1. SCENARI DI RETI SENZA FILI

La comunicazione a distanza e senza fili è stata realizzata dall'uomo in molte forme nel corso della storia. Nell'antichità c'era il *tam-tam*, un tipo di tamburo usato da alcuni popoli africani per diffondere un messaggio di villaggio in villaggio. Gli indiani d'America utilizzavano pelli di bufalo che, agitate sul fuoco, inviavano segnali di fumo a grandi distanze. Anche il codice Morse, usato alla fine dell'Ottocento per far comunicare le navi mediante luci pulsanti, è stato ed è tuttora una forma importante di comunicazione senza fili.
Al giorno d'oggi sono i telefoni cellulari a rappresentare il più diffuso esempio di comunicazione wireless.

LO SAI CHE

Una rete wireless permette alle persone di comunicare e di accedere ad applicazioni e informazioni senza l'utilizzo di connessioni via cavo.

L'arrivo dei personal computer negli anni Ottanta del secolo scorso e la necessità di organizzarsi in reti per il lavoro, ma anche il divertimento, non poteva prescindere dai grandi vantaggi che le trasmissioni via *etere* garantiscono.
Le interfacce wireless sono in grado di utilizzare servizi di rete che consentono l'uso di tutti gli optional che Internet offre: dalla posta elettronica alla navigazione, dai motori di ricerca ai social network, dalle videoconferenze all'accesso alle basi di dati. E tutto questo da qualunque luogo: da casa, dal posto di lavoro o da ambienti pubblici.
Le conseguenze sono molto vantaggiose sia per l'utente privato sia per le aziende. Per esempio: chi viaggia per lavoro può rispondere a un messaggio di posta elettronica mentre aspetta di imbarcarsi su un aereo, mentre uno studente può studiare e fare ricerche con il proprio notebook in biblioteca.
Ma il maggior vantaggio consiste nella facilità con cui si possono estendere le reti aziendali senza dovere effettuare nuovi e costosi cablaggi. Inoltre c'è la comodità di non dover più allestire postazioni fisse di lavoro.

LESSICO

Etere: secondo gli antichi, la parte più alta, pura e limpida dello spazio celeste. È lo spazio inteso come luogo di propagazione delle onde elettromagnetiche. Le onde elettromagnetiche non hanno bisogno di alcun mezzo materiale per propagarsi, basta il vuoto e, quando si dice propagazione via etere, etere è sinonimo di vuoto.

Grazie alle reti wireless, non è più l'utente che si sposta laddove c'è il sistema di elaborazione, ma è il sistema di elaborazione che si sposta con l'utente.

Esistono molti tipi di sistemi di comunicazione wireless, ma la caratteristica comune è la comunicazione tra dispositivi computerizzati, cioè dispositivi dotati di capacità di elaborazione, memorizzazione e input/output. Questi dispositivi includono: tablet, smartphone, notebook, netbook, router e stampanti.
La maggior parte dei produttori ormai integra nei dispositivi di elaborazione la scheda di rete wireless e l'antenna.

Le reti wireless possono utilizzare onde radio o segnali infrarossi per comunicare attraverso l'etere e, così come le reti wired, possono essere classificate in base all'estensione dell'area fisica che sono in grado di coprire:

- **WPAN** (*Wireless Personal Area Network*);
- **WLAN** (*Wireless Local Area Network*);
- **WMAN** (*Wireless Metropolitan Area Network*);
- **WWAN** (*Wireless Wide Area Network*).

La distinzione non è netta, ma solo indicativa dei principali ambiti d'applicazione delle varie tecnologie (figura 1).

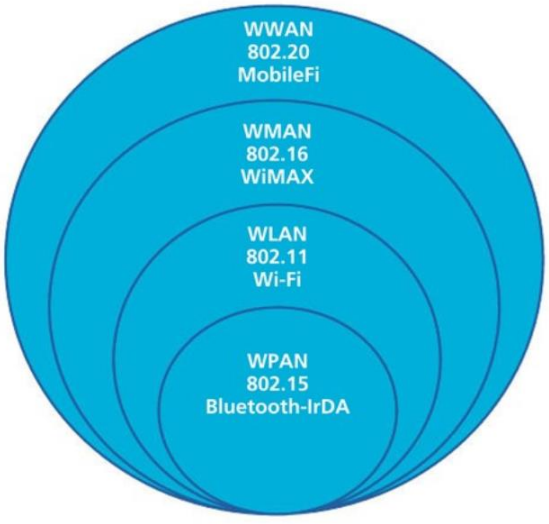


Figura 1 Classificazione delle wireless network

WPAN

Le reti **PAN wireless** coprono il campo d'azione di una persona (10-15 metri) e sono adatte per reti domestiche o per piccoli uffici. Una WPAN, per esempio, potrebbe consentire di sincronizzare in modo wireless il proprio tablet o palmare con un computer portatile per uno scambio di dati. Oppure l'installazione di periferiche come una stampante.

