

**ARSI UNIVERSITY**

**COLLEGE OF BUSINESS AND ECONOMICS**

**DEPARTMENT OF COMPUTER SCIENCE**

**GROUP ASSIGNMENT**

**COURSE : WIRELESS COMMUNICATION AND COMPUTER NETWORKS**

***GROUP MEMBER ID NO***

1. YOBSAN GEMECHU\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UGR/11864/14

***Submitted to: Mr. FEYISA***

***Submission date: December , 2024***

**▎1. Family Members of IEEE 802.11 and Tradeoffs**

The IEEE 802.11 family consists of various standards, each offering distinct capabilities and tradeoffs. Key members include:

**802.11a**:

Operates in the 5 GHz band, providing speeds up to 54 Mbps.

* **Advantages**: High data rates with reduced interference compared to 2.4 GHz standards.
* **Disadvantages**: Shorter range due to higher frequency and susceptibility to obstacles.

**802.11b**:

Uses the 2.4 GHz band, offering speeds up to 11 Mbps.

* **Advantages**: Longer range and better penetration through walls.
* **Disadvantages**: Lower speeds and higher susceptibility to interference from devices like microwaves.

**802.11g**:

Combines the 2.4 GHz band of 802.11b with speeds of up to 54 Mbps.

* **Advantages**: Balances range and speed, backward compatible with 802.11b.
* **Disadvantages**: Faces similar interference issues as 802.11b.

**802.11n**:

Introduces MIMO (Multiple Input, Multiple Output) technology.

Operates in both 2.4 GHz and 5 GHz bands, with speeds up to 600 Mbps.

* **Advantages**: Improved range, speed, and simultaneous data streams for multiple devices.
* **Disadvantages**: Higher cost and complexity.

**802.11ac**:

Operates exclusively in the 5 GHz band, offering multi-gigabit speeds.

* **Advantages**: Enhanced efficiency, less interference, and better performance in crowded environments.
* **Disadvantages**: Shorter range compared to 2.4 GHz standards.

**802.11ax (Wi-Fi 6)**:

Supports both 2.4 GHz and 5 GHz bands, delivering multi-gigabit speeds.

* **Advantages**: Superior capacity, efficiency in dense environments, and better energy management for devices.
* **Disadvantages**: Requires advanced and expensive hardware.

**Tradeoffs:**

* **Speed**: Newer standards (e.g., 802.11ax) offer significantly higher data rates, making them suitable for bandwidth-intensive applications.
* **Range**: Lower frequency bands (e.g., 2.4 GHz in 802.11b) provide longer range but lower speeds. Higher frequencies (e.g., 5 GHz in 802.11ac) offer faster speeds but shorter ranges.
* **Interference**: Standards operating in the 2.4 GHz band are more prone to interference from common household devices, while 5 GHz standards face less interference but struggle with obstacles.
* **Complexity and Cost**: Newer standards demand more sophisticated hardware, increasing costs but delivering superior performance and scalability.

**▎2. Signal Encoding Techniques and Tradeoffs**

Signal encoding techniques convert data into signals suitable for wireless transmission. Common techniques include:

**Amplitude Shift Keying (ASK):**

Represents data by varying the amplitude of the carrier signal.

* **Advantages**: Simple to implement and requires minimal bandwidth.
* **Disadvantages**: Highly susceptible to noise, leading to poor reliability in noisy environments.

**Frequency Shift Keying (FSK):**

Encodes data by varying the frequency of the carrier signal.

* **Advantages**: More robust against noise compared to ASK.
* **Disadvantages**: Less bandwidth-efficient, limiting achievable data rates.

**Phase Shift Keying (PSK):**

Changes the phase of the carrier signal to represent data

* **Advantages**: Offers better noise immunity than ASK and FSK, making it suitable for reliable communication.
* **Disadvantages**: More complex to implement, requiring precise phase synchronization.

