WI-FI 802.11

Lo standard 802.11 definisce due dispositivi:

1. **La Stazione Mobile**
   Una Stazione Mobile (MS) è normalmente un notebook equipaggiato con una wireless network interface card (NIC) di tipo PCMCIA oppure un personal computer con una scheda di rete 802.11, o ancora un terminale di diverso tipo con una soluzione embedded (es.: telefono cordless, stampante portatile di codici a barre, ecc…).

2. **L'Access Point**
   L'Access Point (AP) agisce da bridge tra la rete cablata e quella wireless. Esso è dotato di un'interfaccia radio (funzionante secondo una delle specifiche di livello fisico definite dallo standard), di una interfaccia di rete cablata (per esempio 802.3) e della logica di switching conforme allo standard 802.1d.

Lo standard 802.11 supporta tre principali tipi di topologia di rete:

- **Independent Basic Service Set (IBSS)**
- **Basic Service Set (BSS)**
- **Extended Service Set (ESS)**

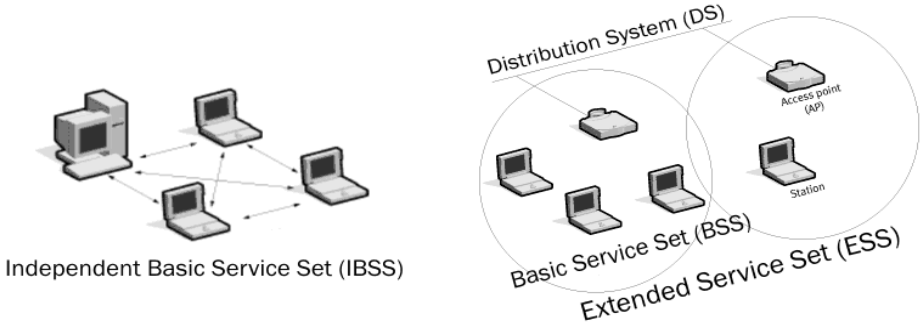


fig. 2-1 Possibili configurazioni di una WLAN 802.11

- **Independent Basic Service Set (IBSS)**
  La configurazione IBSS, anche detta *ad hoc* o *independent*, è costituita da un insieme di stazioni mobili che comunicano fra loro direttamente in modalità peer-to-peer senza la necessità di un nodo che faccia da server, senza l'uso di Access Point o di altri mezzi di connessione con la rete cablata.
  Questo tipo di topologia si rivela estremamente utile qualora vi sia l'esigenza di allestire rapidamente una rete locale provvisoria in luoghi in cui non sono disponibili strutture di rete di tipo fisso (per esempio sale riunioni, centri convegni, ecc…). Una rete *ad hoc* tuttavia non permette l'accesso a reti esterne.

- **Basic Service Set (BSS)**
  Un BSS consiste in almeno un Access Point connesso alla rete cablata e un insieme di terminali mobili.
  In questo tipo di topologia, anche definita *infrastructure,* le stazioni non comunicano direttamente fra loro come avviene in una rete *ad hoc* ma l'Access Point svolge il ruolo di server: le comunicazioni fra il nodo A e il nodo B transitano dal nodo A all'AP e quindi dall'AP al nodo B e viceversa.
  L'AP inoltre costituisce la via d'accesso per la rete esterna agendo come un bridge.

- **Extended Service Set (ESS)**
  Un Extended Service Set consiste infine in una serie di BSS contigui o parzialmente sovrapponentisi contenenti ciascuno un AP e connessi fra loro per mezzo di un *Distributed System* (DS).
  Sebbene lo standard non specifichi un particolare tipo di rete per il DS, questo è costituito solitamente da una LAN Ethernet.

I terminali mobili, associati ad un AP, possono così scambiare informazioni con tutti i terminali appartenenti all'ESS.
Lo standard 802.11 prevede inoltre la possibilità per una stazione mobile di migrare da un basic set ad uno contiguo gestito da un diverso AP senza che il servizio venga interrotto, rendendo possibile in questo modo la copertura di ampie aree. Lo standard tuttavia non definisce le procedure di handover che sono lasciate all'implementazione dei costruttori.

Il problema della mobilità degli utenti assume un ruolo fondamentale. Lo standard 802.11 distingue tra i seguenti tipi di mobilità:

- **No-transition :** questo tipo di mobilità si riferisce a stazioni che non si muovono ed a quelle che si muovono in una BSS;
- **BSS-transition :** questo tipo di mobilità si riferisce a stazioni che si muovono da una BSS in una ESS ad un'altra BSS nella stessa ESS;
- **ESS-transition :** questo tipo di mobilità si riferisce a stazioni che si muovono da una BSS in una ESS ad una BSS in un'altra ESS.

Lo standard 802.11 supporta i primi due tipi di mobilità, definendo i servizi logici necessari a gestire il mapping indirizzo-destinazione e l'integrazione trasparente di BSS multiple, ma non garantisce che una connessione continuerà dopo una ESS-transition.

All'interno di una ESS lo standard permette le seguenti configurazioni di BSS:

- **BSS che si sovrappongono parzialmente** : questa configurazione fornisce una copertura continua all'interno di un'area definita, condizione ideale se le applicazioni non tollerano interruzioni del servizio di rete;
- **BSS fisicamente disgiunte :** in questo caso la configurazione non fornisce copertura continua. Lo standard non specifica un limite di distanza tra BSS;
- **BSS fisicamente coincidenti :** questa configurazione è utile per fornire ridondanza o per realizzare una rete ad alte prestazioni.

Gli strati protocollari

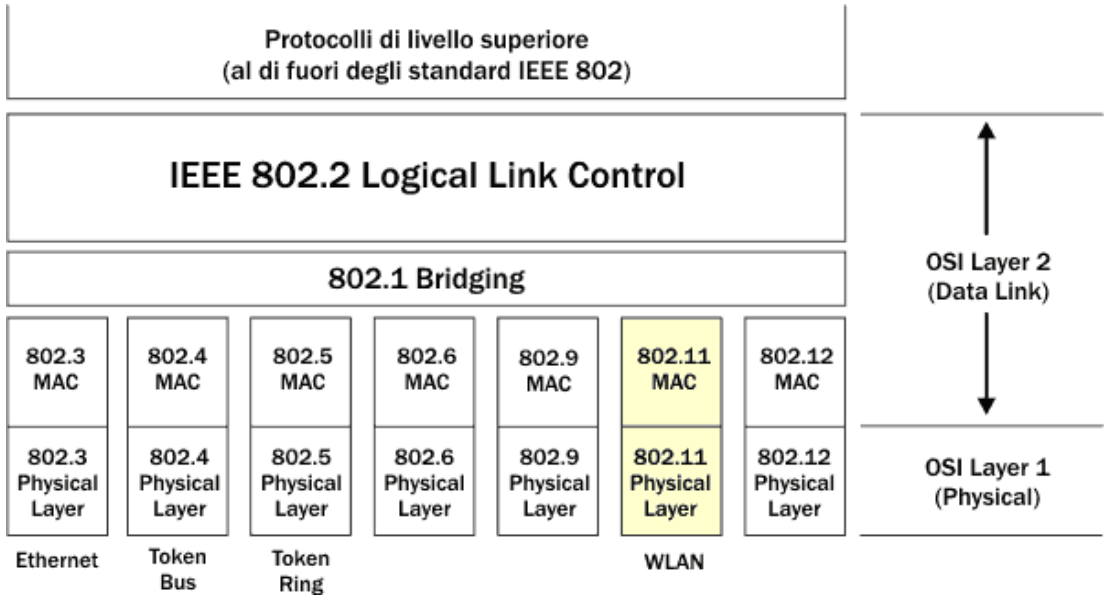


fig. 2-2 La Famiglia IEEE 802.

Lo standard 802.11 si inquadra nell'ambito della famiglia IEEE 802 come mostrato in fig. 2-2.

Il progetto 802, fa riferimento ai due livelli più bassi del modello ISO-OSI: il livello fisico (PHY) ed il livello di data link (DLL).
Quest'ultimo è suddiviso in due sottolivelli: il sottostrato di controllo del collegamento **LLC** (Logical Link Control) e il sottostrato di accesso al mezzo di comunicazione **MAC** (Medium Access Control). I dispositivi conformi alle specifiche 802.11 utilizzano il sottostrato di controllo LLC definito nello standard 802.2, lo stesso condiviso dagli altri sistemi 802 come Ethernet e Token Ring. In comune con questi ultimi sono inoltre le specifiche di bridging 802.1.
Lo standard 802.11 si occupa unicamente del sottostrato MAC, per quanto riguarda il livello data link, e del livello fisico. Per quest'ultimo sono state definite più specifiche, come descritto nel paragrafo seguente, mentre il MAC è unico.