La maggior parte delle WPAN utilizza le **onde radio** per trasferire le informazioni attraverso l'etere. Per esempio, la specifica **Bluetooth** (figura 2) definisce una PAN wireless nella banda di frequenza libera **ISM** (frequenze radio assegnate per scopi industriali, scientifici e medici) a 2.4GHz (vedi Unità 11, volume del secondo biennio) con una portata di una decina di metri e una velocità di trasmissione massima di 2Mbps. Questa tecnologia nasce alla fine degli anni Novanta del secolo scorso a opera di un consorzio guidato dalla Ericsson.

Bluetooth è adatto ai dispositivi di piccole dimensioni, a corto raggio, a basso consumo e poco costosi e la sua specifica è nello standard IEEE 802.15 per le WPAN.

Altre WPAN utilizzano invece **segnali infrarossi** per trasferire le informazioni da un dispositivo a un altro. La specifica **IrDA** (*Infrared Device Application*) definisce una tecnologia di interconnessione dati tramite infrarossi, di tipo bidirezionale, point-to-point, tra dispositivi posizionati in visibilità reciproca **LoS** (*Line of Sight*), con range ridotto (1-2 metri) e *bit rate* di 4Mbps.

Il vantaggio degli infrarossi è la mancanza di interferenze radio. Per contro, la necessità del contatto visivo tra i dispositivi limita le possibilità di posizionamento dei dispositivi stessi. Un pannello divisorio di un ufficio, per esempio, è sufficiente a bloccare il segnale. Per questo motivo, i raggi infrarossi vengono soprattutto utilizzati per connettere via etere tastiere e mouse con personal computer.

Uno dei campi nei quali più si vanno diffondendo le WPAN è la domotica.

Il termine **domotica** (anche nota come *home automation*), indica la disciplina che si occupa delle tecnologie atte a migliorare la qualità della vita nelle case, creando le cosiddette **case intelligenti**.

L'obbiettivo è l'integrazione dei dispositivi di controllo e trasduzione e dei sistemi di interconnessione (*sensor networking*) che si trovano nelle abitazioni.

Figura 2 Logo Bluetooth

LO SAI CHE

Due o più periferiche che condividono un canale di Bluetooth danno vita a una **piconet**, che può essere composta da un numero massimo di otto dispositivi. In ogni piconet un dispositivo assume il ruolo di *master* mentre gli altri assumono il ruolo di *slave* in un collegamento a stella. La **scatternet** è invece costituita da più piconet i cui master comunicano tra loro.

LO SAI CHE

La Wi-Fi Alliance è stata formata nel 1999 per guidare l'adozione di un unico standard per la banda larga senza fili nel mondo. Wi-Fi Alliance è inoltre proprietaria del trademark Wi-Fi che certifica l'interoperabilità di un dispositivo con lo standard wireless IEEE 802.11.

WLAN

Le **LAN wireless** sono simili alle tradizionali LAN Ethernet cablate sia per prestazioni e costi sia per funzionamento e componenti utilizzate. Di fatto, anche i protocolli LAN wireless sono analoghi ai protocolli LAN Ethernet e soprattutto i formati sono completamente compatibili tra loro. Questo rende facile estendere una rete cablata preesistente con componenti wireless.

Lo standard più diffuso per le WLAN è l'IEEE 802.11 (vedi Unità 11, volume del secondo biennio). Le ultime versioni in commercio sono la 802.11g (a 2,4 GHz), la 802.11n (a 2,4 GHz e a 5 GHz) e la 802.11ac (a 5 GHz). La figura 3 riassume le velocità (teoriche) dei tre standard.

