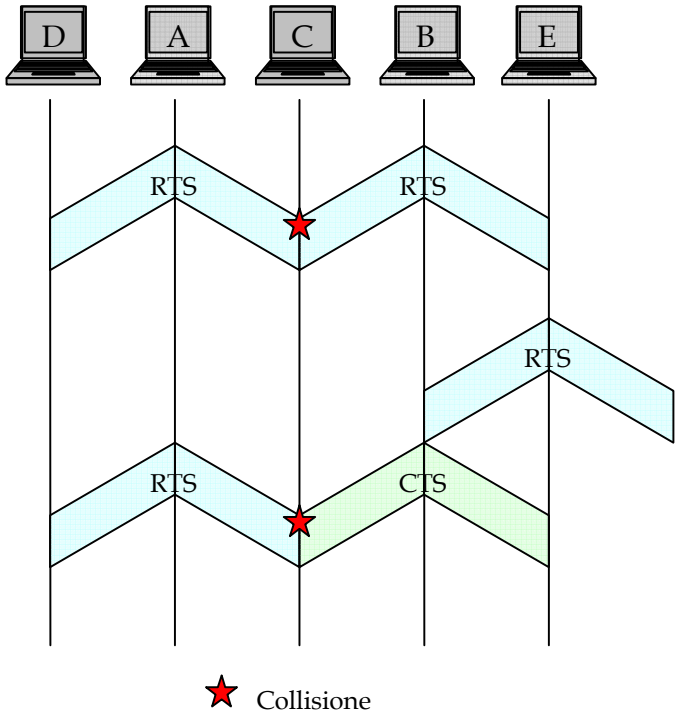

Figura 4-12: Collisioni

Chi ha trasmesso un RTS si accorge se esso provoca una collisione perché non riceve il corrispondente CTS. In tal caso il trasmettitore attende un tempo casuale, che aumenta al crescere del numero di collisioni, e riprova.

Va comunque notato che le collisioni relative ai soli frame RTS e CTS, che sono molto più piccoli dei frame dati, rappresentano un fenomeno meno grave delle collisioni che coinvolgono gli interi frame dati. In MACA queste ultime non possono avvenire.

Una successiva versione del protocollo, chiamata ***MACAW*** (***MACA per Wireless***), introduce alcune ulteriori migliorie, fra le quali:

- Invio di un breve frame ACK dal ricevitore al trasmettitore previa ricezione corretta del frame dati; questo permette di velocizzare la ritrasmissione (altrimenti sarebbero i livelli superiori a doversene occupare) del frame in caso di errori trasmissivi, non infrequenti nel caso dei mezzi wireless;
- Invio da parte del trasmettitore A, dopo la ricezione del CTS, di un breve frame ***DS*** (***Data Send***) contenente la dimensione del frame dati che sarà trasmesso, subito prima di iniziare a trasmettere il frame dati stesso. Questo permette alle stazioni fuori dalla portata del ricevitore di evitare di inviare ad A degli RTS prima che A abbia terminato la trasmissione.

- Accorta gestione distribuita degli algoritmi di aumento del tempo d'attesa dopo un insuccesso, in modo da garantire equità a tutte le stazioni.

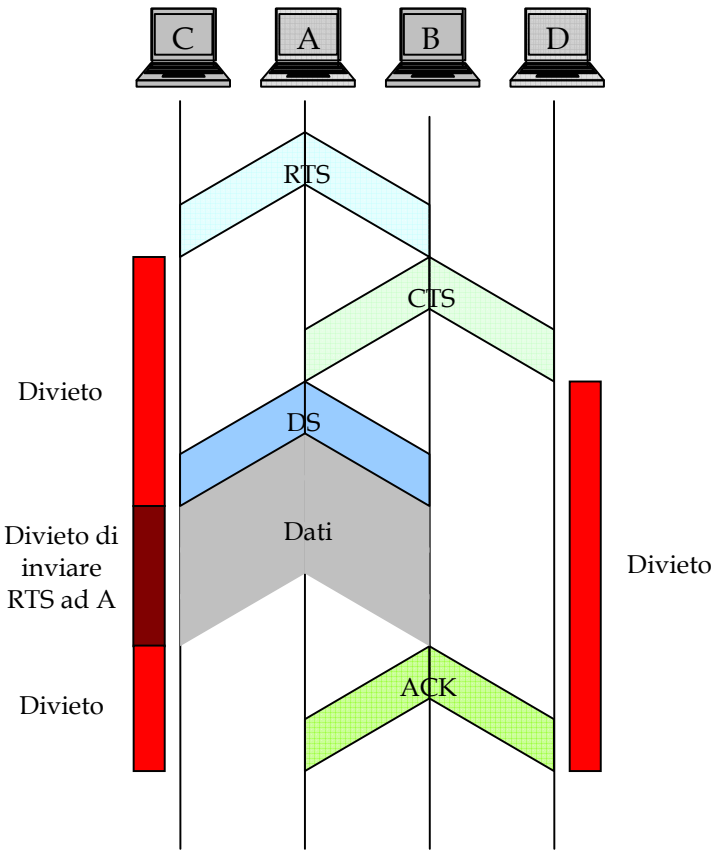

Figura 4-13: MACAW: RST – CTS – DS – Dati - ACK

Come abbiamo già detto, i protocolli MACA e MACAW non ascoltano il canale per decidere in merito alla trasmissione, ma si basano esclusivamente sullo scambio di messaggi di controllo. Tuttavia esiste un ulteriore protocollo, chiamato ***CSMA/CA*** (***Carrier Sense Multiple Access with Collision Avoidance***), utilizzato nello standard IEEE 802.11, che vedremo fra breve e che utilizza, a fianco di tecniche simili a quelle di MACAW, anche l'ascolto del canale prima di trasmettere.

4.6) Lo standard IEEE 802

IEEE ha prodotto diversi standard per le LAN, collettivamente noti come ***IEEE 802***. Essi includono gli standard per:

- ***Specifiche generali*** del progetto (802.1);
- ***Logical link control, LLC*** (802.2)
- ***CSMA/CD*** (802.3);
- ***token bus*** (802.4, destinato a LAN per automazione industriale);
- ***token ring*** (802.5);
- ***DQDB*** (802.6, destinato alle MAN);
- ***WLAN*** (802.11).

I vari standard differiscono a livello fisico e nel sottolivello MAC, ma sono compatibili a livello data link. Ciò è ottenuto separando dal resto, attraverso l'apposito standard LLC, la parte superiore del livello data link, che viene usata da tutti i protocolli standard del gruppo.

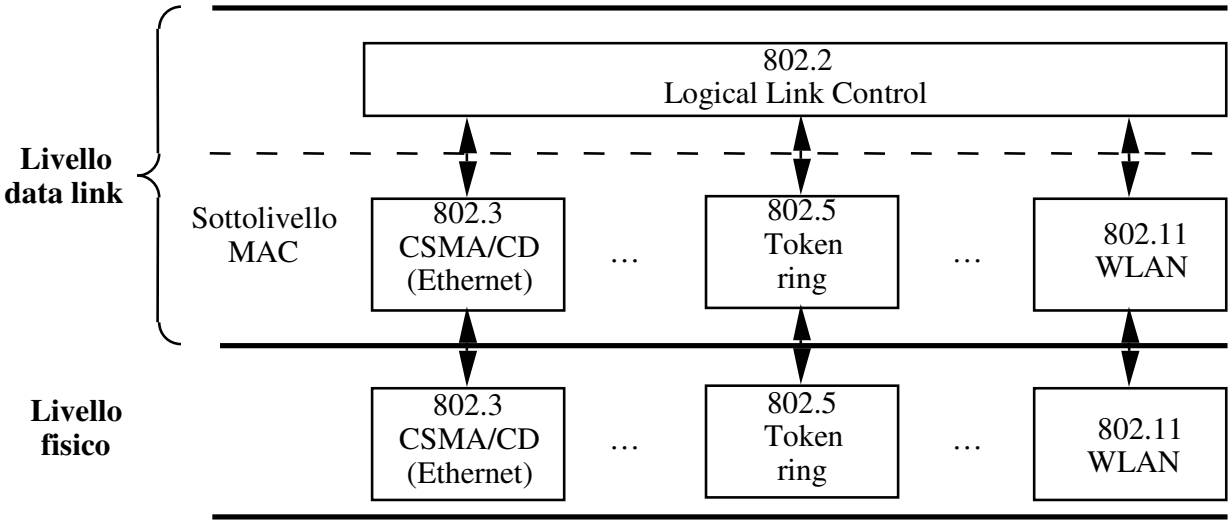

Figura 4-14: Lo standard IEEE 802

4.6.1) IEEE 802.3

E' lo standard per un protocollo CSMA/CD, di tipo 1-persistent, funzionante a 10Mbps.
802.3 è l'evoluzione dello standard ***Ethernet***, proposto da Xerox, DEC e INTEL sulla base dell'esperienza maturata con Aloha prima e nei laboratori Xerox PARC poi.
802.3 e Ethernet hanno alcune differenze, ma sono largamente compatibili.

4.6.1.1) Cablaggio

Sono previsti vari cablaggi:

- ***Thick ethernet***: è il primo storicamente; consiste di un cavo coassiale spesso (lo standard suggerisce il colore giallo per la guaina esterna).
  - Ufficialmente si chiama ***10Base5***, ossia:
    - 10 Mbps;
    - Baseband signaling;
    - 500 metri di lunghezza massima.
  - Possono essere installate 100 macchine su un segmento.
  - Ogni stazione contiene un'***interfaccia di rete*** (detta anche ***scheda ethernet***) che:
    - incapsula i dati del livello superiore;
    - gestisce il protocollo MAC;
    - codifica i dati da trasmettere;
    - in ricezione decapsula i dati, e li consegna al livello superiore (o lo informa dell'errore).
  - All'interfaccia di rete viene collegata una estremità di un corto cavo (pochi metri), detto ***transceiver drop cable***, all'altra estremità del quale è connesso un ***transceiver*** che si aggancia, con un dispositivo detto ***vampiro***, al cavo thick (che non viene interrotto).
  - Il transceiver contiene la circuiteria analogica per l'ascolto del canale e la rilevazione delle collisioni. Quando c'è una collisione, il transceiver informa l'interfaccia ed invia sulla rete uno speciale segnale di 32 bit (***jamming sequence***) per avvisare le altre stazioni, che così scartano quanto già ricevuto.
- ***Thin ethernet***: è un cavo coassiale più sottile, e si piega più facilmente.
  - Ufficialmente si chiama ***10Base2***, ossia:
    - 10 Mbps;
    - Baseband signaling;
    - 200 metri di lunghezza massima per un singolo segmento.
  - Possono essere installate 30 macchine su un segmento.
  - Di norma l'interfaccia di rete contiene anche il transceiver.

