IEEE 802.11 Evolution and Future of Wifi

A concise Journey through the architecture, Innovations and impact of Wireless LAN

Abdulai Tamba Lebbie

16th July, 2025

Content List

Introduction

IEEE 802 and 802.11

- IEEE 802 is a family of Institute of Electrical and Electronics Engineers (IEEE) standards for local area networks (LANs), personal area networks (PANs), and metropolitan area networks (MANs).

- specifies the set of medium access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication.

- The base version of the standard was released in 1997 and has had subsequent amendments, where each amendment is labelled as 802.11x

- IEEE 802.11 uses various frequencies including, but not limited to 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands.

- Although IEEE 802.11 specifications list channels that might be used, the allowed radio frequency spectrum availability varies significantly by regulatory domain.

- This radio frequency spectrum allowed for data transmission across devices

Timeline of Evolution

- 802.11-1997 was the first wireless networking standard in the family, but 802.11b was the first widely accepted one, followed by **802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.** Other standards in the family (c–f, h, j) are service amendments that are used to extend the current scope of the existing standard, which amendments may also include corrections to a previous specification

- 802.11b and 802.11g use the 2.4-GHz ISM band,802.11n can also use that 2.4-GHz band. Because of this choice of frequency band, 802.11b/g/n equipment may occasionally suffer interference in the 2.4-GHz band

- 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively.

Timeline of Evolution from Mbps to Gbps

802.11b (1999): The beginning of widespread Wi-Fi.

- Speed: Up to 11 Mbps
- Frequency: 2.4 GHz

802.11a/g (2003): Significant speed boost.

- Speed: Up to 54 Mbps (802.11a used 5 GHz, 802.11g used 2.4 GHz)

802.11n (2009): The "N"ew era of Wi-Fi.

- Speed: Up to 600 Mbps
- Key Tech: MIMO (Multiple antennas), Dual-band (2.4 GHz & 5 GHz)

802.11ac (2013): Gigabit Wi-Fi arrives.

- Speed: Over 1 Gbps
- Key Tech: MU-MIMO (for multiple users), Primarily 5 GHz band
- signaling methods, respectively.

802.11ax (2019) - Wi-Fi 6 / 6E: Efficiency and Capacity.

- Key Tech: OFDMA (better for many devices), BSS Coloring (reduces interference), Wi-Fi 6E (adds 6 GHz band)

802.11be (Expected 2024) - Wi-Fi 7: The next leap.

- Key Tech: Multi-Link Operation (MLO), Wider Channels (320 MHz), 4K-QAM (more data per signal)

Year	IEEE Standard	Freq (GHz)	Maximum Speed
1999	802.11b	2.4	11 Mbps
1999	802.11a	5.0	54 Mbps
2003	802.11g	2.4	54 Mbps
2008	802.11n	2.4 & 5.0	600 Mbps
2013	802.11ac	5.0	6,933 Mbps

Generalization

Year	Generation	IEEE Standard	Freq (GHz)	Max PHY Rate
1999	*Wi-Fi 1*	802.11b	2.4	1 - 11 Mbps
1999	*Wi-Fi 2*	802.11a	5.0	6 - 54 Mbps
2003	*Wi-Fi 3*	802.11g	2.4	6 - 54 Mbps
2008	Wi-Fi 4	802.11n	2.4 & 5.0	72 - 600 Mbps
2013	Wi-Fi 5	802.11ac	5.0	433 - 6,933 Mbps
2019	Wi-Fi 6	802.11ax	2.4 & 5.0	600 - 9,608 Mbps
2020	Wi-Fi 6E	802.11ax	6.0	600 - 9,608 Mbps
2024	Wi-Fi 7	802.11be	2.4, 5.0 & 6.0	1,376 - 46,120 Mbps

Key Technologies Explained

- **Speed Comparison :** theoretical and real-world speeds, which are Lab specs and daily experience (affected by walls, interference, etc.)

- **Compatibility :** New routers still support older routers for communication (wifi 6 can talk to wifi 4)