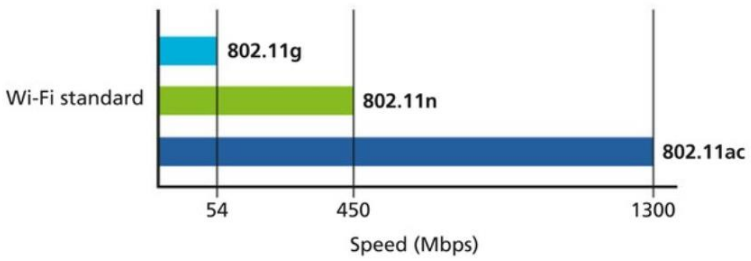


Figura 3 Confronto tra le velocità degli standard 802.11

Ricordiamo che i dispositivi che costituiscono le reti LAN wireless sono:

- i **Wireless Terminal** (WT): sono dispositivi mobili (notebook, smartphone, tablet, ecc.) dotati di interfaccia 802.11, integrata o su schede PCMCIA o USB, oppure fissi (PC) con schede PCI o adattatori USB;
- gli **Access Point** (AP): hanno un doppio uso, sono sia bridge che collegano la parte cablata (*wired*) con la parte wireless, sia consentono ai WT di collegarsi alla rete wireless (agisce quindi da gateway).

LO SAI CHE

Nella maggior parte delle configurazioni, gli Access Point hanno un lato cablato che li collega agli switch e quindi al router della LAN aziendale per la connessione a Internet.

L'insieme formato dall'Access Point e dalle stazioni poste nella sua zona di copertura è detto **Basic Service Set** (**BSS**), ovvero **insieme di servizi di base**, e costituisce una **cella**. Ogni BSS è identificato da un BSS-ID, un identificativo di 6 byte (48 bit). Nella cosiddetta modalità **infrastruttura** (di default dallo standard 802.11b in poi), nella quale i client senza fili sono connessi a un punto di accesso, il BSS-ID corrisponde all'indirizzo MAC del punto di accesso.
È possibile inoltre collegare più AP alla rete cablata o tra loro (*roaming*) creando un **Wireless Distribution System**. Gli AP in questi casi funzionano come un bridge tra BSS e Wireless Distribution System.
Due o più BSS collegati tra loro da un Wireless Distribution System costituiscono un **ESS** (**Extended Service Set**). L'ESS appare come una unica WLAN (**figura 4**).

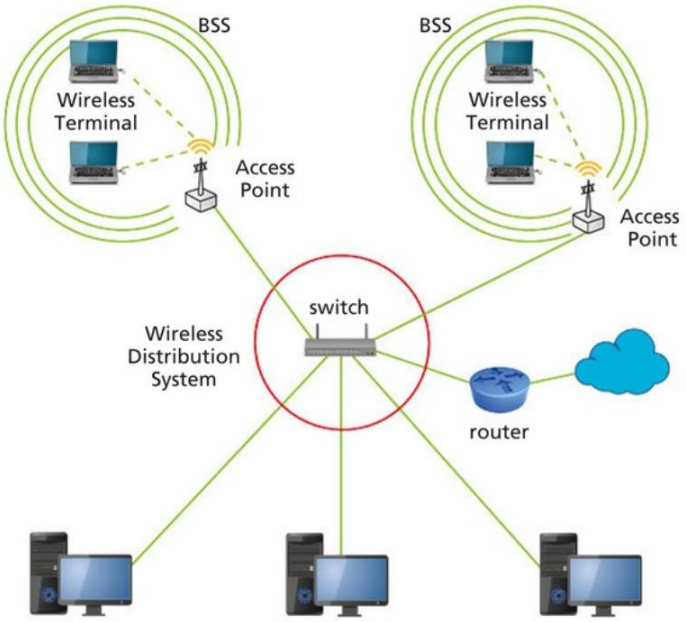


Figura 4 Rete WLAN aziendale (ESS) con parte cablata e infrastruttura wireless

All'interno di un ESS, i diversi BSS fisicamente possono essere locati 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.

La sempre maggior diffusione dei dispositivi mobili collegati in reti wireless ha posto il problema di come consentire la permanenza della connessione a fronte di spostamenti che portano il dispositivo fuori dal raggio d'azione di un Access Point.
Lo standard 802.11 gestisce la mobilità delle stazioni distinguendo tre tipi di transizioni:

- **transizione statica**: la stazione è immobile o si sposta solo entro l'area di un singolo BSS;
- **transizione tra BSS**: la stazione si sposta tra due diversi BSS, parzialmente sovrapposti, appartenenti allo stesso ESS (la connessione resta attiva e non c'è cambiamento di indirizzo IP);
- **transizione tra ESS**: la stazione si sposta tra BSS appartenenti a due ESS diversi.

