

Guida alle reti WIRELESS LAN

appunti tratti da:

- ◆ Garattini, Randazzo, Righi "Guida alle reti LAN"
- ◆ Giordano, Puiatti "Technologies for mobile and wireless networking"
- ◆ ... e altri ...

Alessandro Memo

Sommario

1. Tecnologia delle onde radio
2. Terminologia e architetture
3. Standard 802.11
4. 802.11: livelli fisici
5. 802.11: livello MAC
6. Sicurezza
7. Bluetooth (*cenni*)

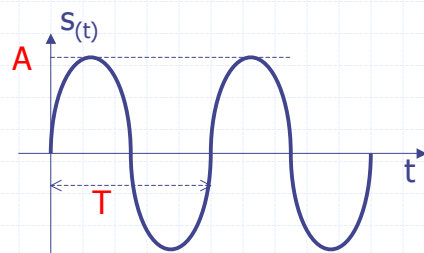
1. Tecnologia delle onde radio

- ◆ Frequenze e canali
- ◆ Normativa
- ◆ Spettro distribuito

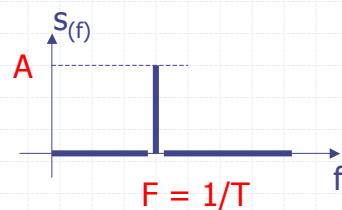
Frequenze e canali (1)

il campo elettromagnetico

la rappresentazione dei
segnali nel dominio
spazio/tempo

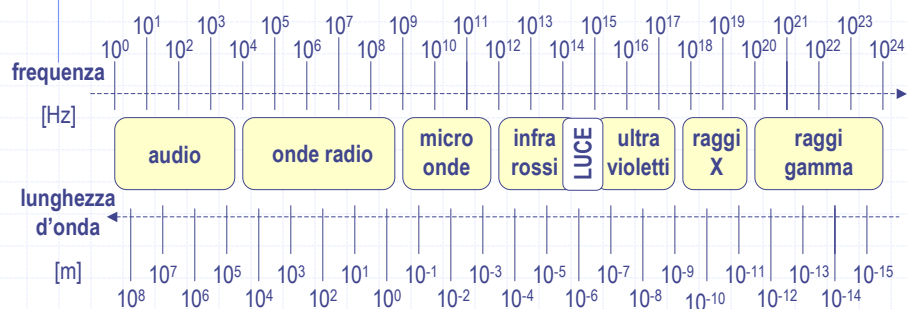


la rappresentazione dei
segnali nel dominio della
frequenza



Frequenze e canali (2)

i concetti di canale, frequenza centrale, banda, spettro



Frequenze e canali (3)

- ◆ caratterizzate da frequenza f e lunghezza d'onda λ [$c = 299.792.458$ m/sec]

$$f \cdot \lambda = c$$

- ◆ hanno una interazione differente con i vari materiali in base alla loro lunghezza d'onda

Normativa (1)

in Italia:

- ◆ il DPR 30/01/2002 ha modificato il rapporto precedente tra stato e cittadino, basato sulla **concessione**, passando a quello di **licenza individuale** e **autorizzazione globale** di servizi di telecomunicazione
- ◆ non più solo all'interno di un edificio di proprietà privata, ma anche all'interno del proprio fondo e di collegamento tra due siti (per ora dello stesso proprietario)

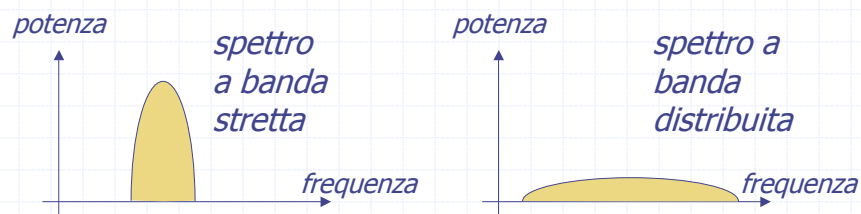
Normativa (2)

nel mondo:

- ◆ organismi (l'americano FCC e l'europeo ETSI)
- ◆ frequenze ISM (Industriale, Scientifico, Medicale): utilizzo senza licenza ma a potenza irradiata limitata ed in ambito locale
 - UHF ISM 902 - 928 MHz
 - **S-Band ISM 2,4 – 2,5 GHz** *[microonde e cell]*
 - **C-Band ISM 5,725 – 5,875 GHz** *[satelliti]*
- ◆ lo standard 802.11 divide la S-Band (2.412-2.484 MHz) in 14 canali

Spettro distribuito (1)

- ◆ le trasmissioni in banda ISM sono a **spettro distribuito** (*Spread Spectrum*)
- ◆ il trasmettitore distribuisce il segnale su un numero elevato di frequenza, al fine di ridurre l'effetto del rumore



Spettro distribuito (2)

- ◆ possibili tecniche di implementazione
 - **Frequency Hopping Spread Spectrum** (FH o FHSS) modulazione a spettro diffuso per salti di frequenza
 - **Direct Sequence Spread Spectrum** (DS o DSSS) modulazione a spettro diffuso per sequenza diretta
 - **Orthogonally Frequency Division Multiplexer** (OFDM) suddivide le informazioni tra più canali che le trasferiscono in parallelo

2. Terminologia ed architetture

- ◆ Glossario wireless LAN
- ◆ Architettura reti wireless
- ◆ Posizionamento WLAN
- ◆ Vantaggi e svantaggi delle reti WLAN

Glossario wireless LAN (1)

- ◆ **BSA**, *Basic Service Area*: ogni cella wireless
- ◆ **AP**, *Access Point*: interfaccia le aree wired-wireless della LAN, agisce come stazione base per ogni cella
- ◆ **STA**, *Station*: una postazione del BSA, detta anche WT, *Wireless Terminal*
- ◆ **DS**, *Distribution System*: interconnette più BSA
- ◆ **BSS**, *Basic Service Set*: il gruppo di stazioni che operano in un BSA
- ◆ **ESS**, *Extended Service Set*: un gruppo di BSS collegate ad una wired LAN tramite AP

Glossario wireless LAN (2)

ESS Extended Service Set

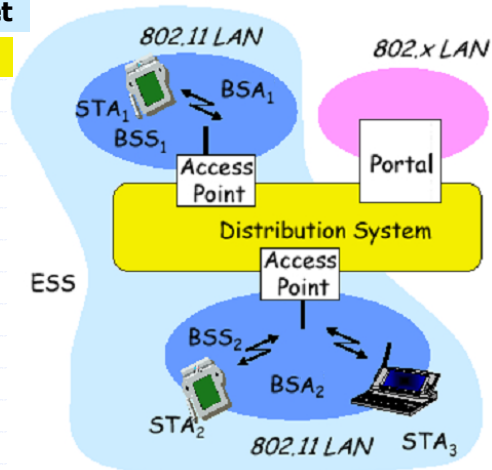
DS Distribution System

AP Access Point

BSS Basic Service Set

BSA Basic Service Area

STA Station



Glossario wireless LAN (3)

