CORSO DI TECNOLOGIE D'ACCESSO

WiFi (Wireless Fidelity)

Wireless Fidelity

- ✓ Cosa è WiFi ?
- ✓ Perché WiFi
- ✓ Tecniche di accesso
- ✓ Modulazioni
- ✓ Evoluzioni
- ✓ Sicurezza su WiFi
- ✓ Limiti di esposizione

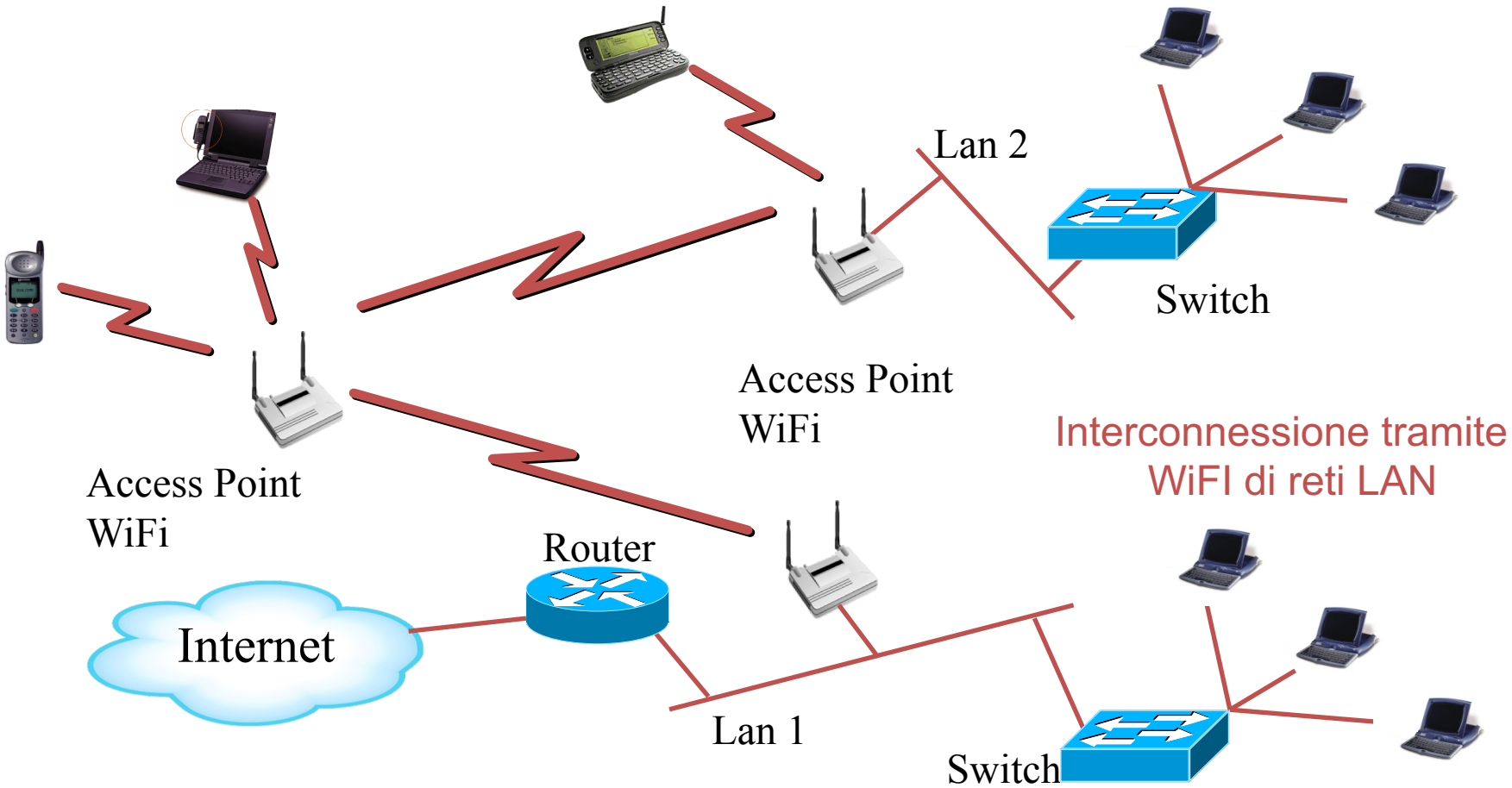
Cosa è WiFi ?

- ✓ Nel 1997 nasce il primo standard IEEE 802.11 che detta le specifiche a livello fisico e datalink per l'implementazione di reti LAN wireless (senza fili)
- ✓ WiFi (Wireless Fidelity) è un protocollo di trasmissione per il supporto di reti che trasmettono dati in modalità wireless ad alta velocità attraverso la trasmissione di onde radio
- ✓ Utilizza serie di tecniche di modulazione half-duplex che utilizzano lo stesso protocollo di base.
- ✓ La famiglia di protocolli 802.11 utilizza l'accesso multiplo con CSMA-CA, per cui ogni dispositivo ascolta un canale per rilevare l'eventuale presenza di altri utenti (inclusi utenti non 802.11) prima di trasmettere ciascun pacchetto.
- ✓ Una rete wireless può essere un'estensione di una normale rete cablata fornendo mediante un Access Point (AP) la connessione a dispositivi mobili

Cosa è WiFi ?

- ✓ L'architettura di una rete Wireless generalmente è basata su due tipologie di dispositivi:
  - **Access Point**: bridge che collegano la sottorete wireless con quella cablata, possono essere implementati via hardware oppure via software, sono equipaggiate con antenne omnidirezionali o direzionali per aumentarne la portata
  - **Wireless terminal**: dispositivi che usufruiscono dei servizi di rete (PC, Tablet, Smartphone)
- ✓ Ogni strumento deve essere posto in maniera tale da ottimizzare le risorse all'interno di un'area che può raggiungere i 100 m nei locali chiusi e 400 m all'aperto

Esempio di Rete



Perché WiFi

- ✓ I vantaggi legati all'utilizzo di una rete WiFi piuttosto che una rete cablata sono numerosi:
  - Mobilità: accesso ad internet ad alta velocità in tutti i locali coperti dal servizio
  - Flessibilità: libera gestione delle postazioni di lavoro, possibilità di accedere alla rete anche in ambienti caratterizzati da una logistica complessa (vecchi edifici piuttosto che monumenti storici) che renderebbero difficile il cablaggio
  - Velocità: data rate dell'ordine dei Mbps
  - Risparmio: minori costi di installazione e manutenzione in seguito alla totale assenza dei cavi e dei lavori di cablatura
  - Semplicità: dopo l'autenticazione, tramite username e password, si può navigare liberamente sulla rete
  - Scalabilità: permette di sviluppare gradualmente le aree che si intendono coprire col servizio Wireless
  - Coesistenza: il servizio WiFi è totalmente compatibile con quello radiomobile. Sono in continuo sviluppo strumenti portatili che consentono di scegliere in ogni luogo la tecnologia più veloce tra quelle disponibili al momento o che più si adattano alle abitudini del singolo utente.

