Velammal College of Engineering and Technology (Autonomous), Madurai

Department of Electronics and Communication Engineering

UNIT III WIRELESS NETWORKS

Wireless LANs and PANs, IEEE 802.11 Standard, Architecture, Services, Bluetooth, Wi-Fi, WiMAX.

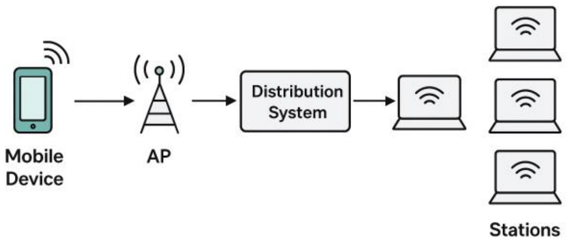
CO3: Illustrate the architecture of wireless LAN technologies.

Wireless LANs

A Wireless Local Area Network (WLAN) is a network that provides high-speed data connectivity to users within a limited geographic area such as homes, offices, campuses, or public hotspots. Instead of using cables to connect devices, WLANs rely on radio waves, making the network more flexible, mobile, and easy to install. The most widely used WLAN technology is IEEE 802.11, commonly known as Wi-Fi. WLANs allow devices such as laptops, smartphones, tablets, and IoT sensors to access network services and the internet without physical wiring.

The architecture of a WLAN typically consists of **Access Points (APs)** and **wireless stations (clients)**. An access point functions as a central transmitter and receiver that connects wireless devices to the wired LAN or the internet. WLANs may be deployed in two modes: **infrastructure mode** and **ad hoc mode**. In infrastructure mode, all communication passes through an AP, which manages authentication, channel allocation, and connection stability. In ad hoc mode, devices communicate directly with one another without any intermediary AP, forming a peer-to-peer network that is suitable for temporary or small-scale communication needs.

WLAN Architecture



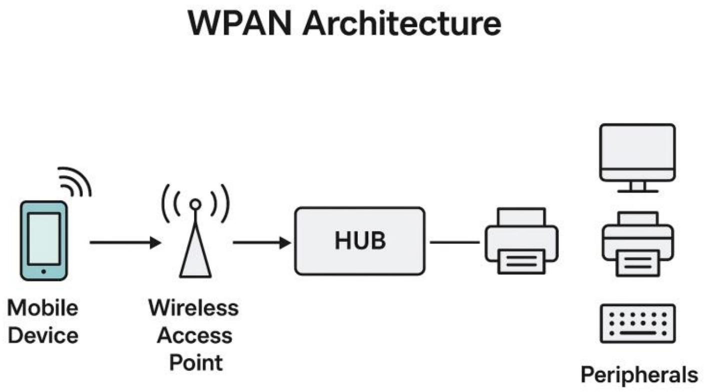
WLANs operate across several frequency bands, mainly **2.4 GHz** and **5 GHz**, using modulation techniques like DSSS, OFDM, and MIMO technologies to enhance speed and reliability. Different IEEE 802.11 standards define various capabilities: 802.11b and 802.11g offer moderate speeds in the 2.4 GHz band, while 802.11n and 802.11ac/ax provide significantly higher throughput using channel bonding, spatial multiplexing, and advanced antenna techniques.

Security is an essential aspect of WLANs because wireless signals can extend beyond physical boundaries, making the network vulnerable to unauthorized access. To address these issues, security protocols such as **WEP, WPA, WPA2, and WPA3** have been developed to ensure encryption, authentication, and integrity. WLANs also incorporate MAC layer mechanisms like **CSMA/CA** to avoid collisions during wireless transmission. WLANs are widely used in enterprise environments, educational institutions, public transport, and smart homes due to their flexibility, scalability, and ability to support large numbers of users.

Wireless PANs (WPANs)

A Wireless Personal Area Network (WPAN) is a short-range wireless network designed to connect devices in close proximity, typically within a range of a few meters. WPANs are intended for personal or individual use, enabling communication among devices such as smartphones, wearables, laptops, headsets, printers, sensors, and other portable electronics. WPAN technologies focus on low power consumption, small coverage space, and simple device pairing, making them ideal for personal device connectivity.

