



# IEEE 802.11

---

Lo standard per Wireless LAN

1

S. Olivieri

## Sommario

---

- Definizione e caratteristiche delle WLAN
- Architettura, topologie di rete e servizi dello standard IEEE 802.11
- Tecnologie e protocolli dello strato fisico 802.11/a/b/g

---

2

S. Olivieri

## Parte 1

---

- ☞ Definizione e caratteristiche delle WLAN
  - Architettura, topologie di rete e servizi dello standard IEEE 802.11
  - Tecnologie e protocolli dello strato fisico 802.11/a/b/g

3

S. Olivieri

## Cos'è una Wireless LAN

---

- Una **Wireless Local Area Network (W-LAN)** è una rete locale i cui nodi comunicano tra loro attraverso il canale radio
- Una WLAN è un sistema di comunicazione dati molto flessibile e può essere utilizzato come estensione o anche alternativa alle normali LAN su cavo
- Nota: wireless significa “senza cavo”
  - Per le reti, si può trattare di radio od infrarossi
  - Noi faremo generalmente riferimento alla tecnologia radio

4

S. Olivieri

## Vantaggi delle WLAN

- Mobilità
  - Gli utenti possono accedere alle risorse di rete da qualsiasi posizione senza doversi collegare ad una presa
- Velocità e semplicità di installazione
  - È possibile installare una WLAN senza dover stendere cavi attraverso muri o sotto i pavimenti
- Flessibilità di installazione
  - La tecnologia radio fa sì che la copertura sia garantita anche dove non è possibile cablare

5

S. Olivieri

## Vantaggi delle WLAN (II)

- Costi
  - L'investimento iniziale necessario per l'hardware di una WLAN può essere superiore rispetto ai costi per una LAN su cavo
  - Le spese di installazione ed i costi di esercizio e manutenzione per una WLAN sono molto inferiori
  - I benefici di costo a lungo termine sono maggiori soprattutto in ambienti dinamici dove ci sono cambiamenti frequenti
- Scalabilità
  - Le WLAN possono essere configurate in diverse topologie in modo da soddisfare le diverse esigenze di particolari applicazioni
    - Reti peer-to-peer adatte per un numero piccolo di utenti
    - Infrastrutture di rete per il supporto di migliaia di stazioni in mobilità su un'area molto estesa
  - La configurazione può essere modificata facilmente

6

S. Olivieri

## Wireless LAN oppure no

- Le WLAN non sono le uniche ad utilizzare la tecnologia wireless
  - Wireless bridges
    - Per connettere due diversi segmenti di LAN via radio
  - Wireless Distribution Systems
    - Usati dagli ISP per collegare diversi clienti ad una stessa base station (ad es. WMAN IEEE 802.16)
  - Cable replacement
    - Per trasferire dati tra due unità senza utilizzare un cavo seriale o parallelo
- In alcuni casi tali tecnologie si basano sulla WLAN ma con funzionalità ristrette (ad es. senza broadcasting) e ammettono solo un insieme di connessioni punto-punto (topologia non basata su TCP/IP)

7

S. Olivieri

## WLAN professionali e domestiche

- Con la riduzione dei costi dovuta al progresso tecnologico, molti produttori implementano dispositivi più economici per il mercato domestico
  - È possibile ridurre i costi del modem (in genere la parte più costosa) utilizzando parti analogiche a prestazioni inferiori
    - La minore sensibilità o la limitata capacità di filtrare i canali adiacenti può ridurre il raggio d'azione e le prestazioni
  - L'interfaccia con l'host offre meno opzioni (solo USB) del professionale (Ethernet, Seriale, PCI, USB)
  - Può mancare la criptatura ed il power management
  - Differenze più sostanziali potrebbero essere nell'Access Point

8

S. Olivieri

## Parte 2

---

- Definizione e caratteristiche delle WLAN
- ☞ Architettura, topologie di rete e servizi dello standard IEEE 802.11
- Tecnologie e protocolli dello strato fisico
  - 802.11
  - 802.11b
  - 802.11a

9

S. Olivieri

## Lo standard IEEE 802.11

---

- Nel 1997 l'Institute of Electrical and Electronics Engineers (IEEE) ha ratificato, dopo ben sette anni di lavoro (!), la specifica **802.11** come standard per le wireless LAN
- Tale sforzo è stato compiuto per garantire l'affidabilità e la compatibilità tra sistemi prodotti da vari produttori, favorendo quindi la diffusione delle WLAN
- IEEE 802.11 soffriva di alcuni problemi
  - Risultava obsoleto ancor prima che uscissero i relativi prodotti
  - Aveva throughput insufficiente (2 Mbit/sec max) a soddisfare la maggior parte dei requisiti soprattutto in ambiente business
- Successivamente sono state ratificate le versioni **802.11a**, **802.11b** ed **802.11g**
  - Modificano lo strato fisico in modo da supportare velocità più elevate
  - Mantengono la compatibilità con lo strato MAC per contenere i costi

10

S. Olivieri

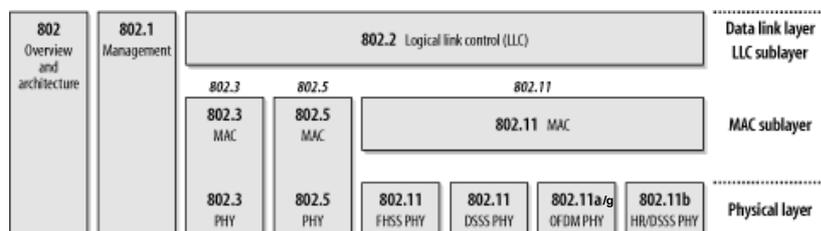
## Gli strati di IEEE 802.11

- Similmente ad Ethernet IEEE 802.3, lo standard IEEE 802.11 definisce
  - Le funzioni necessarie ad una stazione 802.11 per operare sia in modalità peer-to-peer che integrata con una LAN esistente
  - La privacy e la sicurezza dei dati dell'utente trasportati sul mezzo radio
  - Il sottostrato MAC per l'accesso al mezzo
  - Lo strato fisico (PHY) e le relative interfacce