Tecniche di accesso

- ✓ La trasmissione elettromagnetica è fatta seguendo tecniche d'accesso *spread spectrum* che in linea di principio limitano la velocità massima nella banda 2.4 GHz a 2Mbps per l'802.11 versione base.

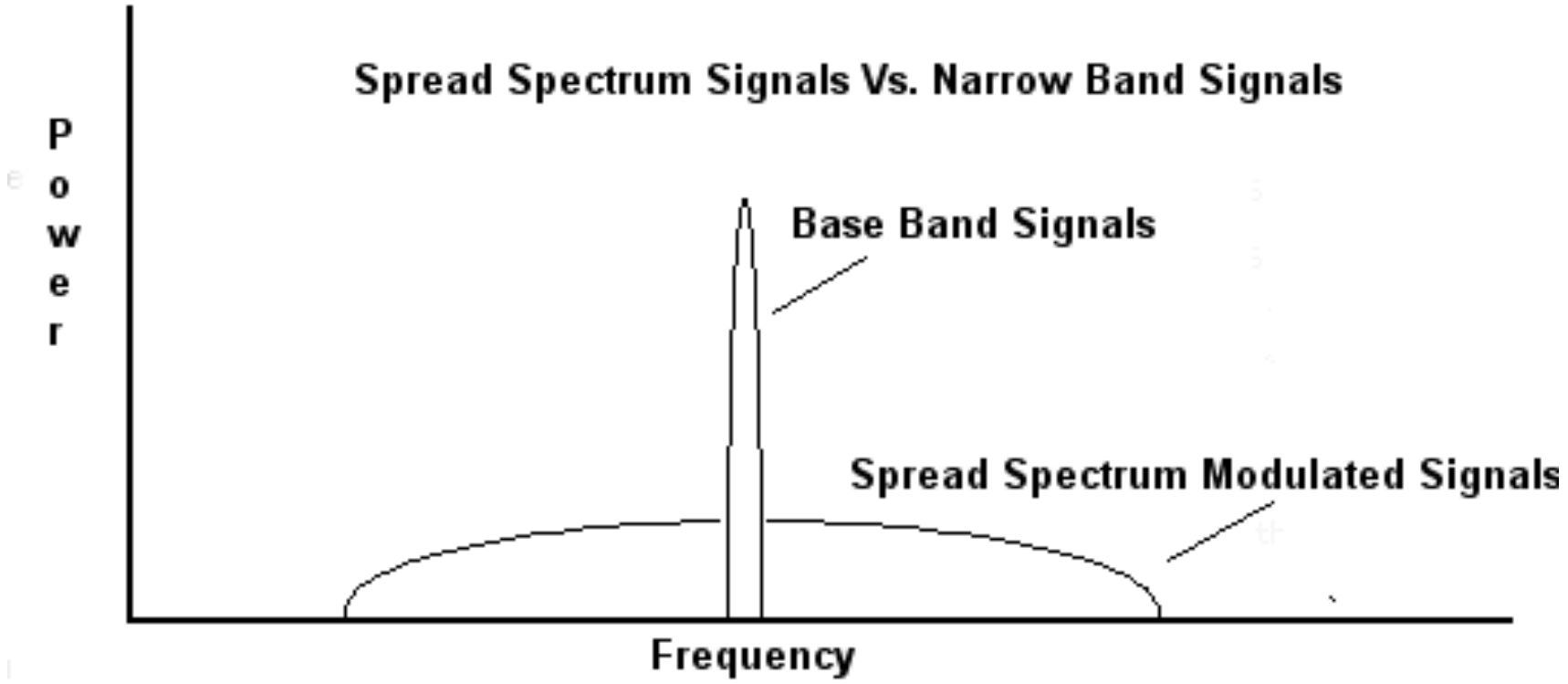
- ✓ A seconda della versione dello standard IEEE 802.11 viene utilizzata una o più tecniche d'accesso

- ✓ L'utilizzo di modulazioni più complesse (OFDM) porta il data rate fino a 9.6 Gbps (Wi-Fi 6)

Spread Spectrum

- ✓ Trasmissione “tradizionale”: più potenza possibile nello spettro più stretto possibile
- ✓ Uso di “trasformazioni matematiche” per disperdere lo spettro originale del segnale da trasmettere in uno spettro molto più largo
- ✓ L’operazione inversa deve essere svolta in ricezione