- **Different Spectrum Bands.**

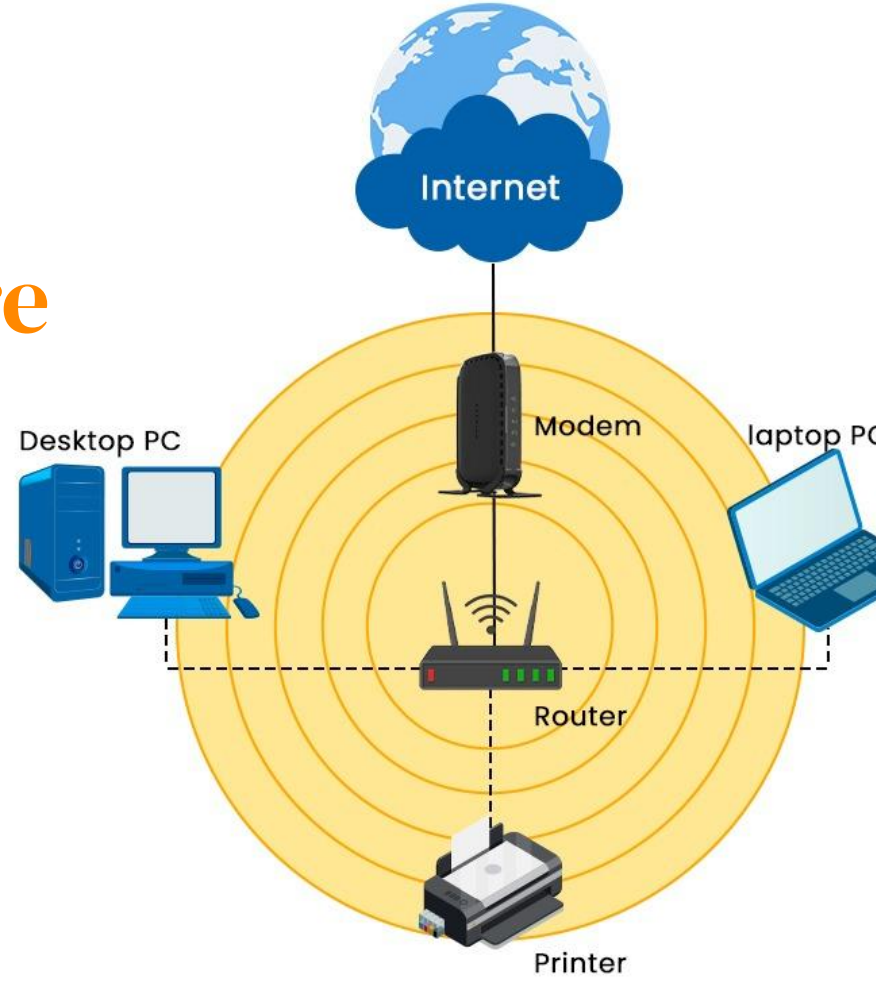
  a. 2.4 GHz: longer range, more interference

  b. 5 GHz: faster, cleaner, shorter range

  c. 6 GHz: newest, fastest, for latest-gen devices only

The Wifi A Architecture (802.11 Stack)

This slide conveys the functionality of the Wifi, how it works under the hood and particularly how devices communicate and manage connections



Basic Service Set (BSS)

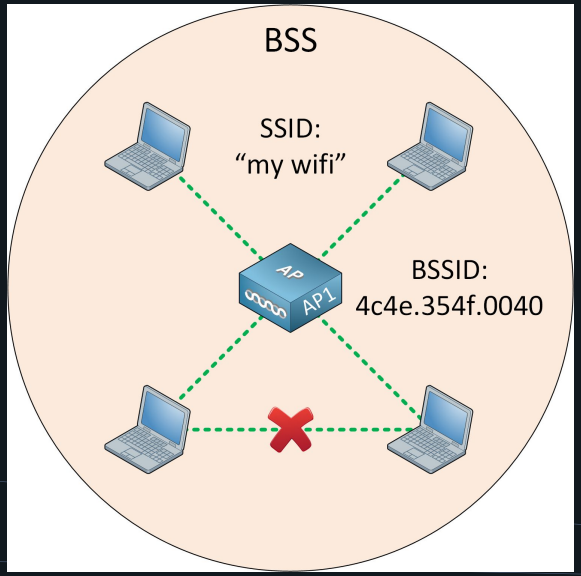
This is the fundamental building block of the IEEE 802.11 wireless network standard. It provides the framework for devices to communicate wirelessly.

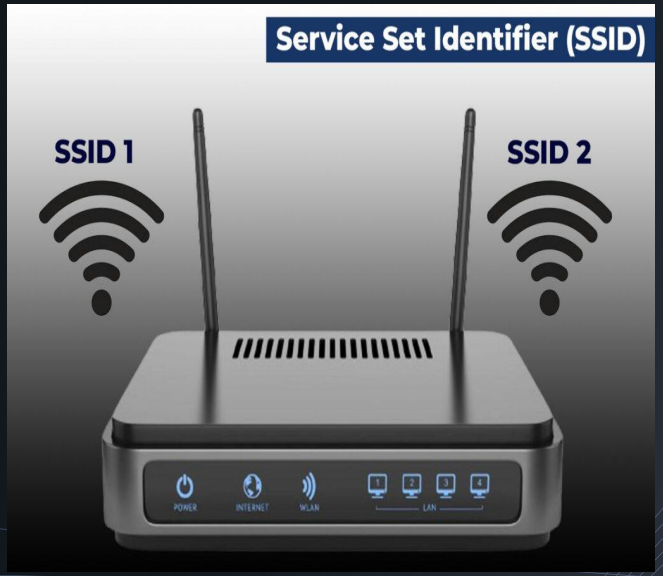
The Key infrastructure in Basic Service Set (BSS) are::

