

WIRELESS LAN

Autori:

Giuliano Paris (TILS)

Gabriella Zitti (TILS)

Cos'è una rete WLAN?

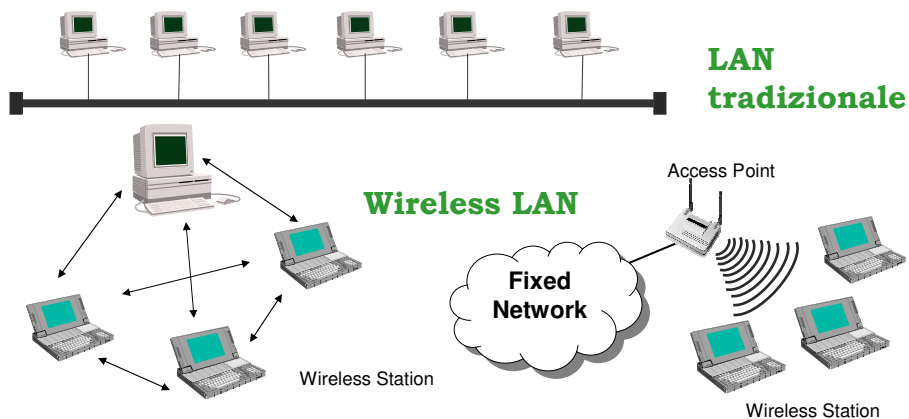
✓Una wireless LAN è una rete dati “senza fili” utilizzabile in un’area di estensione limitata

- aree indoor pubbliche e private (es. uffici, abitazioni, alberghi)
- aree outdoor circoscritte (es. Campus universitari)
- Copertura detta “hot spot”

✓La tecnologia di trasporto dominante è lo standard IEEE 802.11

- La trasmissione dati è realizzata in radiofrequenza utilizzando una banda non licenziata (2.4 GHz ISM (Industrial Scientific and Medical))
- l’uso di queste frequenze non richiede una licenza governativa, ma soltanto il rispetto di limiti (es. potenza di emissione)
- Le prestazioni sono paragonabili a quelle di una rete cablata: è possibile raggiungere un bit-rate di 11 Mbps con IEEE 802.11b e di 54 Mbps con IEEE 802.11a e IEEE 802.11g

Wireless LANs



Wireless station

PC, laptop, palmtop dotato di una wireless network interface card (NIC)

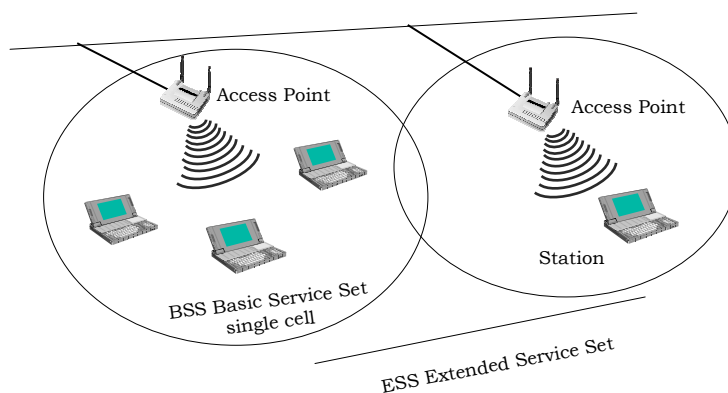
Access point (AP)

Fornisce l'accesso a più wireless stations alla wired network

Wireless LAN

3

Tipologie di rete 802.11: Infrastructure Mode



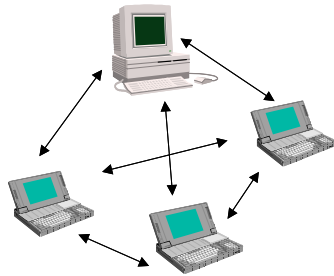
✓La rete wireless consiste di almeno un access point connesso alla rete fissa e un set di wireless stations. Questa configurazione è detta *basic service set* (BSS).

✓Un *extended service set* (ESS) è un insieme di due o più BSSs che formano una singola rete.

Wireless LAN

4

Tipologie di rete 802.11: Ad Hoc Mode



Independent Basic
Service Set (IBSS)

- ✓ E' un insieme di 802.11 wireless stations che comunicano direttamente tra loro senza usare un access point.
- ✓ Molto utile per installare velocemente e facilmente una rete wireless dove non esiste un'infrastruttura di rete.

Perchè Wireless

- ✓ Eliminazione del cablaggio (in tutto o in parte)
- ✓ Mobilità
- ✓ Scalabilità
- ✓ Estensioni di LAN cablate
- ✓ Possibilità di integrazione con le reti wireless geografiche (GSM/GPRS)

Wireless LANs: standards

- ✓IEEE 802.11
- ✓ETSI HIPERLAN

- ✓**IEEE 802.11** permette di realizzare una vera e propria LAN Ethernet “senza fili”
 - Standard affermato
 - Bit-rate più elevato e miglior supporto per la mobilità rispetto a Bluetooth
 - numerosi prodotti disponibili e garanzia di interoperabilità già significativa negli USA ed in espansione anche in Europa

La Wi-Fi Alliance

- ✓La Wi-Fi alliance è una associazione di costruttori di apparati, produttori di software e non solo, nata per promuovere la diffusione delle WLAN.
- ✓Ne fanno parte le più grandi case quali Cisco, Nokia, Ericsson, Microsoft e molte altre.
- ✓Guidano anche lo sviluppo degli standard.
- ✓Certificano la conformità degli apparati alle regole dettate negli standard tramite test di compatibilità ed interoperabilità. Alla fine impongono il marchio che certifica la conformità agli standard IEEE802.11x.

www.wi-fi.org



HIPERLAN (standard ETSI)