    - L'allaccio di una stazione alla rete avviene con una giunzione a T, alla quale sono collegati il cavo che porta alla stazione e due cavi thin che costituiscono una porzione del segmento. Le varie stazioni sono collegate in cascata (***daisy-chain***) sul segmento.
- Doppino telefonico:
    - Lo standard ***10BaseT*** (twisted) prevede il collegamento fra una sola coppia di stazioni.
    - La lunghezza massima è 100 metri (150 se il doppino è di classe 5).
    - Per connettere più di due stazioni serve un ***ripetitore multiporta*** (detto ***HUB***).

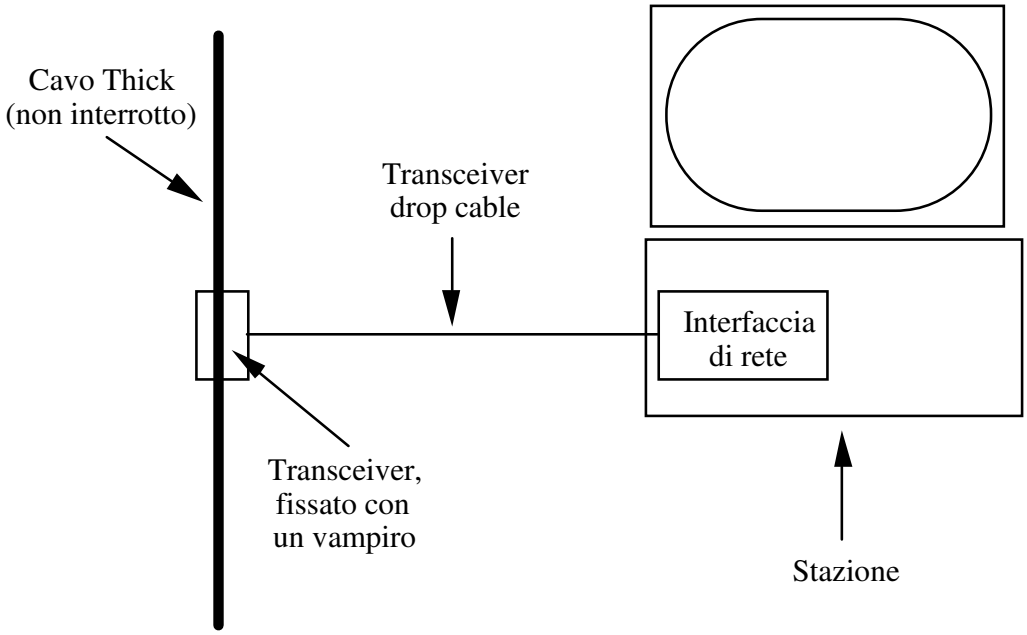

Figura 4-15: Cablaggio Ethernet cavo Thick

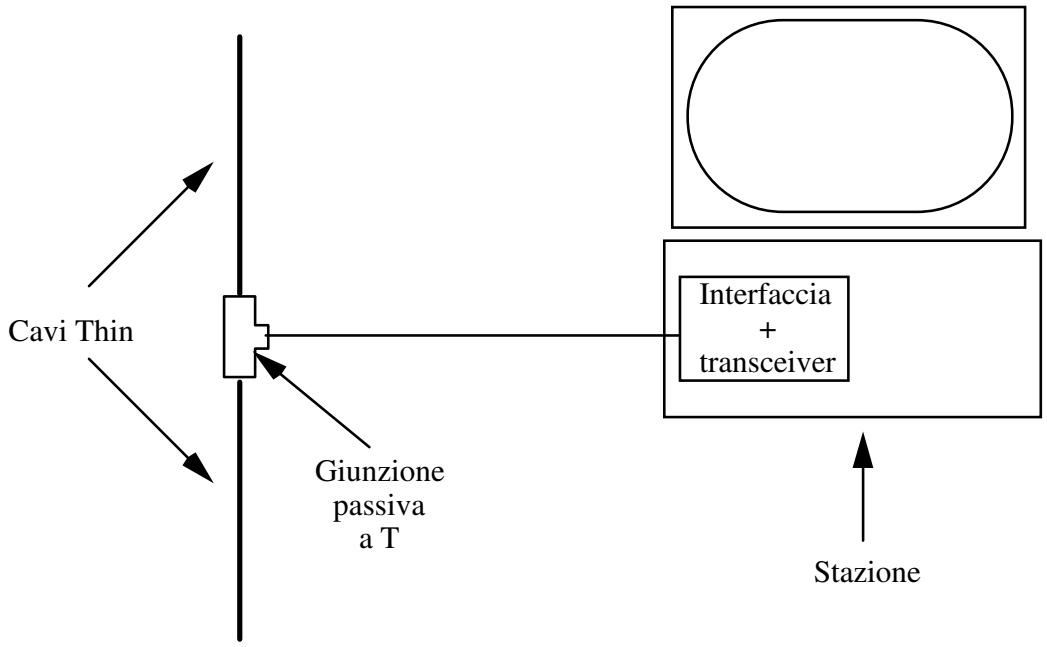

Figura 4-16: Cablaggio Ethernet tramite cavo Thin

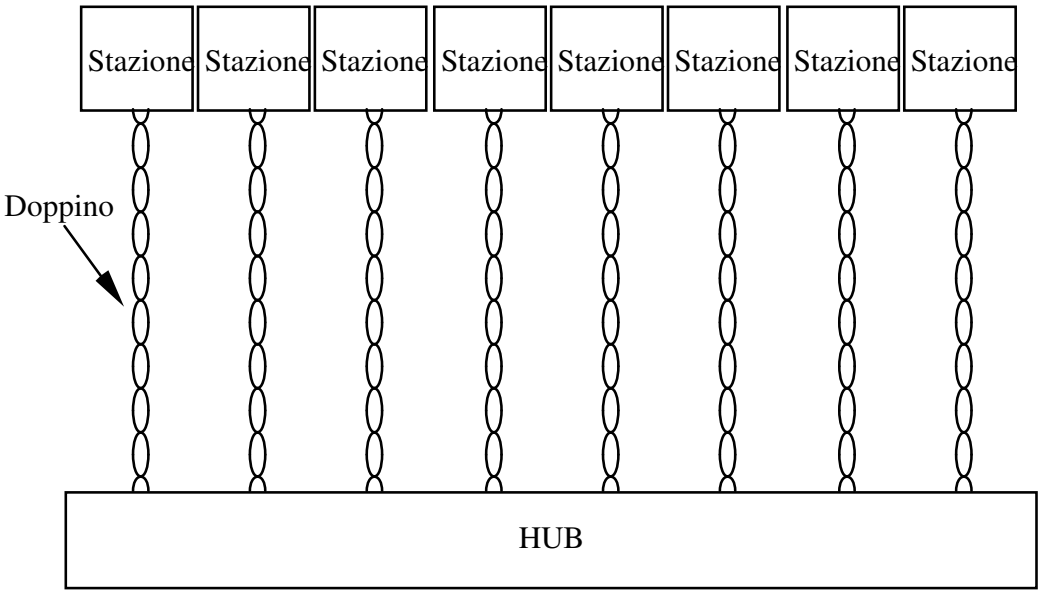

Figura 4-17: Cablaggio Ethernet tramite HUB

Un ripetitore è un dispositivo che opera a livello uno (fisico): riceve il segnale da un segmento, lo amplifica e lo ritrasmette su tutti gli altri segmenti. I ripetitori possono essere usati anche per aumentare la lunghezza complessiva della rete.

Comunque, sono in vigore delle regole generali stabilite dallo standard:
- la lunghezza massima dell'intera rete, fra qualunque coppia di stazioni, non deve superare i 2,5 km;
- fra qualunque coppia di stazioni non devono trovarsi più di quattro ripetitori;
- possono esservi al massimo 1024 stazioni sulla rete.

4.6.1.2) Codifica dei dati

In 802.3 non si usa una codifica diretta dei dati (ad esempio, zero volt per lo zero e cinque volt per l'uno), perché sarebbe difficile rilevare le collisioni. Inoltre, si vuole delimitare con facilità l'inizio e la fine di ogni singolo bit.

Si usa una codifica, detta ***Manchester***, che prevede una transizione del valore del segnale nel mezzo di ogni bit, zero o uno che sia.

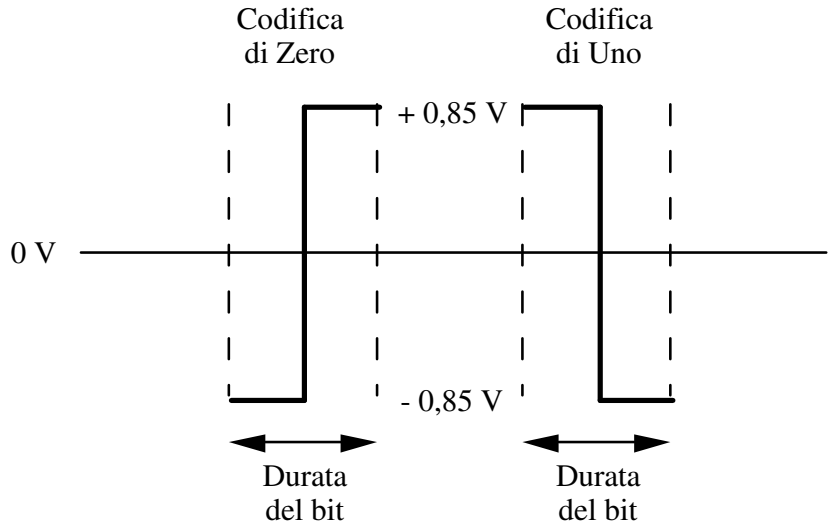

Figura 4-18: Codifica Manchester

Fra i vantaggi di tale codifica:
- facilità di sincronizzazione fra mittente e destinatario;
- il codice trasmissivo è ***bilanciato***, cioé vi è uguale energia per lo zero e per l'uno, e quindi la trasmissione di dati, anche se genera diverse quantità di zeri e uni, non produce

componenti in corrente continua, molto dannose perché ostacolano la trasmissione dei segnali;
- è facile rilevare le collisioni.

