Università di Genova
Facoltà di Ingegneria

Architetture e Protocolli per Reti Wireless

2. Reti Wireless in area locale, personale e d'accesso

2.1 Standard IEEE 802.11 (Wi-Fi)

Prof. Raffaele Bolla

dist

Introduzione
Wireless LAN

- Le ***Wireless* LAN** (WLAN) sono reti *wireless* che forniscono coperture e servizi tipici di una LAN
  - si tratta di reti in area locale in cui i le stazioni terminali (e talvolta anche i nodi intermedi) usano collegamenti senza fili;
  - sono pensate come reti mobili, ma la mobilità è in genere intesa come relativamente lenta;
  - il loro scopo principale è quello sia di agevolare i cablaggi che "liberare" gli utenti da postazioni di lavoro fisse.
  - Sono usate anche come reti d'accesso

Introduzione

Peculiarità dell'ambiente *wireless*

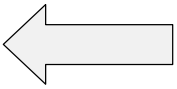
- Tipo di mezzo "difficile"
  - Interferenze e rumore
  - Qualità variabile nello spazio e nel tempo
  - Condiviso con eventuali elementi WLAN "non richiesti"
  - Condiviso con elementi non-WLAN
- Non si può assumere la connettività completa (stazioni nascoste)
- Diversi regolamenti internazionali

Introduzione

Peculiarità dell'ambiente *wireless*

- Presenza della mobilità
  - Variazione della affidabilità del collegamento
  - Funzionamento a batteria: *power management*
  - Gestione del movimento
- Sicurezza
  - Nessun confine fisico
  - LAN sovrapposte

WirelessLAN

- Fra gli standard importanti in questo ambito vanno citati:
  - IEEE 802.11 
  - HIPERLAN (*European HIgh PERformance* LAN)
  - (Bluetooth)
  - HomeRF - Shared Wireless Access Protocol - Cordless Access (SWAP-CA)

WirelessLAN – IEEE 802.11

- Lo standard IEEE 802.11 è stato pubblicato nel 1997
  - inizialmente prevedeva l'utilizzo della banda ISM 2.4 GHz e le velocità di trasmissione a 1-2 Mb/s.
- Nel 1999 è stato aggiornato (**IEEE 802.11:1999**)
  - introduzione di nuove modulazioni e velocità più elevate;
  - definizione di due nuove versioni: **802.11a** e **802.11b**.
- Sempre nel 1999 è stato adottato dall'OSI/IEC come 8802-11:1999.
- Nel 2003 una ulteriore evoluzione ha portato alla definizione delle specifiche **802.11g**.
- Questo standard è anche chiamato **Wireless Fidelity** (**Wi-Fi**) dal nome di una associazione di costruttori che lo promuove e verifica la inter-operabilità dei prodotti

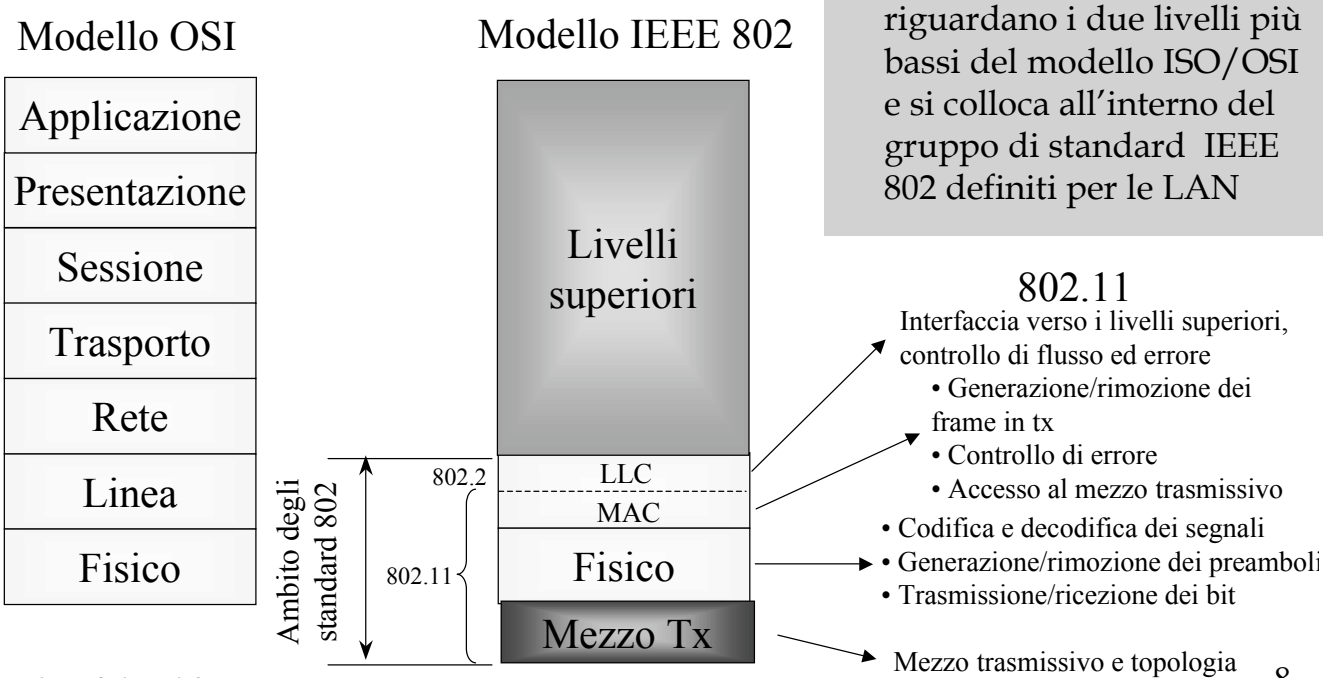
IEEE 802.11

Requisiti di progetto

- Un singolo MAC che supporti diversi livelli fisici
  - Canali singoli e multipli
  - Differenti caratteristiche di "*Medium sense*"
- Permettere la sovrapposizione di più reti nella stessa area geografica
- Robustezza all'interferenza
- Risolvere il problema dei nodi nascosti
- Fornire supporto ai traffici con requisiti di ritardo massimo

IEEE 802.11

- Le specifiche del protocollo riguardano i due livelli più bassi del modello ISO/OSI e si colloca all'interno del gruppo di standard IEEE 802 definiti per le LAN



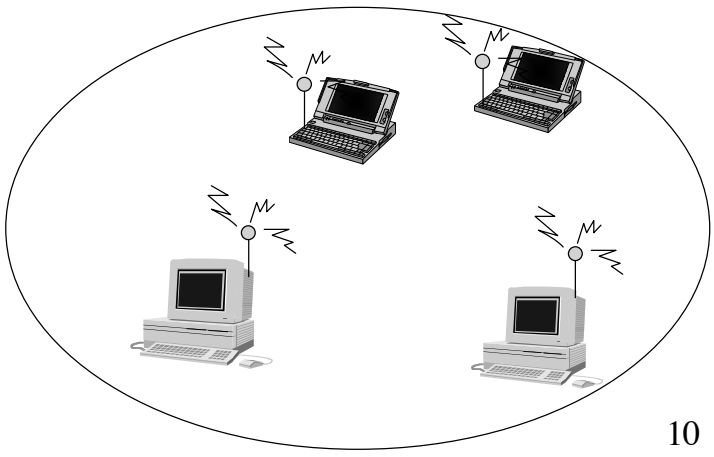
Architettura di rete

- Lo standard definisce due diverse tipologie architetturali:
  - ***Independent Basic Service Set*** (**IBSS**);
  - ***Extended Service Set*** (**ESS**).
- L'elemento base è rappresentato dal ***Basic Service Set*** (BSS), l'area entro la quale tutte le stazioni possono comunicare tra loro.
  - una stazione può muoversi entro il BSS, ma non può più comunicare direttamente con le altre se ne esce.

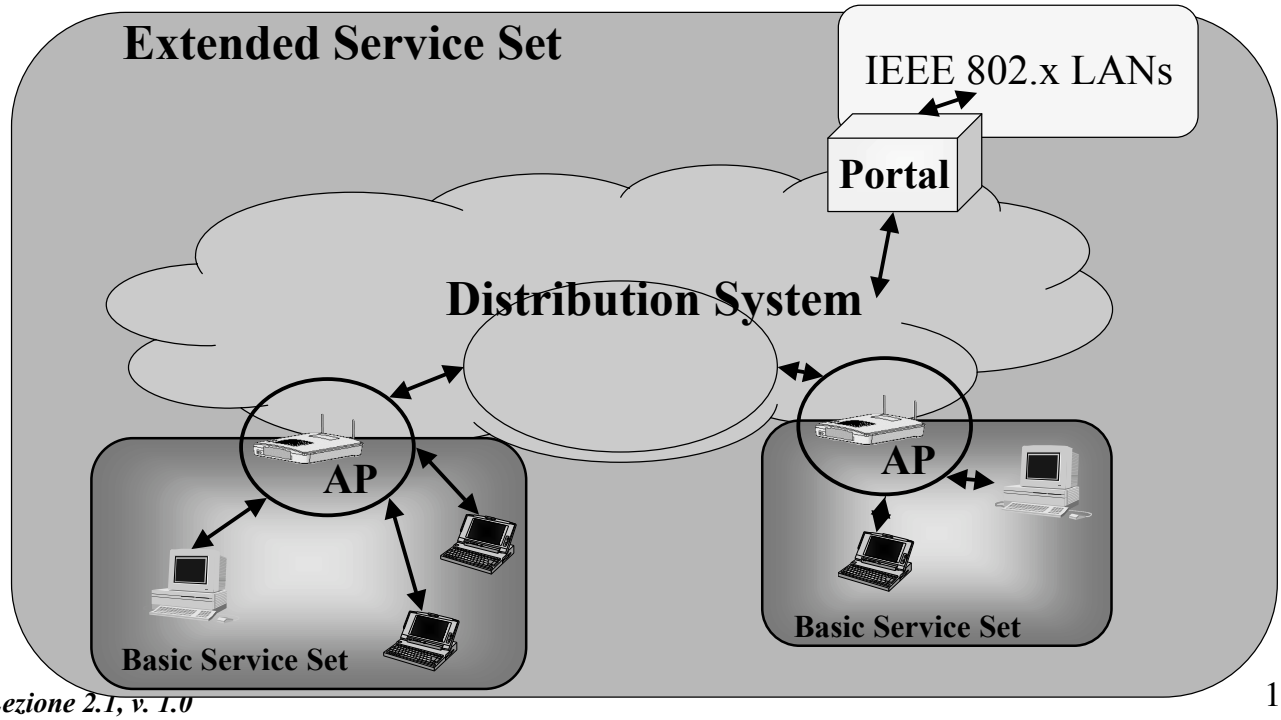
Independent Basic Service Set

- Un IBSS consiste in un BSS autonomo
  - non è presenta nessuna infrastruttura di backbone;
  - almeno due stazioni devono essere presenti.
- Una architettura di questo tipo è definita *ad hoc network*
  - può essere dispiegata molto rapidamente.
- L'archiettura ad hoc soddisfa le esigenze di comunicazioni tra utenti situati in piccole aree
  - l'area di copertura è in genere molto limitata.

IBSS



Extended Service Set



Extended Service Set

- Il ***Basic Service Set*** (**BSS**) è costituito da un insieme di stazioni che competono per l'accesso al mezzo trasmissivo condiviso.
- L'***Access Point*** (**AP**) opera come un *bridge* e permette di collegare un BSS ad un DS.
- Il ***Distribution System*** (**DS**) rappresenta un backbone per collegare diversi BSS e può consistere in una LAN cablata (e.g., *switch)* o wireless.
- L'***Extended Service Set*** (**ESS**) consiste in più BSS collegati tra di loro attraverso un DS; l'ESS appare come una unica LAN al livello LLC.
- Il ***Portal*** interconnette la WLAN con altre LAN cablate.

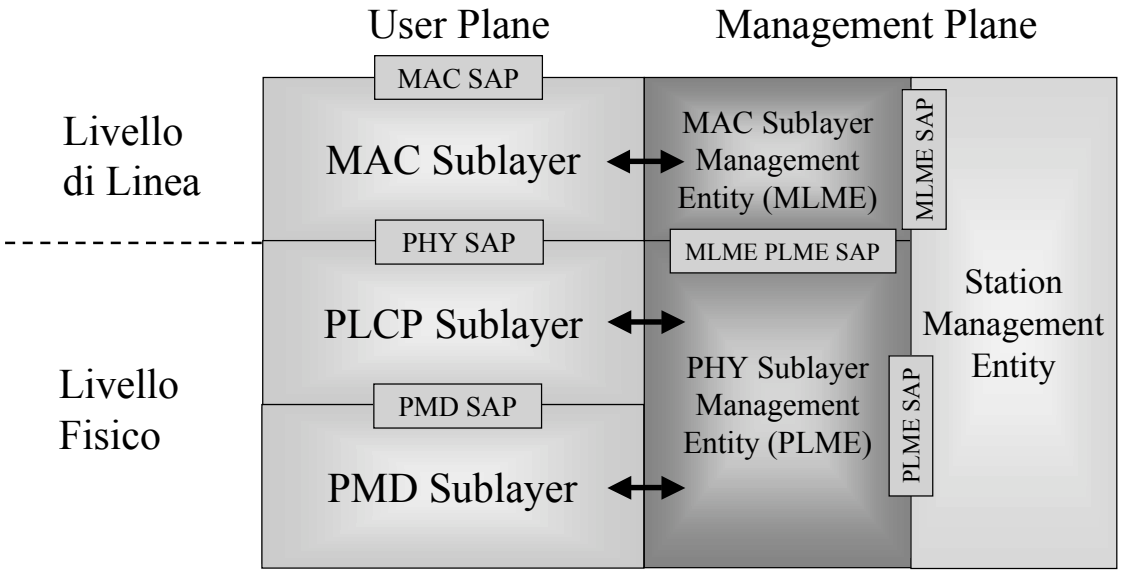
Extended Service Set

- All'interno di un ESS, i diversi BSS fisicamente possono essere locati secondo diversi criteri:
  - BSS parzialmente sovrapposti
    - » permettono di fornire una copertura continua;
  - BSS fisicamente disgiunti
  - BSS co-locati (diversi BSS nella stessa area)
    - » possono fornire una ridondanza alla rete o permettere prestazioni superiori.

Mobilità

- L'802.11 gestisce la mobilità delle stazioni distinguendo tre tipi di transizioni:
  - **Statica**: la stazione è immobile o si sposta solo entro l'area di un singolo BSS;
  - **Transizione tra BSS**: in questo caso la stazione si sposta tra due diversi BSS parzialmente sovrapposti appartenenti allo stesso ESS
    - » il MAC è in grado di gestire questa situazione in maniera trasparente per i livelli superiori;
  - **Transizione tra ESS**: la stazione si sposta tra BSS appartenenti a due ESS diversi
    - » la stazione può muoversi, ma il MAC non è in grado di mantenere la connettività.

Architettura Protocollare



Livello Fisico

- Sottolivello PMD (**Physical Medium Dependent**)
  - definisce i diversi mezzi trasmissivi;
  - si occupa della trasmissione/ricezione dei pacchetti;
  - effettua il *Medium sense* sulla base del mezzo tx.
- Sottolivello PLCP (**Physical Medium Convergence Protocol**)
  - offre un'interfaccia comune verso i diversi mezzi trasmissivi;
  - definisce una metodologia con cui trasformare le MPDU in un *frame* adatto per la tx/rx di informazioni utente e di controllo attraverso il PMD.