In questo paragrafo vengono descritte le caratteristiche delle diverse opzioni disponibili per lo strato fisico: le tre originarie della prima release dello standard e le due introdotte con le estensioni 802.11a e 802.11b due anni dopo:

- **IR**: Trasmissione per mezzo di infrarossi.
- **FHSS**: Trasmissione radio a 2.4 GHz con tecnica di espansione dello spettro con salto delle frequenze e bit rate fino a 2 Mbit/s.
- **DSSS**: Trasmissione radio a 2.4 GHz con tecnica di espansione diretta dello spettro e bit rate fino a 2 Mbit/s.
- **HR/DSSS:** Trasmissione radio a 2.4 GHz con tecnica di espansione diretta dello spettro e bit rate fino a 11 Mbit/s. (High Rate).
- **OFDM**: Trasmissione radio a 5 GHz con bit rate fino a 54 Mbit/s.

La prima delle tre bande, a partire dai 902 MHz, è stata scartata perché già utilizzata massicciamente da altre tecnologie wireless (che avrebbero creato una pesante interferenza).

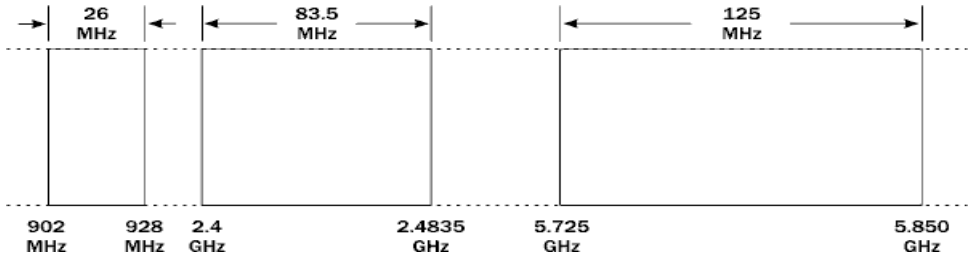


fig. 2-3 Bande ISM.

802.11 DSSS Physical Medium Dependent Sublayer

Per lo strato fisico DSSS, lo standard 802.11 prevede che al posto di ogni bit da trasmettere, venga trasmessa una sequenza di 11 *chip*, sempre uguale e pari a `10110111000` (se il bit vale zero, oppure il suo complemento, se il bit vale 1), detta *sequenza di Baker (*di fatto quindi, la trasmissione a velocità di 1 Mbit/s, ora produce un flusso di chip a velocità di 11 Mchip/s) in combinazione con una modulazione DBPSK o DQPSK per supportare rispettivamente un flusso a 1 o 2 Mbit/s.
Il codice di Barker offre un *processing gain* pari a 11, corrispondente a 10.4 dB. Il ricevitore può quindi tollerare fino a 10.4 dB di potenza interferente in più rispetto alla soglia data dal tipo di modulazione usato. Questa è una proprietà molto importante in uno scenario come quello in cui opera una WLAN caratterizzato dalla possibile coesistenza di diverse reti indipendenti che condividono la stessa banda ISM.
E' da notare che il codice utilizzato nelle operazioni di spreading e despreading è sempre lo stesso per tutti i terminali. Il suo utilizzo non ha infatti lo scopo di rendere intelligibile il contenuto informativo del segnale trasmesso a chi non sia a conoscenza della corretta sequenza di espansione, né quello di permettere un accesso multiplo allo stesso mezzo tramite l'uso di codici differenti da parte di diversi interlocutori (CDMA: Code division Multiple Access). Il motivo per cui la banda del segnale da trasmettere viene espansa è fondamentalmente quello di rendere il segnale stesso più robusto nei confronti di disturbi a banda stretta grazie alle proprietà delle trasmissioni spread spectrum illustrate in precedenza.

Come lo strato fisico FHSS, anche quello DSSS opera nella banda ISM compresa tra 2.4 GHz e 2.4835 GHz in base alla regolamentazione dell'utilizzo dello spettro vigente nei vari paesi. Lo standard 802.11 definisce per le trasmissioni DSSS, 14 canali di 22 MHz di banda l'uno all'interno del range totale di 83.5 MHz.

Numero Canale	*Frequenza centrale (GHz)*	*Numero Canale*	*Frequenza centrale (GHz)*
1	2.412	**8**	2.447
2	2.147	**9**	2.452
3	2.422	**10**	2.457
4	2.427	**11**	2.462
5	2.432	**12**	2.467
6	2.437	**13**	2.472
7	2.442	**14**	2.477

tab. 2-1 Canali DSSS e loro frequenze centrali.

Tutte le stazioni all'interno di uno stesso BSS condividono lo stesso canale; in una stessa area possono quindi coesistere fino ad un massimo di 3 BSS dato che si possono individuare fino ad un massimo di tre canali non sovrapponentisi. In fig. 2-4 sono mostrate le configurazioni suggerite dallo standard per l'allocazione di tre canali indipendenti, la separazione tra le portanti è fissata a 30 MHz.

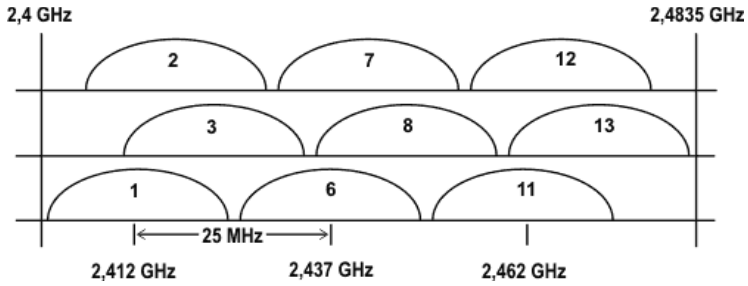


fig. 2-4 Possibili configurazioni per l'allocazione di 3 canali.

Come accennato in precedenza, questo tipo di strato fisico prevede due possibili bit-rate: 1 Mbit/s e 2 Mbit/s per mezzo dell'utilizzo di due diversi tipi di modulazione che vengono applicati direttamente al segnale espanso.

Per la modalità ad 1 Mbit/s viene impiegata la **DBPSK (Differential Binary Phase Shift Key)**; essa consiste nel variare la fase della portante di0 o 1 80° per trasmettere rispettivamente il simbolo "1" o "0".

Per la modalità a 2 Mbit/s, si utilizza la **DQPSK (Differential Quaternary Phase Shift Key)**. In questo caso si raggiunge la velocità di trasmissione di 2 Mbit/s, per mantenendo quella di segnalazione pari a 1 Msimboli/s, attribuendo ad ogni simbolo 2 bit di informazione. Come prima, ad ogni bit da trasmettere si associano gli 11 chip della sequenza di Baker, e la sequenza di chip così ottenuta, viene presa 2 chip alla volta, per produrre un segnale modulato QPSK differenziale, in cui ad ogni simbolo avviene un cambio di fase, corrispondente alle seguenti coppie di chip:

b_0,b_1	*Cambiamento di fase*
00	0°
01	90°
11	180°
10	270°

tab. 2-2 Codifica DQPSK.

Le possibili variazioni di fase sono ora di 4 tipi.

La potenza in trasmissione per questo tipo di strato fisico è stabilita dallo standard tra un minimo di 1 mW ad un massimo che dipende dalle regolamentazioni nazionali (100 mW in Europa).

Caratteristiche dei protocolli MAC per reti wireless

Lo strato di accesso al mezzo fisico MAC (Medium Access Control) fa parte del livello data link della pila ISO – OSI. Esso si occupa di:

- Gestione delle procedure di accesso al canale.
- Indirizzamento a livello di collegamento.
- Allestimento dei frame.
- Controllo d'errore.
- Frammentazione e riassemblaggio dei datagrammi[1].

Lo standard 802.11 appartiene alla vasta categoria dei "sistemi a contesa": in questo tipo di reti più utenti condividono lo stesso canale con la possibilità quindi che si verifichino conflitti. La banda assegnata ad un basic set in una WLAN 802.11 non è gestita infatti con tecniche a divisione di tempo (TDMA), frequenza (FDMA) o codice (CDMA) ma utilizzata per intero da una stazione mobile alla volta in base ad una specifica politica di gestione delle contese così come accade in una rete LAN cablata.
Le reti *wireless* costituiscono un terreno di sfida estremamente interessante per i protocolli di accesso a contesa. Questo è dovuto fondamentalmente alle carenze del mezzo fisico utilizzato e alla necessità di dover gestire una risorsa di solito maggiormente limitata rispetto a quella a disposizione per le reti cablate.