- ◆ **BSSID** e **ESSID**, campo dati che identifica un BSS o un ESS
- ◆ **Association**: una funzione che mappa una stazione nell'AP
- ◆ **MSDU**, *MAC Service Data Unit*: trama dati scambiata tra utente e livello MAC
- ◆ **MPDU**, *MAC Protocol Data Unit*: trama dati scambiata tra livello MAC e livello fisico
- ◆ **PLCP_PDU**, *PLCP Packet*: pacchetto di dati trasferito tra due livelli fisici tramite etere

Architettura wireless LAN (1)

- ◆ si basa su una struttura cellulare simile al GSM
- ◆ le reti wireless possono essere divise in
 - **AD HOC** LAN, stazioni in grado di comunicare direttamente tra loro senza Access Point (dette anche IBSS, da *Independent BSS* o *peer-to-peer*)
 - **INFRASTRUCTURED WIRELESS** LAN, stazioni che comunicano tra loro utilizzando uno o più *Access Point*, collegati da un *Distribution System*

Architettura wireless LAN (2)

compiti degli Access Point:

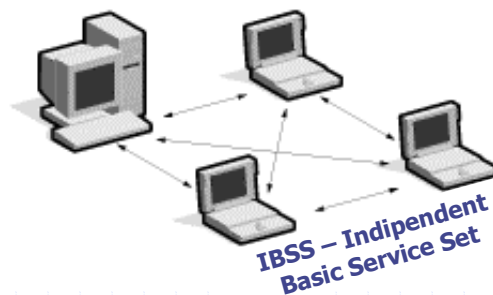
- ◆ collegamento tra rete wireless e rete cablata
- ◆ autenticazione, associazione e riassociazione (***roaming***)
- ◆ gestione del risparmio energetico delle stazioni (*Power Save Mode*)
- ◆ sincronizzazione, in modo che tutte le stazioni agganciate ad un AP siano agganciate ad un clock comune

Architettura wireless LAN (3)

- ◆ Inoltre gli Access Point possono svolgere funzioni di **bridging**
- ◆ ponte wireless tra due o più edifici/postazioni (collegamenti punto-punto o multipunto)
- ◆ distanze raggiungibili da 500 m a 10-15 Km purché siano a vista, tramite antenne direttive

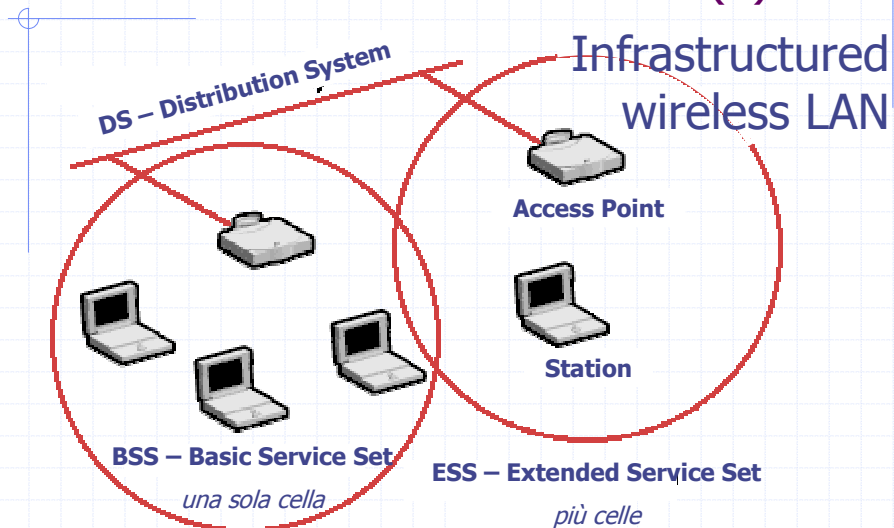
Architettura wireless LAN (4)

Ad Hoc wireless LAN



N.B.: gli host delle reti Ad Hoc devono svolgere anche funzioni di router (instradamento distribuito e dinamico)

Architettura wireless LAN (5)



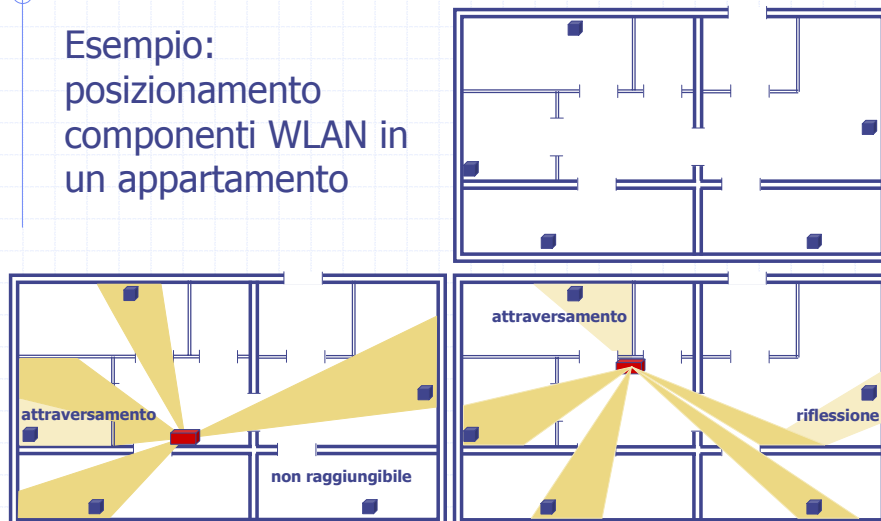
Posizionamento WLAN (1)

Elementi da considerare:

- ◆ Access Point baricentrico e a mezza altezza
- ◆ utenti allineati otticamente all'Access Point
- ◆ attenzione alle schermature metalliche
- ◆ analisi delle riflessioni
- ◆ analisi degli attraversamenti strutturali

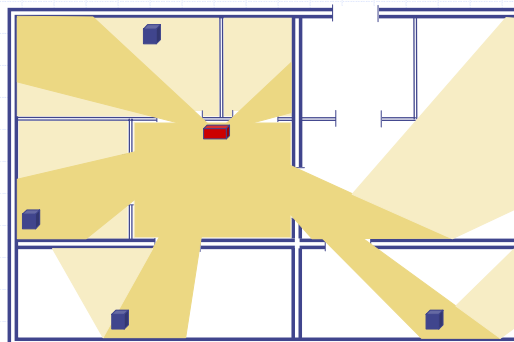
Posizionamento WLAN (2)