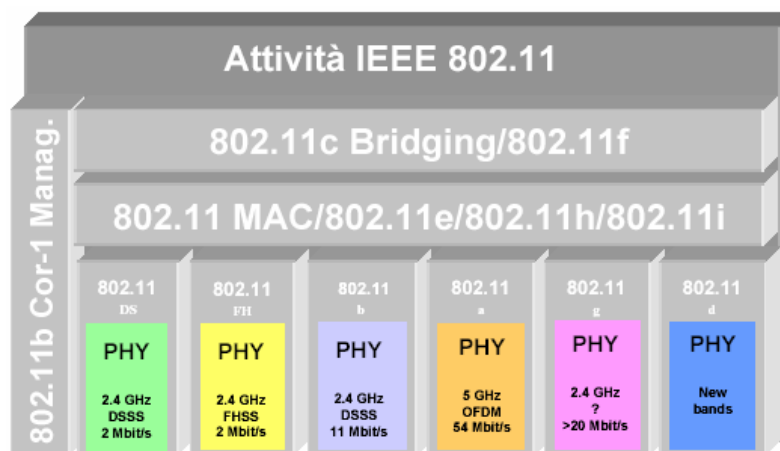
HIPERLAN/1

- Banda 5GHz
- Massima velocità trasmissiva di 17 Mbit/s
- Non controlla né garantisce QoS sul link wireless
- È un sistema per la consegna dei dati di tipo best effort

HIPERLAN/2

- Banda 5GHz
- Massima velocità trasmissiva di 54 Mbit/s
- Possibilità di definire delle priorità (in termini di banda, ritardo, bit error rate) assicurando così una QoS per ogni connessione.
- Disponibilità di apparati prevista per fine 2002 inizio 2003 (scadenza non rispettata).

Standard IEEE 802.11



Standard IEEE 802.11

✓ IEEE 802.11 (Luglio 1997)

- Banda 2.4 GHz
- Fornisce velocità di 1Mbps e 2 Mbps

✓ IEEE 802.11b (Settembre 1999); denominato anche Wi-Fi

- banda 2.4 GHz
- fornisce trasmissioni a 5.5 Mbps and 11 Mbps
- l'architettura di base, le caratteristiche, e i servizi di 802.11b sono definiti nello standard originale 802.11

Standard IEEE 802.11

✓ IEEE 802.11a (1999)

- Versione a 5 GHz per velocità fino a 54 Mbps
- Sarà (forse) in concorrenza con ETSI-HIPERLAN/2
- At close range, it may be possible to achieve up to 25Mbit/s net throughput, but this falls back up to 20Mbit/s as the device moves between 10-20 metres of coverage and then settles to 15 Mbit/s throughput for the outermost 30 metres of coverage
- Consumes more power than 802.11b

✓ IEEE 802.11g (2003)

- Banda ISM a 2,4 GHz fino a 54 Mbit/s; opera con 2 modalità di accesso (entrambi mandatory): CCK (Complementary Code Keying) mode usato da 802.11b (da qui compatibilità con Wi-Fi) e OFDM (Orthogonal Frequency Division Multiplexing) mode usato by 802.11a (ma in questo caso sempre nella banda 2.4GHz).

Standard IEEE 802.11

✓ IEEE 802.11e (Draft)

- Aggiunge al MAC meccanismi per la gestione della QoS (Quality of Service) e la definizione di classi di servizio

✓ IEEE 802.11h (2003)

- Aggiunge allo standard 802.11a le funzioni di TPC e DFS (Dynamic Frequency Selection) richieste dalla CEPT per l'impiego in Europa dei sistemi WLAN a 5 GHz

✓ IEEE 802.11i (2004)

- Migliora i meccanismi di sicurezza e autenticazione previsti oggi dal MAC (diversi studi hanno messo in luce la debolezza del meccanismo di sicurezza com'è ora definito nello standard WEP)

✓ IEEE 802.11f (2003)

- IAPP: Inter Access Point Protocol
- Stabilisce le regole di comunicazione tra AP durante l'handover degli utenti, garantendo l'interoperabilità tra AP di costruttori diversi.

Wireless LAN

13

Standard IEEE 802.11

✓ IEEE 802.11n

- Fornire un Throughput elevato, fino a 100Mbps

✓ IEEE 802.11p

- Fornire un servizio di accesso wireless per utenti che si spostano ad alta velocità (fino a 200 Km/h)