The most widely used WPAN standards include **Bluetooth (IEEE 802.15.1)**, **ZigBee (IEEE 802.15.4)**, and **Infrared (IrDA)**. Bluetooth is the most popular WPAN technology and operates in the 2.4 GHz ISM band using frequency-hopping spread spectrum (FHSS). It supports both voice and data communication and is commonly used for wireless audio, file transfer, peripheral connectivity, and IoT applications. Bluetooth organizes devices into small networks known as **piconets**, where one device acts as a master and the others function as slaves. Multiple piconets can form a larger structure known as a **scatternet**, enabling more complex device relationships.



ZigBee is another important WPAN technology designed for low-power, low-data-rate applications such as home automation, industrial monitoring, and sensor networks. Operating in the 2.4 GHz band, it supports mesh networking, where devices can relay data for one another, greatly extending network coverage. ZigBee is optimized for energy efficiency and long battery life, making it suitable for IoT ecosystems. Infrared communication (IrDA) was an early WPAN method, primarily used for remote controls and short-distance line-of-sight data transfer, but its usage has declined with the rise of Bluetooth and ZigBee.

WPANs emphasize **simplicity and low energy consumption**, using lightweight protocols for connectivity and communication. Security is provided through authorization, device pairing, link keys, and encryption. Bluetooth, for example, offers multiple security modes, including authentication and encryption during data exchange. WPANs have become an integral part of personal computing and IoT applications, enabling seamless interaction among everyday devices through low-cost, low-power wireless links.

WLAN Vs WPAN

Parameter	WLAN (Wireless LAN)	WPAN (Wireless PAN)
Full Form	Wireless Local Area Network	Wireless Personal Area Network
Coverage Range	Large range: 30–300 meters (home, office, campus)	Very small range: 1–10 meters (personal space)

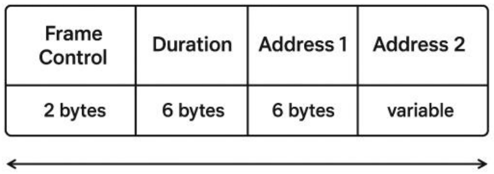
Standard Used	IEEE 802.11 (Wi-Fi)	IEEE 802.15 (Bluetooth, ZigBee, IrDA)
Primary Purpose	Connects many devices for internet and LAN access	Connects personal devices around an individual
Typical Devices	Laptops, PCs, smartphones, printers, routers, IoT devices	Wearables, headsets, phones, smartwatches, sensors
Network Infrastructure	Requires Access Point (AP); supports Infrastructure & Ad-hoc	Usually ad-hoc/piconet; may use master–slave structure
Data Rate	High speeds: 11 Mbps to several Gbps (Wi-Fi 6/6E/7)	Low to moderate: 20 Kbps to 3 Mbps (Bluetooth)
Power Consumption	Medium to high	Very low (optimized for battery devices)
Frequency Bands	Mainly 2.4 GHz, 5 GHz, and now 6 GHz	Mostly 2.4 GHz ISM band
Security Mechanisms	WPA, WPA2, WPA3 encryption, authentication	Bluetooth pairing, link keys, ZigBee AES encryption
Cost of Setup	Medium to high (APs, routers, infrastructure)	Very low (built-in in personal devices)
Network Size	Supports tens to hundreds of devices	Supports few devices (8 for Bluetooth piconet)
Mobility	Offers good mobility within the coverage area	Limited mobility around the user
Applications	Office networks, home Wi-Fi, hotspots, campuses	Wearables, IoT devices, personal connectivity
Interference	More prone due to wide range and many users	Less interference due to low-power signals
Examples	Wi-Fi networks in homes/offices	Bluetooth speakers, smart bands, ZigBee sensors

IEEE 802.11 Standard

The IEEE 802.11 standard is a family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) to define how wireless local area networks (WLANs) operate. First released in 1997, the standard established the foundation for Wi-Fi technology, enabling wireless communication between devices using radio waves instead of wired Ethernet connections. IEEE 802.11 governs both the **Physical Layer (PHY)** and the **Medium Access Control (MAC) Layer**, providing rules for modulation, channel access, authentication, encryption, and power management. Its design allows wireless devices such as laptops, smartphones, printers, and IoT devices to communicate efficiently within homes, offices, campuses, and public hotspots.

