

Le reti LAN senza fili (**WLAN**, *Wireless LAN*) si impongono come modello laddove la connessione guidata via cavo è impossibilitata o costosa o inutilizzabile come nel caso di postazioni mobili. Molto spesso le WLAN si integrano a LAN su cavo preesistenti (*wired LAN*), spesso di tipo Ethernet 802.3, per consentire a determinate stazioni di connettersi a una rete cablata classica.

Lo standard IEEE che si occupa delle specifiche per le reti Wireless LAN è l'IEEE 802.11*.

Nel 1999 l'azienda statunitense Interbrand Inc. ha coniato il termine **Wi-Fi** (si può anche tradurre in *Wireless Fidelity*) che spesso è usato come sinonimo di WLAN 802.11 (anche in questo testo).

Ad oggi (2012) lo standard 802.11* si è evoluto fino alla versione 802.11n, anche se i vari standard nel tempo sono sostanzialmente considerati interoperabili. In sintesi:

Standard	Anno	Frequenza (GHz)	Bit rate (Mbit/s)
802.11	1997	2,4	1, 2
802.11a	1999	5,2; 5,4; 5,8	6, 9, 12, 18, 24, 36, 48, 54
802.11b	1999	2,4	1, 2, 5.5, 11
802.11g	2003	2,4	802.11a, 1, 2, 5.5, 11
802.11n	2009	2,4; 5,4	802.11g, 125, 144, 300

Wi-Fi e ISM

La banda **ISM** (*Industrial, Scientific and Medical*) è una porzione dello spettro elettromagnetico che, sia a livello nazionale che internazionale (anche se con qualche differenza) viene riconosciuto come disponibile liberamente e gratuitamente (anche se solo all'interno di aree private).

Altri tipi di frequenze, invece, sono ristrette da norme severe e rilasciate solo a pagamento. Siccome è intrinsecamente impossibile confinare una trasmissione radio all'interno di una precisa area privata, le normative nazionali tendono a liberalizzare l'uso del Wi-Fi a prescindere da questa limitazione.

La comunicazione wireless Wi-Fi avviene in frequenza radio all'interno della banda di frequenze denominata **ISM** (*Industrial, Scientific and Medical*) che ogni paese riserva ad applicazioni di radiocomunicazioni non commerciali, ma per uso industriale, scientifico e medico.

Wi-Fi può usare antenne omnidirezionali o direttive. Le antenne omnidirezionali sono utilizzate per distribuire la connettività in aree private, relativamente poco estese come aziende private ma anche sottoforma di **hotspot** pubblici (esempio, alberghi, aeroporti, uffici pubblici, ecc.) che attraverso una connessione Wi-Fi spesso offrono un accesso a WAN Internet.

Siccome la comunicazione avviene tramite onde radio, essa può essere messa in crisi da particolari condizioni (ostacoli come alberi, pilastri, muri di edifici), cosicché la portata dei dispositivi Wi-Fi non sempre rispetta i valori promessi, che sono circa 30 m per ambienti interni e circa 100 m per ambienti esterni.

Le antenne direttive sono in genere utilizzate per connettività più estese e sono poste in luoghi strategici per superare le barriere fisiche ambientali.

Come tutti i dispositivi che operano su frequenze radio, anche la tecnologia Wi-Fi genera *smog elettromagnetico* potenzialmente pericoloso per la salute. Bisogna ricordare però che la potenza degli apparati più diffusi è inferiore a quella emanata da un telefono cellulare.

