**WIFI – TRAINING PROGRAM**

**MODULE – 1**

**1.In which OSI layer the Wi-Fi standard/protocol fits?**

The Wi-Fi standard (IEEE 802.11) primarily fits into the **Data Link Layer (Layer 2)** of the OSI model, but it also has components in the **Physical Layer (Layer 1)**.

1. Physical Layer (Layer 1):

**Radio Frequencies:** Wi-Fi operates using radio waves to transmit data wirelessly. The physical layer defines the characteristics of these radio signals, including the frequency bands (e.g., 2.4 GHz, 5 GHz, 6 GHz), modulation techniques (how digital data is encoded onto the radio waves), and transmission power levels.

**Preamble and PHY Header:** At the Physical Layer Convergence Procedure (PLCP) sublayer, a preamble and PHY (Physical Layer) header are added to the PSDU (PLCP Service Data Unit) to create the PPDU (PLCP Protocol Data Unit). The preamble is used for synchronization between the sender and receiver, and the PHY header contains information about the physical layer encoding and transmission parameters.

**Data Transmission as Bits:** The physical layer is responsible for the actual transmission and reception of raw data as a stream of bits over the wireless medium.

**Physical Medium Dependent (PMD):** This sublayer within the Physical Layer specifies the modulation and coding techniques used for transmitting and receiving data over the wireless medium.

**Channel Access:** The physical layer is involved in the initial stages of channel access, such as Clear Channel Assessment (CCA) to determine if the wireless medium is free before transmission.

2. Data Link Layer (Layer 2):

The Data Link Layer in the IEEE 802.11 standard is further divided into two sublayers:

**Media Access Control (MAC) sublayer:**

**MAC Addressing:** This sublayer is responsible for hardware addressing using MAC addresses to identify devices within the same network segment (the wireless LAN).

**Frame Formatting:** The MAC sublayer takes the MSDU (MAC Service Data Unit) from the Logical Link Control (LLC) sublayer and adds a MAC header and trailer to create the MPDU (MAC Protocol Data Unit) or MAC frame, as shown in the image. These headers and trailers contain control information, addressing (source and destination MAC addresses), and error detection mechanisms (like CRC - Cyclic Redundancy Check).

**Channel Access Control:** The MAC sublayer implements the rules for how devices share the wireless medium. Wi-Fi uses a contention-based protocol called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) with mechanisms like DCF (Distributed Coordination Function) and PCF (Point Coordination Function) to manage access and avoid collisions.

**Security Mechanisms:** Protocols like WEP (Wired Equivalent Privacy) and WPA/WPA2/WPA3 (Wi-Fi Protected Access) operate at the MAC sublayer to provide data encryption and authentication.

**Frame Validation and Error Detection:** The MAC layer checks the integrity of received frames using the CRC in the trailer. Corrupted frames are typically discarded.

**Logical Link Control (LLC) sublayer:**

**Interface to Network Layer:** The LLC sublayer provides an interface between the MAC sublayer and the Network Layer (Layer 3). It takes the network layer packets (MSDU in the context of the image, representing Layers 3-7 data) and encapsulates them into MAC frames (MPDU).

**Reliable Link:** While the MAC layer handles error detection, the LLC layer can provide flow and error control mechanisms to ensure reliable data transfer, although these are not always utilized in basic Wi-Fi operation, as reliability is often handled by higher-layer protocols (like TCP in the Transport Layer).

1. **Can you share the Wi-Fi devices that you are using day to day life, share that device’s wireless capability/properties after connecting to network. Match your device to corresponding Wi-Fi Generation based on properties?**