11

S. Olivieri

## I protocolli della famiglia IEEE 802.x



12

S. Olivieri

## L'architettura delle WLAN IEEE 802.11

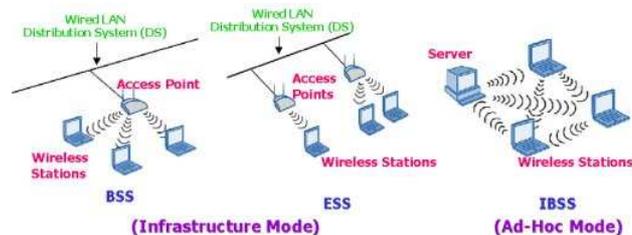
- L'architettura 802.11 è costituita da diversi componenti e servizi che interagiscono al fine di garantire la mobilità delle stazioni in modo trasparente agli strati più alti dello stack di protocolli
- Il componente di base della WLAN 802.11 è la **stazione**
  - È una qualsiasi unità che contiene le funzionalità del protocollo 802.11
  - Le stazioni 802.11 possono essere mobili (palmari), portatili (PC) o stazionarie (Access Point)
- Un insieme di stazioni costituisce un **Basic Service Set (BSS)**

13

S. Olivieri

## Topologie di rete per IEEE 802.11

- Esistono due modalità di funzionamento
  - Independent Basic Service Set (IBSS) o Ad Hoc Network
  - Infrastructure Basic Service Set o Infrastructure Mode

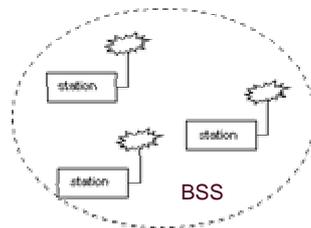


14

S. Olivieri

## Independent Basic Service Set

- È la topologia più semplice dove un insieme di stazioni si sono identificate reciprocamente e sono interconnesse tra di loro in modalità peer-to-peer
- In un IBSS le stazioni comunicano direttamente tra loro
- In una IBSS non ci sono funzioni di relay
  - una stazione è raggiungibile solo se situata entro il raggio di copertura

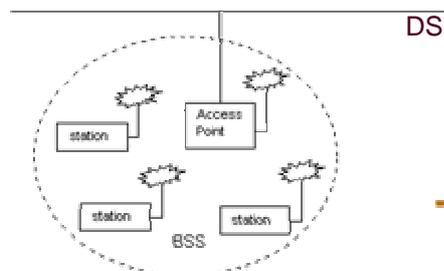


15

S. Olivieri

## Infrastructure Basic Service Set

- È una BSS con un componente chiamato **Access Point** (AP) che fornisce la funzione di relay per la BSS
- L'architettura dell'Infrastructure BSS è di tipo cellulare
  - Il sistema è diviso in celle costituite dalle BSS
  - Ciascuna cella è controllata dall'AP
  - La comunicazione tra stazioni avviene solo attraverso l'AP

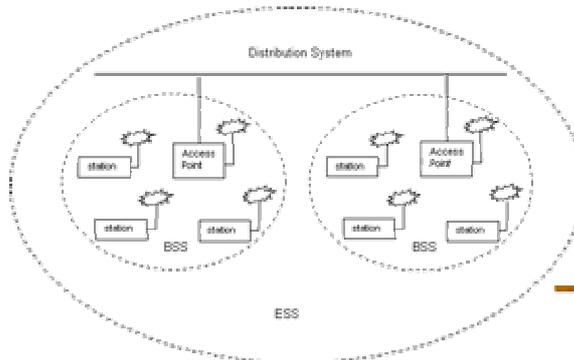


16

S. Olivieri

## Extended Service Set

- In 802.11 l'**Extended Service Set** (ESS) estende la mobilità delle stazioni ad un raggio di azione arbitrario
- Un ESS è un insieme di Infrastructure BSS, dove gli AP comunicano tra di loro attraverso il **Distribution System** (DS) per trasportare il traffico da una BSS all'altra, agevolando lo spostamento delle WS tra BSS



17

S. Olivieri

## Il Distribution System

- Funzionalmente è uno strato residente in ciascun AP che funge da dorsale della WLAN, attraverso il quale un AP comunica con un altro AP per
  1. Scambiare pacchetti destinati alle stazioni nei rispettivi BSS
  2. Girare pacchetti per inseguire le stazioni mobili che si spostano da un BSS ad un altro
  3. Scambiare pacchetti con una rete su cavo
- Lo standard 802.11 lascia libertà di scelta (in ambito IEEE 802 LAN) della tecnologia utilizzabile per l'implementazione del DS, e stabilisce i servizi che esso deve fornire
  - Il DS si può basare sia su una LAN 802.3 su cavo, che su una rete wireless 802.11
  - **802.11f** standardizza il protocollo **Inter-Access Point Protocol (IAPP)**
    - Registrazione degli AP in una rete
    - Scambio di informazioni tra AP quando una stazione si muove tra aree di copertura supportate da AP di diversi produttori

18

S. Olivieri

## L'ESS nel modello OSI

- Gli elementi di rete al di fuori dell'ESS vedono l'ESS e tutte le sue stazioni mobili come una singola rete al livello MAC dove tutte le stazioni sono fisicamente stazionarie
- L'ESS quindi nasconde la mobilità delle stazioni mobili a quanto situato al di fuori dell'ESS, ed è visto dai livelli superiori del modello OSI come una singola rete 802
- Questa caratteristica di 802.11 consente ai protocolli di rete esistenti, che non possiedono il concetto della mobilità, di operare correttamente con una WLAN che supporta la mobilità

19

S. Olivieri

## I servizi di IEEE 802.11

- IEEE 802.11 specifica nove servizi
  - Supporto al delivery dei messaggi tra stazioni
  - Controllo dell'accesso alla rete e sicurezza
- Possono essere suddivisi in due categorie
  - Servizi delle stazioni
  - Servizi di distribuzione
- Ciascun servizio è supportato da opportuni messaggi di management al livello MAC

20

S. Olivieri

## Servizi delle stazioni

- Sono forniti da tutte le stazioni di una WLAN, inclusi gli AP
- L'obiettivo principale è quello di garantire la sicurezza e la distribuzione dei dati
  - Authentication
  - De-authentication
  - Privacy
  - Data delivery