I principali problemi che sorgono nella gestione di un canale radio, a differenza di quanto accade nella controparte *wired,* sono essenzialmente due. Il primo è noto come il problema dell'"*hidden node*" o "nodo nascosto" e si verifica quando alcuni nodi della rete non si rilevano tra loro. Un tipico caso è quello mostrato in fig. 2-5: la stazione A e la stazione B sono entrambe rilevate dall'Access Point e sono in grado di comunicare con esso ma, a causa della distanza a cui si trovano, non sono a conoscenza l'una della presenza dell'altra. A causa di questa situazione una stazione può interrompere la trasmissione dell'altra semplicemente perché non è in grado di rilevare che il canale è occupato.

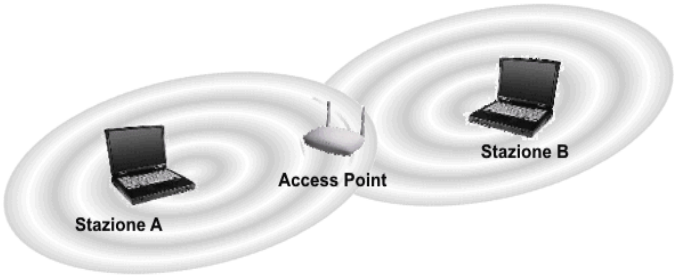


fig. 2-5 Esempio di *hidden node.*

Il secondo inconveniente è dovuto all'impossibilità da parte di una stazione mobile di *ascoltare* il canale mentre sta trasmettendo. Questo impedisce di utilizzare la funzione di rilevazione delle collisioni come implementato dal protocollo CSMA/CD (Carrier Sense Multiple Access with Collision Detection) impiegato da Ethernet. Quando due stazioni trasmettono contemporaneamente, esse non sono in grado di accorgersi che si sta verificando una collisione; l'unico modo per capire se una trasmissione è avvenuta con successo o no è utilizzare il meccanismo degli *acknowledge*: al termine di una ricezione corretta la stazione ricevente invia un riscontro positivo al mittente. Se entro un tempo prefissato quest'ultimo non riceve l'acknowledge, esso apprende che un problema è occorso alla trasmissione, ma non può distinguere quale sia stata la causa del fallimento: una collisione, un errore sul frame o la non raggiungibilità del destinatario. Tuttavia, in una rete *wireless,* questo rappresenta l'unico modo per permettere la rilevazione di errori nel corso della comunicazione.

Lo strato MAC dello standard IEEE 802.11

Lo standard 802.11 supporta, per il sottolivello MAC, tre possibili modalità di gestione dell'accesso al mezzo di comunicazione, la prima è obbligatoria, le altre due opzionali:

[1] Altre importanti funzioni a livello MAC, non indirizzate direttamente allo scambio di dati, sono svolte dal MAC Management Sublayer descritto in seguito nel paragrafo

- **DCF** (Distributed Coordination Function) **basic access**. Sistema a contesa basato sul protocollo CSMA/CA (CSMA with Collisione Avoidance).
- **DCF con handshake.** Modalità analoga alla precedente con scambio aggiuntivo di pacchetti di Request-to-Send (RTS) e Clear-to-Send (CTS) per ottenere l'accesso al canale.
- **PCF** (Point Coordination Function). Gestione *contention-free* del mezzo di comunicazione grazie alla presenza di un coordinatore che assegna la possibilità di trasmettere ad una singola stazione alla volta.

Distributed Coordination Function

Tutte le stazioni conformi allo standard 802.11 supportano questa modalità di accesso. Essa permette il trasferimento asincrono dei dati su una base *best effort* e può essere utilizzata sia nelle reti *ad hoc* che nelle reti *infrastructure*.
La DCF si basa sul protocollo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), una estensione del CSMA standard descritto in precedenza studiato per minimizzare la probabilità che una stazione rilevi come libero un canale occupato, a causa del ritardo di propagazione con cui la stazione riceve il segnale.
Con la tecnica di *collision avoidance* le stazioni non possono trasmettere se non dopo aver rilevato il canale libero per un intervallo di tempo prefissato; questo intervallo di silenzio è scelto sufficientemente grande per compensare il più alto ritardo di propagazione tra i nodi della rete ma allo stesso tempo non troppo esteso per non penalizzare i tempi di trasmissione.
Il meccanismo adottato è una combinazione di *carrier sense* fisico e virtuale che permette al MAC di determinare se il mezzo è libero o occupato.

- Lo strato fisico valuta lo stato del canale e lo comunica al MAC che effettua a sua volta il *carrier sense* virtuale usando l'informazione contenuta nel campo Duration di ogni trama.
- Quest'informazione viene copiata nel NAV (network allocation vector) della stazione.
- Il NAV effettua un conto alla rovescia dal valore del campo Duration fino a zero. Finito il conteggio, se lo strato fisico segnala che il canale è libero, la stazione può trasmettere.
- L'ascolto del canale da parte dello strato fisico e l'uso del NAV forniscono allo strato MAC le informazioni necessarie a decidere se iniziare o meno una trasmissione.

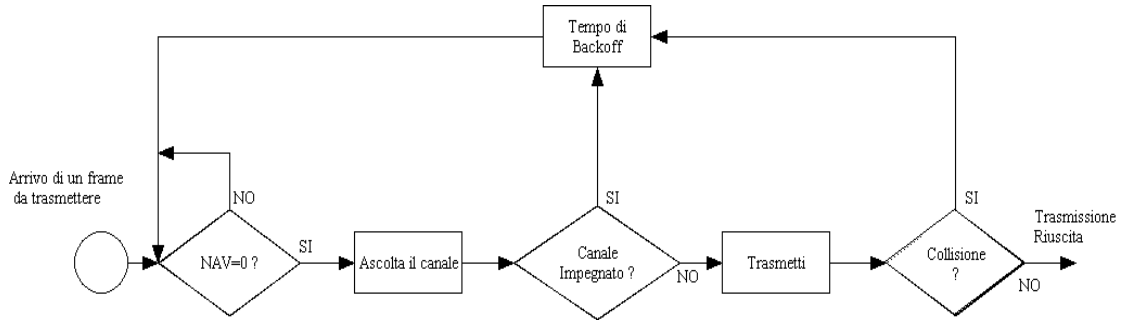


Figura 0.1 *DCF utilizza una combinazione di carrier-sense fisico e virtuale*

- Lo scopo del protocollo CSMA/CA è di diminuire la probabilità che due stazioni trasmettano contemporaneamente. Il periodo di tempo in cui tale probabilità è massima è quello immediatamente seguente una trasmissione. Questo si verifica perché, durante una trasmissione, le stazioni che hanno bisogno di impegnare il canale si mettono in attesa e quando il canale si libera provano a trasmettere contemporaneamente.
- Una stazione con un nuovo pacchetto da trasmettere ascolta il canale.
- Se lo trova libero per un tempo pari ad un DIFS (Distributed InterFrame Spacing) trasmette immediatamente.
- Altrimenti, se il canale è occupato (sia immediatamente sia durante il DIFS), la stazione continua ad ascoltare il canale finché non lo trova libero per un intervallo di durata DIFS.
- A questo punto attende un intervallo di tempo casuale (detto tempo di backoff), per minimizzare la probabilità di collisione con altre stazioni in attesa.
- In più, per evitare la cattura del canale, la stazione deve attendere un tempo di backoff tra due trasmissioni consecutive di nuovi pacchetti, anche se il canale è libero per un DIFS.

