LEZIONE

1 Wireless: comunicare senza fili

IN QUESTA LEZIONE IMPAREREMO...

- i componenti di una rete wireless
- le topologie e gli standard di comunicazione wireless

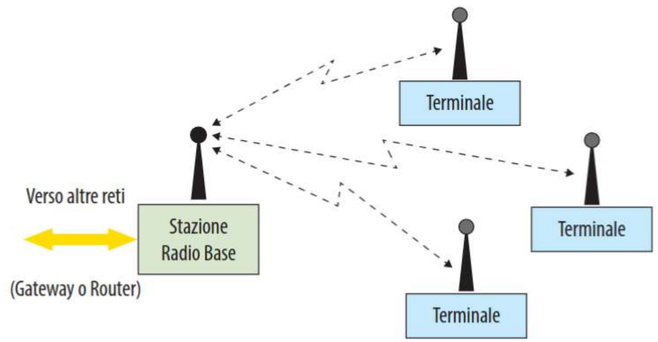
Topologia

Tra le **reti wireless**, cioè tutte le reti in cui i terminali accedono alla rete tramite canali "senza fili" (in genere onde radio), possiamo distinguere due famiglie:

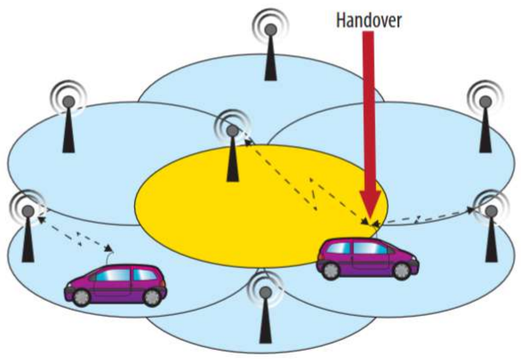
1. **reti radiomobili**: sono reti wireless dove i terminali utenti possono spostarsi sul territorio senza perdere la connettività con la rete, come la rete cellulare;
2. **wireless LAN** (**WLAN**): sono reti wireless che forniscono coperture e servizi tipici di una LAN.

Dobbiamo sottolineare una differenza fondamentale tra reti wireless e reti cellulari.

- **Rete wireless**: è una (sotto) rete in cui l'accesso da un terminale avviene attraverso un canale "senza filo";



- **Rete cellulare**: è una rete la cui copertura geografica è ottenuta con una tassellatura di aree adiacenti e/o sovrapposte, dette celle, dove l'utente si può muovere attraverso la rete passando da una cella all'altra, senza interrompere la comunicazione.



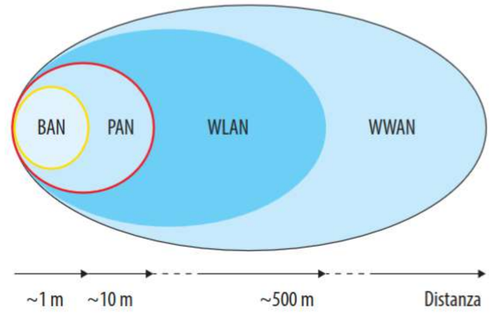
Anche se, in entrambe le tipologie di rete, i dispositivi che sono connessi sono mobili, nel primo l'accesso alla rete è generalmente unico (**stazione radio** base o **access point**) e il terminale mobile si sposta "all'interno della stessa rete" mentre nelle reti cellulari la connessione deve essere "passata" tra celle adiacenti senza che venga a perdersi

il collegamento: questo passaggio prende il nome **handover** (o **handoff**) e, di fatto, è l'elemento distintivo tra le reti cellulari e ogni altro tipo di rete TLC.
Le funzionalità aggiuntive che devono essere svolte in sistemi che presentano utenti in "mobilità" sono sostanzialmente:

- **localizzazione**: ogni utente mobile deve essere localizzato nell'area di copertura individuando la sua posizione;
- **registrazione**: un terminale mobile, dopo che viene localizzato, deve venire "collegato" alla rete e quindi deve venire identificato e autenticato;
- **handover**: al passaggio tra due zone avviene la (ri)localizzazione e, quindi, la sua (ri)registrazione.

Le procedure connesse agli handover sono complesse e richiedono alle reti notevoli requisiti in termini di architettura di rete, di protocolli e di segnalazione.

Come per le reti cablate, anche per le **reti wireless** viene fatta una classificazione sulla base della distanza geografica che il segnale trasmesso dai dispositivi che si connettono alla rete può raggiungere, cioè "l'area di copertura"; definiamo quattro categorie di reti.



BAN (Body Area Network)

Con **Body Area Network** si intendono le reti *wearable*, cioè o indossabili o nelle immediate vicinanze del corpo, con un raggio di copertura al massimo di due metri: i dispositivi coinvolti sono i telefoni cellulari, gli auricolari, i palmari, i lettori Mp3 ecc.
Proprio per l'utilizzo sul corpo questi dispositivi devono essere connessi tra loro senza fili e, generalmente, hanno la capacità di autoconfigurarsi anche se sono di tipo diverso.

PAN (Personal Area Network)

Le **Personal Area Network** sono reti con area di copertura che raggiunge anche i dieci metri, generalmente all'interno di un locale: è per esempio la rete personale dell'ufficio dell'utente, dove i dispositivi mobili si connettono con quelli fissi, computer e/o stampanti per condividere informazioni e risorse.
I moderni sistemi operativi offrono delle applicazioni predisposte alla sincronizzazione automatica dei dispositivi mobili con quelli fissi che nella PAN generalmente si connettono con tecnologie a infrarossi o radio: le macchine digitali per esempio scaricano le fotografie sui desktop, il lettore mp3 riceve nuove canzoni appena scaricate da Internet ecc.
Per la sua sicurezza ed economicità, lo standard **Bluetooth** è di fatto quello prevalentemente usato per scambiare informazioni tra dispositivi diversi attraverso una frequenza radio a corto raggio: sfrutta onde nello spettro dell'infrarosso nelle frequenze libere di 2,45 GHz con un bit rate di 3 Mbps.
Le specifiche per il **Bluetooth** rientrano nello **standard IEEE 802.15**.

WLAN (Wireless Local Area Network)

Le **WLAN** sono le reti maggiormente diffuse con il loro raggio di copertura che va dai 100 ai 500 metri: possono quindi raggiungere i dispositivi all'interno di un edificio di medie dimensioni, come una scuola o una piccola impresa, e possono sostituire a tutti gli effetti le LAN cablate offrendo le stesse prestazioni e possibilità di connettività.
Una rete WLAN è costituita da **STATION (STA)** e **Access Point** (**AP**).

Con **access point** si indica un dispositivo che contiene interfacce wireless **MAC** e **PHY** conformi allo standard IEEE 802.11, che consente l'accesso a un sistema di distribuzione per le stazioni associate: solitamente sono elementi di infrastruttura che sono connessi a backbone cablati.

STATION (STA)
Con **Station** si indica un dispositivo che contiene interfacce MAC e PHY wireless conformi allo standard IEEE 802.11, ma non fornisce accesso al sistema di distribuzione (terminali tipo workstation, laptop ecc.). Le STA sono anche indicate come Wireless Terminal (WT) e sono dotate di una interfaccia 802.11 integrata oppure su schede USB o PCMCIA, e possono essere sia terminali mobili sia fissi (notebook, tablet, smartphone ecc.).

Le wireless LAN sono regolate dallo **standard IEEE 802.11**: dalla 802.11b in poi sono anche chiamate semplicemente **Wi-Fi** (**Wireless Fidelity**), marchio definito da un consorzio di imprese che ormai è divenuto sinonimo di wireless.

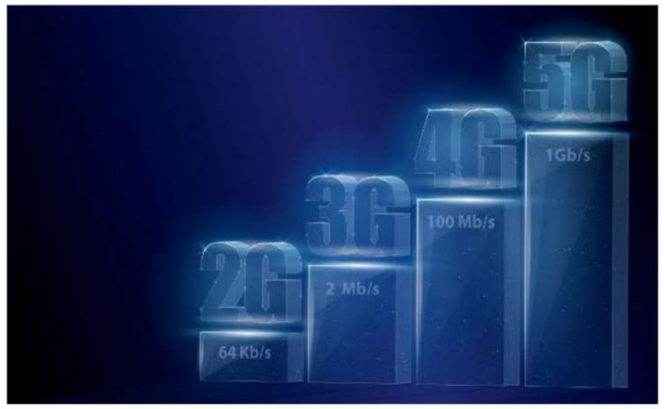
Il termine 802.11 viene usualmente utilizzato per definire la prima serie di apparecchiature 802.11 sebbene si debba preferire il termine "802.11 legacy".

Troviamo nelle WLAN gli stessi requisiti delle tradizionali reti LAN cablate (wired), come la completa connessione fra le stazioni che ne fanno parte e la capacità di inviare messaggi broadcast.
I problemi con questa tipologia di rete sono quelli classici delle connessioni wireless e cioè la sicurezza delle informazioni, la larghezza di banda limitata e il consumo energetico.

WWAN (Wireless Wide Area Network)

Le **WWAN** sono reti wireless di dimensione geografica estesa sino a una decina di kilometri e nascono dall'esigenza di raggiungere utenti che difficilmente potrebbero avere connessioni cablate, come paesi di montagna o aree difficilmente raggiungibili e/o antieconomiche per le normali linee fisse.
Le soluzioni WWAN che si basano su un'infrastruttura **a rete cellulare**, o su **trasmissione satellitare**, rappresentano il futuro della comunicazione dati, permettendo a chiunque di accedere ai dati e scambiare informazioni.
Le reti WWAN sono realizzate con diversi standard; ricordiamo le generazioni che hanno caratterizzato la loro evoluzione:

- prima generazione (**1G**): nato negli Stati Uniti, lo standard *Advanced Mobile Phone Systems* (**AMPS**) permetteva la trasmissione della voce tra cellulari Tacs in tecnologie analogiche su una banda di frequenza di 800 MHz;
- seconda generazione (**2G**): si basavano su tecnologia digitale per servizi telefonici, come il *Global System for Mobile* (**GSM**) in Europa e *Personal Digital Communication* (**PDC**) in Giappone, con data rate previsto che non superava 9.6 Kbps;
- seconda generazione e mezzo (**2.5G**): è l'evoluzione della precedente e con il *General Packet Radio System* (**GPRS**) e EDGE oltre alla voce iniziò a effettuare la trasmissione dei dati (data rate di 384 Kbps);
- terza generazione (**3G**): con l'*Universal Mobile Telecommunication System* (**UMTS**) si raggiungono trasmissioni con data rate fino a 2 Mbps su frequenze di trasmissione comprese fra 1,9 GHz e i 2,2 GHz e si rendono disponibili nuovi servizi quali videotelefonate e trasferimento di filmati;
- quarta generazione (**4G**): nasce il 27 giugno 2011, consente streaming video in HD e 4K, streaming musicale in alta qualità e permette la diffusione della **IoT** (*Internet of Things*). Inoltre, grazie alla stabilità del 4G, si sono diffusi i pagamenti online. Con la tecnologia 4G si arriva a picchi di data rate di 100-150 Mbps e a tempi di latenza compresi tra 40 e 50 ms. La rete 4G utilizza le seguenti bande di frequenza (nella UE):
  - 800 MHz (quando sono state liberate le frequenze televisive da 794 MHz a 858 MHz dal 2013)
  - 850 MHz (quando completato il refarming dello spettro dal GSM)
  - 1,8 GHz (quando liberati alcuni dei canali usati dal GSM)
  - 1,9 GHz
  - 2,1 GHz
  - 2,6 GHz (frequenze già libere in alcune zone ma utilizzate dai Ministeri della Difesa e dai radar in altre zone);
- quinta generazione (**5G**): lo standard 5G (ITU IMT-2020) prevede data rate fino a 10 Gbps con frequenze di 15 GHz. Per la precisione le bande usate dal 5G sono: 700 MHz, 3,4-3,8 GHz, 26 GHz e, successivamente tra 24,25 e 86 GHz.



Le frequenze comprese tra 3,6 e 30 GHz rappresentano una vera novità per le reti di telefonia mobile, in quanto sono usate attualmente da altre applicazioni, fra le quali ricordiamo i ponti radio e le comunicazioni satellitari.

PER SAPERNE DI PIÙ

I PROBLEMI LEGATI AL 5G

Il livello di radiazioni a radiofrequenza, nei paesi industrializzati, è aumentato di ben 5.000 volte tra il 1985 e il 2005. Fino al 1940 il fondo naturale pulsato era di 0,0002 V/m. Il precedente limite legale, in Italia, era di 6 V/m in media su 24 ore. Dal 29 aprile è stato innalzato a 15V/m, per evitare l'installazione di un numero elevatissimo di ripetitori. Le frequenze che preoccupano di più sono quelle superiori ai 24,85 GHz, in quanto rappresentano quelle che vengono comunemente definite **ONDE MILLIMETRICHE**.

Il problema delle onde millimetriche non è solo legato agli eventuali rischi per la salute (elettrosmog), ancora da dimostrare, ma di carattere tecnico, in quanto inducono alla proliferazione di antenne di propagazione del segnale. Infatti le alte frequenze da una parte garantiscono elevate velocità di trasmissione dati, ma al contempo rendono la propagazione del segnale più difficile, in quanto molto sensibile agli ostacoli fisici. È proprio la presenza di numerosissime antenne a creare problemi sia di costi sia di logistica, in quanto devono essere distanziate opportunamente dalle abitazioni e nel contempo essere collocate in modo strategico per diffondere uniformemente il segnale.

ONDE MILLIMETRICHE

Le **onde millimetriche** potrebbero avere effetti biologici non ancora chiari al 100%, come da studi effettuati dal Dott. Agostino Di Ciaula, presidente dell'ISED (International Society of Doctors for Environments). Questo ha giustificato un richiamo alla prudenza da parte di centinaia di studiosi indipendenti internazionali, che ritengono necessari approfondimenti scientifici preliminari prima di passare all'uso capillare di queste frequenze.