At its core, IEEE 802.11 works by transmitting data over unlicensed bands, primarily the **2.4 GHz**, **5 GHz**, and more recently **6 GHz** frequency bands. The standard specifies how devices detect available channels, avoid interference, decide when to transmit, and recover from collisions. It simplifies network deployment by allowing users to form wireless networks without cables, making mobility and flexibility key advantages. The standard supports two modes of operation: **Infrastructure Mode**, where communication occurs through an Access Point (AP), and **Ad-hoc Mode**, where devices communicate directly with each other without a central controller. These modes allow IEEE 802.11 networks to scale from small personal setups to large enterprise environments.

IEEE Frame Format



Frame Control	Duration	Address 1	Address 2
2 bytes	6 bytes	6 bytes	variable

From a structural perspective, the IEEE 802.11 architecture consists of several essential components. The basic building block is the **Basic Service Set (BSS)**, which includes wireless stations and may include an access point. When multiple BSS units are interconnected through a distribution system, they form an **Extended Service Set (ESS)**, which supports roaming between access points. A station (STA) represents any device with a wireless network interface, while the AP serves as a central coordinator that facilitates authentication, data forwarding, association, and connection to the wired LAN. The combination of BSS, ESS, APs, and wired backbone forms a scalable architecture suitable for a wide range of network environments.

The **MAC layer** plays a critical role by controlling when devices can access the shared wireless medium. Because wireless signals cannot detect collisions the same way wired Ethernet does, IEEE 802.11 uses **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**. Before transmitting, a device listens to the channel; if the medium is busy, it waits for a random backoff time. To further reduce collisions, especially in scenarios where some devices cannot detect each other (hidden terminal problem), IEEE 802.11 uses the **RTS/CTS** handshake mechanism. The MAC layer also supports fragmentation, retransmission, acknowledgement frames, and power-saving mechanisms that allow devices to sleep without losing connectivity.

The **Physical Layer (PHY)** in IEEE 802.11 defines how signals are encoded and transmitted. Various modulation techniques have been introduced across different versions of the standard. Early versions used **FHSS (Frequency Hopping Spread Spectrum)** and **DSSS (Direct Sequence Spread Spectrum)**. Later standards adopted more advanced modulation and coding schemes such as **OFDM (Orthogonal Frequency Division Multiplexing)** and **MIMO (Multiple Input Multiple Output)** to achieve significantly higher data rates. Each amendment of IEEE 802.11 brought improvements in throughput, range, and reliability.

Over time, many amendments have extended the capabilities of the original standard. IEEE **802.11b** increased speeds to 11 Mbps using DSSS in the 2.4 GHz band and became widely popular. IEEE **802.11a**, operating in the 5 GHz band with OFDM, offered 54 Mbps but had shorter range. The **802.11g** standard combined the advantages of 802.11b and 802.11a by providing 54 Mbps in the 2.4 GHz band. A major milestone came with **802.11n**, which introduced MIMO technology, enabling speeds up to 600 Mbps. Later, **802.11ac** improved performance in the 5 GHz band using wider channels and multi-user MIMO, achieving over 1 Gbps. The latest standards, **802.11ax (Wi-Fi 6)** and **Wi-Fi 6E**, focus on improving efficiency in dense environments with technologies like OFDMA and operation in the new 6 GHz spectrum, supporting speeds beyond 10 Gbps.

