WIFI

Le reti Wi-Fi si basano sullo standard **IEEE 802.11** e permettono ai dispositivi di **collegarsi a una rete locale senza l'uso di cavi**, sfruttando segnali radio. A differenza delle reti Ethernet, che usano cavi e lo standard **802.3**, le reti wireless devono gestire aspetti particolari come la **mobilità**, l'interferenza del segnale e la **sicurezza**. La rete Wi-Fi è composta da uno o più **Access Point (AP).**

Un Access Point è un dispositivo che trasmette il segnale Wi-Fi, collega i dispositivi wirless alla rete. Gli **Access Point** possono essere posizionati in diversi punti per garantire una copertura continua. Quando mi sposto da una zona all'altra, il mio dispositivo passa automaticamente da un **AP** all'altro senza perdere la connessione: questo si chiama **roaming.**

Un **Access Point**, per farsi riconoscere, manda ogni tanto un messaggio chiamato **beacon.** Questo messaggio contiene informazioni importanti, come il **nome della rete Wi-Fi (SSID)**, il tipo di **sicurezza** usata (per esempio WPA2), e altri dettagli tecnici.
Quando un dispositivo riceve questi messaggi, **può vedere quali reti sono disponibili** e **scegliere a quale AP connettersi**.
Una volta scelto, il dispositivo e l'Access Point **scambiano dei messaggi speciali (chiamati frame di gestione)** per iniziare la connessione.

Abbiamo **due** modalità di connessione:

- **Open:** il client invia una richiesta di connessione e viene identificato solo tramite il proprio indirizzo **MAC**. È una modalità **senza autenticazione**, molto usata in ambienti pubblici o dove non è pratico gestire password condivise.

- **PSK**: Sia il client che l'Access Point condividono la **stessa password** per accedere alla rete. Questa password non viene mai inviata in chiaro, ma viene usata per cifrare i messaggi durante la fase di autenticazione. Questo garantisce un **buon livello di sicurezza.** Infatti **PSK** è usata per le reti domestiche. **la password non viaggia mai in chiaro**. È il meccanismo usato nei protocolli di sicurezza **WPA2 o WPA3**, che proteggono i dati con crittografia e autenticazione forte.

In contesti pubblici, come ad esempio qui ad **UniGe**, si usa spesso la **modalità open** in combinazione con un **captive portal**.
Il captive portal è una **pagina web che appare subito dopo la connessione**, in cui all'utente può essere richiesto di:

- autenticarsi (con credenziali),
- accettare i termini di utilizzo,
- o inserire un codice.

Per distinguere chi è autenticato da chi non lo è, si possono usare tecniche come il **filtraggio degli indirizzi MAC** o regole di firewall che sbloccano l'accesso a Internet solo dopo la registrazione. Esempio della pagina:

Sebbene **WPA2** e **WPA3** garantiscano un buon livello di sicurezza, le reti Wi-Fi restano **esposte a vari rischi**:

- **Sniffing**: in reti non cifrate, un attaccante può ascoltare il traffico.
- **MAC spoofing**: un attaccante può falsificare il proprio indirizzo MAC per accedere a risorse non autorizzate.
- **Attacchi DDoS**: possono rendere inutilizzabile un Access Point.

Per questo è importante configurare gli **AP** in modo sicuro e, se possibile, usare **filtri**, **liste di accesso**, e **separazione in VLAN** per isolare il traffico.