Si noti però che tale codifica richiede, a parità di velocità di trasmissione, una banda doppia rispetto alla codifica diretta (ogni bit richiede la trasmissione di due valori distinti).

4.6.1.3) Protocollo MAC 802.3

La struttura di un frame 802.3 è la seguente:

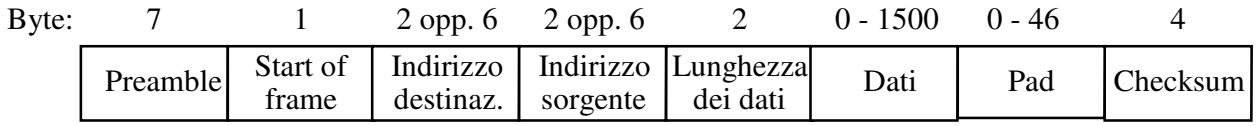

Figura 4-19: Frame 802.3

I campi del frame hanno le seguenti funzioni:

Preamble	7 byte tutti uguali a 10101010. Producono, a 10 Mbps, un'onda quadra a 10 Mhz per 5,6 microsecondi, che consente al ricevitore di sincronizzare il suo clock con quello del trasmettitore.
Start of frame	un byte delimitatore, uguale a 10101011.
Indirizzi	gli indirizzi usati sono sempre a 6 byte, e sono univoci a livello mondiale (sono cablati dentro l'interfaccia). E' possibile specificare un singolo destinatario, un gruppo di destinatari (multicast) oppure un invio in broadcast a tutte le stazioni (indirizzo costituito da una sequenza di uni).
Lunghezza dei dati	indica quanti byte ci sono nel campo dati (da 0 a 1500).
Dati	contiene il payload del livello superiore.
Pad	Se il frame (esclusi preambolo e delimiter) è più corto di 64 byte, con questo campo lo si porta alla lunghezza di 64 byte, vedremo poi perché.
Checksum	è un codice CRC come quelli già visti.

Nessun livello MAC garantisce un servizio affidabile. Ciò è dettato dal fatto che, visto il bassissimo tasso d'errore delle LAN, si preferisce un protocollo datagram ad alte prestazioni.

Vediamo ora perché esiste un limite minimo di 64 byte per la lunghezza di un frame.

Abbiamo già visto che, perché una collisione possa essere certamente rilevata da chi trasmette, deve passare un tempo non inferiore a due volte il tempo di attraversamento dell'intera rete.

Nel caso di IEEE 802.3, che prevede 2,5 km di lunghezza massima totale e l'interposizione di un massimo di quattro ripetitori, si ha che il tempo massimo di attraversamento dell'intera rete moltiplicato per due è pari a 57,6 microsecondi.

Ora, è essenziale che la collisione venga rilevata durante la trasmissione e non dopo, altrimenti il mittente dedurrà erroneamente che la sua trasmissione è andata a buon fine.

Dunque, la trasmissione di un frame non deve durare meno di 57,6 microsecondi, che sono il tempo necessario per trasmettere (a 10 Mbps) proprio 72 byte (e cioé 576 bit, ciascuno dei quali viene trasmesso in un decimo di microsecondo). Dunque, il frame non può essere costituito da meno di 72 byte, 8 dei quali sono costituiti dal preambolo e dal delimitatore, e 64 dal resto del frame.

Si noti che se si vuole aumentare la velocità di un certo fattore, diciamo 10, si deve diminuire di 10 volte la lunghezza massima ammessa per la rete o aumentare di 10 volte la lunghezza minima del frame. Vedremo nel seguito come viene risolto il problema per il protocollo ***Fast Ethernet*** (100 Mbps).

4.6.1.4) Funzionamento di 802.3

Il protocollo 802.3 è un CSMA/CD di tipo 1-persistent:

- prima di trasmettere, la stazione aspetta che il canale sia libero;
- appena è libero inizia a trasmettere;
- se c'è una collisione, la circuiteria contenuta nel transceiver invia una sequenza di jamming di 32 bit, per avvisare le altre stazioni;
- se la trasmissione non riesce, la stazione attende una quantità di tempo casuale e poi riprova.

La quantità di tempo che si lascia passare è regolata da un apposito algoritmo, il ***binary backoff exponential algorithm***:

- dopo una collisione, il tempo si considera discretizzato (slotted) con uno ***slot time*** pari a 51,2 microsecondi (corrispondenti al tempo di trasmissione di 512 bit, ossia 64 byte, pari alla lunghezza minima di un frame senza contare il preambolo ed il delimiter);

- il tempo di attesa prima della prossima ritrasmissione è un multiplo intero dello slot time, e viene scelto a caso in un intervallo i cui estremi dipendono da quante collisioni sono avvenute;
- dopo n collisioni, il numero r di slot time da lasciar passare è scelto a caso nell'intervallo 0 <= r <= 2^k-1, con k = min (n, 10);
- dopo 16 collisioni si rinuncia (inviando un messaggio di errore al livello superiore).

La crescita esponenziale dell'intervallo garantisce una buona adattabilità ad un numero variabile di stazioni, infatti:
- se il range fosse sempre piccolo, con molte stazioni si avrebbero praticamente sempre collisioni;
- se il range fosse sempre grande, non ci sarebbero quasi mai collisioni ma il ritardo medio (metà range*slot time) causato da una collisione sarebbe molto elevato.

4.6.1.5) Prestazioni

Le prestazioni osservate sono molto buone, migliori di quelle stimabili in via teorica.

Peraltro, queste ultime sono fortemente influenzate dal modello di traffico che si assume. Di solito lo si assume poissoniano, ma in realtà è bursty e per di più ***self similar***, ossia il suo andamento su un lungo periodo è simile a quello su un breve periodo, ricordando in questo le caratteristiche dei frattali.

La pratica ha mostrato che 802.3:
- può sopportare un carico medio del 30% (3 Mbps) con picchi del 60% (6 Mbps);
- sotto carico medio:
    - il 2-3% dei pacchetti ha una collisione;
    - qualche pacchetto su 10.000 ha più di una collisione.

4.6.1.6) Fast Ethernet

Questo standard (803.2u), approvato nel 1995, prevede l'aumento di velocità di un fattore 10, da 10 Mbps a 100 Mbps.

Come si risolve il problema del minimo tempo di trasmissione e/o della massima lunghezza della rete? In modo diverso a seconda del supporto fisico utilizzato:
- Doppino classe 3 (100BaseT4)
    - si usano quattro doppini fra l'hub ed ogni stazione:
        - uno viene usato sempre per il traffico dall'hub alla stazione;

        - uno viene usato sempre per il traffico dalla stazione all'hub;
        - 2 vengono usati di volta in volta nella direzione della trasmissione in corso;
    - la codifica è ***8B6T***, cioé 8 bit vengono codificati con 6 ***trit*** (che hanno valore 0, 1 o 2);
    - la velocità di segnalazione è 25 Mhz (solo 25% in più di quella dello standard 802.3, che è di 20 Mhz);
    - si inviano 3 trit sui 3 doppini contemporaneamente a 25 Mhz, ossia 6 trit alla frequenza di 12,5 Mhz. Poiché 6 trit convogliano 8 bit, di fatto si inviano 8 bit a 12,5 Mhz, ottenendo così i 100 Mbps.
- Doppino classe 5 (100BaseT)
    - velocità di segnalazione 124 Mhz;
    - codifica ***4B5B*** (4 bit codificati con 5 bit, introducendo ridondanza);
    - a seconda del tipo di hub:
        - hub tradizionale: la lunghezza massima di un ramo è 100 metri, quindi il diametro della rete è 200 metri (contro i 2,5 km di 802.3).
        - ***switched hub***: ogni ramo è un dominio di collisione separato, e quindi (poiché su esso vi è una sola stazione) non esiste più il problema delle collisioni, ma rimane il limite di 100 metri per i limiti di banda passante del doppino.
- Fibra ottica (100BaseFX)
    - velocità di segnalazione 125 Mhz;
    - codifica 4B5B;
    - obbligatorio switched hub;
    - lunghezza rami fino a 2 km (con uno switched hub non c'è il problema delle collisioni, ed inoltre come sappiamo la fibra regge velocità dell'ordine dei Gbps a distanze anche superiori).

4.6.2) IEEE 802.5

Nel 1972 IBM scelse l'anello per la sua architettura di LAN, a cui diede il nome di ***Token Ring***. Successivamente, IEEE ha definito lo standard IEEE 802.5 sulla base di tale architettura.

Le differenze principali sono che la rete IBM prevede velocità di 4 Mbps e 16 Mbps, mentre 802.5 prevede oltre ad esse anche la velocità di 1 Mbps.

4.6.2.1) Cablaggio

Il cablaggio più diffuso è basato su doppino telefonico:

- schermato (STP);
- non schermato (UTP):

- categoria 3, 4 o 5 per 4 Mbps;
- categoria 4 o 5 per 16 Mbps.

Normalmente il cablaggio è fatto utilizzando un ***wire center***, che ha la possibilità di isolare parti dell'anello guaste: se manca corrente su un lobo il corrispondente relais si chiude automaticamente.

