### Q4)Scanning Process in Wi-Fi Networks: Types and Mechanisms

Scanning is a critical **MAC-layer process** that enables Wi-Fi devices to discover available networks before connecting. There are two primary types of scanning: **Passive Scanning** and **Active Scanning**. Below is a detailed explanation of both methods, their steps, and use cases.

**1. Passive Scanning**

**Purpose**: Discover networks by listening silently without transmitting.  
**Used When**:

* Minimizing power consumption (e.g., IoT devices).
* Avoiding unnecessary network traffic.

**Steps in Passive Scanning**:

1. **Device Tunes to a Channel**:
   * The Wi-Fi adapter switches to a channel (e.g., Channel 6 in 2.4 GHz).
2. **Listens for Beacon Frames**:
   * APs broadcast **Beacon frames** periodically (typically every 100 ms).
   * Beacons contain:
     + **SSID** (Network name).
     + **BSSID** (AP’s MAC address).
     + **Supported rates** (e.g., 802.11ac, 802.11ax).
     + **Security info** (WPA2, WPA3).
3. **Records Network Info**:
   * The device compiles a **scan list** of detected APs.
4. **Repeats on All Channels**:
   * Iterates through all channels (e.g., 1–11 for 2.4 GHz, 36–165 for 5 GHz).

**Advantages**:

* Low power consumption (no transmissions).
* Stealthy (does not reveal the scanner’s presence).

**Disadvantages**:

* Slower (depends on Beacon interval).
* May miss hidden networks (if Beacons are disabled).

**2. Active Scanning**

**Purpose**: Actively probe for networks by sending requests.  
**Used When**:

* Fast network discovery is needed (e.g., smartphones, laptops).
* Hidden networks (non-broadcast SSID) must be detected.

**Steps in Active Scanning**:

1. **Device Sends Probe Request**:
   * Broadcasts a **Probe Request** frame (can include a specific SSID for hidden networks).
2. **APs Respond with Probe Response**:
   * APs matching the request reply with a **Probe Response** (similar to a Beacon but on-demand).
3. **Device Builds Scan List**:
   * Compares signal strength (RSSI), security, and capabilities of APs.
4. **Repeats Across Channels**:
   * Rapidly hops through channels to scan the entire spectrum.

**Advantages**:

* Faster than passive scanning (immediate responses).
* Can discover hidden networks (if SSID is known).

**Disadvantages**:

* Higher power consumption (device transmits).
* Increases network traffic (Probe Requests/Responses).

**3. Scanning Variations**

**A. Directed vs. Broadcast Probe Requests**

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Probe Request | Target | Use Case |
| Broadcast | SSID=null | All APs | General scan. |
| Directed | SSID="MyWiFi" | Specific AP | Hidden networks. |

**B. Background Scanning**

* Devices periodically scan while connected to:
  + **Roam seamlessly** to a better AP.
  + **Maintain network lists** for quick reconnects.

**C. Foreground Scanning**

* Triggered manually (e.g., user refreshing Wi-Fi list).

**4. Real-World Example**

1. **Smartphone Behavior**:
   * Uses **active scanning** when the user opens Wi-Fi settings.
   * Switches to **passive scanning** in sleep mode to save battery.
2. **IoT Devices**:
   * Prefer **passive scanning** to conserve energy.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scanning Type | Method | Speed | Power Use | Best For |
| Passive | Listens for Beacons | Slow | Low | Battery-sensitive devices. |
| Active | Sends Probe Requests | Fast | High | Quick discovery, hidden networks. |

1. **Passive Scanning**:
   * Silent, low-power, but slower.
   * Relies on **Beacon frames**.
2. **Active Scanning**:
   * Faster, but consumes more power.
   * Uses **Probe Request/Response**.
3. **Hybrid Approaches**:
   * Modern devices combine both methods for efficiency.