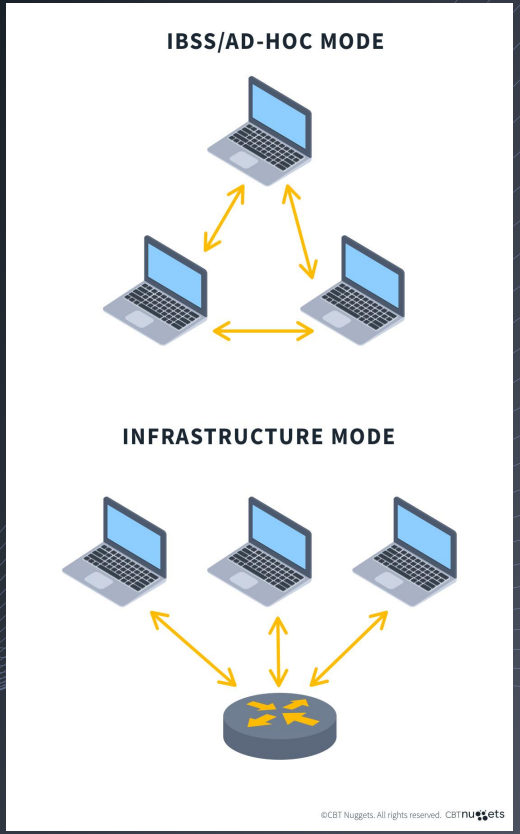
1. Access Point (AP)
2. Stations (STAs)
3. Service Set Identifier (SSID)
4. Basic Service Area (BSA)

Types:

1. Infrastructure BSS
2. Independent BSS (IBSS)


BSS
SSID:
“my wifi”
AP
AP1
BSSID:
4c4e.354f.0040


Service Set Identifier (SSID)
SSID 1
SSID 2
POWER
INTERNET
WLAN
LAN


IBSS/AD-HOC MODE
INFRASTRUCTURE MODE
©CBT Nuggets. All rights reserved. CBTnuggets

Extended Service Set (ESS)

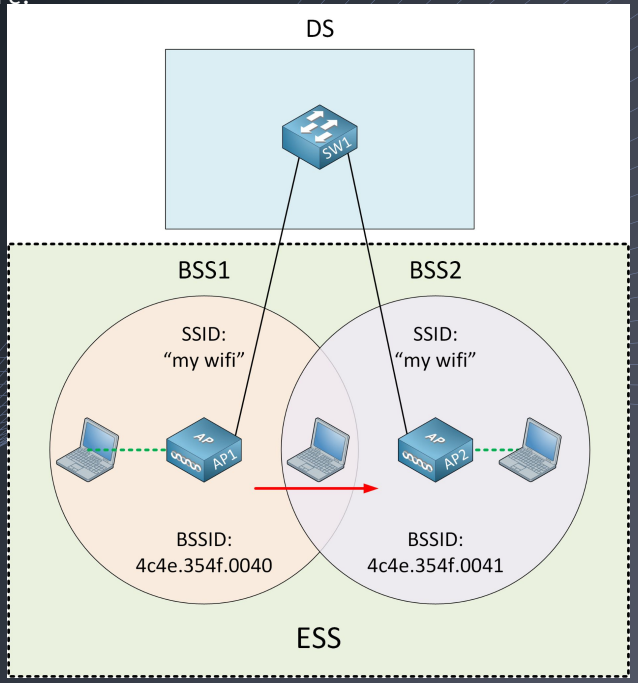
An ESS is created by multiple access points, which appears to users as a single, seamless network. It essentially extends the coverage area of a wireless network beyond a single access point.

The Key infrastructure in Extended Service Set (ESS) are::

1. Distributed System (DS)
2. Seamless Roaming (SR)
3. Service Set Identifier (SSID)
4. Basic Service Area (BSA)

Pros and Cons:

1. Provides broader coverage
2. It's complex and costly



CSMA/CA at MAC Layer

Carrier Sense Multiple Access with Collision Avoidance is a MAC (Media Access Control) layer protocol used in wireless networks to manage data transmission through the channel.