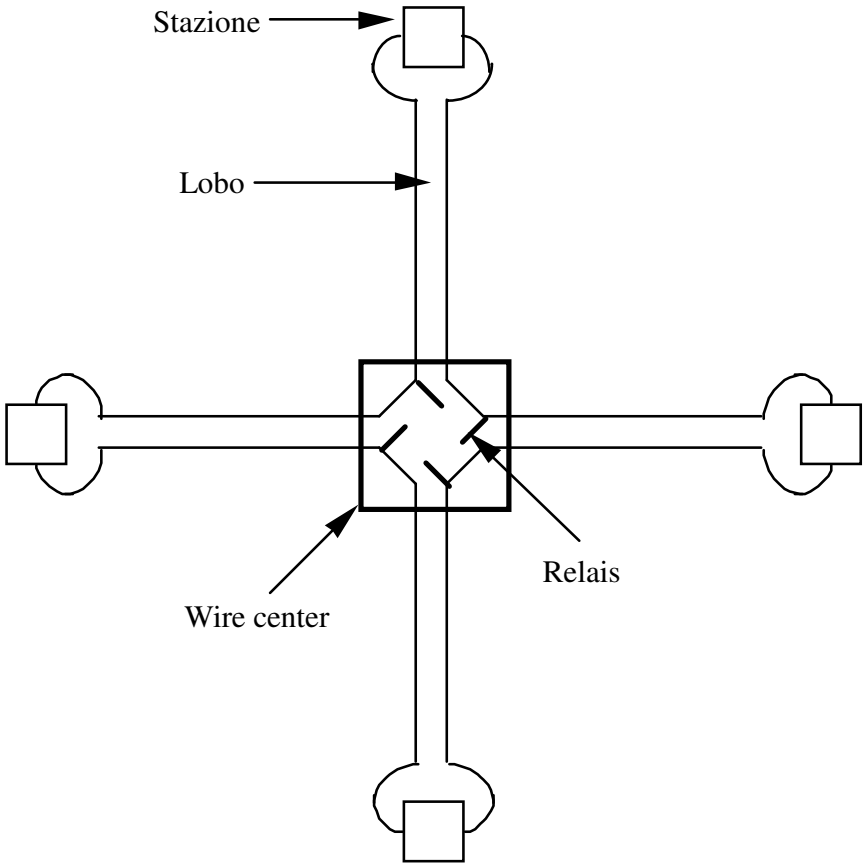

Figura 4-20: Cablaggio con wire center

I lobi hanno una lunghezza massima variabile, a seconda del cablaggio utilizzato:
- UTP cat. 4: 150 metri;
- UTP cat. 5: 195 metri;
- STP: 340 metri.

Le stazioni possono essere al massimo 260.

4.6.2.2) Codifica dei dati

Si usa la codifica ***Differential Manchester Encoding***, definita così:

- valore zero: all'inizio della trasmissione del bit si fa una transizione;
- valore uno: all'inizio della trasmissione del bit non si fa una transizione;
- a metà del bit si fa in entrambi i casi una transizione.

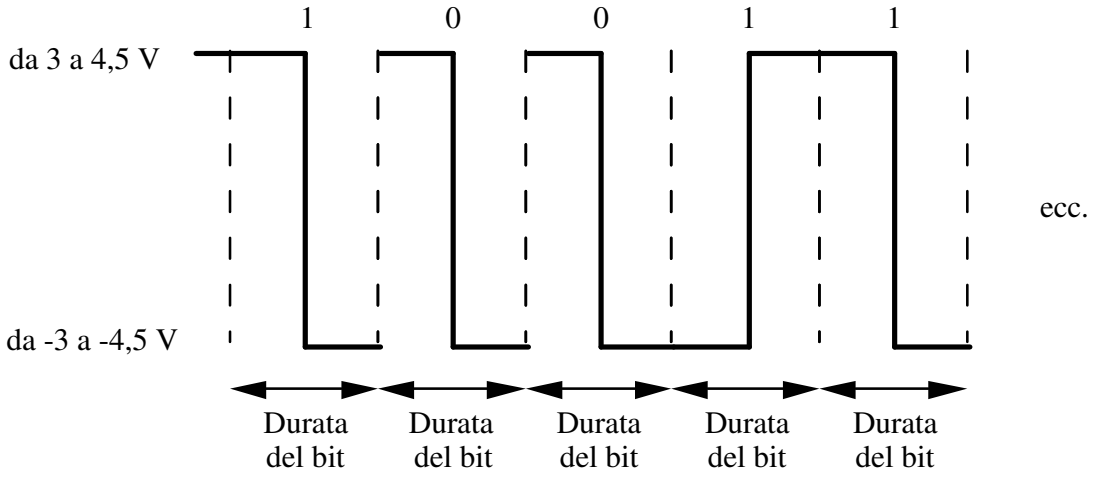

Figura 4-21: Codifica Differential Manchester

4.6.2.3) Protocollo MAC 802.5

La struttura del token e del frame di 802.5 è la seguente:

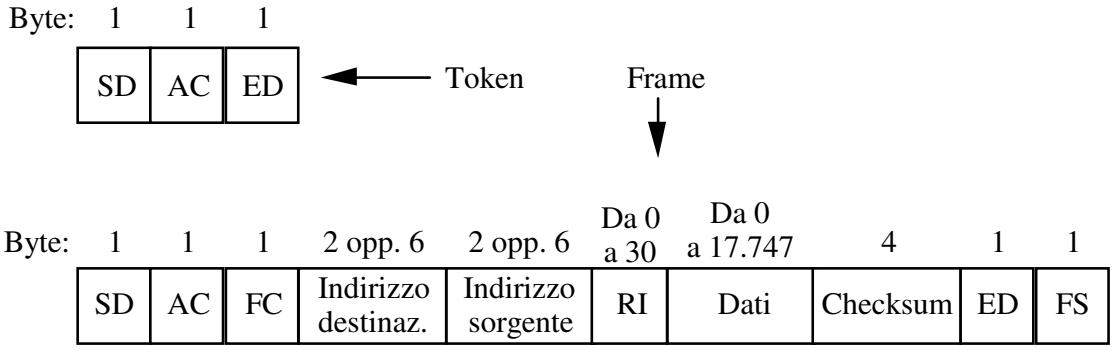

Figura 4-22: Token e frame 802.5

I campi del frame hanno le seguenti funzioni:

SD, ED	Starting e ending delimiter: contengono all'interno due coppie di bit codificati con i valori high-high e low-low, in violazione della codifica Manchester. Si usano high-high e low-low accoppiati per non introdurre uno sbilanciamento del codice.
AC	Access control, serve per il controllo dell'accesso. E' costituito di 8 bit: PPPTMRRR • i tre bit P indicano la ***priorità attuale***; • il bit M serve per il controllo di ***frame orfani***: il monitor lo setta ad 1 al passaggio del frame, e se lo ritrova ad uno al passaggio successivo il frame è orfano e viene tolto dall'anello; • il bit T, detto ***token bit***, identifica un token (se vale 0) o un frame (se vale 1); • i tre bit R indicano la priorità richiesta.
FC	Frame control, distingue frame contenenti dati da frame con funzioni di controllo.
Indirizzi	come 802.3.
RI	Routing information, contiene (se c'è) le informazioni necessarie al source routing (vedremo più avanti).
Dati	contiene il payload del livello superiore.
Checksum	è un codice CRC come quelli già visti.
FS	Frame status, serve per sapere cosa è successo del frame. Contiene, fra l'altro, due bit, A e C, gestiti come segue: • bit A: viene messo ad 1 (dal destinatario) quando il frame gli arriva; • bit C: viene messo ad 1 (dal destinatario) quando il frame gli arriva ed il destinatario lo copia al suo interno.

4.6.2.4) Funzionamento di 802.5

Quando il token circola e una stazione vuole trasmettere, essa, che è in listen mode, opera come segue:

- aspetta che arrivi il token;
- quando il token arriva:
    - lascia passare SD;

        - lascia passare i bit PPP di AC;
        - quando ha nel buffer il token bit T:
            - lo cambia in uno, trasformando il token in un frame;
            - invia il bit T modificato sul ring;
            - si mette immediatamente in transmit mode;
            - invia il resto del frame;
- quando il frame è trasmesso:
    - se non ha esaurito il ***THT*** (***Token holding time***) può trasmettere un altro frame;
    - altrimenti rigenera un nuovo token e lo trasmette;
    - appena trasmesso l'ultimo bit del token si rimette immediatamente in listen mode.

Ogni ring ha una stazione con un ruolo speciale, il ***monitor*** (ogni stazione è in grado di diventare il monitor). Il monitor viene designato all'avvio dell'anello. I suoi compiti principali sono:

- rigenerare il token se esso si perde;
- ripulire il ring dai resti di frame danneggiati;
- ripulire il ring dai frame orfani.

4.6.3) Confronto fra 802.3 ed 802.5

Vantaggi di 802.3:

- ha un'enorme diffusione;
- esibisce un buon funzionamento a dispetto della teoria.

Svantaggi di 802.3

- ha sostanziose componenti analogiche (per il rilevamento delle collisioni);
- il funzionamento peggiora con forte carico.

Vantaggi di 802.5:

- è totalmente digitale;
- va molto bene sotto forte carico.

Svantaggi di 802.5

- c'è ritardo anche senza carico (per avere il token);
- ha bisogno di un monitor (e se è "malato", cioé malfunzionante, e nessuno se ne accorge?).

In definitiva, nessuna delle due può essere giudicata la migliore in assoluto.

4.6.4) IEEE 802.11

Durante gli anni '90 l'IEEE avviò l'attività di standardizzazione delle reti LAN senza fili all'interno dello standard 802. I risultati si concretizzarono in una serie di standard definiti fra il 1997 ed il 2003, collettivamente contraddistinti dalla sigla 802.11, che differiscono fra loro per le bande trasmissive utilizzate, per le tecniche di codifica utilizzate e per le velocità trasmissive raggiungibili.

Ciascuno degli standard 802.11 è suddiviso in due parti, analogamente a quanto visto per 802.3 ed 802.5:

- sottolivello MAC, essenzialmente comune a tutti gli standard. In particolare il formato dei frame, i servizi offerti ed i meccanismi di accesso al canale sono gli stessi per tutti;
- livello fisico, che ovviamente differisce anche sensibilmente da uno standard all'altro.