1. Mobile Hotspot (Wi-Fi shared from a smartphone):

* Wireless Capabilities/Properties :
  + Wi-Fi Standard: Could be 802.11 a/b/g/n/ac/ax (Wi-Fi 1 to Wi-Fi 6 or even Wi-Fi 6E).
  + Frequency Bands: Likely supports 2.4 GHz and 5 GHz. Some newer phones might support 6 GHz (Wi-Fi 6E).
  + Channel Width: Can vary (e.g., 20 MHz, 40 MHz, 80 MHz, 160 MHz). Wider channels generally mean higher potential speeds.
  + Security Protocols: Typically supports WPA2-PSK and WPA3-SAE.
  + Maximum Theoretical Speed: This depends on the Wi-Fi standard and channel width supported by the phone.
  + Number of Spatial Streams: Modern phones often support multiple spatial streams (MIMO) for improved performance.
* Matching to Wi-Fi Generation:
  + 802.11b: Wi-Fi 1 (Max theoretical speed: 11 Mbps, Frequency: 2.4 GHz)
  + 802.11g: Wi-Fi 3 (Max theoretical speed: 54 Mbps, Frequency: 2.4 GHz)
  + 802.11n: Wi-Fi 4 (Max theoretical speed: up to 600 Mbps, Frequencies: 2.4 GHz and/or 5 GHz)
  + 802.11ac: Wi-Fi 5 (Max theoretical speed: up to 3.5 Gbps, Frequency: 5 GHz)
  + 802.11ax: Wi-Fi 6 (Max theoretical speed: up to 9.6 Gbps, Frequencies: 2.4 GHz and 5 GHz)
  + 802.11ax (with 6 GHz band): Wi-Fi 6E (Extends Wi-Fi 6 to the 6 GHz band)

SSID: Redmi A3

Protocol: Wi-Fi 4 (802.11n)

Security type: WPA3-Personal

Manufacturer: Intel Corporation

Description: Intel(R) Wireless-AC 9461

Driver version: 22.220.0.4

Network band: 2.4 GHz

Network channel: 1

Link speed (Receive/Transmit): 65/72 (Mbps)

**2. College Common Wi-Fi (Access Point/Infrastructure):**

* **Wireless Capabilities/Properties (highly variable depending on the college's infrastructure):**
  + **Wi-Fi Standard:** Could range from older standards like 802.11n to more modern ones like 802.11ac or even 802.11ax. Enterprise environments often upgrade their infrastructure.
  + **Frequency Bands:** Likely supports both 2.4 GHz and 5 GHz.
  + **Channel Width:** Configured by the network administrators.
  + **Security Protocols:** Typically uses more robust enterprise-level security like WPA2-Enterprise or WPA3-Enterprise, often with RADIUS authentication.
  + **Maximum Theoretical Speed:** Depends on the access points and the overall network design. It's usually high to accommodate many users.
  + **MIMO Support:** Enterprise-grade access points almost always support MIMO for better performance and handling multiple concurrent users.
* **Matching to Wi-Fi Generation:** Similar to the mobile hotspot, the Wi-Fi standard supported by the college's access points determines the generation (Wi-Fi 4, Wi-Fi 5, Wi-Fi 6, etc.).

**2. College Common Wi-Fi (Access Point/Infrastructure):**

* **Wireless Capabilities/Properties (highly variable depending on the college's infrastructure):**
  + **Wi-Fi Standard:** Could range from older standards like 802.11n to more modern ones like 802.11ac or even 802.11ax. Enterprise environments often upgrade their infrastructure.
  + **Frequency Bands:** Likely supports both 2.4 GHz and 5 GHz.
  + **Channel Width:** Configured by the network administrators.
  + **Security Protocols:** Typically uses more robust enterprise-level security like WPA2-Enterprise or WPA3-Enterprise, often with RADIUS authentication.
  + **Maximum Theoretical Speed:** Depends on the access points and the overall network design. It's usually high to accommodate many users.
  + **MIMO Support:** Enterprise-grade access points almost always support MIMO for better performance and handling multiple concurrent users.
* **Matching to Wi-Fi Generation:** Similar to the mobile hotspot, the Wi-Fi standard supported by the college's access points determines the generation (Wi-Fi 4, Wi-Fi 5, Wi-Fi 6, etc.).