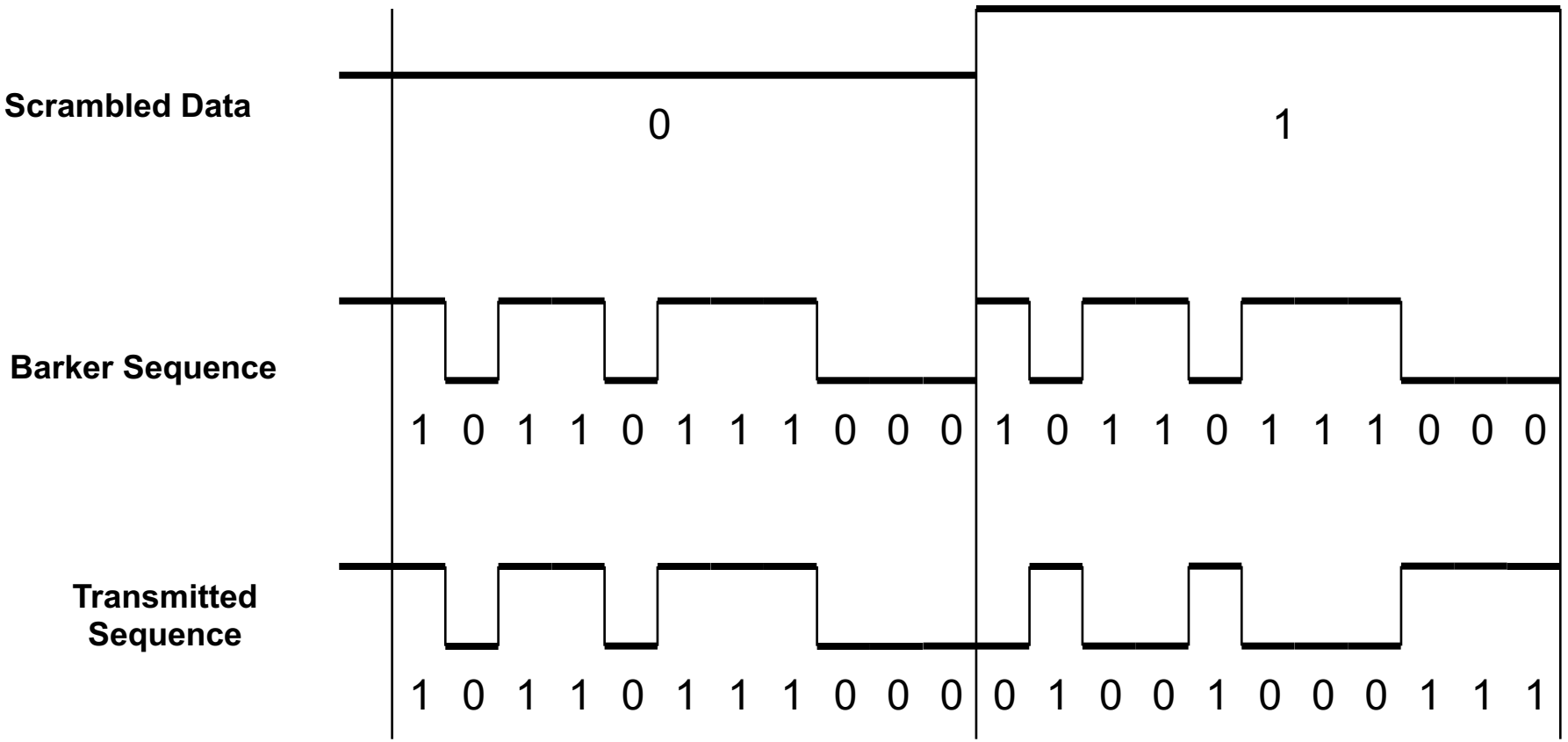
Spread Spectrum



FHSS

- ✓ La tecnica ***Frequency Hopping Spread Spectrum*** ottiene la dispersione dello spettro mediante la variazione rapidissima della frequenza di trasmissione con andamento pseudo-casuale.
- ✓ TX e RX devono essere perfettamente sincronizzati e conoscere la sequenza pseudo-casuale delle frequenza di trasmissione.
- ✓ Non è più utilizzate nelle apparecchiature Wireless fidelity in commercio
- ✓ Esiste anche una tecnica Time hopping (THSS) analoga alla FHSS che trasmette in slot temporali in maniera pseudo-casuale