**Quadrature Amplitude Modulation (QAM):**

Combines amplitude and phase changes to encode data.

* **Advantages**: High data transmission efficiency, supporting high-speed communication.
* **Disadvantages**: Sensitive to noise and requires a high signal-to-noise ratio for reliable operation.

**▎3. CDMA vs. TDMA**

**CDMA (Code Division Multiple Access):**

Allows multiple users to share the same frequency band by assigning unique codes to each user.

* **How It Works**: Each user is assigned a unique code, and their data is spread across the entire bandwidth using this code.
* **Advantages**: Higher capacity, excellent interference resistance, and efficient spectrum utilization. All users transmit simultaneously, increasing overall system throughput.
* **Disadvantages**: Complex implementation due to the need for precise synchronization and code generation. Interference can occur if codes are not perfectly orthogonal.

**TDMA (Time Division Multiple Access):**

Divides the channel into time slots, allowing each user to transmit in a designated slo

* **How It Works**: Each user transmits in a specific time slot, avoiding overlap with others.
* **Advantages**: Simpler implementation and reduced computational requirements compared to CDMA. Bandwidth utilization is straightforward in systems with regular activity.
* **Disadvantages**: Lower capacity as users cannot transmit simultaneously. Inefficient in scenarios where users are idle, leading to bandwidth wastage.

**Tradeoffs:**

* CDMA offers better spectrum efficiency and higher capacity but requires complex management and synchronization.
* TDMA is simpler but can be inefficient in handling variable user activity and bandwidth usage.

**▎4. Spread Spectrum**

****Definition****  
Spread Spectrum is a wireless communication technique that spreads a signal over a broader bandwidth than is necessary for transmission. This method enhances the system's resistance to interference and improves security, making it a preferred choice in various applications.

### How It Works

The core principle of Spread Spectrum is to distribute the signal across a wide frequency band. This dispersion makes the transmitted signal appear as low-power noise to unintended receivers, reducing the likelihood of interception and interference.

### Types of Spread Spectrum

There are two primary types of Spread Spectrum techniques:

****Direct Sequence Spread Spectrum (DSSS)****

In DSSS, each bit of data is represented by multiple bits through the use of a specific spreading code. This effectively disperses the signal energy across a wider bandwidth.

For example, a single bit may be encoded into an 11-bit sequence, meaning that for every bit of actual data, 11 bits are transmitted. This spreading increases the robustness of the communication against interference.

****Frequency Hopping Spread Spectrum (FHSS)****

In FHSS, the signal rapidly hops between different frequency channels during transmission, making it difficult for eavesdroppers to lock onto a specific frequency.This technique is often used in Bluetooth technology, where devices switch frequencies rapidly to maintain a secure connection.

### Advantages of Spread Spectrum

* ****Interference Resistance****: By spreading the signal over a wide frequency range, the system can better withstand interference from other signals, ensuring clearer communication even in noisy environments.
* ****Security****: The dispersion of the signal makes it more challenging for unauthorized receivers to decode the transmitted information, thereby enhancing security.
* ****Robustness****: Spread Spectrum techniques can maintain communication quality even when the signal experiences fading or multipath propagation, which is common in wireless environments.

**▎5. Applications of Wireless LANs**

### **1. Office Networks**

Wireless LANs in office environments significantly enhance operational efficiency and flexibility. By facilitating wireless connectivity, employees can work from different locations within the office without being tethered to a desk. Key benefits include:

* ****Mobility****: Employees can easily move around for collaboration, meetings, or simply to find a more comfortable workspace.
* ****Cost Efficiency****: Reduces costs associated with wiring and maintenance of physical network infrastructure.
* ****Scalability****: New devices can be added to the network easily without the need for extensive wiring or setup.
* ****Enhanced Collaboration****: Tools like video conferencing and screen sharing can be utilized more effectively in a wireless environment, promoting teamwork.