**3. Wi-Fi Modem (Router with integrated modem):**

* **Wireless Capabilities/Properties (depends on the specific model):**
  + **Wi-Fi Standard:** Can range from older 802.11n to the latest 802.11ax (Wi-Fi 6) or even Wi-Fi 6E.
  + **Frequency Bands:** Most modern modems support dual-band (2.4 GHz and 5 GHz). Tri-band modems also exist, adding another 5 GHz band or a 6 GHz band.
  + **Channel Width:** Configurable within the router settings.
  + **Security Protocols:** Typically supports WPA2-PSK and WPA3-SAE.
  + **MIMO Support:** Modern routers heavily utilize MIMO.

1. **What is BSS and ESS ?**

**Basic Service Set (BSS)**

* Definition: A BSS is the fundamental building block of a Wi-Fi network. It consists of a group of wireless stations (devices like laptops, smartphones, tablets) that communicate with each other under the control of a single Access Point (AP).
* Infrastructure Mode: BSS is primarily associated with infrastructure mode, where all communication between wireless stations goes through the central AP. The AP acts as a bridge between the wireless network and a wired network (like Ethernet) or the internet.
* BSSID (Basic Service Set Identifier): Each BSS is uniquely identified by a 48-bit MAC address of the Access Point's wireless interface. This is known as the BSSID. When a wireless station scans for available networks, it sees a list of BSSIDs.
* Analogy: Think of a small office or a home network with a single Wi-Fi router. All your wireless devices connect to this router to communicate with each other and the outside world. This setup forms a single BSS.
* Key Characteristics:
  + Single Access Point.
  + All communication goes through the AP.
  + Identified by a unique BSSID (MAC address of the AP's wireless interface).
  + Provides basic wireless connectivity within a limited area (the coverage area of the AP).

**Extended Service Set (ESS)**

* Definition: An ESS is formed by two or more BSSs that are interconnected by a Distribution System (DS). The DS is typically a wired network (like Ethernet) but can also be another wireless medium.
* Purpose: The primary goal of an ESS is to extend the wireless network coverage area, allowing wireless users to roam seamlessly between different BSSs without losing their network connection.
* ESSID (Extended Service Set Identifier): All the Access Points within the same ESS are configured with the same Service Set Identifier (SSID), which is the human-readable name of the Wi-Fi network (e.g., "MyHomeWiFi," "CollegeNetwork"). This common SSID is what users see and connect to.
* Analogy: Imagine a larger office building or a university campus with multiple Wi-Fi access points strategically placed to provide coverage throughout the area. These APs are connected via a wired network and are all configured with the same network name (SSID). When you move from one part of the building to another, your device automatically connects to the AP with the strongest signal within the same ESS, providing continuous connectivity.
* Key Characteristics:
  + Multiple Access Points.
  + Access Points are interconnected by a Distribution System (usually wired).
  + All Access Points share the same SSID (network name).
  + Provides extended wireless coverage and seamless roaming for users.
  + Each BSS within the ESS still has its own unique BSSID.

1. **What are the basic functionalities of Wi-Fi Accesspoint ?**

A Wi-Fi Access Point (AP) is a crucial component in a wireless local area network (WLAN). Its basic functionalities revolve around enabling wireless devices to connect to a network and communicate with each other and the wired network (if present).