Analogamente a quanto successo con Wi-Fi, è nato **WiMAX**, un consorzio di imprese dedicate a progettare i parametri e gli standard per questa tecnologia che consente l'accesso a reti di telecomunicazioni a banda larga e senza fili.
Oggi WiMAX ha perso rilevanza rispetto ad altre tecnologie di connettività, soprattutto a favore del 4G e 5G, per diversi motivi:

- LTE è diventato lo standard dominante per le reti mobili grazie al supporto delle principali compagnie di telecomunicazioni e produttori di dispositivi;
- ha una copertura e una compatibilità limitate: WiMAX richiedeva infrastrutture dedicate e dispositivi compatibili, mentre LTE è stato integrato facilmente nelle reti esistenti;
- il 5G ha superato WiMAX in termini di prestazioni, latenza e scalabilità.

Attualmente WiMAX viene ancora usato in alcune aree rurali e per applicazioni specifiche, come connessioni aziendali o militari, ma è considerato una tecnologia obsoleta per l'uso commerciale su larga scala.

Lo standard IEEE 802.11

Prima di analizzare le caratteristiche delle reti WLAN è necessario effettuare una panoramica sui protocolli della famiglia dello standard **IEEE 802.11** per le WLAN e sulle specifiche **Bluetooth** per le comunicazioni wireless a corto raggio.

Il protocollo 802.11 legacy

Il **gruppo IEEE 802.11** è stato costituito nel 1989 e ha sviluppato diverse classi di reti: nel 1997 ha divulgato il primo standard di riferimento per le reti wireless, l'IEEE 802.11 legacy, che detta le specifiche a livello "Fisico" (*Physical layer*) e di "Collegamento" (*Data Link layer*) per l'implementazione di una rete LAN wireless:

- **velocità di trasferimento** dei dati compresa tra 1 e 2 Mbps;
- mezzo trasmissivo: **raggi infrarossi** nella frequenza di 2,4 GHz per la trasmissione del segnale.

L'uso dei raggi infrarossi venne successivamente abbandonato preferendo la trasmissione radio che meglio si adatta alle esigenze di una rete LAN.

In Europa la banda disponibile per il 802.11 è suddivisa in 13 canali: la frequenza centrale di ciascun canale è riportata nella tabella seguente, dove si può vedere che dista dalla più vicina per 5 MHz.

CANALE	FREQUENZE
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

Le velocità supportate dallo standard sono riportate nella tabella seguente correlate con la distanza.

CAMPO	11 MBS	5,5 MBS	2 MBS	1 MBS
Ambiente aperto	160 m	270 m	400 m	550 m
Ambiente semi-aperto	50 m	70 m	90 m	115 m
Ambiente chiuso	25 m	35 m	40 m	50 m

802.11 b

Questo standard nato nel 1999 diventa il nuovo standard dominante con il nome di **Wi-Fi** (*Wireless Fidelity*): viene progettato per un data rate massimo di 11 Mbps utilizzando il metodo CSMA/CA per la trasmissione delle informazioni. Il massimo valore di trasferimento ottenibile è di 5,9 Mbps utilizzando il protocollo TCP e 7,1 Mbps con UDP sfruttando le frequenze nell'intorno dei 2,4 GHz.

802.11 a

Nel 2001 viene ratificato il protocollo 802.11a che utilizza lo spazio di frequenze nell'intorno dei 5 GHz operando con una velocità massima teorica di 54 Mbps: nella pratica raggiunge solamente i 20 Mbps. Lo standard definisce 12 canali non sovrapposti, 8 dedicati alle comunicazioni interne e 4 per le connessioni punto a punto.

802.11 f

Chiamato **IAPP** (*Inter Access Point Protocol*), l'802.11f è un protocollo di livello "Applicazione" per la gestione di ESS (Extend Service Set): si occupa di gestire l'handover di terminali da una rete wireless all'altra.

802.11 g

Questo standard viene approvato nel giugno del 2003 e utilizza la stessa frequenza dell'802.11b, ovvero 2,4 GHz. Fornisce una banda teorica di 54 Mbps, che in pratica si traduce a 24,7 Mbps molto simile a quella dell'802.11a; esistono delle varianti proprietarie chiamate **g+** o **SuperG** che utilizzano l'accoppiamento di due canali per raddoppiare la banda disponibile introducendo, però, notevoli interferenze con altre reti.

802.11 i

Lo scopo del progetto 802.11 i è quello di sopperire alle debolezze del sistema crittografico WEP creando una valida alternativa alla crittografia e aumentando la sicurezza generale delle reti wireless.
I risultati ottenuti sono stati ratificati come standard e si dividono in due parti:

1. specifiche crittografiche per l'uso di **AES** (*Advanced Encryption Standard*);
2. IEEE 802.1X Port Based Network Authentication Standard: autenticazione e gestione delle chiavi nelle WLAN.

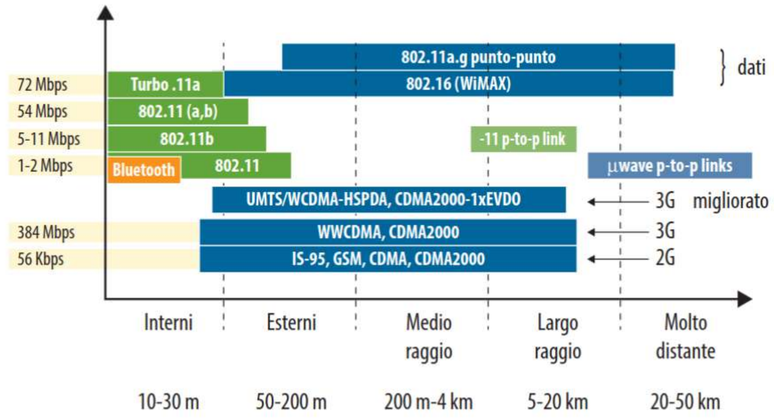
802.11 n

Dal gennaio 2004 l'IEEE attiva un gruppo di studio per realizzare uno standard per le reti wireless di dimensioni metropolitane che dovrebbe supportare una velocità di trasmissione teorica di 250 Mbps (100 Mbps reale) dimostrandosi 5 volte più rapido dell'802.11g e 40 volte più dell'802.11b.

> Una delle caratteristiche innovative del protocollo prevede la possibilità di utilizzare la tecnologia **MIMO** (**Multiple Input Multiple Output**) che consente di utilizzare più antenne per trasmettere e ricevere, ampliando la banda disponibile attraverso una multiplazione spaziale.

802.11ac

Avviato da IEEE nel settembre 2008 questo standard dell'802.11 è correntemente in fase di sviluppo e opera nell'intorno delle frequenze dei 5 GHz. La velocità massima teorica di questo standard all'interno di una WLAN multi-stazione è di 1 Gbit/s con una velocità massima di un singolo collegamento di 500 Mbit/s. Ciò è ottenuto ampliando concetti utilizzati da 802.11n: una più ampia larghezza di banda (fino a 160 MHz), più flussi spaziali MIMO (fino a 8), MIMO multi-utente e modulazione ad alta densità (fino a 256 QAM).
Il seguente grafico riporta in ascissa la distanza e in ordinata la frequenza di trasmissione dei diversi standard sino a ora descritti.



Altre tecnologie wireless

HiperLAN (*HIgh PErformance Radio LAN*), standard per comunicazione wireless WLAN che utilizza una frequenza di 5,4 GHz con bit rate sino a 54 Mbps. Lo standard HiperLAN è derivato dallo standard IEEE 802.11a, con due meccanismi addizionali:

- **TPC** (*Transmitter Power Control*) è la capacità dell'apparato HiperLAN di modificare istantaneamente la sua potenza di trasmissione, gli apparati utilizzano solo la potenza necessaria a portare a buon fine la trasmissione in base, per esempio, alla distanza.
- **DFS** (*Dynamic Frequency Selection*) è la capacità dell'apparato HiperLAN di modificare in modo istantaneo la frequenza di trasmissione, permette all'unità Master di evitare di disturbare i RADAR per la navigazione aerea, comunicando all'unità Slave la nuova frequenza di trasmissione. Infatti le frequenze utilizzate dall'HiperLAN sono le stesse utilizzate dai radar.

IrDA (*Infrared Device Application*), tecnologia di interconnessione dati che utilizza i raggi infrarossi. È bidirezionale e point-to-point, può avvenire solo tra dispositivi visibili reciprocamente (**LoS**, *line of sight*). La distanza è di 2 m e il bit rate è di 4 Mbps.

HomeRF, standard per la trasmissione dati in radio frequenza che utilizza il protocollo Swap. In genere usato per dispositivi domestici, ha una frequenza di lavoro tipica di 2,4 GHz e un bit rate pari a 1,6 Mbps. La versione 2.0 permette un bit rate fino a 10 Mbps e la trasmissione dati/voce con una distanza di 50 m, sia in modalità peer-to-peer sia access point.

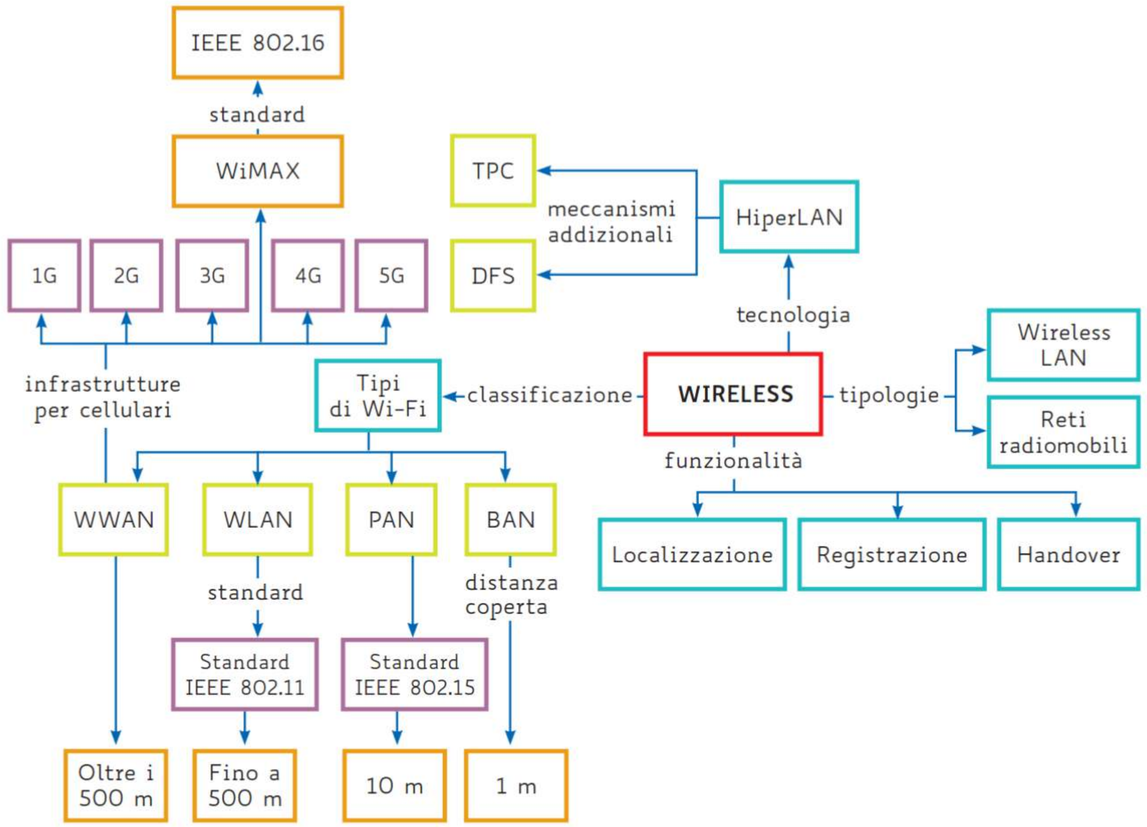
DECT (*Digital Enhanced Cordless Telecommunications*), standard digitale crittato per telefonini cordless che consente di avere 120 canali su 12 frequenze. Si tratta di una evoluzione del cordless analogico, implementa l'interfaccia **Gap** (*Generic Access Profile*) e utilizza la modulazione **GMSK**, bit rate max 348 Kbps.

WIpLL (*Wireless Ip Local Loop*), tecnologia wireless che fornisce servizi sia voce sia dati con copertura ad ampio raggio, utilizzando una frequenza che va da 2 GHz a 5 GHz con un bit rate di 4 Mbps.

Una tipica antenna HiperLAN

MAPPA CONCETTUALE

didattica inclusiva



Che cosa abbiamo imparato?

- Esistono reti radiomobili (per esempio, cellulari) e WLAN (rete locale wireless).
- Le reti BAN, PAN, WLAN e WWAN si distinguono per l'area di copertura.
- Gli standard IEEE 802.11 regolano le WLAN, note anche come Wi-Fi.
- Le reti WLAN utilizzano dispositivi come Station (STA) e Access Point (AP).
- Il 5G offre velocità elevate ma richiede infrastrutture avanzate (per esempio antenne dense).
- Lo standard WiMAX fornisce connessioni wireless a banda larga su grandi aree.
- Gli standard Bluetooth e HiperLAN garantiscono connettività a corto e medio raggio.
- Tecnologie come DECT e IrDA servono per la trasmissione di dati senza fili in specifici contesti.

Ora prova tu a rispondere

- Illustra la differenza tra reti WLAN e reti radiomobili.
- Definisci le principali categorie di reti wireless (BAN, PAN, WLAN, WWAN).
- Elenca i principali vantaggi e svantaggi del 5G.
- Descrivi il ruolo degli standard IEEE 802.11 nelle WLAN.
- Spiega come funzionano le reti WWAN e i loro usi principali.
- Fornisci esempi di tecnologie wireless per uso domestico e aziendale.

VERIFICA DI FINE LEZIONE

VERIFICA... le conoscenze

COMPLETAMENTO

1. Le procedure connesse agli handover sono complesse e richiedono alle reti notevoli requisiti in termini di ....., di ..... e di ..... .
2. Una rete WLAN è costituita da ..... (STA) e ..... (AP).
3. Le wireless LAN sono regolate dallo standard .....: dalla ..... in poi sono anche chiamate semplicemente ....., marchio definito da un consorzio di imprese che ormai è divenuto sinonimo di wireless.
4. L'..... (UMTS) trasmette con data rate fino a ..... su frequenze di trasmissione comprese fra ..... e ..... e rende disponibili nuovi servizi quali ..... e ..... .
5. Con WiMAX si intendono sistemi basati sullo standard ....., conosciuto anche come ..... .
6. L'IEEE 802.11 legacy detta le specifiche a livello ..... e di ..... per l'implementazione di una rete ..... .