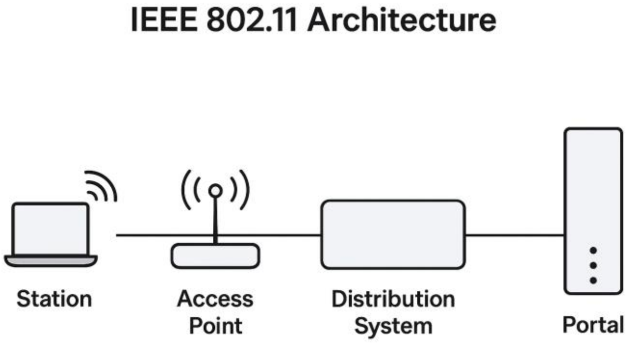
Security has been a significant focus of the IEEE 802.11 family. Early WLANs relied on **WEP (Wired Equivalent Privacy)**, which attempted to provide confidentiality similar to wired networks. However, WEP proved vulnerable due to weak key management and encryption techniques. This led to the introduction of **WPA (Wi-Fi Protected Access)** as an intermediate solution, followed by **WPA2**, which employs the robust **AES-CCMP** encryption algorithm and remains widely used today. The most recent enhancement, **WPA3**, offers stronger authentication, resistance to offline dictionary attacks, and forward secrecy, ensuring that even if keys are compromised in the future, past communications remain protected.

IEEE 802.11 Architecture

The **IEEE 802.11 WLAN architecture** defines how wireless devices communicate within a network using radio waves and how they interact with the wired network infrastructure. The architecture is designed to support mobility, flexibility, scalability, and reliable communication across various environments ranging from small homes to large enterprises. The architecture consists of several essential components, including **Stations (STAs)**, **Access Points (APs)**, **Basic Service Sets (BSS)**, **Extended Service Sets (ESS)**, and the **Distribution System (DS)**, each of which plays a specific role in the overall functioning of the WLAN.

At the lowest level of the architecture lies the **Station (STA)**, which represents any wireless device equipped with an IEEE 802.11 network interface card (NIC). Stations can be laptops, smartphones, tablets, printers, or IoT devices. Each station has the ability to transmit and receive frames using the 802.11 MAC and Physical Layer protocols. Stations may operate in one of two modes: **infrastructure mode** or **ad-hoc mode**. In infrastructure mode, stations communicate through an Access Point (AP), while in ad-hoc mode, stations communicate directly with each other without any centralized control.

The **Access Point (AP)** is a central component in infrastructure-based WLANs. It functions as a bridge between the wireless network and the wired LAN, handling communication, authentication, association, and frame forwarding. APs also manage important tasks such as channel allocation, power management, and roaming support. When a device wants to join a WLAN, it must first discover available APs, authenticate itself, and then associate with one AP. Once associated, all communication between stations in the same BSS, or between wireless and wired devices, is forwarded through the AP.



One of the fundamental building blocks of the IEEE 802.11 architecture is the **Basic Service Set (BSS)**. A BSS is a group of stations that communicate using the same MAC and Physical Layer protocols and share a common wireless channel. There are two types of BSS: **Independent BSS (IBSS)** and **Infrastructure BSS**. IBSS is used in ad-hoc networks where stations connect directly without an AP. This type of network is temporary and suitable for small groups, such as when two laptops connect wirelessly for file sharing. In contrast, an Infrastructure BSS includes an AP, and all communication occurs through it. This is the most common form of WLAN used in homes, offices, and public hotspots.

When multiple BSSs are connected through a central backbone, they form an **Extended Service Set (ESS)**. The ESS allows much larger wireless networks by linking multiple APs through the **Distribution System (DS)**, which is typically a wired Ethernet network but can also be wireless in some cases. The ESS enables seamless roaming, meaning users can move from one AP’s coverage area to another without losing connection. To maintain continuity, APs coordinate through the DS to transfer session information as a station changes its point of attachment.

The **Distribution System (DS)** is the logical and physical structure that interconnects multiple APs within an ESS. It handles tasks such as forwarding frames between APs, maintaining routing information, and managing mobility. The DS ensures that a station connected to one AP can communicate with devices connected to another AP in the same network. IEEE 802.11 does not specify how the DS should be implemented, giving flexibility for vendors to use Ethernet, fiber, wireless mesh, or proprietary technologies.

