smartpixel

Il funzionamento del Wi-Fi domestico

Capire come funziona la rete wireless e rendere il Wi-Fi più veloce ed efficiente

Definizione e cenni storici

Il Wi-Fi è una **tecnologia di trasmissione dati senza fili** che utilizza onde radio e consente a terminali di utenza (computer, smartphone, tablet ecc.) di collegarsi tra loro attraverso una rete locale in modalità wireless (WLAN) basandosi sulle specifiche dello standard dell'Institute of Electrical and Electronics Engineers (IEEE) 802.11

La **rete locale** così ottenuta può essere allacciata a Internet tramite un router e permettere ai terminali connessi di condividere file e usufruire dei servizi di connettività offerti da un ISP

E' convinzione comune che Wi-Fi sia l'acronimo di "*Wireless Fidelity*" così come Hi-Fi deriva da "*High Fidelity*", ma secondo Phil Belanger, cofondatore della Wi-Fi Alliance, il termine non ha alcun significato e **rappresenta il marchio commerciale** della famiglia di protocolli IEEE 802.11

Anche se la Wireless History Foundation pone la **nascita del Wi-Fi** nel 1896, data del primo messaggio senza fili inviato da Guglielmo Marconi (sembra azzardato, ma l'idea di inviare dati senza il tramite di un supporto fisico, come un cavo, rispecchia la filosofia di funzionamento del Wi-Fi) questa invenzione ha richiesto un percorso di ricerca lungo diversi anni

Definizione e cenni storici

L’atto costitutivo della tecnologia Wi-Fi risale al 1985 quando la **Federal Communications Commission** statunitense (ente regolatore del settore delle telecomunicazioni) decide di liberare alcune frequenze e renderle disponibili all’uso civile senza obbligo di licenza

Dal 1985 si intensifica la sperimentazione e le grandi aziende USA iniziano a progettare sistemi di comunicazione senza fili per la trasmissione di dati, ma è solo nel 1991 che vengono presentati i **primi apparecchi wireless**, usati principalmente per la registrazione di incassi

I primi anni di vita furono caratterizzati dall’incertezza dovuta all’assenza di un protocollo di comunicazione standard: nel 1997 nasce la prima versione del protocollo 802.11 sviluppato da una delle commissioni del **Institute of Electrical and Electronic Engineers** (IEEE), associazione internazionale di scienziati professionisti che si occupa di ricerche sulle nuove tecnologie

Due anni più tardi, nel **1999**, nasce il protocollo IEEE 802.11b insieme con il nome Wi-Fi e il relativo logo: da quel momento lo sviluppo di questa tecnologia e la sua diffusione fanno registrare nuovi progressi anno dopo anno

Pro e contro

I vantaggi del Wi-Fi riguardano:

- **installazione semplice**: non richiede di collegare i dispositivi con cavi fisici, basta collegare l'access point per creare in modo pratico e veloce una rete locale
- **mobilità**: permette di collegarsi in movimento a partire da zone differenti
- **costi ridotti**: i costi di installazione e manutenzione delle reti Wi-Fi sono minimi rispetto alle reti cablate (richiedono la posa dei cavi e la manutenzione dell'hardware che si deteriora)

Tra gli svantaggi:

- **sicurezza**: i dati non sono trasmessi via cavo, ma con onde radio che escono dai confini dell'edificio ed espongono la rete al rischio di intercettazione o utilizzo non autorizzato
- **dispersione segnale**: muri di cemento armato, elementi in ferro, ma anche cordless, cellulari, casse musicali e console di gioco wireless, forni a microonde possono disturbare il segnale
- **rallentamenti**: se più utenti usano la stessa rete, questa si satura ripartendo il segnale
- **configurazione**: mettere in sicurezza il Wi-Fi non è semplice per chi non conosce le reti