### **2. Educational Institutions**

Wireless LANs play a crucial role in modern educational settings, providing students and staff with reliable internet access throughout the campus. This includes:

* ****Learning Flexibility****: Students can access online resources, engage in virtual learning environments, and conduct research from anywhere on campus.
* ****Smart Classrooms****: Interactive technologies in classrooms can utilize wireless connections for presentations, group work, and access to online materials.
* ****Faculty Collaboration****: Teachers and staff can easily share information and resources, improving inter-departmental communication.
* ****Guest Access****: Schools can provide limited guest access for parents and visitors, enhancing the community engagement component.

### **3. Public Hotspots**

Public hotspots are ubiquitous in urban areas, providing vital internet access in various locations including cafes, airports, libraries, and hotels. They offer:

* ****Accessibility****: Users can connect their devices and access the internet while on the go, essential for business travelers or students.
* ****Community Connection****: Public hotspots can foster community engagement and local business support by providing a free service that encourages customer loyalty.
* ****Data Collection****: Businesses can gather anonymous usage data to understand customer behavior and preferences better.

### **4. Home Networks**

Wireless LANs are integral to modern home networks, enabling seamless connectivity for an array of devices. This includes:

* ****Device Interconnectivity****: Homes can connect multiple devices like laptops, smartphones, tablets, smart TVs, and smart home devices (such as security cameras and IoT devices) without cumbersome wiring.
* ****Online Entertainment****: Streaming services and online gaming are more accessible and enjoyable thanks to high-speed wireless networks.
* ****Remote Work and Learning****: Ensures a solid internet connection for remote work, video conferencing, and online classes.
* ****Network Security****: Homeowners can implement security measures to protect their networks, such as firewalls and password protection.

### **5. Industrial Automation**

In industrial settings, Wireless LANs enable communication between machines, devices, and systems, enhancing automation and efficiency. Their applications include:

* ****Real-Time Monitoring****: Wireless connectivity allows for real-time data collection and monitoring of machinery, ensuring early detection of issues and maintenance needs.
* ****IoT Integration****: Facilitates the integration of Internet of Things (IoT) devices which can optimize operations through automated processes and data analytics.
* ****Flexibility in Layout****: Manufacturing facilities can adapt quickly to changing production lines or equipment layouts as wireless networking reduces the need for fixed infrastructure.
* ****Enhanced Safety****: Wireless systems can enable safe communication between operators and machines, improving overall safety in hazardous environments.

**▎6. Main Requirements of Wireless LANs**

### The effectiveness of a Wireless LAN depends heavily on these five key factors: high data rates, expansive coverage areas, scalability, robust security measures, and reliability. Each element plays a critical role in delivering an efficient and user-friendly wireless networking experience, allowing users to rely on wireless connectivity for a variety of applications and services.

### **1. High Data Rate**

****Importance****: A high data rate is essential for enabling bandwidth-intensive applications, such as:

* ****Video Streaming****: As video content becomes the norm for entertainment, education, and conferencing, wireless networks need to support high-resolution video streaming (e.g., 4K, 8K) without buffering or interruptions.
* ****Online Gaming****: Low latency and high-speed connectivity are crucial for a smooth gaming experience, particularly for multiplayer games where real-time interactions matter.
* ****File Transfers and Cloud Services****: Quick data transfers and access to cloud applications depend on the ability to transmit large amounts of data rapidly.

### **2. Coverage Area**

****Importance****: Providing adequate coverage is vital in ensuring that users can access the wireless network without encountering dead spots. Key considerations include:

* ****Range****: The network should extend enough to cover the entire intended area, such as homes, offices, or campuses, ensuring all users can connect seamlessly.
* ****Signal Strength****: Strong signal strength maximizes user experience by reducing lag and maintaining stable connections.
* ****Infrastructure Design****: The placement of access points is crucial for optimizing coverage, minimizing physical obstructions, and enhancing overall connectivity.