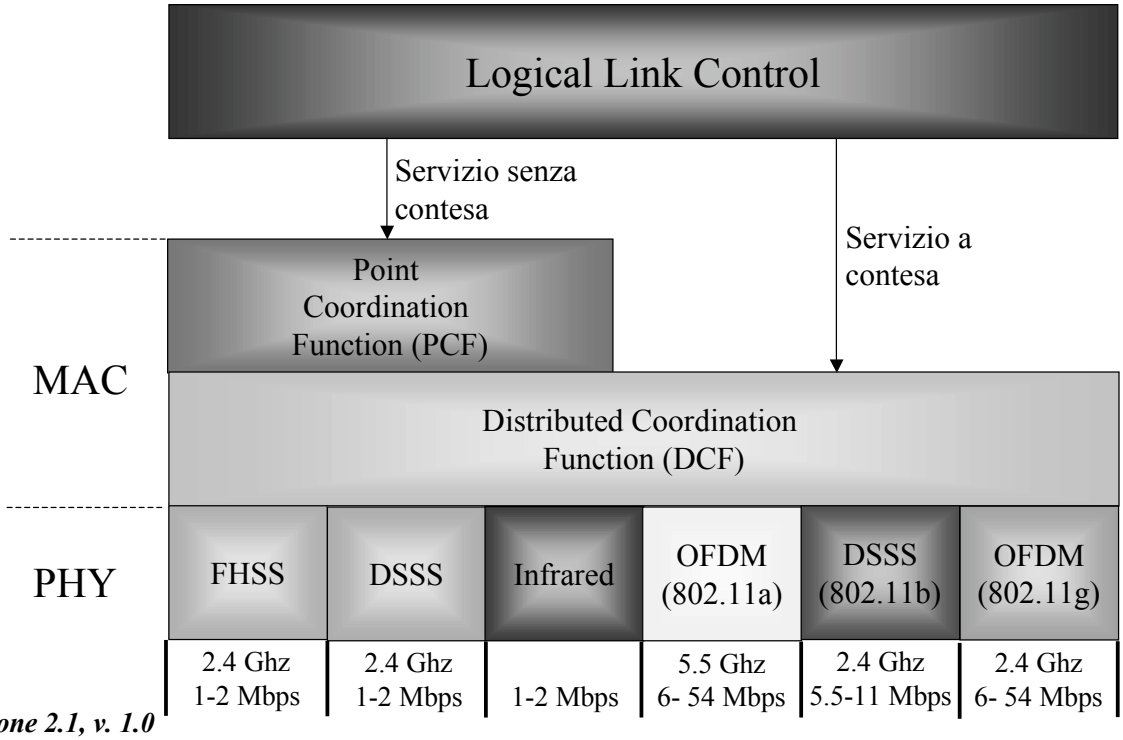
Livello di Linea

- **MAC Sublayer** ha le seguenti funzioni
  - Realizzare un meccanismo di accesso multiplo e contesa del mezzo trasmissivo (CSMA/CA)
    - » unico per diversi mezzi trasmissivi;
  - Fornire servizi con e senza vincoli sul ritardo
    - » DCF e PCF;
  - Realizzare la frammentazione;
  - Realizzare la cifratura.

Piano di gestione

- **Station Management Entity** (SME)
  - è una entità inter-livello
    - » risiede in un piano separato;
  - le sue funzioni non sono specificate nello standard;
  - in genere deve occuparsi di
    - » raccogliere informazioni dai diversi livelli;
    - » impostare i valori dei parametri specifici per ogni livello.
- Entità di gestione dei singoli livelli
  - rappresentano le interfacce attraverso le quali richiamare le funzioni di gestione:
    - » MAC sublayer management;
    - » PHY layer management.

Struttura dello standard



Servizi del MAC

- Lo standard 802.11 prevede una serie di servizi che il livello LLC richiede per poter trasferire *MAC Service Data Units* (MSDU) tra due entità LLC in rete.
- Il MAC 802.11 fornire tali servizi.
- Essi rientrano in due categorie principali:
  - ***Station Services***
    - » **Authentication**, **Deauthentication**, **MSDU Delivery** e **Privacy**;
    - » sono i soli servizi disponibili per le reti IBSS;
  - ***Distribution System Services***
    - » **Association**, **Disassociation**, **Distribution**, **Integration** e **Reassociation**;
    - » disponibili solo per gli ESS.

Servizi
Authentication

- È il meccanismo utilizzato per stabilire l'identità delle stazione che devono comunicare.
- Deve fornire un livello di sicurezza pari a quello della LAN cablate.
- Ogni stazione 802.11 deve effettuare l'autenticazione prima di stabilire essere abiltato a scambiare dati ("associazione") con un'altra stazione.
- 802.11 prevede due meccanismi di autenticazione: ***Open system authentication*** (non sicuro) e ***Shared key***.

Servizi
Deauthentication

- Servizio per terminare una autenticazione esistente verso un'altra stazione.
- La stazione che intende deautenticarsi manda un *frame* di notifica.
- Il servizio non può essere rifiutato dalla stazione ricevente la notifica.

Servizi
Privacy

- Nelle reti wireless il traffico può essere osservato da chiunque si trovi nelle vicinanze.
- Lo standard prevede l'uso opzionale della cifratura per garantire la segretezza delle comunicazioni.
- L'algoritmo utilizzato è denominato WEP (*Wired Equivalent Privacy*) ed ha lo scopo di fornire un livello di sicurezza paragonabile a quello delle LAN cablate
  - ogni utente autorizzato è quindi in grado di osservare il traffico di tutti gli altri.
- La configurazione standard delle interfacce è "invio in chiara". Se si richiama il servizio Privacy la stazione si configura per la cifratura e non accetta più trame in chiaro.

Servizi
Association

- Per poter consegnare un pacchetto all'interno dell'ESS, il *Distribution Service* necessita di conoscere la posizione della stazione di destinazione.
- In particolare, è necessario conoscere l'identità dell'AP a cui consegnare il messaggio.
- Per questa ragione è necessario che ogni stazione effettui una procedura di associazione con l'AP del BSS nel quale si trova.

Servizi
Reassociation

- Il servizio di *Reassociation* consente ad una stazione di cambiare la sua associazione da un AP ad un altro, permettendo la transizione tra diversi BSS all'interno dello stesso ESS.
- È analogo all'*handoff* nelle reti cellulari.
- Le stazioni misurano la potenza con cui ricevono i messaggi di controllo degli AP (*beacom*) per decidere a quale BSS associarsi.

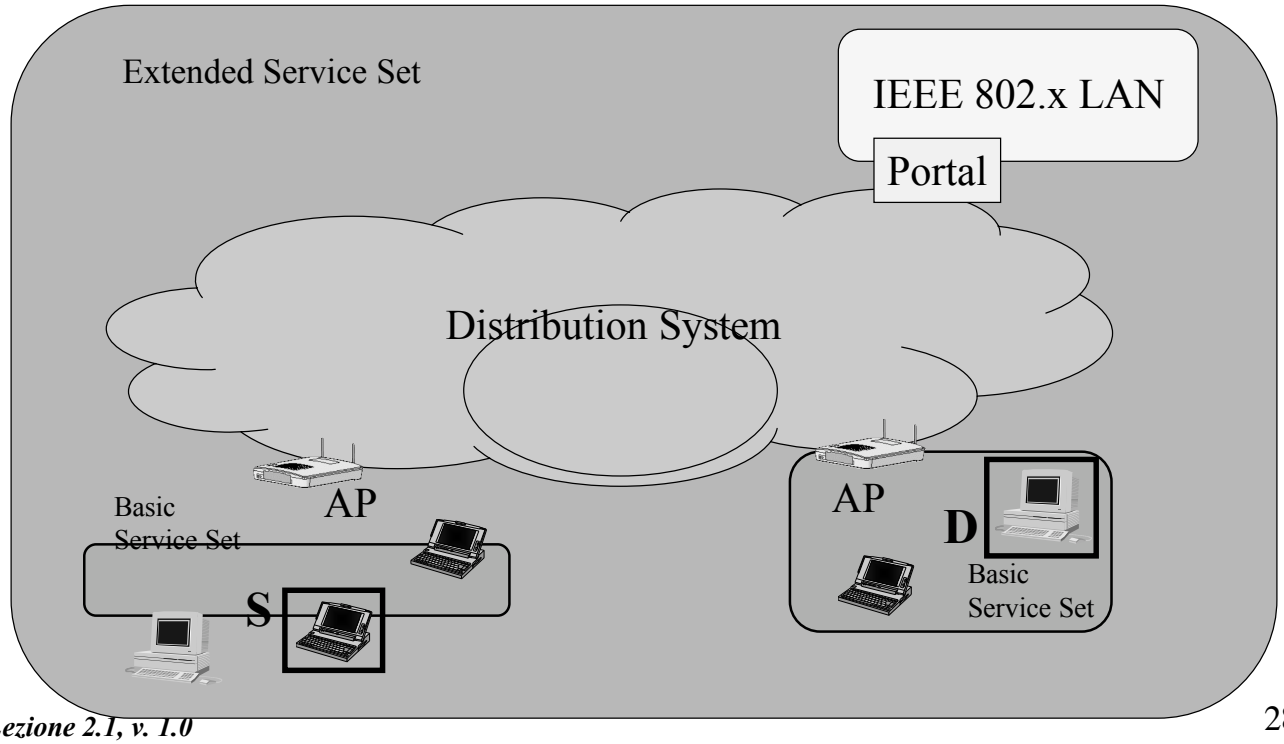
Servizi
Disassociation

- Consiste nella notifica di termine dell'associazione.
- Una stazione effettua la *Disassociation* prima di spegnersi o di uscire dall'ESS.
- Un AP può disassociare tutte le stazione prima di essere spento per operazioni di manutenzione.
- Le stazioni dovrebbero sempre disassociarsi prima di spegnersi
  - la disassociazione protegge il MAC dalla "sparizione" improvvisa delle stazioni precedentemente registrate.

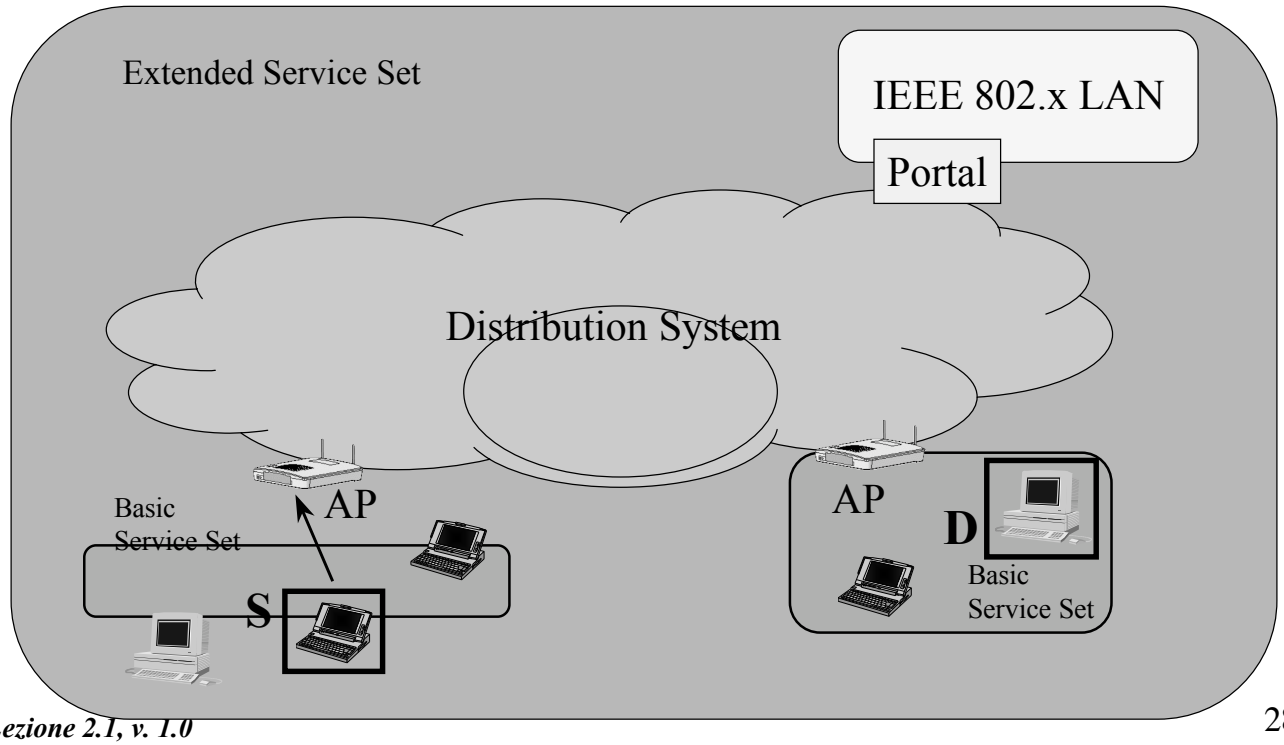
Servizi
Distribution

- Il servizio *Distribution* viene utilizzato dalle stazioni per scambiarsi pacchetti che devono attraversare il DS.
- Gli AP conoscono la posizione delle diverse stazioni grazie al servizio di *Association* e sono in grado di scambiarsi i pacchetti attraverso il DS.
- Il meccanismo di funzionamento del DS non è comunque oggetto dello standard.
- Se le stazioni appartengono allo stesso BSS, il servizio di *Distribution* logicamente coinvolge il solo AP di quel BSS.

Servizi
Distribution

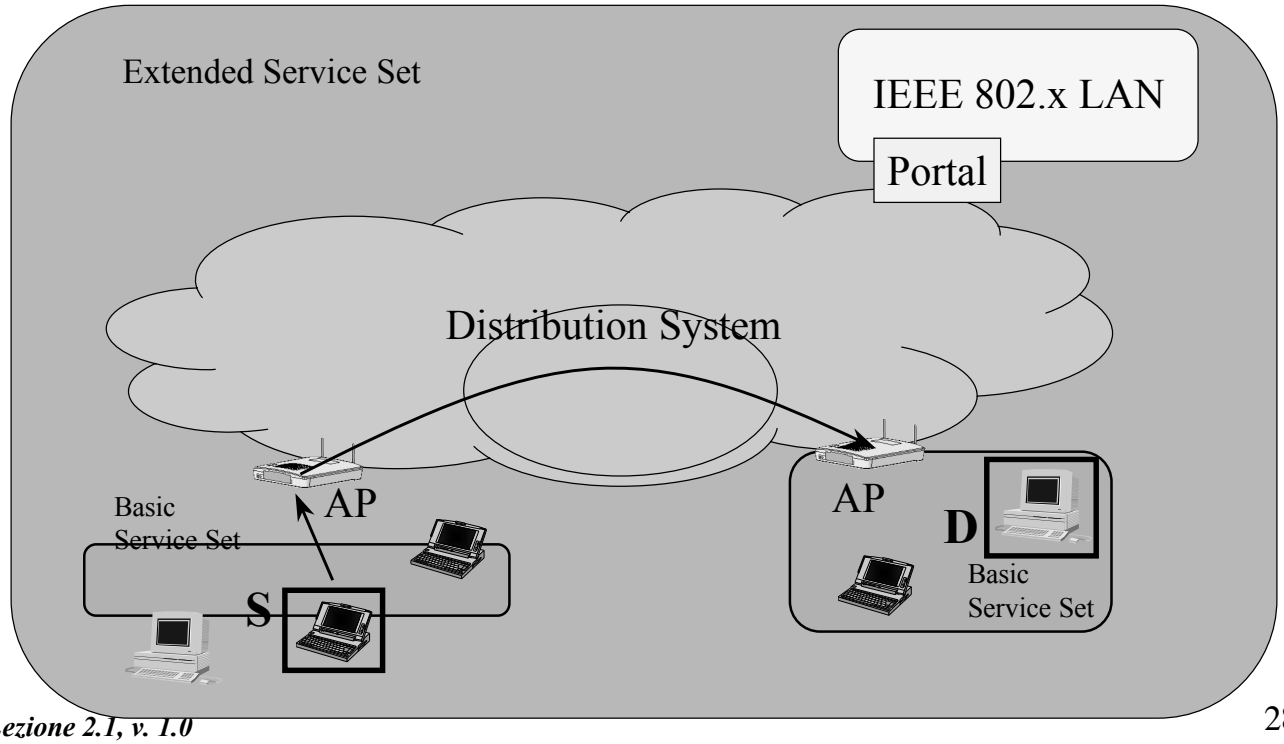


Servizi
Distribution

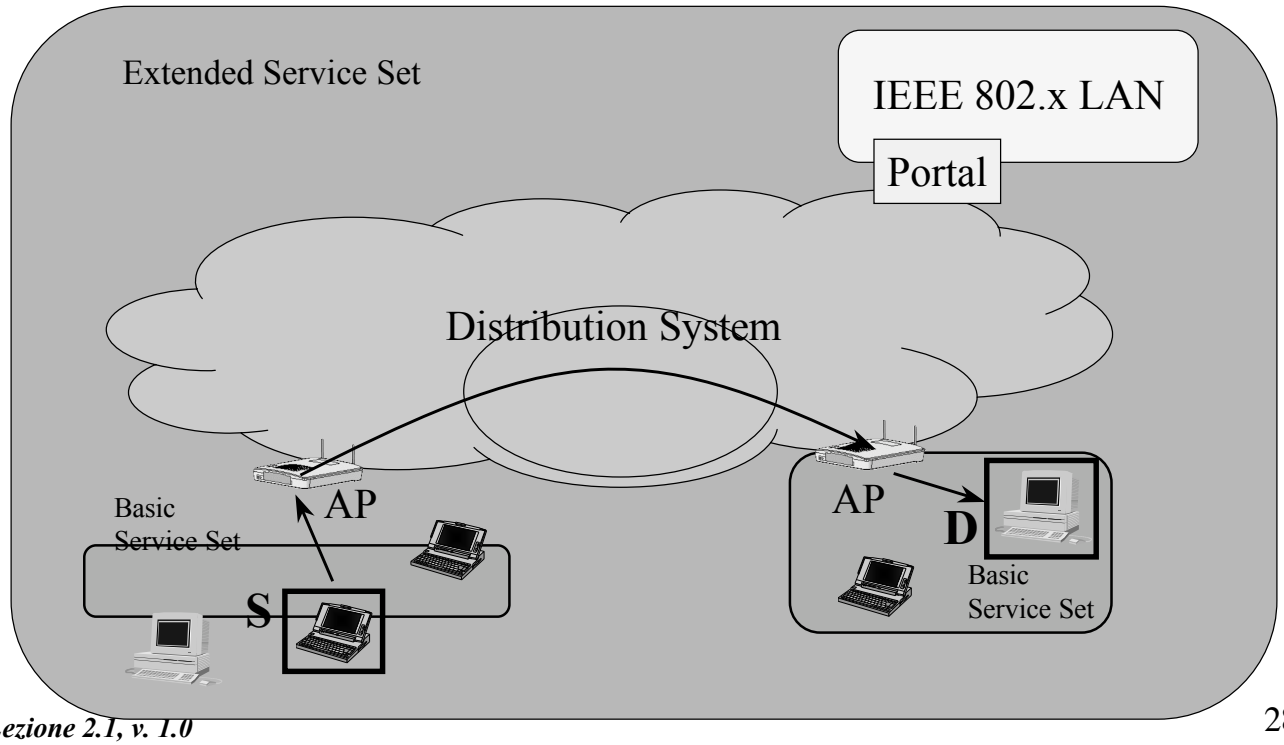


Architetture e Protocolli Wireless -N. O.