Another key component in the architecture is the **Portal**, which acts as the interface between the 802.11 WLAN and other non-802.11 networks, such as the wired Ethernet or external networks. In many cases, a portal is integrated into the AP or the router that connects the WLAN to the internet. The portal ensures proper translation and forwarding of frames across network boundaries.

The architecture also defines several important **services** that ensure smooth operation, such as authentication, association, reassociation, disassociation, distribution, integration, and roaming support. These services allow stations to join the network, remain connected while moving, and interact securely with other devices. For mobile users, the process of **handoff** or **roaming** is crucial. When a station moves away from one AP and closer to another, it initiates a reassociation process to switch APs without interrupting ongoing transmission.

IEEE 802.11 Services

The IEEE 802.11 standard defines a set of essential services that enable wireless stations to communicate efficiently, securely, and reliably within a WLAN. These services ensure that devices can join and leave the network, maintain connectivity while moving, exchange data, and interact with both wireless and wired networks. The services are broadly categorized into **Station Services (SS)** and **Distribution System Services (DSS)**, each supporting specific operations needed for wireless communication.

1. Station Services (SS)

Station services are related to operations that occur within each wireless device (station), enabling it to participate in the WLAN. These include:

(a) Authentication

Authentication is the process by which a wireless station proves its identity to the network before joining. It ensures that only authorized stations can communicate within the BSS. IEEE 802.11 supports several authentication methods, including Open System Authentication (simple request–response), Shared Key Authentication (using WEP keys), and more advanced methods like WPA/WPA2 using 802.1X. Authentication is a prerequisite before association can occur.

(b) De-authentication

De-authentication terminates an existing authenticated relationship between a station and an AP. Once a station or AP sends a de-authentication frame, the station must go through a new authentication process if it wishes to reconnect. This service is used when a device leaves the network, when roaming occurs, or security conditions require session termination.

(c) Privacy (Security)

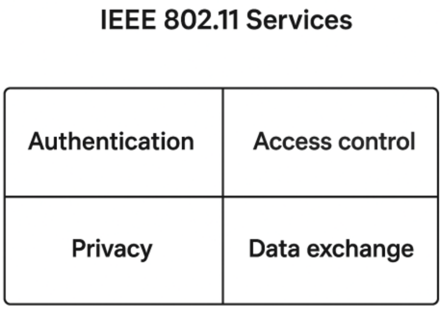
Privacy service ensures the confidentiality of data being transmitted over the air. Since wireless signals are broadcast, encryption is required to prevent unauthorized access. IEEE 802.11 originally used WEP, but due to vulnerabilities, more secure protocols like WPA2 (AES-CCMP) and WPA3 have become standard. Privacy services protect data frames, control frames, and management frames from eavesdropping and tampering.

(d) MAC Service Data Unit (MSDU) Delivery

This service ensures that the station can send and receive data frames properly across the wireless medium. The MAC layer adds necessary headers, performs fragmentation and reassembly, and handles retransmissions if errors occur due to noise or collisions.

(e) Power Management

Since many wireless devices rely on battery power, power management is a crucial service. Stations can enter a sleep mode to conserve energy. The AP buffers packets for sleeping stations and delivers them when the device wakes up. This service is essential for extending battery life in mobile devices and IoT nodes.



IEEE 802.11 Services

Authentication	Access control
Privacy	Data exchange

2. Distribution System Services (DSS)

Distribution System Services relate to the tasks performed by the **Distribution System (DS)** and **Access Points (APs)** to support mobility, forwarding, and network-wide connectivity.

(a) Association

Association allows a station to join an Access Point and become part of a BSS. During association, the AP allocates resources such as buffer space and assigns an association ID (AID) to the device. Without association, a station cannot send or receive data frames via the AP. This service enables the AP to understand which stations are currently active within its coverage area.

(b) Reassociation

Reassociation is used when a station moves from one AP’s coverage area to another. It allows seamless roaming within an ESS. When the station detects a stronger signal from a new AP, it initiates the reassociation process. The new AP contacts the old AP to transfer buffered frames and session information, ensuring continuity of communication without data loss.

