UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione

Protocolli: strato PH e DL nelle Wireless LAN

Luca Veltri
(mail.to: luca.veltri@unipr.it)

Corso di Reti di Telecomunicazioni A, a.a. 2011/2012
http://www.tlc.unipr.it/veltri

Standard per Wireless LAN

- 802.11 (1997)
  - **prima versione dello standard IEEE 802.11 presentata nel 1997**
  - **velocità di trasmissione comprese tra 1 e 2 Mb/s**
  - **banda di frequenze IMS (Industrial Scientific & Medical) sui 2,4 GHz**
  - **differenti strati PH (FHSS, DSSS)**
  - **strato MAC di tiopo CSMA/CA**
- 802.11b (1999)
  - **evoluzione dello standard per trasmissioni a 11 Mbit/s**
  - **banda di frequenze sui 2.4 GHz, modulazione CCK**
  - **in caso di cattiva copertura può lavorare a 5,5, 2 o 1 Mb/s**
  - **spettro diviso in 14 sottocanali da 22 MHz ciascuno**
  - **stesso MAC di tipo CSMA/CA**
  - **lo standard più diffuso**
- IEEE 802.11i (2004)
  - **miglioramento della sicurezza (WPA2)**

Standard per Wireless LAN (cont.)

- 802.11a (2001)
  - **velocità massima di 54 Mb/s sebbene la velocità reale disponibile all'utente sia di circa 20 Mb/s**
  - **la velocità massima può essere ridotta a 48, 36, 24, 18, 9 o 6**
  - **utilizza spazio di frequenze intorno ai 5 GHz, modulazione OFDM**
  - **poco utilizzato, anche perché in molti paesi l'uso delle frequenze a 5 GHz è riservato**
- 802.11g (2003)
  - **stesse frequenze dello standard 802.11b (banda di 2,4 GHz)**
  - **capacità teorica di 54 Mb/s con velocità reali di 24,7 Mb/s (simile a allo standard 802.11a)**
  - **totalmente compatibile con lo standard 802.11b**
- 802.11n (2009)
  - **velocità reale intorno ai 100 Mb/s**
  - **possibilità di operare sia intorno ai 2.4 GHz che 5 GHz**
  - **include possibilità di utilizzare tecnologia MIMO**

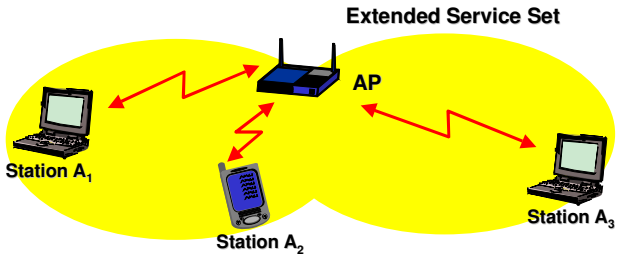
Had-hoc mode

- Definizione: Basic Service Set (BSS)
  - **gruppo di stazioni che sono sotto la stessa area di copertura (i.e. cella) e comunicano tra di loro attraverso una stessa funzione di controllo (CDF o PCF, vedi oltre)**
  - **concettualmente ogni stazione all'interno di una BSS può comunicare direttamente con un'altra**
- Modalità di rete ad-hoc (Ad-hoc mode)
  - **tutte le stazioni si trovano in un unico BSS indipendente (Independent Basic Service Set) IBSS**
  - **solo stazioni all'interno della stessa area di copertura (direttamente raggiungibili tra loro) possono comunicare tra loro**

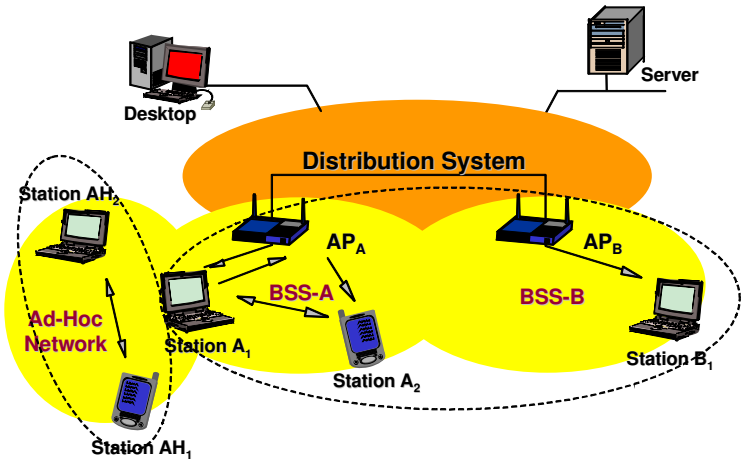
  - **se da una rete ad-hoc si vuole comunicare con un host esterno una stazione deve operare da gateway verso altro accesso e offrire funzionalità di routing (e.g. IP)**