In quest'ultimo caso la connessione attiva viene chiusa in quanto ci troviamo di fronte al passaggio da una WLAN a un'altra. Appena entrati nel raggio d'azione della nuova WLAN occorrerà aprire una nuova connessione con conseguente assegnazione di un nuovo indirizzo IP.
Nelle reti domestiche, l'Access Point funge anche da router-switch, spesso dotato anche di funzionalità firewall, e viene collegato a una connessione Internet a banda larga, per esempio ADSL. La normale portata di un router WLAN è sufficiente a coprire un appartamento, una casa (anche su due piani) o un ufficio.

Un altro scenario importante è quello rappresentato da ospedali, magazzini o ristoranti che vogliano offrire l'accesso a un database centrale ai propri dipendenti mediante dispositivi mobili come palmari o tablet: un magazziniere potrà aggiornare l'inventario ed effettuare un nuovo ordine direttamente dal magazzino e un cameriere potrà trasmettere le ordinazioni in cucina riducendo il tempo di attesa dei clienti. Un medico può richiedere un prelievo al laboratorio tramite un dispositivo mobile e, da questo, vedere il referto appena pronto. Una rete wireless connessa al database contenente le informazioni mediche dei pazienti aumenta la velocità e l'efficacia dell'assistenza sanitaria.
L'utilizzo di una periferica mobile che trasmetta i dati raccolti, attraverso una connessione wireless, a un database centralizzato garantisce tempestività e assicura maggior precisione.

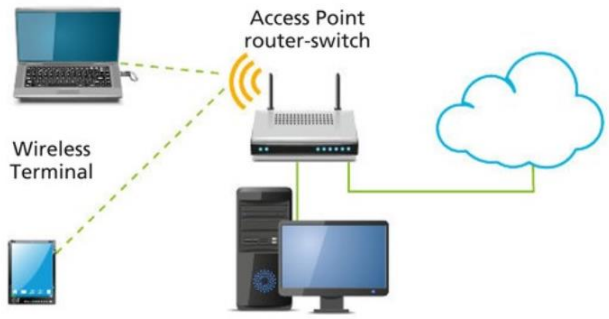
La configurazione di un Access Point in una rete aziendale (figura 4) o domestica (figura 5) prevede l'impostazione di una serie di parametri:

- **SSID** (*Service Set Identifier*): serve ad assegnare un nome alla WLAN affinché gli utenti possano identificarla. L'Access Point può essere configurato per trasmettere in broadcast e in continuazione con l'SSID attraverso un frame periodico detto *beacon*. In questo modo, i wireless terminal sono in grado di rilevare l'elenco delle reti wireless esistenti nel loro raggio d'azione. Non c'è una corrispondenza biunivoca tra Access Point e SSID: è normale che più Access Point condividano lo stesso SSID se forniscono accesso alla stessa rete (tipico delle reti aziendali come in figura 4), ma è anche possibile che uno stesso Access Point si presenti con più SSID, se fornisce accesso a diverse reti. Disabilitando il broadcast di un SSID, è possibile nascondere una rete, cioè far sì che il suo nome non appaia negli elenchi delle reti disponibili. La rete resta comunque individuabile.
- **Potenza**: la normativa tecnica ETS 300-328 dell'ETSI impone di non irradiare segnali con una **EIRP** (*Effective Isotropic Radiated Power*) ovvero Potenza Isotropica Effettiva Irradiata (isotropica significa in ogni direzione) cioè la potenza che effettivamente è emessa dall'antenna, somma della potenza dell'Access Point con il *guadagno dell'antenna,* superiore a 100mW per la banda a 2.4GHz e 1W per la banda a 5GHz.
- **Canale**: si può impostare l'Access Point affinché lavori su uno qualsiasi dei canali disponibili compresi tra 1 e 13. Quando si installa un solo Access Point, il canale scelto non ha importanza. Se invece si installano più Access Point in una WLAN o se due WLAN vicine hanno una portata che sovrappone i rispettivi raggi d'azione, allora, come visto nell'Unità 11 del volume del secondo biennio, bisogna applicare la **regola del 5** che impone di selezionare canali distanti 5 (per esempio 1-6-11).
- **Crittografia**: lo standard di crittografia e di autenticazione di 802.11 è la WEP (*Wired Equivalent Privacy*). È necessario attivarla come livello minimo di sicurezza (al problema fondamentale della sicurezza nelle reti wireless sarà interamente dedicata la Lezione 3). Si deve assegnare una chiave di crittografia a ogni utente per collegarsi all'Access Point con dati crittografati. Le chiavi standard sono da 10 cifre esadecimali (40 bit) o da 26 cifre esadecimali (104 bit) corrispondenti alla crittografia rispettivamente a 64 o 128 bit per via dell'aggiunta, in entrambi i casi, di un vettore d'inizializzazione a 24 bit.
- **Incapsulamento**: se l'Access Point è anche router, occorre settare il protocollo per il trasporto dei frame. Gli standard più usati sono PPPoA *(Point-to-Point Protocol over ATM* - RFC 2364) e PPPoE (*Point-to-Point Protocol over Ethernet* - RFC 2516).