21

S. Olivieri

## Authentication

- Siccome le WLAN hanno dei limiti in termini di sicurezza al livello fisico per prevenire accessi non autorizzati, 802.11 definisce un servizio di autenticazione per il monitoraggio dell'accesso alla rete secondo il quale una stazione può identificare un'altra stazione
- Tutte le stazioni 802.11, siano esse parte di una IBSS o di una rete ESS, devono utilizzare il servizio di autenticazione prima di poter comunicare con un'altra stazione
- Il servizio di Authentication si basa sullo scambio di opportuni frame di management per l'autenticazione (*Type: Management, Subtype: Authentication*) tra la stazione che richiede di autenticarsi (**requester**) e la stazione destinataria (**responder**)
- IEEE 802.11 definisce due tipi di servizi di autenticazione
  - **Open system authentication**
  - **Shared key authentication**

22

S. Olivieri

## Open system authentication

---

- È il metodo di autenticazione di default, molto semplice, basato su un processo a due step
  - Il requester invia al responder un frame di autenticazione contenente l'informazione di identità
  - Il responder invia indietro un frame di avviso dopo aver registrato l'identità del requester

23

S. Olivieri

## Shared key authentication

---

- Questo metodo assume che ogni stazione abbia ricevuto una chiave segreta condivisa attraverso un canale sicuro indipendente dalla rete 802.11
  1. Il requester invia al responder un frame di richiesta per l'autenticazione contenente l'informazione di identità
  2. Il responder risponde con un frame contenente una stringa di ottetti pseudorandom
  3. Il requester copia la stringa di ottetti in un frame che viene codificato con un opportuno algoritmo di crittatura (**Wired Equivalent Privacy**, WEP) che usa la chiave segreta condivisa, ed inviato al responder
  4. Il responder decodifica mediante WEP il frame ricevuto, confronta gli ottetti ricavati con quelli inviati nel 2° frame, ed invia un frame contenente l'esito (positivo o negativo) dell'operazione di autenticazione

24

S. Olivieri

## De-authentication

- Il servizio di deautenticazione è utilizzato per impedire ad un utente precedentemente autorizzato di utilizzare ulteriormente la rete
- Una volta che una stazione è stata deautenticata, essa non è più in grado di accedere alla WLAN senza ripetere di nuovo il processo di autenticazione
- La deautenticazione è una notifica e non può essere rifiutata
  - Per esempio, quando una stazione vuole essere rimossa da un BSS, può inviare un management frame di deautenticazione al relativo AP per informarlo dell'abbandono della rete
  - Un AP potrebbe anche decidere di deautenticare una stazione suo malgrado inviandole un frame di deautenticazione

25

S. Olivieri

## Privacy

- In una WLAN tutte le stazioni possono ascoltare il traffico dati che viaggia sul mezzo radio entro il raggio di copertura, compromettendo seriamente la sicurezza
- Il servizio di privacy di 802.11 è progettato per fornire un livello di protezione dei dati equivalente a quello garantito dalla ristrettezza di accesso al mezzo fisico (tramite connettore) di una LAN su cavo
  - Protegge i dati solo durante l'attraversamento del mezzo radio
  - Non è progettato per fornire una protezione completa dei dati scambiati tra applicazioni che girano su una rete eterogenea
- Il servizio di privacy si basa sull'algoritmo WEP (lo stesso di quello usato per l'autenticazione) ed è applicato a tutti i frame dati
  - Encrypta il payload (corpo del frame+CRC) di ciascun frame al livello MAC

26

S. Olivieri

## Data Delivery

---

- Il servizio di Data Delivery è simile a quello fornito da qualsiasi altra LAN IEEE 802
- Offre un servizio affidabile al livello MAC di distribuzione dei frame dati tra più stazioni minimizzando la duplicazione e l'ordinamento dei frame

27

S. Olivieri

## Servizi di distribuzione

---

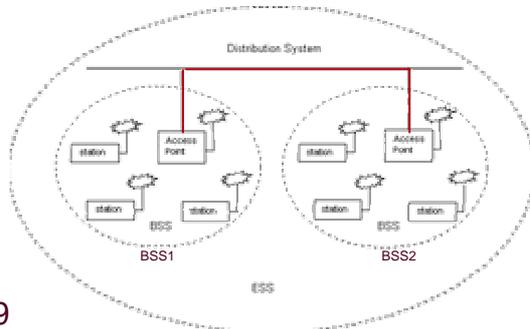
- Sono i servizi forniti dagli AP sul DS
  - Distribution
  - Integration
  - Servizi per il supporto alla mobilità
    - Association
    - Disassociation
    - Re-association

28

S. Olivieri

## Distribution

- È un servizio fornito dal DS che viene invocato tutte le volte che un frame transita attraverso il DS
- Ad esempio, se una stazione di BSS1 deve inviare un messaggio ad una stazione di BSS2, il servizio di Distribution si occupa dell'identificazione dell'AP appropriato
- 802.11f stabilisce i meccanismi specifici (IAPP) per il supporto del servizio di Distribution



29

S. Olivieri

## Integration

- Se il servizio di Distribution determina che il destinatario di un messaggio è membro di una LAN integrata con la WLAN, l'elemento a cui inviare il messaggio è il **Portal** invece che l'AP
  - Il Portal è un concetto architetturale astratto che tipicamente risiede in un AP ma che potrebbe essere parte di un componente di rete separato
- Il servizio di **Integration** viene invocato dal DS, successivamente all'invocazione del servizio di Distribution, per tutti i messaggi che devono essere distribuiti al portal
- Tale servizio fa tutto ciò che è richiesto per gestire la connessione fisica tra la WLAN e la LAN integrata
  - Traduce i frame 802.11 in frame che possono attraversare un'altra rete
  - Traduce frame provenienti da altre reti in frame che possono essere consegnati ad una WLAN 802.11

30

S. Olivieri

## Supporto alla mobilità

- Sono definiti dei servizi per supportare la **mobilità** delle stazioni all'interno di una rete
  - La mobilità è una proprietà specifica delle reti wireless che consente alle stazioni di muoversi restando connesse alla rete e di trasmettere frame in movimento
- In 802.11 ci sono tre tipi di transizioni che una stazione può compiere
  - **No-transition**: assenza di movimento, o limitato all'interno dello stesso BSS
  - **BSS-transition**: movimento di una stazione da un BSS ad un altro appartenenti allo stesso ESS
  - **ESS-transition**: movimento da un BSS ad un altro di ESS diversi