### **3. Scalability**

****Importance****: As organizations grow, their networking needs evolve. Scalability is important for:

* ****Supporting Numerous Devices****: Wireless LANs must handle an increasing number of devices, from smartphones and laptops to IoT devices, without performance degradation.
* ****Ease of Expansion****: The network should allow for the addition of new access points and enhanced features as requirements change. This helps accommodate growth in users or operational scope.
* ****Future-Proofing****: A scalable network design ensures that the infrastructure can adapt to future technologies and increased data demands.

### **4. Security**

****Importance****: Security is paramount for protecting sensitive data and maintaining user trust. Key security features include:

* ****Encryption****: Utilizing robust encryption protocols like WPA3 to protect data transmitted over the network from eavesdropping and unauthorized access.
* ****Authentication****: Implementing strong authentication mechanisms ensures that only authorized devices and users can access the network.
* ****Network Segmentation****: Creating separate networks for guests and employees can enhance security by limiting access to sensitive information or critical systems.
* ****Regular Updates****: Ensuring that firmware and security protocols are regularly updated protects against emerging threats.

### **5. Reliability**

****Importance****: Reliability ensures a consistent and dependable user experience, even under varying conditions. Critical aspects include:

* ****Consistent Performance****: The network should maintain performance levels regardless of the number of connected devices or user activity levels.
* ****Interference Management****: Effective strategies should be in place to minimize interference from physical obstructions or competing wireless signals, such as the use of dual-band or tri-band routers.
* ****Quality of Service (QoS)****: Implementing QoS policies can prioritize traffic for more critical applications, ensuring that essential services remain operational even during high demand.

**▎7. Advantages and Disadvantages of Infrared WLANs**

### **Advantages**

#### **1. Security**

* ****Natural Barrier****: Since infrared signals do not penetrate solid objects like walls, the physical structure of a building provides a natural security barrier. This characteristic helps to confine the signal within a specific area, reducing the risk of unauthorized interception from outside.
* ****Reduced Eavesdropping Risks****: Because infrared communication is localized and directional, it is less susceptible to eavesdropping, making it suitable for sensitive applications requiring secure data transmission.

#### **2. No Radio Frequency Interference**

* ****Minimized Interference****: Infrared technology operates in the infrared spectrum, which is distinct from the radio frequency spectrum used by most wireless devices. This separation makes infrared systems less susceptible to interference from other wireless communications, such as Wi-Fi or Bluetooth.
* ****Stable Communication****: The reduced likelihood of interference can lead to more stable and reliable connections in environments where multiple wireless devices operate simultaneously.

### **Disadvantages**

#### **1. Line of Sight Requirement**

* ****Direct Path Necessity****: Infrared communication requires a direct line of sight between the transmitter and receiver. This limitation restricts mobility and the placement of devices, as any obstruction (e.g., walls, furniture, or even people) can disrupt the communication.
* ****Limited Deployment Flexibility****: Users may need to reposition their devices frequently to maintain connectivity, hampering the fluidity often required in dynamic environments like offices or homes.

#### **2. Limited Range**

* ****Short Distance****: Infrared signals typically have a shorter range compared to radio frequency technologies, making them suitable for specific applications but less effective for broader area coverage.
* ****Effectiveness in Smaller Areas****: This limitation means that infrared is more effectively deployed in confined spaces, such as remote controls or point-to-point communications within the same room, rather than in larger environments where comprehensive coverage is needed.

**▎8. More Common WLAN Technology**

802.11ac (Wi-Fi 5) has become the most widely used WLAN technology due to its superior data rates, efficiency, and ability to perform well in crowded environments. Its advancements over 802.11n make it a preferred choice for modern applications, from home networks to enterprise environments. As technology continues to evolve, 802.11ac lays the groundwork for future standards like 802.11ax (Wi-Fi 6), which offers even greater improvements in speed, capacity, and performance.