VERO/FALSO

1. I problemi di sicurezza delle mail permettono la realizzazione di reti di dati wireless a lungo raggio. V F
2. La IEEE stabilì nel 1987 il comitato 802.11 appositamente per le WLAN. V F
3. Con Body Area Network si intendono le reti wearable, cioè indossabili. V F
4. Le Personal Area Network sono reti con area di copertura al massimo di due metri. V F
5. I dispositivi mobili nella PAN generalmente si connettono con tecnologie a infrarossi o radio. V F
6. Le specifiche per il Bluetooth rientrano nello standard IEEE 802.15. V F
7. I Wireless Terminal WT sono terminali mobili dotati di una interfaccia 802.11. V F
8. Le soluzioni WWAN si basano su un'infrastruttura a rete cellulare o su trasmissione satellitare. V F
9. La terza generazione (3G) è caratterizzata dall'UMTS. V F
10. In Europa la banda disponibile per il 802.11 è suddivisa in 13 canali ciascuno "largo" 22 GHz. V F
11. Il protocollo 802.11f è anche chiamato IAPP (Inter Access Point Protocol). V F
12. Lo standard HomeRF viene utilizzato per trasmissioni con frequenza tipica di lavoro a 2,4 GHz e bit rate a 1,6 Mbps. V F
13. Le HiperLAN utilizzano una frequenza di 5,4 GHz con bit rate sino a 54 Mbps. V F
14. DECT fornisce servizi sia voce sia dati utilizzando una frequenza che va da 2 GHz a 5 GHz. V F

LEZIONE 2

L'autenticazione nelle reti wireless

IN QUESTA LEZIONE IMPAREREMO...

- i meccanismi WEP, WPA e WPA2
- il sistema di autenticazione 802.1X
- il protocollo EAP

La sicurezza delle reti wireless

Come ogni comunicazione cablata, la trasmissione senza fili presenta da sempre diverse problematiche relative alla sicurezza, soprattutto per il fatto che non necessita di una connessione fisica per poter accedere alla LAN.

Le **reti wireless**, trasmettendo dati per mezzo delle onde radio, presentano quindi ulteriori problemi rispetto alle reti wired, dipendenti proprio dalle caratteristiche del canale di comunicazione che utilizzano: una trasmissione nell'etere viene facilmente intercettata e chiunque riesce a manipolare i dati con semplici pacchetti software di pubblico dominio.

Esistono sistemi operativi basati su Ubuntu e progettati per eseguire *penetration test* e un hacker, dopo aver attivato la propria scheda di rete wireless in modalità passiva (*monitor mode*), avvia questi sistemi operativi, magari in modalità live CD, in modo da non lasciare nessuna traccia sul computer utilizzato per il tentativo di intrusione.

> In modalità passiva la scheda di rete intercetta tutti i pacchetti emessi da un router o dalla scheda di rete di altri computer: una volta scoperto l'SSID della rete a cui connettersi, il pirata attiva uno sniffer per catturare i pacchetti necessari a portare a termine l'attacco mediante software come aircrack-ng per estrarre le password di accesso alla rete.

È necessario quindi sviluppare un insieme di meccanismi aggiuntivi per la protezione delle comunicazioni.

Sappiamo che i problemi principali che riguardano una WLAN si possono suddividere in tre categorie:

- **riservatezza**: i dati trasmessi attraverso il canale non devono essere intercettati e interpretati;
- **controllo di accesso** (*Access Control*): alla rete possono accedere solo gli host autorizzati;
- **integrità dei dati**: i messaggi trasmessi non devono essere manomessi, cioè devono giungere integri a destinazione.

Le tipologie di attacchi alle rete wireless si possono suddividere in:

- **eavesdropping** (intercettazione): con questo termine si indica la possibilità che entità non autorizzate riescano a intercettare e ascoltare in maniera fraudolenta i segnali radio scambiati tra una stazione wireless e un access point;
- **accessi non autorizzati**: un intruso si intromette illegalmente nella rete senza averne la autorizzazione e, una volta connesso, viola la riservatezza portando a termine degli attacchi alle risorse e alle applicazioni condivise dagli utenti della rete e immette traffico di rete non previsto;
- **interferenze e jamming**: tutte le apparecchiature in grado di emettere segnali a radiofrequenza entro la banda di funzionamento della rete rappresentano potenziali sorgenti di interferenza; se esiste la volontarietà di queste emissioni attaccanti e/o disturbare la comunicazione radio, si parla di **jamming**;
- **danni materiali**: possono essere fatti danni materiali allo scopo di creare malfunzionamenti o interruzioni dei servizi (*Denial of Service, DoS*) danneggiando gli elementi che compongono la rete come gli access point, le antenne, i cavi dei ripetitori Wi-Fi; anche la natura può portare limitazioni o interruzioni dei servizi dato che le onde elettromagnetiche sono sensibili alle condizioni ambientali sfavorevoli come il vento, le pioggia, le neve e le temperature rigide molto fredde.

> Per la legislatura italiana è illegale procurarsi un accesso a una rete senza averne avuto l'autorizzazione e quindi questi attacchi sono configurabili come reati e di seguito sarà descritto il loro inquadramento ai sensi del Codice Penale.

La crittografia dei dati

Una soluzione alla esigenza di riservatezza è quella di **crittare i dati trasmessi**: l'operazione di codifica dei dati fornisce riservatezza e integrità al sistema nelle operazioni di trasmissione, mentre l'autenticazione dell'utente fornisce la disponibilità e il controllo dell'accesso alla rete.

Wired Equivalent Privacy (WEP)

Le specifiche dello **standard IEEE 802.11** definiscono un meccanismo per la riservatezza dei dati conosciuto con il nome di **Wired Equivalent Privacy** (**WEP**), dato che l'obiettivo è quello di raggiungere per le reti wireless la stessa affidabilità delle reti cablate Ethernet.

È un protocollo di sicurezza a livello Data Link della pila ISO-OSI che si avvale di due meccanismi aggiuntivi:

- l'algoritmo crittografico **RC4**;
- il sistema di controllo dell'integrità dei dati **CRC-32**.

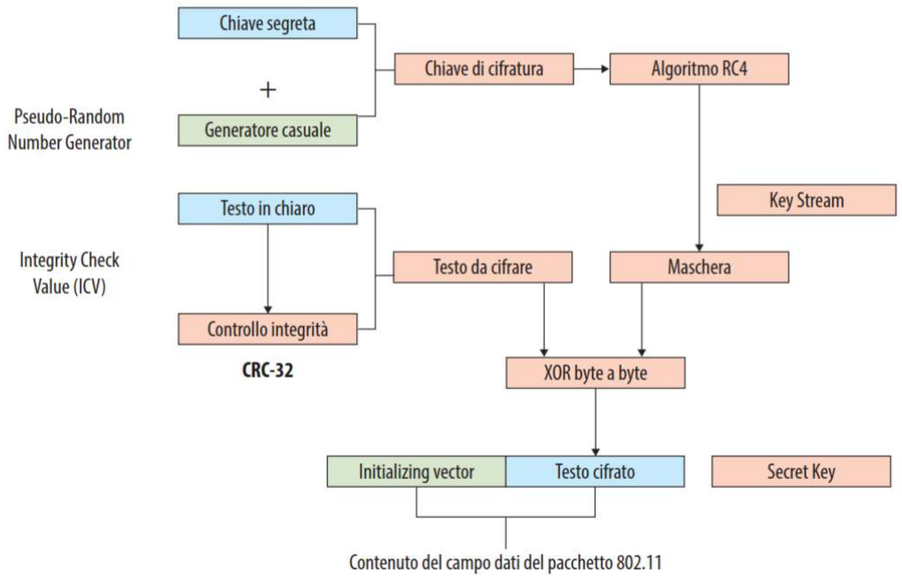
La crittografia utilizzata dal protocollo WEP si basa sul modello a chiave simmetrica mediante un algoritmo che permette di modificare un blocco di testo in chiaro (plaintext) calcolandone lo XOR bit a bit con una chiave di cifratura pseudocasuale di uguale lunghezza (keystream).

Il processo di codifica/decodifica prevede la presenza di una **chiave segreta** che costituisce uno degli input fondamentali dell'algoritmo e questa chiave segreta deve essere condivisa attraverso canali esterni alla rete wireless: questa necessità si traduce in un primo punto di insicurezza dell'intero sistema, poiché bisognerà prevedere delle pratiche adeguate di conservazione e condivisione delle chiavi, nonché una rigenerazione frequente delle stesse, cosa che raramente accade nella realtà nonostante la previsione da parte del legislatore di termini brevi per la sostituzione delle password di accesso ai sistemi informatici su cui risiedono dati personali.

Analizziamo ora nel dettaglio il protocollo nella sua fase di codifica come descritto nello schema sotto riportato.

Codifica

La modalità con cui la chiave segreta viene scelta e distribuita agli host della rete non è specificata dal protocollo e dunque la sua gestione è di competenza dell'amministratore di rete che deve provvedere a comunicarla a tutti gli host che devono connettersi.

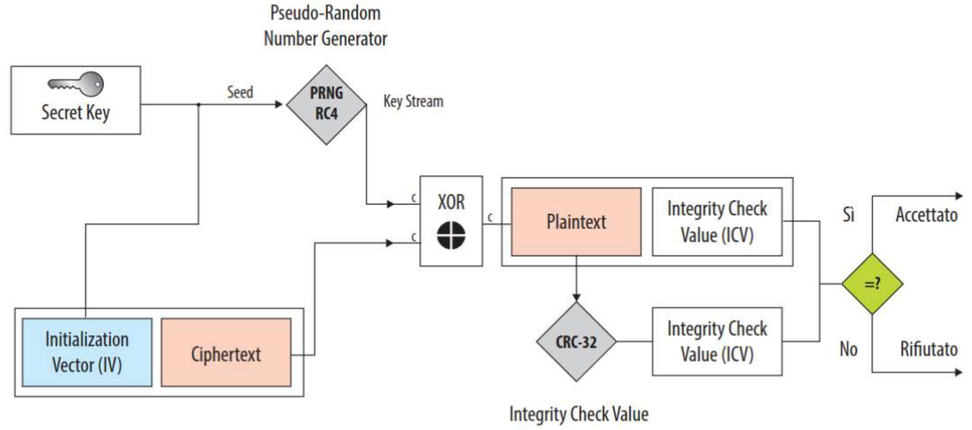


La **chiave di cifratura** viene realizzata a partire dalla chiave segreta che viene concatenata con un **initialization vector** (IV), che è un numero casuale di 24 bit, producendo l'input (**seed**) per il generatore pseudo-casuale **PRNG** (*pseudo-random number generator*), che è la funzione più importante svolta dell'algoritmo crittografico **RC4** (*Rivest Chipher 4*); l'RC4 produce in output la stringa denominata **keystream k** di lunghezza esattamente uguale a quella del messaggio che deve essere trasmesso in rete, dato che deve essere eseguito lo XOR bit a bit con esso.

Prima di essere spedito, il **plaintext** viene analizzato e, tramite l'algoritmo **CRC-32**, viene generata una stringa per il controllo di parità, denominata **Integrity Check Value (ICV)**, che viene utilizzata in ricezione per il controllo di integrità: testo e ICV vengono concatenati e sottoposti allo XOR con il keystream k, originando il testo cifrato denominato **ciphertext**.
Al messaggio finale viene aggiunto in chiaro l'IV iniziale, necessario per la decodifica da parte del destinatario.

Decodifica

Per effettuare la decodifica è necessario ricostruire lo stesso keystream k utilizzato in codifica: a tal fine si prende l'IV in chiaro del messaggio ricevuto, lo si concatena alla chiave segreta in possesso del destinatario e si ottiene un seed da utilizzare come input dell'algoritmo PRGN: questo, avendo le stesso input che ha utilizzato il mittente per la codifica, genererà come output lo stesso keystream k.



Ora si procede eseguendo l'operazione di XOR con il ciphertext: sfruttando l'invertibilità dell'operazione si ottiene il plaintext che viene sottoposto alla verifica di integrità mediante la ricostruzione del CRC-32 e confrontandolo con l'ICV contenuto nel messaggio ricevuto.

Sicurezza del WEP

Il **WEP** venne rilasciato e integrato tra le specifiche di sicurezza delle reti Wi-Fi troppo velocemente senza aver terminato gli appropriati studi sulla sua robustezza e capacità di resistere ad attacchi esterni mirati a scoprire la chiave di codifica.

Soltanto dopo l'immissione sul mercato di migliaia di dispositivi equipaggiati con tale metodo di protezione si dimostrò che la sua sicurezza offerta non era assolutamente assimilabile a quella delle reti cablate e che normali utenti informatici grazie a software "appropriati" avrebbero potuto violare in pochissimo tempo la crittografia utilizzata dai dispositivi 802.11 e impadronirsi del traffico circolante sulla rete.

La debolezza consiste nell'uso del Vettore di Inizializzazione IV: l'algoritmo RC4, infatti, risulta vulnerabile se vengono utilizzate le chiavi per più di una volta ed è quello che accade con il WEP che ammette uno spazio di sole 224 combinazioni: bastano 5 milioni di frame per riuscire a ricavare la chiave WEP.

Wireless Protected Access (WPA-WPA2): generalità

Per sopperire all'insicurezza del WEP, anche per effetto della diffusione sempre più elevata di dispositivi senza fili che richiede la necessità di un continuo sviluppo di protocolli di sicurezza, nell'aprile del 2004 venne così istituita una task force denominata "Task Group i" con il compito di ridefinire le politiche di sicurezza dello **standard IEEE 802.11**.

Il protocollo che nacque venne chiamato **Wireless Protected Access** (**WPA**), rappresenta solo alcune delle funzioni presenti nello standard IEEE 802.11i e viene implementato in due diverse configurazioni:

- **modalità Personal** (**WPA-PSK**);
- **modalità Enterprise** (**WPA-EAP**);

dove la modalità Personal viene pensata per le applicazioni **SOHO** (*Small Office Home Office*) e piccole reti, mentre la modalità Enterprise per soluzioni aziendali e infrastrutture di rete di grandi dimensioni.

Le principali migliorie introdotte dal WPA rispetto a WEP sono nelle dimensioni della chiave (128 bit) e del vettore di inizializzazione IV (48 bit) per cifrare i dati oltre all'aggiunta di un sistema di autenticazione reciproco tra client e rete wireless.