Esempio:
posizionamento
componenti WLAN in
un appartamento



Posizionamento WLAN (3)

calcolo
della
**copertura
totale**



area RAGGIUNGIBILE DIRETTAMENTE	37%
area RAGGIUNGIBILE con UN ATTRAVERSAMENTO	17%
area RAGGIUNGIBILE CON RIFLESSIONE	18%
area NON RAGGIUNGIBILE	28%

Posizionamento WLAN (4)

Con una dotazione minima di 1 AP e 2 WT si può analizzare il throughput in configurazione *Ad-Hoc* e *Infrastructured* al variare di

- ◆ distanza
- ◆ riflessione
- ◆ assorbimento
- ◆ presenza o meno di chiavi WEP (64 o 128 bit)
- ◆ aumento di WT connessi all'AP (in caso di rete *Infrastructured*)

Vantaggi delle reti WLAN

- ◆ costi e tempi della messa in opera
- ◆ non sensibile a degradazione e rottura dei media
- ◆ motivazioni di natura logistica
- ◆ facilità di riorganizzazione, reti temporanee
- ◆ mobilità
- ◆ scalabilità
- ◆ flessibilità

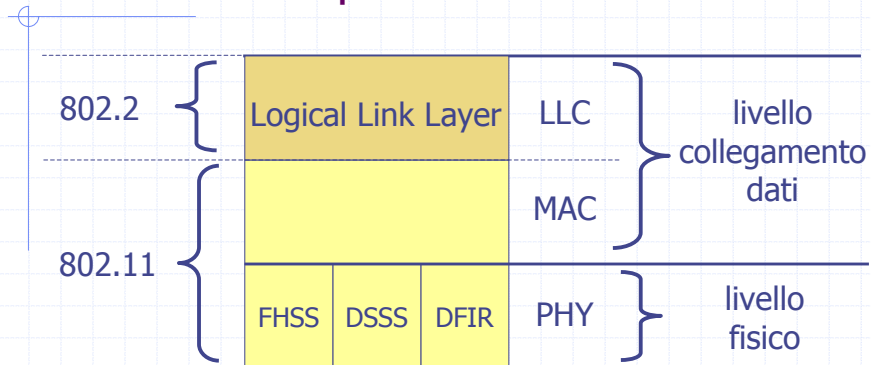
Svantaggi delle reti WLAN

- ◆ inaffidabilità del mezzo
- ◆ sicurezza
- ◆ gestione del roaming
- ◆ multipath fading in ricezione
- ◆ consumo energetico
- ◆ limitata estensione
- ◆ limitata standardizzazione
- ◆ inquinamento elettromagnetico

3. Standard 802.11

- ◆ Standard 802 per le reti LAN
- ◆ Evoluzione dell'802.11

Standard 802 per le reti LAN



802 generalità ed architettura
 802.1 gestione
 802.2 Logical Link Control e Bridging
 802.10 sicurezza

Evoluzione dell'802.11 (1)

802.11 approvato nel 1997, revisionato nel 1999
 banda da 2,400 a 2,500 GHz, da 1 a 2 Mbps
nel '99 si è evoluto in due rami

802.11a rilasciato nel 1999, PHY per WLAN a 5,200 GHz, fino a 54 Mbps

802.11b approvato nel 1999, PHY più veloce, da 5,5 ad 11 Mbps

802.11g rilasciato nel 2002, PHY per WLAN a 2,400 GHz, a 54 Mbps

Evoluzione dell'802.11 (2)

Specification	Connection Speed	Radio Frequency
802.11	1 or 2 Mbps	2.4 GHz
802.11a	Up to 54 Mbps	5 GHz
802.11b	5.5 and 11 Mbps	2.4 GHz WiFi
802.11g	Up to 54 Mbps	2.4 GHz

4. 802.11: livelli fisici

- ◆ Livelli fisici delle reti wireless
- ◆ Frequency Hopping SS
- ◆ FHSS in 802.11
- ◆ Direct Sequence SS
- ◆ DSSS in 802.11
- ◆ DSSS: suddivisione dei canali
- ◆ 802.11b – HR DSSS
- ◆ 802.11a – OFDM
- ◆ 802.11g – Physical layer extensions
- ◆ Infrarossi

Livelli fisici delle reti wireless (1)

Tutti gli standard utilizzano lo stesso livello MAC, ma hanno diversi livelli fisici:

802.11	modulazioni FHSS, DSSS, DFIR; data rate 1 o 2 Mbps distanza max=150m
802.11b	High Rate DSSS (HRDSSS), data rate fino a 11 Mbps
802.11a	OFDM, data rate fino a 54 Mbps, copertura di 30 m (a 54 Mbps)

Livelli fisici delle reti wireless (2)

L'802.11 analizza il livello fisico e quello MAC, e garantisce flussi da 1 o 2 Mbps tra distanze da 20 a 70 metri.

L'unico livello MAC può interagire con 3 livelli fisici operanti a velocità diverse:

- ◆ **Frequency Hopping Spread Spectrum (FHSS)**
- ◆ **Direct Sequence Spread Spectrum (DSSS)**
- ◆ trasmissione **infrarossi** (DFIR)

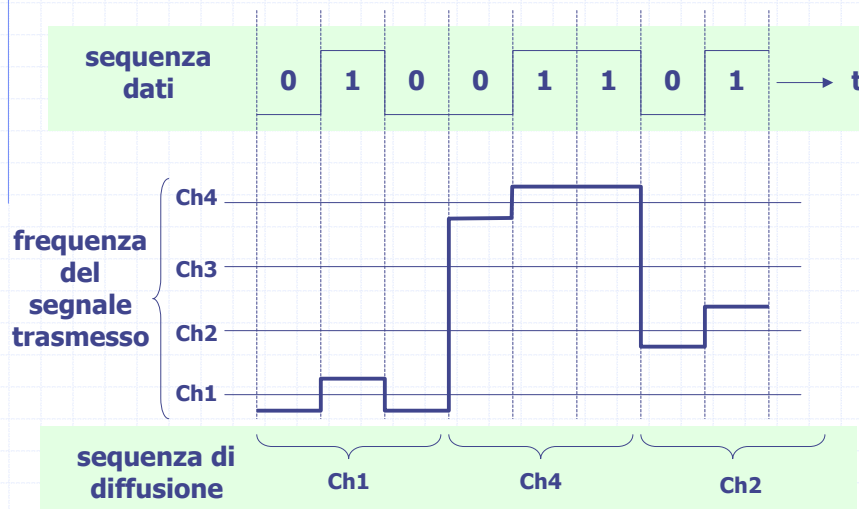
Frequency Hopping SS (1)

- ◆ salta di frequenza secondo un modello pseudocasuale
- ◆ si utilizza un range di frequenze sui 2,4 GHz distanziate tra loro di 1 MHz
- ◆ un codice numerico (*Hopping Code*) determina le frequenze ed il loro ordine
- ◆ la frequenza cambia al massimo ogni 400 mS (*dwell time*) e fino al massimo di 1.600 volte al sec

