www.sunrisetechnology.it

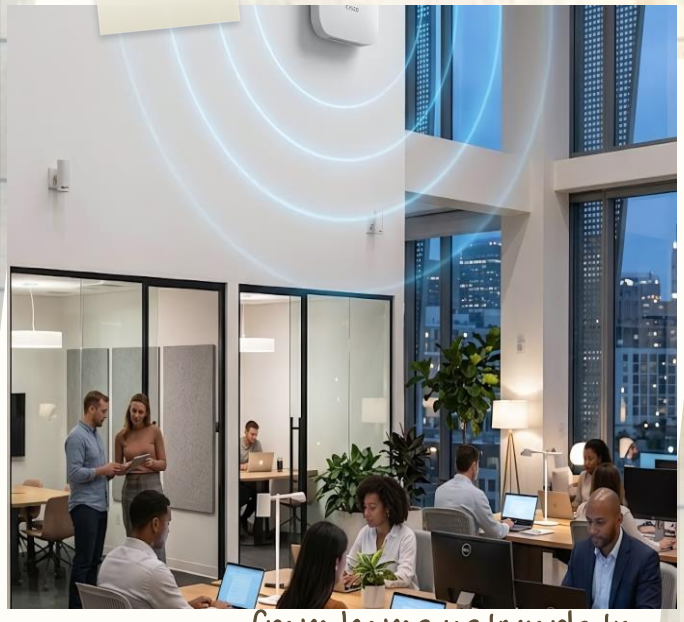
FROM DIAGNOSIS TO ARCHITECTURE

Optimizing business Wi-Fi

Channels · AP placement · VLAN · Security



Slow Wi-Fi = lost productivity



...from home network to infrastructure

AI

Introduction

A slow or unstable Wi-Fi signal in a work environment causes more than frustration: it translates directly into lost productivity, dropped video calls with clients and potential security risks.

1 · Diagnostic tools

Before changing any hardware configuration it is essential to measure the company's airspace, to detect interference, channel overlaps and dead zones. Start with a site survey, mapping the signal room by room.



On-site survey

[APPS & TOOLS]

NetSpot

Windows, macOS, Android, iOS. Quick real-time analysis and creation of real coverage heatmaps inside the rooms.

WiFi Analyzer

Android / Windows Store. Bar or wave chart: which channels are occupied by neighbors and with what intensity (dBm).

inSSIDer

Windows, macOS. Professional tool to identify channel overlaps, saturation and the configurations of neighboring access points.

Wi-Fi SweetSpots

iOS / Android. Measures the actual data transmission speed (throughput) between smartphone and Access Point while you move around the office.

[WHAT TO LOOK FOR]

Interference from non-Wi-Fi devices, channels overlapping with neighbors, areas where real throughput collapses despite a "full" signal: these three symptoms guide the choices described in the following pages.

Parameters to monitor

RSSI — Signal Strength

Expressed in dBm: −50 dBm is an excellent signal; below −75 dBm the connection becomes unstable and slow.

Noise Floor and SNR

Gap between useful signal and radio background noise. An SNR above 25 dB ensures top performance.



Comparing the frequencies

Which band to use

2.4 GHz

Greater range, but strong interference (microwaves, Bluetooth, cordless phones) and only 3 non-overlapping channels: 1, 6, 11 .

5 GHz

Shorter range, but much higher speeds and dozens of non-overlapping channels: it is the working band for business clients.

6 GHz — Wi-Fi 6E / 7

Total absence of legacy interference: ideal for offices with a very high density of devices.

Rule of thumb: 2.4 GHz only for IoT and legacy devices, 5 GHz for PCs and video calls, 6 GHz where client density is highest.

2 · Positioning the APs

The physics of radio propagation determines 80% of the performance of a wireless network: before buying new hardware, check where and how the existing one is installed.

[TYPES]

Ceiling-mounted

"Dome-shaped" radiation pattern pointing downward: place it at the center of the area to cover, away from metal beams, ventilation ducts and reinforced-concrete pillars.

Wall / in-wall

For offices with single rooms or corridors. They radiate on the front plane: never behind metal cabinets or filing cabinets.

Outdoor

On dedicated poles, with surge protective devices (SPD) on the PoE Ethernet line and IP65/IP67 certification.



Wall AP: frontal radiation

The golden rules of positioning

Ideal height: *between 2.5 and 3.5 meters above the floor.*

Distance from obstacles: *at least 1 – 1.5 m from electric motors, main electrical panels, multifunction printers, photovoltaic inverters and unshielded server racks.*

Antenna orientation: *if external and adjustable, and you need to cover a single horizontal floor, position them vertically.*

[COMMON MISTAKES IN SMEs]

An Access Point resting on the desk or inside a closed rack, a single device on the ground floor covering two floors, an AP mounted next to the electrical panel: three situations in which no firmware update or channel change can recover the lost performance.

