

Sottolivello MAC (Medium Access Control)

4.1 Generalità Protocolli Multiple Access:

Nelle reti broadcast uno dei principali problemi è stabilire quale elaboratore ha diritto di utilizzare il canale, in che modo e per quanto tempo quando c'è competizione. Quello che si deve evitare è che più stazioni trasmettano contemporaneamente creando così delle collisioni che porterebbero alla perdita dei frame. I protocolli del sottolivello MAC si occupano proprio di questo tipo di problema. Spesso sono utilizzati nelle LAN ma anche nelle parti di WAN basate su satelliti. Ci sono due tipi di allocazione del canale, quella statica e quella dinamica, che a sua volta può essere ad arbitraggio statico o dinamico.

L'allocazione statica prevede la suddivisione del canale per il numero di utenti, ciascuno dei quali riceve una frazione della banda totale. Questa tecnica porta ad uno spreco di banda quando qualche utente non trasmette, e poiché il traffico generato è bursty i picchi di banda consumata non possono essere gestiti con la banda assegnata.

L'allocazione dinamica d'altro canto cerca di adeguarsi alle esigenze trasmissive degli utenti.

4.1.1. Aloha:

Nel pure aloha le stazioni trasmettono quando vogliono se avviene una collisione le stazioni interessate lasciano passare un tempo random dopodiché ritrasmettono il frame.

Per poter stimare l'efficienza di questo protocollo si deve ricorrere ad alcune considerazioni:

definiamo inizialmente il *frame time* come il tempo necessario al trasferimento di un frame con lunghezza fissa. Complessivamente supponiamo che vengano generati S frame per frame time. Ovviamente se $S \geq 1$ ci saranno continue collisioni, quindi $0 < S < 1$, ma occorre considerare anche i frame ritrasmessi a causa di precedenti collisioni, diciamo quindi che la distribuzione media di tutti i frame segua una distribuzione di Poisson e che sia G. A basso carico G sarà minore di S ma ad alti carichi di lavoro G sarà superiore ad S e quindi ancora meno efficiente.

In ogni caso il *throughput* medio (la quantità di pacchetti che arrivano a destinazione) sarà uguale a:

$Throughput = G * P(0)$, dove P(0) è la probabilità che si generino 0 frame per frame time ossia

$P(0) = \frac{G}{e^G}$ per poter calcolare il throughput effettivo, bisogna inoltre considerare che la

probabilità di generare k frame per frame time è data, secondo Poisson, da $P(k) = \frac{G^k e^{-G}}{k!}$ e che il

periodo di vulnerabilità di un frame, cioè l'intervallo di tempo in cui le possibilità di collidere sono maggiori, è 2 volte il frame time.

In questo periodo vengono generati 2G frame, quindi la probabilità che non si generino nuovi frame in tutto il periodo di vulnerabilità è $P(0) = e^{-2G}$ e quindi il throughput sarà

$$Throughput = G e^{-2G}$$

Analizzando il grafico di questo protocollo otterremo che il max throughput di 0.184 si ottiene con un tasso di frame per frame time pari a 0.5 cioè meno del 20%.

4.1.2. Slotted Aloha:

Il successore del pure aloha è lo slotted aloha, il quale dimezza il tempo di vulnerabilità che diventa uguale ad un solo frame per frame time. In questo periodo vengono generati mediamente G frame, per cui la probabilità che non si generino nuovi frame per tutto il periodo di vulnerabilità è

$P(0) = e^{-G}$ e quindi il throughput sarà $Throughput = G e^{-G}$ il cui max sarà di 0.368 e si avrà in

corrispondenza di un tasso di frame per frame time pari a 1.

4.1.3. CSMA (Carrier sense multiple access):

Entrambi i protocolli Aloha hanno una bassa efficienza, un'evoluzione di questi protocolli, sono quelli che si preoccupano di ascoltare se il canale è libero prima di trasmettere, ottenendo così un'efficienza molto più elevata.

Ci sono diversi protocolli di questa famiglia e sono:

- *1-persistent*: in questo protocollo quando una stazione deve trasmettere ascolta il canale, se è occupato attende finché non si libera, altrimenti trasmette con probabilità 1. Se avviene una collisione, la stazione attende un tempo random, e riprova.