LESSICO

La sigla ETSI sta per *European Telecommunications Standards Institute.*

Figura 5 Rete WLAN domestica con parte cablata e parte wireless



Oggi quasi tutti gli apparati dei gestori dei servizi Internet (ISP) sono configurati in modalità *autosense* così da riconoscere automaticamente il metodo di incapsulamento impostato sul modem/router dell'utente.

- **NAT** e **DHCP**: sempre in caso di Access Point che sia anche router-switch, occorre attivare la funzione NAT ed eventualmente il protocollo DHCP. DHCP e NAT verranno ripresi e approfonditi nelle Unità 5 e 6 rispettivamente. Dal punto di vista della sicurezza, anche se non efficace come un firewall, un NAT nasconde gli host interni e non indirizza loro il traffico generico proveniente dall'esterno. Il DHCP (*Dynamic Host Configuration Protocol*), è un protocollo che prevede un'assegnazione centralizzata degli indirizzi IP, del gateway e dei DNS. L'Access Point che funge da router diventa un server DHCP, col compito di fornire gli indirizzi IP ai nodi che ne fanno richiesta e che sono definiti come client DHCP.

Oltre a WLAN aziendali e domestiche, esistono anche le **WLAN ad hoc**, note anche come **MANET** (*Mobile Ad hoc NETwork*). Si tratta di reti wireless realizzate in situazioni in cui non è possibile installare un Access Point. La modalità ad hoc consente alla scheda di rete 802.11 di operare in quello che lo standard definisce una configurazione di rete *Independent Basic Service Set* (IBSS).
In modalità IBSS non ci sono Access Point e le varie schede di rete comunicano direttamente tra loro in modalità peer-to-peer (figura 6).

LO SAI CHE

Un'altra tecnologia WLAN è la HIPERLAN (*HIgh PErformance Radio LAN*). Si tratta di uno standard sviluppato dalla ETSI (*European Telecommunications Standards Institute*) che funziona alla velocità massima di 54Mbps nella banda a 5GHz. Rappresenta la risposta europea allo standard americano IEEE 802.11. I prodotti presenti sul mercato con questa tecnologia hanno generalmente costi superiori a quelli Wi-Fi e la loro diffusione risulta piuttosto limitata.

Figura 6 WLAN ad hoc

Alcuni esempi applicativi delle WLAN ad hoc sono:

- operazioni di acquisizione dati su terreno inospitale;
- interventi militari in territorio nemico;
- pronto intervento in situazioni di emergenza (uragani, terremoti, ecc.).

WMAN

Un altro dominio di applicazione è quello delle **MAN wireless**, che consente di distribuire dati su di un agglomerato di case tramite una potente antenna. Questa soluzione fornisce un'alternativa al costoso *cablaggio dell'ultimo miglio*. Il gruppo di lavoro **IEEE 802.16** si occupa di questa architettura.
Solitamente le WMAN forniscono interconnessioni tra utenti fissi. Per esempio, un'azienda può collegare la sede centrale con un vicino centro di distribuzione utilizzando componenti wireless quando vi sono limitazioni del diritto d'accesso che vietano la posa dei cavi, o quando affittare linee esistenti risulta troppo costoso.

I **Wireless Internet Service Providers** (**WISP**) talvolta mettono a disposizione MAN wireless nelle città e nelle aree rurali.
La connessione può essere **point-to-point** o **point-to-multipoint**.