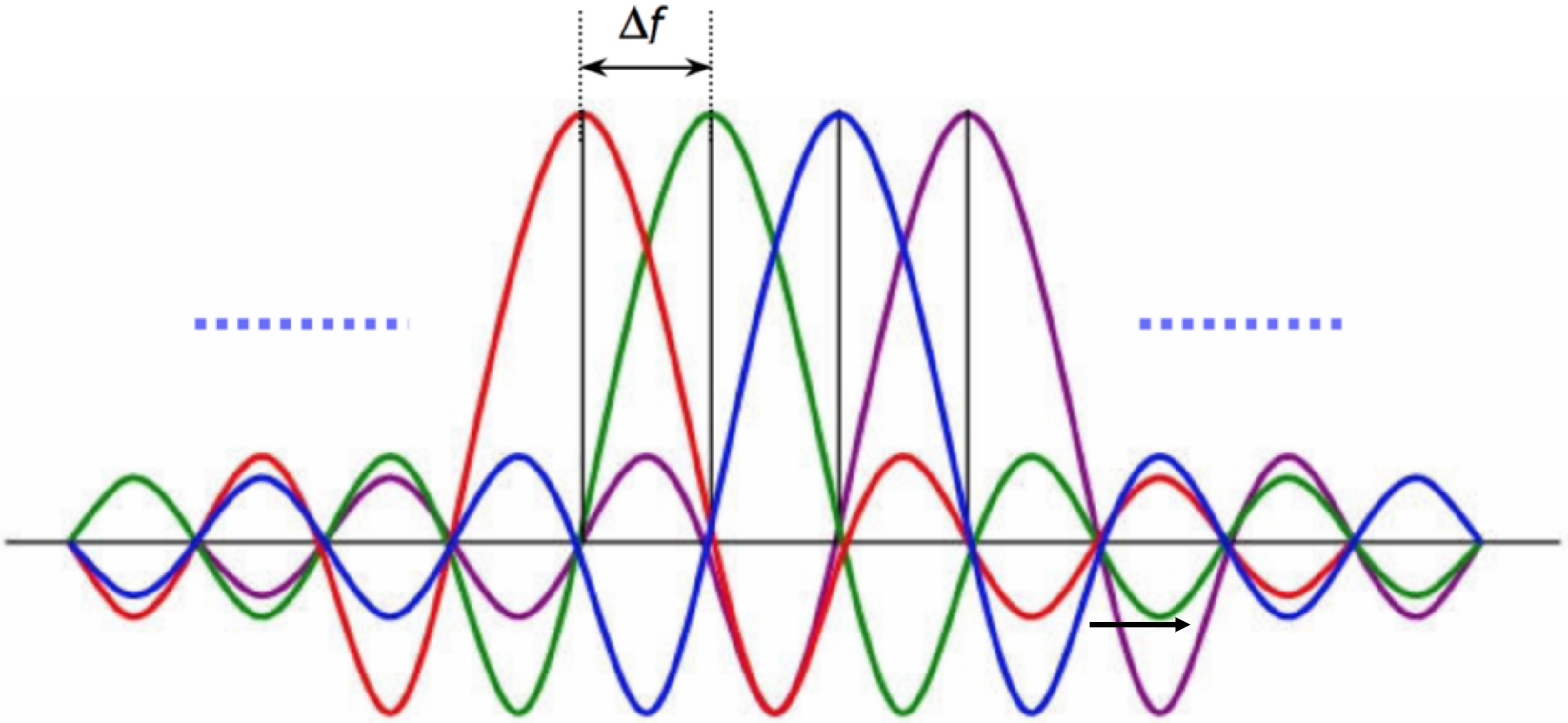
DSSS


Scrambled Data
0
1
Barker Sequence
1 0 1 1 0 1 1 1 0 0 0 1 0 1 1 0 1 1 1 0 0 0
Transmitted Sequence
1 0 1 1 0 1 1 1 0 0 0 0 1 0 0 1 0 0 0 1 1 1

OFDM

- ✓ L'idea fondamentale della modulazione OFDM (Orthogonal Frequency Division Multiplexing) consiste nello scomporre il flusso dei dati da trasmettere (Rbit/s) in N flussi paralleli da trasmettere mediante un insieme di portanti
- ✓ La spaziatura tra le portanti ΔF deve essere tale da non avere interferenza mutua tra i flussi (ortogonalità delle portanti)
- ✓ L'ortogonalità si ha se la durata T_s=N/R dei simboli trasmessi dalle sottoportanti è legata alla spaziatura tra le portanti dalla relazione ΔF=1/ T_s
- ✓ Questa tecnica di trasmissione su più sottoportanti risulta particolarmente efficace nei canali selettivi in frequenza (Fading)

OFDM



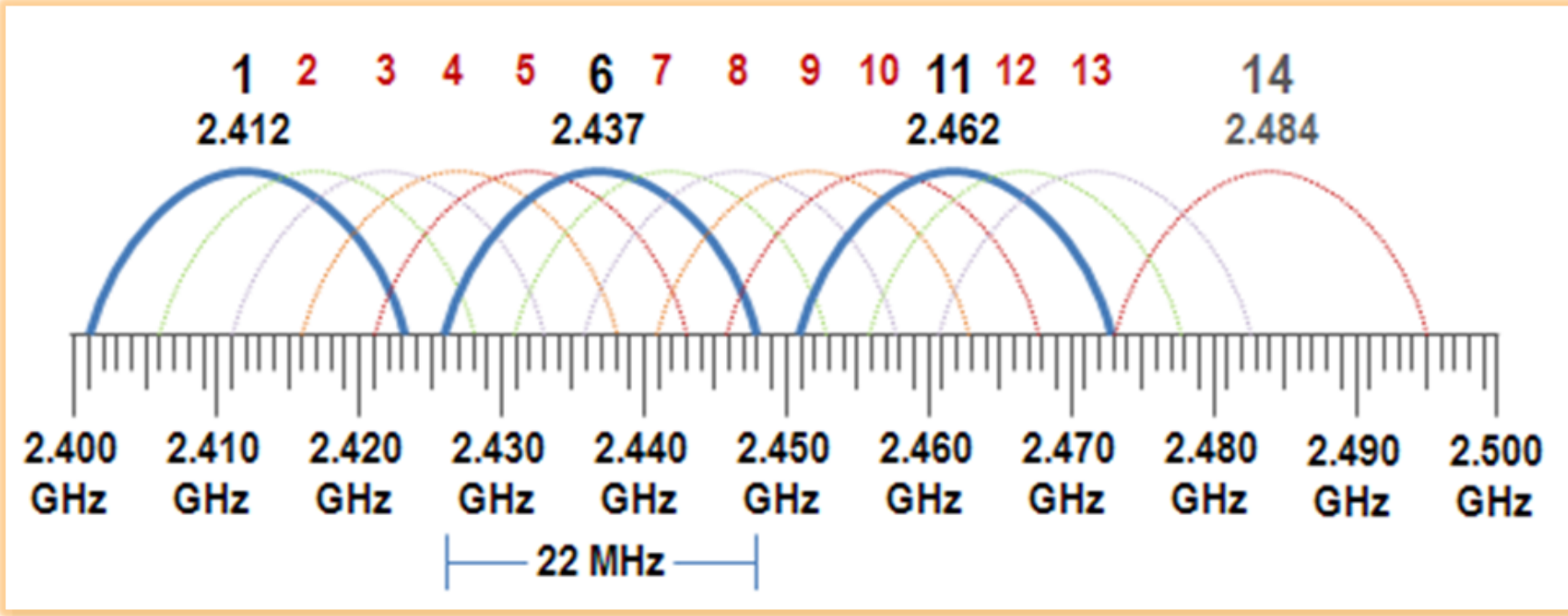
OFDM

- ✓ Le sottoportanti sono ortogonali sull'intervallo di tempo T_s che si sta considerando dunque i segnali di informazione possono essere estratti senza interferenza mutua tra gli N canali in parallelo
- ✓ Il segnale così costruito andrà poi traslato in frequenza nella banda del canale trasmissivo mediante una modulazione opportuna con una opportuna portante f_0
- ✓ Questo tipo di trasmissione può essere realizzata efficientemente con tecniche di elaborazione numerica che consentono di ridurre la complessità computazionale

IEEE 802.11b

- ✓ Lo standard 802.11b utilizza le frequenze della banda a 2.4 GHz
- ✓ Canali da 22 MHz non sovrapposti
- ✓ 802.11b lavora nei 2.4 GHz ed è limitato dai 3 canali non sovrapposti
- ✓ CSMA/CA
- ✓ DSSS con data rate scalabili (1-2-5.5-11 Mbps)