Collision Avoidance

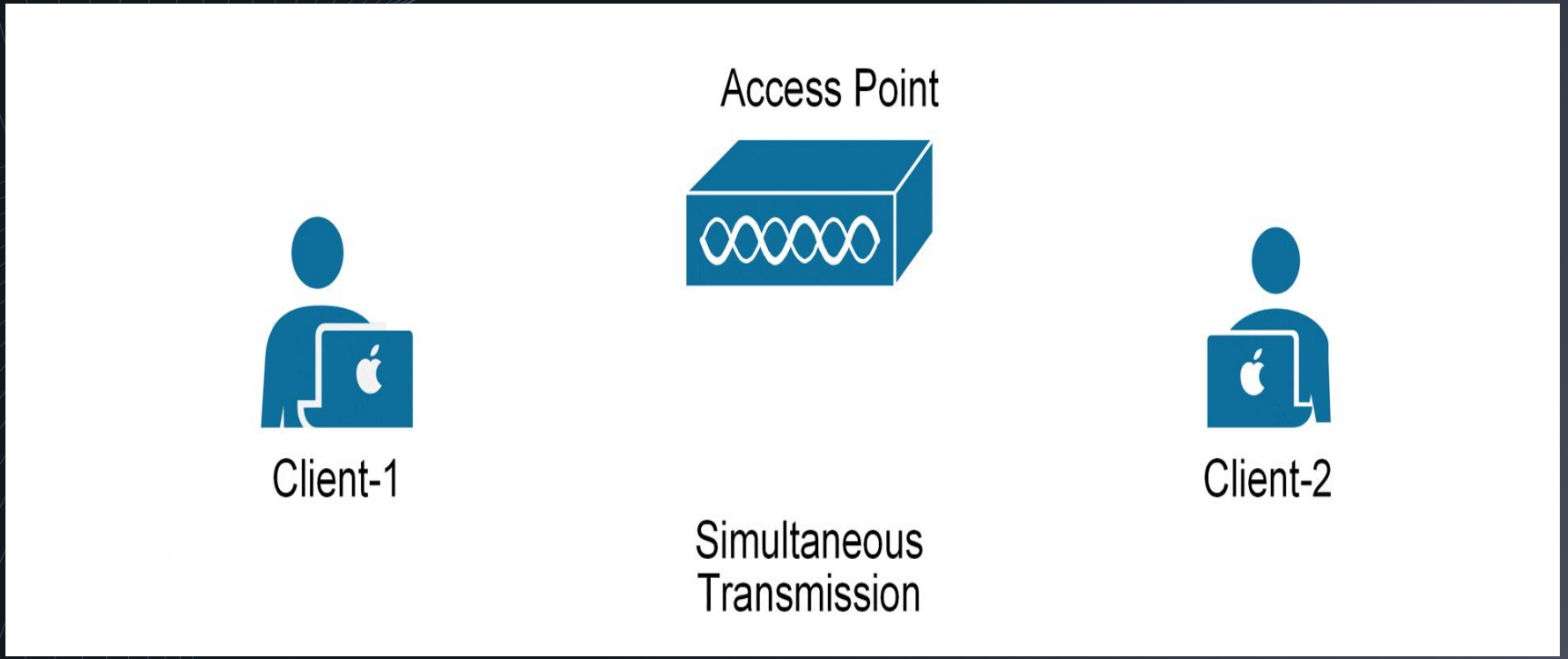
The primary goal is to prevent collison by having devices sense the channel before transmitting and using a random backoff mechanisms.

Distributed

This protocol operate in a distributed manner, by allowing each device to make it own decision about when to transmit data.

Wireless Networks

The CSMA/CA is well-suited for the unique challenges of wireless communication where it's difficult to detect collision directly


Access Point
Client-1
Client-2
Simultaneous
Transmission

Frame Types

IEEE 802.11 frames are categorized into three primary frames types:

1. **Management :** This deals with the establishment and maintenance of connections between stations (STAs) and the access points (AP). Major tasks are: Authentication, Association and Dissociation.

2. **Control :** This frame regulate the access to the wireless medium and ensure reliable data delivery. Mani tasks are: RTS/CTS, ACK, Block Ack