Infrastructure mode

- Modalità di rete infrastructure (Infrastructure mode)
  - **ogni stazione invia tutti i pacchetti/trame (frame) in uscita ad un unica stazione centrale chiamata AP (Access Point)**
  - **l'AP agisce come un bridge Ethernet**
    - rilancia tutti i pacchetti/trame (frame) sul ramo di rete wireless o wired opportuno dove si trova la stazione di destinazione
  - **la zona di rete così formata viene chiamata ESS (Extended Service Set)**



Ad-hoc and Infrastructure modes



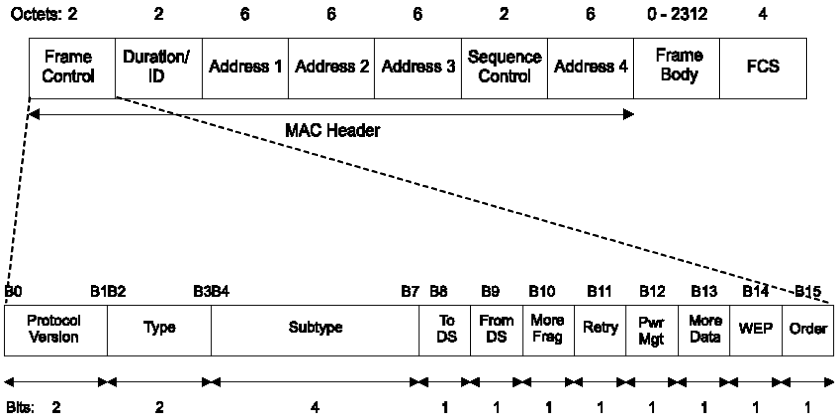
802.11 MAC Layer

- Il sottostrato MAC (Medium Access Control) implementa
  - **procedure di channel allocation**
  - **frame formatting**
  - **MAC-PDU addressing**
  - **error checking**
  - **fragmentation e reassembly**
- Il MAC del IEEE 802.11 è basato su una tecnica di accesso denominata CSMA/CA (Carrier Sense Medium Access with Collision Avoidance)
- Il mezzo fisico può opera in due differenti modalità:
  - **Contention Period (CP) mode**
  - **Contention-Free Period (CFP) mode**
    - Durante il CFP l'accesso al mezzo è controllato direttamente dal AP (vedi PCF più avanti)
- Tre tipi di trame (frame)
  - **management, control, data**

802.11 MAC Layer

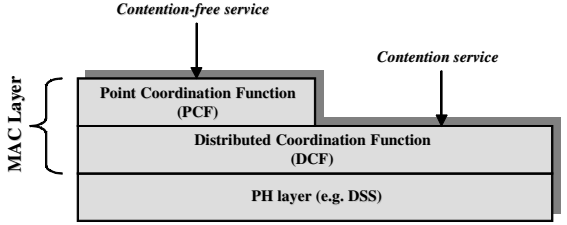
- Trame di Management sono usate per:
  - **association/disassociation con un AP**
  - **timing e synchronization**
  - **authentication**
- Trame di Controllo sono usate per:
  - **handshaking durtante CP**
  - **acknowledgment positivi durante un CP**
  - **per chiudere un CFP**
- Trame Data sono usate per:
  - **trasmettere dati durante un CP o un CFP, e possono essere combinate con trame di polling o acknowledgment**

MAC-PDU format



802.11 MAC Layer

- Sono previste due differenti tipi di modalità di funzionamento per il MAC (spesso legate al fatto che si lavori in modalità ad-hoc o infrastructure):
  - **Distributed Coordination Function (DCF)**
    - sempre utilizzata nelle configurazioni di rete ad-hoc (IBSS), ma può essere usata anche in configurazione infrastructure (con AP)
    - il mezzo lavora solo in CP
  - **Point Coordination Function (PCF)**
    - può essere utilizzata solo se è presente un AP, cioè in ESS



Distributed Coordination Function (DCF)

- Metodo di accesso fondamentale (deve essere sempre supportato) in grado di supportare modalità di trasferimento asincrono
  - **unico metodo di accesso possibile nel caso di modalità ad-hoc**
- DCF è una tecnica di accesso distribuita con collisioni e utilizza il CSMA/CA (Carrier Sense Multiple Access with collision Avoidance)
  - **collision detection (CSMA/CD) di Ethernet non può essere usato per l'impossibilità di trasmettere e contemporaneamente ascoltare lo stesso canale**
  - ***carrier sense* è realizzato sia a livello PH (*PH carrier sensing*) che MAC (*virtual carrier sensing*)**
- Il *virtual carrier sensing* è realizzato inviando informazioni sulla durata temporale di una trasmissione, all'interno dell'intestazione delle trame (MAC-PDU) di *request to send* (RTS), *clear to send* (CTS), e dati (vedi più avanti)

DCF (cont.)