I problemi di questo protocollo sono:

- se una stazione A trasmette e prima che il suo segnale arrivi a B anche B inizia a trasmettere ci sarà una collisione ed entrambi i frame andranno persi. Più alto è il tempo di propagazione più possibilità di collisione ci saranno.
- A e B ascoltano contemporaneamente il canale in attesa che C lo liberi, appena C lo libera, A e B trasmettono contemporaneamente.
- *NonPersistent*: quando una stazione deve trasmettere ascolta il canale, se è occupato invece di trasmettere appena possibile, aspetta un tempo random anche se il canale è libero. Se invece trova il canale libero si comporta esattamente come 1-persistent. Con questo protocollo ci si aspettano maggiori ritardi prima di trasmettere ma minori collisioni.
- *P-persistent*: si applica solo a canali slotted, quando una stazione deve trasmettere ascolta il canale, se è libero con probabilità p trasmette subito, e con probabilità $1-p$ aspetta il prossimo slot. Se il canale è occupato, attende il prossimo slot. Questo processo si ripete finché il frame non è stato trasmesso interamente o qualcun altro ha iniziato a trasmettere. In questo caso, la stazione si comporta come in una collisione.

4.1.4. CSMA-CD (carrier sense multiple access with collision detection):

Un protocollo questo che migliora ulteriormente le prestazioni del CSMA, difatti le stazioni interrompono la trasmissione non appena rilevano una collisione. Per effettuare questo rilevamento si ascolta il canale durante la propria trasmissione, se la potenza del segnale ricevuto è superiore a quella del segnale trasmesso, si scopre la collisione.

Quando si verifica una collisione si attende un tempo casuale prima di ritrasmettere, il tempo necessario per rilevare una collisione è $2T$ dove T è il tempo di propagazione del segnale da un capo all'altro.

4.1.5. Reti wireless:

Un sistema di stazioni mobili capaci di comunicare tra di loro costituisce una LAN senza fili, questo tipo di lan può essere costituita in due modi diversi, il primo prevede la presenza di una *base station* cioè di un punto d'accesso che fornisca connettività e servizi alle stazioni che entrano nel suo raggio d'azione le quali diverranno *celle*, e l'altra quella chiamata *ad hoc* che si realizza semplicemente quando un gruppo di stazioni cominciano a comunicare tra loro senza la presenza di una base station.

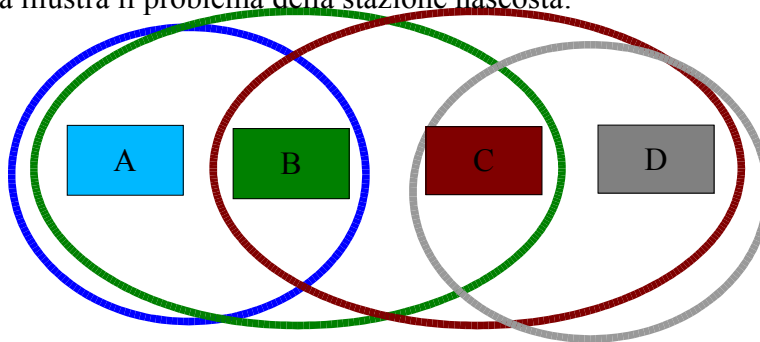
I problemi principali che sorgono quando ci troviamo di fronte ad una WLAN sono:

- *collisioni*
- *interferenze e riflessioni*
- *privacy*
- *mobilità per gli utenti*

4.1.5.1. Il problema della Stazione nascosta:

Innanzitutto va precisato che ogni apparato trasmettente in una wlan è caratterizzato da un *portata*, dipendente dalla potenza dell'apparato stesso; questa portata è il raggio d'azione entro il quale tutte le apparecchiature presenti e in grado di comunicare vengono “sentite”.

La seguente figura illustra il problema della stazione nascosta:



in questo problema occorre stabilire quando A potrà trasmettere a B, il semplice ascolto del canale non è sufficiente, poiché se A si mettesse a trasmettere dopo aver trovato il canale libero, nulla vieterebbe a C di trasmettere creando così una collisione tra A e C su B.