Frequency Hopping SS (2)

- ◆ se uno slot (frequenza) è disturbato, il TX ritrasmette il segnale allo slot successivo
- ◆ si trasferiscono al massimo 2 Mbps
- ◆ si possono avere più comunicazioni contemporaneamente purché l'**hopping pattern** sia compatibile (pattern ortogonali)

Frequency Hopping SS (3)



Frequency Hopping SS (4)

- ◆ gli *Hopping Code* sono raggruppati in 3 set che contengono 26 sequenze ortogonali
- ◆ una BSS utilizza uno di questi set
- ◆ la rete invia periodicamente trame di gestione (**Beacon Frame**) contenenti
 - un *timestamp* per la sincronizzazione
 - un parametro (*FH*) contenente l'Hopping Code e il valore del prossimo canale da utilizzare
- ◆ in tal modo le nuove stazioni sapere quale sarà il prossimo canale utilizzato

Frequency Hopping SS (5)

Caratteristiche generali di FHSS:

- ◆ Basso costo
- ◆ Basso consumo energetico
- ◆ Tolleranza alle interferenze
- ◆ Necessità di sincronizzazione
- ◆ Bassa velocità su singolo canale
- ◆ Alta velocità tramite aggregazione di canali

Frequency Hopping SS (6)

area geografica	frequenza minima	frequenza massima	range frequenze
Nord America ed Europa	2,402 GHz	2,480 GHz	2,400 ~ 2,435
Giappone	2,473 GHz	2,495 GHz	2,471 ~ 2,497
Spagna	2,417 GHz	2,473 GHz	2,445 ~ 2,475
Francia	2,448 GHz	2,482 GHz	2,4465 ~ 2,4835

FHSS in IEEE 802.11 (1)

- ◆ si utilizzano 79 canali con una banda da 1 MHz
- ◆ il *dwell time* vale 390 mS e ogni salto di frequenza richiede 224 μ S
- ◆ la sequenza di canali è data dalla

$$F_{x(i)} = [b_{(i)} + x] \bmod (79) + 2$$

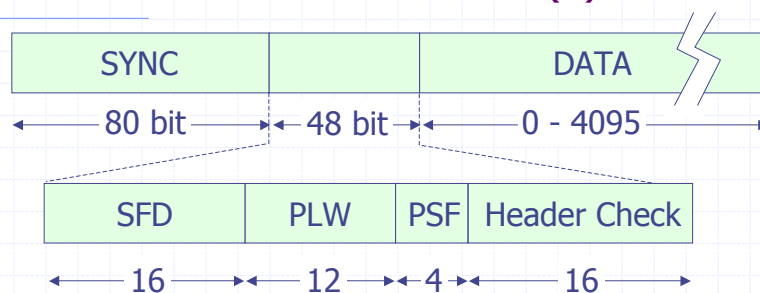
$F_{x(i)}$ è l'*i*-esimo canale utilizzato

$b_{(i)}$ è l'*i*-esimo numero di una sequenza pseudocasuale data di interi tra 1 e 79

x è l'*Hopping Code* (compreso tra 1 e 78)

- TECNICA OBSOLETA, ORA SCARSAMENTE UTILIZZATA -

FHSS in IEEE 802.11 (2)



SYNC sincronizzazione (80 bit = 0101..01) ad 1 Mbps

SFD Start Frame Delimiter (0x0CBB)

PLW PSDY Length Word

PSF PLCP Signaling Frame, data rate

HC CRC-16 (tutti i singoli e i doppi = 99,998%)

DATA da 0 a 4095 Byte, con scrambling e char insertion (1 su 4)

Direct Sequence SS (1)

- ◆ L'espansione dello spettro si ottiene moltiplicando il bit di segnale con una sequenza di bit **PN**, *Pseudorandom Noise*, o *chipping code* (almeno 10 bit)

bit di dato : 0

sequenza PN : 10110111000

segnale trasmesso:

0 0 0 1 1 1 0 1 1 0 1

bit di dato : 1

sequenza PN : 10110111000

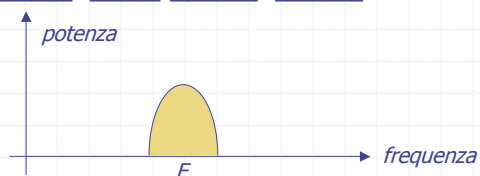
segnale trasmesso:

1 0 1 1 0 1 1 1 0 0 0

Direct Sequence SS (2)

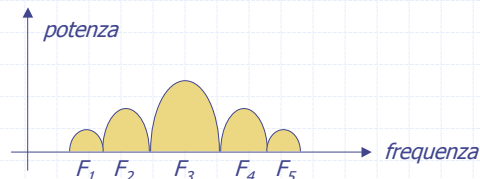
dati trasferiti : 1 0

spettro tipico:



dati codificati : 10110111000 00011101101

spettro tipico:



Direct Sequence SS (3)

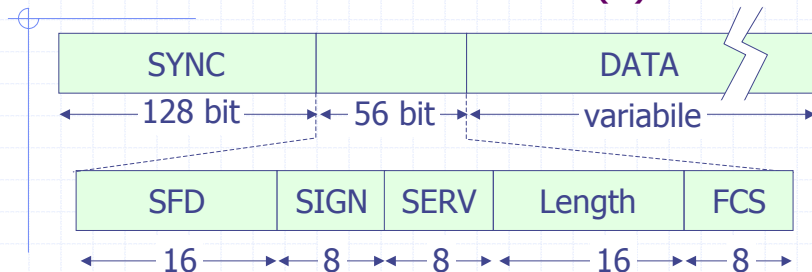
Caratteristiche generali di DSSS:

- ◆ Viene utilizzata la stessa frequenza diretta in trasmissione ed in ricezione
- ◆ Costo elevato
- ◆ Alto consumo energetico (maggiore potenza di trasmissione)
- ◆ Tolleranza alle interferenze ed alle riflessioni (superiore alla FHSS)
- ◆ Maggiore copertura ed alta velocità
- ◆ Scarsa possibilità di aggregazione

DSSS in IEEE 802.11 (1)

- ◆ modulazione DBPSK, Differential Binary Phase Shift Keying con rate di 1 Mbps
- ◆ modulazione DQPSK, Differential Quadrature Phase Shift Keying con rate di 2 Mbps
- ◆ preambolo ed header ad 1 Mbps
- ◆ chipping sequence (Barker code) = +1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1
- ◆ potenza irradiata:
min. 1 mW, max. 100 mW (EU), 1 W (USA)

DSSS in IEEE 802.11 (2)