Router Wi-Fi

Una rete Wi-Fi è individuata dal suo **SSID** (Service Set IDentifier), cioè il nome scelto dall'utente per identificare la propria WLAN ed è composta da uno o più **punti di accesso** (access point o hotspot) che fanno da "*sorgente*" del segnale e uno o più **client** che si connettono alla rete

Il cuore della rete Wi-Fi è il **router**, dispositivo di rete composto da processore, memoria, porte ethernet - una porta WAN (Wide Area Network) che collega il router a Internet tramite cavo e una serie di porte LAN (Local Area Network) per collegare via cavo i terminali di rete locale - ed eventualmente le antenne per fornire connettività wireless → incorpora **diverse funzionalità**:

- **modem**: comunica con Internet, riceve e assegna un indirizzo IP alla rete WAN → usando Internet tramite il router, i terminali si presentano come un'entità unica, perché hanno lo stesso indirizzo di rete (indirizzo IP) che viene assegnato dal provider che è diverso rispetto agli indirizzi di rete LAN che il router stesso assegna ai vari dispositivi: la rete WAN è separata, anche per motivi di sicurezza, dalla rete LAN che collega tra loro i vari dispositivi
- **access point**: permette all'utente di accedere alla rete in modalità wireless direttamente dal suo terminale se dotato di scheda Wi-Fi