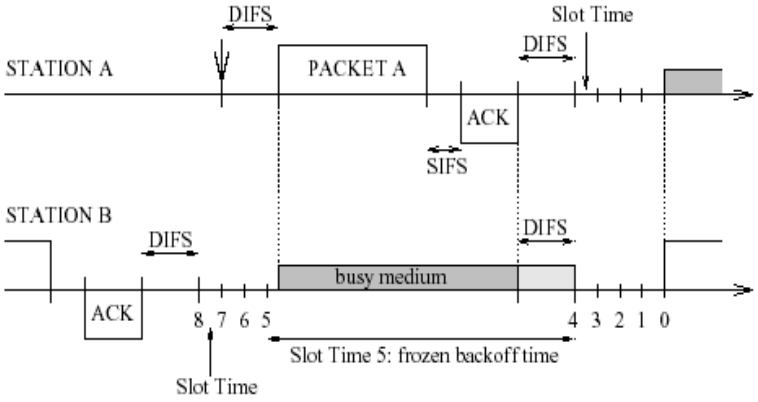


Figura 0.2 *Il meccanismo di Accesso Base*

Per ragioni di efficienza, la DCF utilizza tempi di backoff discreti. Il tempo che segue il DIFS di inattività è suddiviso in intervalli (detti Slot Time) ed una stazione inizia a trasmettere solo all'inizio di uno Slot Time. La durata dello Slot Time è posta uguale al tempo necessario ad ogni stazione per individuare la trasmissione di un pacchetto da parte di ogni altra stazione. Questo tempo dipende dallo strato fisico utilizzato e tiene conto del ritardo di propagazione, del tempo necessario a passare dallo stato di ricezione a quello di trasmissione (RX_TX_Turnaround_Time) e del tempo necessario a segnalare allo strato MAC lo stato del canale (Busy Detect Time).

La DCF adotta uno schema di backoff esponenziale binario.

- Ad ogni trasmissione, il tempo di backoff è scelto con distribuzione uniforme nell'intervallo (0, W_i-1). Il valore di W_i è chiamato *Contention Window* (finestra di contesa) e dipende dal numero di trasmissioni fallite precedentemente.
- Al primo tentativo di trasmissione W_i è posto uguale al valore CW_{min} chiamato finestra di contesa iniziale.
- Dopo ogni trasmissione fallita, W_i è raddoppiato, fino ad un valore massimo $CW_{max} = 2^m CW_{min}$.

PHY	***Slot Time***	***W_{min} (in S.T.)***	***W_{max} (in S.T.)***	***m***
FHSS	50 μs	16	1024	6
DHSS	20 μs	32	1024	5
IR	8 μs	64	1024	4

tab. 2-3 Parametri di backoff specificati dallo standard 802.11

Le trame RTS e CTS contengono la lunghezza del pacchetto da trasmettere. Questa informazione può essere letta da tutte le stazioni in ascolto che possono quindi aggiornare il NAV. Di conseguenza, quando una terza stazione non può comunicare con la stazione trasmittente o con quella ricevente deve solo individuare una trama tra RTS e CTS e può

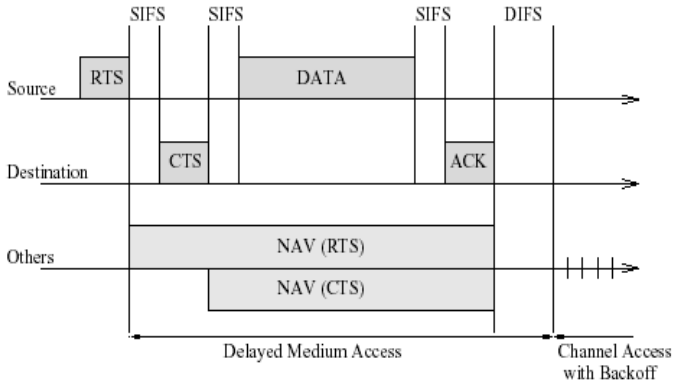


Figura 0.3 *Il meccanismo di accesso RTS/CTS*

ritardare la trasmissione, evitando la collisione. Questo risolve il problema del terminale nascosto.

Il meccanismo RTS/CTS è molto efficiente in termini di prestazioni, specialmente se si considerano pacchetti di grandi dimensioni, perché riduce la lunghezza dei pacchetti coinvolti nel processo di contesa. Infatti, nell'assunzione di canale ideale, una collisione può avvenire solo quando due o più stazioni trasmettono nello stesso Slot Time. Se tutte le stazioni impiegano RTS/CTS le collisioni avvengono solo sui pacchetti RTS e sono individuate immediatamente data la mancanza di pacchetti CTS.

Point Coordination Function

La modalità di accesso PCF si basa sulla possibilità di gestire in maniera centralizzata il canale. Questo avviene per mezzo di un *Point Coordinator* (PC), normalmente l'AP, che abilita a turno le singole stazioni a trasmettere senza dover contendere per l'acceso al mezzo di comunicazione. La tecnica PCF è opzionale e, quando attiva, si alterna temporalmente con la DCF come si vede in figura.

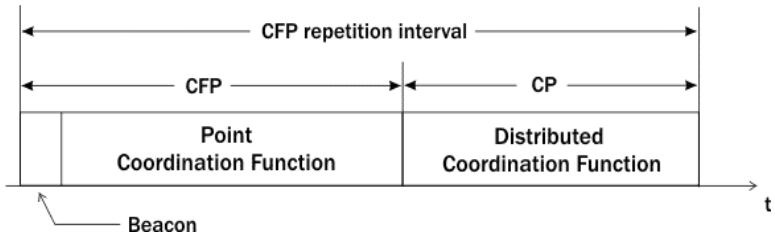


fig. 2-6 Coesistenza di PCF e DCF.

All'interno di un *Contention Free Period repetition interval*, una porzione di tempo, denominata *Contention Free Period* (CFP), è gestita per mezzo della PCF mentre la restante, detta *Contention Period* (CP), è regolata secondo la tecnica a contesa DCF.
L'AP può decidere, in base ad algoritmi non specificati dallo standard, quanto tempo destinare al CFP in ogni *repetition interval* in base alle condizioni di traffico esistenti.
La durata massima del CFP può invece essere impostata manualmente agendo sul MIB.
All'inizio di un intervallo di ripetizione, l'Access Point ascolta il canale attendendo un tempo di silenzio pari ad un PIFS (avendo quindi una maggiore priorità rispetto alle altre stazioni che durante la contesa aspettano un DIFS).
Una volta ottenuto l'accesso al canale, l'AP trasmette quindi un frame di *beacon* con le informazioni sulla durata del CFP. Tutte le stazioni settano il proprio NAV in base ad esso garantendo al point coordinator il controllo del mezzo per tutto il CFP.
In questo intervallo i terminali possono trasmettere solo in risposta ad una chiamata (*polling*) del point coordinator o per inviare un riscontro un SIFS di tempo dopo aver ricevuto correttamente un pacchetto.

Nel corso del CFP l'Access Point può inviare pacchetti dati, pacchetti di CF-*poll* per consentire ad una specifica stazione di accedere al canale, o acknowledge.
Il terminale interpellato con un CF-*poll* può rispondere con un CF-ACK per accedere al canale e inviare un pacchetto, oppure con un *Null Function frame* se non ha nulla da trasmettere.
Spesso i pacchetti dati, di polling e gli acknowledge, vengono accorpati con una tecnica di *piggybacking* per aumentare l'efficienza della trasmissione come mostrato in fig. 2-7.
Per terminare il CFP e lasciare che il tempo rimanente dell'intervallo di ripetizione sia gestito tramite DCF, il Point Coordinator trasmette un CF-*end* frame.

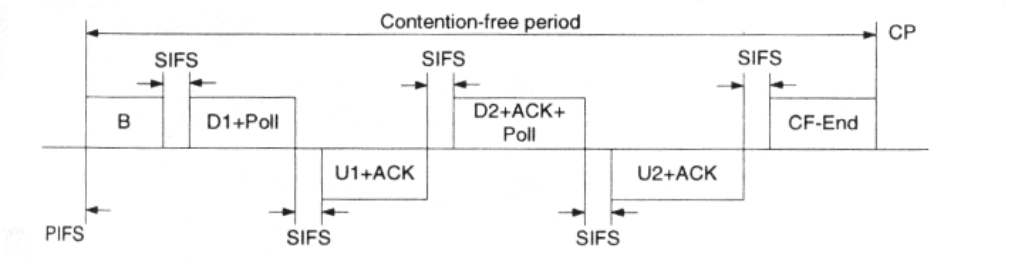


fig. 2-7 Trasmissioni tra point coordinator e una stazione in modalità PCF.