(c) Disassociation

Disassociation ends the association between a station and an AP. It occurs when a station shuts down, leaves the coverage area, or when the AP decides to free resources. After disassociation, the station must undergo authentication and association again if it wants to reconnect.

(d) Distribution

Distribution service handles the delivery of frames from one AP to another AP through the DS, or from the AP to other wired network elements. For example, if Station A and Station B are connected to different APs in the same ESS, the distribution service ensures that frames are forwarded correctly across the DS so they can communicate seamlessly.

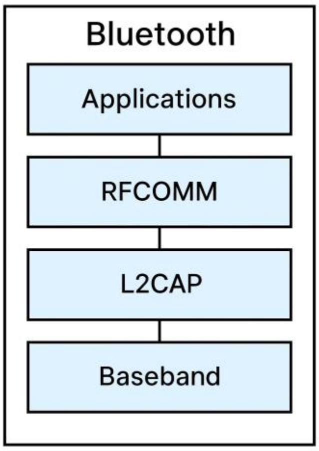
(e) Integration

Integration service enables communication between the 802.11 WLAN and other wired networks such as Ethernet or the Internet. The Portal, often built into a router or gateway, performs this role by translating frames between 802.11 format and external network formats. This service allows wireless devices to access services outside the WLAN.

Bluetooth

Bluetooth is a short-range wireless communication technology designed for creating Wireless Personal Area Networks (WPANs). It enables low-power, low-cost, and short-distance communication between devices such as mobile phones, laptops, headsets, speakers, printers, wearables, and IoT devices. Bluetooth was developed to eliminate the need for cables between electronic devices and operates using radio waves in the 2.4 GHz ISM (Industrial, Scientific, and Medical) band. It is standardized under IEEE 802.15.1, while its development and updates are overseen by the Bluetooth Special Interest Group (SIG).

Bluetooth works using Frequency Hopping Spread Spectrum (FHSS), where the device rapidly switches between 79 channels (each 1 MHz wide) to minimize interference and improve communication reliability. The hopping occurs at a rate of 1600 hops per second, allowing multiple Bluetooth devices to operate in the same area without significant interference. Its typical operating range varies between 10 meters (Class 2) and up to 100 meters (Class 1), depending on power class and environmental conditions.



From an architectural point of view, Bluetooth networks form small structures called piconets. A piconet consists of one master device and up to seven active slave devices. The master controls the clock and the frequency-hopping pattern, while the slaves follow the master's instructions. Multiple piconets can interconnect to form a scatternet, where a device can act as a slave in one piconet and a master in another. This architecture enables flexible and scalable connectivity among various personal devices.

Bluetooth is organized into a protocol stack that ensures smooth communication. At the bottom is the Radio Layer, which handles modulation and transmission of data. Above it lies the Baseband Layer, responsible for physical links, timing, and channel control. The Link Manager Protocol (LMP) manages authentication, pairing, link setup, encryption, and power control. The Logical Link Control and Adaptation Protocol (L2CAP) provide segmentation, multiplexing, and reassembly of data packets, acting as a bridge between higher-level applications and the baseband. Other important protocols include RFCOMM, which emulates serial communication, and SDP (Service Discovery Protocol), which allows devices to identify services offered by other Bluetooth devices.

Bluetooth communication relies on two types of logical links: Synchronous Connection-Oriented (SCO) and Asynchronous Connectionless (ACL) links. SCO links are used for real-time voice communication such as wireless headsets, providing guaranteed bandwidth and low latency. ACL links are used for data transmission, supporting error correction and retransmission mechanisms for reliable communication. Bluetooth devices also implement various power-saving modes, such as sniff, hold, and park, which reduce energy consumption by adjusting device activity based on communication needs.

Bluetooth security is ensured through a combination of authentication, encryption, and key management. When two devices first connect, they go through a pairing process, establishing link keys used for secure communication. Encryption prevents unauthorized eavesdropping, while authentication ensures that devices verify each other before exchanging data. Modern Bluetooth standards use stronger security methods to protect against attacks such as eavesdropping, spoofing, and man-in-the-middle attacks.

