Wireless LANs: Connecting the World Wirelessly

Exploring the technology that powers wireless connectivity in homes, offices, and public spaces worldwide.

The Wireless Revolution: Freedom and Flexibility

The Challenge

Traditional wired LANs restrict mobility and complicate network setup, limiting where users can work and connect.

The Solution

Wireless LANs offer unparalleled flexibility, enabling devices to connect without physical cables or fixed locations.

The Impact

Increased mobility transforms how we work, learn, and play—creating truly connected environments.

The Heart of WLANs: IEEE 802.11 Standards

The IEEE 802.11 family of standards defines the protocols that enable wireless communication. From early speeds of 1-2 Mbps to modern multi-gigabit connections, WLAN technology has evolved dramatically.

1

802.11 (1997)

Introduced wireless networking with speeds of 1-2 Mbps using 2.4 GHz band.

2

802.11b (1999)

First widely adopted standard offering 11 Mbps on 2.4 GHz band.

3

802.11g (2003)

Boosted speeds to 54 Mbps whilst maintaining 2.4 GHz compatibility.

4

802.11n (2009)

Introduced MIMO technology, achieving up to 600 Mbps across dual bands (2.4/5 GHz).

5

802.11ac (2013)

Multi-gigabit speeds (up to 6.9 Gbps) on 5 GHz band with enhanced efficiency.

6

802.11ax (2019/2020)

Wi-Fi 6/6E delivers improved performance in dense environments with better efficiency.

WLAN Architecture: Infrastructure vs. Ad-Hoc

Infrastructure Mode

Utilises Access Points (APs) to connect wireless devices (Stations - STAs) to wired networks. Forms Basic Service Sets (BSS) and Extended Service Sets (ESS).

Most common setup for homes and businesses, providing centralised management and internet access.

Ad-Hoc Mode

Direct peer-to-peer connection between devices without an Access Point intermediary.

Ideal for temporary networks such as file sharing at conferences or small group collaborations.

Navigating the Wireless Landscape: Key Components & Protocols

Stations (STA)

Any device with an 802.11 interface—laptops, smartphones, tablets, IoT devices that connect wirelessly.

Access Points (AP)

Bridge wireless traffic to wired networks, managing connections and providing network access.

Medium Access Control

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) manages access to shared wireless medium, preventing data collisions.

Hidden Terminal Problem

Challenge where two STAs communicate with an AP but not each other, requiring specific MAC layer solutions.

Securing Your Wireless World

Wireless signals broadcast through air, making them susceptible to interception and unauthorised access. Security protocols have evolved significantly to protect data.

WEP (Wired Equivalent Privacy)

Early security now considered insecure and easily compromised.

WPA (Wi-Fi Protected Access)

Improved security over WEP with better encryption protocols.

WPA2

Robust security using AES encryption, widely adopted standard.

WPA3

Latest standard with enhanced security and simplified password management.

Best Practice: Always use WPA2 or WPA3 with a strong, unique password to secure your wireless network.