✓ IEEE 802.11r

- Garantire un FAST-Handover intra BSS

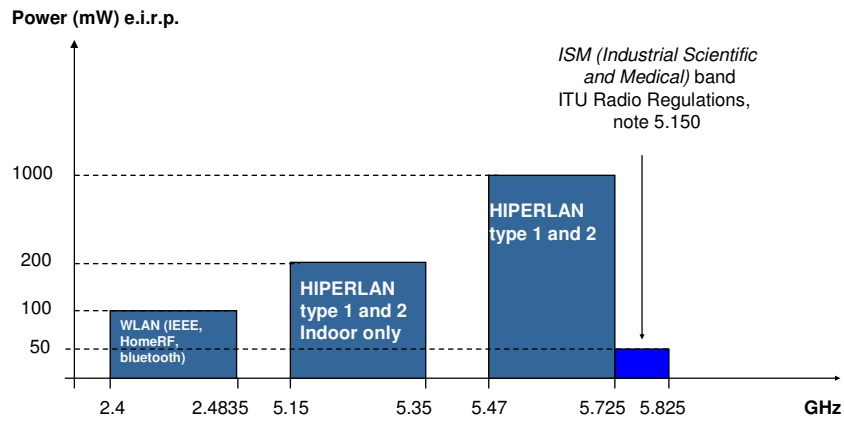
✓ IEEE 802.11s

- Reti MESH

Wireless LAN

14

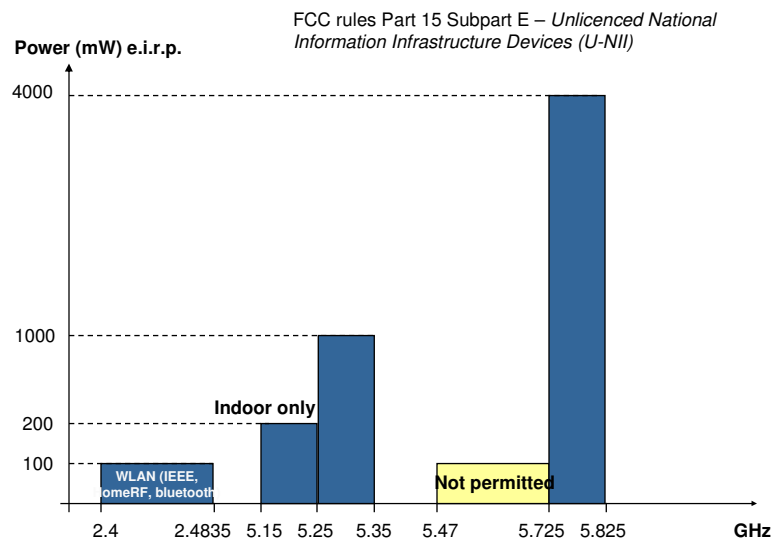
CEPT frequencies for WLAN



Wireless LAN

15

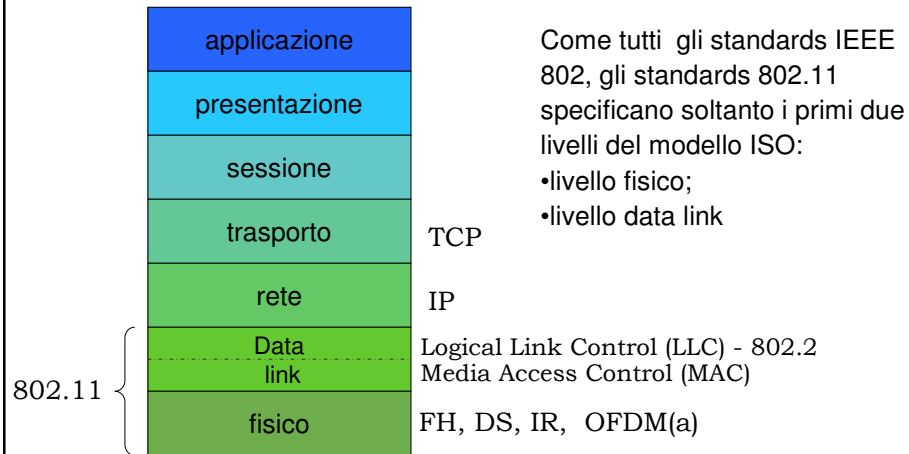
FCC frequencies for WLAN



Wireless LAN

16

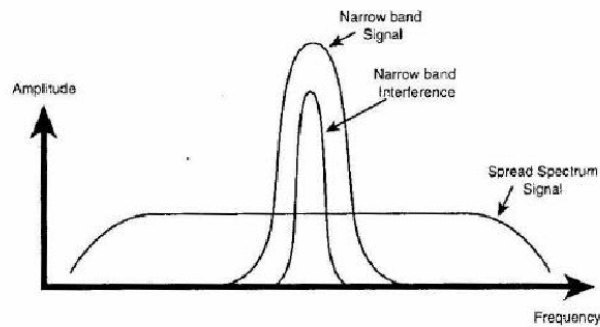
802.11 and ISO model



Livello Fisico

802.11: Livello fisico

- ✓ Impiego della tecnica spread spectrum (spettro espanso) per l'accesso radio
- ✓ prevede l'utilizzo di una banda molto ampia, per ottenere affidabilità e sicurezza nella trasmissione. Se il ricevitore non conosce i parametri dello spread spectrum, rileva un segnale che appare come rumore.



- ✓ Due tipi di tecniche spread spectrum (non sono compatibili):

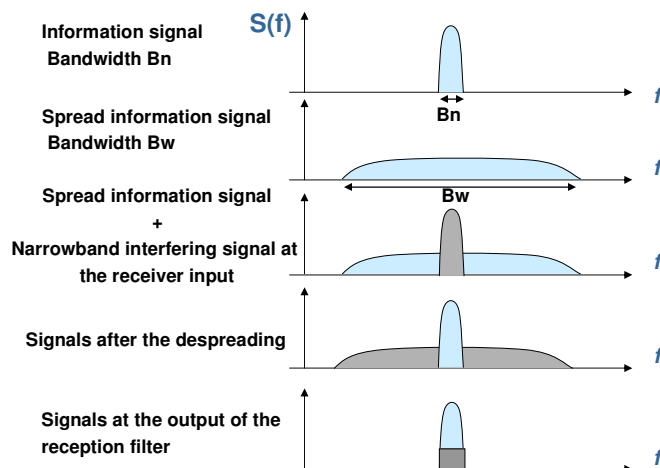
- FHSS
- DSSS

Wireless LAN

19

802.11b: physical level

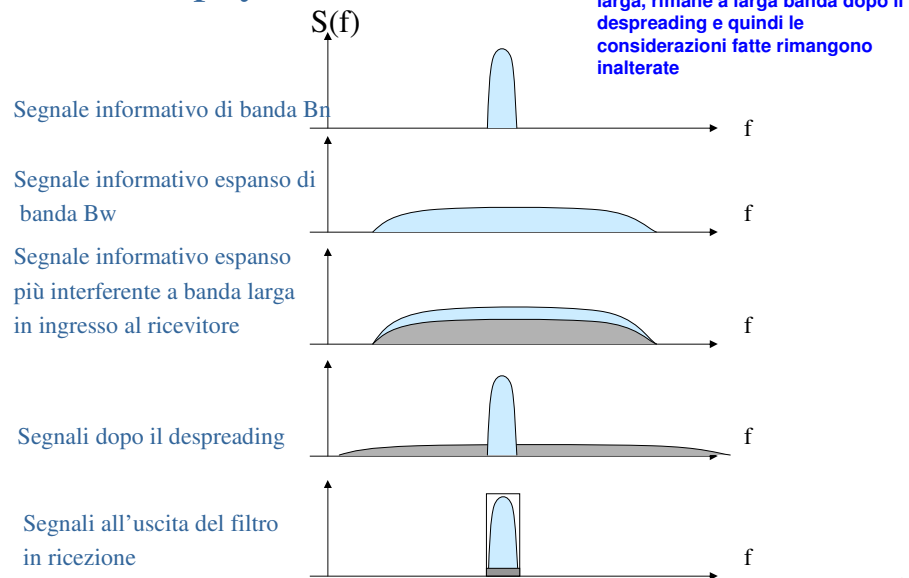
- spread spectrum technique: large bandwidth and low Power Spectral Density



Wireless LAN

20

802.11b: physical level



21

Livello Fisico: FHSS

FHSS (frequency hopping spread spectrum)

- La banda dei 2,4 GHz viene suddivisa in 75 canali da 1 MHz.
- Il segnale viene trasmesso su una definita sequenza di canali
- Nella sequenza i canali devono essere il più possibile “ortogonali”, minimizzando la probabilità che due comunicazioni interferiscano impiegando stesso canale nello stesso intervallo di tempo.
- Velocità non superiori ai 2 Mbps, a causa della limitata larghezza in banda dei canali (1MHz).