Servizi
Distribution



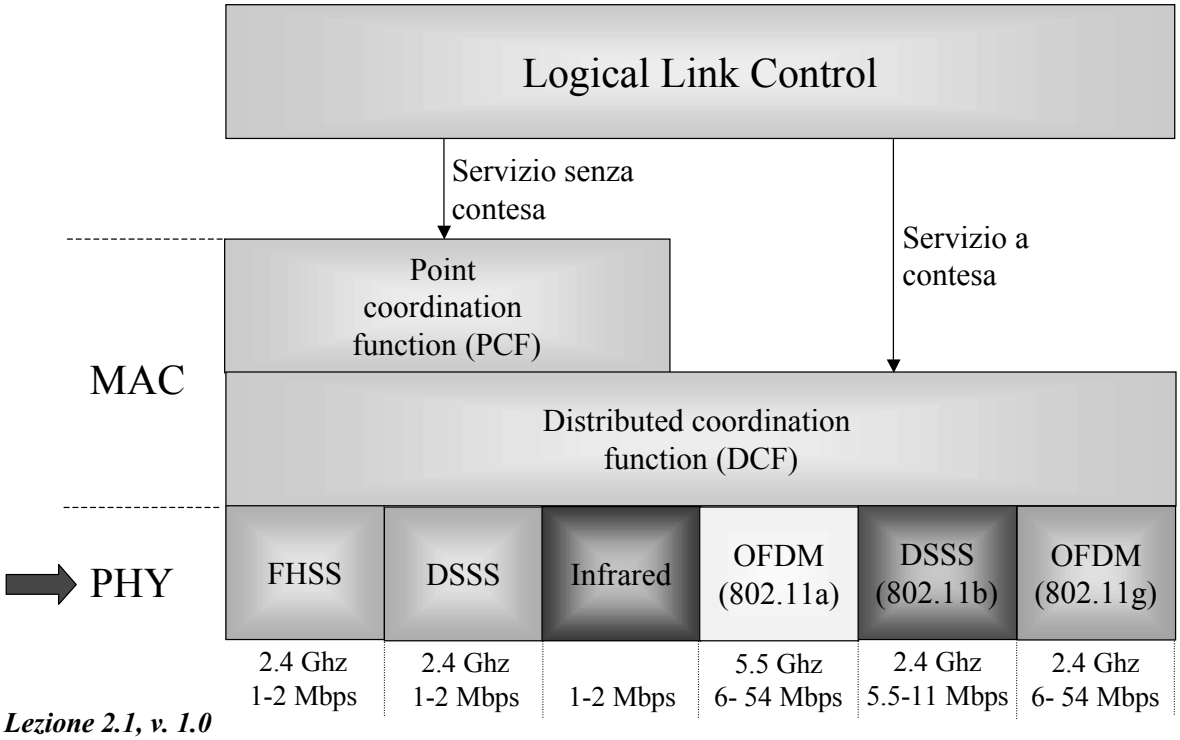
Servizi
Distribution



Servizi
Integration

- Il servizio di *Integration* permette il trasferimento dei dati tra le stazioni della LAN 802.11 e quelle su altre LAN IEEE 802.x.
- La LAN cablata è fisicamente connessa al DS e le sue stazioni possono venire connesse logicamente sfruttando il servizio di *Integration*.
- Il servizio di *Integration* provvede all'eventuale traduzione degli indirizzi e all'adattamento ai diversi media.

Livello Fisico



Mezzi trasmissivi e terminali

- Lo standard prevede la trasmissione mediante l'utilizzo di onde elettromagnetiche nell'etere:
  - radio;
  - infrarossi.
- Terminali supportati:
  - Fissi, spostabili, mobili a velocità pedestre ed eventualmente veicolare.

Livello Fisico

- Velocità di trasmissione
  - le specifiche 802.11 originali prevedevano la trasmissione a **1 e 2 Mb/s**
    - » nella banda ISM 2.4 GHz per i sistemi radio;
    - » ad una lunghezza d'onda tra 850 e 950 nm per i sistemi ad infrarossi;
  - lo standard 802.11b porta la velocità a **5.5 e 11 Mb/s** per i sistemi radio
    - » utilizza ancora la banda ISM 2.4 GHz;
  - con l'introduzione dell'802.11a le velocità ammesse sono **6, 9, 12, 18, 24, 36, 48 e 54 Mb/s**
    - » 6, 12 e 24 sono obbligatorie;
    - » la banda utilizzata è intorno ai 5 GHz.
  - 802.11g permette le stesse velocità dell'11a ma nella banda del 11b (2.4 GHz)

Livello Fisico

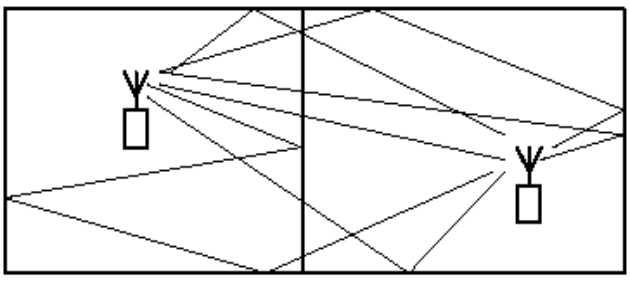
- **Aree di copertura**
  - con antenne omnidirezionali:
    - » **50-100 mt per 802.11b;**
    - » **15-30 mt per 802.11a/g;**
  - con antenne direzionali (collegamenti punto-punto) ad alto guadagno é possibile arrivare fino a **40 Km**.
- **Bande di trasmissione utilizzate:**
  - ISM 2.4 GHz, 2.4 - 2.4835 GHz;
  - 5 GHz, 5.15 - 5.825 GHz.
- Tecniche di trasmissione:
  - *Spread Spectrum*: FHSS, DSSS;
  - OFDM.

Livello Fisico
Frequency Hop Spread Spectrum

- La tecnica consiste nel modificare la frequenza di trasmissione utilizzando sequenze pseudocasuali comuni a tutte le stazioni.
- Lo spettro complessivo è diviso in 79 canali da 1 MHz ciascuno
  - in Giappone sono disponibili solo 23 canali.
- Un elaboratore predesignato genera una lista con le 79 frequenze in un ordine specifico
  - l'hop rate minimo deve essere di 2.5 salti/secondo (USA);
  - ogni "salto" (*hop*) deve distare almeno 6 canali
    - » 5 in Giappone;
  - le diverse possibile sequenze (78) sono ottenute spostando l'inizio della sequenza di un *offset* e ricalcolandola con modulo 79.
- Le 78 sequenze sono organizzate in 3 insiemi di 26 elementi
  - possono essere presenti un massimo di 26 reti co-locate.
- Il *throughput* continua a salire fino a 15 reti colocate, in condizioni di traffico elevato.

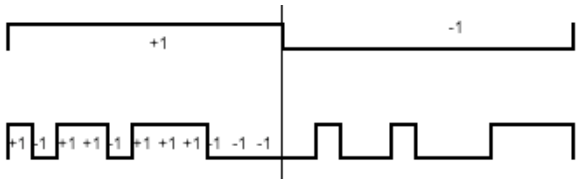
Livello Fisico
Frequency Hop Spread Spectrum

- Permette un buona robustezza al fading dovuto ai cammini multipli (comuni nell'ambienti "indoor").
- Percorsi di propagazione multipli, interferendo l'uno con l'altro, creano del *fading* selettivo in frequenza.
- Le fluttuazioni sono correlate a frequenze adiacenti ma si scorrelano, in ambiente indoor, dopo pochi MHz.

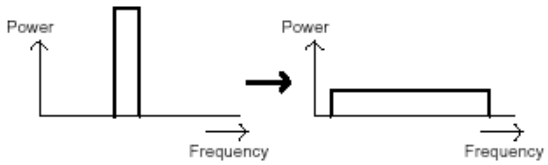


Livello Fisico
Direct Sequence Spread Spectrum

- Il segnale relativo ad un simbolo viene "sparso" su una sequenza:



- Banda più larga
- Potenza meno "densa"



Livello Fisico
Direct Sequence Spread Spectrum

- Tasso di simbolo 1 MHz.
- *Chipping* rate 11 MHz
  - l'802.11 utilizza una sequenza di Baker a 11 bit;
  - l'802.11b utilizza una codifica CCK (*Complementary Code Keying).*
- 14 canali complessivi, radunati in coppie
  - in Europa uno dei canali della prima coppia non può essere usato
    - » solo 13 canali sono utilizzabili;
  - in Giappone è utilizzabile un solo canale;
  - i canali di ogni coppia possono operare simultaneamente senza interferenza.

Livello Fisico

Ortogonal Frequency Division Multiplexing

- Il segnale viene distribuito su 48 sottoportanti.
- Ogni sottoportante è ortogonale rispetto alle altre
  - i diversi segnali non si sovrappongono.
- La modulazione utilizzata in ciascuna sottoportante determina il tasso trasmissivo.
- Vantaggi:
  - alta efficienza spettrale;
  - resistenza alle interferenze radio e alle distorsioni multi-percorso.

Livello Fisico

Le modulazioni (802.11/802.11b)

Direct Sequence Spread Spectrum

Data rate (Mbps)	Chipping Code lengh	Modulation	Symbol rate	Bits/symbol
1	11 (Barker Sequence)	DBPSK	1 Msps	1
2	11 (Barker Sequence)	DQPSK	1 Msps	2
5.5	8 (CCK)	DBPSK	1.375 Msps	4
11	8 (CCK)	DQPSK	1.375 Msps	8

Frequency Hopping Spread Spectrum

Data rate (Mbps)	Modulation	Symbol rate	Bits/symbol
1	Two-level GFSK	1 Msps	1
2	Four-level GFSK	1 Msps	2

Infrarossi

Data rate (Mbps)	Modulation	Symbol rate	Bits/symbol
1	16 PPM	4 Msps	0.25
2	4 PPM	4 Msps	0.5

Livello Fisico
Le modulazioni

Data rate (Mbps)	Modulation	Coding rate	Coded bits per subcarrier	Code bits per OFDM symbol	Data bits for OFDM symbol
6	BPSK	_	1	48	24
9	BPSK	_	1	48	36
12	QPSK	_	2	6	48
18	QPSK	_	2	96	72
24	16-QAM	_	4	192	96
36	16-QAM	_	4	192	144
49	64-QAM	2/3	6	288	192
54	16-QAM	_	6	288	216

Ortogonal Frequency Division Multiplexing

Livello Fisico
Sottolivello PLCP

- Il sottolivello PLCP riceve i pacchetti 802.11 e crea un *frame* per la trasmissione (*PPDU, PLCP Protocol Data Unit*)
- Lo standard 802.11b prevede la possibilità di utilizzare due diverse intestazioni:
  - *Long,* obbligatorio
  - *Short*, opzionale.
- *Long Preamble and Header*:
  - *sync* (128 bit), una sequenza alternata di 0 e 1
    - » il ricevitore si "aggancia" a questo clock;
  - *start frame delimiter* (16 bit), 1111001110100000 delimita l'inizio vero e proprio del *frame*;

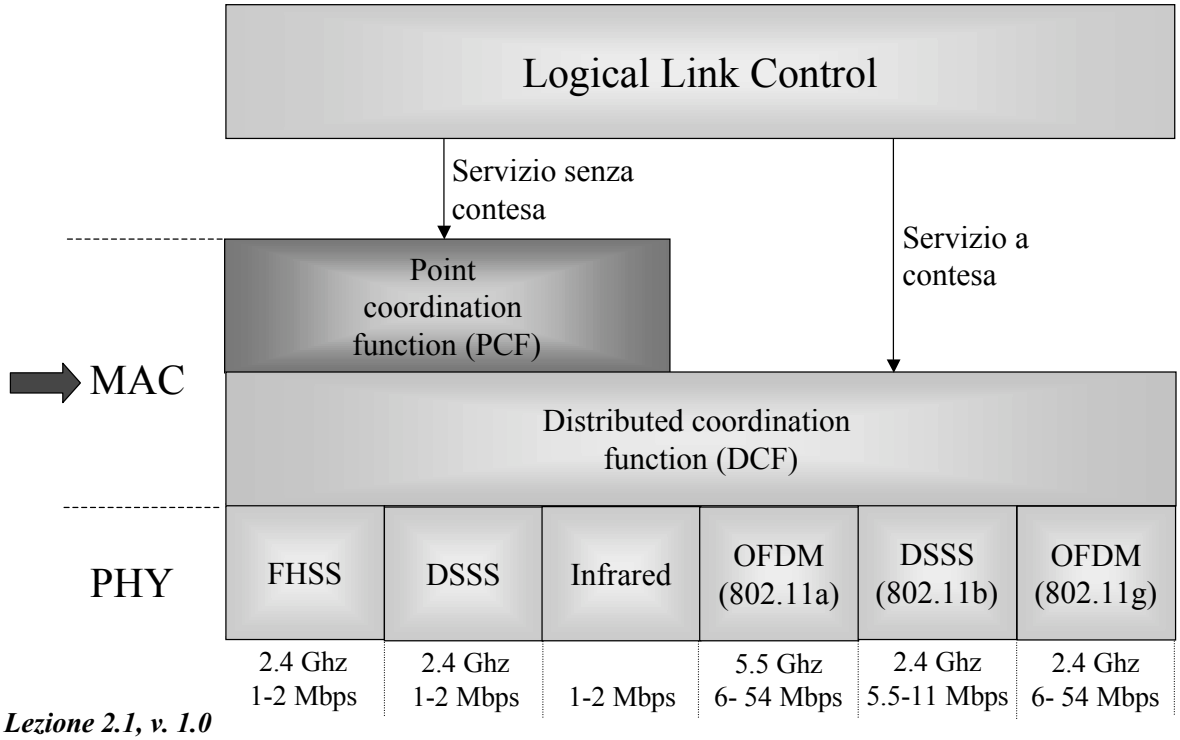
Livello Fisico
Sottolivello PLCP

- *signal* (8 bit), indica la velocità di trasmissione del frame
  - » il valore binario è pari a *rate/100Kbps;*
  - » 0x0A 1 Mbps, 0x14 2 Mbps, 0x6E 11 Mbit, ecc.;
  - » per compatibilità, i campi introdotti dal PLCP sono sempre trasmessi a 1 Mbps;
- *service* (8 bit)
  - » bit 7 per supportare la velocità di 11 Mbps;
  - » bit 3 indica la modulazione (CCK o PBCC);
- *length* (16 bit), indica il numero di μs necessari a tx il contenuto della PPDU
  - » il ricevitore utilizza questo valore per determinare la fine del frame;
  - » i campo *service* indica come questo valore è stato calcolato;
- *frame check sequence* (16 bit), CRC per proteggere l'intestazione della PPDU
- PSDU, che coincide con il pacchetto MAC.

Livello Fisico
Sottolivello PLCP

- *Short Preamble and Header*
  - presenta gli stessi campi del *Long*
    - » il campo *sync* è limitato a 56 bit
  - *signal, service, length* e *CRC* possono essere trasmessi a 2 Mbps;
  - una stazione che trasmette questo preambolo è in grado di comunicare solo con altre stazioni che supportano lo stesso tipo di preambolo;
  - rende più efficiente la trasmissione.
- La versione originale prevede gli stessi campi, ma con un numero di bit diverso.
- L'802.11a introduce alcune modifiche.
- L'802.11g utilizza gli stessi formati 802.11b
  - richiede il supporto anche per lo *short preamble;*
  - utilizza ulteriori bit di *signal* per specificare i maggiori tassi trasmissivi.

Livello di Linea



Livello di Linea
MAC

- La trasmissione *wireless* è decisamente inaffidabile
  - il controllo di errore dei livelli superiori (TCP) richiede timer dell'ordine dei secondi;
  - risulta più efficiente incorporare un controllo di errore anche nel MAC.
- 802.11 specifica quindi un protocollo per la trasmissione dei frame:
  - trasmissione del frame da parte della sorgente;
  - invio di un ACK da parte del ricevitore;
  - questo scambio è considerato come una operazione unica, che non deve essere interrotta dalle altre stazioni
    - » l'ACK deve essere inviato entro un tempo detto SIFS;
    - » le stazioni non possono iniziare una nuova trasmissione in tale intervallo temporale.