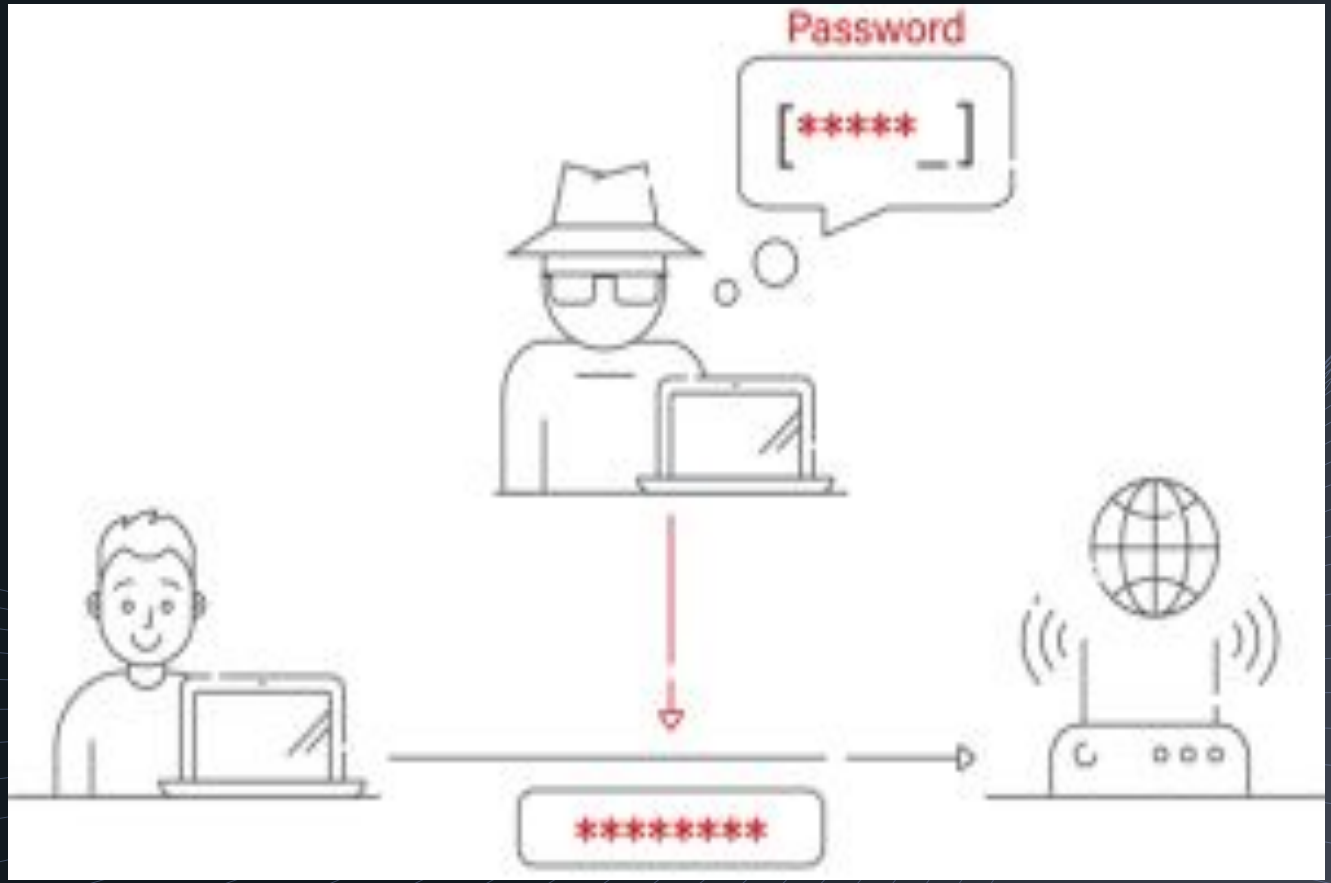
3. **Data Frames :** It carries the actual user data and higher-layer information, i.e TCP/IT Packets .. contains a frame body that includes payload.

The datagrams are called frames. Current 802.11 standards specify frame types for use in the transmission of data as well as management and control of wireless links. The frame is divided into **MAC Header, Payload and Frame Check Sequence.**

Field	Frame control	Duration, id.	Address 1	Address 2	Address 3	Sequence control	Address 4	QoS control	HT control	Frame body	Frame check sequence
Length (Bytes)	2	2	6	6	6	0, or 2	6	0, or 2	0, or 4	*Variable*	4

Security in IEEE 802.11

The Security Measures implementation that have changed the way we use the internet to communicate and engage


Password
[*****_]
****

Wired Equivalent Privacy (WEP)

This is was the first security protocol introduced by IEEE 802.11, but now outdated, because of it significant vulnerabilities and can be easily cracked by hackers.