- Il campo *duration* di una MAC-PDU indica il tempo (µs) che il canale sarà occupato dopo l'invio della trama corrente
- Le stazioni all'interno dello stesso BSS usano questa informazione per aggiornare il proprio "network allocation vector" (NAV) che indica la durata di tempo che il canale deve essere considerato occupato
- La priorità di accesso al canale dopo un periodo di occupato è controllato da un *interframe space* (IFS) variabile a seconda del tipo di trama che si vuole inviare
- Sono definiti tre tipi di IFS:
  - **short IDS (SIFS)**
  - **point coordination function IFS (PIFS)**
  - **distributed coordination function IFS (DIFS)**

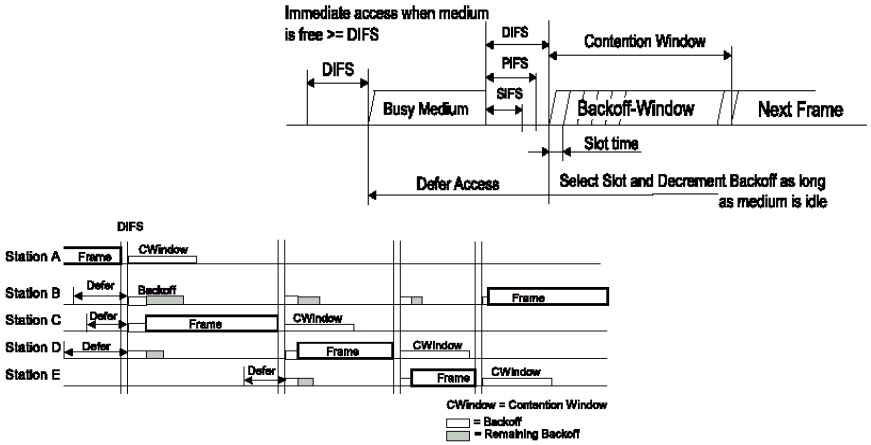
DCF (cont.)

- Stazioni che devono aspettare solo un SIFS hanno priorità di accesso rispetto a quelle che devono attendere un PIFS o DIFS
- Nella modalità di accesso base una stazione che riscontra il canale libero (fisicamente o virtualmente), aspetta un DIFS prima di controllare di nuovo il canale
  - **se il canale è ancora libero allora può trasmettere una MAC-PDU**
- Il ricevitore una volta ricevuta una trama controlla il checksum e dopo un SIFS trasmette un ACK
- Il campo *duration* nelle trame dati include il SIFS e la durata del ACK

DCF (cont.)

- Poiché in questa modalità possono ancora accadere collisioni, prima di inviare una trama dati una stazione invia una trama di controllo di tipo Request To Send (RTS) che deve essere confermata dal ricevitore con una trama di Clear To Send (CTS)
- RTS e CTS sono trame di controllo molto corte (rispettivamente 20 e 14 bytes)
- Se avviene una collisione mentre si invia una trama RTS, il sender non riceve il corrispondente CTS, capisce che ce'è stata una collisione e inizia una procedura di ritrasmissione del RTS ritardata con tempo di subentro incrementato esponenzialmente (exponential-backoff)
- L'algoritmo MAC risultante è equo, ma non garantisce un limite superiore al ritardo di trasmissione

DCF (cont.)



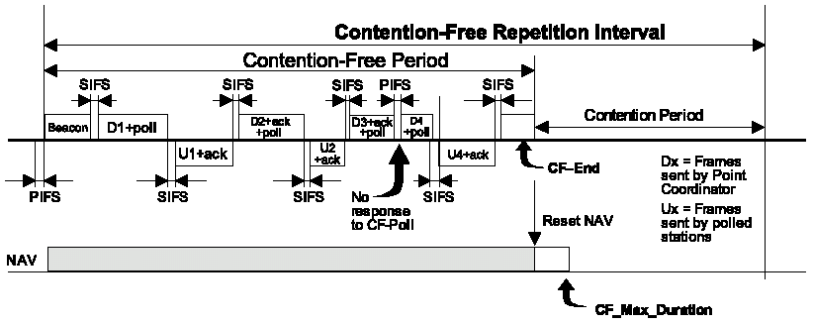
Point Coordination Function (PCF)