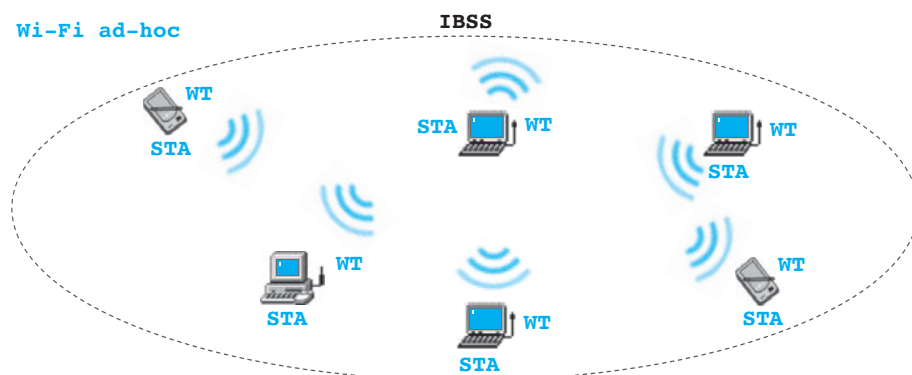
1 Modelli e terminologia

Le reti 802.11 possono presentarsi in due configurazioni differenti, tra loro trasparenti e conviventi: modello **ad-hoc**, in cui le stazioni sono paritarie, e modello **infrastructured**, in cui un apparato dedicato coordina il traffico delle stazioni ed è collegato ad una LAN.

In generale le singole stazioni operanti in Wi-Fi sono denominate **STA**, e sono dotate di un modulo di ricestrasmissione denominato **WT** (*Wireless Terminal*).

Organizzare moduli wireless in configurazione **ad-hoc** è la soluzione ideale per connettività temporanea tipo conferenze, sale riunioni, attività di gruppo all'aperto, ecc. La modalità non richiede particolari configurazioni. È studiata dal gruppo di lavoro IETF denominato *MANET* (*Mobile Ad hoc NETworks*) e in questo testo non sarà trattata.

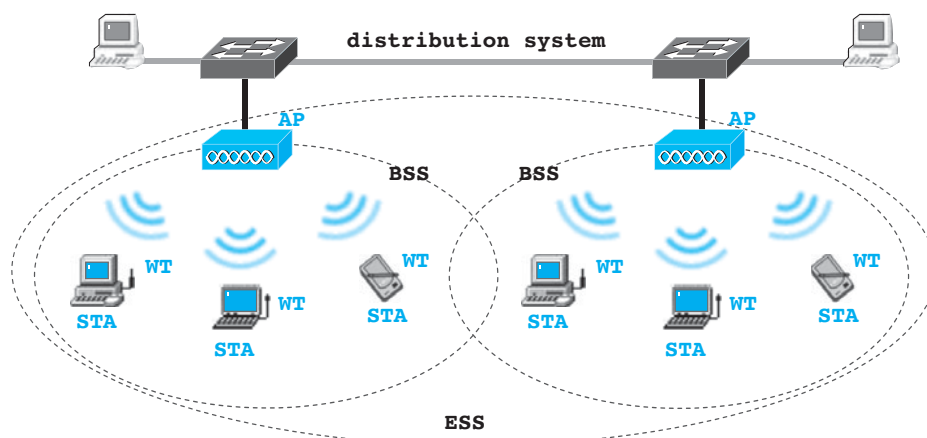
Wi-Fi ad-hoc



La modalità **infrastruttura** (infrastructured) è invece indicata per aggregare su una LAN preesistente e cablata (**distribution system**) uno o più gruppi di stazioni (**BSS**, *Basic Service Set*) attraverso un dispositivo dedicato denominato **Access Point** (**AP**).

Un insieme di BSS che si attestano sullo stesso distribution system è detto **ESS** (*Extended Service Set*).

Wi-Fi infrastructured



Quasi tutti gli Access Point commerciali possono essere configurati per operare in quattro modalità differenti. Quando si utilizza l'AP con un'unica BSS, tipico delle utenze residenziali, si dice modalità **root** (che è quella di fabbrica). Se l'AP deve coordinarsi con altri AP per costituire una ESS, allora va configurato in modalità **bridge**. Se invece lo si volesse usare come ripetitore di segnale per un altro AP, lo si può configurare in modalità **repeater**. Infine, anche se misconosciuta, la modalità **client** consente di trasformare un AP in un modulo WT per una stazione sprovvista di modulo Wi-Fi. In questo caso l'AP va connesso con un cavo Ethernet alla stazione che intende utilizzarlo come modulo WT.

2 MAC di IEEE 802.11

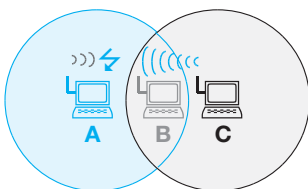
Wi-Fi è strutturalmente half duplex perché un dispositivo o trasmette o riceve. Il mezzo trasmissivo è denominato **etere**, e si può considerarlo condiviso esattamente come per Ethernet, ma in questo caso non è possibile rilevare le collisioni mentre si trasmette, come invece opera CSMA/CD.