31

S. Olivieri

## Association

- È utilizzato per creare una connessione logica tra una stazione mobile ed un AP in modo che il DS sappia a quale AP rivolgersi per poter raggiungere una stazione destinataria
- Ciascuna stazione deve associarsi ad un AP prima di poter inviare dati al DS attraverso l'AP
- La stazione invoca l'associazione solo una volta, tipicamente quando entra nella BSS
- Ciascuna stazione può associarsi ad un solo AP
- Ad un AP possono essere associate più stazioni
- È un servizio necessario (ma non sufficiente) per il supporto della BSS-transition e sufficiente per il supporto della no-transition

32

S. Olivieri

## Re-association

---

- Consente ad una stazione di cambiare la sua attuale associazione con un altro AP
- È usato quando una stazione mobile esce dal BSS, perde il contatto con l'AP a cui è associato ed ha bisogno di associarsi ad un nuovo AP di un altro BSS
- Tale servizio è simile a quello di associazione, con l'eccezione che include l'informazione sull'AP con cui è stato precedentemente associato, in modo che il DS è sempre informato sulla mappatura tra stazione ed AP in fase di mobilità
  - Il nuovo AP può contattare il precedente AP per ricevere frame che potrebbero essere in attesa di essere inviati alla stazione mobile
- Combinato con l'association, è sufficiente per il supporto della BSS-transition

33

S. Olivieri

## Disassociation

---

- Tale servizio è usato
  - Da una stazione mobile per informare l'AP che non ha più bisogno dei servizi del DS
  - Da un AP per forzare una stazione ad eliminare l'associazione
    - A causa di limitazioni di risorse
    - Perché l'AP sta facendo uno shut down
- Il servizio di disassociation è una notifica e può essere invocato da uno dei due apparati in comunicazione
  - Nessuno dei due può rifiutare la terminazione dell'associazione
- Quando una stazione si dissocia, deve cominciare una nuova associazione per poter comunicare di nuovo con un AP

34

S. Olivieri

## Parte 3

---

- Definizione e caratteristiche delle WLAN
- Architettura, topologie di rete e servizi dello standard IEEE 802.11
- ☞ Tecnologie e protocolli dello strato fisico 802.11/a/b/g

35

S. Olivieri

## Funzioni dello strato fisico IEEE 802.11

---

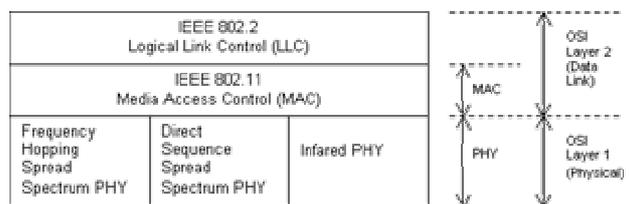
- Fornire un'interfaccia per lo scambio di frame con lo strato MAC per la trasmissione e la ricezione dei dati
- Fornire al MAC un'indicazione sull'attività del mezzo (meccanismo di carrier sense fisico)
- Trasmettere fisicamente i frame attraverso il mezzo fisico nella banda di frequenze assegnata

36

S. Olivieri

## Proprietà del PHY di IEEE 802.11

- Lo standard 802.11 definisce tre tecnologie (diverse tra di loro e quindi non interoperabili) ad 1 e 2 Mbit/sec nella banda a 2.4 GHz
  - Frequency Hopping Spread Spectrum (FHSS)**
  - Direct Sequence Spread Spectrum (DSSS)**
  - Infrarossi



37

S. Olivieri

## Estensioni del PHY IEEE 802.11

- 802.11b** è l'estensione del PHY 802.11 nella banda a 2.4 GHz per il supporto di 5.5 e 11 Mbit/sec, in tecnologia DSSS
- 802.11a** è l'estensione del PHY 802.11 nella banda a 5 GHz per il supporto fino a 54 Mbit/sec, in tecnologia Orthogonal Frequency Division Multiplex (OFDM)
- 802.11g** è l'estensione del PHY 802.11 nella banda a 2.4 GHz per il supporto fino a 54 Mbit/sec, in tecnologia OFDM, compatibile con 802.11b

38

S. Olivieri

## Architettura del PHY 802.11(a/b/g)

- Il PHY di IEEE 802.11 è diviso in due parti
  - Il sottostrato **Physical Medium Dependent (PMD)**
    - Definisce le caratteristiche e la metodologia di trasmissione e ricezione dei dati attraverso il mezzo radio tra due o più stazioni in base alle caratteristiche della specifica tecnologia usata (DSSS, FHSS, infrarossi, OFDM)
  - Il sottostrato **Physical Layer Convergence Protocol (PLCP)**
    - Mappa i frame del MAC in frame adatti per la trasmissione e ricezione dei dati e delle informazioni di gestione tra due o più stazioni utilizzando lo specifico sistema PMD

39

S. Olivieri

## Regolamentazione dello spettro

- In ogni area geografica, l'uso dello spettro di frequenze radio è regolato da organizzazioni
  - **FCC** in America del Nord
  - **ETSI** in Europa
- Tali organizzazioni definiscono l'allocazione di ciascuna banda di frequenze (TV, radio, telecomunicazioni, forze armate,...)
- Lo spettro è una risorsa scarsa, e per poter usare una banda di frequenze, bisogna quindi
  - Negoziare con tali organizzazioni
  - Registrare la propria architettura
  - Acquistare il diritto per l'uso delle frequenze

40

S. Olivieri

## Le bande ISM

---

- Le organizzazioni hanno allocato le bande di frequenza **ISM** (Industrial, Scientific and Medical) a 900 MHz e a 2.4 GHz (80 MHz di banda a 2.40÷2.48 GHz) per le comunicazioni di utenti individuali
  - La banda a 2.4 GHz è disponibile ovunque nel mondo
  - FCC alloca sia la banda a 900 MHz che quella a 2.4 GHz
  - ETSI alloca solo la banda a 2.4 GHz (la banda a 900 MHz in Europa è usata per il GSM)
- Queste bande sono *non licenziate*, l'utente cioè è libero di utilizzarle senza doversi registrare o pagare nulla
  - Per il fatto che le bande ISM sono libere, soffrono dell'inquinamento derivante da altri sistemi operanti nelle stesse bande
  - La banda a 2.4 GHz soffre anche delle radiazioni dei forni a microonde (le particelle d'acqua risuonano a questa frequenza) e ciò spiega perchè questa banda è stata concessa gratis...