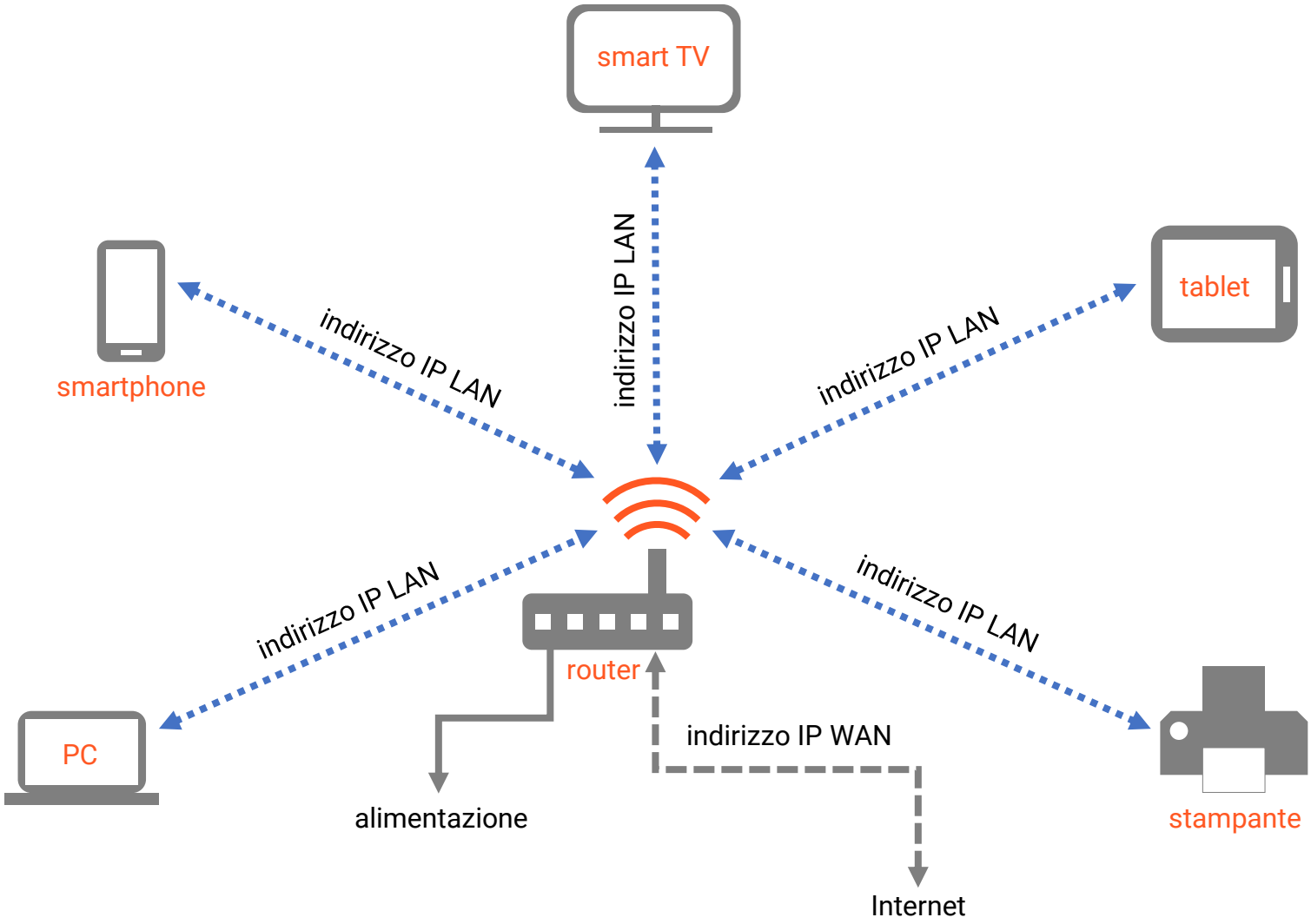
Router Wi-Fi

Il **router** si occupa di creare e gestire sottoreti locali indirizzando i dati, organizzati in pacchetti, tra i vari nodi della rete, assicura che i dispositivi collegati comunichino efficacemente tra loro e permette l'uso contemporaneo della stessa connessione Internet ai terminali collegati:

- il router scarica i dati da Internet e indirizza l'informazione ai dispositivi collegati assegnando ad ognuno un **indirizzo IP locale**, in modo da creare una strada separata per ogni sistema collegato a Internet che assicura che tutti i dati siano trasmessi correttamente
- i diversi dispositivi inviano e ricevono i **pacchetti di dati** contenenti le informazioni richieste dal funzionamento del web attraverso il router che fa da centralino di smistamento
- il **client** (dispositivo dotato di scheda Wi-Fi o ripetitore di segnale) si collega alla rete attraverso il riconoscimento dell'SSID e, se la rete è protetta, della password

Il **segnale del router** copre un'area compresa tra 50 e 100 metri (dipende dalle caratteristiche architettoniche dell'area) ma può essere esteso collegando differenti access point via cavo, oppure creando un "*ponte*" wireless con ripetitori o amplificatori Wi-Fi (extender o repeater) che ritrasmettono il segnale facendolo rimbalzare negli angoli più lontani della casa

Funzionamento del Wi-Fi



La sicurezza delle reti wireless

Le reti wireless introducono **rischi supplementari di sicurezza**: dei malintenzionati all'interno dell'area wireless possono intercettare la connessione che pertanto va protetta impostando una chiave di sicurezza (**password di accesso**)

Esistono tre protocolli di sicurezza: **WEP** (Wired Equivalent Privacy), **WPA** (Wi-Fi Protected Access) e **WPA2**, conosciuto come IEEE 802.11i è il più sicuro perché permette di crittografare la password con l'algoritmo AES (Advanced Encryption Standard) a 256 bit → per minimizzare i rischi della propria rete wireless:

- **cambiare l'SSID di default** con uno più difficile da indovinare ed evitare di divulgarlo
- **cambiare la password di default** del router e impostare una password robusta (alfanumerica e sufficientemente lunga) da cambiare con regolarità
- **controllare l'accesso alla rete** ed eventualmente limitarlo attraverso il filtro MAC address, indirizzo fisico della scheda di rete che individua in modo univoco i singoli dispositivi e consente di creare delle Access List (ACL) di dispositivi autorizzati all'uso della rete
- installare un **firewall** e un software **antivirus** e **antimalware** sui dispositivi in uso

Vulnerabilità: il caso KRACK

L'attacco **Key Reinstallation Attacks** (KRACK) del 2017 ha mostrato una serie di gravi falle del protocollo WPA2 che consentono di intercettare dati sensibili (ad es. le password usate per autenticarsi ai siti) e riguardano tutti i dispositivi di ogni marca dotati di Wi-Fi