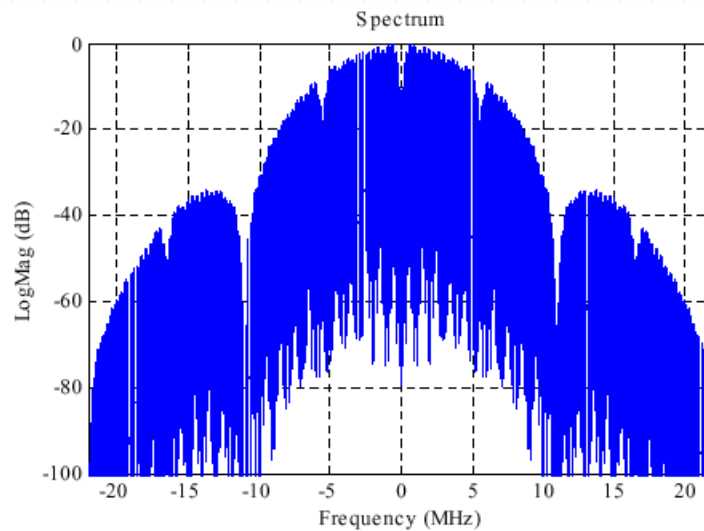


SYNC sincronizzazione (128 bit = 0101..01) ad 1 Mbps
SFD Start Frame Delimiter (0x0CBB)
SIGN tipo di modulazione (1 o 2 Mbps)
SERV per sviluppi futuri
Length durata in microsecondi trasmissione del campo dati
FCS Frame Check Sequence, con CRC-16
DATA campo dati

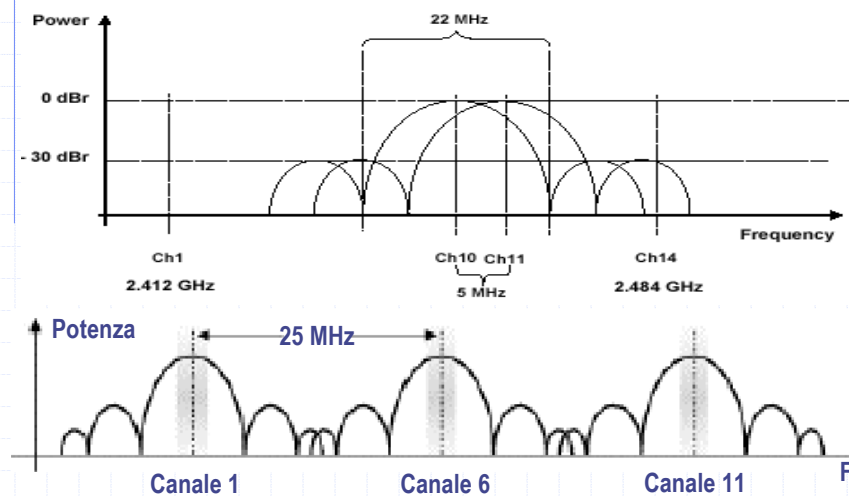
DSSS in IEEE 802.11 (3)

- ◆ dato un chipping code di 11 bit, con 1 MHz di dati si ottiene un segnale da 11 MHz
- ◆ la banda disponibile (2,4 – 2,5 GHz) è divisa in 14 canali (11 in USA) da 22 MHz
- ◆ la portante di ogni canale dista 5 MHz da quelle adiacenti
- ◆ la maggior parte dell'energia trasmessa occupa una banda di 22 MHz (a -30 dB)

DSSS: suddivisione dei canali (1)



DSSS: suddivisione dei canali (2)



DSSS: suddivisione dei canali (3)

- ◆ è possibile trasmettere più segnali DSSS nella stessa area, purché su canali diversi separati da più di 30 MHz
- ◆ quindi si possono accavallare fino a 3 BSA
- ◆ per prevenire interferenze conviene avere celle adiacenti con canali spazati almeno 25 MHz (ad es. canali 1, 6 e 11) o meglio 30 MHz (ad es. canali 1, 7 e 14)

DSSS: suddivisione dei canali (4)

Canali permessi

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
USA	X	X	X	X	X	X	X	X	X	X	X			
Canada	X	X	X	X	X	X	X	X	X	X	X			
EUROPA (...)	X	X	X	X	X	X	X	X	X	X	X	X	X	
Francia										X	X			
Spagna										X	X			
Giappone														X

CANALE DI DEFAULT = 11 (per le reti AD HOC = 10)

Confronto tra FHSS e DSSS

- ◆ alta potenza su piccola banda
- ◆ la frequenza cambia molto rapidamente
- ◆ grande resistenza alle interferenze
- ◆ velocità massima di 2 Mbps
- ◆ bassa potenza su ampia banda
- ◆ frequenze usate costanti
- ◆ bassa resistenza alle interferenze
- ◆ velocità massima di 5 Mbps

802.11b – HR DSSS (1)

- ◆ nel 1997 si passa dall'802.11 all'802.11b, di cui rimane compatibile
- ◆ successivamente denominato WiFi
- ◆ throughput più elevato: 5.5 e 11 Mbps (1 e 2 Mbps per compatibilità)
- ◆ varia la velocità per adeguarsi al canale
- ◆ cambia automaticamente banda e AP in base alla qualità del segnale

802.11b – HR DSSS (2)

- ◆ roaming del tutto trasparente
- ◆ introduce la tecnologia **WEP** (Wired Equivalent Protocol) per la sicurezza
- ◆ per aumentare il data rate, invece di utilizzare chipping sequence da 11 bit, adotta la codifica **CCK**, *Complementary Code Keying*, basata su 64 parole da 8 bit

802.11b – HR DSSS (3)

usa la stessa trama del DSSS, eccetto:

- ◆ SYNC più breve, per diminuire l'overhead
- ◆ il campo SIGN specifica il tipo di modulazione, che ora può essere 1, 2, 5.5 e 11 Mbps
- ◆ SERV contiene indicazioni sulla modulazione

802.11b – HR DSSS (4)