Livello di Linea
MAC

- Il meccanismo di trasferimento richiede quindi lo scambio di due frame.
- È possibile aumentare l'affidabilità del meccanismo attraverso uno scambio a 4 vie:
  - la sorgente invia una richiesta di trasmissione (RTS) alla destinazione;
  - la destinazione conferma (CTS);
  - la sorgente invia il frame contenente l'informazione;
  - la destinazione conferma la ricezione del frame (ACK).
- Questo meccanismo può essere escluso.
- Il meccanismo RTS/CTS viene utilizzato anche per risolvere il problema delle stazioni nascoste.

Livello di Linea
MAC

- La tecnica di contesa scelta è denominata Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA).
- Due funzionalità presenti
  - *Distribution Coordiantion Function*
    - » realizza il meccanismo di MAC in forma completamente distribuita;
  - *Point Coordination Function*
    - » versione centralizzata per permettere le realizzazione di servizi "*delay bounded*".

Livello di Linea

MAC

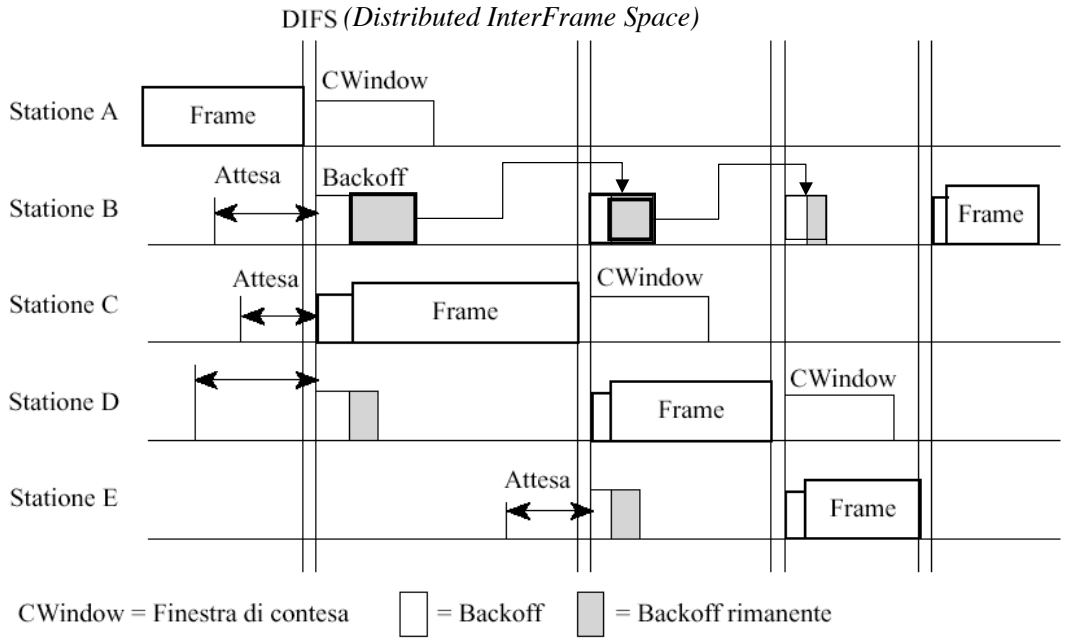
- Ogni stazione che deve trasmettere un pacchetto verifica che il canale sia libero (CSMA)
  - in caso negativo rimanda la trasmissione;
  - in caso positivo attende per un tempo pari a un DIFS (ricezione corretta del pacchetto) o a un EIFS (ricezione non corretta) (CA);
    - » se nessun'altra trasmissione inizia in questo intervallo la trasmissione ha luogo;
    - » in caso contrario la trasmissione viene rimandata.
- Nel caso in cui la trasmissione venga rimandata, la stazione estrae un tempo casuale di attesa (*tempo di backoff*):
  - tale tempo viene decrementato mentre il canale è libero;
  - al termine del conteggio, il canale deve rimanere libero per un ulteriore tempo DIFS prima di iniziare la trasmissione.

Livello di Linea

MAC

- Nel caso in cui la trasmissione venga rimandata, la stazione estrae un tempo casuale di attesa (*tempo di backoff*):
  - tale tempo viene decrementato mentre il canale è libero;
  - al termine del conteggio, il canale deve rimanere libero per un ulteriore tempo DIFS prima di iniziare la trasmissione.
- La mancata ricezione di un ACK
  - può essere dovuta ad errori o collisioni
    - » tempi di propagazione non trascurabili;
  - richiede la ritrasmissione del pacchetto relativo
    - » riattivazione del meccanismo di contesa;
    - » fino ad un numero massimo di tentativi.

Livello di Linea
MAC - DCF



Livello di Linea
MAC - DCF

- La procedura di backoff estrae un tempo casuale B∈[0,CW]
  - B indica il numero di slot di attesa
    - » la durata di una slot è il tempo necessario affinché una stazione possa stabilire se un'altra stazione è accessa al mezzo trasmissivo all'inzio della slot precedente;
    - » varia a seconda del mezzo fisico utilizzato;
  - $CW_{min} \leq CW \leq CW_{max}$:
    - » CW_{min}, CW_{max} sono parametri scelti dalla stazione;
    - » CW viene raddoppiato ad ogni collisione;
    - » CW viene riportato al valore di CW dopo ogni trasmissione con successo.
- Questa procedura, denominata *binary exponential backoff* serve a rendere stabile il meccanismo di accesso.

Livello di Linea

MAC – Algoritmo di Backoff Esponenziale

- L'algoritmo di **Backoff Esponenziale** deve essere utilizzato
  - quando una stazione tenta la trasmissione di un pacchetto e trova il canale occupato;
  - dopo ciascuna ritrasmissione;
  - dopo il termine di una trasmissione con successo.
- L'unico caso in cui non viene utilizzato è nel caso in cui la stazioni trovi il canale libero al primo tentativo di trasmissione.

Livello di Linea

MAC - Inter Frame Spaces

- **SIFS** (*Short Inter Frame Space*) - separa la trasmissione di pacchetti appartenenti allo stesso dialogo (es. Pacchetto + ACK). Viene calcolato in base ai tempi necessari agli apparati hw per commutare tra tx/rx.
- **PIFS** (*Point Coordination Inter Frame Space*) – è utilizzato dal Point Coordinator per gestire il polling. È pari allo SIFS + il tempo di una slot.
- **DIFS** (*Distributed Inter Frame Space*) - il tempo che una stazione deve attendere prima di accedere al canale. Corrisponde al PIFS + il tempo di una slot.
- **EIFS** (*Extended Inter Frame Space*) - utilizzato da una stazione che non riceve correttamente il pacchetto per non collidere con un pacchetto successivo appartenente allo stesso dialogo
  - la stazione potrebbe non aver ricevuto correttamente l'informazione relativa al *Virtual Carrier Sense*.

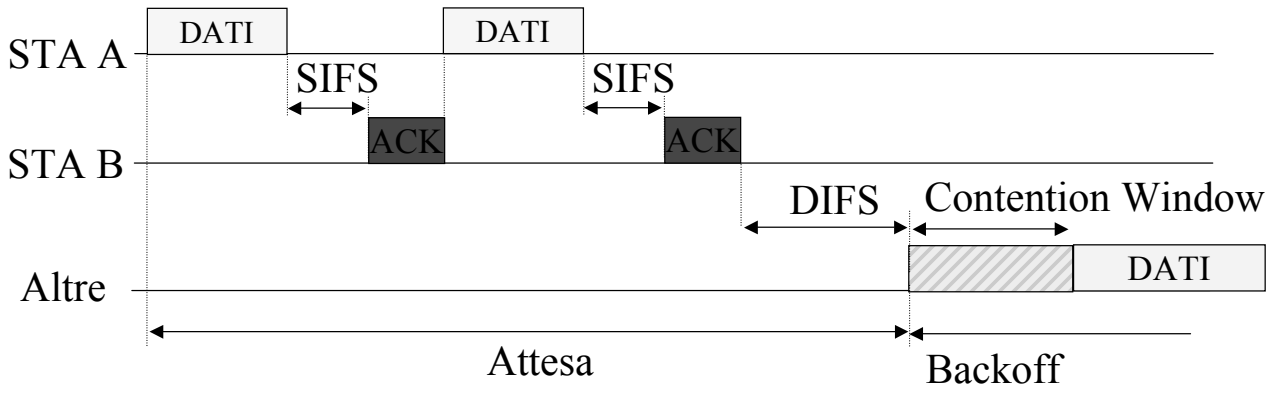
Livello di Linea

MAC - DCF

- L'utilizzo di tempi inter-frame diversi permette ad una stazione di inviare più pacchetti in sequenza
  - esistono dei limiti entro cui il canale deve essere rilasciato
    - » temporali;
    - » logici (esaurimento dei segmenti dello stesso pacchetto);
    - » di altra natura (***dwell time***);
  - alla scadenza di questi la stazione deve rilasciare il canale;
    - » la stazione torna a competere con le altre;
  - viene utilizzata questa possibilità nella trasmissione in sequenza dei segmenti in caso di frammentazione.

Livello di Linea

MAC - DCF



Livello di Linea

Meccanismo di *Carrier Sense*

- L'indicazione di mezzo occupato avviene attraverso due meccanismi:
  - *physical carrier-sense*
    - » fornito dal livello fisico;
    - » indica la presenza di una trasmissione sul canale;
  - *virtual carrier-sense*
    - » realizzato all'interno del MAC;
    - » le intestazioni MAC contengono l'indicazione sulla durata delle transazioni;
    - » questo meccanismo viene indicato come NAV (*Network Allocation Vector*);
    - » il NAV contiene un valore che viene decrementato dalla stazione, fino a raggiungere il valore 0 (canale libero).

Livello di Linea

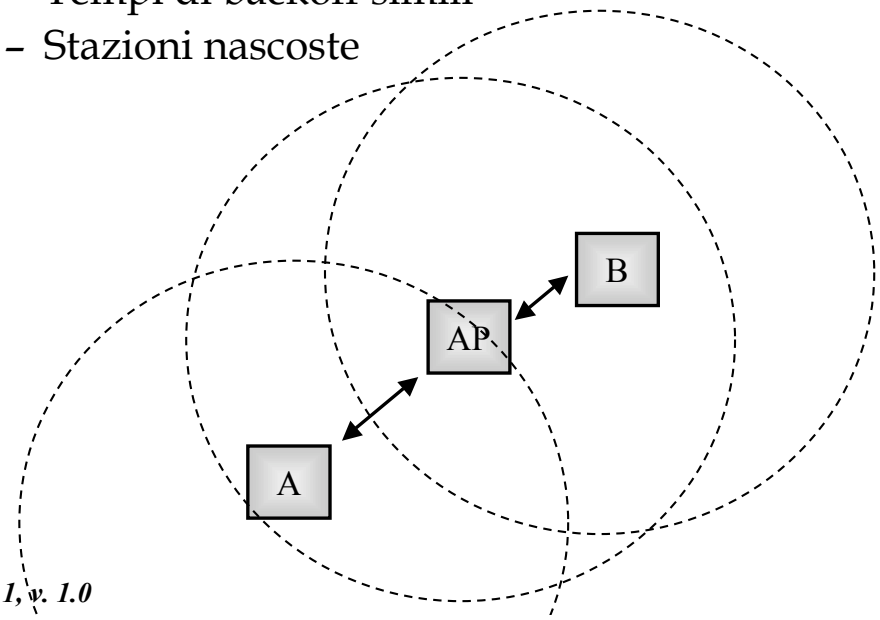
NAV

- Le stazioni che ricevono un frame aggiornano il NAV
  - solo se maggiore di quello attuale;
  - tranne la stazione a cui è indirizzato il pacchetto.
- L'utilizzo del NAV permette di risolvere il problema delle stazioni nascoste
  - nelle WLAN non è possibile assumere la connettività completa delle stazioni.

Livello di Linea

Il problema delle stazioni nascoste

- Le collisioni non sono evitate completamente per due motivi:
  - Tempi di backoff simili
  - Stazioni nascoste

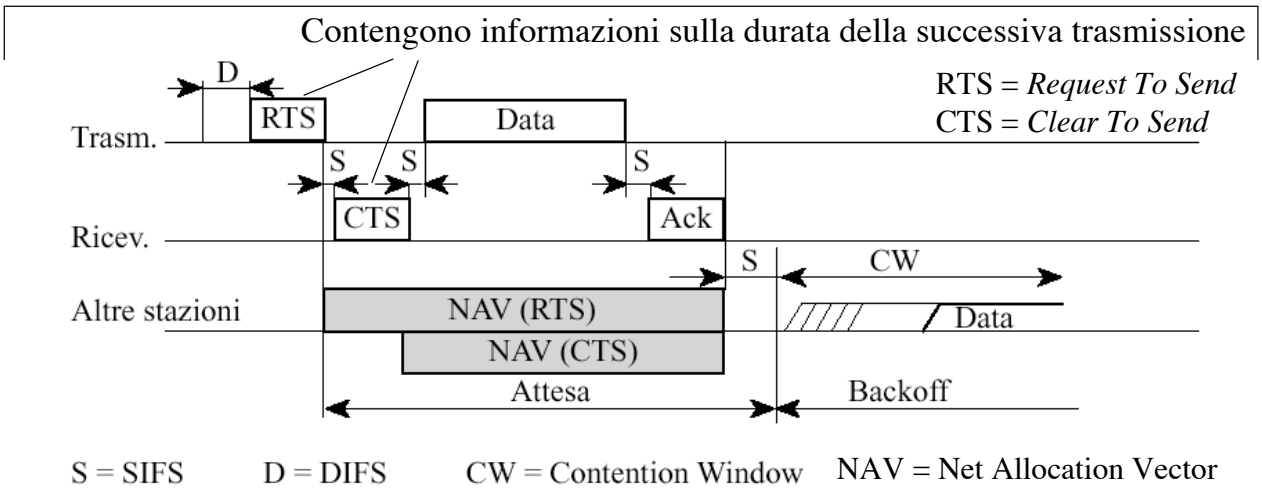


Le stazioni A e B possono comunicare con l'AP ma non direttamente tra di loro.

Livello di Linea

NAV e RTS/CTS

L'utilizzo del NAV permette di risolvere le situazioni in cui la rilevazione del mezzo occupato non è possibile a livello fisico.

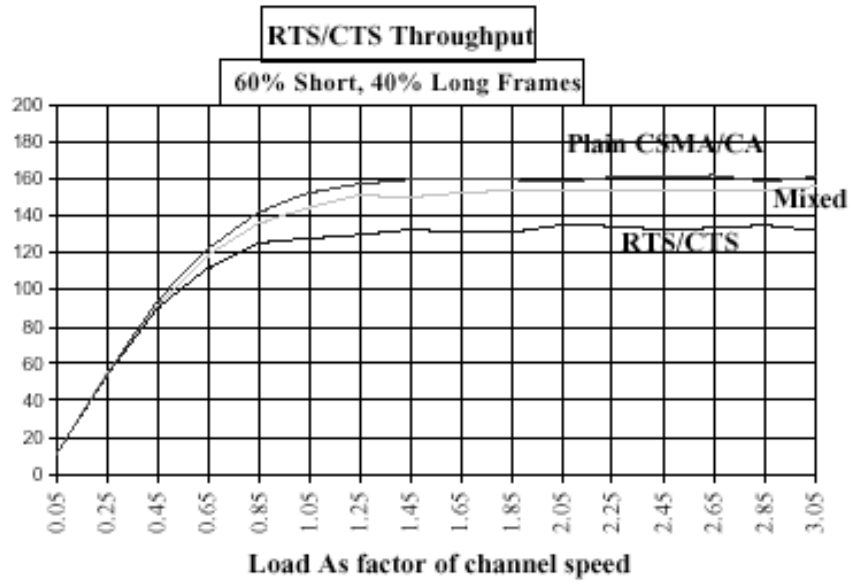


Se i pacchetti sono molto corti il sistema è inefficiente per cui per lunghezze sotto una certa soglia è prevista la tx senza RTS/CTS.

La tx diretta viene effettuata anche nel caso di broadcast.