L'**attacco KRACK funziona solo se** l'aggressore si trova nel raggio di azione della rete Wi-Fi della vittima (man in the middle) e la vittima utilizza connessioni non cifrate HTTP: se usa HTTPS (come molti siti web, soprattutto quelli che richiedono autenticazione tramite password o permettono transazioni finanziarie) o una buona VPN questo attacco non è possibile

La **protezione dalla vulnerabilità** avviene solo tramite software: in attesa del rilascio degli aggiornamenti di sicurezza da parte dei produttori di dispositivi, non è da scartare l'idea che la Wi-Fi Alliance possa sviluppare un protocollo di sicurezza più affidabile

Nel frattempo è meglio connettersi via cavo o utilizzare le connessioni mobili 3G/4G ed evitare di collegarsi a reti Wi-Fi pubbliche: non possiamo sapere se l'access point è vulnerabile ed è più probabile che nell'area d'azione ci sia qualcuno intenzionato ad attaccarci

Come ottenere il massimo dal Wi-Fi

- il router invia segnali in tutte le direzioni, pertanto va posizionato nella stanza dove si usa di più Internet, possibilmente al **centro della casa** per massimizzare l'area coperta dal segnale, magari aiutandosi con dei cavi per spostare il router nella zona migliore
- se è necessario avere una copertura più estesa o su più piani, si può usare un **Wi-Fi extender** che rimbalza il segnale in modo da raggiungere anche i locali dell'abitazione più lontani
- **sollevare il router da terra** (il segnale tende naturalmente dall'antenna verso il basso e penetra difficilmente alcuni materiali come metallo, cemento e calcestruzzo) ad almeno 1m. di altezza in un punto in cui il segnale raggiunga tutti i locali
- **tenere il router libero da ostacoli** su uno scaffale o un tavolo (non nell'armadio, tra due mobili o vicino all'acquario → l'acqua può potenzialmente bloccare il segnale): se il router è libero, il segnale migliora perché le onde radio si trasmettono meglio attraverso l'aria
- tenere il router **distante da altri dispositivi elettronici** che possono interferire col segnale (in genere tutto ciò che genera un segnale elettromagnetico)
- **posizionare le antenne verticalmente**: il segnale si estende perpendicolarmente alla direzione delle antenne → se l'antenna è verticale il segnale è trasmesso orizzontalmente e riesce a coprire un'area più vasta della casa

Come ottenere il massimo dal Wi-Fi

- **misurare la potenza del segnale**: diverse applicazioni permettono di mappare il segnale in casa per verificare dov'è più performante e capire dove è meglio posizionare il router
- per prestazioni migliori **utilizzare router e dispositivi recenti** o di ultima generazione (ad es. i dispositivi recenti permettono di usare il Bluetooth senza causare interferenze)
- **scegliere la frequenza di trasmissione** migliore in base al tipo di abitazione → le frequenze sono gestite in automatico, ma è possibile modificarle nelle impostazioni del router:
  - se la casa ha più piani ed è isolata, la frequenza classica a 2,4 GHz supera meglio gli ostacoli, ma soffre di più i disturbi e le interferenze di reti e dispositivi in prossimità
  - in palazzi o condomini con molte reti in prossimità la frequenza a 5 GHz è più performante in situazioni di sovraffollamento ma ha raggio minore ed è meno efficace nel superare gli ostacoli di quella a 2.4 GHz
- **configurare le impostazioni del router** eventualmente modificando il canale del router nel caso di interferenze dovute alla sovrapposizione con altre reti presenti nelle vicinanze:
  - i router lavorano su 14 canali di frequenza 2.4 GHz, numerati da 1 a 14
  - di default, come impostazione di fabbrica, il canale selezionato è il 6
  - i canali 1, 6 e 11 sono i migliori perché tendono a sovrapporsi di meno degli altri