Wireless LAN

22

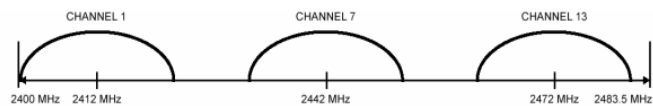
Livello fisico: DSSS

DSSS (Direct Sequence Spread Spectrum)

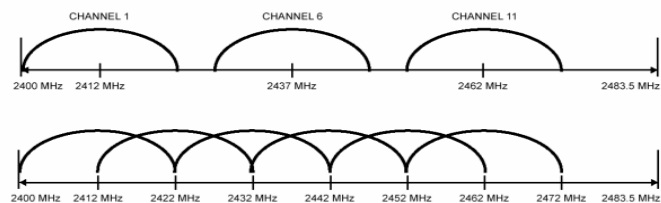
- Banda dei 2,4 GHz suddivisa in 14 canali di 22 MHz l'uno.
- Canali adiacenti parzialmente sovrapposti, soltanto 3 dei 14 completamente non sovrapposti. Ogni Access Point gestisce un canale.
- Ogni bit da trasmettere viene convertito in una sequenza di bit (chipping code). Il chipping code espande il segnale sui 22MHz del canale.
- Tramite il chipping code l'informazione utile viene ridondata (se un bit giunge errato la ridondanza associata al segnale permette di recuperare l'informazione).
- Più è lungo il chipping code, più è alta la probabilità che il segnale utile venga ricevuto correttamente e più è ampia la banda richiesta (spread spectrum).

WLAN channels

✓DSSS Europe
(distinguished and superimposed radio channels)



✓DSSS Nord-America
(distinguished and superimposed radio channels)



Architettura cellulare e riuso frequenziale (1)

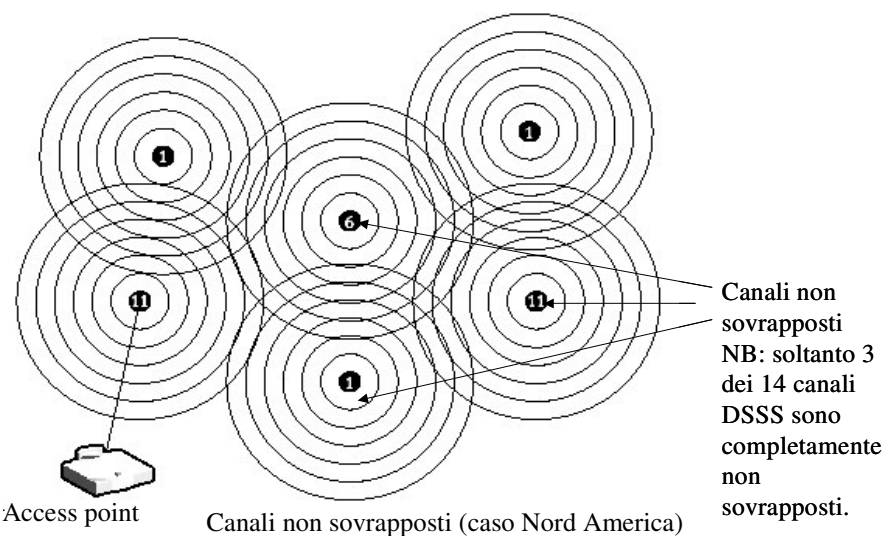
✓ Ogni cella (AP) gestisce un canale, con un throughput disponibile fino a 11 Mbps (condivisi tra tutti gli utenti della cella) che è funzione di:

- numero di utenti
- range della cella
- interferenza presente
- eventuali cammini multipli
- tempi di latenza dovuti ad eventuali bottleneck

✓ Per avere una copertura più ampia:

- copertura multicella: si impiegano più celle 802.11b parzialmente sovrapposte
- riuso frequenziale, utilizzando per ogni AP un canale (802.11/b DSSS) diverso e non sovrapposto con i canali impiegati dagli AP adiacenti (l'interferenza reciproca diminuirebbe la banda disponibile nella relativa area di copertura comune)

Architettura cellulare e riuso frequenziale (2)

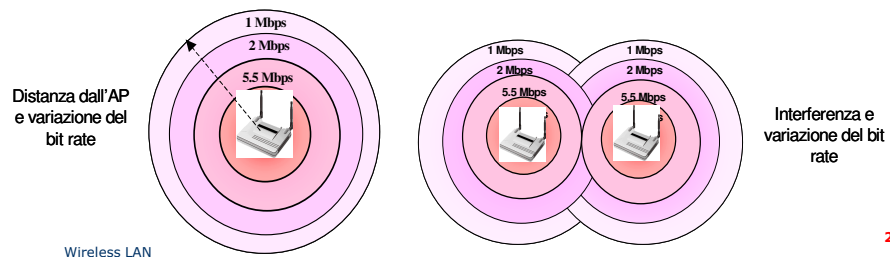


802.11b

- ✓ La specifica 802.11b modifica il livello fisico per consentire il supporto di velocità di 5,5 Mbps e 11 Mbps (mediante l'impiego di una tecnica di codifica (chipping code) più avanzata).
- ✓ Per ottenere queste velocità, è stata scelta la tecnica DSSS, poiché con il FHSS non si possono superare i 2 Mbps.
- ✓ Dynamic Rate Shifting: per ambienti radio molto rumorosi, l'802.11b consente di adattare automaticamente il data rate per compensare le modifiche che intervengono sul canale radio.

