



www.sunrisetechnology.it

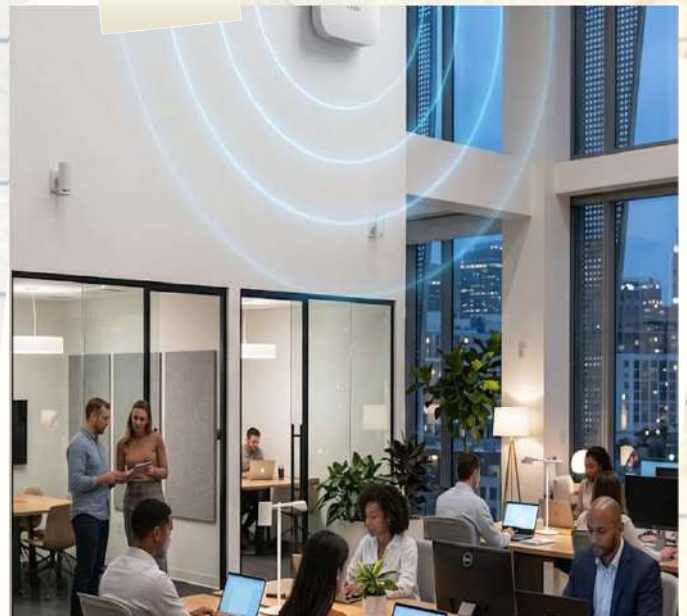
DALLA DIAGNOSI ALL'ARCHITETTURA

Ottimizzare il Wi-Fi aziendale

Canali · Posizionamento AP · VLAN · Security



Wi-Fi lento = produttività persa



...da rete domestica a
infrastruttura



Introduzione

Un Wi-Fi lento o instabile non provoca soltanto frustrazione: si traduce direttamente in perdita di produttività, disconnessioni in videochiamate con i clienti e potenziali rischi di sicurezza.

1 · Strumenti di diagnosi

Prima di modificare la configurazione hardware occorre misurare l'ambiente aereo aziendale, per individuare interferenze, sovrapposizioni di canale e zone d'ombra. Si parte da un site survey, la mappatura del segnale stanza per stanza.



Site survey sul campo

[APP e SOFTWARE]

NetSpot

***(Windows, macOS, Android, iOS).
Analisi rapida in tempo reale e
creazione di heatmap di copertura
all'interno delle stanze.***

WiFi Analyzer

(Android / Windows Store). Grafico a barre / onde dei canali sono occupati dai vicini e con quale intensità (dBm).

inSSIDer

(Windows, macOS). Analisi professionale di sovrapposizioni di canale, saturazione e configurazioni dei punti di accesso limitrofi.

Wi-Fi SweetSpots

(iOS, Android). Misura la velocità effettiva di trasmissione dati (throughput) tra smartphone e Access Point in movimento.

[COSA CERCARE]

Interferenze da apparati non-Wi-Fi, canali sovrapposti, aree in cui il throughput reale crolla pur con segnale "pieno": sono i tre sintomi guida per le ottimizzazioni descritte nelle pagine seguenti.

Parametri da monitorare

RSSI — Signal Strength

Espresso in dBm: -50 dBm è un ottimo segnale, sotto i -75 dBm la connessione diventa instabile e lenta.

Noise Floor e SNR

Differenza tra segnale utile e rumore di fondo elettrostatico/radio. Un SNR superiore a 25 dB garantisce prestazioni elevate.



Le frequenze a confronto

Quale banda usare

2.4 GHz

Maggiore portata, ma forti interferenze (microonde, Bluetooth, cordless) e solo 3 canali non sovrapposti: 1, 6, 11.

5 GHz

Minore portata, ma velocità superiori e decine di canali senza sovrapposizione: è la banda di lavoro dei client aziendali.

6 GHz — Wi-Fi 6E / 7

Assenza di interferenze legacy: ideale per uffici ad altissima densità di dispositivi.

Regola pratica: 2.4 GHz solo per IoT e dispositivi legacy, 5 GHz per PC e videocall, 6 GHz dove la densità di client è massima.

2 • Posizionare gli AP

La fisica della propagazione radio determina l'80% delle prestazioni della rete wireless: prima di sostituire l'hardware, verifica dove e come è installato quello esistente.

[TIPOLOGIE]

Da soffitto

Irradiazione "a cupola" verso il basso: al centro dell'area da coprire, lontano da travi metalliche, canaline di aerazione e pilastri in cemento armato.

Da parete / in-wall

Per uffici a stanze singole o corridoi. Irradiano frontalmente: mai dietro armadiature metalliche o schedari.

Outdoor

Su pali dedicati, con scaricatori di sovratensione (SPD) sulla linea Ethernet PoE e certificazione IP65/IP67.



AP a parete: irradiazione frontale

Le regole d'oro della posizione

Altezza ideale: tra 2,5 e 3,5 metri da terra.

Distanza dagli ostacoli: almeno 1 – 1,5 m da motori elettrici, quadri elettrici generali, stampanti multifunzione, inverter fotovoltaici e server rack non schermati.

Orientamento antenne: se esterne e direzionabili, per coprire un unico piano orizzontale da posizionare verticalmente.