Le specifiche 802.11 definiscono 3 diversi tipi di *Inter Frame Space* (IFS) cioè intervalli di attesa tra la trasmissione dei pacchetti:

- **Short IFS** (SIFS)
  L'intervallo più breve dei tre e garantisce quindi il più alto grado di priorità. Il SIFS è utilizzato dalle stazioni prima della trasmissione di frame che necessitano con particolare urgenza di giungere a destinazione, specificatamente: i riscontri, i frame CTS di richiesta del canale e i pacchetti contenenti il secondo (o successivo) frammento di uno stesso datagramma.
- **Point Coordination IFS** (PIFS)
  Viene utilizzato dalle stazioni che funzionano in modalità PCF. Questo attribuisce un maggiore livello di priorità a queste stazioni rispetto a quelle che impiegano lo schema DCF. Quest'ultime infatti, prima di trasmettere un frame dati, devono rilevare il canale libero per un **DIFS**.
- **Distributed Coordination IFS** (DIFS)
  Il più lungo tra gli *inter frame space*. La durata di un DIFS è solitamente fissata ad un valore pari alla durata di un SIFS più due volte quella di uno *slot time di sistema*. Quest'ultimo rappresenta il più piccolo intervallo di tempo definito nelle specifiche dello standard. Tutti gli altri tempi (dagli IFS ai timer di backoff) sono sempre suoi multipli interi. La durata dello slot time di sistema può essere fissata manualmente agendo sul *Management Information Base* (MIB) di una stazione mobile o di un Access Point.

L'uso di intervalli di attesa di durata diversa prima della trasmissione di un pacchetto permette la gestione di una scala di priorità tra le stazioni che tentano di accedere al canale.

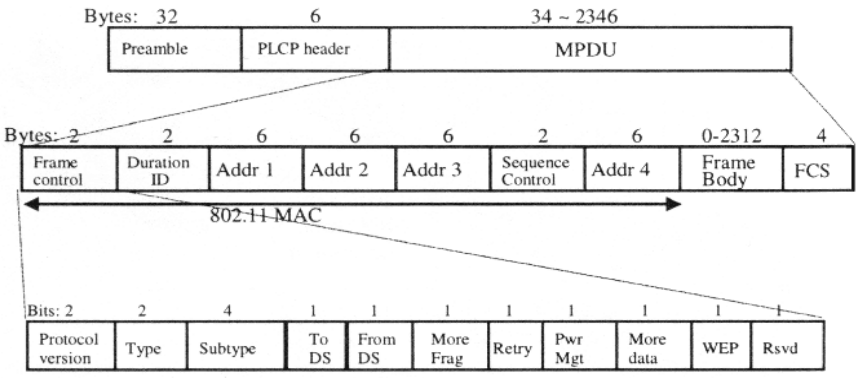
Virtual Carrier Sensing

Per migliorare le prestazioni dello strato d'accesso, lo standard 802.11 prevede l'implementazione di un meccanismo detto di *virtual carrier sensing*. Esso si affianca alla operazione di rilevamento di trasmissione effettuato tramite l'ascolto "fisico" della portante. All'interno di ogni MPDU è presente un campo, detto *duration field*, che indica il tempo totale (in microsecondi) dopo il quale, a partire dalla fine della ricezione del frame corrente, il canale sarà nuovamente libero e disponibile per una nuova trasmissione. Questa informazione è utilizzata da tutte le stazioni di un BSS per aggiornare il proprio *Network Allocation Vector* (NAV). Esso indica l'ammontare di tempo necessario per completare la sessione di trasferimento in corso e al termine della quale è possibile controllare nuovamente lo stato del canale.

Frame

Per effettuare la consegna di MSDU tra terminali 802.11, lo strato MAC utilizza diversi tipi di frame ciascuno specifico per un particolare scopo. Lo standard definisce tre categorie:

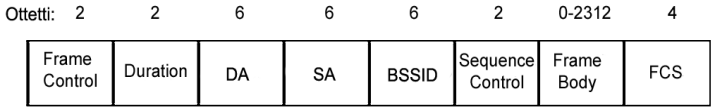
- **Management Frames.** Sono impiegati nelle operazioni di associazione e disassociazione con l'Access Point, nelle procedure di autenticazione e per la gestione della sincronizzazione.
- **Control Frames.** Comprendono i frame di handshake RTS e CTS, i riscontri ACK e i pacchetti di gestione degli intervalli senza contesa nella modalità PCF: PS-poll e PS-end.
- **Data Frames.** Sono utilizzati per la trasmissione di dati destinati agli strati superiori del terminale ricevente. In modalità PCF, durante gli intervalli gestiti senza contesa, possono essere combinati con acknowledge e comandi di polling.



Formato MAC-PDU

Trame di gestione

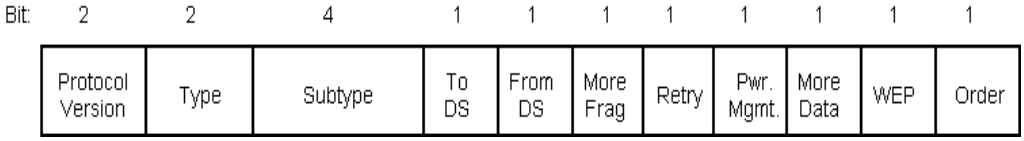
Lo scopo delle trame di gestione è di stabilire le comunicazioni preliminari tra le stazioni e gli AP, fornendo servizi come l'autenticazione e l'associazione.



Una stazione che riceve una trama di gestione confronta l'indirizzo contenuto nel campo DA con il proprio: se i due coincidono, copia la trama e la passa agli strati protocollari più alti, altrimenti la ignora.
Nei periodi a contesa (quelli gestiti da DCF), il campo Duration delle trame di gestione assume i valori seguenti:

- se l'indirizzo di destinazione è un indirizzo di gruppo, il campo Duration è posto a zero;
- se **More Frag=0** e l'indirizzo di destinazione è un indirizzo individuale, il campo Duration contiene il numero di microsecondi necessari a trasmettere un ACK ed un SIFS;
- se **More Frag=1**e l'indirizzo di destinazione è un indirizzo individuale, il campo Duration contiene il numero di microsecondi necessari a trasmettere il frammento successivo, due ACK e tre SIFS.

Campo Frame Control



Il campo **Frame Control** contiene le seguenti informazioni di controllo:

- **Protocol Version :** per lo standard attuale questo campo vale sempre zero
- **Type :** questo campo indica se una trama è di gestione, di controllo o di dati
- **Subtype :** questo campo definisce la funzione della trama
- **To DS :** il MAC pone questo campo ad 1 in tutte le trame destinate al sistema di distribuzione
- **From DS :** questo campo vale 1 se la trama proviene dal sistema di distribuzione
- **More Frag :** questo campo è posto ad 1 se un altro frammento della stessa MSDU viene trasmesso in una trama seguente
- **Retry :** se la trama ha già subito una collisione, questo campo è posto ad 1
- **Power Management :** questo campo indica la modalità di risparmio energetico in cui si troverà la stazione dopo aver trasmesso la trama corrente; un 1 indica che la stazione sarà in modalità di Risparmio Energetico, uno 0 indica che sarà in modalità Attiva
- **More Data :** se una stazione ha altre MSDU da mandare ad una stazione in modalità Risparmio pone questo campo ad 1; questo permette alla stazione ricevente di tenersi pronta per altre trasmissioni
- **WEP :** un 1 in questo campo avverte la stazione ricevente che il corpo della trama è stato crittato con l'algoritmo WEP
- **Order** : questo campo è posto a 1 nelle trame trasmesse usando la classe di servizio StrictlyOrdered ed indica alla stazione ricevente che tali trame vanno elaborate in ordine

Tipi di trame di gestione

In base al valore di Subtype

- **Association Request** - una stazione invia questa trama per richiedere l'associazione con un AP
- **Association Response** - dopo aver ricevuto una richiesta di associazione, l'AP invia questa trama di risposta per indicare se ha accettato o meno l'associazione
- **Reassociation Request** - una stazione invia questa trama se si vuole riassociare con un AP. Una riassociazione può avere luogo quando una stazione esce dalla portata di un AP e si avvicina ad un altro.
  La stazione si dovrà riassociare (e non solo associare) con il nuovo AP in modo che quest'ultimo sappia che deve negoziare l'inoltro di trame dati dal vecchio AP.