Anche se un dispositivo wireless prima di trasmettere può stabilire se l'etere è impegnato, durante la trasmissione non è in grado di stabilire se altri dispositivi stanno a loro volta trasmettendo (collisione).

2.1 Stazione nascosta e stazione esposta

La modalità half duplex di Wi-Fi si può tradurre nel principio che, data la singola cella di portata radio di un dispositivo, è necessario che la stazione riceva da un solo trasmettitore alla volta.

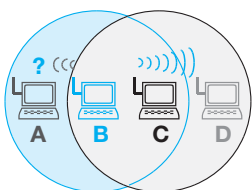
Questo comporta che possono presentarsi due problemi tipici delle comunicazioni radio half duplex, che impediscono del tutto di tentare un approccio con rilevamento di collisioni:



Stazione nascosta

In questo caso **B** sta ricevendo da **C**.

A vede il canale libero perché il segnale di **C** non gli arriva (**C** è fuori dalla cella di **A**), quindi trasmette, ma viola il principio (nella sua cella c'è una ricezione in corso).



Stazione esposta

In questo caso **D** sta ricevendo da **C**.

B vuole trasmettere ad **A**, ma non può farlo perché rileva una trasmissione nella sua cella e non sapendo dove si trovano **D** e **A**, non può rischiare. Però **B** avrebbe potuto trasmettere ad **A**, perché non è violato il principio (nessuna stazione sta ricevendo nella sua cella).

I due problemi suddetti vengono superati introducendo una breve fase di negoziazione, da effettuarsi prima di una qualsiasi trasmissione, tramite un protocollo **RTS/CTS** (*Request To Send/Clear To Send*).

In pratica il trasmettitore invita il ricevente (con un pacchetto RTS contenente l'indirizzo MAC del destinatario) a emettere un pacchetto (CTS), così che tutti i vicini del ricevente possano rendersi conto del tentativo di trasmissione in atto.

Qualunque stazione riceva un CTS viene a conoscenza del fatto che una ricezione sarà in corso nella propria cella.

Sarà così in grado di evitare di trasmettere, come nel caso della *stazione nascosta*: infatti A ha ricevuto il CTS di B.

Oppure potrà trasmettere, se necessario, come nel caso della *stazione esposta*: infatti B non ha ricevuto il CTS di D.

2.2 CSMA/CA

In Wi-Fi, non potendo rilevare le collisioni, si cerca di evitarle adottando il protocollo **CSMA/CA** (acronimo inglese di *Carrier Sense Multiple Access with collision avoidance*).

Per ottenere lo scopo il CSMA/CA usa la negoziazione RTS/CTS contenente il **NAV** (*Network Allocation Vector*): il pacchetto RTS, oltre all'indirizzo MAC del destinatario, contiene questo valore che indica la durata, in tempo, della trasmissione che si intende attuare. Anche il CTS di risposta contiene lo stesso NAV, in modo tale che qualsiasi stazione che riceve l'RTS o il CTS e non è coinvolta in questa sessione, possa impostare il valore di NAV in un proprio registro interno; questo valore verrà decrementato dalle stazioni in base al trascorrere del tempo, cosicché se una stazione ha il NAV diverso da zero, sa che è in atto una trasmissione nella sua cella. Questa condizione realizza un *Carrier Sense virtuale*: una stazione che vuole trasmettere sa che non può farlo se ha il NAV diverso da zero.

Dotato di Carrier Sense reale (rilevazione se l'etere è in idle, cioè libero) e del Carrier Sense virtuale (se il NAV è uguale a zero), una stazione può attuare il CSMA/CA:

- **Carrier Sense**. La stazione trasmittente cerca di determinare lo stato del mezzo valutando il contenuto di NAV ed ascoltando il mezzo. Il canale è considerato libero, quando sia il carrier sensing virtuale sia quello reale non rilevano attività.
- **Backoff**. Il trasmettitore attende che un proprio contatore interno di backoff vada a 0. Il contatore inizialmente parte da 7 e si decrementa nel tempo solo se il canale rimane libero. Se il canale viene occupato, il contatore rimane al valore che ha raggiunto, ma la stazione ritorna al Carrier Sense.
- **Carrier Sense virtuale**. La stazione emette un RTS. Se entro un intervallo di tempo ben definito (timeout), la stazione non riceve il CTS, deduce che c'è stata collisione. Allora riparte dal backoff, ma il valore iniziale del