Attualmente la situazione è la seguente:

- 802.11 (1997), che specifica tre diverse bande trasmissive:
  - banda degli infrarossi, tecnica trasmissiva in banda base, velocità di 1 Mbps e (opzionale) 2 Mbps;
  - banda ISM di 2,4 GHz, tecnica trasmissiva FHSS, velocità di 1 e 2 Mbps;
  - banda ISM di 2,4 GHz, tecnica trasmissiva DSSS, velocità di 1 e 2 Mbps;
- 802.11a (1999): banda ISM di 5 GHz, tecnica trasmissiva spread spectrum di tipo ***OFDM*** (***Orthogonal Frequency Division Multiplexing***, concettualmente simile a quanto visto per l'ADSL), velocità fino a 54 Mbps;
- 802.11b (1999): banda ISM di 2,4 GHz, velocità di 1, 2, 5.5, 11 Mbps;
  - tecnica trasmissiva DSSS per 1 e 2 Mbps;
  - tecnica trasmissiva ***HR-DSSS*** (***High Rate DSSS***) per 5.5 e 11 Mbps;
- 802.11g (2003): banda ISM di 2,4 GHz, velocità fino a 54 Mbps;
  - stesse tecniche trasmissive di 802.11b alle velocità di 1, 2, 5.5 ed 11 Mbps;
  - tecnica trasmissiva OFDM per le velocità più alte.

Tutti gli standard elencati supportano reti con e senza stazione base (***AP***, ***Access Point*** nella terminologia 802.11).

Il blocco principale dell'architettura 802.11 è la cella, detta ***BSS*** (***Base Service Unit***). Uno o più AP collegati alla rete fissa (Ethernet ad esempio) formano un ***DS*** (***Distribution System***).

Vedremo ora più in dettaglio lo standard 802.11b, che appare destinato ad una sempre più ampia diffusione.

4.6.4.1)Codifica dei dati

Come già anticipato, 802.11b può funzionare a 1, a 2, a 5,5 ed a 11 Mbps.

Si utilizza la banda ISM di 2,4 Ghz, che viene suddivisa in 13 canali larghi 5 MHz ciascuno. La trasmissione avviene modulando in fase una portante centrata nel canale scelto, fra i 13 disponibili, per la comunicazione (ovviamente trasmettitore e ricevitore devono usare lo stesso canale).

Con le tecniche di codifica adottate da 802.11b una singola trasmissione impegna una banda di frequenza di circa 22 MHz, per cui due trasmissioni indipendenti e contemporanee, per non interferire a vicenda, devono essere spaziate di almeno 5 canali (ossia di almeno 25 MHz). Dunque, celle adiacenti ed a portata una dell'altra devono essere spaziate di almeno 5 canali.

Trasmissione a 1 e 2 Mbps

Si usa DSSS. Ogni bit è codificato mediante una particolare sequenza di 11 chip, chiamata ***Sequenza di Barker*** e caratterizzata da una elevata autocorrelazione.

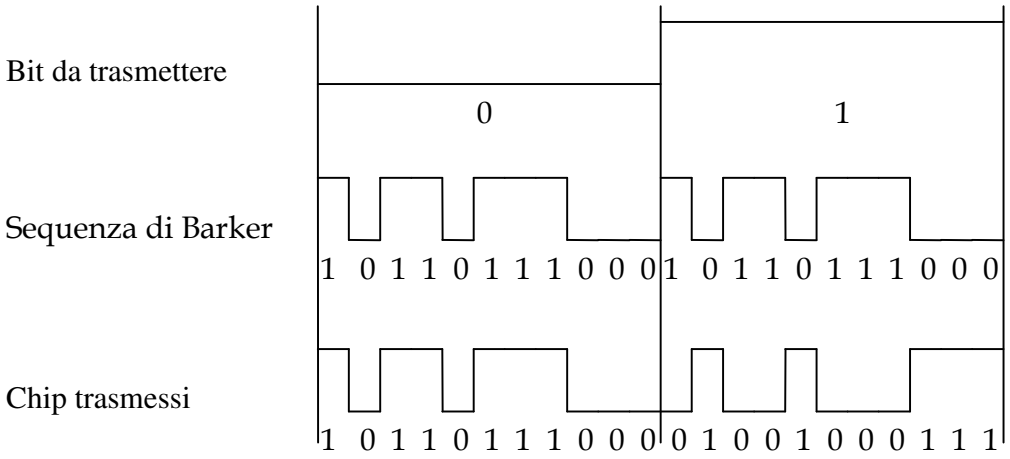

Figura 4-23: Codifica mediante sequenza di Barker

I singoli chip della sequenza vengono trasmessi modulando in fase la portante, alla velocità di segnalazione di 11 Mbaud:

- per la trasmissione a 1 Mbps si usano due soli valori di modulazione. Di conseguenza ogni variazione del valore di fase convoglia un chip, per cui si hanno 11 Mchip/sec che corrispondono a 1 Mbps;
- per la trasmissione a 2 Mbps si usano invece quattro valori diversi di modulazione. Di conseguenza ogni variazione del valore di fase convoglia due chip, per cui si hanno 22 Mchip/sec che corrispondono a 2 Mbps;

Trasmissione a 5,5 e 11 Mbps

Si usa HR-DSSS. Grazie all'introduzione di una tecnica di codifica completamente nuova, si riescono a raggiungere velocità superiori senza aumentare la banda richiesta da una singola trasmissione, che resta di circa 22 MHz. Questo offre il vantaggio di poter mantenere la identica struttura di canali usata per 1 e 2 Mbps, consentendo quindi la coesistenza dentro una stessa cella di apparecchiature operanti a velocità diverse.

La codifica utilizzata è la cosiddetta ***codifica CCK*** (***Complementary Code Keying***), basata sull'uso di un ***codice complementare***. Un codice complementare è un codice (ossia un insieme predefinito di parole costruite su un alfabeto dato) che possiede una particolare caratteristica: alcune delle parole di tale codice sono ***ortogonali*** fra loro, ossia sono "particolarmente" distinguibili.

Il codice costituito da *tutte le parole di 8 simboli quaternari* è un codice complementare costituito da $4^8 = 65536$ parole, al cui interno sono individuabili 64 parole ortogonali fra loro.

La codifica CCK di 802.11b utilizza proprio tali 64 parole ortogonali per codificare i bit da trasmettere in sequenze di chip. Come per le velocità di 1 e 2 Mbps, i chip vengono poi trasmessi modulando in fase la portante centrata nel canale prescelto a 11 Mbaud. Ogni valore di modulazione è sempre scelto fra un insieme di 4 possibili, sia per 5,5 che per 11 Mbps.

Per la trasmissione a 5,5 Mbps si opera come segue:

- i bit vengono codificati a gruppi di 4;
- 2 bit del gruppo determinano la parola di codice da trasmettere, che in questo caso è scelta fra le 4 parole ($2^2 = 4$) "più ortogonali" entro le 64 parole ortogonali: gli 8 valori quaternari della parola scelta determinano una successione di 8 valori di modulazione di fase;
- i rimanenti 2 bit del gruppo vengono usati dal trasmettitore per "ruotare" di fase l'intera parola di codice, ossia la intera successione di 8 valori di modulazione da applicare durante la trasmissione;
- dato che con questa tecnica 4 bit sono codificati con 8 chip, trasmettendo a 11 Mchip/sec si ottengono 5,5 Mbps.

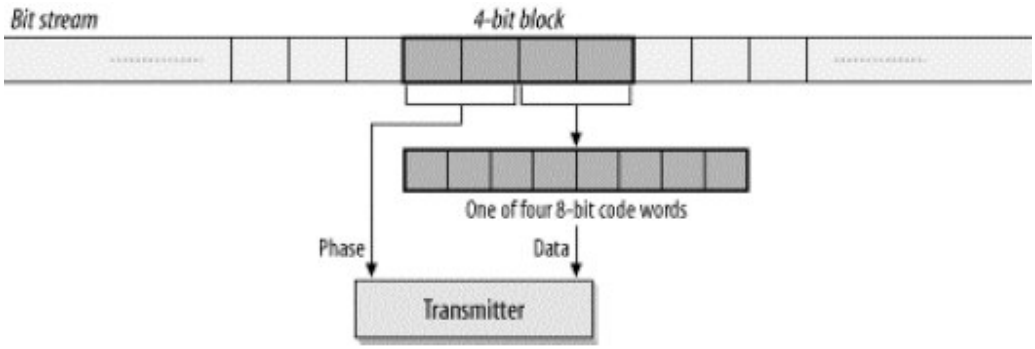

Figura 4-24: Trasmissione a 5,5 Mbps

Per la trasmissione a 11 Mbps si opera come segue:

- i bit vengono codificati a gruppi di 8;
- 6 bit del gruppo determinano la parola di codice da trasmettere, che è scelta fra tutte le 64 parole ($2^6 = 64$) ortogonali del codice: gli 8 valori quaternari della parola scelta, come nel caso precedente, determinano una successione di 8 valori di modulazione di fase;
- i rimanenti 2 bit del gruppo, come nel caso precedente, vengono usati dal trasmettitore per "ruotare" di fase l'intera parola di codice;
- con questa tecnica 8 bit sono codificati con 8 chip, quindi trasmettendo a 11 Mchip/sec si ottengono 11 Mbps.