WPA utilizza inoltre un nuovo protocollo, il *Temporary Key Integrity Protocol* (**TKIP**), che permette di cambiare le chiavi crittografiche utilizzate dopo un certo numero di dati scambiati.
Al posto del CRC-32 viene utilizzato il *Message Integrity Code* (**MIC**) per effettuare il controllo dell'integrità dei dati, che in WPA prende il nome di "Michael".
Altra novità del protocollo è la netta suddivisione tra la fase che effettua la crittografia dei dati e la fase di autenticazione dei client di rete.

> Il protocollo che sfrutta completamente le funzionalità dell'IEEE 802.11i nacque nel giugno 2004, venne chiamato Wireless Protected Access 2 (WPA2) e utilizza un diverso meccanismo di cifratura:
> - WPA utilizza l'algoritmo RC4;
> - WPA2 utilizza l'algoritmo AES.
>
> L'RC4 fu utilizzato nel WPA in quanto la Wi-Fi Alliance decise in un primo tempo di riutilizzare l'hardware dei dispositivi già diffusi sul mercato che implementavano WEP.

WPA (TKIP)

WPA utilizza un sistema software di crittaggio e di sicurezza dei dati chiamato *Temporary Key Integrity Protocol* (**TKIP**) che a tutti gli effetti si comporta da "involucro" attorno al preesistente meccanismo WEP rendendolo così un sottocomponente del processo.

È composto dai seguenti elementi:

- meccanismo di controllo dell'integrità dei dati crittografati Michael (**MIC**);
- sistema di sequenziamento dei pacchetti trasmessi;
- sistema di rimescolamento delle chiavi;
- meccanismo di ri-generazione casuale delle chiavi durante il processo (distribuzione dinamica).

TKIP

Il sistema **TKIP** non utilizza mai lo stesso valore di **IV** più di una volta per ogni chiave di sessione fino a che non le esaurisce tutte generandole in modo casuale: il destinatario del flusso scarta tutti i pacchetti il cui valore è già stato utilizzato come IV e crittato con la stessa chiave.
Sia il mittente che il destinatario inizializzano lo spazio di sequenziamento a zero quando si scambiano una nuova chiave **k** e il mittente incrementa il numero sequenziale a ogni pacchetto inviato (sequenziamento dei pacchetti).
TKIP trasforma inoltre una chiave temporanea e un contatore sequenziale di pacchetti in una chiave di cifratura utilizzabile per una sola sequenza: quindi l'architettura **TGi** (*Task Group i*) per la generazione di chiavi dipende da una gerarchia di almeno tre tipi di chiave: chiavi temporanee, chiavi di cifratura e chiavi "master" (chiave condivisa tra i client della rete e il server di autenticazione 802.1X).

MIC

Il **MIC** è un dispositivo crittografico per rilevare la presenza di messaggi falsi nella comunicazione, cioè un *Message Authentication Code* (**MAC**): include **CBC-MAC**, costituito da un cipher block e ampiamente usato nelle applicazioni bancarie, e **HMAC** utilizzato da *Internet Protocol Security* (**Ipsec**).

Il sistema è composto da tre componenti: una chiave segreta **k** formata da 64 bit nota solo a mittente e destinatario, una funzione di etichettatura e un attributo di verifica.

La funzione di etichettatura **E** prende in input la chiave **k** e il messaggio **M** da inviare sulla rete, genera come output un'etichetta **T**, chiamata anche "codice di integrità" del messaggio, che viene inviata assieme al messaggio: il destinatario ripete lo stesso procedimento per verificarne l'autenticità e, in caso positivo, restituisce come risultato il valore logico TRUE, altrimenti FALSE presumendo che il messaggio ricevuto sia stato manipolato.

WPA2 (AES)

La differenza tra **WPAZ** e WPA è l'adozione di un nuovo algoritmo di sicurezza, il più diffuso al mondo tra gli algoritmi a chiave simmetrica: l'**Advanced Encryption Standard** (**AES**).
Essendo a chiave simmetrica, l'algoritmo utilizza la stessa chiave sia per la codifica sia per la decodifica dei dati, con lunghezze di chiavi pari a 128, 192 e 256 bit.

AES può avere diverse modalità di utilizzo, chiamate **modalità operative**: una modalità operativa è una precisa "ricetta" per utilizzare l'algoritmo e sbagliare qualche passo di tale "ricetta" può compromettere la garanzia di sicurezza della cifratura.

Le modalità operative più note sono:

- Electronic Codebook (**ECB**);
- Counter (**CTR**);
- Cipher-Block Chaining (**CBC**).

Senza entrare nel dettaglio delle singole modalità, quella che viene maggiormente utilizzata è la CBC alla quale spesso viene aggiunto un controllo di integrità dei dati MIC per offrire maggiori garanzie sulla trasmissione dei messaggi (la modalità assume il nome di CBC-MAC).

Autenticazione

Nell'ambito informatico il termine *autenticazione* assume un preciso significato, cioè quello così definito:

AUTENTICAZIONE

L'**autenticazione** è il processo tramite il quale un computer, un software o un utente, verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole comunicare attraverso una connessione.

Un esempio che tutti noi effettuiamo tutti i giorni è la comune procedura di "login" per accedere a un sistema di elaborazione oppure a una sezione riservata di un portale web, dove solo gli utenti autorizzati possono accedere.

Durante una comunicazione in rete è fondamentale che entrambi gli interlocutori siano riconosciuti: l'identità del richiedente di un servizio deve essere nota per premettergli l'accesso ai dati e alle risorse e, d'altra parte, anche il destinatario deve essere noto, in quanto bisogna essere sicuri della identità del soggetto al quale il mittente sta inviando i propri dati.

> Il termine autorizzazione viene spesso identificato con autenticazione: i protocolli per la sicurezza standard, per esempio, si basano su questo presupposto, ma in alcuni casi queste due azioni vengono affrontate con strategie differenti.

Il Sistema di autenticazione 802.1X

La prima forma di autenticazione si basava sulla conoscenza del **SSID** della rete: prende il nome di **OSA**, cioè *Open Systems Authentication*, dove l'access point autorizzava chiunque fosse a conoscenza del SSID della rete che, però, "essendo trasmesso in chiaro", veniva subito individuato dagli sniffer.

La **protezione WEP statica**, ancora oggi molto utilizzata da privati e aziende per l'accesso alle reti wireless, si basa sulla condivisione della password segreta (o chiave condivisa) per l'autenticazione dell'utente nella WLAN: basta quindi conoscere la chiave segreta per accedere alla rete.

> Lo standard WEP non prevede un metodo per l'automazione dell'aggiornamento o della distribuzione di tali chiavi, quindi risulta estremamente difficile modificarle periodicamente: generalmente la chiave di accesso rimane la stessa per mesi (o anni)!

Un sistema di autenticazione aggiuntivo è quello che si basa sul **filtraggio dei MAC Address** dei dispositivi wireless, ma prevede una lunga procedura manuale a opera degli amministratori di rete: la crittografia WEP non codifica il campo dell'indirizzo MAC del frame, quindi un hacker è in grado di monitorare il traffico di una rete e individuare indirizzi MAC validi e abilitati.

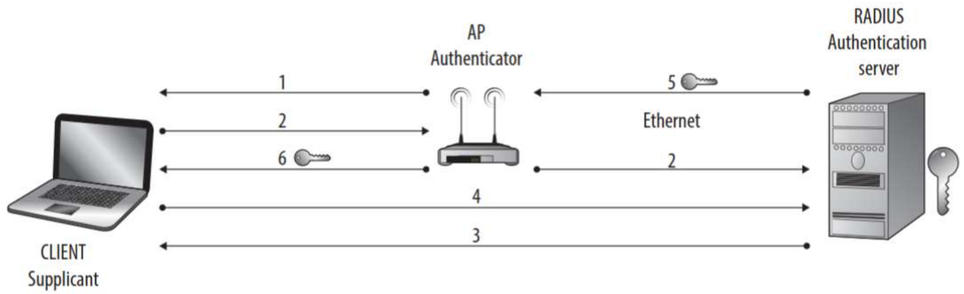
Per garantire un metodo più affidabile di autenticazione e autorizzazione, l'IEEE 802.11i ha proposto una struttura di protezione WLAN basata sul **protocollo 802.1X**, uno standard per l'autenticazione dell'accesso alla rete che si affida alla gestione delle porte (*Port based Network Access Control*) e che viene utilizzato per la gestione delle chiavi di protezione del traffico di rete.

> Oltre alle reti senza fili, il protocollo 802.1X viene implementato in numerosi switch di fascia alta della rete LAN cablata.

I componenti del sistema di autenticazione previsto dal protocollo 802.1X sono:

- l'utente di rete (**supplicant**);
- un dispositivo di accesso alla rete (o **gateway**) come un punto di accesso senza fili (**authenticator**);
- un **servizio di autenticazione**, **autorizzazione** e **accesso** (**AAA**) costituito generalmente da un server **RADIUS** (*Remote Authentication Dial In User Service*).

Tra supplicant e authenticator viene definito un collegamento come fosse "una connessione", chiamata "porta", nella quale viene impedito l'inoltro del traffico dei dati senza una chiave di autenticazione valida che viene gestita dal server RADIUS, che detiene le credenziali dell'utente e di autorizzazione dell'accesso alla WLAN.
Il seguente schema ci aiuta a seguire il processo necessario per ottenere una chiave di autenticazione valida.



1. Un **client senza fili** entra nel raggio di azione di un **AP** senza fili e questo richiede le credenziali di accesso al client.
2. Il client wireless si identifica all'AP, che inoltra le informazioni ricevute a un **server RADIUS**.
3. Il server RADIUS richiede altre credenziali del client per verificarne l'identità, specificando il tipo di credenziali necessarie.
4. Il client invia le proprie credenziali al server RADIUS.
5. Il **server RADIUS** verifica le credenziali del client: se le credenziali sono valide, il server RADIUS invia una chiave di autenticazione crittografata al punto di accesso.
6. L'**AP** utilizza la chiave di autenticazione per trasmettere in modo protetto le chiavi di autenticazione.

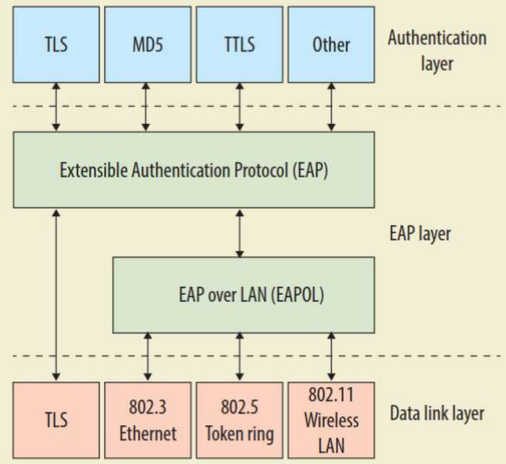
> Lo standard **WPA** prevede quindi due modalità di autenticazione:
> - la prima basata su **802.1X** e sull'autenticazione **RADIUS** appena descritta;
> - la seconda, la **WPA-PSK**, che propone uno schema più semplice per ambienti **SOHO** utilizzando una passphrase (**PSK**) precondivisa senza incappare nelle note vulnerabilità del WEP statico.

PER SAPERNE DI PIÙ

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

Per gestire lo scambio di dati di autenticazione tra il client e il server RADIUS inoltrati dal punto di accesso, lo standard 1X si basa su un protocollo denominato **EAP** (*Extensible Authentication Protocol*): originariamente questo protocollo fu proposto come fase di autenticazione opzionale per il protocollo **PPP** (*Point-to-point Protocol*) dopo l'instaurarsi di una connessione.
Ogni meccanismo indicato nella figura si basa su EAP e può quindi essere utilizzato a livello "Autenticazione" (Authentication layer) senza effettuare una prenegoziazione: l'AP (authenticator) invia una richiesta di identificazione o **request identity**, seguita da una o più richieste di autenticazione del client (supplicant).

> È un protocollo di autenticazione multiscopo che supporta numerosi metodi di autenticazione come **token card**, **Kerberos**, **one-time password**, **certificate**, **public key authentication** e **smartcard**.



Un frame di richiesta contiene un campo "tipo", per indicare quali sono le informazioni necessarie per l'autenticazione: alla sua ricezione il client invia una risposta per ogni request impostando il campo "tipo" con le informazioni necessarie.
I principali tipi di AEP sono :

- EAP Message Digest 5 (**EAP-MD5**): si basa principalmente sull'uso di una funzione hash "one-way";
- EAP Transport Layer Security (**EAP-TLS**): si basa sul protocollo TLS come dice il nome stesso;
- EAP Tunneled Transport Layer Security (**EAP-TTLS**): la modalità di autenticazione EAP-TTLS estende EAP-TLS permettendo lo scambio di informazioni aggiuntive tra client e server, utilizzando il tunnel di comunicazione stabilito con l'uso del protocollo TLS.
- Protected Extensible Authentication Protocol (**PEAP**): fornisce un tunnel di comunicazione crittato e autenticato come TLS, quindi i messaggi EAP incapsulati all'interno del tunnel TLS sono protetti contro svariati attacchi;
- Microsoft Challenge Handshake Authentication Protocol vers.2 (**MS-CHAPv.2**): è il protocollo di autenticazione sviluppato dall'azienda Microsoft basato sull'architettura del meccanismo CHAP (Challenge Handshake Authentication Protocol), che è uno schema di autenticazione usato dai server PPP per convalidare l'identità dei client remoti.

> Il numero di request-response che vengono scambiati dal protocollo varia a seconda del meccanismo di autenticazione scelto: il **server** di autenticazione invia al **client** una autorizzazione positiva o negativa di accesso alla rete dopo aver analizzato tutte le informazioni richieste.

LEZIONE

3 La trasmissione wireless

IN QUESTA LEZIONE IMPAREREMO...

- il livello fisico e la trasmissione dei segnali wireless
- il formato del frame 802.11

Cenni sulle tecnologie trasmissive

Lo strato fisico

Le **reti WLAN** possono essere realizzate mediante due diverse tecnologie:

- **tecnologie radio**: sono quelle normalmente utilizzate e sono soggette a norme molto precise per evitare interferenze con altri servizi e problemi di inquinamento elettromagnetico con tutti i dispositivi; le bande radio di trasmissione sono spesso sature;
- **tecnologie ottiche**: presentano numerosi problemi su distanze superiori a qualche chilometro e risentono di condizioni atmosferiche particolari, come la presenza di nebbia.