3 · Network design

Entrusting the management of the company network to a single "all-in-one" router/modem supplied by the phone carrier is one of the main bottlenecks. In professional environments, routing logic must be separated from the wireless one.

Gateway / Firewall

Dedicated hardware: handles IP addressing, DHCP, security rules and all network traffic.

Access Point

One or more centrally managed devices: they handle the wireless transmission of the clients.



Guest network isolated from company devices

[SEPARATE SUBNETS: SSID + VLAN]

Not all devices browsing over Wi-Fi should see each other: for security and performance, traffic must be separated on dedicated SSIDs with their own VLANs.

Corporate / Office — VLAN 10

Reserved exclusively for company computers: full access to internal servers, NAS, network printers and management software.

Guest — VLAN 20

Customers, suppliers and employees' personal smartphones: allows only Internet browsing and completely blocks communication toward company devices (Guest Isolation).

IoT / Smart — VLAN 30

IP cameras, thermostats, alarms, POS and Wi-Fi printers: they often suffer from software vulnerabilities, so it is best to isolate them from the rest of the network.

4 · Capacity & access

When dozens of smartphones, PCs and tablets try to communicate at the same time on the same Access Point, the radio channel saturates through packet collisions: you don't need more power, you need more well-distributed APs and devices of the right class.

Router / carrier modem
15–20
devices connected simultaneously: beyond that slowdowns and disconnections set in.

Business Access Point
60–150+
devices per single AP on Wi-Fi 6/6E models, thanks to MU-MIMO and OFDMA.

Access control

MAC filter — whitelist and blacklist

Useful for blocking specific unwanted devices, but on its own it does not guarantee security: MAC addresses can be spoofed.

WPA3 Enterprise — IEEE 802.1X

Instead of a single password shared among all employees — which risks remaining in the hands of those who leave the company — a RADIUS authentication server is used: each person signs in with personal credentials (username and password or certificate), which can be revoked individually.

A single password for everyone is not a security policy.

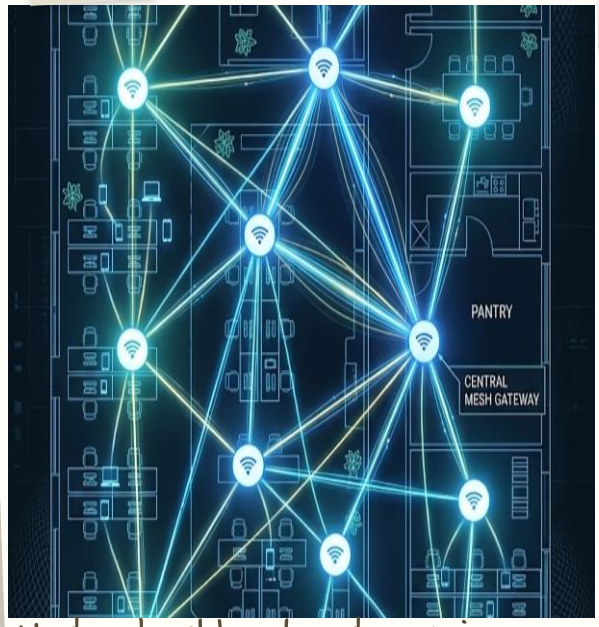
5 · Secure firmware

Updating the firmware of routers, switches and Access Points is essential to close zero-day security flaws and improve signal stability. A faulty update, however, can halt business operations — the dreaded "brick".

Very delicate operation: it requires planning, uniform updates and versions across all devices involved...
proceed with extreme caution or consult an expert.

6 · Mesh or wired APs?

In a Mesh network the nodes communicate with each other by radio, without a network cable for each node. It is easy to install and requires no construction work; but if the backhaul is wireless, part of the bandwidth is consumed by internal transmission and performance drops as nodes are added.



Nodes, backhaul and roaming zones

PROFESSIONAL SOLUTION

In business, the ideal is wired Access Points (Cat 6/6A) with PoE from a central switch: full bandwidth per node, centralized management.

***802.11k** — helps clients quickly find nearby APs.*

***802.11r** — reduces authentication time when moving around.*

***802.11v** — suggests to the device the AP with the best signal.*

Result: VoIP and video conferences that don't drop.



A network that is measured is a network that is governed

For a professional analysis, contact Sunrise Technology

Explore more tips and tutorials at

www.sunrisetechnology.it →

Created with the support of AI tools | © Sunrise Technology