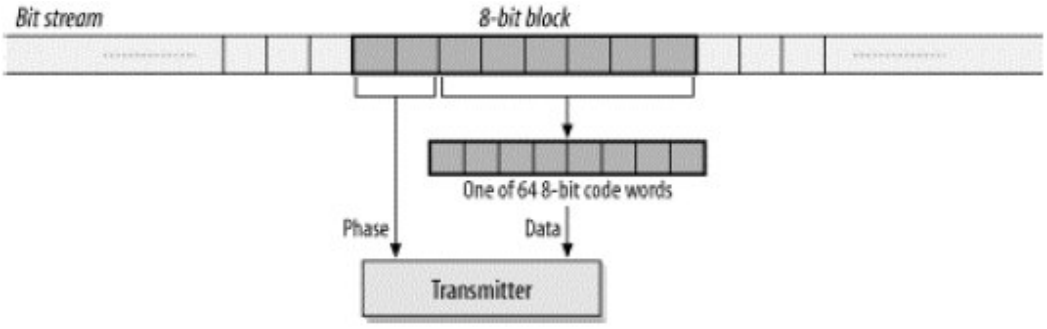

Figura 4-25: Trasmissione a 11 Mbps

4.6.4.2) Protocollo MAC 802.11

La struttura di un frame 802.11 è la seguente:

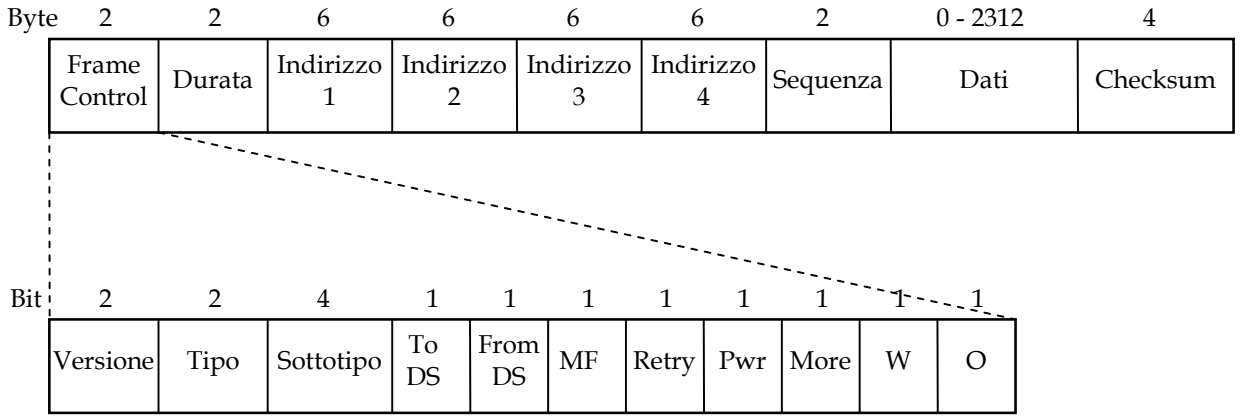

Figura 4-26: Frame 802.11

I sottocampi del campo *Frame Control* hanno le seguenti funzioni:

Versione	Indica il tipo del protocollo (802.11, 802.11b, ecc.).
Tipo	Specifica se il frame è un frame dati, di controllo (ad es. CTS o RTS) o di gestione (ad es. richiesta di associazione o autenticazione). I frame dati possono passare da una cella all'altra, mentre i frame di controllo e di gestione sono confinati all'interno di una singola cella.
Sottotipo	Ulteriore specifica del tipo di frame. Ad esempio, per i frame di controllo può esserse RTS, CTS, ACK.
To DS	1 se il frame e' destinato al DS (e quindi deve uscire dalla cella per mezzo dell'AP).
From DS	1 se il frame proviene dal DS (e quindi è entrato nella cella per mezzo dell'AP).
MF	More Fragments: 1 indica che vi sono ulteriori frammenti dopo questo.
Retry	1 se il frame è la ritrasmissione di un frame precedente.
Pwr	Power: 1 indica che a conclusione della trasmissione la stazione si metterà in uno stato di risparmio energetico; 0 che rimarrà attiva.
More	1 indica che altri dati sono disponibili per il ricevitore. Ciò eviterà che esso si metta in uno stato di risparmio energetico.

W	WEP (Wired Equivalent Privacy): 1 indica che il payload è cifrato.
O	Ordered: 1 indica che il payload va consegnato in ordine rispetto agli altri frame con lo stesso valore di questo campo.

I campi del frame hanno invece le seguenti funzioni:

Durata	Indica (in millisecondi) per quanto tempo il frame più il relativo ack occuperanno il canale.
Indirizzo 1 *Indirizzo 2* *Indirizzo 3* *Indirizzo 4*	Indirizzi a 48 bit identici a 802.3 ed 802.5; due sono gli indirizzi di mittente e destinatario, altri due gli indirizzi di AP sorgente ed AP destinatario (nel caso di traffico fra celle diverse).
Sequenza	Serve per numerare gli eventuali frammenti di un frame: 12 bit identificano il frame, 4 bit il segmento.
Dati	Payload.
Checksum	Codice CRC a 32 bit.

4.6.4.3) Funzionamento di MAC 802.11

Lo standard definisce due differenti modalità di funzionamento:

- *DCF* (*Distributed Coordination Function*): tale modalità, utilizzabile sia in presenza di un AP sia in una rete ad-hoc, realizza un arbitraggio distribuito per l'accesso al canale per mezzo del protocollo CSMA/CD;
- *PCF* (*Point Coordination Function*): tale modalità, che è facoltativa, richiede la presenza di un AP e realizza un arbitraggio centralizzato per l'accesso al canale.

Le due modalità, come vedremo, possono coesistere all'interno di una stessa cella.

Modalità DCF

Questa modalità deve obbligatoriamente essere supportata in tutte le apparecchiature conformi allo standard.

Viene adottato il protocollo CSMA/CA, che essenzialmente è un MACA con l'aggiunta dell'ascolto del canale prima di trasmettere.

Oltre ad ascoltare il canale fisico (rilevando la eventuale presenza di una portante) ogni stazione prende in considerazione anche un canale virtuale tramite il cosiddetto *NAV* (*Network Allocation Vector*). Il NAV, gestito individualmente da ciascuna stazione, fornisce l'indicazione della quantità di tempo durante la quale il mezzo trasmissivo rimarrà occupato

dalle trasmissioni già iniziate. Ogni stazione determina il valore del NAV sulla base dei frame RTS e CTS che riceve.

Una stazione considera libero il canale solo quando sia il canale fisico che quello virtuale (NAV) sono liberi.

Il funzionamento del CSMA/CA è il seguente.

- Una stazione A che vuole trasmettere un frame dati a B ascolta il canale. Se esso rimane libero per una certa quantità di tempo, detta ***DIFS*** (***Distributed Inter Frame Spacing***), invia un frame RTS indirizzato a B e resta in attesa del corrispondente CTS;
- la stazione B, appena ricevuto il frame RTS, ascolta il canale. Se esso rimane libero per una certa quantità di tempo, detta ***SIFS*** (***Short Inter Frame Spacing***, più breve del DIFS), invia un frame CTS indirizzato ad A;
- tutte le altre stazioni che ricevono il frame RTS assegnano al loro NAV una durata pari al tempo necessario per l'invio del frame dati e del corrispondente frame ACK;
- la stazione A, ricevuto il frame CTS, ascolta il canale. Se esso rimane libero per un tempo SIFS inizia a trasmettere il frame dati indirizzato a B;
- tutte le altre stazioni che ricevono il frame CTS assegnano al loro NAV una durata pari al tempo necessario per l'invio del frame dati e del corrispondente frame ACK;
- la stazione B, ricevuto il frame dati, ascolta il canale. Se esso rimane libero per un tempo SIFS invia un frame ACK indirizzato ad A;

Se all'inizio della procedura la stazione A trova il canale occupato, essa attende un tempo casuale (determinato con un binary backoff exponential algorithm analogo a quello di 802.3) e ricomincia daccapo. Uguale comportamento viene adottato se A non riceve il frame CTS dopo aver inviato il frame RTS, o se non riceve il frame di ACK dopo aver inviato il frame dati.

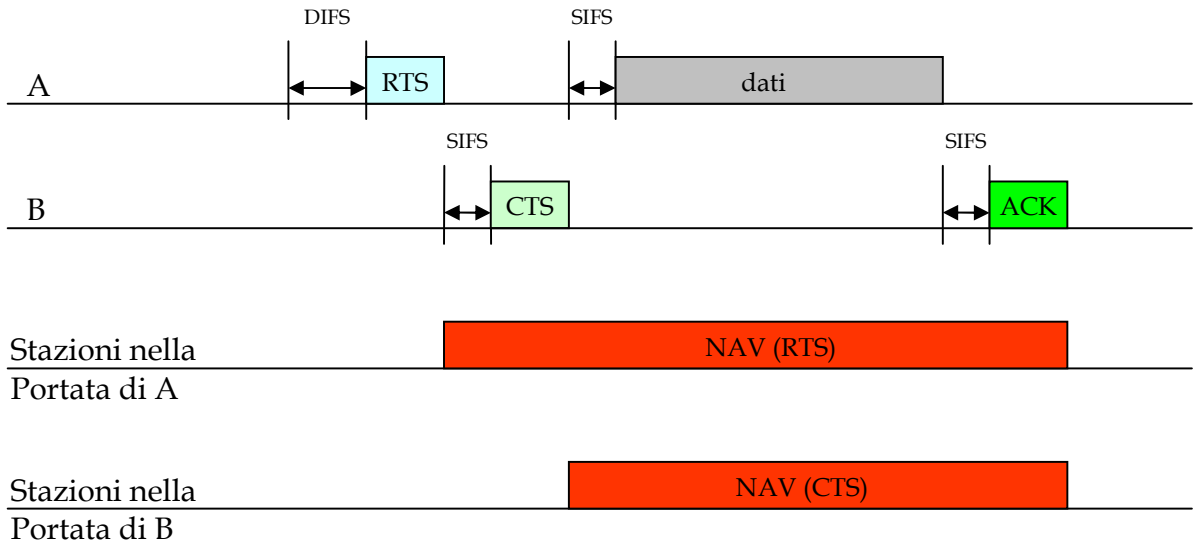

Figura 4-27: Trasmissione di un frame

Il protocollo possiede come visto meccanismi per la frammentazione dei frame, in considerazione dell'elevato tasso d'errore dei mezzi wireless. I frammenti sono confermati individualmente per permettere la ritrasmissione selettiva dei soli frame rovinati. Inoltre, per dare la priorità alla trasmissione dei frammenti di uno stesso frame rispetto alla trasmissione di un frame interamente nuovo:

- per la trasmissione del prossimo segmento si attende un tempo SIFS e non DIFS;
- ogni segmento (tranne l'ultimo) si comporta come un RTS virtuale per il frammento successivo ed ogni ACK (tranne l'ultimo) si comporta come un CTS virtuale per il frammento successivo.