1. Wireless Signal Transmission and Reception:
   * The primary function of an AP is to transmit and receive radio waves that carry network data. It acts as a central hub for wireless communication within its coverage area.
   * It uses specific Wi-Fi standards (like 802.11n, ac, ax) and frequencies (2.4 GHz, 5 GHz) to establish wireless connections with client devices.
2. Bridging Wireless and Wired Networks:
   * Most APs have a wired Ethernet port that connects them to the existing wired network infrastructure (e.g., a router, switch, or modem).
   * The AP acts as a bridge, translating data between the wireless and wired mediums. This allows wireless devices to access resources on the wired network, including the internet.
3. Service Set Identification (SSID) Broadcasting:
   * The AP broadcasts a Service Set Identifier (SSID), which is the name of the Wi-Fi network (e.g., "HomeWiFi," "OfficeNetwork").
   * This broadcast allows nearby wireless devices to discover the available Wi-Fi networks and choose which one to connect to.
4. Association and Authentication of Wireless Clients:
   * When a wireless device attempts to connect to the network, the AP manages the association process. This involves the client device identifying itself and negotiating the connection parameters.
   * The AP also handles authentication, verifying the identity of the connecting device. This is typically done using a pre-shared key (for WPA/WPA2/WPA3 Personal) or through an authentication server (for WPA/WPA2/WPA3 Enterprise).
5. Data Forwarding and Routing (Basic):
   * The AP forwards data packets between connected wireless clients and the wired network.
   * In simpler setups, the AP might perform very basic routing functions, but more complex routing is usually handled by a dedicated router in the network.
6. Basic Security Enforcement:
   * APs implement security protocols (like WEP, WPA, WPA2, WPA3) to encrypt wireless communication and prevent unauthorized access to the network.
   * They manage the encryption and decryption of data transmitted over the wireless link based on the configured security settings.
7. Channel Selection:
   * APs operate on specific wireless channels within the chosen frequency band (2.4 GHz or 5 GHz).
   * Many modern APs can automatically select the least congested channel to improve performance.
8. Management Interface:
   * APs typically provide a management interface (usually web-based) that allows administrators to configure various settings, including the SSID, security protocols, passwords, channel selection, and other advanced options.
9. **Difference between bridge mode and repeater mode**

Both bridge mode and repeater mode are ways to extend the reach of a Wi-Fi network, but they function in fundamentally different ways and have distinct use cases and limitations.

Bridge Mode:

* Purpose: Primarily used to connect two or more wired network segments wirelessly. It essentially makes the wireless link transparent, as if the two wired networks were directly connected by a cable.
* Functionality:
  + Acts as a Wireless Bridge: The device in bridge mode connects to an existing Wi-Fi network and then provides wired Ethernet ports for connecting wired devices. It doesn't typically broadcast its own separate Wi-Fi network for clients to directly connect wirelessly.
  + Transparent Layer 2 Bridging: It operates at Layer 2 (Data Link Layer) of the OSI model. It forwards MAC addresses between the connected wired segments and the main wireless network.
  + Extends Wired Connectivity: The main goal is to bring wired devices into the existing wireless network's scope without needing to run physical cables.
* Network Configuration: Usually requires configuration on both ends of the bridge link (both devices need to be set up to bridge to each other or a central AP).
* Client Connectivity: Wired clients connect to the bridge's Ethernet ports. Wireless clients connect directly to the main Wi-Fi network (the one the bridge is connected to).
* IP Addressing: Wired clients connected through the bridge typically obtain their IP addresses from the main network's DHCP server. They are part of the same IP subnet as the main network.
* SSID: Doesn't usually broadcast its own independent SSID for direct wireless client connections. It connects to an existing SSID.
* Analogy: Imagine you have a wired network in your living room and want to connect a wired device in your bedroom without running a cable. You could use two devices configured in bridge mode to create a wireless link that acts like a long Ethernet cable between the two rooms.
* Use Cases:
  + Connecting a wired gaming console or smart TV in a different room to your main router.
  + Linking two separate wired network segments in different buildings (if wireless signal is strong enough).

Repeater Mode:

* Purpose: Used to extend the coverage area of an existing Wi-Fi network wirelessly. It receives the existing Wi-Fi signal and rebroadcasts it, effectively amplifying and extending its reach.
* Functionality:
  + Wireless Extension: The device in repeater mode connects to an existing Wi-Fi network wirelessly and then creates a *new*, separate Wi-Fi network with the same or a different SSID.
  + Operates at a Lower Efficiency: Because it has to receive and then retransmit the signal, there's often a reduction in bandwidth (speed) for devices connected to the repeater. The available bandwidth is essentially halved.
  + Wireless Client Connectivity: Wireless clients connect directly to the repeater's Wi-Fi network.
* Network Configuration: Needs to be configured to connect to the existing Wi-Fi network and then set up its own rebroadcasted network.
* Client Connectivity: Wireless clients connect to the repeater's Wi-Fi network. The repeater then communicates wirelessly with the main router.
* IP Addressing: Clients connected to the repeater usually still get their IP addresses from the main router's DHCP server, so they are generally on the same IP subnet.
* SSID: Can either rebroadcast the original SSID (making it appear as one larger network) or broadcast a new, different SSID. Using the same SSID can facilitate seamless roaming (if implemented well), but can also sometimes cause confusion.
* Analogy: Imagine your Wi-Fi signal is weak in a certain part of your house. A repeater can be placed in an area with a decent signal to pick it up and then rebroadcast a stronger signal to cover the dead zone.
* Use Cases:
  + Extending Wi-Fi coverage to areas where the main router's signal is weak or doesn't reach.
  + Covering larger homes or spaces without running Ethernet cables.