[ERRORI RICORRENTI IN PMI]

AP poggiati sulla scrivania o nel rack chiuso, apparato unico al piano terra per coprire due piani, AP montati vicino al quadro elettrico: scenari in cui nessuna ottimizzazione potrà recuperare le prestazioni.

3 • Architettura di rete

*Affidare la rete aziendale a un unico router/modem "tutto-in-uno" fornito dall'operatore telefonico genera **colli di bottiglia** . Nelle strutture professionali la logica di routing va separata da quella wireless.*

Gateway / Firewall

Hardware dedicato: gestisce indirizzamento IP, DHCP, sicurezza e traffico di rete.

Access Point

Uno o più apparati gestiti centralmente: gestiscono la trasmissione wireless dei client.



Rete ospiti isolata dai dispositivi aziendali

[SOTTO-RETI SEPARATE: SSID + VLAN]

Per sicurezza e prestazioni, non tutti i dispositivi devono comunicare tra loro: il traffico va diviso su SSID dedicati abbinati a specifiche VLAN (802.1Q).

Corporate / Ufficio — VLAN 10

Riservata ai PC aziendali: accesso completo a server interni, NAS, stampanti di rete e gestionale.

Guest / Ospiti — VLAN 20

Clienti, fornitori e smartphone personali dei dipendenti: consente solo la navigazione Internet e blocca le comunicazioni verso i dispositivi aziendali (Guest Isolation).

IoT / Smart — VLAN 30

Videocamere IP, termostati, allarmi, POS e stampanti Wi-Fi. Isola dal resto della rete i dispositivi più esposti a vulnerabilità.

4 • Capacità e accessi

Quando decine di dispositivi comunicano contemporaneamente sullo stesso AP, il canale radio si satura per collisione dei pacchetti: non serve più potenza, ma più AP ben distribuiti e di classe adeguata.

Router / modem operatore

15–20

dispositivi connessi contemporaneamente: oltre iniziano rallentamenti e disconnessioni.

Access Point business

60–150+

dispositivi per singolo AP su modelli Wi-Fi 6/6E, grazie a OFDMA e MU-MIMO.

Controllo degli accessi

Filtro MAC — whitelist e blacklist

Utile per bloccare specifici dispositivi indesiderati, ma non garantisce la sicurezza : gli indirizzi MAC possono essere contraffatti.

WPA3 Enterprise — IEEE 802.1X

Sostituire l'unica password condivisa — che rischia di restare in possesso anche a chi lascia l'azienda — tramite un server di autenticazione RADIUS : ogni utente accede con proprie credenziali personali (username e password o certificato), revocabili singolarmente.

Una password unica per tutti non è una politica di sicurezza.

5 • Firmware in sicurezza

Aggiornare il firmware di router, switch e AP chiude falle di sicurezza zero-day e migliora la stabilità del segnale. Un aggiornamento errato, però, può bloccare la rete (effetto "brick").

Operazione molto delicata: serve pianificazione, uniformità di aggiornamenti e versioni su tutti i dispositivi presenti...

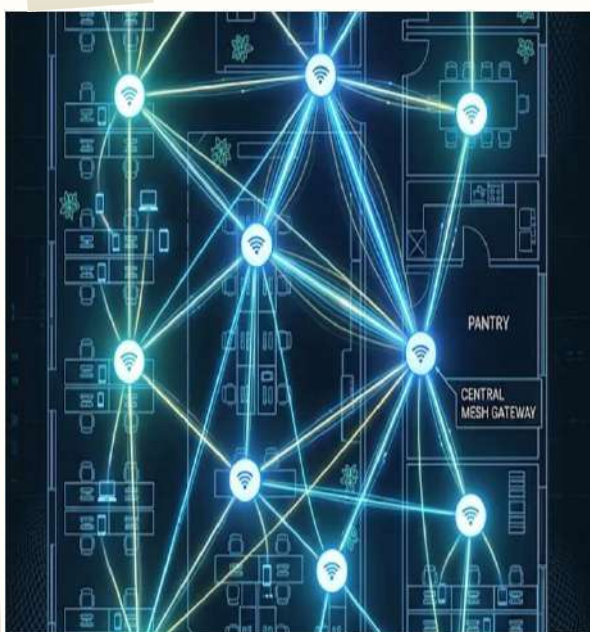
procedere con estrema cautela o rivolgersi ad un esperto.



www.sunrisetechnology.it

6 • Mesh o AP cablati?

Nelle reti Mesh i nodi comunicano tra loro via radio, senza un cavo di rete dedicato. Facili da installare e non richiedono opere murarie, ma se il backhaul è wireless, parte della banda viene usata per l'interconnessione e le prestazioni calano all'aumentare dei nodi.



Nodi, backhaul e zone di roaming

SOLUZIONE PROFESSIONALE

In azienda l'ideale sono Access Point collegati via cavo Cat 6 o 6A con alimentazione PoE a uno switch centrale: banda piena su ogni nodo e gestione centralizzata.

802.11k — aiuta i client a trovare rapidamente gli AP vicini.

802.11r — riduce i tempi di autenticazione quando ci si sposta.

802.11v — suggerisce al dispositivo l'AP con il segnale migliore.

Risultato: VoIP e videoconferenze che non cadono.



Una rete che si misura è una rete che si governa

Esplora altri trucchi e tutorial su
www.sunrisetechnology.it →