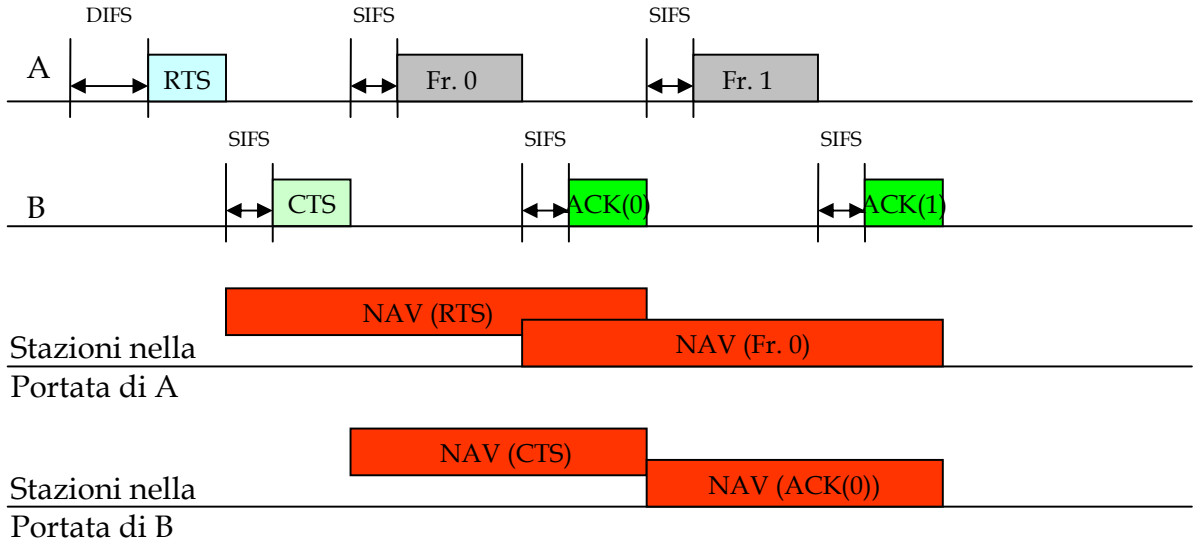

Figura 4-28: Trasmissione di un frame frammentato

Una stazione può adottare una versione semplificata del protocollo quando:

- deve trasmettere frame dati molto brevi (al di sotto di una soglia, impostabile su ogni singola stazione);
- non esiste il problema della stazione nascosta (ad esempio in una WLAN confinata all'interno di una stanza).

In tal caso non vengono inviati i frame RTS e CTS, ma solo il frame dati ed il corrispondente frame di ACK.

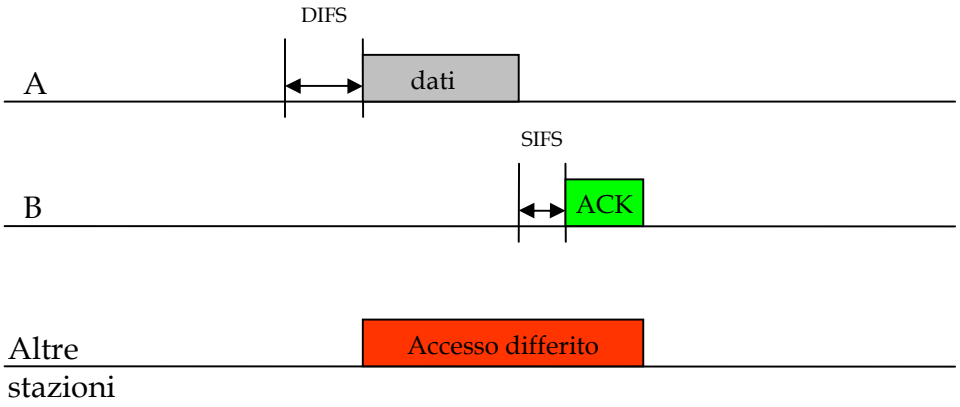

Figura 4-29: Trasmissione diretta di un frame

Le altre stazioni si astengono dal trasmettere per la durata della trasmissione del frame e del relativo ACK.

Modalità PCF

E' opzionale, ossia non è obbligatorio supportarla. In questa modalità l'AP realizza un arbitraggio centralizzato per l'accesso al mezzo trasmissivo.

Le stazioni che desiderano servirsene devono "registrarsi" presso l'AP per poterne usufruire. L'AP successivamente interroga a turno tutte le stazioni registrate ed assegna loro il mezzo trasmissivo a turno. Nessuna stazione può trasmettere con questa modalità se non è autorizzata esplicitamente dall'AP.

PCF può essere utile nel caso di applicazioni che abbiano bisogno di una banda minima garantita (ad esempio trasmissione di audio e video), che possono richiedere all'atto della registrazione presso l'AP.

PCF può convivere dentro una stassa cella col DCF grazie al fatto che è definito un ulteriore intervallo di tempo, detto ***PIFS*** (***PCF Inter Frame Spacing***), maggiore di SIFS e minore di DIFS, che governa l'accesso al mezzo per trasmissioni PCF.

Di conseguenza se nessuno impegna il mezzo trasmissivo dopo un tempo SIFS (il che significa che una trasmissione DCF è terminata), l'AP può impossessarsi del canale dopo un tempo PIFS, al fine di gestire trasmissioni PCF, prima che qualunque altra stazione, che deve attendere il più elevato tempo DIFS per trasmettere in DCF, possa farlo.

Servizi

Lo standard definisce vari sevizi che ogni DS ed ogni cella conformi allo standard devono fornire (quindi tali servizi presuppongono l'esistenza di uno o più AP).

I servizi relativi ad un DS nel suo complesso sono:
- ***Associazione***: utilizzato da una stazione mobile quando entra in contatto con un AP. La stazione si annuncia e può negoziare vari aspetti della comunicazione (ad es. uso di PCF con banda minima garantita). L'AP può accettare o rifiutare la stazione, e se essa viene accettata deve autenticarsi;
- ***Separazione***: utilizzato quando una stazione abbandona una cella, la precedente associazione termina;
- ***Riassociazione***: utilizzato per cambiare il proprio AP preferito o nel transito da una cella ad un'altra. Lo standard non specifica il supporto alla mobilità fra celle, che per il momento è lasciato a soluzioni ad hoc proposte dai costruttori;
- ***Distribuzione***: specifica come instradare i frame, se all'interno della cella (via radio) o all'esterno della cella (via rete fissa);
- ***Integrazione***: specifica i meccanismi per inviare i frame a reti non 802.11 (ad esempio verso la rete 802.3 cui è connesso l'AP) operando eventualmente le necessarie conversioni di protocollo;

I servizi relativi ad una singola cella invece sono:
- ***Autenticazione***: servizio successivo all'associazione, in cui la stazione mobile deve autenticarsi. L'autenticazione può essere fatta sulla base dell'indirizzo MAC della stazione, o con varie tecniche crittografiche;
- ***Invalidamento***: utilizzato quando una stazione abbandona una cella, la precedente autenticazione perde di validità e la stazione non è più autorizzata a trasmettere dati;
- ***Riservatezza***: protezione dei dati trasmessi, ottenuta con crittografia a chiave segreta;
- ***Trasferimento dati***: il servizio è datagram, come in 802.3.

4.6.5) IEEE 802.2

Questo standard, chiamato ***Logical Link Control*** (***LLC***),definisce la parte superiore del livello data link in modo indipendente dai vari sottolivelli MAC.

Ha due funzioni principali:
- fornire al livello network un'interfaccia unica, nascondendo le differenze fra i vari sottolivelli MAC;

- fornire, se è richiesto dal livello superiore, un servizio più sofisticato di quello offerto dai vari sottolivelli MAC (che, ricordiamo, offrono solo servizi datagram). Esso infatti offre:
    - servizi datagram;
    - servizi datagram confermati;
    - servizi affidabili orientati alla connessione.

Il frame LLC è modellato ispirandosi a HDLC, con indirizzi di mittente e destinatario, numeri di sequenze, numeri di ack (questi ultimi due omessi per i servizi datagram), ecc.

Gli indirizzi LLC sono lunghi un byte e servono sostanzialmente ad indicare quale protocollo di livello superiore deve ricevere il pacchetto di livello tre; in questo modo LLC offre un supporto multiprotocollo al livello superiore.

Il frame LLC viene imbustato, in trasmissione, in un frame dell'opportuno sottolivello MAC. Il processo inverso ha luogo in ricezione.

