CAPITOLO 7 – RETI WIRELESS E TECNOLOGIE WI-FI

Obiettivi del Capitolo

Al termine di questo capitolo il corsista sarà in grado di:

- Comprendere il funzionamento delle reti wireless.
- Conoscere gli standard IEEE 802.11.
- Comprendere il ruolo degli Access Point.
- Analizzare frequenze, canali e interferenze.
- Configurare correttamente una rete Wi-Fi.
- Comprendere le tecnologie di sicurezza WPA2 e WPA3.
- Progettare una semplice rete WLAN aziendale.

7.1 Introduzione alle reti wireless

Le reti wireless consentono ai dispositivi di comunicare senza l'utilizzo di cavi fisici.

La trasmissione dei dati avviene attraverso onde radio.

Oggi le reti Wi-Fi sono utilizzate in:

- abitazioni;
- scuole;
- uffici;
- aziende;
- aeroporti;
- strutture sanitarie;
- industrie.

La diffusione dei dispositivi mobili ha reso le reti wireless una componente essenziale delle infrastrutture moderne.

7.2 Cos'è una WLAN

WLAN significa:

Wireless Local Area Network

Si tratta di una rete locale che utilizza collegamenti radio anziché cavi Ethernet.

Una WLAN offre gli stessi servizi di una LAN tradizionale:

- accesso a Internet;
- condivisione file;
- accesso ai server;
- stampa di rete;
- servizi cloud.

La differenza principale consiste nel mezzo trasmissivo utilizzato.

7.3 Componenti di una rete Wi-Fi

Una rete wireless è generalmente composta da:

Access Point

Fornisce la copertura radio.

Client Wireless

Dispositivi che si collegano alla rete.

Esempi:

- smartphone;
- notebook;
- tablet;
- smart TV;
- telecamere IP;
- stampanti Wi-Fi.

Controller Wireless

Presente nelle reti aziendali più grandi.

Permette la gestione centralizzata degli Access Point.

7.4 Come funziona una comunicazione Wi-Fi

Quando un dispositivo si collega ad una rete wireless:

1. Individua le reti disponibili.
2. Seleziona l'SSID corretto.
3. Esegue l'autenticazione.
4. Ottiene un indirizzo IP.
5. Inizia la comunicazione.

Dal punto di vista dell'utente il processo appare immediato.

In realtà vengono eseguite numerose operazioni di rete.

7.5 Lo standard IEEE 802.11

Le reti Wi-Fi sono regolamentate dalla famiglia di standard:

IEEE 802.11

Ogni revisione introduce miglioramenti in termini di:

- velocità;
- copertura;
- efficienza;
- sicurezza.

7.6 Evoluzione degli standard Wi-Fi

802.11b

Anno: 1999

Velocità massima:

11 Mbps

Frequenza:

2,4 GHz

802.11g

Velocità:

54 Mbps

Frequenza:

2,4 GHz

802.11n (Wi-Fi 4)

Velocità:

fino a 600 Mbps

Frequenze:

- 2,4 GHz
- 5 GHz

Introduzione della tecnologia MIMO.

802.11ac (Wi-Fi 5)

Velocità:

oltre 1 Gbps

Frequenza:

5 GHz

Maggiore efficienza e prestazioni.

802.11ax (Wi-Fi 6)

Velocità teorica:

oltre 9 Gbps

Miglior gestione di molti dispositivi simultanei.

Particolarmente indicato per:

- aziende;
- scuole;
- ambienti ad alta densità.

Wi-Fi 6E

Estende il Wi-Fi 6 alla banda:

6 GHz

Riduce ulteriormente le interferenze.

7.7 Le frequenze Wi-Fi

Le reti wireless utilizzano principalmente tre bande:

Banda 2,4 GHz

Vantaggi:

- maggiore copertura;
- migliore attraversamento degli ostacoli.

Svantaggi:

- maggiore congestione;
- velocità inferiori.

Banda 5 GHz

Vantaggi:

- maggiore velocità;
- minori interferenze.

Svantaggi:

- copertura inferiore.

Banda 6 GHz

Utilizzata dal Wi-Fi 6E.

Vantaggi:

- elevata capacità;
- minore congestione.

7.8 I Canali Radio

Le frequenze Wi-Fi sono suddivise in canali.

Ogni Access Point utilizza uno specifico canale radio.

Quando Access Point vicini utilizzano lo stesso canale possono verificarsi interferenze.

7.9 Interferenze

Le interferenze rappresentano uno dei principali problemi delle reti wireless.

Possono essere causate da:

- altri Access Point;
- dispositivi Bluetooth;
- forni a microonde;
- telefoni cordless;
- apparecchiature industriali.

Effetti:

- rallentamenti;
- disconnessioni;
- aumento della latenza.

7.10 SSID

SSID significa:

Service Set Identifier

È il nome della rete wireless.