41

S. Olivieri

## Normativa italiana su WLAN a 2.4 GHz

---

- Il decreto Gasparri del 28/05/03 in pratica consente solo agli operatori telefonici di fornire connettività ad Internet tramite WLAN su **suolo pubblico**, con l'obbligo di autenticazione degli utenti, accounting, conservazione dei log per 5 anni ecc.
- Un privato non può fornire servizi di questo tipo, neanche gratuitamente, ma è libero di utilizzare le WLAN su **suolo privato**

42

S. Olivieri

## Regole per le bande ISM

---

- Per evitare abusi, le organizzazioni hanno comunque imposto delle regole per queste bande, e solo i prodotti conformi con queste regole possono emettere in tali bande
  - Uso della tecnica di **Spread Spectrum** (FHSS o DSSS)
  - Limiti sulla massima potenza trasmessa in banda e sulle emissioni fuori banda per limitare l'inquinamento dei sistemi adiacenti nello spettro
    - FCC impone 1 W sulle bande a 900 MHz e 2.4 GHz
    - ETSI impone 100 mW sulla banda a 2.4 GHz
  - Definizione dei canali per garantire la coesistenza tra sistemi

43

S. Olivieri

## Spread Spectrum

---

- Il segnale è sparpagliato, a pari potenza totale, su una banda più ampia di quanta realmente necessaria per la trasmissione
- In questo modo si riduce l'efficienza del sistema perché non si utilizza l'intera capacità di banda

44

S. Olivieri

## Vantaggi dello Spread Spectrum

---

- Impedendo a ciascun sistema di usare l'intera capacità di banda, sistemi indipendenti possono essere sovrapposti nella stessa banda con un impatto trascurabile sulle prestazioni
- Viene ridotto l'impatto sul sistema di interferenze localizzate
  - Si ha maggiore robustezza in ambienti disturbati
- Si riduce il **delay spread** dovuto al multipath
  - Si garantiscono prestazioni migliori in ambienti dove il multipath è maggiormente accentuato (ad es. ambienti indoor), con un aumento del raggio d'azione e del rate raggiungibile

45

S. Olivieri

## Frequency Hopping Spread Spectrum

---

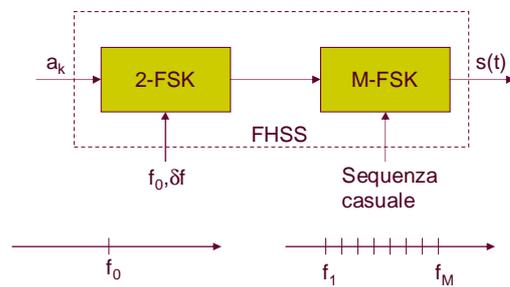
- Anziché trasmettere un segnale in corrispondenza di una certa frequenza, il FHSS usa un insieme di canali stretti e salta su ciascuno di essi seguendo un predeterminato pattern di hopping ciclico pseudocasuale
  - L'hopping sui canali produce il desiderato sparpagliamento del segnale trasmesso
  - L'effetto di eventuali canali disturbati viene mediato nel tempo

46

S. Olivieri

## Architettura di un sistema FHSS

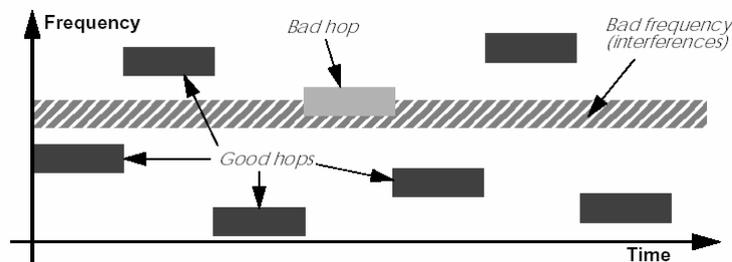
- Il FHSS può essere visto come un sistema di modulazione a due stadi
  - Il primo stadio è uno schema di modulazione numerica (FSK nel caso 802.11)
  - Il secondo stadio può essere visto come un M-FSK in cui la frequenza portante viene selezionata in modo pseudo-random fra una delle M frequenze disponibili



S. Olivieri

## Effetto di interferenze a banda stretta

- In caso di interferenze a banda stretta, il FHSS è disturbato solo in corrispondenza di alcuni salti



S. Olivieri

## Proprietà del Frequency Hopping

- Lo sparpagliamento (**spreading**) è eseguito direttamente nel dominio delle frequenze
- ⊙ Il FHSS occupa nel tempo solo una porzione dello spettro per volta
  - Diversi sistemi FHSS (aventi sequenze di hopping ortogonali) possono coesistere nella stessa banda di frequenze
- ⊙ La gestione al livello MAC risulta abbastanza complicata, perché si deve
  - trovare la rete in fase di inizializzazione (salta di continuo da una frequenza all'altra)
  - Mantenere la sincronizzazione tra i nodi
  - Gestire le sequenze di hopping
- ⊙ Il FHSS è soggetto ad overhead dovuto
  - Alla gestione della sincronizzazione
  - Ai tempi morti nella trasmissione quando il sistema salta

49

S. Olivieri

## Caratteristiche del FHSS per 802.11

- Per il FHSS, la regolamentazione impone che
  - La banda ISM sia divisa in 79 canali da 1 MHz
  - Si può rimanere su un canale per un tempo massimo di 0.4 sec ed usare almeno 75 canali diversi in un periodo di 30 sec
- Il segnale FHSS 802.11 è trasmesso ad 1 MSymb/sec
  - Il caso 1 Mbit/sec è ottenuto usando la modulazione 2-GFSK
  - Il caso 2 Mbit/sec è ottenuto usando la 4-GFSK

50

S. Olivieri

## Direct Sequence Spread Spectrum

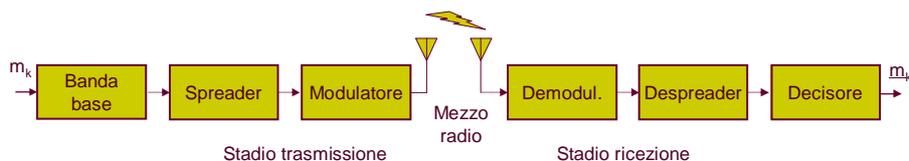
- Il segnale viene sparpagliato su una banda di frequenze più larga di quella originariamente occupata mediante moltiplicazione con un particolare codice rappresentato da un pattern periodico di rate maggiore di quello del segnale
- In ricezione, il segnale originale è recuperato rilevando l'intero segnale sparpagliato e demultiplandolo con lo stesso codice