- PCF è una modalità di trasferimento opzionale (spesso non implementata) che garantisce un invio delle MAC-PDU senza collisioni
- PCF necessita di un AP (in ogni BSS), che periodicamente interroga le stazioni e le abilita alla trasmissione (senza competizione nell'accesso al mezzo)
- PCF deve poter coesistere con DCF
- L'asse dei tempi è diviso in intervalli di contention-free (CFP) alternati con intervalli di contention (CP)
- Durante un CFP non sono usate trame di RTS/CTS; è l'AP che indica alle singole stazioni (operazione di *poll*) quando possono iniziare a trasmettere

Point Coordination Function (PCF)

- All'istante di inizio nominale di un CFP l'AP ascolta il mezzo e, se libero, aspetta un PIFS e poi inizia il CFP con una trama di "beacon"
- Successivamente, possono essere inviate le seguenti trame:
  - **CF-Poll (no data): usata dal AP per interrogare una stazione**
  - **Data: usata per trasmettere dei dati (dopo una CF-Poll)**
  - **Data+CF-Poll: usata dal AP per trasmettere dati e per interrogare una stazione**
  - **CF-ACK: usata da una stazione per confermare la ricezione di una trama dati (dopo un SIFS)**
  - **Data+CF-ACK: combinazione di Data e CF-ACK**
  - **Data+CF-ACK+CF-Pool: combinazione di CF-ACK + Data + CF-Poll**
  - **Null (no data): usata da una stazione come risposta a una CF-Poll se non ha dati da trasmettere**
  - **CF-End: usata dal AP per terminare un CFP**

PCF (cont.)



Client-AP association

- Prima di iniziare a comunicare direttamente tra loro, due stazioni (e.g. un terminale e l'AP) devono stabilire una relazione denominata associazione
- Un terminale si riesce ad associare ad un AP nel seguente modo:
  - **tutti gli AP trasmettono periodicamente delle trame di management dette beacon**
  - **per associarsi ad un AP ed entrare così in un BSS, un terminale ascolta eventuali trame di beacon per identificare un eventuale AP**
  - **il terminale sceglie il BSS (tra vari possibili) in modi diversi, basati su preconfigurazione o su scelta dell'utente, ad esempio in base al nome della rete o SSID (Service Set ID) pubblicizzato**
  - **un terminale può anche inviare una trama di sollecitazione (trama di probe request management) specificando un particolare SSID richiesto**
  - **dopo aver identificato l'AP, il terminale inizia una procedura di mutua autenticazione utilizzando diverse trame di controllo**

Sicurezza nelle WLAN IEEE 802.11

- La protezione degli accessi e la sicurezza della comunicazione è un aspetto molto delicato nelle WLAN in quanto:
  - **la trasmissione avviene via etere esponendo i dati alla ricezione di utenti/stazioni non autorizzate**
    - è semplice ricevere il segnale delle WLAN
  - **poiché gli AP danno accesso alle stazioni wireless indipendentemente dalla loro posizione fisica, risulta moto più agevole introdursi all'interno di una rete**
- Lo standard originale IEEE 802.11 prevede alcuni meccanismi che possono essere utilizzati per tentare di proteggere la comunicazione
  - **Media Access Control (MAC) address filtering**
  - **Wired Equivalent Privacy (WEP)**
    - un protocollo di crittografia definito per lo standard originario IEEE 802.11, e in grado di garantire confidenzialità dei dati
    - ha come scopo quello di fornire una sicurezza simile a quella ottenibile tramite accesso wired
    - sfortunatamente è stato dimostrato essere assai debole e vulnerabile a vari tipi di attacchi

Tecnologie per la protezione delle WLAN

- Le debolezze dello standard originale vengono superate dai nuovi standard IEEE 802.11(x,i) e altre tecnologie:
  - **Standard IEEE 802.1x, WPA**
    - filtraggio dei pacchetti non autorizzati, utilizzo di server di autenticazione, miglioramenti dell'algoritmo di cifratura
  - **Standard IEEE 802.11i, WPA2**
    - sostituzione del WEP con nuovo algoritmo di cifratura AES
  - **WPN IPSec**
    - sicurezza fornita a livello IP
  - **Captive portal**
    - filtraggio, autenticazione fornita a livello applicativo tramite browser
- La scelta della particolare tecnologia da usare dipende da vari fattori come
  - **scenario di utilizzo (accesso pubblico, aziendale, o residenziale)**
  - **tipologia dei terminale e applicativi**
  - **livello di sicurezza richiesto**