### **Overview of 802.11ac**

802.11ac, also known as Wi-Fi 5, is a wireless networking standard developed by the IEEE (Institute of Electrical and Electronics Engineers) as an improvement over its predecessor, 802.11n. It is designed to operate in the 5 GHz frequency band, which offers several advantages in terms of speed and performance.

### **Key Features**

****High Data Rates****:

* ****Speed****: 802.11ac supports data rates of up to 3.5 Gbps under optimal conditions, significantly higher than the maximum of 600 Mbps offered by 802.11n.
* ****Multi-User MIMO****: This technology allows multiple devices to communicate with the access point simultaneously, improving overall network efficiency and throughput.

****Channel Width****:

* ****Wider Channels****: 802.11ac supports channel widths of up to 160 MHz, compared to 40 MHz in 802.11n. This increase allows for more data to be transmitted at once, leading to faster speeds.

****Improved Modulation****:

* ****256-QAM (Quadrature Amplitude Modulation)****: This advanced modulation technique increases the amount of data transmitted in each signal, enhancing the efficiency of data transfer.

****Beamforming****:

* ****Directional Signal Transmission****: Beamforming technology helps focus the Wi-Fi signal directly toward connected devices rather than broadcasting it in all directions. This results in better range and reliability, especially in environments with obstacles.

****Backward Compatibility****:

* ****Support for Older Standards****: 802.11ac is backward compatible with 802.11n and earlier standards, allowing devices using these older technologies to connect to 802.11ac networks.

### **Advantages of 802.11ac**

* ****Enhanced Performance in Crowded Environments****: 802.11ac is designed to perform better in environments with many connected devices, such as offices, schools, and public areas, thanks to its advanced technologies like MU-MIMO and beamforming.
* ****Increased Capacity****: The ability to handle more devices simultaneously makes it ideal for high-density environments where multiple users are streaming video, gaming, or using bandwidth-intensive applications.
* ****Better Range and Coverage****: The use of the 5 GHz band, along with beamforming, helps extend the effective range of the network and improves connectivity in areas that may have been challenging with previous standards.

**▎9. MANET (Mobile Ad Hoc Network)**

### **Overview of Mobile Ad Hoc Networks (MANET)**

A ****Mobile Ad Hoc Network (MANET)**** is a type of wireless network that can be quickly set up without the need for fixed infrastructure such as routers or access points. Devices in a MANET (often referred to as nodes) can move freely and communicate directly with each other. The network is self-organizing, meaning that nodes can dynamically join or leave the network without centralized management. This capability is particularly useful in scenarios where rapid and flexible communication is essential.

### **Key Characteristics of MANETs**

* ****Self-Configuration****: Nodes can automatically configure themselves to establish a new network without any manual intervention.
* ****Dynamic Topology****: The topology of the network changes frequently as nodes move, which can lead to frequent changes in the connectivity between nodes.
* ****Wireless Communication****: All nodes communicate wirelessly, typically using protocols designed for mobile scenarios.
* ****Decentralization****: There is no fixed infrastructure or central control; each node acts as both a host and a router.
* ****Variable Bandwidth and Delay****: The available bandwidth can be variable and communication delays may occur due to the mobile nature of the nodes.

### **Applications of MANETs**

#### **Example 1: Disaster Relief Operations**

During a disaster such as an earthquake, flood, or hurricane, existing communication infrastructures (like cell towers and telephone lines) may be damaged or overloaded. In such cases, a ****MANET**** can be invaluable for coordinating rescue and relief efforts:

* ****Communication****: Rescue teams can set up a MANET to facilitate real-time communication between different units (e.g., medical, search and rescue, logistics).
* ****Adaptability****: As teams move within the disaster zone, the network can adapt to changing locations, ensuring that all teams stay connected, regardless of the destruction of traditional infrastructure.
* ****Real-Time Updates****: Teams can share critical information, resources, and locations of trapped individuals or hazardous areas, improving response efficiency.

