adapt to rapidly changing
→ needs and
wireless technologies ⑤

WAN
— ~~Wireless~~ Area Net.
wireless

wireless

④ types:

WPAN   WLAN   WWAN   WMAN
↓   ↓   ↓   ↓
Personal   Local   Wireless   metropolitan
                            Wide

Ex: Bluetooth
    Zigbee

wireless technologies:

Bluetooth :   mesh, point-to-point

WiMAX :   Alt. broadband wired internet
          connections with a long range.

Cellular Broadband: phones, tablets, laptops,
                     automobiles
                → (GSM) and CDMA standards

Satellite Broadband : rural areas

(AP) 2 types

- Autonomous
- Controller based

(Antennas) 3 types

- omnidirectional
- directional
- MIMO (multiple input multiple output)

Wireless Standard Organizations: 1) ITU

2) IEEE

3) Wi-Fi Alliance

access point
switch
router

serve as

Home **(Router)**

WLAN Components:

1) Wireless NIC
2) " Home (Router)
3) " Access point
4) " Antennas

5) Internet Port

6) Autonomous and controller-based access points
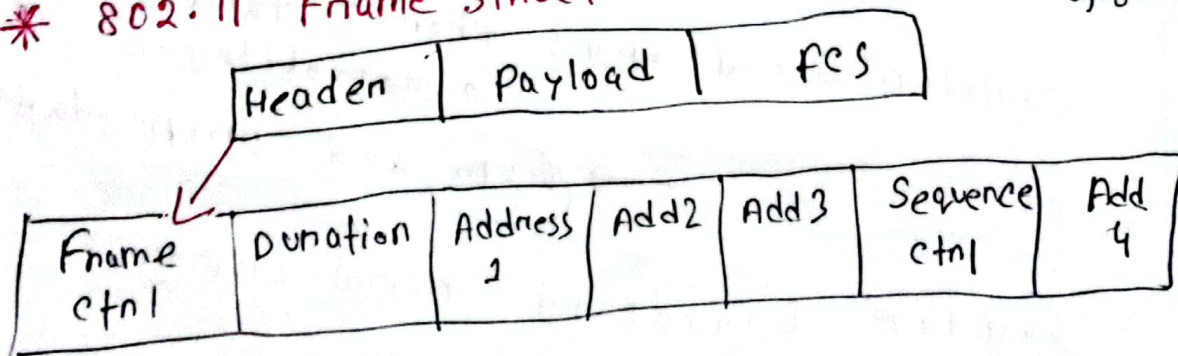
WLAN Operation:

1) Wireless Topology modes:

- Ad hoc mode (peer to peer, no AP)
- Infrastructure (use AP)
- Tethering → personal hotspot

2) **(B)SS** and **(E)SS** → **(Extended)** Ser. Set.

↓

Basic Service set

* 802.11 Frame Structure → similar to ethernet frame format

Header	Payload	FCS

Frame ctrl	Duration	Address 1	Add 2	Add 3	Sequence ctrl	Add 4

_In WLAN, wireless devices associate with
an AP (access point)

_This association process has | 3 stages |.
                                      daa
  1) discover a wireless AP
  2) authenticate with AP | 2 scanning (probing)
                                   | processes:
  3) associate   "   " | 1) Passive 2) Active

        8 5 parameters ——→ AP agrees on
    1) SSID (service set identifier)

    2) Password

    3) Network mode   5) channel the setting
    4) security   "   read / modify data

                                   | MITM (man in the middle)
Wireless Networks' Threats: | → hacker positioned
                                   | between 2 legitimate
1) Data interception | entities

2) Wireless intruders   (Reason) - improperly configured
                                          devices
3) Denial of service (DoS)   — malicious user
      attacks   — accidental interfere
                                                        nce
4) Rogue APs → - data interception
               — wireless intruders

Secure WLANS:

1) Open System authentication

2) Shared key "
   $\longrightarrow$ WEP, WPA, WPA2, WPA3

3) SSID cloaking

4) MAC Address filtering

5) Home User authentication $\longrightarrow$ personal, enterprise

6) Encryption
   - $\longrightarrow$ TKIP, AES (2 methods)
   - $\longrightarrow$ used by WPA and WPA2