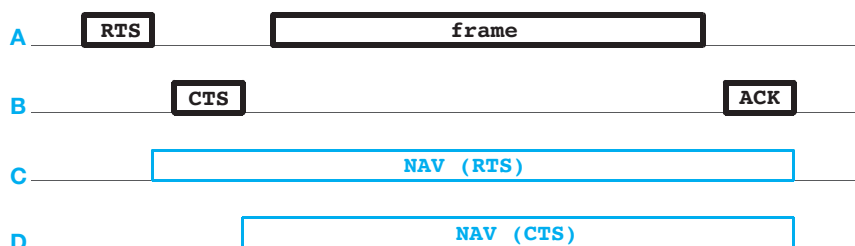
contatore di backoff verrà raddoppiato (esempio, varrà 15). Se invece il CTS viene ricevuto, il trasmettitore spedisce il pacchetto.

- **Data transmission.** Se entro un intervallo di tempo dopo aver spedito il pacchetto (timeout), il trasmettitore non riceve un riscontro dal ricevente (ACK), la procedura viene ripetuta da capo, e il contatore di backoff raddoppiato.

Il CSMA/CA di una trasmissione regolare dalla stazione A alla stazione B, con le stazioni C e D nelle vicinanze, può essere schematizzato dalla figura:

CSMA/CA semplificato

tempo →



SSID

Il **SSID** (*Service Set Identifier*) è, in effetti, la stringa che identifica un Access Point quando l'utente ricerca la lista dei dispositivi Wi-Fi in una certa area. Anche se generalmente un SSID specifica un Access Point, in effetti non è esattamente identificabile con un solo e determinato AP, dato che è normale che in una ESS vi siano più AP con lo stesso SSID o che un singolo AP possa possedere più di un SSID.

Quando C e D ricevono RTS e CTS, impostano il proprio NAV: ora sanno che il canale sarà occupato, e per quanto tempo.

Si nota che la stazione C è nella cella di A (riceve l'RTS), mentre D no.

A sua volta D è nella cella di B (riceve il CTS).

Un tipico inconveniente del CSMA/CA avviene durante la fase di trasmissione del pacchetto: la collisione viene rilevata solo dopo averlo spedito interamente e aver atteso invano l'ACK: più il pacchetto è grande, più tempo viene perso nel rilevare la collisione. Per questo motivo il MAC di 802.3 **frammenta** i pacchetti lunghi e li ricompatta in ricezione.

Purtroppo il CSMA/CA così descritto comporta numerose collisioni proprio sul pacchetto RTS (e CTS): pur «funzionando», il protocollo impone numerose fasi di backoff ripetute e/o numerose scadenze di timeout nella fase di Carrier Sense virtuale che fanno attendere inutilmente la stazione che deve trasmettere.

Per superare questo problema le stazioni si sincronizzano utilizzando un tempo base denominato **slot time** e suoi derivati: SIFS (<2 slot time), PIFS (SIFS+slot time), DIFS (SIFS+2 slot time), EIFS (SIFS+3 slot time).

L'analisi di queste sincronizzazioni, benché fondamentali per il funzionamento di 802.11, esula dagli obiettivi di questo testo.

3 Modalità infrastruttura

Nelle WLAN paritarie (o ad-hoc) è attivo solo il MAC descritto: ogni stazione può tentare di comunicare con ogni altra. Questa modalità è detta **DCF** (*Distributed Coordination Function*).

Nelle WLAN centralizzate (o infrastrutturate) è attiva anche una seconda modalità di comunicazione, detta **PCF** (*Point Coordination Function*).

Questa seconda modalità fu prevista per il traffico real time (esempio, flussi audio/video), ma nel 2005 fu resa obsoleta perché non ritenuta sufficientemente efficace (IEEE 802.11e-2005/2007).

La modalità operativa effettivamente utilizzata nei dispositivi Wi-Fi commerciali è quindi la **DCF** nella quale, in modalità infrastruttura, l'AP funge da **nodo coordinatore** (*point coordinator*).

Le comunicazioni tra le stazioni, infatti, dovranno compiere due passi nella rete senza fili: un primo passo dalla stazione sorgente all'AP e un secondo passo dall'AP alla stazione destinazione.