#### **Example 2: Military Communications**

In military operations, soldiers often operate in remote or hostile environments where traditional communication networks may be compromised or unavailable. A ****MANET**** can support effective communication in such scenarios:

* ****Tactical Communication****: Soldiers equipped with handheld devices can communicate with their unit in real-time to coordinate movements, share intelligence, and report back on conditions.
* ****Mobility****: As soldiers move throughout the operation area, the MANET dynamically reconfigures, allowing continuous communication without reliance on fixed base stations.
* ****Robustness****: The resilience of MANETs to changes in node availability (such as movement, battery failure, or environmental factors) enhances operational effectiveness.

### **Benefits of MANETs**

* ****Rapid Deployment****: MANETs can be set up quickly since they do not require physical infrastructure.
* ****Flexibility****: They can easily accommodate an increasing number of nodes as more devices are added to the network.
* ****Cost-Effectiveness****: They eliminate the need for expensive infrastructure, making them a cost-effective option for temporary networking solutions.

### **Challenges of MANETs**

While MANETs offer significant advantages, they also face challenges such as:

* ****Routing Complexity****: The dynamic nature of the network makes routing decisions more complex and challenging.
* ****Security****: Because of the open nature of wireless communications, MANETs are vulnerable to various security threats, including eavesdropping and unauthorized access.
* ****Limited Resources****: Nodes often rely on battery power, making energy efficiency a critical concern for prolonged operation.

**▎10. Main Layers of 802.11 WLANs**

The ****802.11 WLAN architecture**** is structured in layers that work together to facilitate reliable and efficient wireless communication. Each layer has its distinct roles and responsibilities, ensuring that data can be transmitted, received, and processed effectively in a wireless environment. Understanding these layers is essential for comprehending how WLANs operate and how they handle the complexities of wireless communications.

### **1. Physical Layer**

* ****Function****: The Physical Layer is responsible for the transmission of raw bitstreams over the physical medium, including the modulation and demodulation of signals.

****Components****: This layer includes specifications for wireless transmission techniques, such as:

* ****Frequency Bands****: Defines the frequencies used for communication (e.g., 2.4 GHz and 5 GHz).
* ****Modulation Schemes****: Specifies how data is modulated onto the radio waves (e.g., OFDM for 802.11ac).
* ****Signal Strength****: Manages how strong the signals need to be for reliable transmission.
* ****Data Rates****: Determines the possible data rates based on channel width and modulation methods.

### **2. Data Link Layer**

The Data Link Layer is divided into two sublayers:

#### **a) MAC (Medium Access Control) Sublayer**

* ****Function****: The MAC sublayer manages access to the wireless medium, ensuring that multiple devices can communicate without conflicts over the same channel.

****Key Responsibilities****:

* ****Frame Control****: Controls the encapsulation of packets into frames for transmission.
* ****Addressing****: Assigns MAC addresses to devices, ensuring that frames are delivered to the correct destination.
* ****Access Methods****: Implements protocols such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), allowing devices to sense the medium before transmitting to minimize collisions.
* ****Error Handling****: Detects errors in transmission through checksums.

#### **b) LLC (Logical Link Control) Sublayer**

* ****Function****: The LLC sublayer provides a standardized method for managing communication between devices.

****Key Responsibilities****:

* ****Framing****: Defines the protocol for framing, addressing, and encapsulating data packets from higher layers for transmission.
* ****Flow Control****: Facilitates the management of data flow to prevent overflow or loss during transmission.
* ****Logical Addressing****: Provides a means for logical addressing that is independent of the MAC addressing.

### **3. Network Layer**

* ****Function****: While not explicitly defined by the 802.11 standard, the Network Layer is typically concerned with routing packets between different networks and ensuring that data can reach its final destination.
* ****Protocols****: Often involves the Internet Protocol (IP), which facilitates packet forwarding and routing within and beyond the local network. The interaction between the Network Layer and the Data Link Layer allows devices to function on larger networks.

