Reti Wireless

Le reti wireless permettono la comunicazione tra dispositivi senza l'uso di cavi, sfruttando onde radio o segnali infrarossi. Come le reti cablate, possono essere classificate in base all'estensione dell'area coperta.

WPAN

Le **WPAN** (Wireless Personal Area Network) coprono pochi metri e sono adatte per ambienti domestici o piccoli uffici, usando tecnologie come **Bluetooth** o **IrDA**, impiegate anche nella domotica.

Il **Bluetooth** opera a 2,4 GHz, ha una velocità massima di 2 Mbps e segue lo standard **IEEE 802.15**. Una rete Bluetooth, detta **piconet**, è costituita da un dispositivo Master che gestisce fino a sette dispositivi Slave. Più piconet possono formare una **scatternet**. Con **Bluetooth 5.0**, la velocità arriva a 2 Mbps e la portata può raggiungere i 240 metri, migliorando le prestazioni rispetto alle versioni precedenti, soprattutto per dispositivi a basso consumo.

WLAN

Le **WLAN** (Wireless Local Area Network) sono simili alle tradizionali LAN cablate, ma senza fili. Lo standard più usato è **IEEE 802.11**. Le WLAN includono dispositivi mobili (WT) e uno o più **Access Point (AP)**, che fungono da ponte tra la rete wireless e quella cablata. Un **Basic Service Set (BSS)** è formato da un AP e dai dispositivi nella sua area di copertura. Più BSS collegati formano un **Extended Service Set (ESS)**, che si comporta come una sola rete WLAN.

Gli **ESS** possono includere BSS parzialmente sovrapposti, disgiunti o co-locati per garantire continuità, ridondanza o migliori prestazioni. Lo standard 802.11 gestisce la **mobilità** dei dispositivi, distinguendo tra transizioni statiche, tra BSS e tra ESS. In quest'ultimo caso, la connessione viene interrotta poiché si passa da una WLAN a un'altra.

La configurazione di un Access Point in ambito aziendale richiede la definizione di parametri come **SSID**, **potenza**, **canale**, **crittografia**, **incapsulamento**, **NAT** e **DHCP**.

WMAN

Le **WMAN** (Wireless Metropolitan Area Network) permettono la distribuzione dei dati in aree urbane tramite antenne potenti, offrendo una valida alternativa al cablaggio tradizionale. Il collegamento può essere **point-to-point**, tra due bridge wireless, o **point-to-multipoint**, con un'antenna centrale e più terminali puntati verso di essa. Lo standard usato è **IEEE 802.16**, da cui nasce il progetto **WiMAX**, simile alla Wi-Fi Alliance per le WLAN.

La trasmissione WiMAX può avvenire in modalità **non-line-of-sight**, con frequenze tra 2 e 11 GHz per ambienti urbani, o in modalità **line-of-sight**, su frequenze attorno ai 60 GHz, per coprire grandi distanze.

Le **WWAN** (Wireless Wide Area Network) coprono aree molto estese, fino a livello nazionale o continentale. I **WISP** (Wireless Internet Service Providers) offrono questi servizi con infrastrutture dedicate, e tramite accordi di roaming garantiscono connettività globale.

La Sicurezza nelle Reti Wireless

Dal punto di vista della **sicurezza**, le reti wireless presentano rischi specifici. Lo **sniffing** consente di intercettare passivamente i dati, per cui è essenziale usare meccanismi di crittografia. L'**accesso non autorizzato** avviene spesso tramite **Access Point Rouge** (non autorizzati), contrastabile con l'**autenticazione reciproca** tra WT e AP.

Un'altra minaccia è lo **spoofing**, dove un terminale falso si sostituisce a un dispositivo legittimo. Il **protocollo SARP** può prevenire questo rischio creando tunnel protetti. Gli **attacchi DoS** (Denial of Service) possono bloccare la rete sovrapponendo segnali radio. Barriere fisiche come vernici schermanti possono ridurre l'impatto.

La Crittografia

Tra i principali sistemi di crittografia utilizzati troviamo:

- **WEP (Wired Equivalent Privacy)**: è stato uno dei primi metodi usati per proteggere le reti Wi-Fi. Cifra solo il payload del frame utilizzando l'algoritmo **RC4**, un cifrario a flusso con chiave simmetrica. Tuttavia, è oggi considerato **insicuro** a causa delle sue vulnerabilità;
- **TKIP (Temporal Key Integrity Protocol)**: è una **evoluzione del WEP**, ancora basata su RC4, ma con miglioramenti. Utilizza una **chiave temporanea a 128 bit** condivisa tra il terminale wireless (WT) e l'Access Point (AP), che viene rigenerata ad ogni pacchetto o burst. Aggiunge anche un **IV (Initialization Vector)** di 128 bit per aumentare la complessità della chiave di cifratura. Nonostante ciò, anche TKIP è ormai superato;
- **AES (Advanced Encryption Standard)**: rappresenta lo standard di sicurezza attuale. Utilizza l'algoritmo a blocchi **Rijndael**, considerato estremamente sicuro e praticamente indecifrabile con le tecnologie attuali. Viene usato nei protocolli più recenti come **WPA** e **WPA2**, che

includono anche meccanismi di distribuzione dinamica delle chiavi e **autenticazione reciproca**;

L'Autenticazione

Sul fronte dell'**autenticazione**, esistono diversi metodi per impedire l'accesso non autorizzato alla rete wireless:

- **SSID (Service Set Identifier)**: è il nome della rete. L'Access Point consente l'accesso solo ai dispositivi che cercano di connettersi utilizzando il SSID corretto. Tuttavia, poiché il SSID può essere facilmente intercettato, questo metodo da solo non è sufficiente;
- **Filtraggio degli indirizzi MAC**: l'amministratore di rete può creare una lista di indirizzi MAC autorizzati. Gli Access Point accettano solo i dispositivi presenti nella lista. Anche se utile, questo metodo può essere aggirato da un attaccante che clona un indirizzo MAC valido;
- **EAP (Extensible Authentication Protocol)**: è un protocollo avanzato per l'autenticazione, usato su entrambe le sezioni della rete, cablata e wireless. Si basa su un **server di autenticazione centrale**, che consente un controllo accurato degli accessi e può essere integrato con sistemi di identità aziendali (come RADIUS). EAP permette di implementare forme di autenticazione sicure, come l'autenticazione tramite certificati o credenziali univoche;

Infine, un'infrastruttura wireless aziendale completa può includere un **router Wi-Fi** collegato a un **server AAA** (Authentication, Authorization, Accounting), che gestisce centralmente l'accesso, le autorizzazioni e tiene traccia delle attività degli utenti in rete.