Allocazione dei canali-802.11b



IEEE 802.11g

- ✓ Lo standard **802.11g** utilizza le frequenze della banda a 2.4 GHz ed è in grado di trasmettere con data-rate teorici da 1 a 54 Mbps
- ✓ Come l'802.11b lavora nei 2.4 GHz ed è limitato dai 3 canali non sovrapposti da 20 MHz
- ✓ OFDM per trasmettere i dati e in questo modo è in grado di garantire alti data-rate usando modulazioni sino a 64 QAM
- ✓ Combinando tecniche di trasmissione DSSS e OFDM mette a disposizione una vasta gamma di data-rate e mantiene la compatibilità con l'802.11b

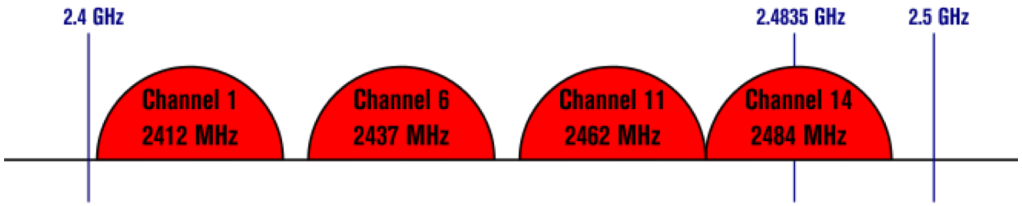
IEEE 802.11n

- ✓ Lo standard **802.11n** utilizza le frequenze della banda a 2.4 GHz e 5 GHz ed è in grado di trasmettere con data-rate teorici da 1 a 600 Mbps
- ✓ Utilizza canali da 20 e 40 MHz
- ✓ OFDM per trasmettere i dati e in questo modo è in grado di garantire alti data-rate con modulazione 64 QAM
- ✓ Combinando tecniche di trasmissione MIMO (PHY) e Frame Aggregation (MAC) mette a disposizione una vasta gamma di data-rate e mantiene la compatibilità con l'802.11 b/g

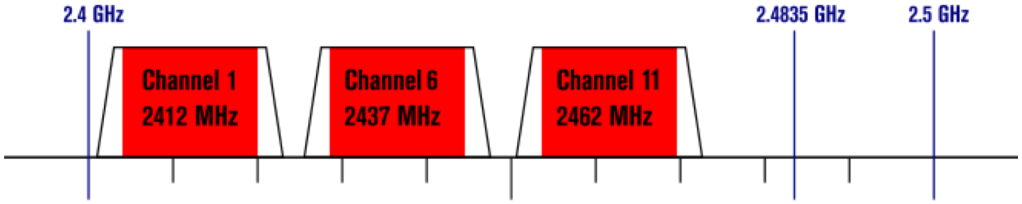
Allocazione dei canali-802.11g/n

Non-Overlapping Channels for 2.4 GHz WLAN

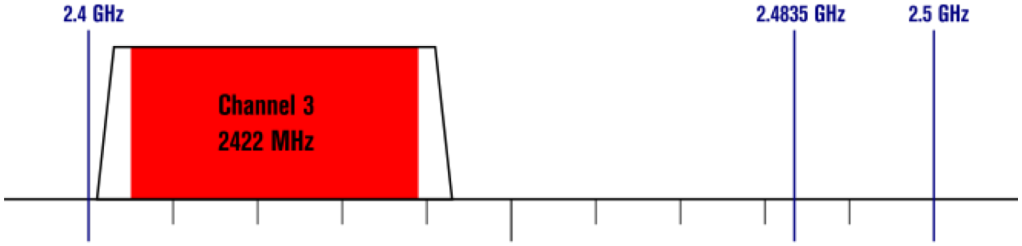
802.11b (DSSS) channel width 22 MHz



802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers

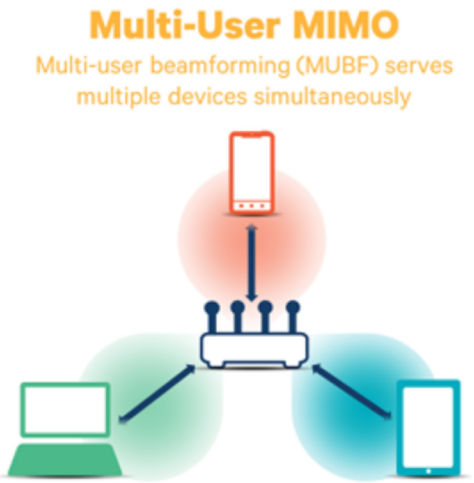


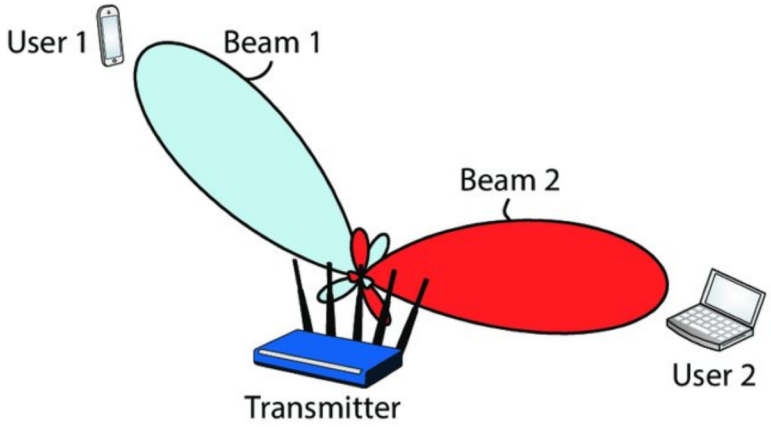
802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers



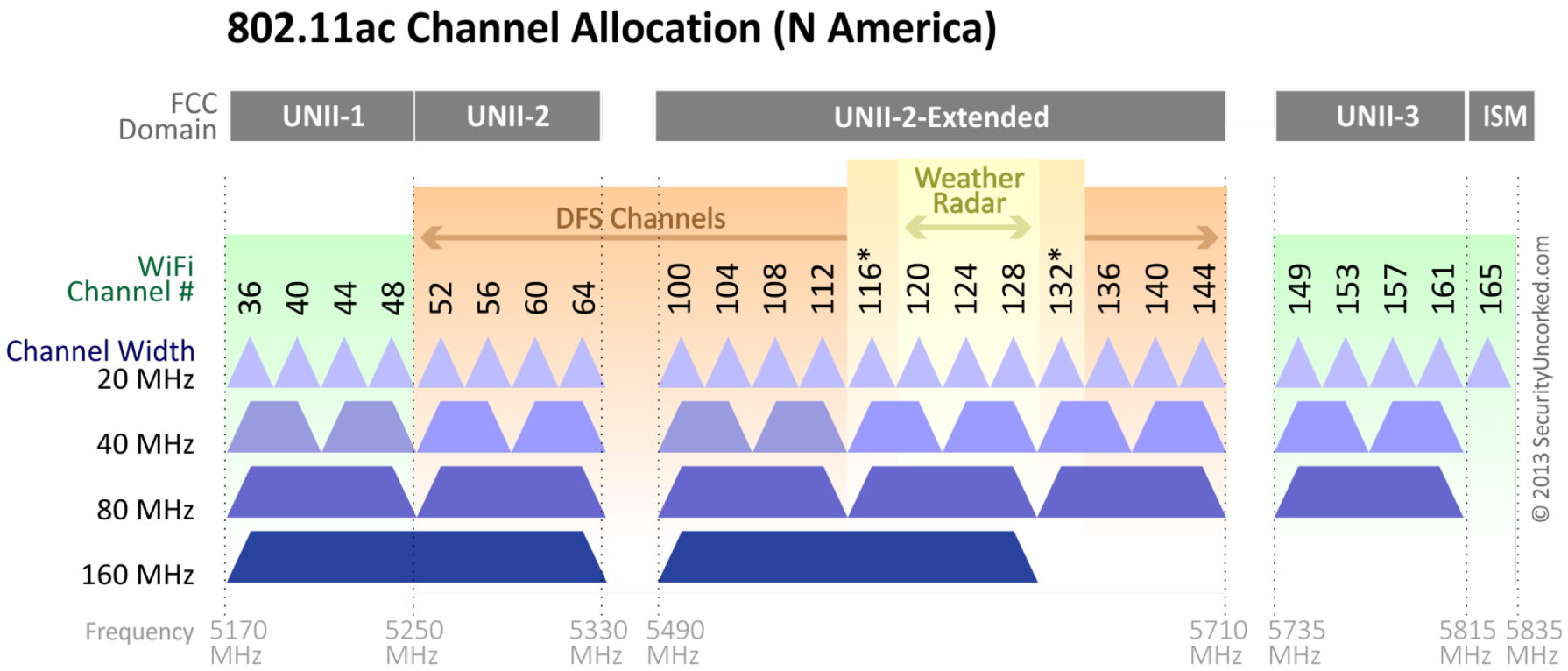
IEEE 802.11ac

- ✓ Lo standard **802.11ac** utilizza le frequenze della banda a 5 GHz ed è in grado di trasmettere con data-rate teorici sino a 1 Gbps
- ✓ Utilizza canali da 20 - 40 - 80 – (80+80) -160 MHz
- ✓ OFDM per trasmettere i dati e in questo modo è in grado di garantire alti data-rate con modulazione 256 QAM
- ✓ Multi User MIMO
- ✓ Beamforming





Allocazione dei canali 802.11ac



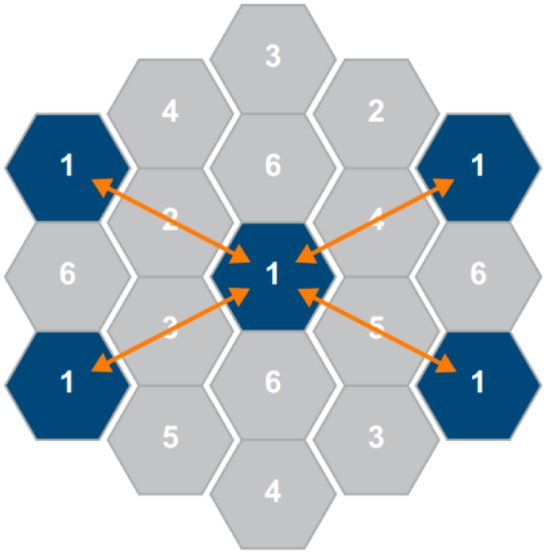
*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

IEEE 802.11ax – Wi-Fi 6

- ✓ Lo standard **802.11ax** utilizza le frequenze della banda a 2.4 a 6 GHz ed è in grado di trasmettere con data-rate teorici sino a 9.6 Gbps
- ✓ Utilizza canali da 20 - 40 - 80 – (80+80) -160 MHz
- ✓ OFDM per trasmettere i dati e in questo modo è in grado di garantire alti data-rate con modulazione 1024 QAM
- ✓ Multi User MIMO
- ✓ Beamforming
- ✓ Riutilizzo delle frequenze spaziali
- ✓ Accesso di tipo OFDMA

Riutilizzo Spaziale delle Frequenze

- ✓ Se più AP operano sullo stesso / i canale / i, possono trasmettere dati con un identificatore "colore" univoco che consente loro di comunicare contemporaneamente senza attendere poiché i colori consentono loro di differenziare tra loro i dati.