4.1.5.2. Il problema della Stazione esposta:

Il problema della stazione esposta si presenta quando B vuole trasmettere ad A e C a D, C prima di trasmettere ascolterà il canale trovandolo occupato dalla trasmissione di B, quindi si metterà in attesa quando invece avrebbe potuto tranquillamente trasmettere non generando alcuna collisione su D.

4.1.6. MACA- MACAW:

Dall'analisi dei due problemi precedenti abbiamo potuto notare come l'utilizzo di protocolli di MA tipo il CSMA-CD non siano sufficienti. Una prima soluzione a questo problema è data dal protocollo *MACA* (*multiple access with collision avoidance*) nel quale non c'è ascolto del canale e si cerca di evitare le collisioni, anziché rilevarle.

Il canale non viene più ascoltato in base a questi presupposti: se il canale è libero per il trasmettitore, non è detto che lo sia per il ricevitore; se il canale è occupato per il trasmettitore non è detto che lo sia per il ricevitore.

L'idea di fondo quindi è quello dello scambio di brevi messaggi di controllo che consentano a trasmettitore e ricevitore di accordarsi sulla trasmissione. Se il ricevitore sarà in grado di accettare la trasmissione, risponderà con un messaggio di conferma, che solo se ricevuto correttamente dal trasmettitore potrà iniziare la trasmissione.

Il funzionamento è il seguente:

- A invia un breve pacchetto a B chiamato *RTS* (*request to send*) contenente la lunghezza del frame dati;
- B se non è impegnato nella ricezione di altri dati, risponde con un pacchetto chiamato *CTS* (*clear to send*) che autorizzerà A ad iniziare a trasmettere;

Per quanto riguarda tutte le altre stazioni il loro comportamento sarà il seguente:

- tutte le stazioni che ricevono il pacchetto RTS di A devono rimanere in silenzio per un tempo che consenta al frame CTS di arrivare ad A, dopodiché potranno ricominciare a trasmettere;
- tutte le stazioni che ricevono il solo frame CTS (quindi nella portata di B, ma non di A) devono rimanere in silenzio per il tempo necessario alla trasmissione del frame dati (la cui

lunghezza è riportata nel CTS);

- le stazioni che ricevono sia il frame RTS che quello CTS (situate nella portata di A e B) applicheranno entrambe le regole;

Tutto questo non garantisce comunque l'assenza totale di collisioni, però fa sì che al massimo le collisioni avvengano tra i frame cts e rts che essendo di pochi Kb non influiranno in modo molto negativo. In ogni caso dopo ogni collisione il trasmettitore aspetterà un tempo casuale prima di ricominciare a trasmettere.

Un'evoluzione del protocollo MACA è rappresentata da *MACAW (Maca per Wireless)*, che introduce alcune ulteriori migliorie:

- invio di ACK ad avvenuta ricezione corretta del frame dati; questo permette ritrasmissioni più rapide;
- invio da parte del trasmettitore dopo la ricezione del CTS di un breve frame *DS(Data Send)* contenente la dimensione del frame dati che verrà trasmesso. Questo consente alle stazioni fuori dalla portata di A di non inviargli degli RTS prima che A abbia terminato;
- gestione distribuita degli algoritmi per il tempo d'attesa; questo garantisce equità nelle ritrasmissioni;

4.2 Lo standard IEEE 802:

IEEE ha prodotto diversi standard per le reti lan, questi standard includono:

- specifiche generali del progetto (802.1)
- LLC logical link control (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)

Tutti questi standard differiscono a livello fisico e MAC ma sono compatibili nel livello data link.