Le **reti WLAN radio** presenti oggi sul mercato utilizzano prevalentemente la banda di frequenze **ISM** (*Industrial Scientific Medical band*) composta dalle seguenti zone: 902 - 928 MHz; 2,400 - 2,480 GHz; 5,150 - 5,250 GHz.

Nella seguente tabella sono riportate le caratteristiche fisiche delle varie tipologie di **802.11**.

PROTOCOLLO	MODULAZIONE	VELOCITÀ	BANDA UTILIZZATA
802.11	Infrarosso diffuso	1 o 2 Mbps	–
	FHSS	1 o 2 Mbps	2,4 GHz ISM
	DSSS	1 o 2 Mpbs	2,4 GHz ISM
802.11a	OFDM	54 Mbps (max)	5,2 GHz UNII
802.11b	HR-DSSS	11 Mbps (max)	2,4 GHz ISM
802.11g	OFDM	54 Mbps (max)	2,4 GHz ISM

La velocità viene adattata dinamicamente sulla base del rapporto segnale/disturbo: per evitare le interferenze tra dispositivi che usano la stessa banda si sfrutta la tecnica **spread spectrum**, che consiste nell'utilizzare una banda più larga di quanto richiesto così che per i dispositivi non interessati questo venga interpretato come disturbo.
Le tecniche di modulazione utilizzate nelle trasmissione wireless sono quattro:

- **FHSS**, Frequency Hopping Spread Spectrum;
- **DSSS**, Direct Sequence Spread Spectrum;
- **HR-DSSS**, High Rate DSSS;
- **OFDM**, Orthogonal Frequency Division Multiplexing.

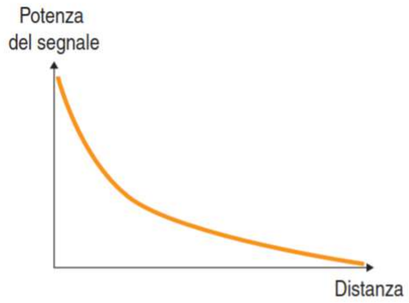
PER SAPERNE DI PIÙ

MODULAZIONI

Nel sistema FHSS il segnale modulato di tipo FKS o GFKS a una data frequenza viene fatto "saltare" da una canale all'altro, distribuendosi su una banda di frequenze. Il sistema DSSS è una tecnologia di trasmissione a "frequenza diretta" su banda larga dove ogni bit viene trasmesso come una sequenza ridondante, detta **chip**. HR-DSSS lavora in modo analogo a DSSS, ma utilizza un diverso tipo di modulazione, il **CCK** (*complementary code keying*), che consente di raggiungere data rate più elevati. OFDM divide il messaggio da trasmettere in diversi sotto segnali a bassa velocità che vengono trasmessi in parallelo a diverse frequenze: da questo fatto deriva il nome **ortogonalità**.

La diffusione delle reti wireless domestiche e soprattutto in ambiente scolastico ha suscitato discussioni in merito alla pericolosità per la salute degli utenti: sicuramente le radiazioni "non fanno bene", ma un telefono cellulare irradia dalle 20 alle 2000 volte la potenza irradiata dai comuni apparati per telecomunicazioni senza fili. Più precisamente:

- potenza massima irradiata da un telefono cellulare GSM: ≈ 2 W;
- grazie all'efficienza migliorata delle reti più recenti, il 3G irradia una potenza da 0,125 W a 0,25 W, il 4G LTE da 0,2 W a 0,25 W, il 5G da 0,2 W a 0,4 W.



Inoltre l'intensità della radiazione emessa è inversamente proporzionale al quadrato della distanza e quindi è praticamente impossibile che un utente venga raggiunto dalla potenza massima del trasmettitore.

CDMA e CTS/RTS

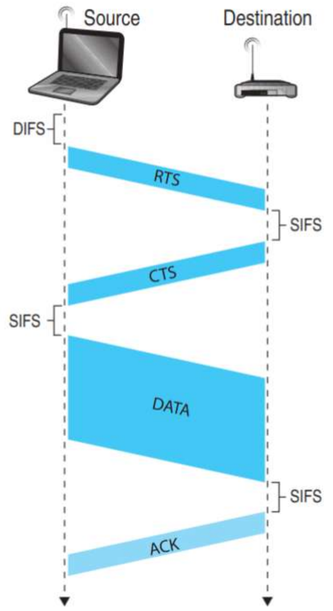
Il protocollo di accesso al canale condiviso più diffuso nelle reti wireless e nelle tecnologie cellulari è lo stesso utilizzato da **Ethernet**, cioè *Code Division Multiple Access* (**CDMA**): un "codice" unico viene assegnato a ciascun utente (*code set partitioning*) che condivide con gli altri la stessa frequenza, ma ciascun utente ha una propria sequenza "chipping" per codificare i dati.

Nello standard 802.11 sono previste due modalità di funzionamento:

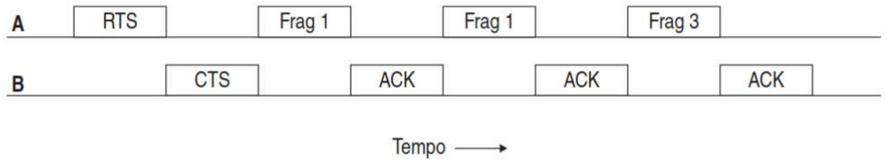
- DCF (*Distributed Coordination Function*), prevede che siano le stazioni a gestire l'accesso al mezzo trasmissivo secondo il protocollo CSMA/CA;
- PCF (*Point Coordination Function*) affida all'AP la coordinazione di tutte le stazioni nella sua cella (è raramente implementato).

Diversamente da Ethernet non si rilevano le collisioni anche perché c'è difficoltà in ricezione (**sense collision**) a causa della debolezza del segnale ricevuto (**fading**); per evitare collisioni durante la trasmissione è possibile per il mittente "prenotare" il canale mediante il meccanismo **RTS/CTS**: il mittente inizia a trasmettere un piccolo pacchetto **RTS** (*request-to-send*) all'AP usando CSMA e l'AP risponde diffondendo in broadcast il pacchetto **CTS** (*clear-to-send*) in risposta al pacchetto RTS ricevuto.
Quindi inizia a trasmettere il pacchetto di dati e, dato che CTS è ricevuto da tutti i nodi, le altre stazioni rimanderanno eventuali trasmissioni.

Nella modalità **DCF** è prevista una tecnica di frammentazione dei frame che vengono scomposti in più frammenti, ognuno numerato e riscontrato separatamente (**ACK**): la motivazione principale alla base di questa scelta è che essendo l'etere molto rumoroso è molto alta la probabilità che le trasmissioni vengano danneggiate e, quindi, devono essere ritrasmessi i dati: è sicuramente meglio ritrasmettere piccole porzioni anziché il frame intero.

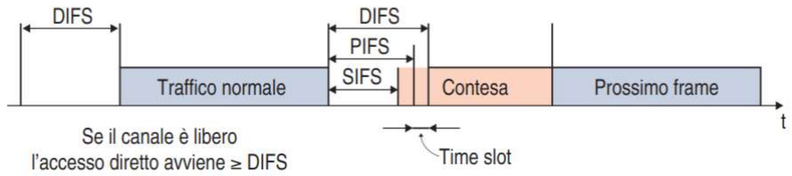


Quando il mittente acquisisce il canale con **RTS** e **CTS** può inviare in sequenza più frammenti generando quello che viene chiamato un **fragment burst**:



Si può osservare che tra i frame viene lasciato un intervallo di tempo (**IFS**, *Inter Frame Spacing*) definito nelle specifiche MAC, che può essere di dimensioni diverse a seconda del suo utilizzo:

- **DIFS** (*DCF, Distributed Coordination Function IFS*): se l'AP non ha nulla da trasmettere, trascorso l'intervallo DIFS, ogni stazione può tentare di acquisire il canale per iniziare una nuova trasmissione (bassa priorità);
- **PIFS** (*PCF, Point Coordination Function IFS*): è l'intervallo di dimensioni medie (media priorità) utilizzato per i servizi time-bounded che utilizzano PCF;
- **SIFS** (*Short Inter Frame Spacing*): è l'intervallo più breve (alta priorità), usato per separare i frame appartenenti a una singola trasmissione, tra i frame RTS, CTS, Frag e ACK di un fragment burst.



Si può osservare che la differenza di durata tra di essi equivale a un time slot.

Lo standard 802.11 definisce anche un ulteriore intervallo di tempo, l'**EIFS** (*Extended Inter Frame Space*), che viene usato al posto di DIFS dalle stazioni che hanno ricevuto un frame incomprensibile: la sua dimensione è la maggiore di tutti ed è stata studiata in modo tale da consentire a un'altra stazione di rispondere al frame ignoto, risincronizzandola.

Quando una stazione è pronta a trasmettere inizia a effettuare il controllo del mezzo trasmissivo (etere): se lo trova libero per tutta la durata di un IFS (la cui durata dipende dal tipo di servizio come prima descritto) può iniziare a inviare i dati; se il mezzo è occupato, la stazione deve attendere un DIFS e un tempo casuale di back-off per prevenire le collisioni, multiplo di un time-slot.

Problemi nelle trasmissioni wireless

Problematiche legate alla trasmissione delle onde nell'etere

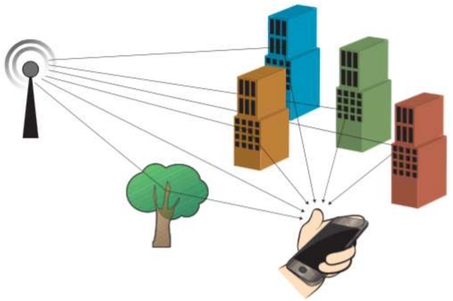
Riportiamo sinteticamente le principali differenze esistenti tra un sistema wireless e un sistema cablato dovute proprio al mezzo trasmissivo.

1. **Attenuazione del segnale**: le radiazioni elettromagnetiche hanno problemi nel superare gli ostacoli e l'indebolimento della potenza del segnale è in gran parte dovuto alle proprietà degli ambienti attraversati dall'onda. Nella seguente tabella vengono riportati alcuni livelli di attenuazione per i diversi materiali.

MATERIALI	INDEBOLIMENTO	ESEMPI
Aria	Nessuno	Spazio aperto, cortile
Legno	Debole	Porta, tavola, separatore
Plastica	Debole	Separatore
Vetro	Debole	Finestre non colorate
Vetro colorato	Medio	Finestre colorate
Mattoni	Medio	Muri
Gesso	Medio	Separatore
Ceramica	Alto	Pavimentazione
Cemento	Alto	Muri portanti, piani, piloni
Vetro blindato	Alto	Vetri anti-proiettili
Metallo	Molto alto	Cemento armato, specchi, armadi metallici, cabine di ascensori

Nello spazio "libero" l'intensità del segnale si attenua al crescere della distanza (path loss).

2. **Interferenze da parte di altre sorgenti**: l'etere è "saturo " di dispositivi che trasmettono a radiofrequenza; la frequenza wireless standard come per esempio a 2,4 GHz è condivisa da altri dispositivi, come per esempio la telefonia cellulare; anche rumori ambientali, come motori, trasformatori, telecomandi ecc. causano problemi legati all'interferenza dei segnali.
3. **Propagazione su più cammini**: oltre all'**assorbimento** del segnale nei materiali prima descritti, il segnale si riflette su oggetti e sul terreno, compiendo cammini di diversa distanza tra trasmittente e ricevente e quindi subisce un indebolimento dovuto alla **riflessione**, alla **rifrazione** e alla **diffrazione**. Quando l'onda incontra oggetti più piccoli della lunghezza d'onda, come la vegetazione, le nuvole, i segnali stradali ecc. si possono inoltre verificare problemi di **SCATTERING**.



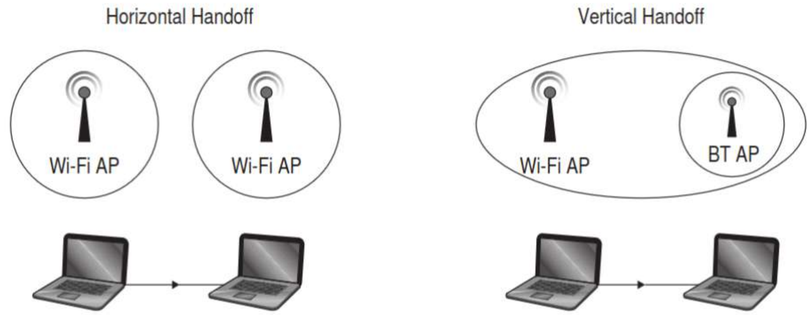
SCATTERING
È il fenomeno che si verifica quando la luce colpisce le molecole sospese, per esempio nell'aria: parte di essa viene in parte diffusa, cioè deviata dall'originaria traiettoria di propagazione, e in parte trasmessa, proseguendo il cammino lungo la stessa direzione di incidenza.

4. **Shadowing**: un problema molto frequente nei sistemi radiomobili è quello delle zone d'ombra dato che in ambito urbano, la presenza di edifici e ostacoli di ogni genere, può creare problemi nella propagazione delle onde elettromagnetiche.
5. **Effetto Doppler**: a causa del moto dell'utente rispetto alle stazioni radio base si verifica anche questo importante problema.

Problemi di posizionamento degli host

Handoff

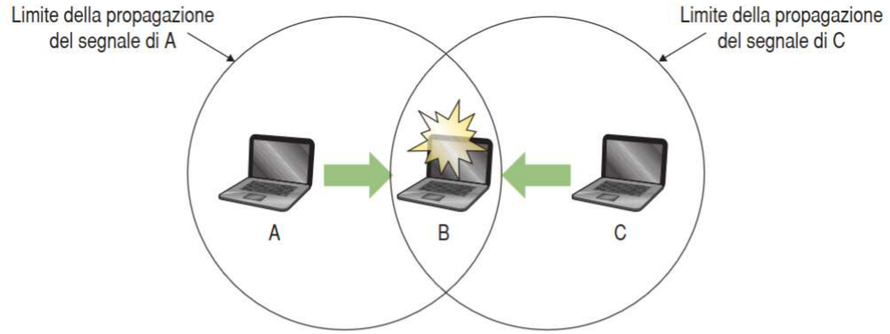
Si definisce **handoff** la situazione in cui l'host si sposta dall'area di copertura di una stazione base a un'altra cambiando il suo punto di collegamento con la rete globale.
Esistono due tipi di handoff: quello **orizzontale**, che si verifica quando un terminale effettua il passaggio tra gli AP della stessa tecnologia, e quello **verticale**, che si verifica quando un terminale effettua il passaggio tra gli AP di diverse tecnologie.