L'AP si serve dell'invio periodico di uno speciale pacchetto «broadcast» detto **beacon** che contiene varie informazioni generali come per esempio un valore per sincronizzare le stazioni (*timestamp*) e un valore per annunciarsi alle stazioni (**SSID**, *Service Set Identifier*). Il SSID è una stringa ASCII che consente l'identificazione dell'AP da parte dei client Wi-Fi.

3.1 Accesso alla rete

Una volta attivato l'AP e collegato alla rete cablata, si pone il problema dell'accesso alla rete wireless delle stazioni (STA). Esso avviene attraverso quattro fasi:

- **Scansione.** È il primo passo che una stazione deve intraprendere per individuare quante e quali reti Wi-Fi sono disponibili nel suo raggio di azione. La stazione può effettuare una scansione passiva, ovvero attendere i vari pacchetti di beacon circolanti nella sua cella e decodificare il SSID in essi contenuto. Oppure può richiedere espressamente la risposta ad uno speciale pacchetto (*probe request*) da parte degli AP disponibili sul suo canale.
- **Autenticazione.** Una volta selezionato il SSID, è necessario che la stazione si autentichi prima di poter operare. L'autenticazione può avvenire in diversi modi, anche se l'algoritmo di autenticazione con chiave condivisa basato su WPA2 è ritenuto accettabile.

Per una procedura di autenticazione più affidabile si può optare per l'utilizzo di servizi di autenticazione basati sullo standard **RADIUS** (*Remote Authentication Dial In User Service*, RFC 2865).

- **Associazione.** Una volta autenticata, la stazione richiede di poter entrare a far parte del BSS relativo all'AP. L'AP in questa fase memorizza in un buffer interno l'indirizzo MAC della stazione in modo da inserirla nel novero degli host raggiungibili dalla rete cablata Ethernet a cui è connesso.
- **Roaming.** Le stazioni mobili, per definizione, potrebbero spostarsi all'interno dell'ESS tra le varie BSS (tra un Access Point e un altro). Wi-Fi garantisce questi passaggi senza l'interruzione del servizio, mediante fasi di disassociazione/associazione determinate dalla circolazione dei pacchetti di beacon.

4 Il pacchetto MAC

In una rete Wi-Fi circolano vari tipi di pacchetti: pacchetti di **controllo**, (ACK, RTS e CTS); pacchetti di **gestione**, (beacon, probe request, probe response, association request, association response, ecc.) e pacchetti **dati**.

WPA2?

WPA2 (*Wi-Fi-Protected Access*) è lo standard che dal 2004 offre la sicurezza per i dispositivi Wi-Fi: tramite la scelta di una chiave condivisa (**PSK**, *Pre-Shared Key*) e usando l'algoritmo crittografico **AES** (*Advanced Encryption Standard*) garantisce, ad oggi, la protezione delle sessioni di comunicazione radio.

Purtroppo per un lungo periodo di tempo le PSK fornite dai più importanti costruttori di apparati Wi-Fi (Telecom, Fastweb e altri) si potevano dedurre, con opportuni calcoli, dal MAC address del dispositivo e/o dal SSID preimpostati dal costruttore.

Se l'utente non cambiava la chiave segreta fornita con l'apparecchio (la PSK), i dati pubblici del MAC address e del SSID consentivano di ricavarla: la rete Wi-Fi ora diventava utilizzabile da chiunque fosse nel raggio di portata dell'Access Point.

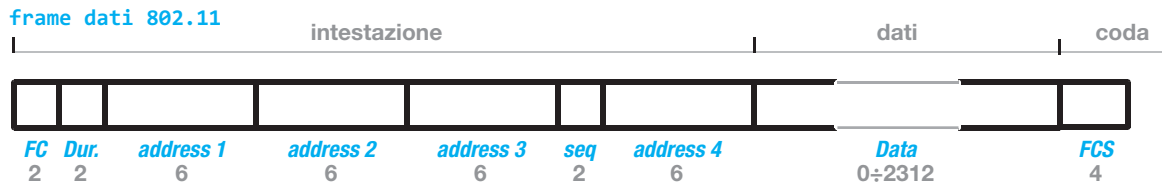
Un algoritmo potenzialmente sicuro (AES, 2012) non può nulla circa una erronea o ingenua scelta della chiave.