Nota: 11Mbps in condizioni ottimali, ma, se si supera la distanza ottimale per tale bit rate, oppure c'è interferenza, il sistema 802.11b riduce la velocità di trasmissione, a 5,5Mbps, 2Mbps, 1Mbps. Nel verso contrario il terminale aumenta la velocità di trasmissione, fino a tornare ad 11Mbps.

Il dynamic rate shifting è un meccanismo di livello fisico, trasparente per l'utente e per i livelli protocollari superiori.



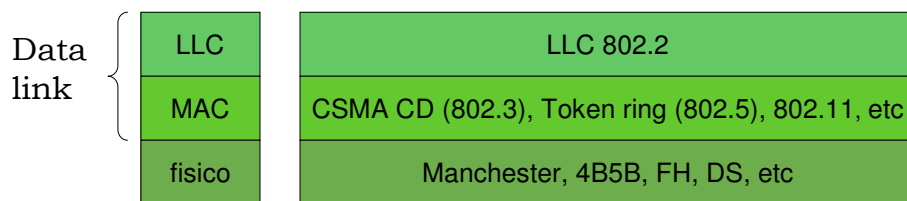
27

Medium Access Control (MAC)

802.11 Data Link Layer

✓ Consists of two sublayers:

- Logical Link Control
- Media Access Control: CSMA/CA, CRC checksum, packet fragmentation



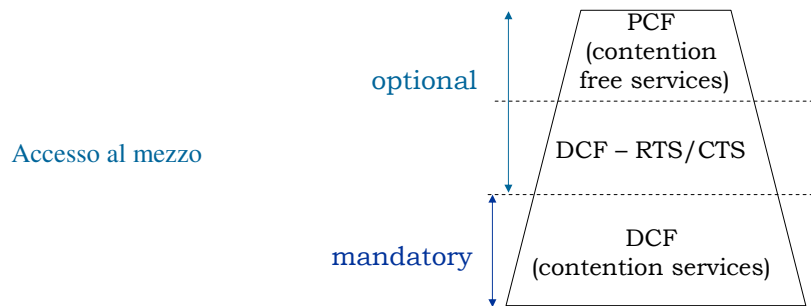
Power Saving

- ✓ By default, Wireless LANS use CAM (*Constant Access Mode*) to constantly listen to the network and get the data they need
- ✓ Workstations and AP can be configured for PAM (*Polled Access Mode*)
 - The clients wake up on regular periods and listen for a special packet called TIM (*Traffic Information Map*)
 - A client stays awake when the TIM indicated it has messages buffered at the AP and until those messages are transferred
 - The AP buffers the data until it receives a poll request from the destination station

802.11 e 802.11b: livello MAC

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

- concettualmente simile al MAC 802.3 wired: entrambi disciplinano l'accesso di più utenti ad un mezzo condiviso, i quali effettuano l'ascolto della portante (carrier sensing) prima di trasmettere.
- le stazioni trasmettono dopo aver ascoltato il mezzo senza rilevare altre trasmissioni. Alla ricezione corretta di ogni pacchetto dati, la stazione ricevente invia un messaggio di acknowledgement (ACK) al mittente. Nessun messaggio viene inviato se il pacchetto arriva corrotto.



802.11 e 802.11b: livello MAC

✓DCF (Distributed Coordination Function)

- capacità di ascoltare per un po' di tempo la rete e poi decidere di trasmettere.

✓DCF - RTS/CTS

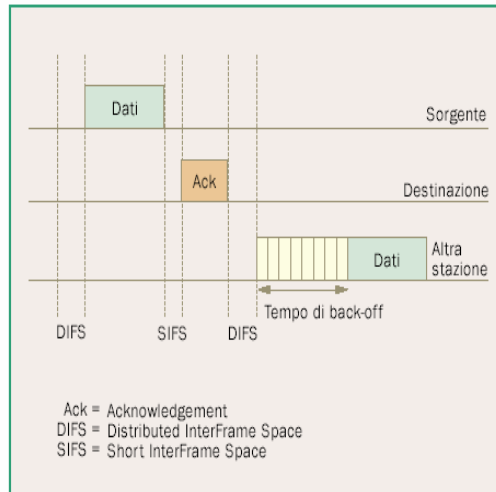
- viene utilizzata per risolvere il problema dell'hidden node:
- un nodo prima di trasmettere, invia, un pacchetto request-to-send (RTS) e aspetta che l'access point risponda con un pacchetto clear-to-send (CTS).

✓PCF (Point Coordination Function)

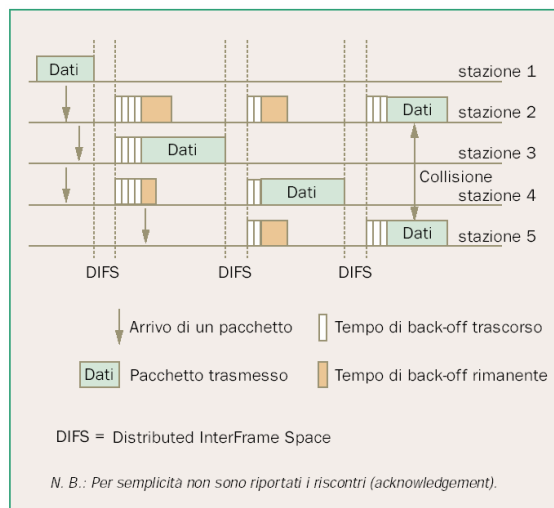
- fornisce un trasferimento di trama contention-free.
- Point Coordinator (PC) per eseguire il polling, abilitando le stazioni interrogate (polled) a trasmettere senza dover prima contendere per ottenere il canale libero.