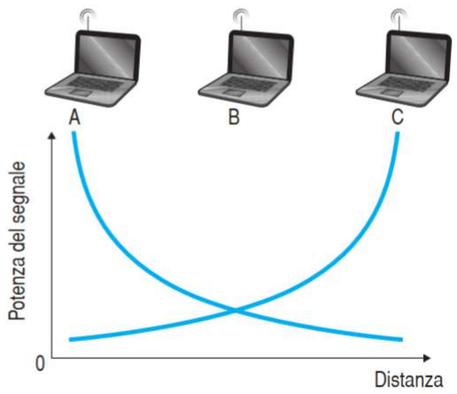


È intuitivo pensare che queste discontinuità portano a una riduzione della qualità del servizio: se per esempio un utente sta guardando un filmato in streaming mentre si muove, a un certo punto avviene l'handoff durante il quale l'utente non riceve più i nuovi dati e quindi la visualizzazione del filmato sarà ferma all'ultimo dato ricevuto, fino al passaggio dell'handoff.

Problema della stazione nascosta (hidden terminal)

Siano date tre stazioni A, B, C con i raggi d'azione raffigurati, e A stia trasmettendo a B: se C ascolta il mezzo trasmissivo lo troverà libero e sarà convinta di poter trasmettere a B, ma cominciando a trasmettere disturberà la trasmissione di A, impedendo a B di riceverla.
Quindi sia A che C saranno costrette a ritrasmettere il messaggio: questo è noto come il problema della **stazione nascosta.**



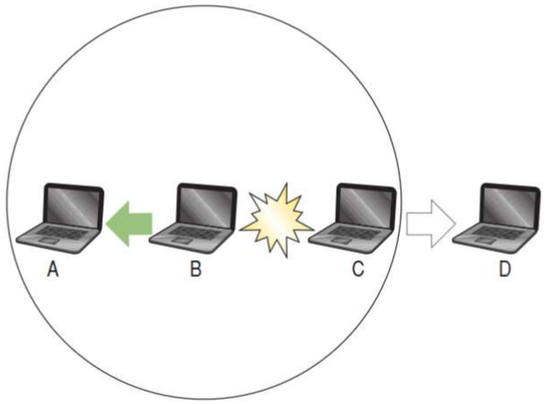


- B e A possono comunicare
- B e C possono comunicare
- A e C non possono sentirsi ma possono causare interferenza

> Stazioni mittenti in collisione non sono in grado di rilevare tale condizione, ma credono che la trasmissione stia avvenendo con successo.

Problema della stazione esposta (Exposed Terminal)

È il problema inverso del precedente: supponiamo che B stia trasmettendo ad A e che C voglia trasmettere a D: ascoltando l'etere, C sentirà la trasmissione di B e concluderà erroneamente di non poter trasmettere; invece, essendo D fuori della portata di B e A fuori della portata di C, le due trasmissioni potrebbero avvenire parallelamente senza interferenze.
Questo è noto come il problema della **stazione esposta.**



- B sta trasmettendo ad A
- C deve trasmettere a D
- C ascolta il canale e lo trova occupato, quindi aspetta (erroneamente)

> Una stazione mittente non inizia una trasmissione, anche se quest'ultima potrebbe avvenire con successo.

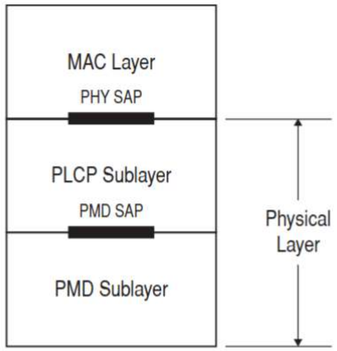
Struttura del frame 802.11

Prima di descrivere la composizione del **frame 802.11** vediamo brevemente come è organizzato il livello fisico che anche nelle reti wireless ha il compito di fornire un canale per la comunicazione attraverso la definizione di specifiche relative alla parte elettrica, meccanica e procedurale.

Livello fisico (physical layer)

Nelle WLAN esistono differenti tipi di livelli fisici, ognuno dei quali si contraddistingue principalmente in base al meccanismo di trasmissione; a partire dalle prime versioni di 8**02.11**, che si basavano su FHSS e DSSS si sono, con il passare del tempo e con il superamento di problemi tecnologici, implementati nuovi sistemi di trasmissione, come:

- **HR-DSSS**: definito per **802.11b**;
- **OFDM**: su cui si basa il più recente **802.11a**.



Lo standard prevede una scomposizione in due sottolivelli per il physical layer:

- **PLCP**, *Physical Layer Convergence Protocol*: interfaccia il MAC con il livello sottostante;
- **PMD**, *Physical Medium Dependent*: provvede alla trasmissione e alla ricezione interfacciandosi al mezzo (l'etere).

Al **MAC** giunge il **frame 801.11** cosi composto:

dove il **PLCP header** contiene le informazioni per l'interfacciamento tra lo strato **PMD** e **MAC** ed è previsto uno specifico **PLPC** per le diverse tecniche di trasmissione, in particolare per:

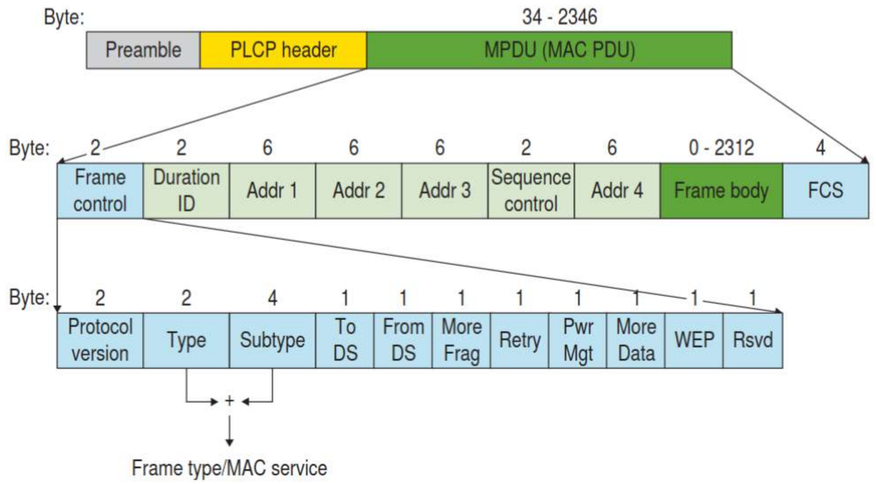
- FHSS;
- DSSS in 802.11 (1 ÷ 2 Mb/s);
- DSSS in 802.11a (6 ÷ 54 Mb/s);
- DSSS in 802.11b (1 ÷ 11 Mb/s);
- DSSS in 802.11g (1 ÷ 54 Mb/s);

e serve per definire la velocità operativa, il tipo di modulazione e la codifica da utilizzare per i dati.

Formato del frame

Lo **standard IEEE 802.11** specifica il formato di tutti i campi dei tre tipi di frame previsti, **Dati**, **Controllo** e **Gestione**, aventi la stessa struttura composta da una header, un body di lunghezza variabile e un Frame Check Sequence di 32 bit (FCS).
La sequenza di bit viene passata dall'entità MAC al PLCP a partire dal primo bit del campo **Frame Control** fino all'ultimo bit del campo FCS.

I frame di tipo "Dati" (**Data frame**) hanno la struttura rappresentata nella figura seguente.



Nel dettaglio il **Frame Control** è composto dai seguenti campi:

- **Protocol Version**: zero per lo standard 802.11;
- **Type**: tipo di frame, che può assumere tre valori: data, gestione, controllo;
- **Subtype**: sottotipo di frame (RTS, CTS, Ack o gestione);
- **ToDS**: quando è impostato indica che la destinazione è il distribution system;
- **FromDS**: quando è impostato indica che proviene dal distribution system;
- **More fragments**: è impostato a 1 se a esso seguono altri frammenti della stessa comunicazione;
- **Retry**: è impostato a 1 se il frame è una ritrasmissione;
- **Power Management**: è impostato a 1 se al termine la stazione va in Power Save mode (PS);
- **More Data**: è impostato a 1 se l'AP ha altri dati per la stazione che è in PS;
- **WEP**: è impostato a 1 se nel campo Frame Body ci sono dati che devono essere analizzati con l'algoritmo WEP;
- **Order**: se è impostato a 1 indica che la trasmissione è soggetta a restrizioni.

ESEMPIO

Vediamo per esempio il significato delle quattro possibili combinazioni dei bit **ToDS** e **FromDS**.

1. Nella trasmissione tra stazioni che appartengono alla stesso **BSS** (*Basic Server Set*) si ha:

Byte:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				0	0						

2. Nella trasmissione del frame da una stazione verso il distribution system si ha:

Byte:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				1	0						

3. Se il frame è proveniente dal distribution system si ha:

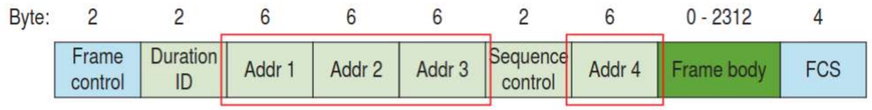
Byte:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				0	1						

4. Nel caso di trasmissione STA appartenente a un altro BSS, trasmessi tra AP attraverso wireless distribution system i due flag sono impostati a 1:

Byte:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				1	1						

Il campo **Duration ID** consente alle stazioni che hanno ricevuto il frame di prevedere per quanto tempo il mezzo rimarrà occupato.

Gli indirizzi sono quattro, in quanto, oltre agli indirizzi delle stazioni di origine e di destinazione, sono presenti anche quelli degli AP di entrata e uscita nelle comunicazioni fra celle differenti.



Gli indirizzi sono tutti nel formato standard IEEE 802 a 48 bit e hanno un diverso contenuto a seconda del valore dei bit **ToDS** e **FromDS**.

TO DS	FROM DS	ADDRESS 1	ADDRESS 2	ADDRESS 3	ADDRESS 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

dove:

- **DA** = Destination MAC Address
- **SA** = Source MAC Address
- **RA** = Receiver Address indica il MAC Address della stazione WM che ha ricevuto il frame
- **TA** = Transmitter Address indica la stazione che ha trasmesso il frame in WM
- **BSSID**: identificativo di sei byte (48 bit) di ogni BSS

Il risparmio energetico nella trasmissione

I dispositivi portatili e/o mobili in generale per poter operare hanno bisogno di sorgenti esterne di energia (batterie, celle solari) che hanno notoriamente una durata che generalmente non supera le 24 ore per un utilizzo medio oltre ad avere un tempo di vita limitato.
Con l'aumentare delle prestazioni dei dispositivi portatili aumentano le richieste di energia e le aspettative di autonomia dei dispositivi da parte degli utenti: se da una parte si stanno studiando nuove tecnologie, per le batterie occorre mettere in atto tutte le tecniche possibili per cercare di evitare il più possibile sprechi di energia per massimizzare il tempo in cui i dispositivi possono essere operativi.

Se analizziamo un laptop, gli elementi che hanno un consumo energetico significativo sono il microprocessore (CPU), lo schermo LCD, l'hard disk, la system memory (DRAM), la keyboard/mouse, CD-ROM drive, I/O subsystem e la wireless network interface card; l'interfaccia per le comunicazioni wireless radio è una delle componenti più significative (dopo il display) del consumo energetico.

ESEMPIO
In un laptop possiamo così ripartire il consumo energetico:
- Display e schede video grafiche: 45-50%;
- CPU + memoria: 25-30%;
- Interfaccia Wi-Fi, Bluetooth, 5G: 15-20%;
- SSD: 5-10%;
- Sistemi di raffreddamento: 10-20%;
- Retroilluminazione tastiera: 5-10%.

Dalla fine degli anni '90 si è iniziato a ricercare tecniche per abbassare il consumo energetico dell'interfaccia radio, sostanzialmente dovuto a due fattori:
- **computazione**: processing associato alle operazioni del protocollo;
- **comunicazione**: uso del transceiver per inviare e ricevere pacchetti dati e di controllo.

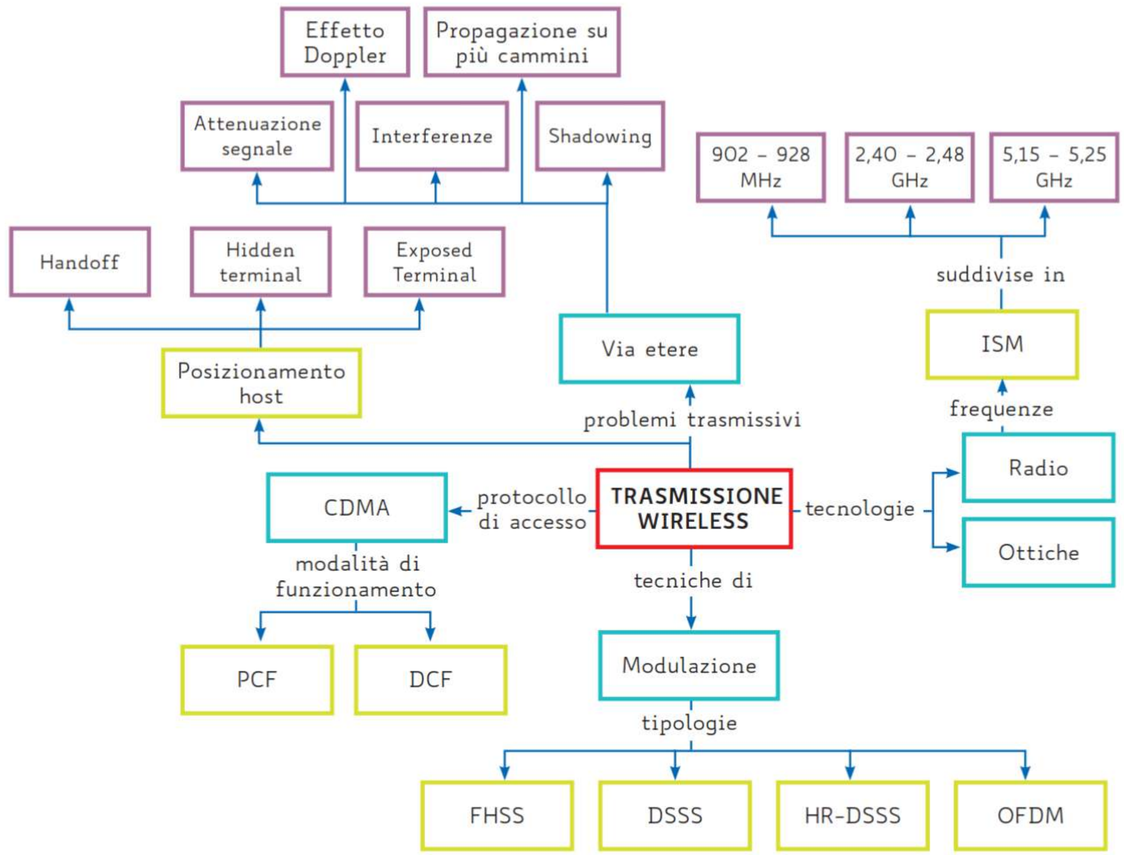
Tra computazione e comunicazione c'è comunque un conflitto di esigenze: i protocolli a basso consumo energetico per la comunicazione tipicamente aggiungono complessità di calcolo e quindi necessitano di maggior computazione con maggior spreco di energia.