Livello di Linea

MAC – DCF e RTS/CTS



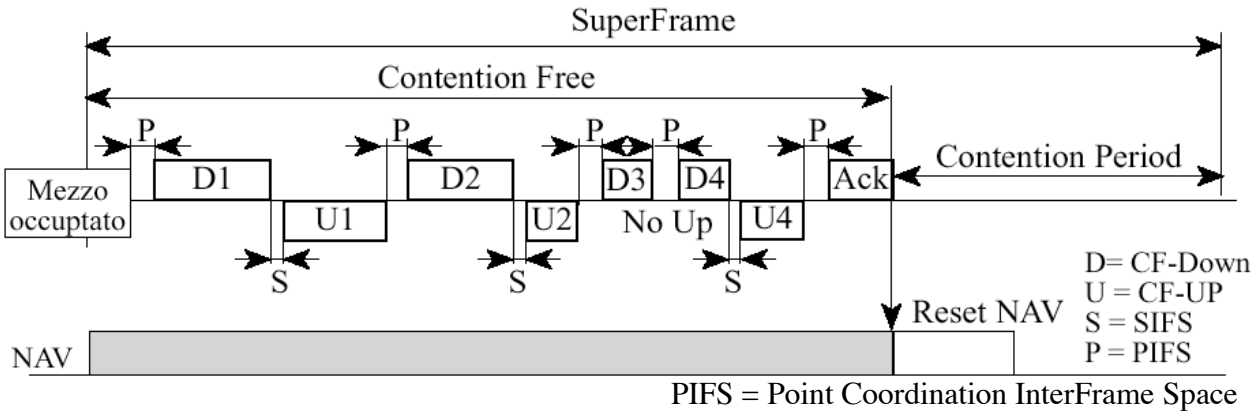
Livello di Linea

MAC – PCF

- Il PCF rappresenta un metodo di contesa alternativo costruito sopra la struttura DCF.
- Fondalmentalmente si tratta di un *polling* gestito da una stazione specializzata (per es. AP), denominata *Point Coordinator (PC)*.
- Una PCF non può sovrapporsi ad un'altra sullo stesso canale trasmissivo.
- In sostanza viene creata una struttura temporale detta Superframe divisa in due parti:
  - Contention free period (CFP): gestita da un PC con un meccanismo polling
  - Contention period (CF): gestito come nel DCF.
- Serve a fornire servizi con requisiti di ritardo.

Livello di Linea

MAC – PCF



•L'ack viene inserito nel frame successivo di una tx (trannel'ultimo)
•Le stazioni che non trasmettono per più di un certo numero di turni vengono escluse

Livello di Linea

MAC – PCF

- Il PC effettua il polling dopo un tempo pari a PIFS.
- Le stazioni interrogate rispondono dopo un tempo SIFS
  - se non si hanno risposte entro tale intervallo, il PC effettua un altro polling entro un tempo PIFS.
- Le relazioni tra i diversi IFS stabiliscono una priorità:
  - pacchetti appartenenti allo stesso dialogo (ACK, RTS/CTS);
  - interrogazioni da parte del PC;
  - acceso casuale (DCF).

Livello di Linea

Frammentazione

- Si osservi che il MAC prevede una funzione di frammentazione *point to point*.
- Questo perché
  - nei collegamenti radio la BER è alta e la probabilità di avere un pacchetto errato aumenta con la lunghezza del pacchetto stesso;
  - più i pacchetti sono corti, meno *overhead* genera una eventuale ritrasmissione;
  - nei sistemi frequency hopping la trasmissione di pacchetti corti hanno una minore probabilità di essere rimandata a causa dell'imminenza di un cambio di frequenza.

Livello di Linea

Frammentazione

- Il processo di segmentare una *MAC Service Data Unit* (MSDU) in unità più piccole viene chiamata frammentazione
  - l'operazione inversa può essere definita deframmentazione o riassemblaggio.
- La frammentazione delle MSDU
  - rende più affidabile la trasmissione sul canale
    - » la probabilità di errore cresce all'aumentare della lunghezza del frame;
    - » la ritrasmissione di frame corti introduce un minor overhead;
  - aumenta l'overhead nella gestione e nella trasmissione dei frammenti.

Livello di Linea
Frammentazione

- La frammentazione non è prevista per i datagram multicast/broadcast.
- Ogni frammento deve essere confermato separatamente.
- I segmenti appartenenti alla stessa MSDU vengono trasmessi come un unico *burst* nel caso di CP
  - la contesa DCF viene effettuata solo una volta;
- Nel caso CFP ogni segmento viene spedito separatamente
  - prevale la politica imposta dal PC.

Livello di Linea
Frammentazione

- La trasmissione dei frammenti utilizza un controllo di flusso di tipo Stop-and-Wait:
  - la stazione si blocca fino a quando
    - » si riceve l'ACK relativo al precedente trasmesso;
    - » il frammento è stato ritrasmesso troppe volte e l'intero pacchetto viene scartato;
  - è comunque permesso inframezzare trasmissioni verso altre destinazioni.

Livello di Linea
Frammentazione

- Tutti i frammenti (eccetto l'ultimo) dovrebbero
  - avere la stessa dimensione.
  - trasportare un numero pari di ottetti.
- I frammenti non devono superare una certa dimensione massima impostabile.
- Dopo la frammentazione, i segmenti non dovrebbero essere più modificati.

Livello di Linea
Frammentazione

- Ogni stazione deve essere in grado di ricevere frammenti di dimensione arbitraria.
- La trasmissione dei diversi frammenti viene effettuata con modalità simili alla frammentazione IPv4
  - *sequence control*, contiene un identificatore del pacchetto (8 bit) e un numero di frammento (4 bit);
  - *more fragments*, per individuare l'ultimo segmento.
- Un unico timer viene mantenuto per la trasmissione di un pacchetto
  - alla scadenza tutti i frammenti vengono scartati.
- Il WEP viene applicato ad ogni singolo frammento.

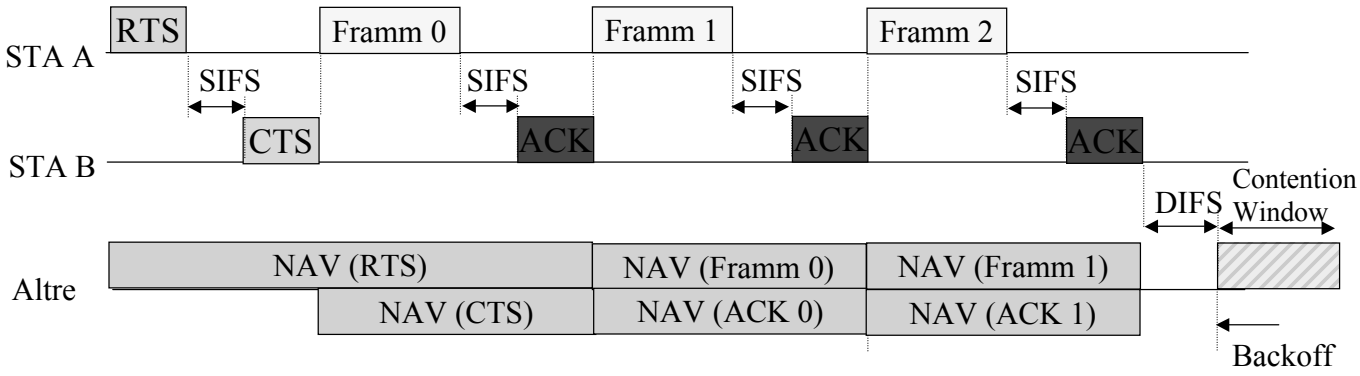
Livello di Linea
Riassemblaggio

- Ogni pacchetto viene decifrato.
- La completa ricezione di un pacchetto viene rilevata sulla base del flag *More Fragments*.
- Ogni stazione deve essere in grado di gestire la ricezione contemporanea di almeno 3 pacchetti
  - un timer deve essere mantenuto per ogni diverso pacchetto;
  - allo scadere del timer tutti i frammenti del relativo pacchetto devono essere scartati;
  - i segmenti duplicati o ricevuti oltre la scadenza del timer vanno confermati ma scartati.

Livello di Linea
RTS/CTS con frammentazione

- I pacchetti RTS/CTS contengono una indicazione sulla durata del successivo frame.
- Ogni segmento trasporta l'informazione sulla durata della successiva trasmissione
  - in pratica ogni segmento si comporta come un RTS/CTS virtuale.
- L'ultimo segmento deve indicare un NAV pari alla durata di un ACK più un SIFS
  - il corrispondente ACK deve avere una durata pari a 0.

Livello di Linea
RTS/CTS con frammentazione



Sicurezza

- Un aspetto fondamen tale nelle WLAN è rappresentato dalla sicurezza
  - l'utilizzo delle onde radio non permette di controllare in modo preciso l'estensione fisica della rete.
- Due sono gli aspetti legati alla sicurezza:
  - prevenire l'utilizzo da parte della rete da parte di stazioni non autorizzate;
  - evitare l'ascolto del traffico della LAN da parte di stazioni esterne.
- Lo standard 802.11 presenta meccanismi di protezione non completamente adeguati
  - autenticazione
    - » *Open Authentication* e *Shared Key;*
  - cifratura
    - » WEP
- Entrambi i meccanismi hanno come obiettivo quello di fornire un livello di protezione equivalente a quello delle reti cablate
  - in molte situazioni questo non può essere considerato sufficiente;
  - esistono varie tecniche attraverso le quale è possibile violare con successo questi meccanismi di protezione.

Sicurezza
Autenticazione

- L'autenticazione consente di stabilire l'identità delle parti comunicanti.
- Lo standard prevede due forme di autenticazione
  - l'informazione è contenuta nel corpo dei pacchetti stessi.
- Una relazione di autenticazione reciproca esiste alla fine della procedura.
- L'autenticazione deve essere stabilita
  - tra le stazione e l'AP, nei sistemi ad infrastruttura;
  - tra le stazioni, nelle reti ad hoc (IBSS).

Sicurezza
Autenticazione

- *Open system authentication*
  - le parti si scambiano una trama contenente la propria identità;
  - in pratica consiste in uno scambio di informazioni senza nessun algoritmo di autenticazione;
  - è un semplice meccanismo per accordarsi sullo scambio di dati, senza prevedere nessuna politica di sicurezza;
  - è il meccanismo di default dell'802.11.

Sicurezza
Autenticazione

- *Shared key authentication*
  - le parti possiedono una chiave segreta condivisa;
  - l'algoritmo prevede l'autenticazione senza richiedere lo scambio delle password in chiaro;
  - la distribuzione delle chiavi segrete deve avvenire attraverso un canale sicuro esterno a 802.11
    - » la chiave viene mantenuta in un registro di sola scrittura, in modo che possa essere letto solo dal MAC;
  - l'autenticazione avviene cifrando un messaggio di prova
    - » la stazione che richiede l'autenticazione invia il messaggio di prova;
    - » l'altra stazione cifra il messaggio;
    - » la stazione iniziale verifica la corretta cifratura del messaggio.

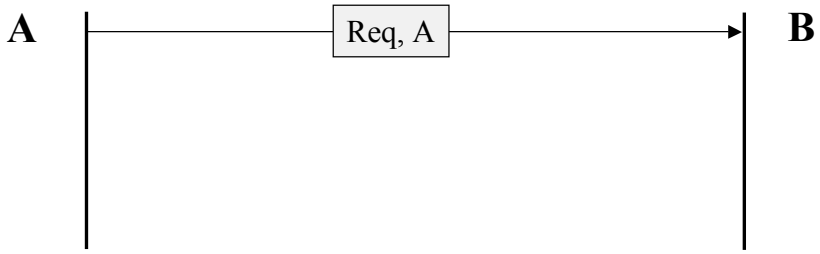
Sicurezza
Autenticazione

Sicurezza
Autenticazione

K_{ab} chiave segreta condivisa

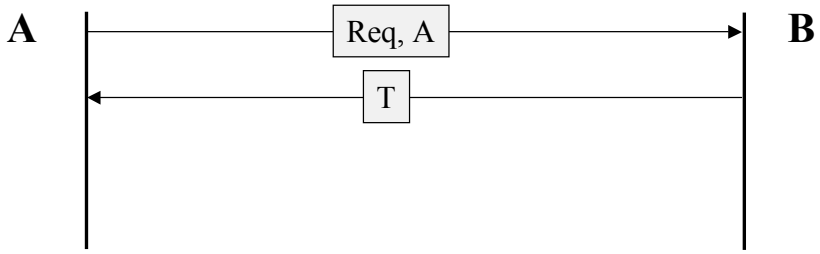
Architetture e Protocolli Wireless -N. O.

Sicurezza
Autenticazione



K_{ab} chiave segreta condivisa

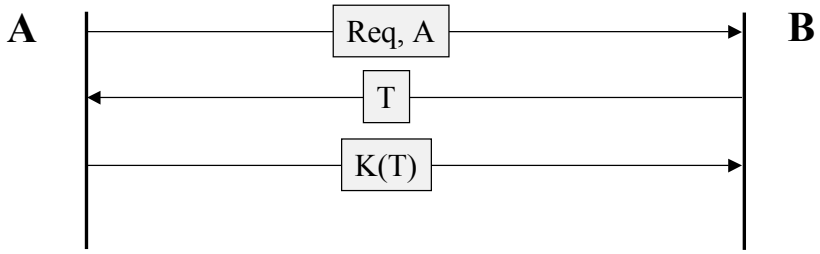
Sicurezza
Autenticazione



T = Challenge Text K_{ab} chiave segreta condivisa

Architetture e Protocolli Wireless -N. O.

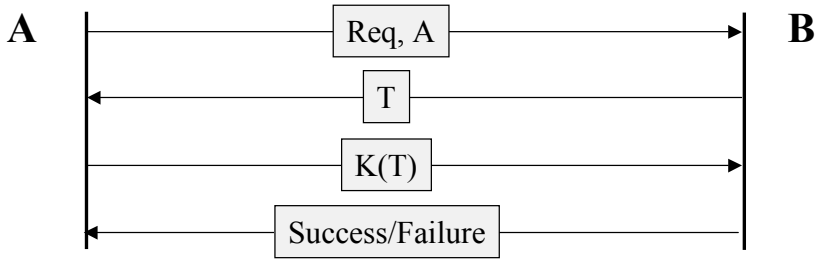
Sicurezza
Autenticazione



T = Challenge Text K_{ab} chiave segreta condivisa

$E_{Kab}(M,T)$ pacchetto contentente il Challenge Text cifrato con WEP

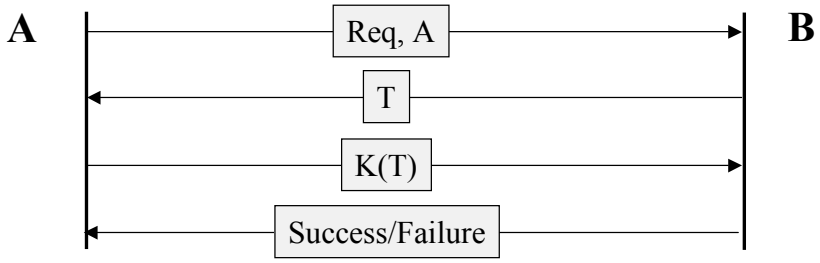
Sicurezza
Autenticazione



T = Challenge Text K_{ab} chiave segreta condivisa

$E_{Kab}(M,T)$ pacchetto contentente il Challenge Text cifrato con WEP

Sicurezza
Autenticazione



T = Challenge Text K_{ab} chiave segreta condivisa

$E_{Kab}(M,T)$ pacchetto contentente il Challenge Text cifrato con WEP

- Il livello di sicurezza fornito è inferiore all'altro meccanismo!
  - il contenuto del pacchetto cifrato è noto
    - » è possibile ricavare il keystream utilizzato per la cifratura
    - » è possibile risalire alla coppia chiave/IV utilizzata per la cifratura (si veda l'algoritmo WEP).

Sicurezza
Wired Equivalent Privacy (WEP)

- L'802.11 prevede un meccanismo di sicurezza che dovrebbe fornire lo stesso livello di sicurezza di una LAN cablata
  - la sicurezza di una LAN cablata consiste nel solo collegamento fisico
    - » i dati sono visibili a tutti gli utenti appartenenti alla stessa LAN;
  - nelle WLAN la sicurezza si appoggia sulla crittografia e sulla condivisione da parte degli utenti della stessa chiave simmetrica.

Sicurezza
Wired Equivalent Privacy (WEP)

- Proprietà dell'algoritmo WEP
  - *ragionevole sicurezza*
    - » resistente agli attacchi a forza bruta;
    - » cambio frequente delle chiavi/IV;
  - *auto-sincronizzazione*
    - » fondamentale per un livello di linea soggetto ad un alto tasso di errore;
  - *efficienza*
    - » WEP può essere realizzato in sw o hw;
  - *esportabilità*
    - » non ci sono garanzie che tutte le implementazione del WEP possano essere esportate dagli USA;
  - *discrezionalità*
    - » l'utilizzo di WEP non è obbligatorio.