51

S. Olivieri

## Architettura di un sistema DSSS

- Stadio trasmissione
  - Si genera un segnale in banda base come sequenza di rettangoli
  - Lo spreader sparpaglia il segnale in banda base
  - Il modulatore converte il segnale banda base in ingresso in un segnale in banda radio
- Stadio ricezione
  - Il demodulatore estrae il segnale in banda base
  - Il despreader recupera il segnale originale
  - Il decisore estrae i messaggi da consegnare alla destinazione

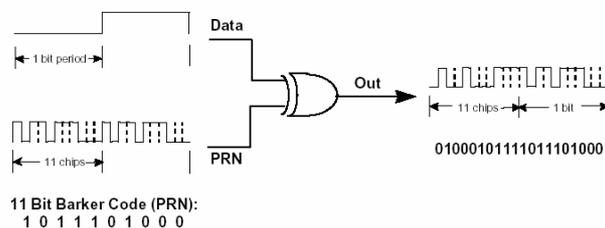


52

S. Olivieri

## Spreading del segnale per moltiplicazione

- Il segnale spread-spectrum è formato moltiplicando ciascun bit, rappresentato da un rettangolo di durata  $T$ , con una sequenza di  $N$  impulsi stretti di durata  $T_c < T$  chiamati **chips**
  - La banda del segnale moltiplicato risulta estesa di un fattore  $G=T/T_c$  (**processing gain**)
  - L'altezza dello spettro del segnale è  $G$  volte minore essendo la potenza distribuita su una banda  $G$  volte più larga



53

S. Olivieri

## Robustezza in presenza di multipath

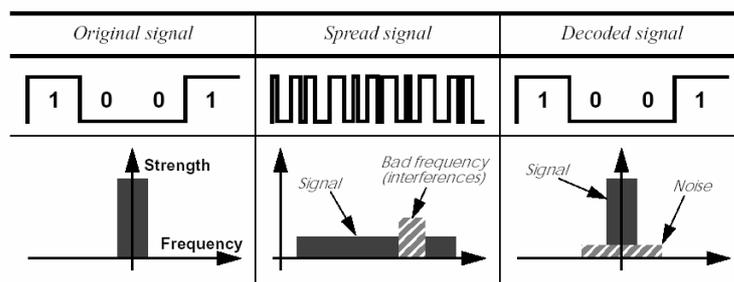
- In presenza di cammini multipli, il ricevitore si sincronizza con il primo segnale ricevuto ed esegue il despreading
- Le riflessioni successive non sono sincronizzate con il ricevitore, e sono viste come delle interferenze ridotte di un fattore pari al processing gain

54

S. Olivieri

## Immunità ad interferenze a banda stretta

- Un'interferenza a banda stretta in ricezione appare molto più debole del segnale, perché in aria occupa solo una piccola parte della banda totale usata dal sistema
- L'immunità alle interferenze in banda è tanto maggiore quanto maggiore è il processing gain



55

S. Olivieri

## Proprietà del Direct Sequence

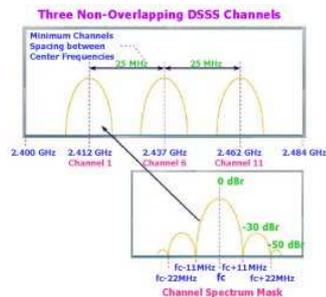
- Lo spreading è eseguito nel dominio del tempo
- Il DSSS usa un intero canale per tutta la durata della trasmissione
- ☺ Il fatto di lavorare su un singolo canale statico nel tempo (al contrario del Frequency Hopping) agevola il MAC
- ⊗ La moltiplicazione con il codice per effettuare lo spargimento è abbastanza complicato
  - Sono necessari circuiti più veloci ed un DSP per effettuare lo spreading

56

S. Olivieri

## Regolamentazione per il DSSS 802.11

- Il processing gain del DSSS deve essere  $\geq 10$  dB
- La banda a 2.4 GHz è suddivisa in 14 canali
- Ciascun canale occupa 22 MHz di banda
  - È possibile allocare al massimo tre canali non sovrapposti



57

S. Olivieri

## Caratteristiche del DSSS per 802.11

- Spreading
  - il DSSS 802.11 usa una sequenza ad 11 chip, detta di Barker, per garantire il vincolo sul processing gain
  - Ciascun bit è associato ad una intera sequenza di Barker (un simbolo)
- Modulazione
  - il segnale modulato è trasmesso alla velocità  $R_s = 1/T = 1\text{MSymb/sec}$
  - Il caso 1 Mbit/sec si ottiene usando la modulazione DBPSK (*Differential Binary Phase Shift Keying*, cioè 2-PSK differenziale)  
( $1 \times 1\text{MSymb/sec} = 1\text{Mbit/sec}$ )
  - Il caso 2 Mbit/sec si ottiene usando la modulazione DQPSK (*Differential Quadrature Phase Shift Keying*, cioè 4-PSK differenziale)  
( $2 \times 1\text{MSymb/sec} = 2\text{Mbit/sec}$ )
- Occupazione in banda
  - Il segnale, in banda traslata, in assenza di spreading occuperebbe una banda di  $2 \times 1/T = 2 \times 10^6 = 2\text{ MHz}$
  - La banda occupata dal segnale DSSS per effetto dello spreading è quindi di  $2 \times 11 = 22\text{ MHz}$

58

S. Olivieri

## Caratteristiche del DSSS per 802.11b

- Spreading
  - Al posto della sequenza di Barker, 802.11b utilizza una tecnica di codifica chiamata Complementary Code Keying (CCK)
  - Il CCK consiste in un set di 64 parole di codice da 8 chip complessi (parte reale e parte immaginaria) con un chipping rate di 11 Mchip/sec
  - Un insieme di  $N$  bit di informazione è mappato in una parola di codice (un simbolo) scelta tra le 64 possibili
- Modulazione
  - Il segnale modulato è trasmesso ad una velocità di 1.375 MSymb/sec con modulazione DQPSK
  - Il caso 5.5 Mbit/sec si ottiene mappando 4 bit d'informazione con un simbolo CCK ( $4 \times 1.375 \text{ MSymb/sec} = 5.5 \text{ Mbit/sec}$ )
  - Il caso 11 Mbit/sec si ottiene mappando 8 bit d'informazione con un simbolo CCK ( $8 \times 1.375 \text{ MSymb/sec} = 11 \text{ Mbit/sec}$ )
- Occupazione in banda
  - La banda occupata dal segnale modulato è ancora  $2 \times 8 \times 1.375 = 22 \text{ MHz}$