### **4. MAC Layer (Medium Access Control)**

* ****Note****: The MAC layer is actually considered part of the Data Link Layer, specifically the MAC sublayer mentioned above. However, it’s crucial to highlight it as a distinct area due to its importance in WLANs.
* ****Reinforcement of Responsibilities****: It is essential to note that the MAC layer includes several important functionalities already mentioned, such as:
* ****Access Control****: Managing how devices access the shared wireless medium.
* ****Frame Handling****: Ensuring the correct creation and transmission of frames to/from the physical layer.

### **Summary of Layer Interactions**

* ****Interaction****: These layers work together to ensure effective communication in a WLAN:
* Data from the higher layers (like Transport and Application) is framed and passed to the MAC layer for addressing and control.
* The MAC sublayer prepares these frames for transmission through the Physical Layer, where they are converted into electromagnetic signals for wireless transmission.
* Incoming signals are received by the Physical Layer, converted back into digital data, and processed by the MAC and LLC sublayers before being handed off to higher layers.

**▎11. 802.11 Services**

### **1. Authentication**

* ****Purpose****: Authentication is the process of validating users and devices before they are allowed to access the network.
* ****Types****:
* ****Open Authentication****: Provides unrestricted access but does not verify the identity of the user.
* ****Shared Key Authentication****: Uses a shared secret key for validation.
* ****EAP (Extensible Authentication Protocol)****: Supports various authentication methods like WPA2-Enterprise, using protocols such as PEAP (Protected EAP) or EAP-TLS (Transport Layer Security).
* ****Importance****: Proper authentication processes safeguard the network against unauthorized access.

### **2. Association**

* ****Purpose****: The association process establishes a connection between a client device and an access point (AP).
* ****Process****:
* ****Request/Response****: The client sends an association request to the AP, which responds with an association response.
* ****Role****: This step involves the exchange of necessary information like the client’s capabilities and roaming parameters, allowing the device to communicate over the network.

### **3. Reassociation**

* ****Purpose****: Reassociation allows a client to switch from one access point to another while maintaining an active connection to the network.
* ****Process****: When a client moves out of the range of its current AP but remains connected to the same network, it can send a reassociation request to a new AP. If successful, this process helps maintain an uninterrupted network experience.
* ****Importance****: This capability is crucial in mobile computing scenarios, ensuring seamless connectivity for users on the move.

### **4. Disassociation**

* ****Purpose****: Disassociation is the process of terminating the connection between a client and an access point.
* ****Process****: Either the client or the AP can initiate disassociation. The device sends a disassociation request, and the receiving end confirms the termination of the connection.
* ****Importance****: It helps free up resources on the AP, particularly when a user is leaving the network area or switching to a different network.

### **5. Data Delivery Services**

* ****Purpose****: This function ensures the reliable transmission of data frames between devices within the WLAN.
* ****Responsibilities****:
* ****Frame Delivery****: Guarantees that data frames are delivered to the appropriate destination.
* ****Error Detection and Retransmission****: Implements error-checking mechanisms (like checksums) and strategies for retransmitting lost or corrupted frames.
* ****Importance****: Reliable data delivery is fundamental to effective communication, particularly in applications that require high data integrity, such as video streaming and file transfers.

### **6. Privacy**

* ****Purpose****: Privacy ensures the confidentiality of data transmitted over the wireless network through encryption.
* ****Methods****:
* ****WEP (Wired Equivalent Privacy)****: The original encryption method, now considered insecure due to vulnerabilities.
* ****WPA (Wi-Fi Protected Access) & WPA2****: Improved encryption standards that use techniques such as TKIP (Temporal Key Integrity Protocol) for WPA and AES (Advanced Encryption Standard) for WPA2, providing stronger security for data transmission.
* ****Importance****: Protecting data from eavesdropping and unauthorized access is critical in today’s wireless networks, especially for sensitive information.