- Il collegamento **point-to-point** viene realizzato mediante una coppia di dispositivi che supportano la connettività fissa da un punto all'altro. Tale coppia di dispositivi è solitamente rappresentata da due bridge wireless. I bridge wireless hanno una porta cablata che li collega alla rete aziendale e una porta wireless che li collega a un'*antenna direzionale*.
- Il collegamento **point-to-multipoint** prevede invece un'*antenna centralizzata omnidirezionale* (per esempio posta in un edificio ubicato nel centro di una città) e una serie di *antenne direzionali* puntate verso l'antenna centrale (per esempio da una serie di edifici decentrati) come mostrato in figura 7.

Figura 7 WMAN point-to-multipoint

Figura 8 Logo del WiMAX Forum

Dallo standard IEEE 802.16 è nato il progetto **WiMAX Forum,** figura 8, (dove WiMAX è acronimo di *Worldwide Interoperability for Microwave Access*): consorzio di imprese, con ruolo simile alla Wi-Fi Alliance per IEEE 802.11.

La trasmissione dei dati può avvenire secondo due differenti modalità. ***Non-line-of-sight*** su frequenze basse utilizzata in ambienti urbani, dove il segnale ha un'alta probabilità di essere schermato; il range va dai 2 GHz agli 11 GHz e il computer si connette alla rete WiMAX tramite piccole antenne (*dongle*) portatili da collegare direttamente al computer.
La seconda modalità operativa è ***line-of-sight*** su frequenze molto più alte, utilizzata in aree dove la probabilità che il segnale venga schermato sono molto basse; questa funziona con frequenze vicine ai 60 Ghz ed è ideale per coprire aree molto estese (una singola antenna può diffondere il proprio segnale fino a 50 chilometri di distanza, per una copertura d'area di quasi 8.000 chilometri quadrati) assicurandovi una velocità di circa 70 megabit al secondo.

WWAN

Le **WAN wireless** offrono applicazioni mobili che coprono vaste aree, come uno stato o un continente. La necessità di garantire una copertura ampia implica l'utilizzo di tecnologie diverse da quelle utilizzate per le altre reti. Queste tecnologie sono offerte a livello regionale e nazionale dai *Wireless Internet Service Providers* (WISP) che garantiscono la realizzazione di infrastrutture WWAN per fornire la connettività a grande raggio. Accordi di roaming tra gli operatori di telecomunicazioni permettono poi la connettività anche a livello globale. Pagando un solo provider, un utente può accedere a servizi Internet su una WWAN da qualsiasi luogo. I costi delle infrastrutture, benché piuttosto alti, possono essere suddivisi tra molti utenti garantendo costi di abbonamento relativamente bassi.
Lo svantaggio delle WWAN è la limitata disponibilità dello spettro in frequenza, che implica basse prestazioni e sicurezza limitata. La velocità di trasmissione è inferiore al Wi-Fi e si avvicina al WiMAX; siamo quindi nell'ordine dei Mbps. Le prestazioni aumentano utilizzando tecnologie di telefonia mobile.
Il vantaggio della WWAN è invece quello di consentire, per esempio, di controllare la posta elettronica mentre si è in viaggio, senza dover aspettare di arrivare in albergo per poter utilizzare la WLAN dall'hotspot Wi-Fi dell'albergo stesso.
Gli hotspot che offrono la connessione in Italia sono alcune migliaia. Uno dei più aggiornati motori di ricerca per hotspot è *http://www.hotspots-wifi.it*.

LO SAI CHE

I raggi infrarossi richiedono un percorso esente da ostacoli; migliore è la situazione se si usano i segnali radio. Ma le connessioni tra edifici tramite raggi infrarossi possono raggiungere i 100Gbps e oltre, mentre i collegamenti radio su una distanza di 30 km potrebbero non superare i 100Kbps.

Figura 9 Logo di WiFi°Italia°It

Nel 2017 nasce **WiFi°Italia°It** (figura 9) l'applicazione per navigare gratuitamente sulle reti Wi-Fi italiane.
Il Progetto WiFi°Italia°It ha come obiettivo principale quello di permettere a cittadini e turisti, italiani e stranieri, di connettersi gratuitamente e in modo semplice a una rete wireless libera e diffusa su tutto il territorio nazionale.