4.2.1. IEEE 802.3:

È lo standard per un protocollo di tipo CSMA-CD 1 persistent, funzionante a 10Mbps. Questo protocollo è l'evoluzione di Ethernet. Il suo funzionamento segue questo schema:

- prima di trasmettere si ascolta il canale
- appena il canale è libero si trasmette
- se c'è collisione la circuiteria del transceiver emette il jamming sequence
- se la trasmissione non riesce la stazione attende un tempo casuale e poi ritrasmette

La quantità di tempo che si lascia passare in caso di collisione è regolata dall'algoritmo *binary backoff exponential algorithm* che funziona in questo modo:

- dopo una collisione il tempo si considera suddiviso in slot, con uno slot time di 51,2 microsec
- il tempo d'attesa prima della prossima ritrasmissione è un multiplo intero dello slot time, e viene scelto casualmente in un intervallo che dipende dal numero di collisioni già avvenute
- dopo n collisioni, il numero r di slot time da lasciar passare è scelto casualmente in $0 \leq r \leq 2^k - 1$ dove k è il min(n,10)
- dopo 16 collisioni si rinuncia

Questo algoritmo avendo una crescita esponenziale garantisce una buona adattabilità ad un numero variabile di stazioni, perché se il range fosse troppo piccolo e le stazioni fossero molte si avrebbero continue collisioni, mentre se il range fosse grande e le stazioni poche non ci sarebbero collisioni ma il ritardo causato da una collisione sarebbe troppo elevato.

4.2.1.1. Cablaggio:

Sono previsti diversi tipi di cablaggio:

- *Thick Ethernet*: è il primo sistema, consiste in un cavo coassiale spesso. Ufficialmente

conosciuto come *10Base5*, perché raggiunge una velocità di trasmissione di 10 Mbps e una distanza massima di 500 m. Su un unico segmento possono essere installate al massimo 100 macchine, ognuna delle quali ha una *interfaccia di rete* alla quale viene attaccato un cavo il *transceiver drop cable* che si innesta su un *transceiver* collegato ad un *vampiro* posizionato sul cavo coassiale. È compito del transceiver di verificare se avvengono collisioni, e in tal caso di inviare un segnale a 32 bit sul canale chiamato *jamming sequence*.

- *Thin Ethernet*: composto da un cavo coassiale più sottile rispetto al thick ethernet, conosciuto come *10Base2*, raggiunge una velocità di 10Mbps, e copre una distanza massima di 200 m con non più di 30 macchine per segmento. In questo tipo di cablaggio l'interfaccia di rete di ciascuna stazione contiene al suo interno anche il transceiver. L'allaccio di una stazione avviene con una congiunzione a T alla quale sono collegati due segmenti del cavo thin e uno cavo che porta alla stazione. Tutte le stazioni sono collegate in cascata (*daisy chain*).
- *Doppino telefonico*: chiamato *10BaseT*, prevede il collegamento tramite il normale doppino telefonico fra coppie di stazioni, può coprire una distanza di 100 m o 150 se il cavo è di categoria 5, per poter effettuare il collegamento tra più stazioni occorre un *ripetitore multiporta* o *HUB*. Il numero massimo di stazioni su una rete è di 1024 e non possono esserci più di 4 HUB tra ogni coppia di stazioni.

4.2.1.2. Codifica dati:

In 802.3 non viene utilizzata una codifica diretta dei dati, che renderebbe estremamente difficile l'individuazione di collisioni ed errori, viene invece utilizzata la *codifica Manchester*, che prevede una transazione del segnale nel mezzo di ogni bit.

I vantaggi derivanti da questo tipo di codifica sono:

- facilità di sincronizzazione tra i clock delle varie stazioni
- il codice è bilanciato, cioè vi è la stessa energia per la codifica dello 0 e per quella dell'1, questo impedisce che si generino delle correnti continue all'interno del mezzo trasmissivo.

Di contro uno dei principali svantaggi di questa codifica è che a parità di velocità trasmissiva si richiede il doppio della banda rispetto alla codifica diretta.

4.2.1.3. Formato frame:

Il frame 802.3 è così composto:

<i>Preamble</i>	7 byte tutti uguali a 10101010, utili per la sincronizzazione dei clock, producono un'onda quadra a 10MHz
<i>Start of frame</i>	un byte delimitatore 10101011
<i>Indirizzi</i>	gli indirizzi sempre di 6 byte sono univoci a livello mondiale (sono inseriti all'interno delle interfacce), è possibile in questo campo inserire l'indirizzo di un singolo destinatario o un indirizzo di tipo multicast, oppure broadcast.
<i>Lunghezza dati</i>	indica di quanti byte è composto il campo dati
<i>Dati</i>	il payload vero e proprio
<i>Pad</i>	se il frame è più corto di 64 byte si inseriscono in questo campo bit fino al raggiungimento di questa dimensione