59

S. Olivieri

## Specifiche del rate dati per 802.11b

Data Rate (Mbit/sec)	Lunghezza codice	Modulazione	Symbol Rate (MSymb/sec)	Bit/Simbolo
1	11 (Seq. Barker)	DBPSK	1	1
2	11 (Seq. Barker)	DQPSK	1	2
5.5	8 (CCK)	DQPSK	1.375	4
11	8 (CCK)	DQPSK	1.375	8

60

S. Olivieri

## Dynamic Rate Shifting

- È un meccanismo del PHY di 802.11b che consente di modificare automaticamente la velocità di trasmissione dei dati al fine di compensare le variazioni del canale
  - Il rate varia in funzione della
    - Attenuazione dovuta alla distanza tra la stazione e l'access point (potenza, fattore al numeratore del SNR)
    - entità delle interferenze (rumore, fattore al denominatore del SNR)
- Tale tecnica è trasparente all'utente ed agli strati superiori dello stack di protocolli

61

S. Olivieri

## Lo standard IEEE 802.11a

- Molti dispositivi wireless attualmente presenti nel mercato lavorano nella banda a 2.4 GHz, che quindi sta diventando via via più affollata
- La versione 802.11a, basata su tecnologia **Orthogonal Frequency Division Multiplexing** (OFDM), è stata standardizzata nella banda a 5 GHz con l'obiettivo di ottenere
  - Maggiore immunità ad interferenze
  - Maggiore scalabilità
  - Rate più elevati (fino a 54 Mbit/sec)

62

S. Olivieri

## Bande libere a 5 GHz

- L'ETSI ha allocato
  - La banda a 5.2 GHz solo per il sistema HiperLan
  - La banda a 5.4 GHz solo per HiperLan II (BRAN)
- L'FCC ha allocato la banda **UNII** (Unlicensed National Information Infrastructure) costituita da 300 MHz di banda tra 5.2 e 5.8 GHz con regole abbastanza libere
  - Rilassamento del requisito sulla coesistenza (nessun obbligo di usare lo Spread Spectrum)
  - Limiti solo sull'uso della potenza

63

S. Olivieri

## Proprietà delle bande a 5 GHz

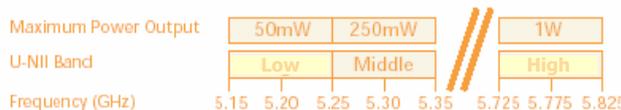
- ⊙ Pochi sistemi utilizzano la banda a 5 GHz
    - Diminuisce il problema delle interferenze
  - ⊙ Maggiore disponibilità di banda
    - È possibile realizzare sistemi più veloci
  - ⊙ Ad una frequenza più alta è richiesta maggiore potenza in trasmissione perché
    - Aumenta l'attenuazione in spazio libero
    - Aumenta il livello di rumore
    - Gli ostacoli ed i muri sono più opachi alle trasmissioni
- Il raggio d'azione è inferiore rispetto ai sistemi a 2.4 GHz
- Gli AP vanno disposti più densamente di un fattore pari a circa 1.5

64

S. Olivieri

## La banda UNII

- I 300 MHz sono suddivisi in tre domini da 100 MHz ciascuno con un diverso valore per la massima potenza in uscita
  - Potenza max 50 mW per la banda “low” a 5.15 - 5.25 GHz
  - Potenza max 250 mW per la banda “middle” a 5.25 - 5.35 GHz
  - Potenza max 1 W per la banda “high” a 5.725 – 5.825 GHz
- I dispositivi nella banda “high” sono prevalentemente prodotti outdoor (Wireless Distribution Systems), mentre quelli in banda “middle” e “low” sono prodotti indoor



65

S. Olivieri

## Situazione europea per IEEE 802.11a

- Poiché le normative non prevedono l'uso di 802.11a in Europa, IEEE ed ETSI hanno definito congiuntamente delle versioni europee
- IEEE 802.11g è un sistema a 54 Mbit/sec nella banda a 2.4 GHz basato su OFDM
- IEEE 802.11h è un'evoluzione di 802.11a, con funzionalità richieste da ETSI per garantire la coesistenza in Europa con Hiperlan II
  - Transmission Power Control (TPC), per limitare la potenza in trasmissione solo quando serve
  - Dynamic Frequency Selection (DFS), per evitare di occupare frequenze già in uso

66

S. Olivieri

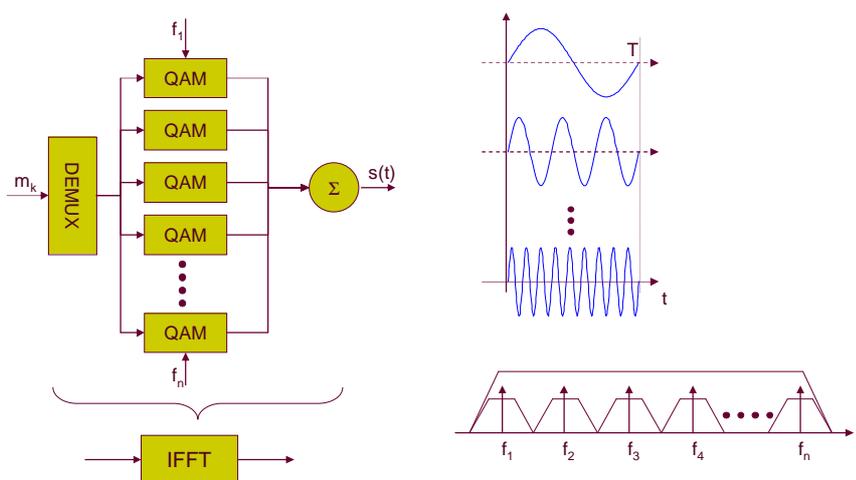
## La modulazione OFDM

- Usa un insieme di **sottoportanti** (segnali sinusoidali adiacenti in frequenza), ciascuna delle quali è modulata individualmente
- Il rate di trasmissione e la potenza di ciascuna sottoportante può variare in funzione della qualità del canale per quella frequenza (scalabilità), in modo da massimizzare le prestazioni del sistema
  - Ad esempio si possono trasmettere più bit d'informazione nelle frequenze buone e meno bit in quelle cattive
- Le sottoportanti sono trasmesse in parallelo sovrappoendole nel tempo in modo da generare un unico segnale che viene trasmesso sul canale
  - I dati trasportati da ciascuna sottoportante sono quindi inviati e ricevuti simultaneamente
- L'unità ricevente elabora separatamente i segnali associati a ciascuna sottoportante per ricostruire poi l'intera sequenza dei dati della sorgente