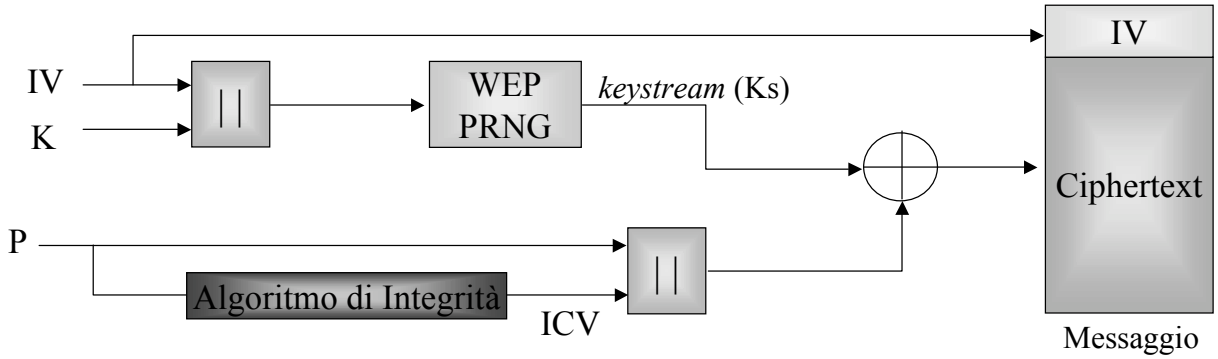
Sicurezza
Wired Equivalent Privacy (WEP)

- Richiami di crittografia
  - *cifratura*, processo per convertire un messaggio in una forma non comprensibile;
  - *plaintext* (P), testo in chiaro;
  - *ciphertext* (C), testo cifrato;
  - *cipher* o *algoritmo crittografico*, funzione matematica per trasformare il *plaintext* in *ciphertext* (E) o viceversa (D)

$$E_K(P) = C$$
$$D_K(C) = P$$
$$D_K(E_K(P)) = P$$

Sicurezza
Wired Equivalent Privacy (WEP)

Cifratura



IV Initialization Vector (24 bit)
K Secret Key (40 bit)
ICV Integrity Check Value (4 byte)
PRNG Pseudo Random Number Generator (RC4)
P Frame MAC in chiaro
|| Concatenazione

Sicurezza

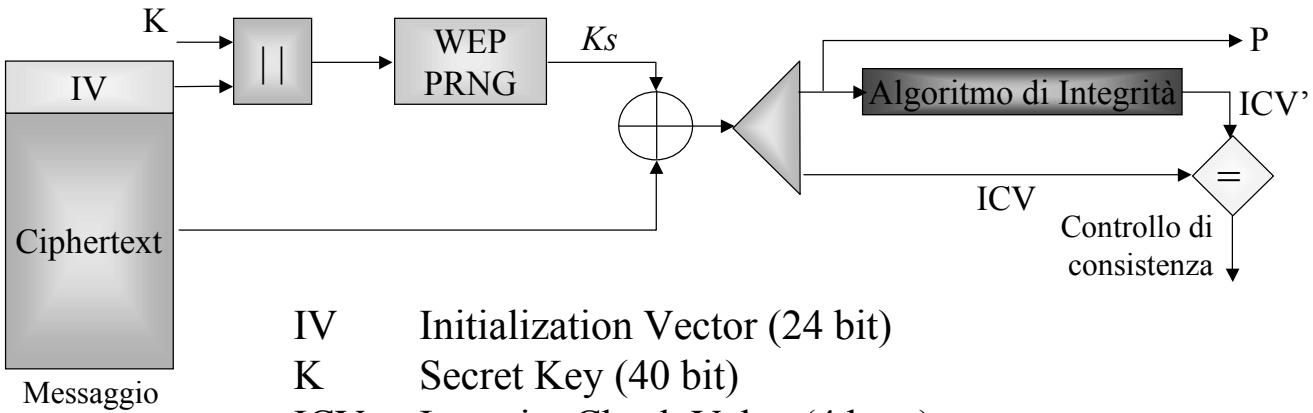
Wired Equivalent Privacy (WEP)

- La cifratura è di tipo a flusso.
- L'utilizzo di un ICV protegge contro possibili alterazioni del messaggio
  - CRC a 32 bit.
- L'utilizzo di un IV rende la chiave variabile dinamicamente
  - protezione contro la criptoanalisi;
  - necessità di cambiare spesso l'IV
    - » possibilmente ad ogni frame;
  - chiave segreta di lunghezza limitata (attacchi a forza bruta).
- La lunghezza della chiave può essere 40 o 104 bit (a cui vanno in ogni caso aggiunti 24 bit di IV).

Sicurezza

Wired Equivalent Privacy (WEP)

Decifratura



IV	Initialization Vector (24 bit)
K	Secret Key (40 bit)
ICV	Integrity Check Value (4 byte)
PRNG	Pseudo Random Number Generator (RC4)
P	Frame MAC in chiaro
Ks	Keystream
||	Concatenazione

Sicurezza
Wired Equivalent Privacy (WEP)

- In ricezione
  - la chiave è nota;
  - l'IV viene recuperato dal messaggio ricevuto;
  - viene generato lo stesso *keystream* utilizzato in trasmissione
    - » la decodifica si basa sul fatto che:

$$P \oplus Ks \oplus Ks = P$$

  - viene ricalcolato il CRC sul messaggio ICV' e confrontato con quello ricevuto ICV;
    - » i pacchetti non decifrati correttamente vengono scartati.

Sicurezza
Cifratura a flussi

- Una cifratura a flussi è in grado di eseguire la crittografia del testo in chiaro un bit alla volta
  - tipicamente opera su almeno un byte alla volta.
- Il meccanismo consiste nel
  - generare una sequenza (*keystream*) pseudocasuale a partire da una chiave;
  - eseguire un OR esclusivo (XOR) tra il *keystream* ed il testo in chiaro.
- La cifratura a flussi è simile alla tecnica *One-Time Pad*
  - la tecnica one-time pad usa sequenze veramente casuali.

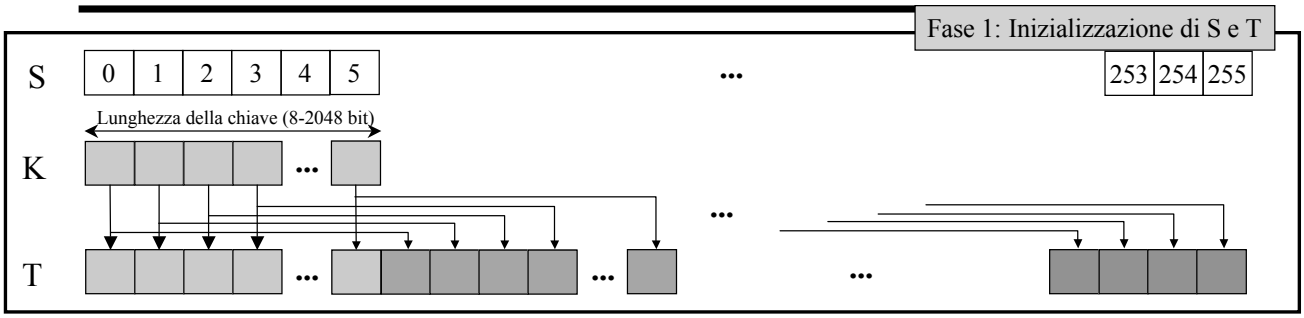
Sicurezza
Cifratura a flussi

- Proprietà di un codificatore a flussi
  - il *keystream* deve avere un periodo molto elevato
    - » rende difficile l'analisi crittografica;
  - il *keystream* deve approssimare le proprietà di un numero casuale
    - » rende minima l'informazione contenuta nel testo cifrato;
  - la chiave deve essere sufficientemente lunga
    - » impedisce gli attacchi a forza bruta;
    - » almeno 128 bit.
- La cifratura a flussi può essere sicura quanto la cifratura a blocchi
  - il generatore pseudocasuale deve essere progettato in modo accurato;
  - è in genere più veloce e semplice
  - non permette di riutilizzare la stessa chiave
    - » lo XOR di due testi crittografati elimina la cifratura;
  - rappresenta la soluzione preferita per flussi di dati
    - » canali di comunicazioni sicuri (SSL, browser-Web).

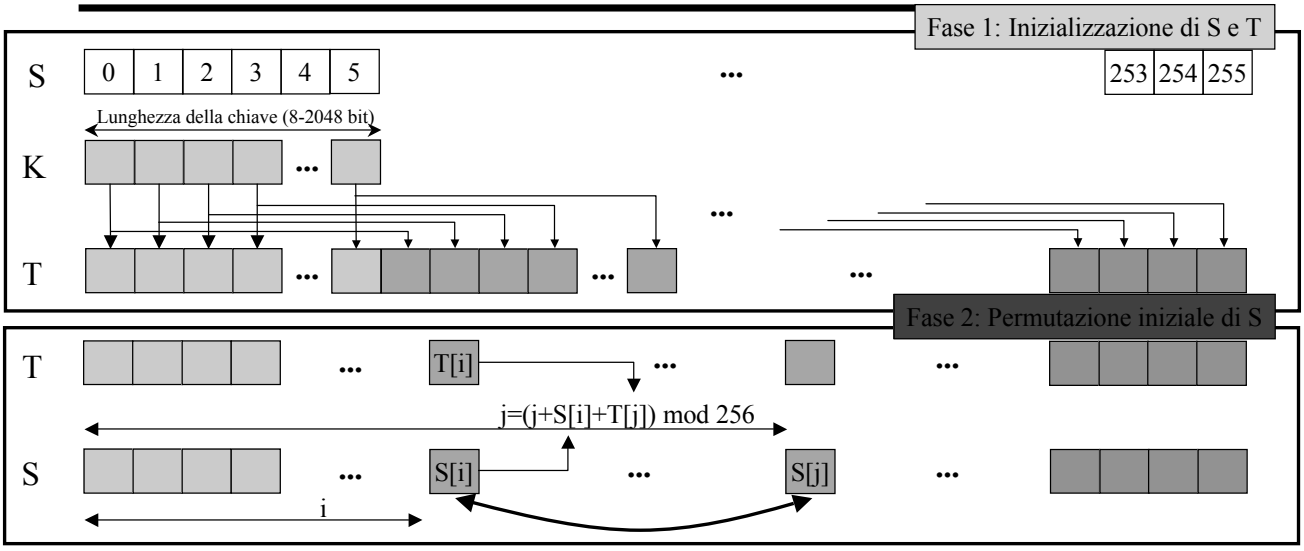
Sicurezza
Cifratura a flussi – RC4

- Progettato nel 1987 da Ron Rivest per RSA Security.
- Chiave di dimensione variabile e operazioni orientate al byte.
- Il periodo della cifratura è enorme ($>10^{100}$).
- RC4 è attualmente la cifratura di flussi più diffusa
  - è molto veloce anche nelle implementazioni software;
  - è utilizzata anche dagli standard TLS/SSL.
- L'algoritmo RC4 è stato inizialmente tenuto segreto da RSA Security
  - nel 1994 la comunità degli hacker lo ha diffuso in rete.

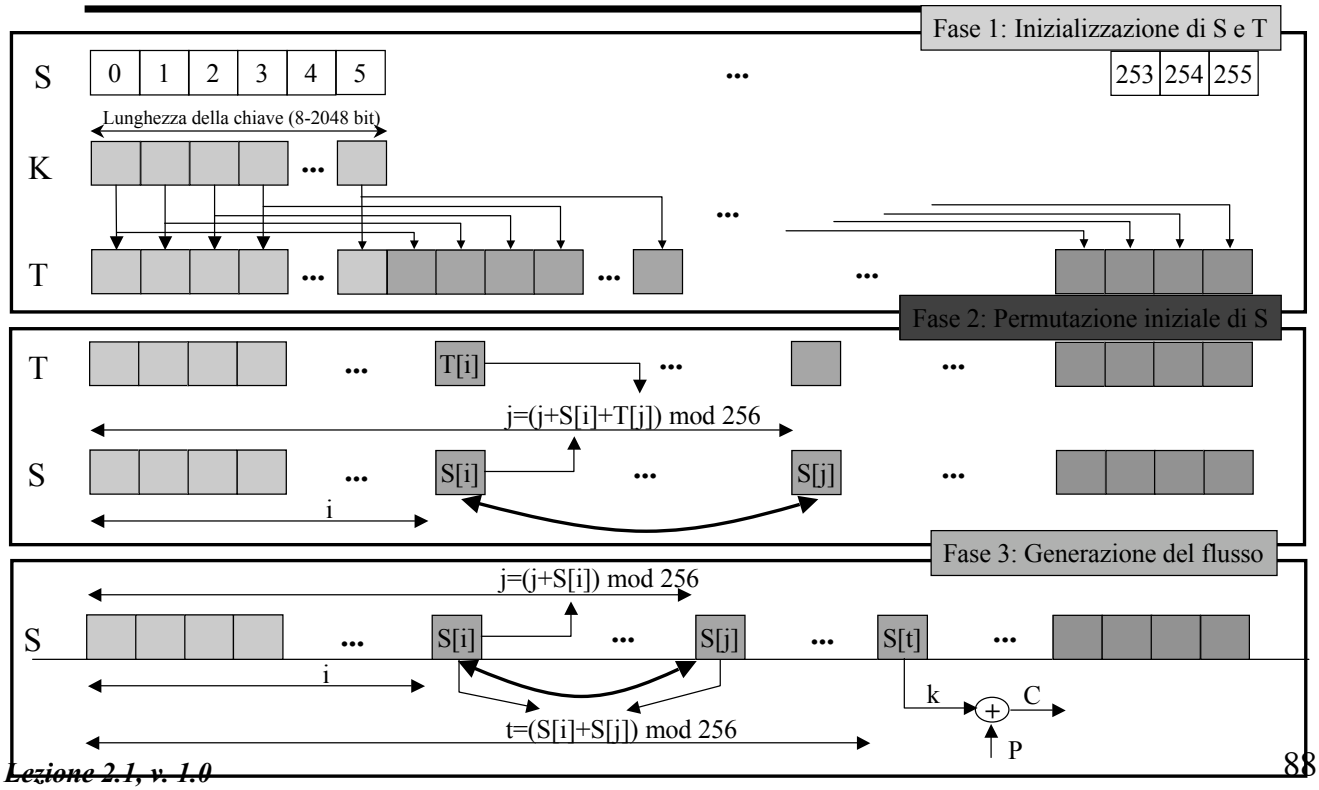
Sicurezza
L'algoritmo RC4



Sicurezza
L'algoritmo RC4



Sicurezza
L'algoritmo RC4



Sicurezza
Resistenza di RC4

- Diversi lavori su metodi di attacco all'algoritmo RC4 sono stati pubblicati
  - nessun approccio è realistico utilizzando una chiave di almeno 128 bit.
- Il protocollo WEP tuttavia è altamente insicuro
  - la vulnerabilità deriva dal modo in cui vengono generate le chiavi dell'algoritmo e non dall'algoritmo stesso;
  - il problema sembra non estendersi ad altre applicazioni basate su RC4.

Sicurezza

Sicurezza del WEP

- Problematiche connesse all'algoritmo WEP:
  - modifiche ai pacchetti in transito (anche senza la possibilità di decifrarli)
    - » CRC a 32 bit
  - l'utilizzo dello stesso *keystream* permette di ricavare facilmente lo XOR del testo in chiaro:

M_1 e M_2 messaggi, k_s keystream:

$$C_1 = k_s \oplus M_1 \text{ e } C_2 = k_s \oplus M_2$$

$$C_1 \oplus C_2 = k_s \oplus M_1 \oplus k_s \oplus M_2 = M_1 \oplus M_2$$

- » possibilità di usare tecniche di analisi crittografica;
- » utilizzo dell'*Initial Vector*.

Sicurezza

Debolezze del WEP

- Il CRC a 32 bit è lineare
  - la modifica di uno o più bit si ripercuote in maniera lineare sul CRC;
  - il *keystream* agisce sui singoli bit del pacchetto;
  - una modifica su un bit si ripercuote in una modifica deterministica di ben precisi bit del CRC.
- Un intruso può invertire i valori di alcuni bit del messaggio e i corrispondenti del CRC in modo che il messaggio decodificato appaia ancora valido.

Sicurezza
Debolezze del WEP

- Il vettore di inizializzazione IV è di 24 bit
  - il riutilizzo degli stessi *keystream* è garantito!!!
  - un AP che invia pacchetti di 1500 byte a 11 Mbps esaurisce lo spazio degli IV in:

    $1500*8/(11*10^6)*2^{24} \approx 18000$ s = 5 ore
  - questo permette ad un intruso di collezionare due pacchetti crittati con lo stesso *keystream* e tentare un attacco statistico;
  - l'intruso può anche ricavare il *keystream* per un determinato valore IV
    - » a questo punto può interferire in modo attivo nella trasmissione;
    - » l'utilizzo dello stesso IV da parte di una stazione non invalida i pacchetti inviati.

Sicurezza
Debolezze del WEP

- In realtà le cose sono ancora più semplici:
  - l'utilizzo da parte di più stazioni della stessa chiave rende più semplice l'individuazione di pacchetti cifrati con lo stesso IV
    - » secondo la teoria del *birthday attack* basta osservare 2^{12} pacchetti;
  - molte schede di rete inizializzano IV a 0 all'avvio e lo incrementano di 1 per ogni pacchetto inviato
    - » due schede inserite quasi contemporaneamente forniscono una quantità di collisioni sull'IV superiore a quelle necessarie;
    - » lo standard addirittura non richiede che l'IV vari per ogni pacchetto!