Distributed Coordination Function (DCF)

- ✓ Una stazione può avviare la tx solo dopo aver rilevato il canale libero per un tempo detto DIFS (Distributed InterFrame Space)
- ✓ Altrimenti la stazione avvia un processo di back-off
- ✓ La stazione ricevente invia un riscontro (Ack)
- ✓ L'invio di quest'ultimo avviene dopo un tempo detto SIFS (Short InterFrame Space)

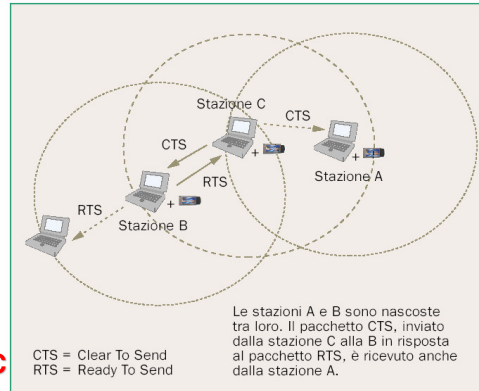
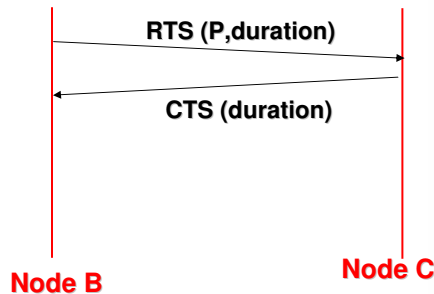


DCF: Esempio con più stazioni



The hidden node problem

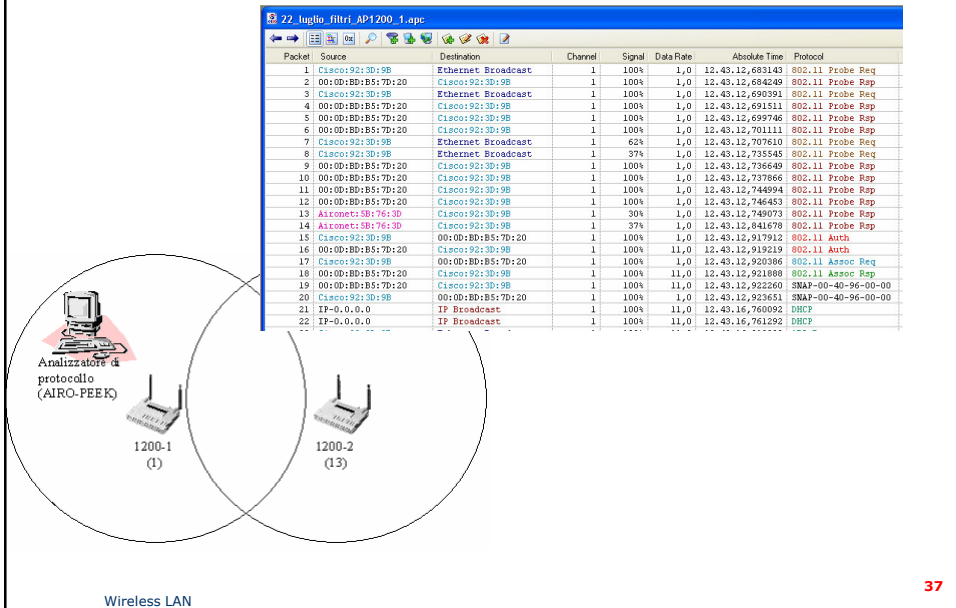
- ✓ Workstations A, B, and C can all see wireless access point P
- ✓ A and B can see one another, so B and C BUT A can't see C
- ✓ RTS/CTS handles the problem



Scanning

- Effettuato da qualsiasi STA per verificare il Service Set Identifier (SSID) ovvero per diventare membro della ESS associata al SSID controllato
- Serve per:
 - Cercare una BSS (IBSS) a cui associarsi
 - Cercare un nuovo AP durante il roaming
- ✓ **Scanning Passivo:** la STA controlla il SSID delle trame Beacon di ogni canale.
- ✓ **Scanning Attivo:**
 - la STA trasmette delle trame Probe contenenti il SSID da verificare e attende le trame di Risposta. Procedimento iterato per ogni canale.
 - Effettuato lo scanning, la STA avrà le informazioni sulla BSS
 - In una IBSS la STA che per ultima ha generato il Beacon risponderà al Probe; per collisione o per fallimento della ricezione del Beacon più STA potrebbero rispondere alla trama Probe.

Associazione e riassociazione



37

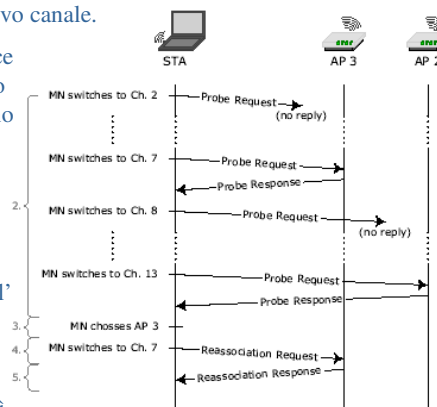
Scanning

✓ Il livello MAC 802.11 gestisce l'associazione di ogni client con un determinato Access Point. Il mobile sceglie quello al quale associarsi basandosi sul livello di segnale e sul tasso di errore che osserva, e si sintonizza sul canale radio sul quale è settato l'AP.

✓ Periodicamente il mobile supervisiona i canali adiacenti (scanning), per rilevare un altro AP che possa fornirgli un canale migliore. Se lo trova, si associa con il nuovo AP (riassociazione), sintonizzandosi sul nuovo canale.

✓ **Passive scanning:** la stazione scandisce tutti i diversi canali rimanendo in ascolto per un certo periodo di tempo su ciascuno di essi in attesa di un beacon (frame di sincronizzazione inviato periodicamente da un AP).

✓ **Active scanning:** la stazione manda una probe request, cioè un frame broadcast contenente l'identificatore dell'AP cercato, ossia l'SSID. Rimane poi in attesa per un certo periodo di tempo di una probe response. Se non riceve risposta passa al canale successivo e così via.