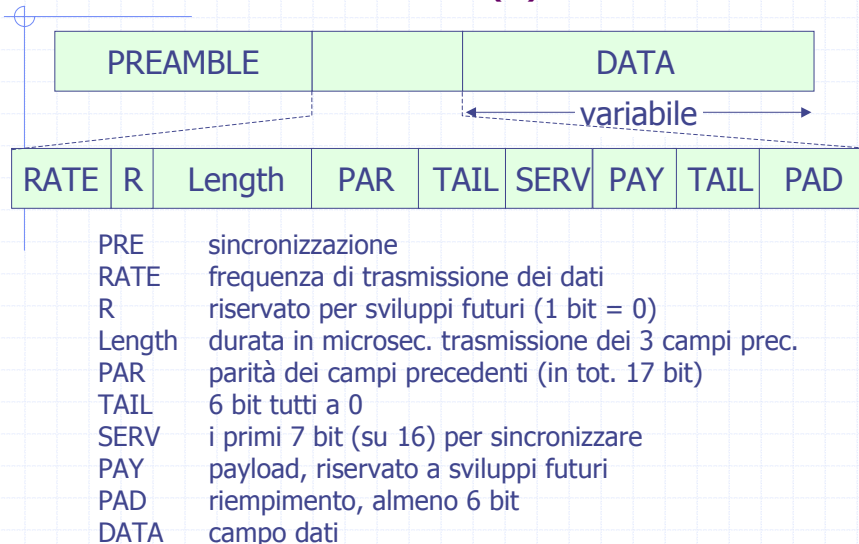
Specifiche dello standard 802.11b

data rate	code length	modulation	symbol rate	bits per symbol
1 Mbps	11 (Barker sequence)	BPSK	1 Msps	1
2 Mbps	11 (Barker sequence)	QPSK	1 Msps	2
5,5 Mbps	8 (CCK)	QPSK	1,375 Msps	4
11 Mbps	8 (CCK)	QPSK	1,375 Msps	8

802.11a – OFDM (1)

- ◆ **Orthogonal Frequency Division Multiplexing**
- ◆ ripartisce le informazioni da trasmettere ad alta velocità in più segnali da trasmettere a bassa velocità in parallelo su altrettanti canali
- ◆ ha un'alta efficienza spettrale, alta resistenza alle interferenze, bassa distorsione
- ◆ 802.11a utilizza la banda a 5 GHz, e trasferisce un data rate fino a 54 Mbps

802.11a – OFDM (2)



802.11g – Physical layer extensions

- ◆ compatibile con 802.11 ed 802.11b
- ◆ opera sulla banda dei 2,4 GHz
- ◆ data rate fino a 54 Mbps
- ◆ modulazione OFDM
- ◆ codifica CCK

Infrarossi

- ◆ lunghezza d'onda tra 850 e 950 nm
- ◆ luce diffusa
- ◆ distanza massima di 10 m
- ◆ solo per uso interno
- ◆ migliora la sicurezza, dato che diminuiscono le possibilità di intrusione
- ◆ banda più ampia $\Rightarrow$ maggiori prestazioni
- ◆ una minore copertura e mobilità
- ◆ normalmente sfrutta la riflessione del soffitto

5. 802.11: livello MAC

- ◆ 802.11: Livello MAC e DCF
- ◆ MAC: condivisione del mezzo
- ◆ 802.11: Livello MAC e PCF
- ◆ 802.11: trama MAC
- ◆ 802.11: frammentazione
- ◆ 802.11: gestione del MAC

802.11: livello MAC e DCF (1)

- ◆ nel wireless (802.11) la condivisione del mezzo avviene in maniera diversa da Ethernet (802.3)
- ◆ in radio non è possibile ascoltare quello che si trasmette dato che l'antenna è unica
- ◆ invece di CSMA/CD si ricorre al **CSMA/CA** (*Collision Avoidance*) o **DCF** (*Distributed Coordination Function*)
- ◆ questo protocollo prevede un riscontro (ACK) ad ogni trama
- ◆ determina un consumo di circa il 50% della banda disponibile

802.11: livello MAC e DCF (2)

- ◆ la priorità nell'802.11 viene implementata modificando gli intervalli di tempo IFS, *InterFrame Space*, tra una trama e la successiva
 - **SIFS**, Short IFS (priorità elevata)
 - **PIFS**, PCF IFS, pacchetti con gestione PCF
 - **DIFS**, DCF IFS, intervallo con gestione DCF
 - **EIFS**, Extended IFS, minimo intervallo di ritrasmissione per FCS errato
- $SIFS < PIFS < DIFS < EIFS$

802.11: livello MAC e DCF (3)

- ◆ per evitare le collisioni non è sufficiente il CSMA/CA
- ◆ si adotta anche una pausa di un *backoff counter* prima di ogni trasmissione
- ◆ ad ogni collisione il *backoff counter* viene incrementato
- ◆ il *backoff counter* viene usato come indice in uno schema di **Binary Exponential Backoff**

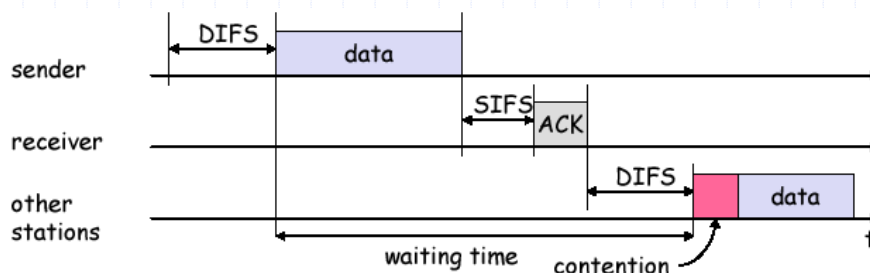
802.11: livello MAC e DCF (4)

Quando una stazione deve trasmettere:

- ◆ controlla se nell'etere ci sono trasmissioni
- ◆ se l'etere rimane libero per un IFS, la stazione inizia a trasmettere
- ◆ se l'etere è occupato, aspetta il primo intervallo IFS libero, e poi aspetta un ulteriore intervallo casuale di *backoff*
- ◆ se una stazione occupa l'etere durante un intervallo di *backoff*, il contatore viene azzerato

802.11: livello MAC e DCF (5)

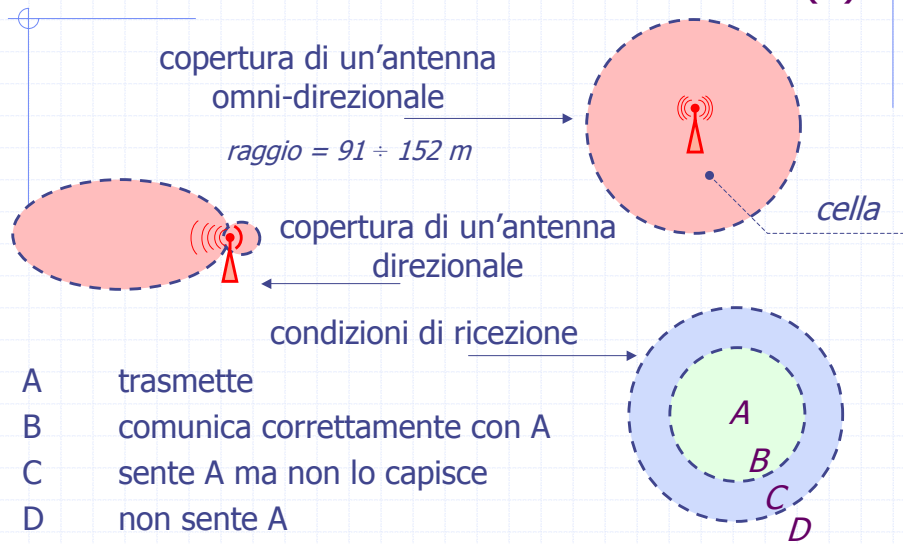
- ◆ la stazione TX aspetta un DIFS libero e poi invia i dati
- ◆ La stazione RX, se i dati ricevuti sono corretti, aspetta un SIFS e poi invia il riscontro ACK