Inoltre una ulteriore problematica è legata al posto dove fisicamente viene elaborata l'informazione, cioè in locale o in rete: processare le informazioni in rete può ridurre la necessità di comunicazione ma richiede maggiore energia "consumata" dai nodi che la elaborano.

I protocolli di comunicazione a basso consumo energetico cercano di ottimizzare questi compromessi.

MAPPA CONCETTUALE

didattica inclusiva



Che cosa abbiamo imparato?

- Nelle reti WLAN le bande ISM (2.4 GHz, 5 GHz) sono usate per trasmissioni wireless.
- Le tecniche di modulazione includono FHSS, DSSS, HR-DSSS e OFDM.
- Problemi come interferenze e shadowing possono ridurre la qualità del segnale.
- Lo standard 802.11 definisce le modalità come DCF e PCF per la gestione delle reti.
- Il livello fisico nelle reti WLAN si divide in PLCP e PMD per l'interfacciamento.
- La struttura del frame 802.11 include header, body e FCS per garantire l'integrità.
- I meccanismi RTS/CTS aiutano a evitare collisioni nelle trasmissioni wireless.

Ora prova tu a rispondere

- Illustra le tecnologie radio e ottiche nelle reti WLAN.
- Definisci le tecniche di modulazione FHSS e OFDM.
- Elenca i principali problemi delle trasmissioni wireless.
- Descrivi la struttura del frame 802.11 e il suo scopo.
- Spiega il ruolo di RTS/CTS nella prevenzione delle collisioni.

VERIFICA DI FINE LEZIONE

VERIFICA... le conoscenze

COMPLETAMENTO

1. Le reti WLAN possono essere realizzate mediante due diverse tecnologie:
   - ..... • .....
2. Le tecniche di modulazione utilizzate nella trasmissione wireless sono quattro:
   - ..... • .....
   - ..... • .....
3. Il protocollo di accesso al canale condiviso più diffuso nelle reti wireless e nelle tecnologie cellulari è lo stesso utilizzato da Ethernet, cioè ..... che nello standard 802.11 prevede due modalità di funzionamento:
   - ..... • .....
4. Il mittente prenota il canale mediante il meccanismo .....: inizia a trasmettere un piccolo pacchetto ..... all'AP usando ..... e l'AP risponde diffondendo in broadcast il pacchetto ..... in risposta al pacchetto ..... ricevuto.
5. Tra i frame viene lasciato un intervallo di tempo ..... definito nelle specifiche MAC, che può essere di dimensioni diverse a seconda del suo utilizzo:
   - ..... • .....
   - .....
6. Problematiche legate alla trasmissione delle onde nell'etere:
   1. ..... 4. .....
   2. ..... 5. .....
   3. .....
7. Problematiche legate al posizionamento degli host:
   1. .....
   2. .....
   3. .....

VERO/FALSO

1.	Le reti WLAN radio utilizzano prevalentemente la banda di frequenze ISM: 2,4 ÷ 2,48 GHz.	V	F
2.	La potenza massima irradiata da un telefono cellulare GSM: ≈ 2 W.	V	F
3.	La potenza massima irradiata in tecnologia Spread Spectrum: 0,001 ÷ 0,1 mW.	V	F
4.	Per evitare collisioni durante la trasmissione il mittente utilizza il meccanismo RTS/CTS.	V	F
5.	In Ethernet si rilevano le collisioni con il protocollo CSMA/CA.	V	F
6.	Nella modalità DCF è prevista una tecnica di frammentazione dei frame.	V	F
7.	La differenza di durata tra gli IFS equivale a un time slot.	V	F
8.	Nel gesso l'attenuazione del segnale è maggiore che nella plastica.	V	F
9.	Nel vetro colorato l'attenuazione del segnale è maggiore che nella plastica.	V	F
10.	HR-DSSS è definito per 802.11b mentre l'OFDM è nel più recente 802.11a.	V	F

LEZIONE

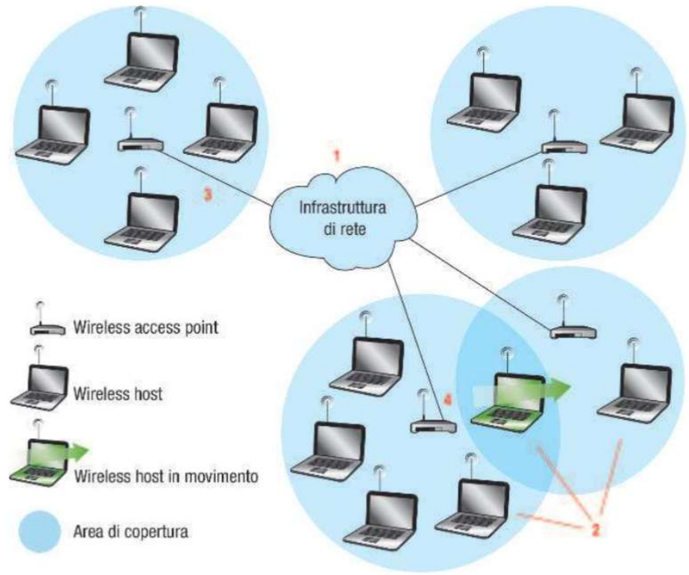
4 L'architettura delle reti wireless

IN QUESTA LEZIONE IMPAREREMO...

- i componenti di una rete wireless
- le topologie e le architetture di rete wireless

Componenti di una rete wireless

Prima di definire le diverse architetture e/o topologie, individuiamo nello schema seguente i **componenti di una rete wireless**.



1. **Infrastruttura di rete**: rete con la quale l'host wireless vuole connettersi.
2. **Host wireless**: possono essere laptop, PDA, telefoni IP che mandano in esecuzione applicazioni TCP/IP; non necessariamente devono essere mobili (per esempio la stampante connessa Wi-Fi).
3. **Collegamenti**: i dispositivi si connettono alla stazione base tramite l'etere mentre i collegamenti wired presenti nelle reti wireless sono usati per collegare la stazione base a una rete cablata: la presenza di un collegamento wired fa assumere alla rete il nome di "rete con infrastruttura".
4. **Stazione base**: è in genere connessa a una rete cablata e ha la funzione di ripetitore in quanto è responsabile dell'invio di pacchetti tra reti cablate e host wireless nella sua "area di copertura" (prende il nome di **Cell Tower** nelle reti cellulari e di **access point** nelle **LAN 802.11**).

Possiamo definire la seguente tassonomia delle reti wireless.

1. **Hop singolo, senza infrastruttura**: non è presente nessuna stazione base dato che la rete è composta da un singolo nodo che gestisce la trasmissione (esempio: Bluetooth).
2. **Hop singolo con infrastruttura**: una stazione è collegata alla rete cablata e gli altri dispositivi sono collegati con un singolo hop tra host e stazione (esempio: rete 802.11 di casa, di una biblioteca ecc.).
3. **Hop multipli, senza infrastruttura**: non vi è nessuna stazione base e la destinazione può essere raggiunta attraverso i nodi intermedi, che possono essere mobili (esempio: rete mobile *ad hoc*, rete veicolare *ad hoc*).

4. **Hop multipli con infrastruttura**: un host (la stazione base) è collegata alla infrastruttura mentre i nodi si connettono wireless alla stazione base e trasmettono i dati anche tra di loro (esempio: reti di sensori wireless, reti mesh wireless).

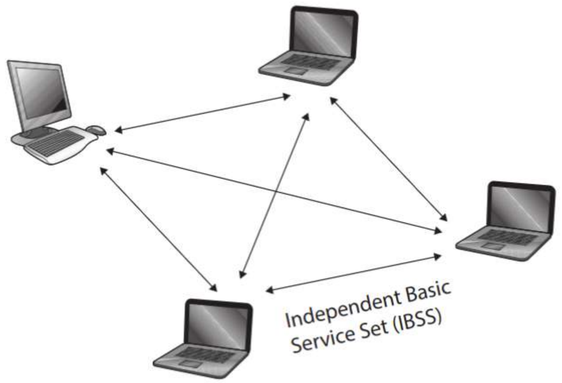
Lo **standard 802.11** definisce due topologie di rete:

- **reti IBSS** (Independent Basic Service Set) o reti *ad hoc*;
- **reti ESS** (Extended Service Set) o reti a "infrastruttura".

Con il termine *Extended Service Set* (**ESS**) si intende una configurazione che prevede il collegamento di due o più BSS in una singola sottorete: più AP comunicano tra loro, consentendo una ottimizzazione del traffico tra le stazioni.

Reti IBSS o modalità *ad hoc*

La prima tipologia di reti wireless non prevede l'utilizzo di infrastrutture di supporto per la comunicazione; viene definita ad hoc e in essa le reti sono formate da un insieme di nodi mobili che comunicano fra loro attraverso link wireless.



L'Independent Basic Service Set (IBSS) è la forma più semplice di rete ad hoc, composta da un insieme di STA che comunicano senza l'aiuto di una infrastruttura e quindi ogni stazione può comunicare con un'altra stazione del medesimo IBSS senza che il traffico passi attraverso un AP centralizzato.

Nella topologia **IBSS** si realizzano comunicazioni peer-to-peer tra le stazioni (STA) che sono localizzate nella medesima area (**BSA**, *Basic Service Area*) e che costituiscono un insieme denominato *Basic Service Set* (**BSS**): il mezzo trasmissivo condiviso della WLAN è l'etere.

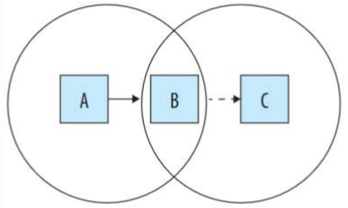
Le stazioni **STA** localizzate nell'area BSA sono sotto il controllo di una funzione di coordinamento che generalmente è del tipo distribuito, cioè *Distributed Coordination Function* (DCF), e quindi la funzione DCF deve essere presente in tutte le stazioni.

Esistono situazioni in cui viene applicato il concetto **master/slave** e il controllo è **concentrato** (PCF, *Point Coordination Function*), dove una STA viene eletta master ed effettua il polling verso le altre stazioni.

Nel tipo **distribuito** i nodi della rete possono liberamente e dinamicamente organizzarsi in maniera arbitraria e temporanea permettendo agli utenti di collaborare in modo improvvisato ovunque essi si trovino: essendo formate da nodi mobili, le reti ad hoc, sono note anche con il nome di **MANET** (*Mobile ad hoc NETwork*) e sono dinamiche, nel senso che, essendo i dispositivi mobili, continuano a cambiare di numero dato che quando un host si allontana esce dal raggio di azione della rete.

Ogni nodo di una rete ad hoc opera non solo come **host** ma anche come **router** provvedendo a instradare quei pacchetti che non possono essere trasmessi direttamente al destinatario a causa del limitato raggio d'azione, che però si trovano nella sua area di raggiungibilità.

ESEMPIO
A vuole trasmettere un messaggio a C ma non è in grado di raggiungerlo: B li raggiunge entrambi e quindi può fare funzione di router instradando i pacchetti di A verso C.



Ogni host appartenente alle rete **ad hoc** è in grado di configurarsi in modo tale da "far rimbalzare automaticamente" le informazioni verso un altro nodo che si trova più vicino al destinatario del pacchetto: per questo motivo le MANET sono reti "multi hop" in quanto, oltre a far comunicare direttamente due nodi che si trovano a breve distanza, possono trasmettere le informazioni anche tra due nodi lontani facendo "rimbalzare" le informazioni attraverso diversi nodi intermedi.

Dato che la topologia di queste reti è in continua mutazione per le connessioni/sconnessioni dei dispositivi, i meccanismi di routing devono essere continuamente rivisti e aggiornati.

Inserimento di una stazione in un IBSS

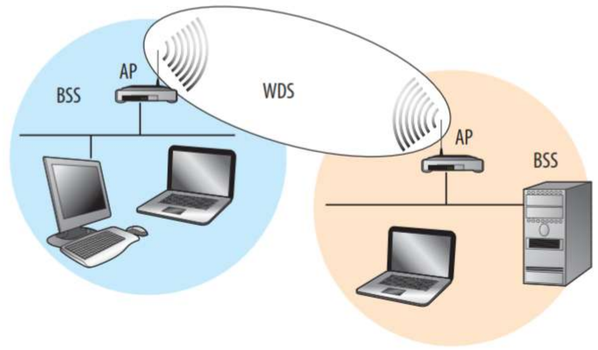
Quando una nuova stazione vuole unirsi a un IBSS deve sintonizzarsi e sincronizzarsi con le altre stazioni e lo fa mediante la scansione di tutti i canali, generalmente in modo passivo (*passive-scanning*): la stazione rimane in ascolto su ogni canale per un certo tempo in attesa che le giunga un **BEACON** e quando le arriva ne estrae il SSID e lo confronta con quello in suo possesso per verificare se ha l'autorizzazione per connettersi a quel IBSS.

BEACON
I **beacon** sono dei pacchetti speciali di Management che contengono le informazioni di Service Set ID (SSID) e timestamp necessarie alla sincronizzazione della stazione: in una rete ad hoc tutte le stazioni partecipano alla generazione di pacchetti di beacon.