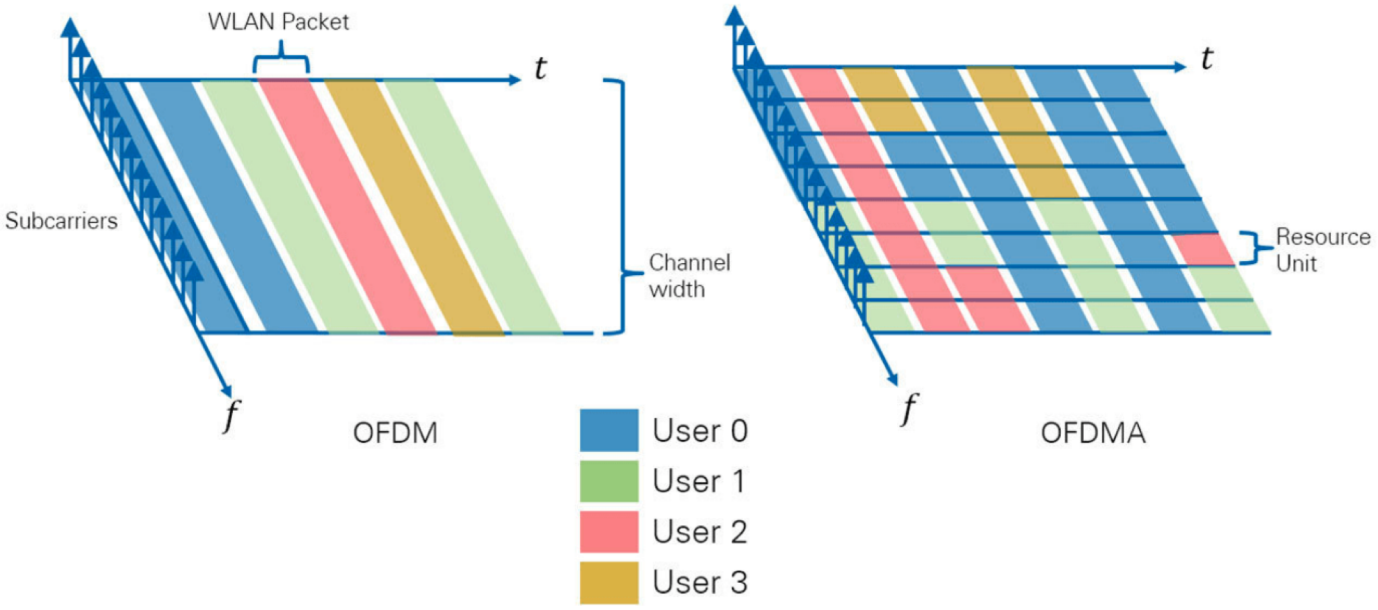


Network without BSS Coloring

Network with BSS Coloring

Accesso Multiplo con OFDM (OFDMA)

- ✓ In OFDM in un istante di tempo tutte le sottoportanti sono assegnate al medesimo utente e l' accesso multiplo si realizza nel tempo
- ✓ In Orthogonal Frequency Division Multiple Access (OFDMA) in un dato istante le sottoportanti disponibili sono divise tra più utenti



IEEE 802.11

Standard	Banda di Frequenza	Larghezza di Banda	Modulazione	Data Rate Massimo
802.11	2.4 GHz	20 MHz	DSSS - FHSS	2 Mbps
802.11b	2.4 GHz	22 MHz	DSSS	11 Mbps
802.11a	5 GHz	20 MHz	OFDM	54 Mbps
802.11g	2.4 GHz	20 MHz	DSSS – OFDM 64 QAM	54 Mbps
802.11n	2.4GHz 5 GHz	20 - 40 MHz	MIMO-OFDM 64 QAM	600 Mbps
802.11ac	5 GHz	20 - 40 - 80 80+80-160 MHz	MU-MIMO-OFDM 256 QAM	1 Gbps
802.11ax	2.4GHz 5 GHz 6GHz	20 - 40 - 80 80+80 -160 MHz	MU-MIMO-OFDMA 1024 QAM	9.76 Gbps

Sicurezza su WiFi

- La sicurezza sulle reti wireless dipende dal tipo di algoritmo di protezione utilizzato dall'access Point:
  - Access Point in configurazione di default
  - MAC Address Authentication
  - Crittografia e autenticazione con **Wired Equivalent Privacy (WEP)**
  - **Wi-Fi Protected Access (WPA)** è un protocollo per la sicurezza delle WLAN creato per tamponare i problemi di scarsa sicurezza del WEP

Configurazione di Default

- ✓ Un utente acquista un Access Point al computer shop sotto l'ufficio e lo connette senza autorizzazione alla rete aziendale
- ✓ Nessuna sistema di sicurezza predefinito:
  - ➢ Autenticazione in modalità "Open Key" senza alcuna chiave WEP **chiunque può accedere!**
  - ➢ Nessuna autenticazione centralizzata
  - ➢ Nessuna gestione delle autorizzazioni e degli utenti collegati
  - ➢ I possibili rischi comprendono:
    - Accesso ad informazioni riservate
    - Interruzioni di servizio

MAC Address Authentication

- ✓ Molti AP permettono di limitare l'accesso alla WLAN basandosi su una tabella di MAC Address
  - ➢ L'Access Point controlla se il MAC Address del client che richiede l'accesso alla WLAN fa parte dell'elenco di quelli abilitati
  - ➢ Il client il cui MAC Address non risulta compreso nella suddetta lista non viene autenticato e di conseguenza non può accedere alla rete
- ✓ Il sistema basato sull' autenticazione degli indirizzi MAC è ancora vulnerabile:
  - ➢ "sniffing" della WLAN per recuperare IP e MAC Address validi
  - ➢ modifica del MAC Address per presentarsi come un utente abilitato

Wired Equivalent Privacy

- ✓ WEP è il meccanismo di protezione standard del protocollo 802.11:
  - Il WEP è un algoritmo di cifratura (e autenticazione) dei dati trasmessi via radio tra Access Point e schede Wireless presenti nei client in ambito WLAN
- ✓ Tutti gli utenti condividono la stessa chiave:
  - La secret key (chiave segreta) è lunga 40 bit ed è concatenata a un vettore di inizializzazione lungo 24 bit, ottenendo così una sequenza di 64 bit totali
  - Le ultime versioni dell'algoritmo di crittografia WEP prevedono una chiave a 128 bit garantendo una maggior sicurezza e affidabilità *(ulteriormente inclusa nella WPA2)* con 104 bit di chiave e vettore di inizializzazione a 24 bit

Wi-Fi Protected Access

- ✓ WPA è progettato per gestire l'autentificazione obbligatoria e la distribuzione di differenti chiavi per ogni utente
- ✓ Per questioni di compatibilità supporta la precedente gestione a chiave condivisa (private secret key - PSK)
- ✓ I dati sono cifrati con algoritmo di cifratura a stream RC4 con chiave a 128 bit e vettore di inizializzazione a 48 bit
- ✓ Maggiore robustezza all'algoritmo con la definizione del **Temporal Key Integrity Protocol** (**TKIP**)