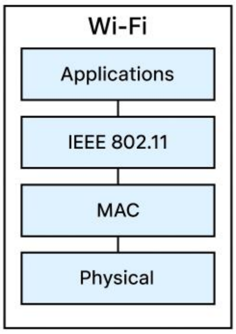
Bluetooth technology has evolved significantly since its introduction. Earlier versions (1.0 and 1.2) offered basic functionality, but later versions improved speed, range, and efficiency. Bluetooth 2.0+EDR introduced Enhanced Data Rate for faster data transmission. Bluetooth 3.0 + HS enabled high-speed transfers by using Wi-Fi for large data packets. Bluetooth 4.0 introduced Bluetooth Low Energy (BLE), which is optimized for low-power applications such as fitness trackers and IoT sensors. Modern versions like Bluetooth 5.0 and 5.2 offer longer range, improved speed, better broadcasting capacity, and efficient performance in dense environments.

Wi-Fi

Wi-Fi is a wireless networking technology based on the **IEEE 802.11** family of standards that enables devices to communicate over a local area network without physical cables. Wi-Fi has become the most widely used wireless communication technology in homes, offices, educational institutions, public hotspots, and IoT environments. It operates primarily in the **2.4 GHz**, **5 GHz**, and **6 GHz** unlicensed frequency bands, allowing high-speed data access and mobility within a limited coverage area, usually ranging from **30 meters indoors to 100 meters outdoors**.

The Wi-Fi architecture is built around two main components: **Access Points (APs)** and **Stations (STAs)**. In the infrastructure mode—the most common mode—devices connect to the network through an AP, which forwards data to the wired LAN or the internet. In **ad-hoc mode**, stations communicate directly without an AP, forming a peer-to-peer network. A group of stations associated with an AP forms a **Basic Service Set (BSS)**, and interconnected BSS units create an **Extended Service Set (ESS)**, which allows seamless roaming across multiple APs.

Wi-Fi uses **OFDM (Orthogonal Frequency Division Multiplexing)** and **MIMO (Multiple Input Multiple Output)** technologies to achieve high data rates. Early standards like **802.11b (11 Mbps)** and **802.11g (54 Mbps)** were widely adopted, while later versions like **802.11n** increased efficiency with MIMO and channel bonding. Modern Wi-Fi standards, such as **802.11ac** and **802.11ax (Wi-Fi 6/6E)**, provide multi-gigabit speeds, improved performance in dense environments, and enhanced battery efficiency for connected devices through technologies like OFDMA (Orthogonal Frequency Division Multiple Access) and MU-MIMO (Multi-User MIMO).



Wi-Fi employs **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** to manage access to the shared wireless medium. Since wireless devices cannot detect collisions easily, the CSMA/CA mechanism ensures smooth communication by listening before transmitting, using random back-off timers, and employing RTS/CTS frames to avoid hidden terminal issues.

Security in Wi-Fi has evolved significantly. The initial security protocol, **WEP**, proved weak and vulnerable, leading to the introduction of **WPA**, and ultimately **WPA2**, which uses **AES-**

CCMP encryption and became the industry standard. The latest protocol, **WPA3**, improves protection against brute-force attacks and provides individualized data encryption even in public hotspots. These advancements make Wi-Fi secure enough for both personal and enterprise environments.

In summary, Wi-Fi provides a flexible, scalable, and cost-effective wireless communication solution. Its ease of deployment, widespread adoption, high bandwidth capabilities, and strong security features have made it indispensable for modern networking, supporting everything from smartphones and laptops to smart home appliances and industrial IoT systems.

Worldwide Interoperability for Microwave Access (WiMAX)

WiMAX is a broadband wireless access technology based on the IEEE 802.16 standard. Unlike Wi-Fi, which is designed for short-range local networks, WiMAX provides high-speed wireless broadband over long distances, with coverage ranging from a few kilometers in urban areas to more than 50 km in rural regions. WiMAX was developed to offer an alternative to cable and DSL broadband, enabling wide-area wireless connectivity for fixed and mobile users.