Sicurezza
Attacchi al WEP

- Attacchi passivi per la decifratura
  - collezione di pacchetti cifrati con lo stesso IV;
  - analisi statistica dello XOR dei testi in chiaro;
  - il traffico IP è abbastanza prevedibile;
  - utilizzando più pacchetti con lo stesso IV la probabilità di successo dall'analisi statistica aumenta rapidamente;
  - ricavato un intero messaggio in chiaro, la decifratura degli altri con lo stesso IV è immediata
    - » lo *keystream* è banale da ricavare: $k_s = C \oplus M$;
    - » l'utilizzo dell'autenticazione *shared key* presenta questo inconveniente;
  - mandando traffico da un host in internet verso la WLAN si facilita la collezione di coppie (IV, *keystream*).

Sicurezza
Attacchi al WEP

- Attacchi attivi per la modifica dei messaggi
  - conoscendo esattamente il contenuto del messaggio in chiaro X;
  - è possibile generare un nuovo messaggio Y con CRC valido;
  - l'alterazione avviene senza la violazione della cifratura RC4:

$$RC4(X) \oplus X \oplus Y = k_s \oplus X \oplus X \oplus Y = k_s \oplus Y = RC4(Y)$$

  - è possibile alterare il messaggio anche senza la conoscenza del testo in chiaro
    - » modificando i bit che interessano (le cifrature a flusso non alterano la sequenza originale delle informazioni);
    - » aggiustando il CRC come descritto in precedenza.

Sicurezza
Attacchi al WEP

- Attacchi attivi alla destinazione
  - è un'estensione della tipologia precedente;
  - l'intruso può tentare di indovinare informazioni relative all'intestazione dei pacchetti, piuttosto che la contenuto;
  - in particolare interessa indovinare l'indirizzo IP di destinazione;
  - l'indirizzo IP di destinazione può essere modificato con un host esterno alla WLAN
    - » il pacchetto viene inviato in chiaro all'host fasullo
    - » se si riesce a modificare anche la porta TCP di destinazione (80) è possibile bypassare la maggior parte dei firewall.

Sicurezza
Attacchi al WEP

- Attacchi basati sulla creazione di una tabella
  - l'intruso può utilizzare gli attacchi di tipo passivo per costruire una tabella di corrispondenze (IV, k_s);
    - » queste informazioni permettono di decifrare tutto il traffico in transito e di effettuare trasmissioni;
  - col passare del tempo, la tabella di corrispondenze può arrivare a coprire tutto lo spazio degli IV
    - » in totale lo spazio richiesto dalla tabella è abbastanza limitato (ca 15 GB);
    - » ovviamente indicizzare un database di tali dimensioni non è un problema banale!
  - il completamento della tabella permette all'intruso di decifrare qualsiasi pacchetto, fino a quando la chiave non viene modificata.

Sicurezza
Difficoltà degli attacchi al WEP

- La maggior parte degli attacchi passivi non richiede particolari dispositivi
  - le normali schede wireless collezionano il tutto il traffico
    - » con poche modifiche nei driver è possibile intercettare anche le trasmissioni cifrate a livello software.
- Gli attacchi attivi appaiono più complessi, anche se non impossibili
  - molti apparati 802.11 sono dotati di un firmware che è possibile analizzare e modificare tramite un *reverse ingeneering*
    - » le comunità di hacker si scambiano spesso i loro "prodotti"...
    - » il lavoro di routine viene fatto dai "semplici operai"

Sicurezza
Difficoltà degli attacchi al WEP

- Diverse tecniche di decifratura del WEP sono state proposte
  - l'implementazione di alcune di esse ha dimostrato
    - » la relativa facilità di implementazione;
    - » l'efficacia.
- L'IEEE ha risposto a questi attacchi con alcune precisazioni:
  - il WEP non è stato progettato per garantire maggior sicurezza di Ethernet;
  - è molto peggio non usare affatto il WEP;
  - suggerisce di realizzare la sicurezza a livelli più alti;
  - l'introduzione di un livello di sicurezza adeguato è rimandato al successivo 802.11i.

MAC Management Sublayer

- Sincronizzazione.
- *Power management.*
- *Roaming*.

MAC Management Sublayer
Sincronizzazione

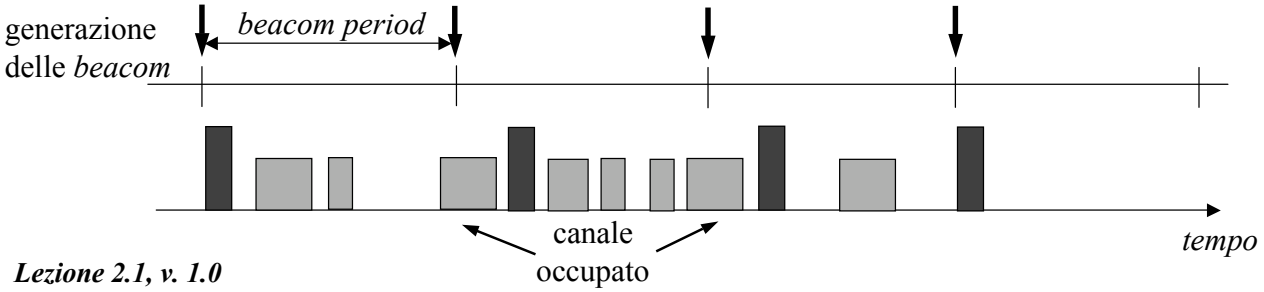
- Tutte le stazioni devono essere sincronizzate.
- Ogni stazione deve mantenere un orologio locale.
- L'aggiornamento degli orologi avviene con pacchetti denominati *beacom*
  - nelle reti con infrastruttura vengono trasmessi dall'AP;
  - nelle IBSS sono inviate da ciascuna stazione
    - » il clock viene aggiornato al valore di quello più "avanti".

MAC Management Sublayer
Sincronizzazione

- L'ora locale è espressa in microsecondi
  - viene memorizzata modulo 2^{64}.
- Il valore contenuto nel *beacom* si riferisce all'istante reale di invio del pacchetto
  - viene compensato il ritardo introdotto dall'interfaccia MAC/PHY e dall'attraversamento del livello fisico,
  - l'algoritmo mantiene una sincronizzazione entro 4 μs + tempo di propagazione.

MAC Management Sublayer
Sincronizzazione – Infrastruttura

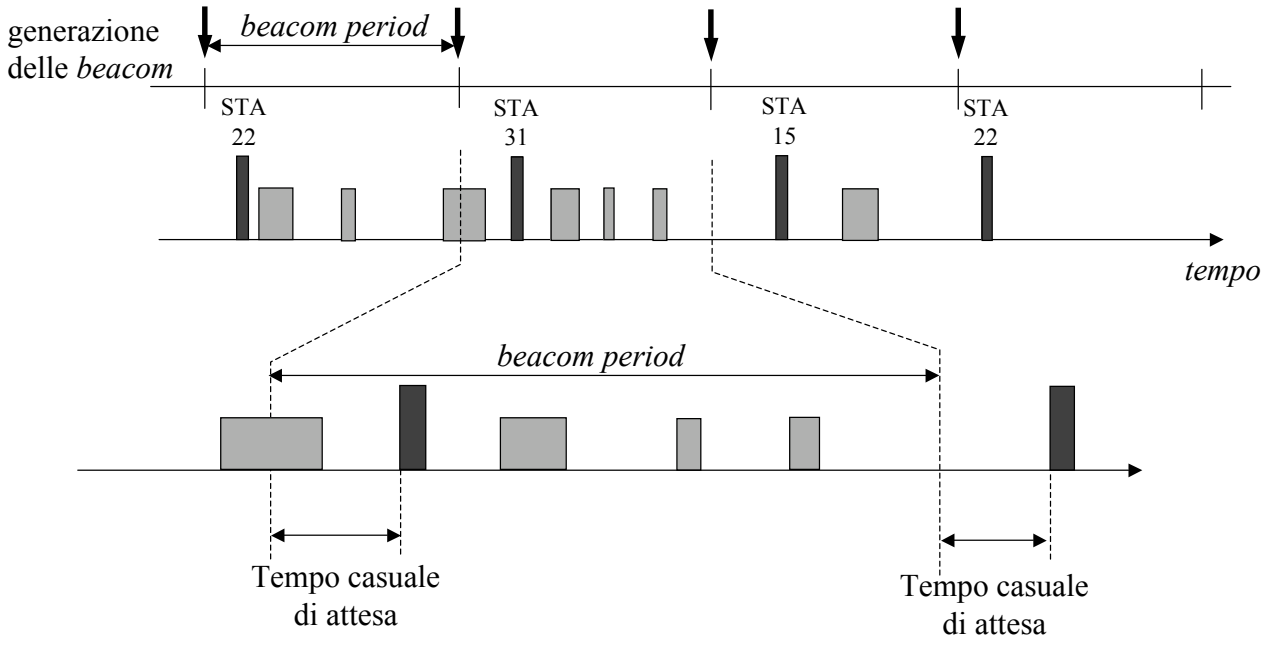
- Le *beacom* vengono inviate ad intervalli costanti (*beacom period*)
  - la stazione schedula la trasmissione delle *beacom* in maniera prioritaria rispetto agli altri pacchetti;
  - la trasmissione delle *beacom* segue le regole del CSMA;
  - il *beacom period* viene notificato dentro il pacchetto *beacom*.



MAC Management Sublayer
Sincronizzazione – IBSS

- La generazione delle *beacom* è distribuita
  - ogni stazione genera delle *beacom*;
  - l'intervallo di generazione delle *beacom* è scelto dalla stazione che inizializza l'IBSS
    - » tale valore è riportato in tutte le *beacom* trasmesse;
  - ad ogni istante di generazione delle *beacom* ciascuna stazione deve
    - » interrompere il decremento del timer di backoff;
    - » calcolare un tempo casuale con distribuzione uniforme in [0, CW_{min}];
    - » attivare un timer e decrementarlo con un'algoritmo uguale a quello di backoff;
    - » cancellare l'operazione se arriva una *beacom* prima dello scadere del timer;
    - » inviare la *beacom* allo scadere del timer.

MAC Management Sublayer
Sincronizzazione – IBSS



MAC Management Sublayer
Sincronizzazione

- Il valore dell'orologio ricevuto
  - viene incrementato del tempo necessario ad attraversare la circuiteria dal livello fisico al MAC;
  - viene incrementato del tempo di trasmissione della *beacom*;
  - viene utilizzato per aggiornare l'orologio locale
    - » nel caso di IBSS l'orologio locale viene aggiornato solo se il valore ricevuto è successivo.
- L'accuratezza della sincronizzazione dovrebbe essere dell'ordine di ±0,01%.

MAC Management Sublayer
Beacom frames

- Un pacchetto *beacom* è sempre inviato in broadcast
  - tutte le stazioni sono obbligate a riceverlo.
- I campi di un *beacom* sono:
  - *beacom interval* l'intervallo di trasmissione dei *beacom*, informazione particolarmente utile per le stazioni in modalità *power save*;
  - *timestamp*, il valore dell'orologio di riferimento;
  - *SSID (Service Set ID)*, l'identificativo della WLAN;

MAC Management Sublayer
Beacom frames

- *supported rates*, in quanto la WLAN potrebbe non supportare tutte le velocità previste;
- *parameter Sets*, indica le modalità di trasmissione (FHSS, DSSS), il canale utilizzato, informazioni specifiche
  - » sequenza dei salti e frequenza per il FH;
- *capability information*, requisiti per le stazioni che desiderano associarsi (es. WEP);
- *traffic indication map (TIM)*, identifica quali stazioni in *power save* hanno dati in attesa presso l'AP.

MAC Management Sublayer
Beacom frames

- Incrementando la frequenza di invio delle *beacom*
  - i processi di associazioni e roaming richiedono una latenza minore;
  - cresce l'overhad del sistema.
- Diminuendo la frequenza delle *beacom* si ottiengono risultati opposti.
- Molte NIC monitorano tutte le *beacom*
  - individuazione dell'AP più adatto;
  - *roaming*;
  - supporto alle stazioni in *power save*;
  - per ragioni di sicurezza l'invio del SSID all'interno delle *beacom* può essere disabilitato;
  - senza le *beacom* una WLAN non può funzionare!

MAC Management Sublayer
Scanning

- L'operazione di ascolto delle *beacom* è denominata *scanning*:
  - ***passive scanning***, la stazione ascolta ogni canale per un determinato tempo;
  - ***active scanning***, la stazione invia delle *Probe Request* per ogni canale, a cui seguiranno dei *Probe Response* con struttura analoga alle *beacom*
    - » nelle reti ad infrastruttura sono inviati dall'AP;
    - » nelle reti ad-hoc sono inviati dalla stazione che per ultima ha trasmesso la *beacom*;
    - » una stazione deve sempre essere attiva per rispondere ai *Probe Request*.
- Dopo aver effettuato la procedura di *scanning* la stazione può entrare a far parte della rete tramite le procedure di autenticazione e associazione.

MAC Management Sublayer
Power management

- L'ambito operativo delle WLAN coinvolge tipicamente applicazioni legati alla mobilità
  - gli apparati sono spesso alimentati a batteria;
  - il problema del consumo di potenza è significativo;
  - l'802.11 si occupa del problema del risparmio di potenza
    - » definisce un meccanismo che permette alle stazioni di rimanere inattive per lunghi periodi senza
      - perdere informazioni;
      - scollegarsi dalla rete.

MAC Management Sublayer
Power management

- L'idea di base:
  - mantenere una lista presso l'AP delle stazioni che si trovano in *power saving*;
  - memorizzare i pacchetti diretti a queste stazioni;
  - inviare le informazioni sui pacchetti in attesa all'interno delle *beacom*;
  - inviare i pacchetti alle stazioni quando
    - » li richiedono,
    - » abbandonano la modalità *power saving*;
  - anche i pacchetti multicast/broadcast vengono memorizzati
    - » vengono inviati ad istanti ben noti.

MAC Management Sublayer
Power management

- Una stazione può trovarsi in due differenti stati:
  - *awake*: pienamente funzionante ed alimentata;
  - *doze*: non è in grado di trasmettere o ricevere e ha consumi bassissimi.
- Dal punto di vista delle modalità di funzionamento si distingue:
  - *active mode (AM)*: la stazione di trova nello stato *awake* e può ricevere frame ad ogni istante;
  - *power save (PS)*: la stazione si alterna tra gli stati *awake* e *doze*.

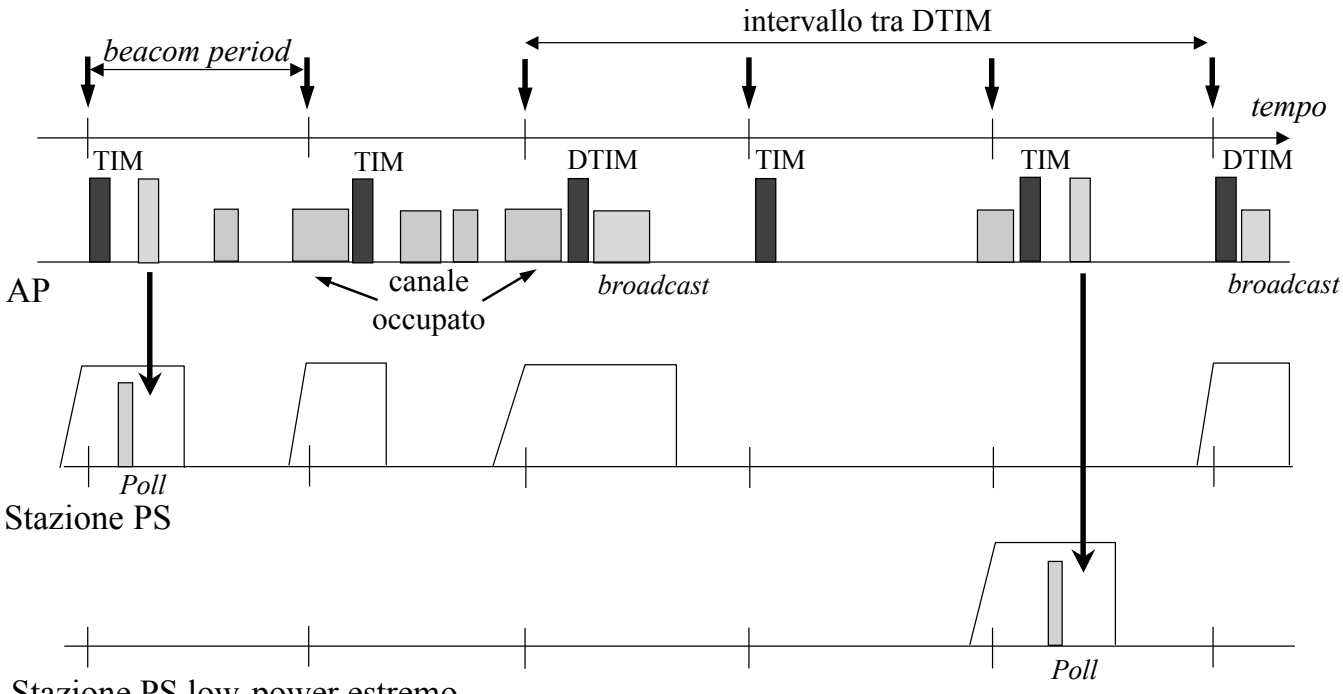
MAC Management Sublayer
Modalità *Power Save* – Infrastruttura

- La stazione che desidera attivare la modalità PS:
  - deve informare l'AP attraverso un determinato meccanismo di *handshake*;
  - deve passare periodicamente allo state *awake* per ascoltare le *beacom*;
  - richiede la trasmissione dei propri pacchetti tramite *polling*;
- L'AP:
  - deve mantenere una lista di stazioni attualmente in modalità PS;
  - memorizza tutti i pacchetti unicast e multicast/broadcast diretti verso le stazioni in modalità PS;
  - trasmette un elenco di tutte le stazioni che hanno pacchetti memorizzati (*Traffic Indication Map, TIM*) all'interno delle *beacom*.