Esempi:

- AziendaWiFi
- UfficioTecnico
- GuestNetwork

Gli utenti identificano la rete attraverso il suo SSID.

7.11 BSSID

Ogni Access Point possiede anche un identificativo univoco chiamato:

BSSID

Generalmente coincide con il MAC Address dell'interfaccia wireless.

7.12 Modalità di funzionamento

Infrastructure Mode

È la modalità più comune.

Tutti i dispositivi comunicano attraverso un Access Point.

Ad-Hoc Mode

I dispositivi comunicano direttamente tra loro.

Non è necessario un Access Point.

Oggi viene utilizzata raramente.

7.13 Sicurezza delle reti Wi-Fi

Le reti wireless sono maggiormente esposte ai rischi rispetto alle reti cablate.

Chiunque si trovi nel raggio di copertura può tentare di intercettare il traffico.

Per questo motivo è fondamentale utilizzare sistemi di protezione adeguati.

7.14 WEP

WEP (Wired Equivalent Privacy) è stato il primo sistema di protezione Wi-Fi.

Oggi è considerato completamente insicuro.

Non deve essere utilizzato.

7.15 WPA

WPA (Wi-Fi Protected Access) è stato introdotto per correggere le vulnerabilità di WEP.

Ha migliorato significativamente la sicurezza.

Tuttavia è stato successivamente sostituito.

7.16 WPA2

WPA2 è stato per molti anni lo standard di riferimento.

Utilizza:

AES (Advanced Encryption Standard)

per proteggere le comunicazioni.

Vantaggi:

- elevata sicurezza;
- ampia compatibilità;
- buona affidabilità.

7.17 WPA3

WPA3 rappresenta l'evoluzione di WPA2.

Migliora:

- autenticazione;
- crittografia;
- protezione delle password.

Vantaggi:

- maggiore resistenza agli attacchi;
- protezione avanzata degli utenti.

È oggi la soluzione consigliata.

7.18 Password sicure

Una rete Wi-Fi deve utilizzare password robuste.

Caratteristiche consigliate:

- almeno 12 caratteri;
- lettere maiuscole e minuscole;
- numeri;
- simboli.

Esempio:

R3t3!Azienda#2025

7.19 Reti Guest

Molte organizzazioni implementano una rete ospiti separata.

Esempio:

SSID Aziendale

SSID Guest

La rete Guest consente l'accesso a Internet senza permettere l'accesso alle risorse interne.

Vantaggi:

- maggiore sicurezza;
- isolamento degli utenti esterni.

7.20 Roaming Wireless

Nelle reti aziendali possono essere presenti numerosi Access Point.

Quando un utente si sposta:

- il dispositivo cambia automaticamente Access Point;
- la connessione rimane attiva.

Questo processo è chiamato:

Roaming

7.21 Progettazione di una WLAN

La progettazione di una rete wireless richiede la valutazione di diversi fattori.

Numero di utenti

Più utenti richiedono maggiore capacità.

Dimensione dell'area

Occorre valutare:

- metri quadrati;
- numero di piani;

- ambienti da coprire.

Ostacoli

Pareti, strutture metalliche e vetri possono influenzare il segnale.

7.22 Site Survey

Prima dell'installazione si esegue generalmente un:

Wireless Site Survey

Consiste nell'analisi dell'ambiente per individuare:

- copertura;
- interferenze;
- posizionamento ottimale degli Access Point.

7.23 Caso di studio: rete Wi-Fi aziendale

Un ufficio di 150 dipendenti necessita di:

- copertura completa;
- roaming continuo;
- accesso ospiti;
- elevata sicurezza.

La soluzione prevede:

- 12 Access Point Wi-Fi 6;
- controller centralizzato;
- WPA3;
- VLAN dedicate;
- rete Guest separata.

Risultato:

- migliori prestazioni;
- maggiore sicurezza;
- gestione semplificata.

Riepilogo

In questo capitolo abbiamo studiato:

- WLAN;
- Access Point;
- Standard IEEE 802.11;
- Wi-Fi 4, 5, 6 e 6E;
- Frequenze radio;
- Canali e interferenze;
- SSID e BSSID;
- WPA2 e WPA3;
- Roaming;
- Site Survey;
- Progettazione delle reti wireless.

Le reti Wi-Fi rappresentano oggi una componente fondamentale delle infrastrutture moderne e richiedono un'attenta progettazione per garantire prestazioni e sicurezza adeguate.

Domande di verifica

1. Cos'è una WLAN?
2. Qual è il ruolo di un Access Point?
3. Cosa identifica un SSID?
4. Quali differenze esistono tra 2,4 GHz e 5 GHz?
5. Cos'è un'interferenza radio?
6. Perché WEP non è più sicuro?
7. Quali vantaggi offre WPA3?
8. Cos'è il roaming wireless?
9. Qual è lo scopo di una rete Guest?
10. Cos'è un Wireless Site Survey?