Radiotap header

Il **radiotap header** è una sequenza di byte che compare prima del frame 802.11, la cui lunghezza è sempre specificata dal terzo e quarto byte (little endian). Dato un pacchetto Wi-Fi in sequenza di ottetti, per raggiungere il pacchetto MAC di 802.11 (cioè il primo campo *Frame Control*) bisogna quindi saltare un numero di byte equivalente alla lunghezza dell'header radiotap.

I byte del radiotap header non circolano effettivamente in rete, ma sono creati dal driver che cattura i pacchetti. In essi è contenuta una sintesi delle informazioni del livello 1 Fisico di 802.11, come la frequenza del canale in uso, il segnale dell'antenna e la qualità del segnale attuale.

Il pacchetto dati di 802.11* è piuttosto articolato:



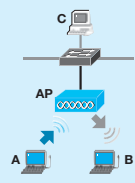
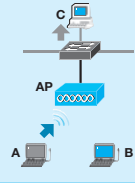
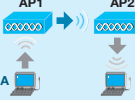
I campi del pacchetto:

- **FC**, *Frame Control*, campo codificato a bit che dispone i parametri dell'attuale trasmissione (da peso 15 a peso 0):
 - *SubType* (4 bit), specifica se RTS o CTS.
 - *Type* (2 bit), indica se pacchetto dati o pacchetto di servizio.
 - *Version* (2 bit), indica il numero di versione del protocollo.
 - *Order* (1 bit), indica se la sequenza in corso è ordinata.
 - *P* (1 bit), indica che il pacchetto è protetto (criptato).
 - *More* (1 bit), indica il frammento di un pacchetto.
 - *Pwr* (1 bit), usato dall'AP per sospendere una stazione.
 - *Retry* (1 bit), specifica se si tratta di un pacchetto ritrasmesso.
 - *MF* (1 bit), specifica se pacchetto frammentato.
 - *ToDS/FromDS* (2 bit), tipo di circolazione.
- **Dur.**, *Duration*, che indica la durata del pacchetto in termini di lunghezza. Serve per impostare il NAV.
- **address1**, **address2**, **address3**, **address4**, indirizzi MAC mittenti e destinatari, 6 ottetti come per 802.3, interpretati in base ai bit *ToDS* e *FromDS* del *Frame Control*.
- **S**, numero di sequenza del frammento.
- **FCS**, firma di integrità calcolata con CRC.

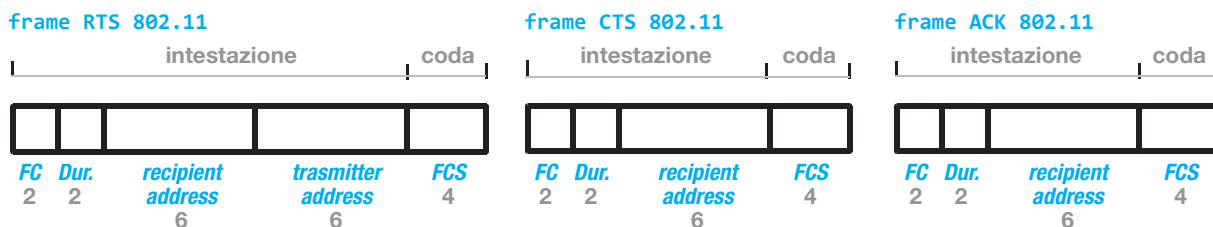
I tipi di circolazione dei pacchetti in Wi-Fi sono determinati dai bit *ToDS/FromDS* del *Frame Control* e seguono il seguente schema:

To DS	From DS	address 1	address 2	address 3	address 4	schema	nota
0	0	B	A	AP ^(NB)	–		solo modo ad-hoc
0	1	B	AP	A	–		downlink
0	1	B	AP	C	–		downlink

NB. In una combinazione **ad-hoc** una delle stazioni, di solito quella che viene avviata per prima, assume il compito di **master** per le altre, ovvero ha l'incarico di orchestrare la comunicazione come se fosse in Access Point, inviando regolarmente i pacchetti di beacon. L'identificazione della rete ad-hoc, ovvero della IBSS viene definita dalla stazione master generando un indirizzo MAC pseudocasuale (il contenuto del campo address 3).