802.11: livello MAC e DCF (6)

- ◆ se durante un intervallo IFS non si sentono trasmissioni si suppone che il canale sia libero
- ◆ ma questa assunzione può essere fatta anche da altre stazioni, determinando collisione
- ◆ quando c'è una collisione, non potendo ascoltare contemporaneamente il canale, si deve aspettare la ricezione dell'ACK per individuarla

MAC: condivisione del mezzo (1)



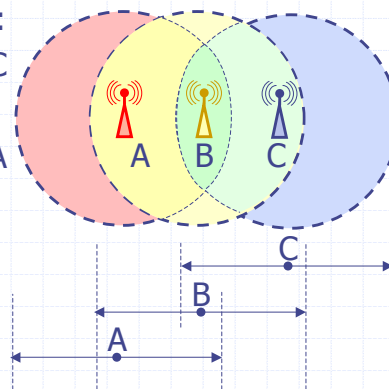
MAC: condivisione del mezzo (2)

il problema del **nodo nascosto**:

- ♦ A parla con B, ma non con C
- ♦ B parla con A e C
- ♦ C parla con B, ma non con A

possibile collisione:

- ♦ A inizia a parlare con B
- ♦ C non sente A, e quindi si mette a parlare con B



A e C hanno un'alta probabilità di collidere

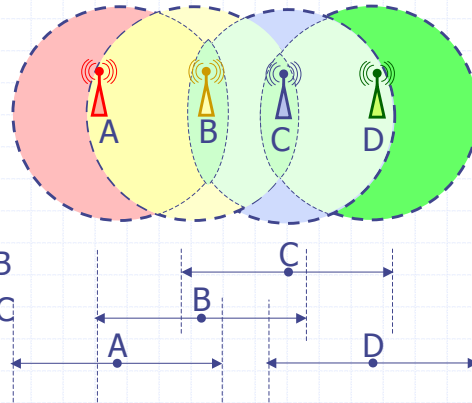
MAC: condivisione del mezzo (3)

il problema del **nodo esposto**:

- ♦ A parla solo con B
- ♦ B parla con A e C
- ♦ C parla con B e D
- ♦ D parla solo con C

possibile collisione:

- ♦ A inizia a parlare con B
- ♦ D inizia a parlare con C
- ♦ B e C non possono rispondere



B e C hanno un'alta probabilità di collidere

MAC: condivisione del mezzo (4)

- ♦ per ridurre ulteriormente le collisioni si adotta un meccanismo di prenotazione basato su RTS-CTS (Request To Send - Clear To Send)
- ♦ dopo il DIFS iniziale, il mittente (client) invia un RTS (in un suo campo è specificato il tempo **NAV**, *Network Allocation Vector*, di durata dell'intera trasmissione dei dati)
- ♦ dopo un SIFS, il destinatario (server o l'AP) risponde con un CTS con il suo NAV ricalcolato; questo CTS viene sentito da tutti, e quindi inibisce la loro trasmissione per il tempo NAV
- ♦ dopo un SIFS il mittente invia i dati

802.11: livello MAC e PCF (1)

In alternativa al metodo DCF si può usare:

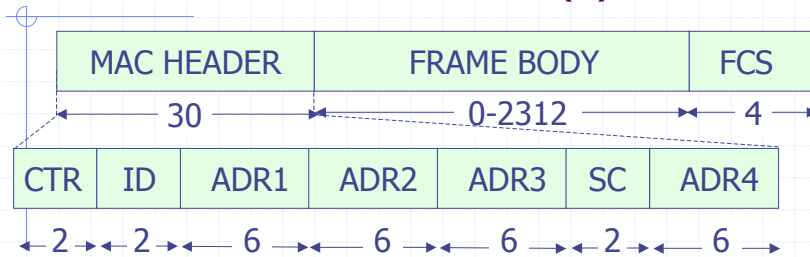
- ♦ **PCF**, *Point Coordination Function*, accesso a controllo centralizzato gestito mediante priorità, compatibile CSMA/CA, *contention free*
- ♦ viene utilizzato nel caso si richieda una continuità di servizio (audio e video)

P.S.: DCF e PCF possono funzionare contemporaneamente in un unico BSS per alternare periodi di contesa ad altri senza contesa.

802.11: livello MAC e PCF (2)

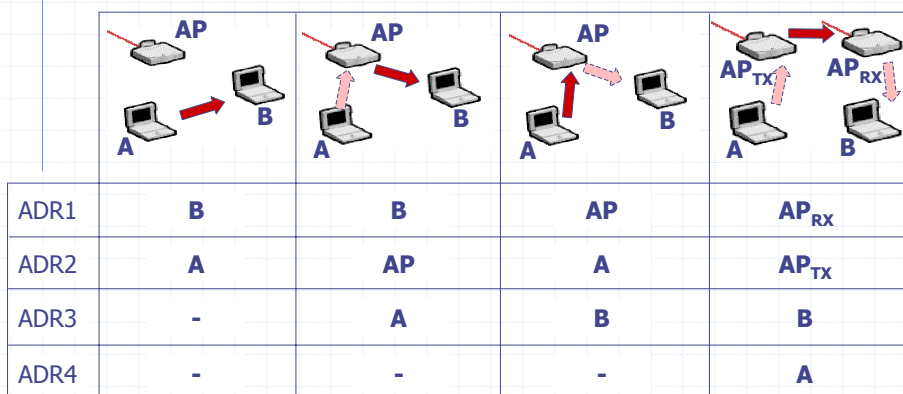
- ◆ l'AP (detto anche *Point Coordinator*) gestisce lo scambio di informazioni
- ◆ se il PCF è abilitato, si alternano fasi di gestione DCF (*contention*) a fasi PCF (*contention free*)
- ◆ nelle fasi PCF, l'AP fa il polling a tutte le stazioni e ne abilita l'eventuale trasmissione

802.11: trama MAC (1)



CTR FRAME CONTROL
 ID DURATION/ID: durata della trama (NAV)/ ID
 ADR1 SOURCE ADDR. (mittente)
 ADR2 DESTINATION ADDR. (destinatario)
 ADR3 TRANSMITTING STATION ADDR. (trasmettitore WM)
 SC SEQUENCE CONTROL (Sequence + Fragment num.)
 ADR4 RECEIVING STATION ADDR. (ricevitore WM)

802.11: trama MAC (2)



802.11: Frammentazione

Nel Wireless conviene usare pacchetti piccoli.