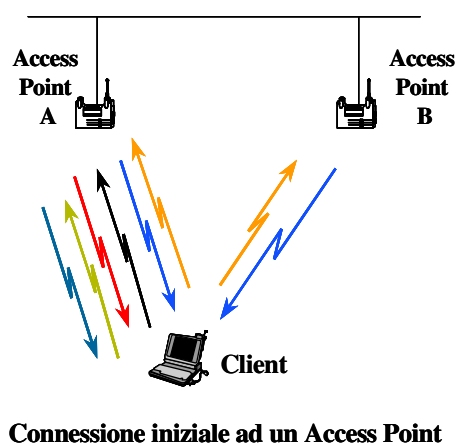
38

Wireless LAN

Servizi IEEE 802.11

- ✓Definiscono come una stazione ottiene l'accesso ad un BSS e come viene gestito il traffico in un BSS e tra BSS.
- ✓Autenticazione: per controllare l'accesso alla WLAN.
 - Open system;
 - Shared key (basato su WEP).
- ✓Associazione: connessione logica che la wireless station deve instaurare con un AP per lo scambio dei dati
- ✓Riassociazione: avviene quando una stazione wireless si sposta da un access point ad un altro.
- ✓Disassociazione: tramite questo servizio la stazione notifica all'access point che sta lasciando il BSS.

Associazione all'Access Point

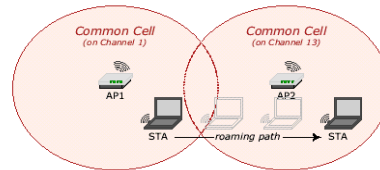


Passi per l'Associazione:

- Il Client invia la richiesta
- AP invia la risposta
- Il Client esamina la risposta e seleziona il miglior AP
- Il Client richiede l'autenticazione all' AP selezionato (A)
- L' AP A conferma l'autenticazione e registra il client
- Il Client richiede l'associazione all' AP selezionato
- L' AP A conferma l'associazione e registra il client

Roaming

Possibilità di spostarsi da una cella all'altra senza perdere la connettività



- **Mobilità:**

- Tra celle appartenenti allo stesso ESS (mobilità di livello 2)
 - Per il seamless roaming si sfrutta la sovrapposizione
- Tra celle appartenenti ad ESS diversi (mobilità di livello 3: cambia l'indirizzo IP a livello di subnet)
 - Per realizzare il seamless roaming si può utilizzare il protocollo Mobile IP

Standard nuovo (802.11f):

- **Inter Access Point Protocol (IAPP)**

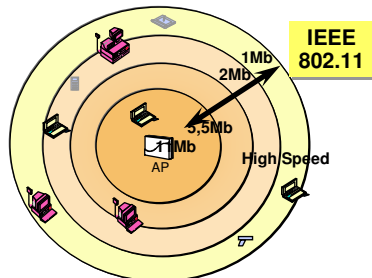
Protocollo che definisce le modalità per:

- Handover, mobilità e coordinazione tra AP;
- Interoperabilità tra AP appartenenti a produttori diversi.

Access Point Range 802.11b

Access point range at different speeds

Speed 802.11b	Open environment coverage	Semi-open environment coverage	Closed environment coverage
11 Mbps	160 mt	40 mt	25 mt
5,5 Mbps	270 mt	55 mt	35 mt
2 Mbps	400 mt	90 mt	50 mt
1 Mbps	550 mt	115 mt	65 mt



Real throughput

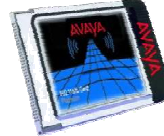
Data Rate	Throughput
11 Mbps	5 Mbps
5,5 Mbps	3,3 Mbps
2 Mbps	1,4 Mbps
1 Mbps	0,8 Mbps

Area di copertura e Prestazioni 802.11b/g

Ampia copertura...per le basse velocità ma solo per i sistemi noti 802.11b. L'aumento di velocità trasmissiva comporta una *diminuzione della dimensione della cella, anche notevole*

Reali velocità ottenibili

Data Rate	Throughput
54 Mbps	22 Mbps
24 Mbps	10 Mbps
11 Mbps	5 Mbps
1 Mbps	0,8 Mbps



Raggio d'azione alle diverse velocità

Velocità 802.11b/g	Copertura Ambiente Aperto	Copertura Semi Aperto	Copertura Ambiente Chiuso
54 Mbps	40 m	20 m	15 m
24 Mbps	90 m	30 m	20 m
11 Mbps	160 m	40 m	25 m
1 Mbps	550 m	115 m	65 m

Nota: Tutte le distanze indicate rappresentano valori limiti approssimati e sono **strettamente** legate alla corretta installazione delle antenne

Fonte: G. Palmieri (AVAYA)

Evoluzione del GSM verso il 3G

Generazione	Sistema	Tipo di Commutazione	Velocità dati (fino a)
2 G	GSM	Circuito	~ 10-14.4 Kbit/sec
2.5 G	HSCSD	Circuito	~ 38-56 Kbit/sec
2.5 G	GPRS	Pacchetto	~ 50 Kbit/sec
2.5-3 G (2.75 G)	EDGE	Pacchetto EGPRS	~ 180-200 Kbit/sec
		Circuito ECSD	64 Kbit/sec
3 G	UMTS	Circuit domain	64 Kbit/sec
		Packet domain	384 Kbit/sec

Sicurezza nelle WLAN

Sicurezza per WLAN: I generazione

✓ Meccanismi per il controllo dell'accesso alla rete previsti dallo standard 802.11:

- SSID: per associarsi con un AP le stazioni devono conoscere l'SSID (identificativo associato con la rete). L'utilizzo di SSID per il controllo dell'accesso non è sicuro poiché l'AP può essere configurato in modo da inviare in broadcast SSID nel beacon.
- MAC address filtering: ciascun AP può essere configurato con una lista di indirizzi MAC di stazioni a cui è consentito l'accesso
- WEP (Wired Equivalent Privacy)

✓ Metodi di sicurezza deboli in quanto device- dependent: la chiave WEP e il MAC address sono presenti nel dispositivo

Autenticazione

Due metodi di autenticazione: Open System, and Private (Shared) Key

- *Open system* permette a qualunque client 802.11 di associarsi con un AP. Consiste di due passi:
 - Invio dell'identità e richiesta di autenticazione
 - Risposta con il risultato dell'autenticazione
- *Private (Shared) key* consente l'autenticazione solo a quei client che conoscono la chiave privata (condivisa e statica) (*)
 - Lo standard IEEE 802.11 assume che la chiave privata venga consegnata ai client attraverso meccanismi sicuri indipendenti dallo stesso standard