WiMAX operates across multiple licensed and unlicensed frequency bands, typically 2.3 GHz, 2.5 GHz, and 3.5 GHz, depending on country regulations. It uses OFDM and advanced antenna technologies such as MIMO and beamforming to achieve high throughput, resistance to interference, and robust performance in non-line-of-sight (NLOS) conditions. WiMAX supports data rates up to 70 Mbps or more and can serve hundreds of users within a single coverage cell.

The WiMAX network architecture consists of three main components: the Base Station (BS), the Subscriber Station (SS) or Mobile Station (MS), and the Access Service Network (ASN). The base station acts as the central transmitter, managing radio resources, authentication, mobility, and data scheduling. Subscriber stations represent user devices such as modems, laptops, dongles, and mobile devices. The ASN handles connectivity, roaming support, and integration with external IP networks.

WiMAX supports two major service types: Fixed WiMAX (802.16-2004) and Mobile WiMAX (802.16e-2005). Fixed WiMAX provides broadband to homes, offices, and rural areas as a wireless alternative to DSL. Mobile WiMAX adds mobility and handover capabilities, enabling users to access broadband on the move, similar to cellular networks. This made WiMAX a strong competitor to early 3G and 4G technologies before LTE became dominant.

QoS (Quality of Service) is a key strength of WiMAX. It supports multiple service classes, including Unsolicited Grant Service (UGS), Real-Time Polling Service (rtPS), Non-Real-Time Polling Service (nrtPS), and Best Effort (BE). These classes allow WiMAX to handle voice, video, and data traffic efficiently, making it suitable for VoIP, streaming services, and enterprise applications.

Security in WiMAX is ensured through strong encryption and authentication mechanisms. WiMAX employs Public Key Infrastructure (PKI), AES encryption, and secure key exchange protocols to protect user data. This gives WiMAX a high level of security comparable to cellular networks.

<u>Comparison of Bluetooth, Wi-Fi & WiMAX</u>

Parameter	Bluetooth	Wi-Fi	WiMAX
Full Form	Bluetooth (Named after King Harald Bluetooth)	Wireless Fidelity	Worldwide Interoperability for Microwave Access
Standard	IEEE 802.15.1	IEEE 802.11 (a/b/g/n/ac/ax)	IEEE 802.16 (802.16d – Fixed, 802.16e – Mobile)
Network Type	PAN (Personal Area Network)	WLAN (Wireless Local Area Network)	WMAN (Wireless Metropolitan Area Network)
Coverage Range	Very short range: 1–10 m (up to 100 m for Class 1)	Medium range: 30–100 m	Long range: 5–50 km
Frequency Band	2.4 GHz ISM	2.4 GHz, 5 GHz, 6 GHz	2.3 GHz, 2.5 GHz, 3.5 GHz
Bandwidth / Data Rate	1–3 Mbps (Classic) up to 24 Mbps (Bluetooth 3.0+)	11 Mbps (802.11b) to several Gbps (Wi-Fi 6)	Up to 70 Mbps or more
Main Technology Used	FHSS (Frequency Hopping Spread Spectrum)	OFDM, MIMO, OFDMA	OFDM, MIMO, Beamforming
Primary Purpose	Wireless peripherals & short-range communication	High-speed local wireless networking	Broadband wireless access over long distances

Power Consumption	Very low	Medium	High
Applications	Headsets, IoT devices, file transfer, wearables	Laptops, smartphones, routers, hotspots	Rural broadband, backhaul, enterprise connectivity
Security	128-bit encryption, pairing	WPA2 / WPA3	Strong AES encryption, PKI
Mobility Support	Low mobility	Limited mobility (within WLAN)	High mobility (handover supported in 802.16e)
Deployment Cost	Very low	Medium	High (towers, licensed spectrum)
Typical Topology	Point-to-point / piconet	Infrastructure (AP-based)	Cell-based (Base Station + Subscriber Station)
Examples	Bluetooth speakers, keyboards	Wi-Fi routers, campus Wi-Fi	City-wide broadband, ISP wireless links