- **Reassociation Response** - un AP invia questa trama per indicare se ha accettato o meno una richiesta di riassociazione
- **Probe Request** - una stazione invia una trama di questo tipo per ottenere informazioni da un'altra stazione. Per esempio, può inviare una trama di Probe Request per determinare se un certo AP è disponibile
- **Probe Response** - una stazione che riceve un Probe Request risponde con una trama di questo tipo inviando le informazione che le erano state richieste
- **Beacon** - in una rete di tipo infrastructure, un AP invia periodicamente dei Beacon che forniscono sincronizzazione alle stazioni con lo stesso strato fisico; il Beacon contiene un timestamp che le stazioni usano per aggiornare ciò che lo standard definisce funzione di sincronizzazione dei tempi (*timing synchronization function*, TSF)
- **ATIM** - se una stazione ha del traffico in attesa per altre stazioni invia loro una trama ATIM (*announcement traffic indication message*) durante la finestra ATIM, che segue immediatamente la trasmissione di un Beacon; in seguito la stazione trasmette le trame in attesa a chi è in grado di ricevere.
- **Disassociation** - se una stazione o un AP vuole terminare un'associazione, invia questa trama; una singola trama di dissociazione può concludere l'associazione con più di una stazione contemporaneamente
- **Authentication** - una stazione invia una trama di autenticazione ad un AP col quale si vuole autenticare; la sequenza di autenticazione dipende dal tipo di autenticazione implementata (a sistema aperto o a chiave comune)
- **Deauthentication** - una stazione invia questa trama per terminare la comunicazione sicura.

Associazione

Una volta identificato un Access Point per accedere alla rete, la stazione mobile deve associarsi ad esso. Le comunicazioni tra l'AP e la stazione sono le seguenti:

- La stazione invia una serie di *probe* (scanning attivo);
- uno o più AP inviano una risposta con le informazioni relative al proprio BSS;
- dopo aver selezionato il migliore AP la stazione mobile invia ad esso una richiesta di associazione (*association request*);
- l'AP interpellato invia alla stazione una risposta (*association response*).

Sicurezza

Possono essere adottate diverse modalità di protezione delle comunicazioni all'interno di una rete wireless basata sul protocollo 802.11, tra i quali il filtraggio degli indirizzi MAC oppure l'utilizzo di sistemi come WEP (Wired Equivalent Privacy) ed IPSec. Generalmente i tre metodi base per garantire un accesso sicuro ad un AP all'interno di reti 802.11 sono:

- Service set identifier (SSID)
- Filtraggio degli indirizzi Media Access Control (MAC)
- Wired Equivalent Privacy (WEP)

E' possibile implementare uno di questi metodi, anche se usarli tutti insieme assicura una soluzione più robusta.

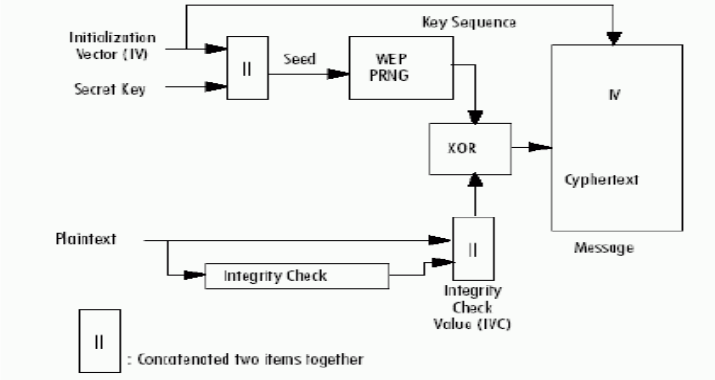
SSID

Il Service Set ID è generalmente una stringa leggibile all'uomo (una sorta di nome di rete) che rappresenta una chiave segreta condivisa (password): all'inizio era stata concepita per permettere a gruppi diversi di usare AP diversi. Un SSID può essere associato ad un AP oppure ad un gruppo di AP, come una forma di controllo di accesso alla rete e come semplice password: gli SSID forniscono un meccanismo per "segmentare" una rete wireless in diverse reti servite da uno o più AP.
Per accedere alla rete, i client devono essere stati preventivamente configurati con l'SSID corretto.
L'uso di un SSID rappresenta però una soluzione debole per la protezione delle comunicazioni e la garanzia di un accesso sicuro poiché in primo luogo la stringa non è cifrata ma risulta essere distribuita in chiaro; inoltre l'indentificativo della rete deve essere noto a tutto coloro che la stanno attualmente utilizzando (diventa un segreto ampiamente condiviso) ed è per questo che l'AP lo invia periodicamente in broadcast. Tale comportamento compromette la già minima sicurezza fornita da un sistema di protezione che utilizza gli SSID.

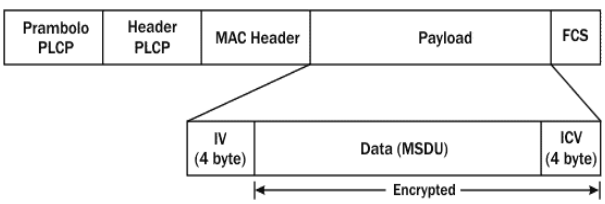
WEP

Lo standard 802.11 prevede due tipi di autenticazione: open system o shared key. La prima permette a qualsiasi client di accedere alla WLAN; tutti i pacchetti scambiati tra la stazione e l'AP per effettuare l'operazione di autenticazione e associazione avvengono in chiaro, senza cifratura.
La modalità di autenticazione *shared key* offre invece un maggiore grado di sicurezza grazie al protocollo WEP (*Wired Equivalent Privacy*). Affinché la stazione possa accedere alla WLAN, occorre che essa sia in possesso delle stesse chiavi condivise dall'AP. Lo standard presume che queste chiavi siano state consegnate alla stazione attraverso un canale sicuro. La procedura di autenticazione è illustrata in figura:

Il client che desidera l'accesso alla WLAN invia un richiesta di autenticazione all'Access Point il quale risponde con una stringa generata casualmente di 128 byte detta "di sfida". Il client utilizza quindi questa stringa, insieme alla chiave da lui posseduta e all'algoritmo WEP, per ricavare una sequenza criptata che recapita all'AP. L'Access Point, che nel frattempo ha effettuato la stessa operazione in parallelo alla stazione, controlla quindi che la stringa ricevuta corrisponda a quella da lui ottenuta e, in caso affermativo, autorizza l'accesso. Segue a questo punto la procedura di associazione.
WEP utilizza l'algoritmo di cifratura simmetrico RC4 PRNG (*Ron's Code 4 Pseudo Random Number Generator*) a 64 bit. Esso presuppone che venga distribuita, alle stazioni a cui è permesso l'accesso alla rete, una chiave segreta (WEP *key*) a 40 bit che viene impiegata sia nella procedura di cifratura che in quella di decifratura.
In trasmissione la chiave WEP (*static key*) viene concatenata con un vettore di inizializzazione (IV) a 24 bit. La stringa



così ottenuta viene inviata in ingresso ad un generatore di numeri pseudo-casuale per ottenere in uscita una sequenza di *k* byte che costituisce la chiave di cifratura vera e propria.
Per ogni pacchetto da trasmettere l'operazione di cifratura viene effettuata calcolando il risultato della funzione logica di "XOR" tra la chiave di cifratura di *k* byte e la sequenza di uguale lunghezza composta dal payload del pacchetto più 4 byte di ICV (*Integrity Check Value*) introdotto dal protocollo WEP come controllo aggiuntivo sull'integrità del frame. Alla stringa criptata viene anteposto il vettore di inizializzazione in chiaro e il tutto trasmesso come payload del MPDU.



In ricezione la stazione estrae per prima cosa il vettore di inizializzazione dal payload del MPDU e lo usa, insieme alla propria chiave WEP (la stessa del mittente), per ricavare tramite il PRNG la chiave di cifratura. Quindi utilizza la chiave così ottenuta per decifrare il resto del payload. Esso è composto dai dati veri e propri e l'ICV. Per controllare se la procedura di decifrazione è avvenuta correttamente, la stazione calcola l'ICV sulla sequenza dati e lo confronta con l'ICV contenuto nel pacchetto ricevuto. Se questi coincidono vuol dire che la chiave usata è corretta e i dati possono essere inviati al sottolivello LLC, altrimenti si verifica un errore e il pacchetto viene scartato.

Numerosi studi hanno messo in evidenza come il sistema di autenticazione e cifratura definito dallo standard 802.11, e basato sul protocollo WEP, sia piuttosto debole e facilmente eludibile da chi volesse violarlo per accedere clandestinamente alla WLAN. Questo è dovuto principalmente all'utilizzo "statico" delle chiavi WEP che rende un eventuale furto di hardware sufficiente per entrare in possesso di tutti gli elementi necessari per effettuare l'autenticazione e decifrare le informazioni scambiate sul canale. E' stato dimostrato inoltre che le chiavi di cifratura possono essere ricavate abusivamente grazie a semplici software e poche ore di "ascolto" delle comunicazioni.