Reasons on why it is outdated:

1. Vulnerable Encryption (RC4)
2. Lacks Robustness
3. Easily to Exploit

Wi-Fi Protected Access (WPA)

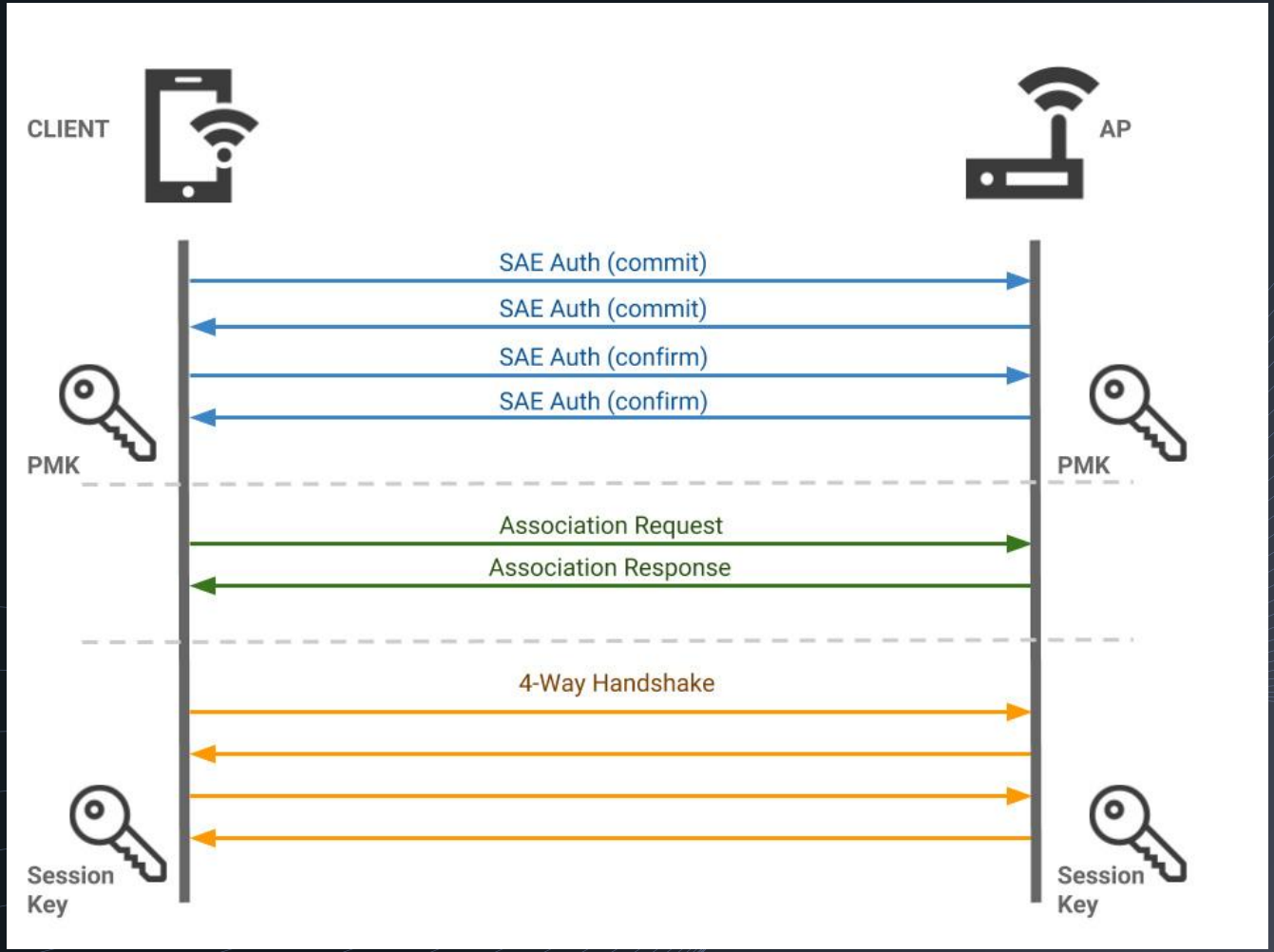
This security mechanism uses Advance Security Standard (AES) for Encryption, it offers stronger security than the older TKIP (Temporal Key Integrity Protocol) used in some WPA Implementation.

1. **Its advance version is WPA2, which uses AES (Advanced Encryption Standard), which is a robust encryption algorithm used for strong security in data transmission.**

WPA3: Modern secure authentication (SAE)

This is the latest Wifi security standard. It offers Simultaneous Authentication of Equals (SAE), as a more secure alternative to the pre-shared key in WPA2.