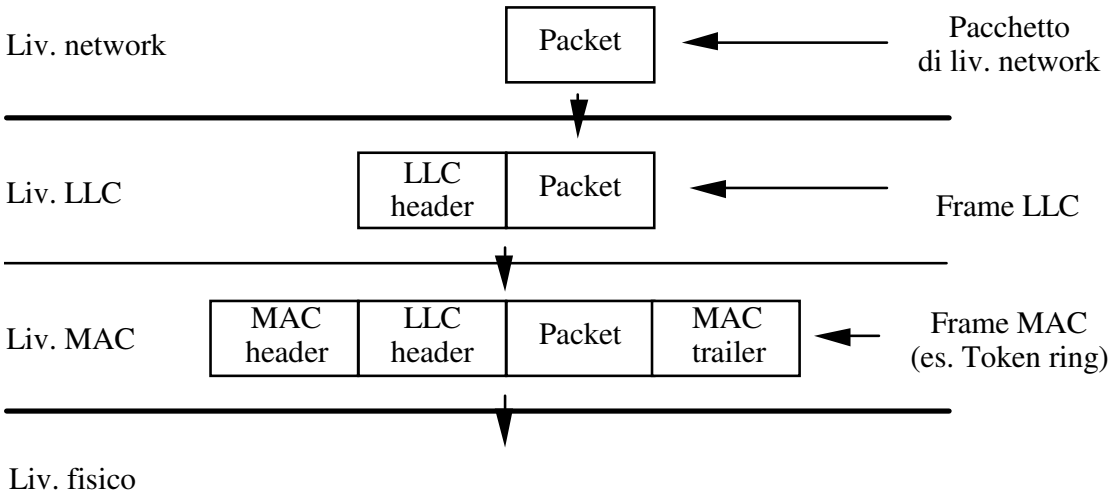

Figura 4-30: Buste LLC e MAC

4.7) Il bridge

Molto spesso c'è la necessità di connettere fra di loro LAN distinte, per molte ragioni:

- due LAN di tipo differente (ad esempio una Ethernet ed una Token ring), che non si possono semplicemente collegare l'una con l'altra, contengono host che vogliono dialogare fra loro;
- si vuole una LAN la cui lunghezza superi i limiti massimi consentiti (ad esempio, 2,5 km per Ethernet);
- si desidera, nel caso di una LAN contenente molti host, suddividerla in molteplici LAN interconnesse. Questo per tenere separato il traffico generato nelle sue parti, in modo da avere un traffico totale molto superiore a quello possibile su una singola LAN.

Due o più LAN possono essere interconnesse con dispositivi detti ***bridge***, che operano a livello data link.

Ciò significa che la loro operatività è basata esclusivamente sulle informazioni contenute nelle buste di livello due, mentre non vengono prese affatto in considerazione quelle di livello tre. Questa è la caratteristica fondamentale che li differenzia dai ***router***, che invece agiscono a livello tre.

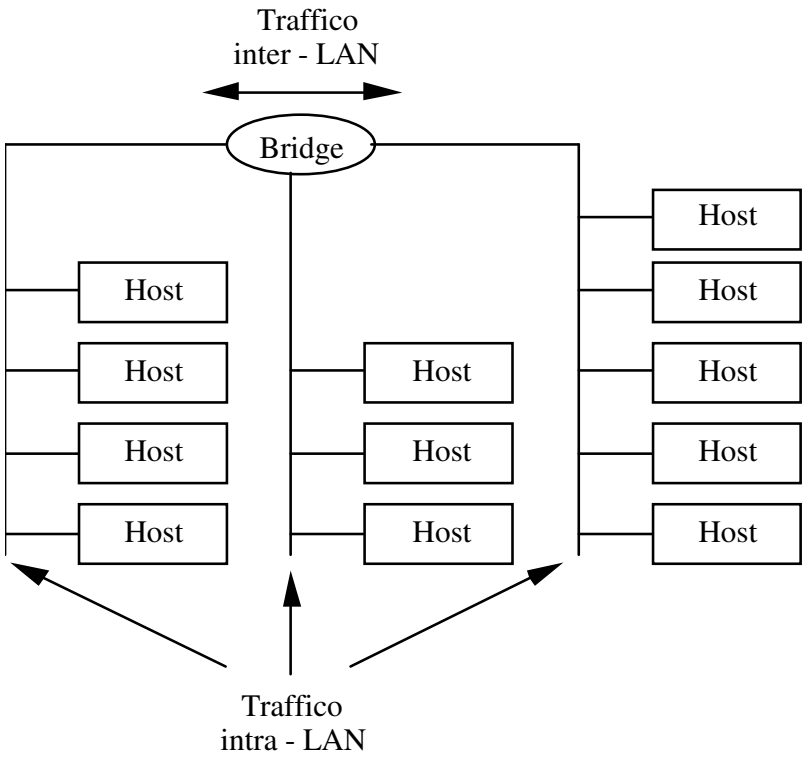

Figura 4-31: Interconnessione di LAN tramite bridge

In questo esempio il traffico totale (se è tutto confinato entro le singole LAN) può arrivare a tre volte quello di una singola LAN. Solo il traffico fra host di LAN diverse attraversa il bridge.

I bridge si occupano di instradare il traffico da una LAN all'altra. E' importante sottolineare che, anche se l'instradamento di per se è una funzione tipica del livello tre, qui avviene sulla base dei soli indirizzi di livello due, quindi il bridge appartiene in tutto e per tutto al livello data link.

Il funzionamento di un bridge, che ha tante interfacce di rete quante sono le LAN alle quali è fisicamente collegato, è il seguente:

- quando una delle interfacce di rete del bridge riceve un frame MAC, lo passa al relativo software di livello MAC che toglie la busta MAC;
- il resto viene passato dal livello MAC al software di livello LLC del bridge, nel quale, sulla base dell'indirizzo di destinazione, si decide a quale LAN inviarlo:
    - se la destinazione si trova sulla LAN di provenienza il frame viene scartato;
    - altrimenti, il frame LLC viene passato al livello MAC competente per la LAN di destinazione, che lo imbusta in un frame MAC e provvede ad inviarlo su tale LAN, secondo le regole di quest'ultima.

Si noti che un bridge è ben diverso da un ripetitore, che copia pedissequamente tutto ciò che riceve da una linea su tutte le altre. Il bridge infatti acquisisce un frame, lo analizza, lo ricostruisce e lo instrada, quindi può anche essere configurato in modo da ***filtrare*** (cioé non far passare) alcuni tipi di traffico. Ciò tipicamente avviene in funzione dell'indirizzo LLC, che identifica il protocollo di livello superiore, o sulla base dell'indirizzo MAC del mittente o del destinatario.

I bridge progettati per interconnettere LAN di tipo diverso devono risolvere vari problemi legati alle diverse regole in vigore su tali LAN, tra cui:

- formati dei frame differenti;
- data rate differenti;
- massima lunghezza di frame differente: è fuori questione spezzare un frame in questo livello, dato che tutti i protocolli si aspettano che il frame o arrivi per intero o non arrivi affatto; ad esempio, nello standard 802 i frame troppo grandi devono essere scartati;
- funzioni previste da un tipo di LAN ma non dall'altra: ad esempio, il concetto di priorità ed i bit A e C presenti in 802.5 non hanno un equivalente in 802.3.

4.7.1) Standard IEEE per i bridge

Ci sono due tipi di bridge standardizzati da IEEE:

- ***transparent bridge*** (promossi dai comitati 802.3 e 802.4)
- ***source-routing bridge*** (scelti dal comitato 802.5)

Il ***transparent bridge*** (IEEE 802.1 part D) può essere installato e diventare operativo in modo totalmente trasparente, senza richiedere niente altro che la connessione fisica e l'accensione. Incredibile a dirsi, la cosa funziona!

Il mecccanismo è il seguente:

- Dal momento in cui il bridge viene attivato, esamina tutti i frame che gli arrivano dalle varie LAN, e sulla base di questi costruisce progressivamente le sue tabelle di instradamento. Infatti, ogni frame ricevuto consente al bridge di sapere su quale LAN si trova la stazione che lo ha inviato.
- Ogni frame che arriva al bridge viene ritrasmesso:
    - se il bridge ha nelle sue tabelle di instradamento l'indirizzo del destinatario, invia il frame sulla corrispondente LAN;
    - altrimenti il frame viene inviato a tutte le LAN tranne quella di provenienza, con una tecnica detta ***flooding*** (che vedremo meglio più avanti);
    - man mano che il bridge aumenta la sua conoscenza degli indirizzi delle varie macchine, la ritrasmissione diventa sempre più selettiva (e quindi più efficiente).
- Le tabelle vengono aggiornate ogni qualche minuto, rimuovendo gli indirizzi che non si sono fatti vivi nell'ultimo periodo (così, se una macchina si sposta, entro pochi minuti viene di nuovo indirizzata correttamente) Questa tecnica si chiama ***backward learning***.
- Se ci sono maglie nella topologia di connessione delle LAN, i bridge si costruiscono di essa uno ***spanning tree***, che poi utilizzano per l'instradamento, al fine di evitare la generazione di un infinito numero di duplicati durante il flooding.

Il ***source-routing bridge*** (nato per le reti 802.5) è progettato invece per ottenere l'instradamento più efficiente possibile, anche a scapito della trasparenza.

L'idea di base è che il mittente indichi esplicitamente il cammino (espresso come sequenza di bridge e reti) che il frame deve percorrere. L'amministratore di sistema deve assegnare numeri di identificazione distinti ad ogni rete e ad ogni bridge, operazione che deve essere fatta manualmente.

Tali informazioni sono incluse in un apposito campo ***RI*** (***Routing Information***) del frame 802.5, e la loro eventuale presenza è indicata dal valore 1 del bit più significativo dell'indirizzo sorgente (che, essendo sempre relativo a un indirizzo singolo e mai di gruppo o

broadcast, originariamente è sempre zero). Il bridge esamina solo i frame che hanno tale bit a uno.

E' ovvio che ogni host deve avere il quadro della topologia delle connessioni, memorizzato in un'apposita struttura dati. Per costruirla e mantenerla, il meccanismo usato è il seguente:

- quando un host deve spedire un frame ma non conosce il cammino da seguire per raggiungere la destinazione, invia un ***discovery frame***, chiedendo tale informazione;
- il discovery frame viene inviato in flooding da ogni bridge a tutti gli altri, e quindi raggiunge tutti gli host. In questa fase, ogni bridge scrive nel discovery frame il suo ID, che si aggiunge a quello dei bridge precedentemente incontrati. Quando un discovery frame arriva alla destinazione, contiene tutto il cammino percorso;
- quando l'host di destinazione riceve un discovery frame, lo invia indietro al mittente;
- il mittente, sulla base del primo discovery frame che ritorna (considerando il relativo cammino quello più conveniente) aggiorna le sue tabelle e può mandare il frame che voleva spedire originariamente.

Un vantaggio di questo schema di funzionamento è che si trova sempre il cammino ottimo; uno svantaggio è l'esplosione del numero di discovery frame.

Dopo un periodo in cui entrambi gli standard sopra descritti erano abbastanza diffusi, oggi praticamente tutti i bridge costruiti sono di tipo transparent, ed al più offrono la funzionalità source-routing come un'opzione supplementare.