1	0	AP	A	B	-		uplink
1	0	AP	A	C	-		uplink
1	1	AP2	AP1	B	A		interlink

I **pacchetti di controllo** hanno una struttura più semplice, senza parte dati e con un'intestazione breve:



RTS (*Type/Subtype* = 01/1011): Come per il pacchetto dati il campo *Frame Control* contiene la codifica a bit descritta; il campo *Duration* serve per impostare i NAV, e conterrà il valore temporale della dimensione del pacchetto che si intende trasmettere sommato al valore temporale di un CTS e un ACK necessari per completare la sessione. *Recipient address* contiene l'indirizzo MAC della stazione destinataria candidata, mentre *transmitter address* è l'indirizzo MAC del mittente.

CTS (*Type/Subtype* = 01/1100): Come per il pacchetto dati il campo *Frame Control* contiene la codifica a bit descritta; il campo *Duration* serve per impostare i NAV, e conterrà il valore temporale ricavato dal frame RTS appena ricevuto sottratto del valore temporale di un CTS. *Recipient address* contiene sempre l'*address 2* della trama dati ricevuta. Infatti, se si consulta la tabella precedente, in *address 2* compare sempre il destinatario della trama Wi-Fi.

ACK (*Type/Subtype* = 01/1101): Come per il pacchetto dati il campo *Frame Control* contiene la codifica a bit descritta; il campo *Duration* serve per impostare i NAV, ma solo se si tratta del riscontro a un pacchetto frammentato (cioè non l'ultimo di una sequenza). In questo caso è uguale al valore *Duration* contenuto nella trama dati ricevuta meno il tempo equivalente a un ACK. Se invece si tratta del riscontro all'ultimo frammento di un pacchetto (o di un pacchetto unico), situazione deducibile dal campo *More* del *Frame Control*, allora contiene 0. *Recipient address* contiene sempre il destinatario della trama Wi-Fi, come in CTS.

**Trama 802.11**

Data una sequenza di byte che rappresenta l'intestazione di una trama 802.11, scrivere un programma in linguaggio C che ne decodifichi il tipo.

LAYOUT

Frame 802.11: c4 00 68 00 00 0c 41 82 b2 55 55 09 cb 58 0e 00

Frame control=c400h (1100010000000000b): TYPE control; SUBTYPE CTS

Un programma in linguaggio C potrebbe essere:

```

00 #include <stdio.h>
01 #include <string.h>
02
03 #define TYPEMASK      (0x0c) //0ch = 00001100b
04 #define TYPE_MNGMT   (0x00) //00h = 00000000b
05 #define TYPE_CTRL    (0x04) //04h = 00000100b
06
07 #define SUBTYPEMASK   (0xf0) //f0h = 11110000b
08 #define SUBTYPE_RTS   (0xb0) //b0h = 10110000b
09 #define SUBTYPE_CTS   (0xc0) //c0h = 11000000b
10 #define SUBTYPE_ACK   (0xd0) //d0h = 11010000b
11
12 char* DectoszBin(int quale, int contenitore, char* szbinary);
13
14 int main (void)
15 {
16     unsigned char aFrame[14]={0xc4,0x00,0x68,0x00,0x00,0x0c,0x41,0x82,0xb2,0x55,0x55,0x09,0xcb,0x58};
17     char szMsg[80], szBinary[17];
18     int i;
19
20     printf("Frame 802.11: ");
21     for (i=0;i<16;i++) printf("%02x ",aFrame[i]);
22
23     strcpy(szMsg,"TYPE ");
24     if ((TYPEMASK & aFrame[0]) == TYPE_CTRL)
25     {
26         strcat(szMsg,"control; SUBTYPE ");
27         if ((SUBTYPEMASK & aFrame[0]) == SUBTYPE_ACK)
28             strcat(szMsg,"ACK");
29         else
30         {
31             if ((SUBTYPEMASK & aFrame[0]) == SUBTYPE_CTS) strcat(szMsg,"CTS");
32             else strcat(szMsg,"RTS");
33         }
34     }
35     else
36         strcat(szMsg,"management");
37
38     printf("\nFrame control=%02x%02xh (%sb): %s",
39         aFrame[0],aFrame[1],DectoszBin(aFrame[0]*0x100+aFrame[1],16,szBinary),szMsg);
40
41     return 0;

```