Rischi conosciuti

Sebbene intrusioni nelle reti 802.11 cresceranno indubbiamente nel tempo in numero e complessità, i rischi attualmente vengono classificati in sette categorie:

- Inserimento di apparati non autorizzati nella rete.
- Intercettazione e monitoraggio non autorizzato del traffico di rete.
- Disturbo del segnale radio (jamming).
- Attacchi punto-punto.
- Attacchi a forza bruta contro le password dei punti di accesso.
- Attacchi ai meccanismi di cifratura.
- Errori di Configurazione.

Bisogna notare che queste classificazioni sono riconducibili a qualsiasi tecnologia wireless, non soltanto allo standard 802.11b.

Inserimento di apparati non autorizzati nella rete

Queste tipologie di attacco si basano sull'installazione di dispositivi non autorizzati o sulla creazione di nuove reti wireless al di fuori di ogni meccanismo di controllo della sicurezza. Si hanno i seguenti casi:

- **Terminali non autorizzati** – Un aggressore cerca di connettere un terminale mobile, tipicamente un laptop o un PDA, a un punto di accesso senza autorizzazione. I punti di accesso dovrebbero essere configurati per richiedere una password per garantire l'accesso alla rete alle macchine.
- **Punti di Accesso non autorizzati** – Un organizzazione può non venire a conoscenza dell'installazione di una rete wireless all'interno della rete aziendale. Questo porta ad attacchi descritti nel punto precedente, con terminali non autorizzati che ottengono l'accesso a risorse aziendali tramite un punto di accesso nascosto.

Intercettazione e monitoraggio non autorizzato del traffico di rete

Così come avviene nelle reti cablate, è possibile nelle reti 802.11 monitorare il traffico tramite appositi programmi. L'aggressore deve trovarsi nel raggio d'azione del punto di accesso per effettuare l'intrusione; in ambito wireless è sufficiente catturare il flusso di dati dalla propria postazione.
Si è esposti a uno dei seguenti rischi:

- **Analisi dei pacchetti** – Un aggressore con particolari competenze può catturare il traffico di rete, con tecniche simili a quelle utilizzate nelle reti cablate. La maggior parte di questi strumenti catturano la prima parte della sessione di collegamento, dove all'interno sono contenuti normalmente il nome utente e la password. Quindi l'intruso si può collegare alla rete come utente autorizzato e compiere azioni proibite.
- **Monitoraggio del traffico di broadcast** – Se il punto di accesso viene collegato ad un hub piuttosto che a uno switch, tutto il traffico sulla rete cablata viene inoltrato al punto di accesso, permettendo l'analisi da parte di un aggressore di ulteriori dati non destinati ai terminali mobili.
- **Intercettazione del traffico tramite clonazione del Punto di Accesso (Evil Twin)** – Un aggressore può dirottare la connessione dei dispositivi wireless verso la propria rete installando un punto di accesso con un segnale più potente nelle loro vicinanze. Gli utenti tenteranno di collegarsi ai falsi server, fornendo nome utente e password e qualsiasi altra informazione riservata.

Disturbo del segnale radio (jamming)
Attacchi tesi a provocare il rifiuto del servizio (DoS – Denial of Service) possono essere implementati anche in questo ambito. Un aggressore, con un adeguato equipaggiamento, è in grado di disturbare la banda di frequenze attorno ai 2.4 Ghz, corrompendo il segnale emesso dai dispositivi e causando l'inutilizzo della rete. In aggiunta, telefoni senza filo, dispositivi per il monitoraggio dei neonati, terminali Bluetooth o altri apparati operanti alla frequenza di 2.4 Ghz possono disturbare le trasmissioni radio nella rete. Queste cessazioni di attività della rete possono essere provocate da dispositivi al di fuori del raggio d'azione dei punti di accesso, o inavvertitamente da altre reti 802.11 installate nelle vicinanze.

Attacchi punto-punto
Due terminali wireless possono comunicare direttamente nella modalità ad-hoc, non utilizzando il punto di accesso. L'utente deve difendersi non soltanto da attacchi esterni ma anche dalle altre macchine sulla rete.

- **Attacchi alle condivisioni di rete e altri servizi TCP/IP** – Terminali su cui operano servizi quali server Web o condivisione dei file sono esposti agli stessi rischi presenti nel caso di reti cablate.
- **Rifiuto del Servizio (DoS – Denial of Service)** – Un dispositivo wireless può congestionare la rete trasmettendo una notevole quantità di pacchetti. Inoltre, indirizzi IP o MAC duplicati, sia voluti sia accidentali, possono creare ulteriori problemi nella rete.

Attacchi a forza bruta contro le password dei punti di accesso
La maggior parte dei punti di accesso utilizzano un'unica chiave condivisa da tutti i dispositivi sulla rete. Attacchi a forza bruta basati su un dizionario precostruito cercano di comprometterla, testando periodicamente ogni possibile combinazione. L'aggressore, una volta in possesso della password, entrerà a far parte della rete.
In aggiunta le password possono essere scoperte attraverso mezzi meno aggressivi. Un terminale che sia stato compromesso può esporre a rischi il relativo punto di accesso.

Attacchi ai meccanismi di cifratura
Lo standard IEEE 802.11 prevede la possibilità di utilizzo del protocollo WEP – Wired Equivalent Privacy – come mezzo di cifratura dei dati trasmessi. Il protocollo WEP si avvale del noto algoritmo di cifratura RC4. Lo scopo del WEP è costituire un livello di sicurezza pari alle reti cablate; in realtà tale scopo non è stato raggiunto per un errato utilizzo dell'algoritmo RC4. Come visto in precedenza il protocollo WEP prevede l'utilizzo di un vettore di inizializzazione (IV) per la codifica dei dati: proprio l'uso di quest'ultimo ha determinato la maggior debolezza del protocollo WEP: infatti l'algoritmo RC4 risulta vulnerabile se vengono utilizzate le chiavi più di una volta.
Questo è esattamente quello che accade con il WEP: il vettore di inizializzazione è lungo soltanto 24 bit, quindi ammette uno spazio di 224 combinazioni. In aggiunta, il protocollo WEP prevede la reinizializzazione del'IV ogni qual volta si origini una collisione nella trasmissione dei pacchetti dati. In una rete di medie dimensioni e con un discreto volume di traffico sono sufficienti pochi minuti affinché vengano riutilizzate le chiavi di cifratura.
Tramite meccanismi di criptoanalisi differenziata, ad esempio, si può risalire in poco tempo alla chiave WEP e decifrare tutto il traffico da quel momento.

Attacchi al protocollo WEP attuali

- **Attacchi a forza bruta –** Nel caso generatore di chiavi a 40 bit ci vogliono 20 secondi per ricavare la chiave, poiché esso utilizza solamente 21 bit dello spazio delle chiavi disponibile. Una chiave generata in maniera sicura invece potrebbe richiedere un rete distribuita di computer per essere ricavata. Le chiavi a 104 bit risultanto ancora immuni ad attacchi a forza bruta.
- **Attacchi FMS -** Fluhrer, Mantin e Shamir hanno dimostrato la debolezza dell'algoritmo KSA[2] (Key Scheduling Algorithm) dell'RC4 utilizzato nell'implementazione WEP. Il loro attacco si basa sull'utilizzo del solo primo byte della sequenza pseudo-random prodotto dall'output generator di RC4.

Errori di Configurazione
Molti punti di accesso sono configurati dalle case produttrici in maniera errata, privilegiando la facilità d'uso e d'installazione alla sicurezza.

[2] Inizializza i fattori generativi della chiave. Genera una permutazione che appare casuale della shared key; la permutazione è ciclica con un periodo molto lungo (più di 10100).

Architettura con incremento della sicurezza

Per risolvere i problemi di sicurezza introdotti dal protocollo WEP sono stati progettati sistemi alterrnativi per la gestione sicura dei meccanismi di autenticazione e delle comunicazioni.