1. **Uses Stronger Encryption**
2. **Resistance to Password Attacks**
3. **Forward Secrecy**
4. **Simultaneous Authentication of Equals (SAE)**


CLIENT
AP
SAE Auth (commit)
SAE Auth (commit)
SAE Auth (confirm)
SAE Auth (confirm)
PMK
PMK
Association Request
Association Response
4-Way Handshake
Session Key
Session Key

The Future
Wifi 7 and Beyond

Wi-Fi 7 :: 802.11be

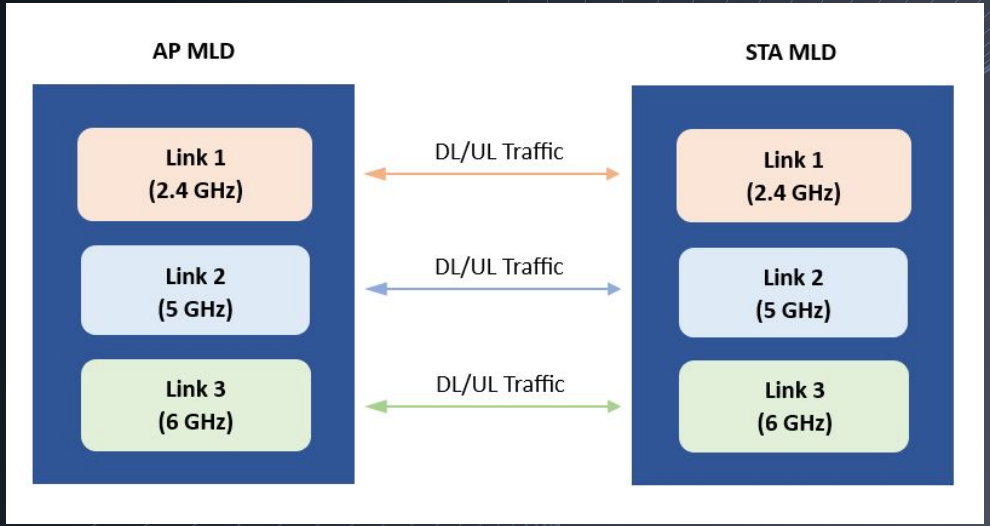
This is the latest Wifi- Standard designed for a very high throughput in order to offer much higher speed, capacity and efficiency compared to its predecessors. This feature will support high-definition video conferencing, large-scale IoT deployment and beyond.

Key Capabilities:

1. Higher Data Rates
2. Multi-Link Operation (MLO)
3. Improved Efficiency and Capacity
4. Lower Latency

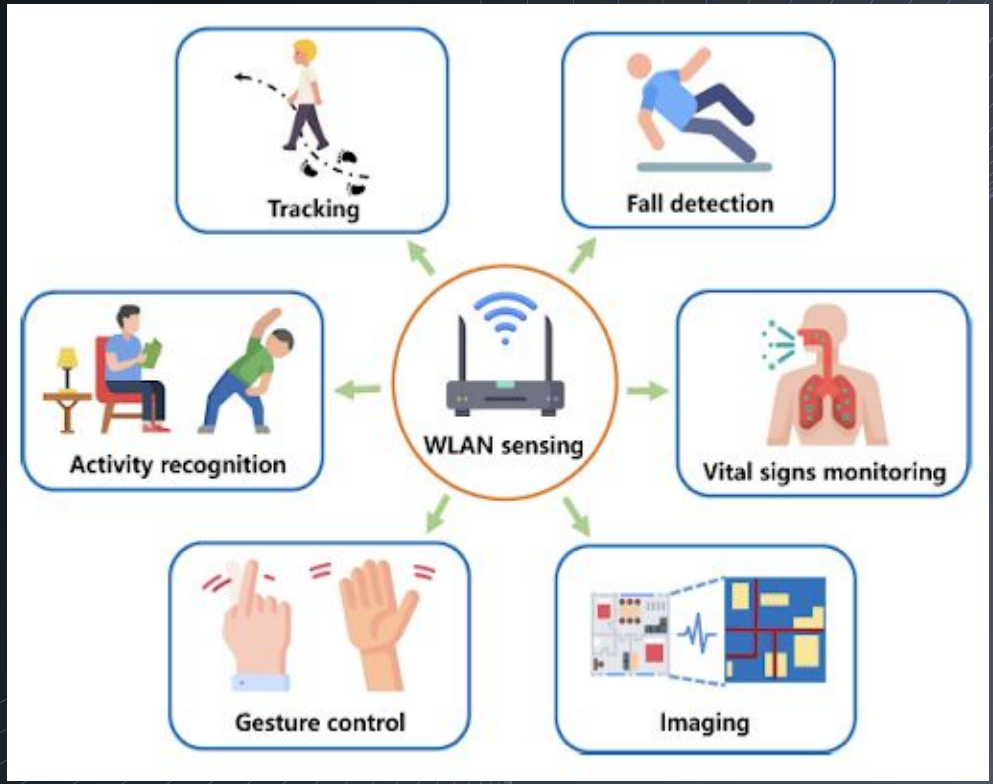
Multi-Link Operation

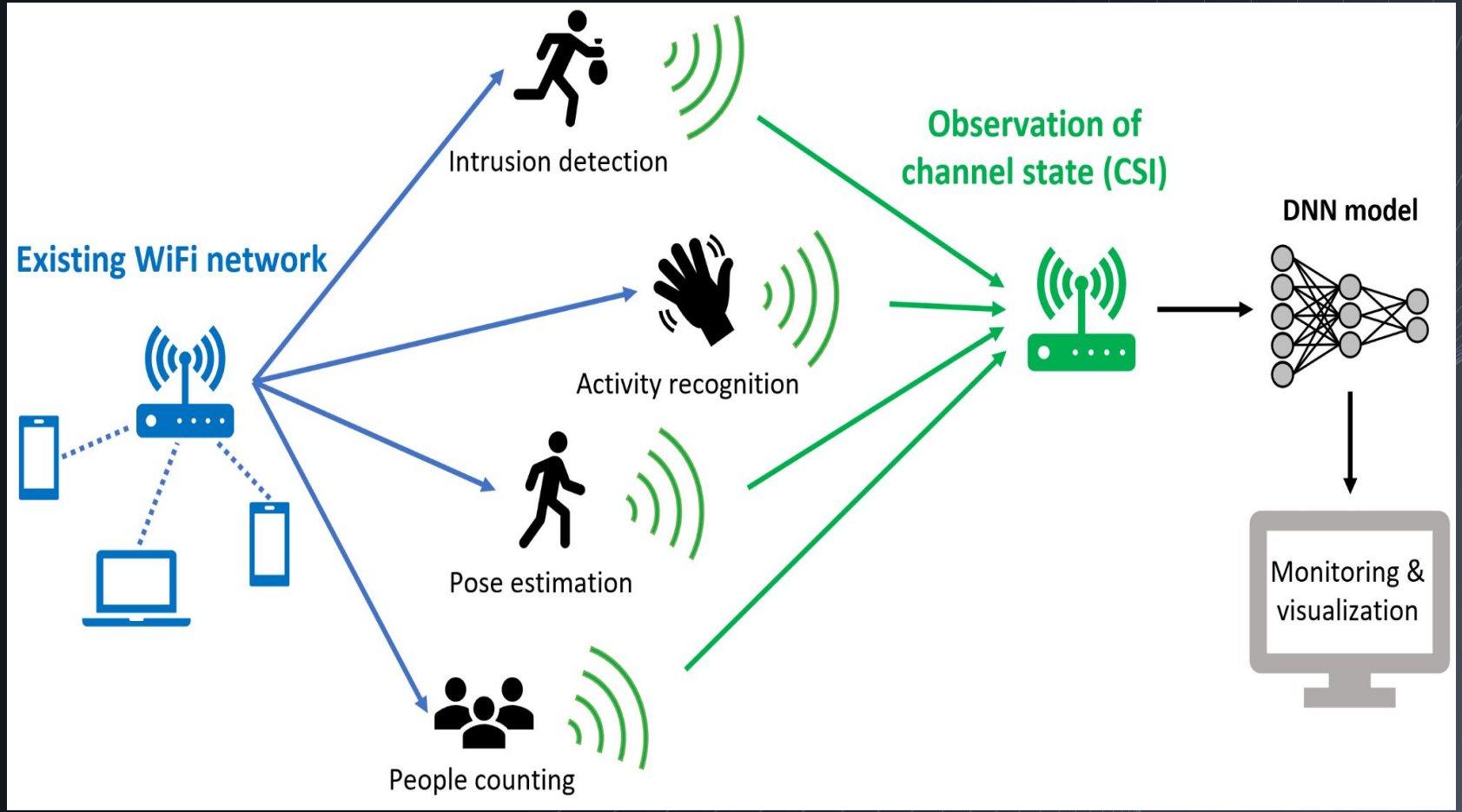
This feature allows devices to use multiple Wi-Fi interfaces simultaneously across different frequency bands (2.4 GHz, 5 GHz and 6 GHz) to increase the throughput, reduce latency, and improved spectrum reuse efficiency.



Potential of Wifi Sensing

The 802.11 framework relies on channel state information (CSI) to dynamically know what shape the normal operation of a Wi-Fi transmission is in and how to self-adjust for the best chance of working well. Changes of varying magnitude are almost constant, and CSI gathers a slew of information that end users generally don't care about. It's part of the magic behind the Wi-Fi curtain.




Existing WiFi network
Intrusion detection
Activity recognition
Pose estimation
People counting
Observation of channel state (CSI)
DNN model
Monitoring & visualization

Conclusion

- IEEE 802.11 has evolved to meet growing demands
- Wi-Fi remains foundational to connectivity
- Future standards continue to push boundaries