Detta **BER**, *Bit Error Rate*, la probabilità di errore

- ◆ il livello MAC riceve dagli utenti un pacchetto (MSDU) e lo suddivide in MPDU più piccole, numerandole e passandole poi al livello fisico
 - ◆ in tal modo diminuisce il BER
 - ◆ aumenta la distanza massima raggiungibile
 - ◆ diminuisce l'effetto delle collisioni

802.11: gestione del MAC (1)

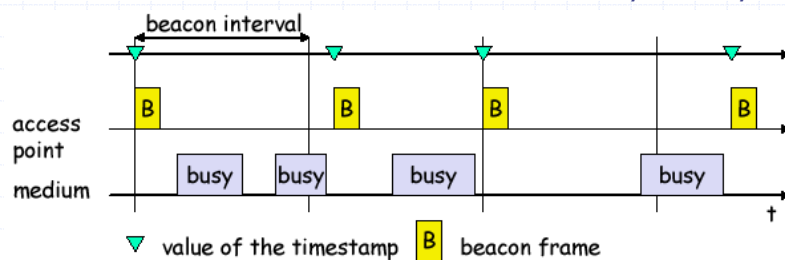
Il livello MAC deve garantire 4 funzionalità base:

- ◆ sincronizzazione
- ◆ consumo energetico
- ◆ roaming (appartenenza e rilascio da una WLAN)
- ◆ scanning
- ◆ gestione dei parametri d'informazione

802.11: gestione del MAC (2)

◆ Sincronizzazione

- cerca di trovare una LAN
- cerca di rimanere in una LAN
- generazione dei segnali beacon
- sincronizzazione dei clock locali, timer, ...



802.11: gestione del MAC (3)

◆ Consumo energetico

- spegnere il TX quando non necessario
- memorizzare lo stato (sleep & awake)
- nei beacon, l'AP inserisce anche una lista dei pacchetti persi da stazioni che erano in sleep
- quando le stazioni si risvegliano, avvisano l'AP e ricevono i dati bufferizzati

802.11: gestione del MAC (4)

- ◆ Roaming: spostarsi di cella in cella mantenendo la connessione
- ◆ gestisce 3 tipi di roaming:
 - **No-transition**
 - si muovono all'interno di una BSS
 - **BSS-transition**
 - da una BSS ad un'altra BSS, entro una ESS
 - **ESS-transition**
 - da una BSS di una ESS ad una BSS di un'altra ESS
- ◆ non è possibile fare roaming tra ESS diverse

802.11: gestione del MAC (5)

- ◆ Scanning: all'accensione una stazione, questa cerca di collegarsi ad un'altra stazione o ad un AP, e ne riceve l'SSID
- ◆ ci sono 2 tipi di scanning:
 - **Passive scanning**
 - la stazione ascolta, in attesa di un beacon
 - **Active scanning**
 - la stazione invia una richiesta di connessione ed aspetta una risposta di accettazione

6. La Sicurezza

- ◆ 802.11: Livello MAC e DCF
- ◆ MAC: condivisione del mezzo
- ◆ 802.11: Livello MAC e PCF

La Sicurezza (1)

- ◆ sistema intrinsecamente insicuro
- ◆ le onde radio possono attraversare i limiti fisici ambientali ed essere intercettate

La Sicurezza (2)

Tecniche di protezione:

- ◆ sicurezza fisica (*limitazione del campo*)
- ◆ disabilitazione del DHCP
- ◆ Access Point con indirizzo dinamico
- ◆ autenticazione dell'accesso
- ◆ controllo dell'accesso ai dati
- ◆ riservatezza dei dati accessibili

La Sicurezza (3)

Protocolli utilizzabili:

SSID – Service Set Identifier

- ◆ etichetta identificativa della rete
- ◆ comune a tutti i dispositivi di una WLAN

WEP – Wired Equivalent Privacy

- ◆ chiave di codifica dei dati in trasmissione
lunga 64 o 128 bit (40 o 104 + *Initial Vector*)
- ◆ schema di crittografia a chiave simmetrica

La Sicurezza (4)

Metodi di protezione standard:

- ◆ ad autenticazione aperta
 - ◆ *basata solo sul codice **SSID** della rete*
- ◆ ad autenticazione con chiave condivisa
 - ◆ *richiede una **WEP***
 - ◆ *l'Access Point invia un pacchetto di testo al client*
 - ◆ *il client lo codifica con la sua chiave e lo invia all'AP*
 - ◆ *l'AP decide se la codifica è corretta oppure no*
 - ◆ *alcuni usano il MAC address del client come chiave (devono essere inseriti manualmente nell'AP)*

La Sicurezza (5)

- ◆ per accrescere il livello di sicurezza, si possono accettare collegamenti solo tramite verifica del MAC address
- ◆ ulteriori standard di sicurezza sono in fase di perfezionamento (802.11i)

La Sicurezza (6)

- ◆ ci sono pareri discordanti sull'influenza dei campi elettromagnetici nell'uomo
- ◆ l'A.P. di norma non è classificabile come dannoso (installazione distante dall'uomo, consigliata almeno di 3 m)
- ◆ la vera fonte *'pericolosa'* è la scheda dell'WT (si pensi ad un laboratorio wireless)
- ◆ un cellulare ha una potenza **30 volte** maggiore di un A.P.

7. Bluetooth (1)

Rete che permette il trasferimento di informazioni senza cavi tra dispositivi adiacenti di piccole dimensioni



Bluetooth (2)

- ◆ operano nella banda dei **2,4 GHz**
(interferenze con 802.11x !!!)
- ◆ utilizza la tecnica FHSS
- ◆ throughput massimo di 1 Mbps
- ◆ utilizzano la tecnica TDD, *Time Division Duplex*
- ◆ potenze emesse divise per classe
 - classe 1 = 100 mW
 - classe 2 = 2,5 mW
 - classe 3 = 1 mW

Bluetooth (3)

- ◆ si creano piccole reti wireless dette **WPAN**,
Wireless Personal Area Network
- ◆ nello standard Bluetooth vengono chiamate **piconet**, e possono collegare fino a 8/16 dispositivi
- ◆ più *piconet* possono collegarsi tra loro, formando una **scatternet**
- ◆ gestiscono sia dati che voce
- ◆ per determinare i servizi disponibili in un dispositivo si utilizza il protocollo **SDP**,
Service Discovery Protocol

Bluetooth (4)

Adotta due possibili tecniche di comunicazione:

- ◆ **ACL**, *Asynchronous ConnectionLess*,
trasmissione asincrona di solo dati alla
velocità di
 - 434 Kbps (simmetrica)
 - 723 Kbps / 57,6Kbps (asimmetrica)
- ◆ **SCO**, *Synchronous Connection Oriented*,
trasmissione sincrona bidirezionale di 64
Kbps di dati e fonia