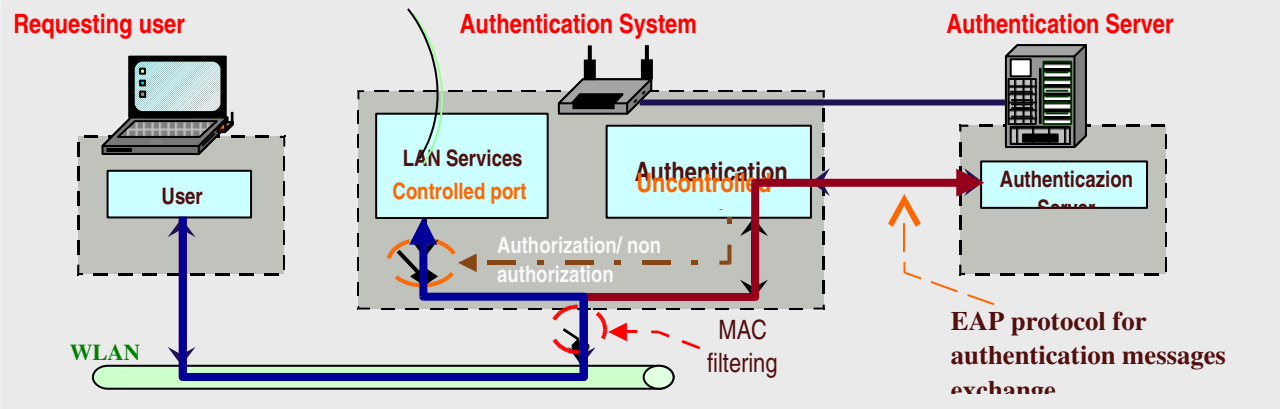
- Server RADIUS con entià separate (client, unità di accesso all'autenticazione, unità centrale di autenticazione). Remote Authentication Dial-In User Service (RADIUS) è un protocollo client/server ed un software che permette a dei server di accesso remoto di comunicare con un server centrale per autenticare gli utenti ed autorizzarli ad accedere ai servizi
- Protocolli di sicurezza IEEE802.1x
- EAP/TLS (Extendibile Authentication Protocol / Transport Layer Security) -

  Extensible Authentication Protocol (EAP) è un semplice protocollo progettato per il trasporto di informazioni arbitrarie di autenticazione: per le comunicazioni tra la MS e l'AP viene utilizzato EAP over LAN (EAPOL), mentre per le comunicazioni tra AP e server di autenticazione viene utilizzato EAP over RADIUS.

  Transport Layer Security – è la versione standardizzata da RFC di SSL e viene trasportata su EAP : impiegato in maniera specifica nei processi di autenticazione.

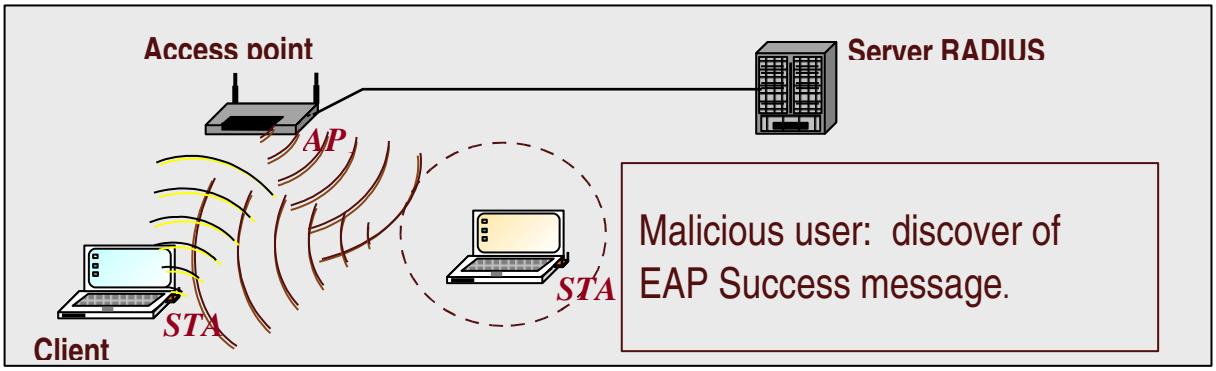
IEEE 802.1x

Lo standard IEEE per i servizi di autenticazione in un LAN



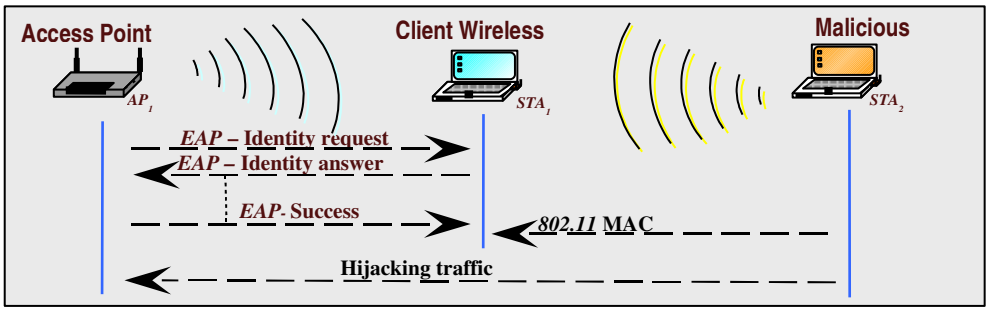
Limiti di EAP

- Attacco *Man In the Middle*



Una terza entità non autorizzata agisce tra l'AP e la MS.
Devia la trasmissione su se stesso in maniera trasparente: né il client né l'AP si possono rendere conto che il flusso è stato modificato.

- Dirottamento



Basato sull'intercettazione del messaggio EAP-Success inviato dall'AP al client ed utilizzato per chiudere la procedura di autenticazione reciproca. Dopo tale messaggio si comincia una sessione “sicura”.

IPsec

IPsec è l'abbreviazione di **IP Security** ed è uno standard per ottenere connessioni basate su IP sicure. La sicurezza viene raggiunta attraverso la cifratura e l'autenticazione dei pacchetti IP. La sicurezza viene fornita, quindi, a livello di rete. La capacità di fornire protezione a livello di rete rende questo protocollo trasparente al livello delle applicazioni che non devono essere modificate.
IPsec è una collezione di protocolli formata da

- Protocolli che forniscono la cifratura del flusso di dati
- Protocolli che implementano lo *scambio delle chiavi* per realizzare il flusso crittografato.

Per quanto riguarda il primo aspetto, esistono due protocolli:Authentication Header (AH) e Encapsulated Security Payload (ESP). **ESP** fornisce autenticazione, confidenzialità e controllo di integrità del messaggio ed è il protocollo IP 50. **AH**, invece, garantisce l'autenticazione e l'integrità del messaggio ma non offre la confidenzialità; per questo motivo ESP è molto più usato di AH; AH è il protocollo IP 51. Attualmente esiste un solo protocollo per lo *scambio delle chiavi*, il protocollo **IKE**. IPsec è parte integrante di IPv6, mentre è opzionale in IPv4.

Wi-Fi Protected Access (WPA)

E' un protocollo per la sicurezza delle reti wireless Wi-Fi creato per tamponare i problemi di scarsa sicurezza del precedente protocollo di sicurezza, il WEP. Studi sul WEP avevano individuato delle falle nella sicurezza talmente gravi da renderlo quasi inutile. Il WPA implementa parte del protocollo IEEE 802.11i e rappresenta un passaggio intermedio per il raggiungimento della piena sicurezza, quando i dispositivi implementeranno completamente tale standard.
WPA è progettato per utilizzare lo standard 802.1x per gestire l'autenticazione dei server e la distribuzione di differenti chiavi per ogni utente, sebbene per questioni di compatibilità supporta la precedente gestione a chiave condivisa (PSK).
I dati sono cifrati con l'algoritmo di cifratura a blocchi RC4 con chiave a 128 bit e vettore di inizializzazione a 48 bit.
Una delle modifiche che introducono maggiore robustezza all'algoritmo è la definizione del Temporal Key Integrity Protocol (TKIP). Questo protocollo dinamicamente cambia la chiave in uso e questo combinato con il vettore di inizializzazione di dimensione doppia rispetto al WEP rende inefficaci i metodi di attacco utilizzati contro il WEP.
In aggiunta all'autenticazione e alla cifratura il WPA introduce notevoli miglioramenti nella gestione dell'integrità. Il CRC utilizzato dal WEP non era sicuro, era possibile modificare il messaggio mantenendo coerente in CRC anche senza conoscere la chiave. Per evitarlo il WPA utilizza un nuovo metodo per verificare l'integrità dei messaggi (MIC – Message integrity check) chiamato "Michael". Questo include un contatore associato al messaggio per impedire all'attaccante di ritrasmettere un messaggio che è già stato trasmesso nella rete.
In sostanza il WPA aumenta la dimensione della chiave, il numero delle chiavi in uso, include un sistema per verificare l'autenticità dei messaggi migliore e quindi incrementa la sicurezza della WLAN rendendola effettivamente analoga a quella di una rete su cavo.