Wi-Fi Protected Access

- **Temporal Key Integrity Protocol (TKIP)**
  - **chiave per-station:** si crea una chiave per ogni stazione appartenente al BSS dunque tutti i nodi wireless hanno chiavi diverse
  - **chiave per-packet**: la chiave cambia ogni pacchetto limitando la possibilità che vi siano due pacchetti cifrati con la medesima chiave
  - **Integrità**: basata sull'algoritmo *Michael*
  - **key refresh**: se si verificano più di due MIC-failure in un minuto l'AP considera questo come un attacco e de-associa il client eliminando le chiavi
  - **IV mixing** è il seme per il cifrario RC4: non è la semplice concatenazione del IV e della PTK (chiave per-session) ma è derivato da due fasi di mixing del IV con la PTK e con il MAC address della stazione trasmittente

Wi-Fi Protected Access

- ✓ Il WPA utilizza un metodo per verificare l'integrità dei messaggi chiamato "Michael" che include un contatore associato al messaggio per impedire all'attaccante di ritrasmettere un messaggio che è già stato trasmesso nella rete
- ✓ In sostanza il WPA
  - ➢ aumenta la dimensione della chiave
  - ➢ Aumenta il numero delle chiavi in uso
  - ➢ ha un sistema per verificare l'autenticità dei messaggi migliore
  - ➢ incrementa notevolmente la sicurezza della WLAN
- ✓ WPA2 è l'evoluzione del WPA, introducendo un nuovo algoritmo basato su AES, CCMP, considerato molto più sicuro

Wi-Fi Protected Access

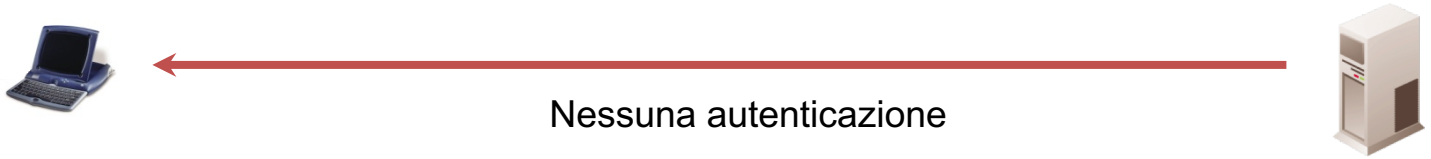
- ✓ WPA2 è l'evoluzione del WPA introducendo un nuovo algoritmo basato sui protocolli AES (Advanced Encryption Standard) e CCMP (Counter with CBC-MAC) ed è considerato molto più sicuro
- ✓ Nel CCMP l'AES viene utilizzato in una particolare modalità operativa definita CCM (Counter with CBC-MAC) in cui all'algoritmo crittografico che opera in modalità Cipher Block Chaining (CBC) viene accoppiato un codice di autenticazione MAC (CBC-MAC)

Supporto di client WPA e WEP misti

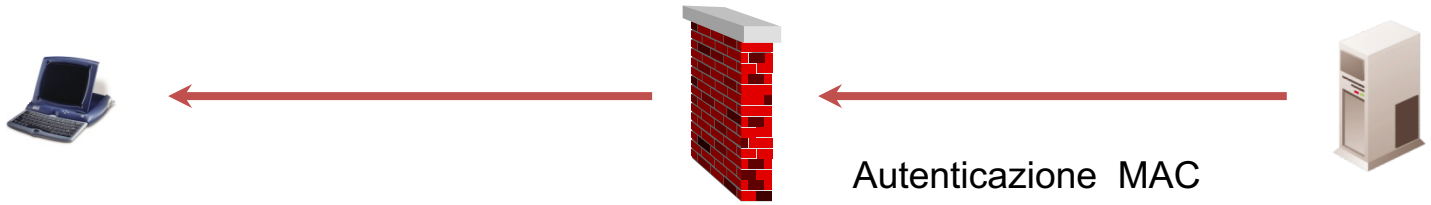
- ✓ Per supportare la transizione graduale alla tecnologia WPA delle WLAN basate su WEP un AP può supportare sia client WEP che WPA
- ✓ Durante l'associazione l'AP determina quali client utilizzano WEP e quali utilizzano WPA
- ✓ Nasce un problema: la chiave di crittografia globale non è dinamica perché i client WEP non sono in grado di supportarla
- ✓ Sono mantenuti tutti gli altri vantaggi per i client WPA compresa l'integrità

Sicurezza su Wifi

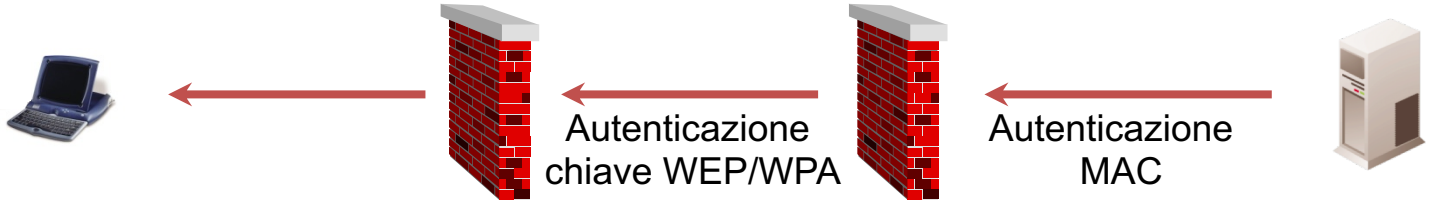
- ✓ Configurazione di Default:



- ✓ MAC Address Authentication:



- ✓ Wired Equivalent Privacy/ Wi-Fi Protected Access :



Normativa italiana

- ✓ DPR 447 del 5 Ottobre 2001
- ✓ Decreto Gasparri 28 Maggio 2003
- ✓ Decreto Pisanu 27 Luglio 2005
- ✓ Decreto Landolfi 4 ottobre 2005
- ✓ I limiti di potenza attuali

I limiti di potenza attuali

- ✓ I limiti di potenza, secondo le norme **ETSI** (European Telecomunications Standard Institute) attuali per i servizi radio LAN sono:
  - ➢ 100 mW per la banda a 2.4 GHz
  - ➢ 1 W per la banda a 5 GHz