Checksum	CRC
----------	-----

4.2.1.4. MAC:

Il livello MAC non garantisce affatto un servizio affidabile, si è preferito, visto il bassissimo tasso d'errore delle LAN, utilizzare un protocollo di tipo datagram. Il campo Pad del frame, viene utilizzato perché viste le specifiche dell'802.3 sappiamo che la distanza massima di una rete di questo tipo è 2,5 Km e l'inserimento di massimo 4 HUB, quindi il tempo massimo di attraversamento dell'intera rete moltiplicato per 2 è di 57,6 microsec, questo dato è molto utile per l'individuazione delle collisioni, che debbono essere trovate durante il tempo di trasmissione del frame e non dopo, quindi mantenere la dimensione del frame prefissata fa sì che il tempo di propagazione si mantenga stabile, e quindi sia più facile individuare errori.

4.2.1.5. Fast Ethernet:

Questo standard prevede l'aumento di velocità di un fattore 10 rispetto all'802.3, quindi da 10Mbps a 100Mbps.

Con questo aumento però si presenta il problema di come mantenere il minimo tempo di trasmissione e/o la massima lunghezza della rete, il modo per risolvere questi problemi è in funzione del supporto fisico utilizzato:

- *Doppino classe 3 (100BaseT4)*: si usano 4 doppini tra l'hub e ogni stazione, uno è sempre usato per il traffico tra hub e stazione, uno sempre per il traffico tra stazione e hub, 2 vengono usati di volta in volta nella direzione della trasmissione in corso. La codifica usata è *8B6T* ossia 8 bit vengono codificati in 6 *trit* (che hanno valore 0,1 o 2). La velocità di segnalazione è di 25Mhz e si inviano 3 trit su 3 doppini contemporaneamente a 25Mhz ossia 6 trit alla frequenza di 12,5 Mhz, quindi poiché 6 trit convogliano 8bit, si inviano 8bit a 12.5Mhz ottenendo così 100Mbps.
- *Doppino classe 5 (100BaseT)*: la velocità di segnalazione in questo caso è di 124Mhz, la codifica è *4B5B* cioè 4 bit vengono codificati con 5 bit. A seconda del tipo di hub la lunghezza massima di un ramo è di 100m, quindi il diametro della rete è 200m, nel caso di *switched hub* ogni ramo è un dominio di collisione separato, e quindi non esiste più il problema delle collisioni.
- *Fibra ottica (100BaseFX)*: la velocità di segnalazione è 125mhz la codifica è *4B5B*, sono obbligatori gli *switched hub*, e la lunghezza massima dei rami è 2km.

4.2.2. IEEE 802.11:

Una famiglia di standard nati intorno agli anni '90 come evoluzione dell'802.3 per le reti wireless, i vari standard differiscono tra loro nella banda utilizzata, nei sistemi di codifica e nelle velocità trasmissive. Attualmente sono presenti i seguenti standard:

1. 802.11 : specifica tre diverse bande trasmissive:
 1. banda degli infrarossi, velocità 1-2Mbps
 2. banda ISM di 2,4GHz, tecnica trasmissiva FHSS (Frequency Hopping Spread Spectrum) con velocità di 1-2Mbps
 3. banda ISM di 2,4GHz, tecnica trasmissiva DSSS (Direct Sequence Spread Spectrum) con velocità di 1-2Mbps
2. 802.11a : banda ISM si 5GHz, tecnica trasmissiva spread spectrum di tipo OFDM, velocità vicina a 54 Mbps
3. 802.11b : banda ISM si 2,4GHz , tecniche trasmissive DSSS per 1 e 2 Mbps e HR-DSS (High Rate Direct Sequence Spread Spectrum) per 5,5 e 11 Mbps
4. 802.11g : banda ISM si 2,4GHz , tecniche trasmissive DSSS per 1 e 2 Mbps e HR-DSS per 5,5 e 11 Mbps e OFDM per velocità fino a 54Mbps

Tutti questi standard supportano reti con e senza base station.