(*) Implica l'impiego del WEP

MAC Filtering

- ✓ Media Access Control – Address – Indirizzo hardware assegnato alle schede di rete dal costruttore
 - Unico in modo tale che non esistono due schede con lo stesso MAC address
 - Permanente e non può essere cambiato (*)
- ✓ Alcuni Access Point supportano i “Filtri MAC”
 - Si può specificare sugli AP quali indirizzi MAC hanno la possibilità di associarsi
 - Disabilitare tutti gli altri indirizzi MAC

(*) Può essere mascherato tramite software (spoofing)

WEP (Wired Equivalent Privacy)

- ✓ Metodo di crittografia dei dati
 - Algoritmo RC4 PRNG con shared key a 40 bit o 104 bit.
 - La chiave statica è posseduta sia dal client wireless che dall'AP
 - Tutti i dati scambiati tra AP e client wireless vengono cifrati tramite questa chiave.
- ✓ Metodo di autenticazione
 - L'AP invia al client un pacchetto di challenge che il client deve cifrare con la corretta chiave e restituire all'AP. Se il client non possiede la chiave corretta, il processo di autenticazione fallisce e il client non può associarsi con l'AP (Shared Key Authentication).
- ✓ WEP NON è sicuro
 - Airsnort: programma in grado di ascoltare una trasmissione e ricavarne una chiave
 - Articolo "Weakness in the key scheduling algorithm of RC4",
 - Fluhrer, Mantin, Shamir

Limitazioni del WEP

- ✓ Molte implementazioni usano chiavi globali che vengono cambiate raramente
- ✓ Queste chiavi sono facilmente "crackabili" con tool quali AirSnort e WEPcrack
- ✓ WEP utilizza una implementazione dell'algoritmo RC4 con l'impiego dell'Initialization Vector (IV)
- ✓ Lo standard va bene per reti private o di piccole dimensioni:
 - Poche collisioni: gli IV si ripetono di rado
 - Poche stazioni: la gestione manuale delle chiavi è accettabile
- ✓ Nuove soluzioni sono necessarie per reti pubbliche e/o di grandi dimensioni per:
 - Autenticazione
 - Integrità/Riservatezza dei dati

Sicurezza per WLAN: II generazione

- ✓ Autenticazione tramite Server centralizzati (Server AAA ad es. RADIUS)
- ✓ Chiavi dinamiche per la cifratura e relativa distribuzione
- ✓ Autenticazione mutua
- ✓ Algoritmi di cifratura ed integrità più robusti

Nuove soluzioni

Due approcci paralleli

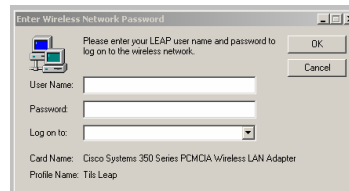
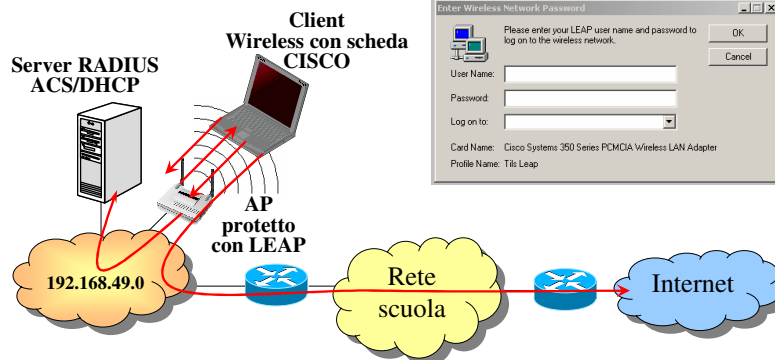
- 802.11i: nuovo standard per la sicurezza sviluppato dall'IEEE ultimato a giugno del 2004
- WPA (Wireless Protected Access): l'industria non poteva aspettare i tempi lunghi della standardizzazione, così la Wi-Fi Alliance, in collaborazione con IEEE, ha promosso il WPA. E' un sottoinsieme dello standard 802.11i, consolidato all'inizio del 2003 e certificato nel luglio 2003.

Lo standard 802.11i verrà testato e diffuso commercialmente con il nome di WPA2

Caratteristiche essenziali dello standard 802.1x

- ✓ **Mutua autenticazione.** Oltre all'autenticazione del client wireless presso la rete, è prevista l'autenticazione della rete presso il client. Questo allo scopo di evitare attacchi del tipo Rogue AP dove un AP intruso si inseriva tra il client e l'AP "vero" catturando i dati del client. Il nuovo standard prevede che anche l'AP (o il server di autenticazione) si debba autenticare presso il client.
- ✓ **Generazione dinamica delle chiavi.** Nell'802.1x sono previsti meccanismi di generazione dinamica delle chiavi di cifratura che vengono generate e distribuite dopo le procedure di autenticazione.
- ✓ **Politica centralizzata di controllo.** Viene previsto che il controllo degli accessi venga realizzato attraverso un server AAA (es. RADIUS).

Sicurezza WLAN con CISCO LEAP



1. Il client tenta l'accesso; l'AP blocca il client
2. L'AP richiede le credenziali all'utente
3. L'utente si identifica con username e password
4. L'AP invia la username al server RADIUS che autorizza l'accesso, assegnando le chiavi WEP dinamiche
5. A questo punto l'utente ha accesso alla rete

Cifratura in 802.11i

- **Temporal Key Integrity Protocol (TKIP):** un insieme di aggiornamenti software al WEP (basato su RC4)
 - *IV a 48 bit.* Un IV di 48 bit riduce il suo “riuso” e la possibilità per un hacker di raccogliere frame sufficienti per ricavare la chiave di cifratura
 - *Per Packet Keying (PPK).* Vengono generate automaticamente e periodicamente chiavi univoche per ciascun utente
 - *Message Integrity Code (MIC).* Campo di controllo inserito prima dell’ Integrity Check Value (ICV) nel payload 802.11
- **AES :** un algoritmo di cifratura più robusto dell’algoritmo RC4
 - Obbligatorio in 802.11i
 - E’ un sistema cipher block: combina
 - Cipher Block Chaining Counter (CBC-CTR) mode per l’encryption
 - Cipher Block Chaining Message Authenticity Check (CBC-MAC) per data integrity
 - Complessivamente detto AES-CCM

Grazie per l’attenzione