1. **What are the differences between 802.11a and 802.11b ?**

|  |  |  |
| --- | --- | --- |
| **Feature** | **802.11a** | **802.11b** |
| **Release Year** | 1999 | 1999 |
| **Operating Frequency** | 5 GHz (Gigahertz) | 2.4 GHz (Gigahertz) |
| **Maximum Data Rate** | 54 Mbps (Megabits per second) | 11 Mbps (Megabits per second) |
| **Modulation Techniques** | OFDM (Orthogonal Frequency Division Multiplexing) | DSSS (Direct Sequence Spread Spectrum) and HR-DSSS (High-Rate DSSS) |
| **Channel Width** | 20 MHz | 22 MHz (though often referred to as 20 MHz) |
| **Range** | Shorter than 802.11b due to higher frequency (more susceptible to obstacles) | Longer than 802.11a at the same power level (better penetration of obstacles) |
| **Interference** | Less prone to interference from common household devices (microwaves, Bluetooth) operating at 2.4 GHz | More prone to interference from common household devices operating at 2.4 GHz |
| **Compatibility** | Not backward compatible with 802.11b | Not backward compatible with 802.11a |
| **Number of Channels** | More available channels in the 5 GHz band (varying by region) | Fewer non-overlapping channels available in the 2.4 GHz band (typically 3 in many regions) |
| **Complexity** | More complex modulation, requiring more processing power | Simpler modulation |
| **Cost (at the time)** | Generally more expensive hardware | Generally less expensive hardware |

1. **Configure your modem/hotspot to operate only in 2.4Ghz and connect your laptop/Wi-Fi device and capture the capability /properties in your Wi-Fi device. Repat the same in 5Ghz and tabulate all the differences you observed during this**

|  |  |  |
| --- | --- | --- |
| Network band | 2.4 GHz | 5 GHz |
| Link speed (Receive/Transmit): | 65/72 (Mbps) | 390/433 (Mbps) |
| Protocol | Wi-Fi 4 (802.11n) | Wi-Fi 5 (802.11ac) |
| Signal | 93% | 95% |
| Security type | WPA2-Personal | WPA2-Personal |
| Network channel | 12 | 36 |

1. **Difference between IEEE and WFA**

The IEEE (Institute of Electrical and Electronics Engineers) and the WFA (Wi-Fi Alliance) are both important organizations in the world of Wi-Fi, but they have distinct roles and functions:

|  |  |  |
| --- | --- | --- |
| **Feature** | **IEEE (Institute of Electrical and Electronics Engineers)** | **Wi-Fi Alliance (WFA)** |
| **Type of Organization** | Technical Professional Organization | Non-profit Industry Association |
| **Primary Role** | Develops technical standards (IEEE 802.11) | Certifies product interoperability; owns "Wi-Fi" brand |
| **Focus** | Defining how Wi-Fi works technically | Ensuring devices work together; promoting Wi-Fi |
| **Output** | Detailed technical specifications and protocols | Certification programs, "Wi-Fi CERTIFIED" logo, branding |
| **Certification** | Does not directly certify products | Runs the Wi-Fi CERTIFIED program |
| **Branding** | No role in "Wi-Fi" brand management | Owns and manages the "Wi-Fi" trademark and logo |
| **Membership** | Individual engineers, scientists, professionals | Companies in the Wi-Fi ecosystem |