4.2.2.1. Codifica dati:

Analizzando 802.11b, sappiamo che può funzionare a velocità pari a 1,2,5.5,11Mbps, si utilizza una banda ISM di 2,4GHz suddivisa in 13 canali di 5Mhz ciascuno. La trasmissione avviene modulando in fase una portante centrata sul canale scelto, una singola trasmissione occupa una banda di 22Mhz, quindi per poter mantenere due comunicazioni adiacenti e indipendenti in modo tale che non interferiscano tra loro occorre distanziarle di almeno 5 canali ossia 25Mhz.

1. *Trasmissioni a 1 e 2 Mbps:* Si usa DSSS, ogni bit è codificato con una particolare sequenza di 11 chip, chiamata *sequenza di Baker*. I singoli chip di questa sequenza vengono trasmessi modulando in fase la portante alla velocità di segnalazione di 11Mbaud. per la trasmissione a 1Mbps si utilizzano due soli valori di modulazione, quindi ogni variazione del valore di fase convoglia un chip per cui si hanno 11Mchip/sec che corrispondono a 1Mbps. Per le trasmissioni a 2Mbps invece si usano quattro valori diversi di modulazione, quindi si ottengono 22Mchip/sec uguali a 2Mbps.
2. *Trasmissioni a 5.5 e 11 Mbps:* Si usa HR-DSSS, le velocità di trasmissione superiori si ottengono grazie ad un sistema diverso di codifica, difatti si utilizza la codifica *CCK* (complementary code keyring), basata su di un codice complementare, ossia un insieme predefinito di parole costruite su un alfabeto dato. Questo tipo di codice possiede la caratteristica che alcune parole sono ortogonali tra loro quindi particolarmente distinguibili. Il codice è costituito da tutte le parole di 8 simboli quaternari, quindi è costituito da $4^8=65536$ parole, e di queste 64 sono ortogonali tra loro. Proprio queste 64 parole vengono utilizzate per codificare i bit da trasmettere in sequenze di chip.

Per la trasmissione a 5,5 Mbps si effettuano i seguenti passi:

1. i bit vengono codificati a gruppi di 4
2. 2 bit del gruppo determinano la parola di codice da trasmettere, che è scelta tra le 4 parole più ortogonali, gli 8 valori quaternari della parola scelta determinano una successione di 8 valori per la modulazione della fase
3. i rimanenti 2bit del gruppo vengono usati dal trasmettitore per ruotare di fase l'intera parola, ossia l'intera successione di 8 valori di modulazione
4. poiché 4bit sono codificati con 8 chip, trasmettendo a 11Mchip/sec si ottengono 5,5 Mbps

Per la trasmissione a 11 Mbps i passi sono i seguenti:

5. i bit vengono codificati a gruppi di 8
6. 6 bit del gruppo determinano la parola di codice da trasmettere che è scelta tra le 64 (2^6) parole più ortogonali, gli 8 valori quaternari determinano una successione di 8 valori di modulazione di fase
7. i rimanenti 2 bit servono per ruotare di fase l'intera parola
8. con questa tecnica quindi 8 bit sono codificati con 8 chip, quindi trasmettendo a 11 Mchip/sec si ottengono 11 Mbps

4.2.2.2. *Formato frame:*

I campi del frame sono :

<i>Frame Control</i>	Vedi tabella sotto
<i>Durata</i>	indica in millisec per quanto tempo il frame più il relativo ack occuperanno il canale
<i>Indirizzo1</i> <i>Indirizzo2</i> <i>Indirizzo3</i> <i>Indirizzo4</i>	Indirizzi a 48 bit identici a 802.3 e 802.5; due sono gli indirizzi di mittente e destinatario gli altri due sono di AP sorgente e AP destinatario nel caso di traffico tra celle diverse
<i>Sequenza</i>	Serve per numerare gli eventuali frammenti di un frame, 12 bit identificano il frame, 4 il segmento
<i>Dati</i>	Payload
<i>Checksum</i>	Controllo con codice CRC a 32 bit

I sotto campi del campo Frame Control sono:

<i>Versione</i>	indica il protocollo utilizzato
<i>Tipo</i>	Specifica se il frame è dati, controllo o gestione
<i>Sottotipo</i>	ulteriore specifica del tipo di frame ad esempio nel caso di frame di controllo, può essere RTS, CTS, ACK
<i>To Ds</i>	1 se il frame è destinato al DS
<i>From DS</i>	1 se il frame proviene dal DS
<i>MF</i>	More Fragments indica se ci sono ulteriori frammenti dopo questo
<i>Retry</i>	1 se il frame è in ritrasmissione
<i>Pwr</i>	Power 1 se è a conclusione della trasmissione la stazione si metterà in uno stato di risparmio, 0 la stazione rimarrà attiva
<i>More</i>	1 indica che altri dati sono disponibili per il ricevitore evitando che si metta in risparmio energetico
<i>W</i>	WEP (Wired Equivalent Privacy) 1 indica che il payload è cifrato
<i>O</i>	Ordered 1 indica che il payload va consegnato ordinato

4.2.2.3. MAC:

Il funzionamento di questo standard può essere in due modalità:

1. *DCF (Distributed Coordination Function)*: in questa modalità, che deve essere necessariamente supportata da tutte le apparecchiature conformi allo standard, la presenza di un Access Point (AP) è facoltativa, l'arbitraggio per la trasmissione è di tipo distribuito ed è quindi adatto sia per reti con AP che ad hoc, il protocollo utilizzato è CSMA-CA che è essenzialmente un MACA con l'aggiunta dell'ascolto del canale. Oltre all'ascolto del canale fisico questa modalità si occupa di ascoltare anche un canale virtuale il *NAV (network allocation vector)*, questo canale è gestito individualmente da ciascuna stazione, e mantiene in memoria il tempo di occupazione del mezzo trasmissivo, dovuto alle trasmissioni già iniziate, ogni stazione determina il proprio nav in funzione dei frame RTS e CTS che riceve, una stazione considera il canale libero soltanto quando sia quello fisico che quello virtuale sono liberi.

Il protocollo interno CSMA-CA funziona in questo modo:

- Una stazione A che vuole trasmettere verso B ascolta il canale, se rimane libero per un certo tempo (detto *DIFS Distributed Inter Frame Spacing*) dopo di che invia un frame RTS e attende il corrispondente CTS;
- B appena ricevuto il frame RTS ascolta il canale, se è libero e lo rimane per un tempo detto *SIFS (Short Inter Frame Spacing)*, più breve rispetto al DIFS, risponde con il CTS;
- tutte le stazioni che ricevono il frame RTS assegnano al loro NAV un tempo pari alla trasmissione del frame più il relativo ack;
- non appena A riceve il frame CTS, si mette in ascolto del canale, se rimane libero per un tempo SIFS, inizia a trasmettere;
- tutte le stazioni che ricevono il frame CTS, assegnano al loro NAV una durata pari al tempo per l'invio del frame e del relativo ack;
- B ricevuto il frame dati, si mette in ascolto del canale, se rimane libero per un tempo SIFS, allora invia ad A il relativo ack;

Se la stazione trasmittente dovesse trovare il canale occupato si metterà in attesa per un tempo casuale e poi ricomincerà l'ascolto del canale.

Questo protocollo, prevede la frammentazione dei frame, e visto l'elevato tasso d'errore dei canali wireless i frammenti dei frame vengono confermati singolarmente, permettendo così la ritrasmissione selettiva.

2. *PCF (Point Coordination Function)*: richiede necessariamente la presenza di un AP che gestisce in modo centralizzato l'arbitraggio delle trasmissioni.

È una modalità assolutamente opzionale da supportare, le stazioni che intendono servirsene debbono registrarsi presso l'AP, successivamente è l'AP stesso che interroga tutte le stazioni registrate e a turno assegna loro il mezzo trasmissivo. PCF può convivere all'interno della stessa cella con DCF difatti utilizza un ulteriore intervallo di tempo il *PIFS (PCF Inter Frame Spacing)* che è leggermente più lungo del SIFS e più corto del DIFS, quindi dopo un tempo SIFS l'AP è in grado di determinare che una trasmissione DCF è terminata e quindi si può impossessare del canale distribuendolo ai registrati.

