WLAN Basics

1. Introduction to WLAN

- What is WLAN?- A **WLAN** stands for **Wireless Local Area Network** — basically, it's a local network that uses **radio waves instead of cables** to connect devices.

- Difference between WLAN and LAN - WLAN uses wireless signals (Wi-Fi), while LAN uses Ethernet cables.

Key Points

- **"Wireless"** → Uses Wi-Fi (IEEE 802.11 standards) instead of Ethernet cables.
- **"Local Area"** → Covers a limited area like a home, office, school, or coffee shop.
- **"Network"** → Allows multiple devices (laptops, phones, printers, IoT devices) to communicate with each other and/or connect to the internet.

How it Works

- Devices use **802.11 radio signals** to connect to an AP.
- The AP forwards data to other devices on the LAN or to the internet via a wired connection.
- Uses **frequency bands** like **2.4 GHz**, **5 GHz**, and **6 GHz**.

- Use cases of WLAN in real-world scenarios - Home Wi-Fi, enterprise wireless networks, public hotspots, IoT devices, etc

Example

When you connect your laptop to your home Wi-Fi, you're joining your **WLAN**.
If you connect to a hotspot at a café, that's also a WLAN — just in a public space.

2. IEEE 802.11 Standards Overview

- Evolution of Wi-Fi (802.11a/b/g/n/ac/ax/be)

Standard	Frequency Band	Bandwidth	Modulation	Max Data rate
802.11	2.4 GHz	20 MHz	FHSS, DSSS	1-2 Mbps
802.11b	2.4 GHz	20 MHz	DSSS, HR-dsss,cck	5.5-11Mbps
802.11a	5 GHz	20 MHz	OFDM, 16 QAM	54 Mbps
802.11g	2.4 GHz	20 MHz	OFDM, 16 QAM	54 Mbps
802.11n	2.4 GHz	20-40 MHz	MIMO, 64 QAM	600 Mbps

802.11ac(Wave 1) (wifi 5)	5 GHz	Upto 80 MHz	SU-MIMO, 256 QAM, beamforming	1.7 Gbps
802.11ac(Wave 2) (wifi 5)	5 GHz	Upto 160 MHz	MU-MIMO, 256 QAM, beamforming	6.93 Gbps
802.11 ax (wifi 6)	2.4/5/6 GHz	160 MHz	8x8 MU-MIMO, 1024 QAM, OFDMA, BSS color, TWT	9.3 Gbps
802.11be (wifi 7)	2.4/5/6 GHz	320 MHz	MLO, 4096 QAM,16x16 MU-MIMO	46 Gbps

- Frequency bands used (2.4 GHz, 5 GHz, 6 GHz)

- **2.4 GHz Band** – upto 14 channels available (based on country) - 1,6,11 non overlapping channels
- Frequency Range - The 2.4 GHz band ranges from 2.400 GHz to 2.4835 GHz. This gives a total of 83.5 MHz of usable spectrum.
- **5 GHz band** - Total 25 channels
- Non DFS - 9 channels (36, 40, 44, 48, 149, 153, 157, 161, 165)
- DFS - 16 channels(52, 56, 60, 64, 100–144)
- DFS channels - DFS is a regulatory mechanism used in Wi-Fi networks (especially in the 5 GHz band) to ensure Wi-Fi devices do not interfere with radar systems, such as:
  1.Weather radar
  2. Air traffic control radar
  3. Military radar
- 6 GHz band - Total 59 channels(PSC and Non PSC) - 5925 MHz to 7125 MHz

3. WLAN Architecture

- Basic components:
  Access Point (AP) - Provides wireless access to clients.
  Wireless Client (Station) - Any device with Wi-Fi (phone, laptop, etc.).
  Wireless Controller(in enterprise setups) - Manages APs centrally (in enterprise setups).
  Distribution System(DS) - The wired or wireless backbone connecting APs to the network.
- Infrastructure mode vs Ad-hoc mode
  Infrastructure mode: Clients connect via AP.
  Ad-hoc mode: Devices connect directly without AP.(wifi direct,file sharing)

4. WLAN Frame Types

- Management frames (Beacon, Probe Request/Response, Authentication, Association)

- Control frames (RTS/CTS, ACK) - help manage medium access.
- Data frames - Carry actual payload (user data).

5. WLAN Communication Process

- Scanning (Passive vs Active) - Station listens for beacon frames.
- Authentication-Verifies identity (Open or 802.1X) and Association - Station joins the AP and gets connection parameters.
- DHCP and IP acquisition - Station gets an IP address from the DHCP server.

6. WLAN Security Basics

- Open-No security (public Wi-Fi), WEP- Obsolete and insecure, WPA2-Still widely used, uses AES, WPA3-More secure, uses SAE handshake, stronger encryption.
- Authentication methods (PSK, 802.1X)-Enterprise security with RADIUS authentication.
- Encryption methods (TKIP, AES, CCMP)

7. Channel, Frequency & Interference

- Channel width (20/40/80/160 MHz)
- Non-overlapping channels in 2.4 GHz- 3 non-overlapping channels (1, 6, 11), more interference. and 5 GHz-More non-overlapping channels, less congestion.
  6 GHz: Introduced in Wi-Fi 6E and 7, much cleaner spectrum.
- DFS channels - DFS is a regulatory mechanism used in Wi-Fi networks (especially in the 5 GHz band) to ensure Wi-Fi devices do not interfere with radar systems, such as:
  1.Weather radar
  2. Air traffic control radar
  3. Military radar

8. WLAN Performance Factors

- RSSI- (Received Signal Strength Indicator): Signal strength, SNR-(Signal-to-Noise Ratio): Higher = better quality.Throughput
- MIMO-Multiple antennas for higher throughput, MU-MIMO-Multiple users served simultaneously, OFDMA-Divides channel into sub-carriers to serve multiple clients.
- Roaming basics - Station switches between APs with better signal.(802.11 k/v/r)

9. WLAN Tools and Testing

- Wireshark, OmniPeek
- iPerf/ixia-chariot for throughput testing-Measures network throughput.