Reti ESS

Le **reti ESS**, anche denominate di tipo Infrastructure, sono caratterizzate dalla presenza di una LAN di distribuzione denominata **distribution system**, che interconnette diversi BSS e trasporta a livello MAC le trame: può essere cablata oppure wireless e in questo caso prende il nome di *Wireless Distribution System* (**WDS**).

Un access point con l'insieme delle stazioni a esso associate (WT Wireless Terminal) prende il nome di BSS (Basic Service Set) e costituisce una cella il cui diametro è circa il doppio della copertura/distanza tra due stazioni wireless: ciascuna cella viene identificata tramite un numero unico di 48 bit, il BSS-ID.
Nella modalità infrastruttura, il BSS-ID corrisponde all'indirizzo MAC del punto di accesso.

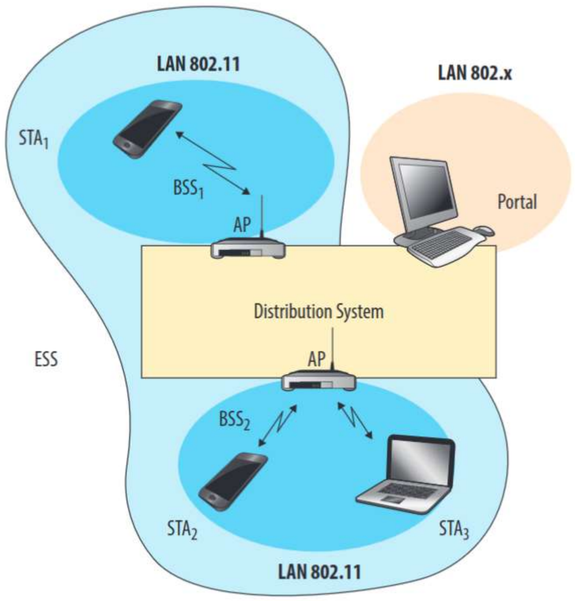


Non bisogna confondere il **BSS-ID** con il **SSID**: il primo è l'identificativo della cella mentre il secondo è il nome con cui una WLAN si identifica ai suoi utenti.

L'**SSID vuoto**, o a lunghezza zero, corrisponde a un'identità di broadcast ed è utilizzato nel probing delle reti disponibili. Inoltre, su alcuni **AP** si può inibire la trasmissione dell'**SSID**, in modo che solo chi conosce l'**SSID** della **WLAN** si possa associare.

L'AP coordina la trasmissione dei dati e la comunicazione tra i client e generalmente svolge anche la funzione di ponte tra LAN wireless, eventuali reti fisse e la rete telefonica pubblica (quindi anche Internet).
Tutto il traffico radio dei dati transita da e verso l'access point.

L'area coperta dal **BSS** è anche nota come **BSA** (**Basic Service Area**).



Le **reti ESS** sono costituite dall'unione di più Basic Service Set (BSS).

L'AP può essere visto come un bridge posto tra il BSS e il DS e il BSS può essere considerato come un'unica WLAN.

Una stazione presente sul sistema di distribuzione, detta **Portal**, interconnette la WLAN con altre reti: è un bridge tra il distribution system e un'altra rete wired.

I diversi **BSS** fisicamente possono essere locati all'interno di un **ESS** secondo diversi criteri:

- **BSS parzialmente sovrapposti**: permettono di fornire una copertura continua;
- **BSS fisicamente disgiunti**;
- **BSS co-locati** (diversi BSS nella stessa area): possono fornire una ridondanza alla rete o permettere prestazioni superiori.

Se un dispositivo mobile è in movimento può naturalmente raggiungere il confine della sua cella e deve poter essere "agganciato" dalla cella successiva, in modo da avere la permanenza della connessione.

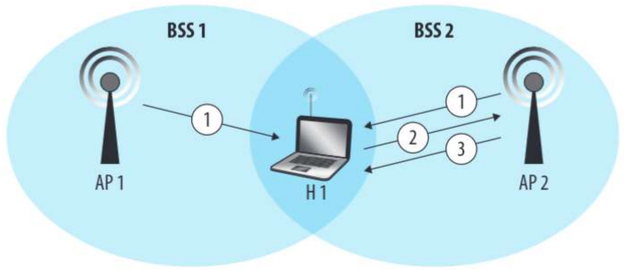
L'802.11 gestisce il passaggio tra stazioni con tre diverse modalità di transizione:

- **transizione tra ESS**: la stazione si sposta tra BSS appartenenti a due ESS diversi: la stazione può muoversi ma non si è in grado di mantenere la connettività dato che si passa da una LAN a un'altra;
- **transizione tra BSS**: in questo caso la stazione si sposta tra due diversi BSS parzialmente sovrapposti appartenenti allo stesso EES, questa situazione viene gestita in maniera trasparente per i livelli superiori;
- **statica**: la stazione è immobile o si sposta solo entro l'area di un singolo BSS, quindi il problema non sussiste.

Scanning in una rete

I dispositivi wireless per potersi connettere "fiutano" l'etere effettuando una scansione delle possibili frequenze di trasmissione. Lo **scan** può essere utilizzato per trovare una rete e connettersi a essa, per trovare un nuovo AP (**Roaming**) oppure per inizializzare una IBSS e può essere di tipo **passive** o **active**.

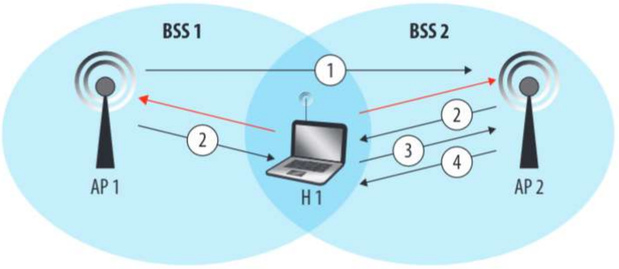
- **Tipo passive**, basato sulla trasmissione periodica di beacon che contengono il proprio codice SSID e il proprio indirizzo MAC (il BSS-ID).



1. Rimane in attesa per un certo tempo per la ricezione di un beacon.
2. La stazione seleziona l'AP migliore e invia a questo una richiesta di associazione con una trama Association-Request.
3. L'AP risponde inviando una trama Association-Response.

La STA si mette in ascolto su ciascun canale specificato nella Channel List della primitiva per il tempo specificato, aspettando di riconoscere dei frame di tipo beacon contenenti il particolare SSID scelto oppure aspettando di riconoscere un beacon con l'SSID broadcast, a seconda di quanto specificato nella primitiva stessa.

- **Tipo active**, dove l'AP risponde alle richieste di sondaggio da parte delle STA attraverso i **Probe-Request** inviando le conferme di **Probe-Response**. Per associarsi a un AP la stazione deve scambiare con esso tre tipi di pacchetti: un pacchetto chiamato "**Probe**" (dove *probe* ha il senso di sondaggio o indagine), un pacchetto di autenticazione e un pacchetto di associazione.



Questo meccanismo è adottato sulle reti di tipo di ESS in cui l'AP ha l'incarico di rispondere al probe-request.

Descriviamo le operazioni che vengono eseguite da una stazione che vuole entrare a far parte di una rete:

1. invia un pacchetto di management di tipo Probe-Request in broadcast con gli identificativi della rete cercata: questo pacchetto contiene informazioni sulla stazione 802.11 come il bit rate supportato dalla stazione, il SSID di appartenenza della stazione ecc.;

2. rimane in attesa per un certo tempo di ricevere il pacchetto di Probe-Response: se non riceve risposta passa al canale successivo (nel caso in cui non abbia un canale fisso preimpostato);
3. la stazione seleziona l'AP migliore e invia a questo una richiesta di associazione con una trama **Association-Request**;
4. l'AP risponde inviando una trama **Association-Response**.

Il ruolo dell'access point

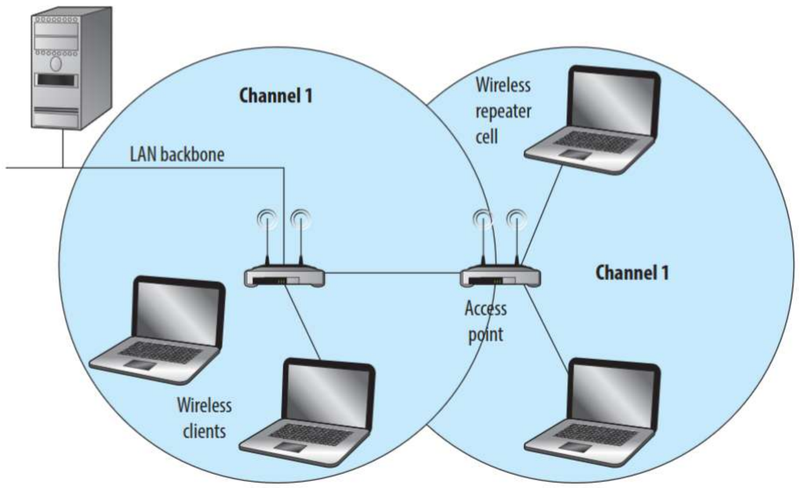
Un **access point** è un'entità che permette la distribuzione dei servizi MAC via Wireless Medium (WM) per le stazioni a esso associate. In genere è una sorta di bridge locale che interfaccia la **rete wireless** con una **wired** e copre una ben determinata area consentendo ai dispositivi di passare da una cella all'altra garantendo la connettività. Può anche essere utilizzato semplicemente come ripetitore di segnale ed effettua le funzioni di **bridging**, fondamentali per la traduzione dei frame tra la rete wired e wireless.
L'access point è tipicamente un apparato con ridotte funzioni che può essere configurato per funzionare in due modalità, come **root access point** oppure come **repeater access point**.

Root access point

Se viene configurato come **root access point** realizza le funzione di DCF e di apparato di associazione per le stazioni presenti nel BSS (Active Scanning): questa è la configurazione di default che troviamo in ogni AP.
Quando una stazione viene associata all'AP, questo ne scrive l'indirizzo MAC in una tabella che mantiene aggiornata con le nuove connessioni/disconnessioni.
Alla ricezione di un pacchetto dal WM, se l'indirizzo MAC di destinazione è presente nella tabella delle stazioni associate al AP, il pacchetto viene ritrasmesso nel WM, altrimenti se l'indirizzo MAC di destinazione non è presente nella tabella delle stazioni associate al AP il pacchetto viene tradotto e trasmesso nella porta wired (tipicamente Ethernet).
A quel punto, quando la porta wired riceve il pacchetto, si comporta in modo analogo alla **Default Route**: se l'indirizzo MAC di destinazione è presente nella tabella delle stazioni associate al AP il pacchetto viene tradotto e trasmesso nel WM mentre se l'indirizzo MAC di destinazione non è presente nella tabella delle stazioni associate al AP il pacchetto viene scartato.

Repeater access point

Se invece viene configurato come **repeater access point**, le stazioni in portata radio del Repeater risultano associate al root access point e alla ricezione di un pacchetto dal WM il repeater lo ritrasmette nel WM.
L'access point è quindi impiegato come Repeater nel WM che permette di utilizzare lo stesso canale ripetendo le trame con peggioramento delle prestazioni della rete: la stazione che si trova nell'area di sovrapposizione si aggancia al segnale migliore.



Servizi del distribution system

Anche se nello **standard 802.11** il **distribution system** (**DS**) non è esplicitamente specificato, sono specificati i servizi che il DS deve supportare e sono divisi in due sezioni:

- **Distribution System Services** (**DSS**);
- **Station Services** (**SS**).

La SS vale per entrambe le modalità di costituzione della WLAN mentre la DSS vale solo per le WLAN a infrastruttura: i "servizi di distribuzione" sono forniti dall'AP mentre i "servizi host" devono essere assolti da tutte le stazioni.

DSS (servizi di distribuzione)

- **Association** (associazione): appena una stazione entra nel raggio d'azione di un AP, invoca questo servizio per informare la stazione base della sua presenza nella BSS e comunica le proprie necessità; una STA non può associarsi con più di un AP in uno stesso momento, questo per assicurare che il servizio di distribuzione trovi un AP unico per trasportare i messaggi del DS.
- **Disassociation** (dissociazione): sia le stazioni sia gli AP possono terminare una precedente associazione; è una *notifica*, non una richiesta e quindi non può essere *rifiutata* da nessuna delle due parti.
- **Reassociation** (riassociazione): in una stazione in moto per supportare la transizione di tipo "BSS-transition" è necessario invocare il servizio di riassociazione in modo da trasferire il controllo da un AP all'altro; questo tiene informato il DS della mappa tra AP e STA quando quest'ultima si sposta da una BSS a un'altra.
- **Distribution** (distribuzione): viene utilizzato dalle stazioni per scambiarsi pacchetti che devono attraversare il DS: l'AP conosce la posizione delle diverse stazioni grazie al servizio di Association ed è in grado di smistare i frame che lo raggiungono verso le stazioni della propria cella (via radio) o verso gli altri AP, attraverso il sistema di distribuzione.
- **Integration** (integrazione): questo servizio gestisce la traduzione dei frame 802.11 verso le altre LAN IEEE 802.x. che utilizzano altri formati; il servizio di Integration provvede all'eventuale traduzione degli indirizzi e all'adattamento ai diversi media.

SS (Servizi host)

- **Authentication** (autenticazione): una stazione deve dimostrare di essere autorizzata a usufruire del servizio di trasmissione e l'AP deve a sua volta farsi riconoscere: un esempio di schema di autenticazione supportato è lo schema "a chiave condivisa" (shared key).
- **Deauthentication** (deautenticazione): una stazione che voglia abbandonare la rete deve "de-autenticarsi" e "dissociarsi"; la de-autenticazione è una notifica, non una richiesta e quindi non può essere rifiutata da nessuna delle due parti.
- **Privacy** (segretezza): bisogna raggiungere un livello di riservatezza dei dati paragonabile a quello di una rete cablata dato che i dati trasmessi via radio possono essere ascoltati da chiunque si trovi all'interno dell'area di diffusione: questo servizio gestisce la crittografia dei frame attraverso l'algoritmo RC4.
- **Transmission** (trasmissione): è il servizio principale usato dalla STA 802.11 e viene invocato da ciascun messaggio all'interno della ESS; in sintesi consiste nello scambio di frame fra due stazioni a livello di MAC sublayer.