I servizi offerti dallo standard per i sistemi Wireless sono:

- Per ogni DS :
 - associazione: utilizzato da una stazione quando entra in contatto con un AP
 - separazione: utilizzato quando una stazione abbandona una cella
 - riassociazione: utilizzato per il cambio di AP
 - distribuzione: specifica come instradare i frame, se internamente alla cella o esternamente
 - integrazione: specifica i meccanismi per inviare i frame a reti non 802.11

- Per ogni cella:
 - autenticazione: successivo all'associazione, la stazione si deve autenticare
 - invalidamento: all'abbandono della cella
 - riservatezza: protezione dati trasmessi
 - trasferimento dati: il servizio è datagram come in 802.3

4.2.3. IEEE 802.2:

Questo standard chiamato anche *Logical Link Control (LLC)* definisce la parte superiore del livello network indipendentemente dal livello MAC, si occupa di:

- fornire al livello network un'interfaccia unica indipendentemente dai sottolivelli MAC
- offrire un servizio più avanzato rispetto a quello offerto dai vari sottolivelli MAC, che offrono solo un servizio datagram, difatti LLC offre anche un servizio datagram confermato e servizi affidabili orientati alla connessione.

4.2.3.1. Formato frame:

La struttura del frame LLC è modellata su HDLC.

4.3 Bridge:

Quando c'è la necessità di connettere tra loro LAN distinte, si possono utilizzare dei dispositivi detti *bridge* che operano a livello data link.

La loro operatività è basata esclusivamente su buste di livello due, mentre le altre non vengono prese in considerazione, questa è la differenza che li contraddistingue dai *router* che invece si occupano anche dei livelli superiori.

Il funzionamento di queste apparecchiature è il seguente:

- i bridge dispongono di diverse interfacce di rete, in particolare ne hanno tante quante sono le LAN alle quali sono connessi
- appena un bridge riceve un frame MAC su una interfaccia, lo passa al relativo software di livello MAC che estrae i dati dalla busta
- passa questi dati al software di livello LLC nel quale sulla base dell'indirizzo di destinazione si decide su quale LAN inoltrarlo; se la destinazione si trova sulla LAN di partenza il frame viene scartato, altrimenti viene inviato sulla sola interfaccia connessa alla LAN di destinazione, inviando il pacchetto al livello LLC dell'interfaccia in questione che provvederà ad imbustarlo in un frame MAC

I bridge sono molto più sofisticati dei semplici HUB o ripetitori, che provvedono a replicare il frame in ingresso su tutte le linee d'uscita.

Ci sono inoltre i bridge usati per interconnettere LAN di tipo diverso, queste apparecchiature si trovano ad affrontare problemi di natura molto più complessa rispetto ai normali bridge, in particolare:

- i formati dei frame sono differenti
- i data rate sono differenti
- la massima lunghezza dei frame è differente
- alcune funzioni potrebbero essere previste da un tipo di lan ma non da un'altra

4.3.1. Standard IEEE per i BRIDGE:

Ci sono due tipi di bridge standardizzati:

- *transparent bridge*
- *source-routing bridge*

4.3.1.1. *Transparent bridge* :

Richiede la semplice connessione fisica e diviene immediatamente operativo in modo del tutto automatico, il meccanismo è il seguente:

- Dal momento in cui il bridge viene attivato esamina tutti i frame che gli arrivano dalle varie Lan e costruisce progressivamente le tabelle di instradamento, in particolare ogni frame ricevuto consente al bridge di sapere a quale lan appartiene la stazione che lo ha inviato
- ogni frame che arriva al bridge viene ritrasmesso
- se il bridge ha nelle sue tabelle d'instradamento l'indirizzo del destinatario invia il frame sulla lan corrispondente altrimenti invia il frame a tutte le lan connesse utilizzando la tecnica del *flooding*
- man mano che il bridge aumenta la sua conoscenza degli indirizzi delle varie macchine, la ritrasmissione diventa sempre più selettiva

Le tabelle del bridge vengono aggiornate ad intervalli di qualche minuto, rimuovendo gli indirizzi che delle macchine che non hanno più comunicato per qualche minuto, questa tecnica si chiama *backward learning*.