67

S. Olivieri

## Schema di principio di un modulatore OFDM



68

S. Olivieri

## Proprietà della modulazione OFDM

- ⊙ Contrasta in modo intrinseco il delay spread, offrendo benefici in termini di prestazioni rispetto allo Spread Spectrum
  - E' relativamente semplice equalizzare in frequenza l'effetto del multipath agendo su ciascuna sottoportante
  - Si riescono ad ottenere elevate velocità in trasmissione senza diminuire il tempo di simbolo, ma sovrapponendo nel tempo le sottoportanti sinusoidali, che invece sono separate nel dominio delle frequenze
  - Il segnale OFDM quindi, a parità di efficienza spettrale, è costituito da simboli con una durata nel tempo maggiore rispetto ai comuni sistemi di modulazione digitale
- ⊙ A differenza dello Spread Spectrum, è soggetto a degrado delle prestazioni in presenza di disturbi in banda

69

S. Olivieri

## Componenti dello strato fisico di 802.11a

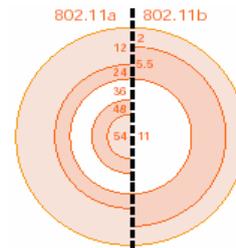
- Codifica di canale
  - Usa un codice convoluzionale con rate 1/2, 2/3 o 3/4
- Modulazione delle sottoportanti
  - Si usa uno dei quattro schemi di modulazione (BPSK, QPSK, 16QAM, 64QAM)
  - Combinando opportunamente modulazione e codifica di canale si ottengono otto diverse modalità di trasmissione
- Modulazione OFDM
  - Si usano 52 portanti (48 per i dati e 4 di servizio), ciascuna delle quali occupa una banda approssimativamente di 300 KHz (0.3125 MHz)
  - La durata del simbolo OFDM è di 4 μsec
  - La banda occupata dal segnale è di 16.6 MHz

70

S. Olivieri

## Rate dati e raggio d'azione di 802.11a

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N <sub>BPSK</sub> )	Coded bits per OFDM symbol (N <sub>CBPS</sub> )	Data bits per OFDM symbol (N <sub>DBPS</sub> )
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

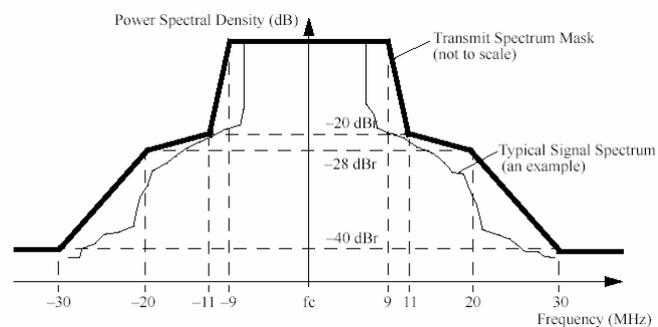


71

S. Olivieri

## Maschera dello spettro del segnale

- Il segnale deve soddisfare dei requisiti in termini di potenza definiti da una opportuna maschera



72

S. Olivieri

## Canalizzazione per 802.11a

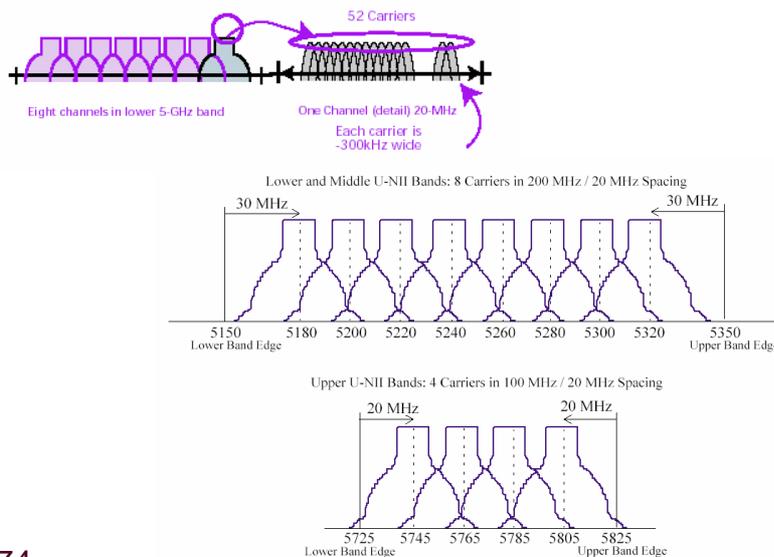
- Per la trasmissione del segnale, sono definiti otto canali non sovrapposti da 20 MHz nelle due bande inferiori, e quattro canali da 20 MHz nella banda superiore

Regulatory domain	Band (GHz)	Operating channel numbers	Channel center frequencies (MHz)
United States	U-NII lower band (5.15–5.25)	36	5180
		40	5200
		44	5220
		48	5240
United States	U-NII middle band (5.25–5.35)	52	5260
		56	5280
		60	5300
		64	5320
United States	U-NII upper band (5.725–5.825)	149	5745
		153	5765
		157	5785
		161	5805

73

S. Olivieri

## Allocazione dei canali OFDM



74

S. Olivieri

## Demo – Video Streaming

---

- Streaming server
    - Windows XP su Intel Pentium III 700 MHz
    - MPEG, DivX
  - Streaming client
    - Familiar Linux su Compaq Ipaq 3760
  - Protocolli
    - Trasporto su UDP
    - Connessione punto-punto tra server e client su 802.11b in modalità ad-hoc
-