MAC Management Sublayer
TIM – *Traffic Indication Map*

- Le TIM contengono un identificativo delle stazione per le quali sono presenti pacchetti
  - l'identificativo viene assegnato dall'AP in fase di associazione.
- Esistono due tipi di TIM
  - TIM, che segnale la presenza di pacchetti unicast;
  - DTIM (*Delivery TIM*) che segnala la presenza di pacchetti multicast/broadcast
    - » le DTIM sostituiscono le TIM a intervalli regolari;
    - » dopo le DTIM i pacchetti multicast/broacast sono trasmessi immediatamente;
    - » i pacchetti unicast possono essere richiesti solo dopo la trasmissione di quelli multicast/broadcast.

MAC Management Sublayer
Modalità *Power Save* – Infrastruttura



MAC Management Sublayer
Modalità *Power Save* – CP

- Durante i *Contention Period*
  - I frame in broadcast vanno memorizzati se è presente almeno una stazione in PS.
  - Nel caso in cui non fosse possibile inviare tutti i pacchetti multicast/broadcast memorizzati
    - » l'AP continua ad emettere DTIM al posto di TIM fino all'esaurimento dei pacchetti in coda.
  - I pacchetti unicast vanno inoltrati solo su richiesta
    - » le stazioni devono rimanere nello stato *awake* fino
      - alla ricezione delle TIM,
      - alla ricezione delle risposte alle loro interrogazioni;
    - » le richieste delle stazioni sono differite di un tempo casuale (uniformemente distribuito in [0, CW_{min}].

MAC Management Sublayer
Modalità *Power Save* – CP

- Se le stazioni sono configurate per ricevere i pacchetti multicast/broadcast
  - » devono passare allo stato *awake* in tempo per ricevere le DTIM,
  - » devono attendere nello stato *awake* fino
    - alla completa ricezione di tutto il traffico multicast/broadcast
    - alla ricezione di una TIM che indica che non è più presente traffico di questo tipo.
- È necessaria una funzione per eliminare i pacchetti da troppo tempo in coda.
- Appena una stazione commuta in modalità *Active* l'AP invia tutti le trame memorizzati senza attendere il *polling*.

MAC Management Sublayer
Modalità *Power Save* – CFP

- Durante i *Contention Free Period*
  - Il meccanismo coinvolge solo le stazioni che possono essere interrogate dal PC
    - » queste devono passare allo stato *awake* all'inizio del CFP per ricevere la prima DTIM.
  - L'AP indica nelle TIM le stazioni che il PC interrogherà.
  - Vengono trasmesse solo TIM di tipo DTIM.
  - I frame in broadcast vanno memorizzati se è presente almeno una stazione in PS, anche tra quelle non interrogabili.
  - Le stazioni devono passare allo stato *awake* per ricevere le DTIM e rimanervi con regole analoghe a quelle per il CP per
    - » ricezione pacchetti broadcast/multicast,
    - » ricezione dei pacchetti unicast.

MAC Management Sublayer
Modalità *Power Save* – CFP

- Ad ogni DTIM
  - » vengono inviati i pacchetti broadcast/multicast,
    - nel caso l'intervallo tra le *beacom* non fosse successivo alla tx di tutti i pacchetti si continua in quello successivo;
  - » La trasmissione dei pacchetti unicast avviene sotto il controllo del PC,
    - le stazioni PS devono rimanere attive per la ricezione dei loro pacchetti,
    - dopo la ricezione dell'ultimo pacchetto possono tornare nello stato *doze;*
  - » se il CFP termina prima della fine della trasmissione dei pacchetti unicast, la stazione interessata può
    - rimanere nello stato *awake* e trasmettere frame PS-Poll durante il CP,
    - tornare nello stato *doze* e attendere il successivo CFP.
- È necessaria una funzione per eliminare i pacchetti da troppo tempo in coda.
- Appena una stazione commuta in modalità *Active* l'AP prepara tutti i pacchetti in coda per l'invio nella successiva fase di *polling* da parte del PC.

MAC Management Sublayer
Modalità *Power Save* – Ad-hoc

- Le stazioni sono sincronizzate.
- I pacchetti verso destinazioni in PS sono memorizzati.
- I pacchetti memorizzati sono annunciati tramite ATIM (*Ad hoc TIM*)
  - le ATIM sono inviate durante intervalli in cui tutte le stazioni sono nello stato *awake* (*ATIM Window*)
    - » le ATIM Window si estendono a partire dall'istante di trasmissione delle *beacom*,
    - » durante una ATIM Window possono essere trasmesse solo *beacom* e ATIM,
    - » l'invio delle ATIM segue l'invio o la ricezione di una *beacom*.

MAC Management Sublayer
Modalità *Power Save* – Ad-hoc

- la trasmissione delle ATIM è resa casuale utilizzando la procedura di backoff
  - » la finestra di contesa è pari a $[0,CW_{min}]$;
- le ATIM unicast devono essere riscontrate
  - » in caso di mancata ricezione di un ACK la ritrasmissione avviene con la procedura di backoff,
  - » in caso di esaurimento della ATIM Window prima del riscontro si rimanda all'ATIM Window seguente;
- le stazioni che ricevono le ATIM devono rimanere *awake* per l'intero *beacom period* in attesa dell'invio vero e proprio dei pacchetti
  - » le altre possono entrare nello stato *doze*;

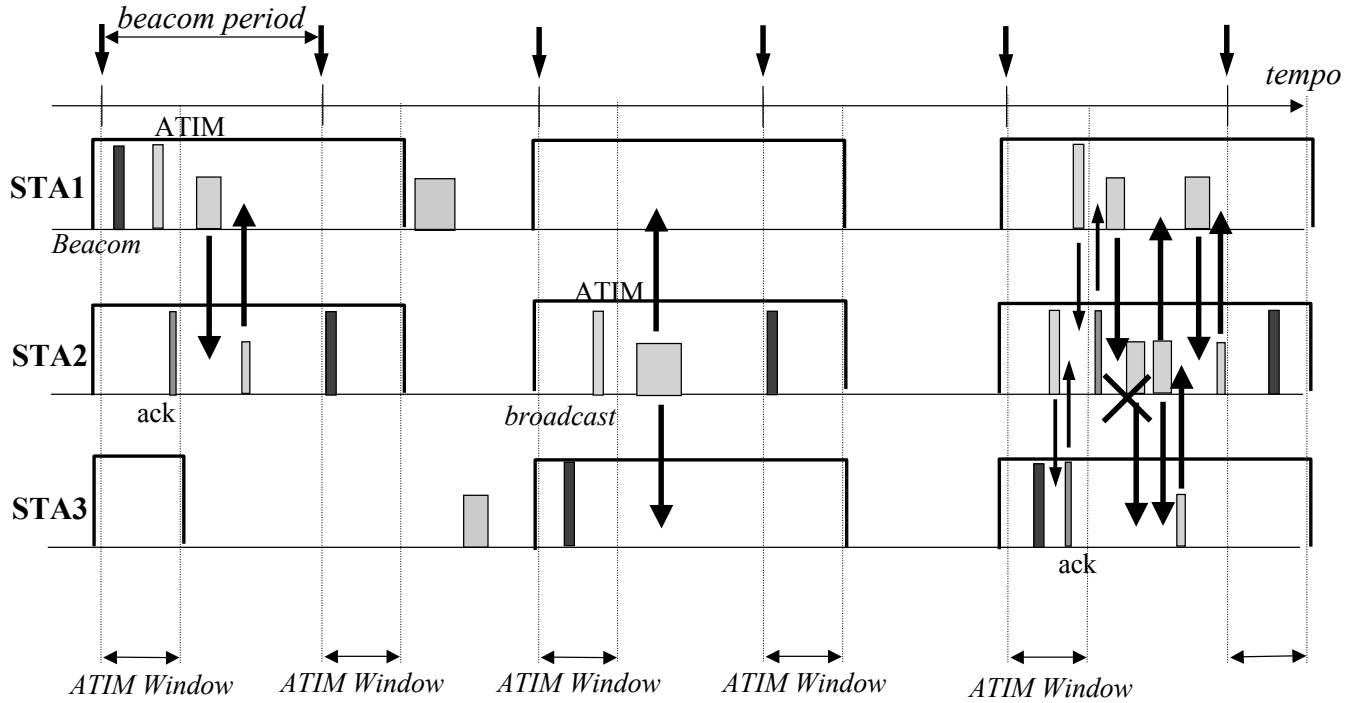
MAC Management Sublayer
Modalità *Power Save* – Ad-hoc

- dopo l'intervallo di invio delle ATIM
  - » possono essere inviate solo le MSDU per cui l'invio della ATIM è avvenuto correttamente,
  - » la trasmissione avviene con il meccanismo DCF,
  - » i pacchetti non inviati entro la *beacom* successiva vengono nuovamente annunciati,
  - » terminata la trasmissione dei pacchetti annunciati una stazione può inviare ulteriori pacchetti alle altre *awake*;
- l'accodamento dei pacchetti è limitato ad un certo intervallo temporale.

MAC Management Sublayer
Modalità *Power Save* – Ad-hoc

- Ogni stazione deve conoscere lo stato PS delle altre
  - stima
    - » informazioni *power management* trasmesse,
    - » informazioni locali (tentativi falliti),
    - » lo standard non specifica nessun meccanismo.
- L'utilizzo del meccanismo RTS/CTS riduce il numero di trasmissioni alle stazioni in PS.

MAC Management Sublayer
Modalità *Power Save* – Ad-hoc

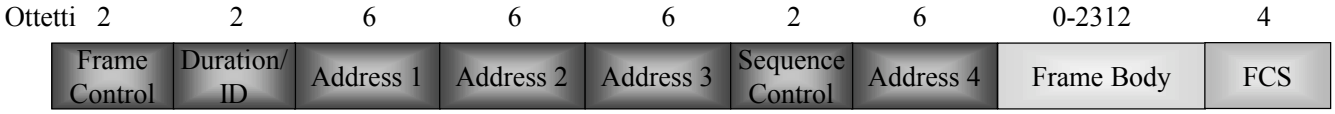


MAC Management Sublayer
Roaming

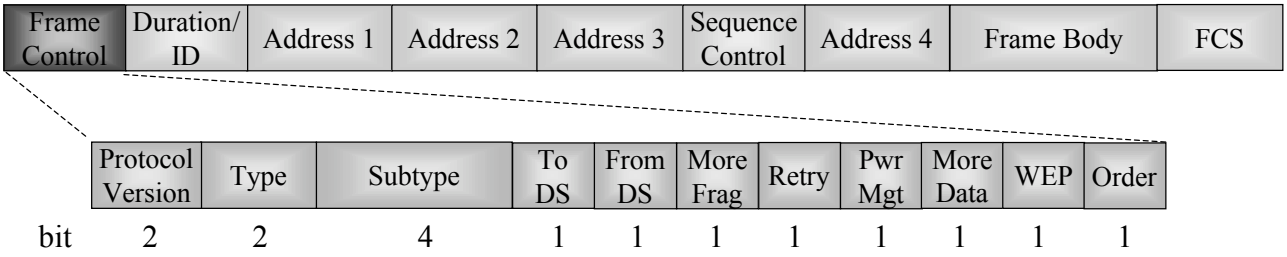
- L'operazione di *roaming* consiste nel passaggio tra due diverse BSS.
- È simile al processo di *handover* ma:
  - la transizione in una rete a pacchetto è leggermente più semplice rispetto ad una rete a commutazione di circuito;
  - la disconnessione temporanea in una rete a pacchetto ha conseguenze più significative sulle prestazioni del sistema
    - » scadenze timeout e ritrasmissione da parte dei protocolli di livello superiore.
- 802.11 non specifica come deve avvenire il *roaming* ma fornisce tutti gli strumenti necessari:
  - *active/passive scanning, re-association*.

Livello di Linea
Formato dei pacchetti

- A livello di linea ogni pacchetto è formato da
  - *intestazione MAC,*
  - *corpo del messaggio,*
  - *frame check sequence*.



Frame Control



- *Protocol Version*, attualmente 0.
- *Type*, identifica il tipo di frame
  - *management;*
  - *control;*
  - *data.*
- *Subtype*, identifica la funzione specifica del pacchetto.

Frame Control

Type/Subtype – *Management*

00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved

Frame Control
Type/Subtype – *Control*

01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack

Frame Control
Type/Subtype – *Data*

10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

Frame Control

- *ToDS*, indica i pacchetti destinati al DS
  - include tutti i pacchetti di tipo *data* inviati dalle stazioni associate ad un AP.
- *FromDS*, indica i pacchetti di tipo *data* provenienti dal DS.

Valori To/From DS		*Significato*
ToDS=0	FromDS=0	Pacchetto *data* da una stazione ad un'altra nella stessa IBSS. Pacchetti *management* e *control*.
ToDS=1	FromDS=0	Pacchetti *data* destinati al DS.
ToDS=0	FromDS=1	Pacchetti *data* provenienti dal DS.
ToDS=1	FromDS=1	Pacchetti scambiati tra gli AP attraverso il DS.

Frame Control

- *More Fragment*, indica la presenza di ulteriori frammenti appartenenti allo stesso pacchetto.
- *Retry*, il pacchetto è una ritrasmissione.
- *Pwr Mgt (Power Management)*, indica lo stato energetico della stazione al termine della trasmissione del pacchetto:
  - *0, power save mode;*
  - *1, active mode.*
- *More Data*, notifica alle stazioni in *power save* che ulteriori pacchetti sono memorizzati presso l'AP.
- *WEP*, il corpo del messaggio è stato cifrato.
- *Order*, il pacchetto è stato inviato attraverso la classe di servizio *StrictlyOrdered*.

Livello di Linea

Formato dei pacchetti

Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- *Duration/ID*
  - nei pacchetti di Poll delle stazioni in *power save* contiene un identificativo dell'associazione della stazione;
  - negli altri pacchetti indicata il valore di durata da utilizzare per il NAV.
- *Sequence Control*, è formato da due sottocampi:
  - *sequence number* (12 bit), assegnato ad ogni pacchetto
    - » è utile per la ritrasmissione;
  - *fragment number* (4 bit), distingue i diversi frammenti di uno stesso pacchetto.
- *Frame Body*, contiene informazioni specifiche per i diversi tipi di pacchetti.
- *FCS*, CRC a 32 bit che copre tutti i precedenti campi.

Livello di Linea

Formato dei pacchetti

Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- *Address*, contengono dei valori diversi, a seconda del tipo di frame e del valore dei campi To/FromDS:
  - *BSSID*, identificativo a 48 bit della BSS
    - » nel caso di infrastruttura coincide con l'indirizzo MAC dell'AP,
    - » nel caso di IBSS viene generato in modo casuale;
  - *Destination Address (DA)*, la/e destinazione/i finale del pacchetto;
  - *Source Address (SA)*, la stazione che ha generato il pacchetto;
  - *Receiver Address (RA)*, l'indirizzo MAC della stazione che deve ricevere il pacchetto;
  - *Transmitter Address (TA)*, l'indirizzo della stazione che ha trasmesso il pacchetto.

Livello di Linea

Formato dei pacchetti

- *Address-1*, è il *Recipient Address*
  - coincide con DA se il pacchetto è indirizzato all'interno della BSS.
- *Address-2*, è il *Transmitter Address*
  - coincide con con il SA se il pacchetto proviene dall'interno della cella.
- *Address-3*, è l'indirizzo che non è stato specificato nei precedenti campi (IBSS, SA o DA).
- *Address-4*, serve quando si utilizza un DS wireless per le comunicazioni tra AP.

ToDS	*FromDS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

802.11

- Lo standard prevede una serie di emendamente addizionali oltre a quelli precedentemente introdotti:
  - **802.11d**: Specification for Operation in Additional Regulartory Domains;
  - **802.11f**: IEEE Recommended Practice for Multi-Vendor Access Point;
  - Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation;
  - **802.11h**: Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe;
  - **802.11k**: Radio Resource Measurement.
- Altri emendamenti devono essere ancora approvati:
  - **802.11e**: Quality of Service (QoS) Enhancements;
  - **802.11i:** Authentication and Security;
  - **802.11j**: 4.9 GHz-5 GHz Operation in Japan;
  - **802.11n**: Estensione per portare la velocità massima a 108 Mbps.