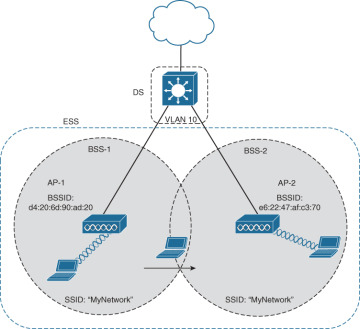
1. **List down the type of Wi-Fi connectivity backhaul, share your home/college’s wireless internet connectivity backhaul name and its properties.**

|  |  |
| --- | --- |
| **Name** | Cellular Data Network – 4G LTE |
| **SSID** | Redmi A3 |
| **Network type** | Infrastructure |
| **Radio type** | 802.11n |
| **Authentication** | WPA3-Personal |
| **Cipher** | CCMP |
| **Band** | 2.4 GHz |
| **Channel** | 11 |
| **Receive rate (Mbps)** | 65 |
| **Transmit rate (Mbps)** | 72.2 |
| **Signal** | 99% |

1. **List down the Wi-Fi topologies and use cases of each one.**

The 802.11 standard identifies two main wireless topology modes:

1. Infrastructure mode
2. Independent Basic Service Set (IBSS)/ Ad hoc mode
3. With the ubiquity of wireless networks, mesh topologies are now common.
4. **Infrastructure mode**



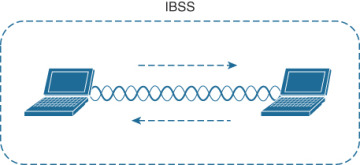
**Example of ESS Infrastructure Mode**

Wireless stations (clients like laptops, smartphones) communicate with each other and the wired network through a central Access Point (AP). The AP acts as a bridge between the wireless and wired networks. This is the most common Wi-Fi topology.

**Use Cases:**

* **Home Networks:** Connecting personal devices (computers, phones, smart home devices) to a home internet connection via a Wi-Fi router.
* **Office Networks:** Providing wireless access to company resources and the internet for employees and guests.
* **Public Wi-Fi Hotspots:** Offering internet access in cafes, airports, libraries, and other public spaces.
* **Enterprise Wireless Networks:** Large-scale deployments with multiple APs managed centrally to provide seamless roaming and extensive coverage in offices, campuses, and warehouses.
* **Retail Environments:** Connecting point-of-sale systems, inventory management devices, and providing guest Wi-Fi.
* **Industrial IoT:** Connecting sensors, controllers, and other industrial devices wirelessly, often through ruggedized access points.

1. **Ad-Hoc Mode (Peer-to-Peer)**



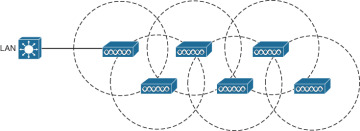
**IBSS – Ad Hoc Mode**

Two or more wireless stations communicate directly with each other without the need for a central AP. Each station acts as both a client and a limited access point. This mode is less common today**.**

**Use Cases:**

* Direct File Sharing: Quickly transferring files between two laptops without needing a router or internet connection (e.g., using features like Wi-Fi Direct, which is a more advanced form of ad-hoc).
* Temporary Connections: Setting up a temporary wireless link for a specific purpose, like multiplayer gaming between nearby computers without an internet connection.
* Wireless Printing: Some devices can connect directly to a wireless printer in an ad-hoc fashion.
* Early Wireless Sensor Networks (Less Common Now): In very basic or isolated sensor setups where a central controller might not be necessary.

1. **Mesh Topology:**



**Example of Wireless Mesh Network**

A network of wireless nodes (APs or routers) that can communicate directly with each other and forward traffic to other nodes. This creates multiple pathways for data to travel, enhancing reliability and coverage. Typically, one node is connected to the wired internet (the gateway).

**Use Cases:**

* **Whole-Home/Building Wi-Fi Coverage:** Eliminating dead spots and providing seamless roaming in larger homes or buildings where a single router's signal is insufficient.
* **Extending Network Reach in Difficult-to-Wire Areas:** Connecting outbuildings or areas where running Ethernet cables is challenging.
* **Temporary or Rapidly Deployed Networks:** Setting up wireless connectivity quickly in emergency situations or temporary events.