Scanning

Scanning is typically the first step a station undertakes to connect to a Wi-Fi network, whether during initial association, roaming, or network selection.The scanning process involves a station listening for or soliciting information about nearby APs to build a list of available networks. The MAC layer uses **management frames**, specifically **Beacon frames** (for passive scanning) and **Probe Request/Response frames** (for active scanning), to perform this task. The collected information helps the station decide which AP to associate with based on criteria like signal strength (RSSI), channel congestion, security, or QoS capabilities.

Key Objectives of Scanning:

1. Discover available APs and their BSSs.
2. Collect network parameters (e.g., SSID, BSSID, channel, supported rates, security protocols).
3. Identify the best AP for association or reassociation (e.g., during roaming).
4. Support mobility by enabling seamless transitions between APs in an ESS.

Steps in the Scanning Process:

1. **Initiation**: The station's MAC layer triggers scanning, either automatically (e.g., when powered on or roaming) or manually (e.g., user selects "scan for networks").
2. **Channel Selection**: The station scans specific frequency channels (e.g., 2.4 GHz, 5 GHz, or 6 GHz bands) based on regulatory domain and supported bands.
3. **Information Collection**: The station gathers AP details using passive or active scanning (detailed below).
4. **Evaluation**: The station processes collected data to select an AP based on signal strength, security, or other criteria.
5. **Association**: After selecting an AP, the station proceeds with authentication and association.

Types of Scanning

1. Passive Scanning

In **passive scanning**, the station listens for **Beacon frames** periodically broadcast by APs without transmitting any frames itself. These Beacon frames contain essential information about the AP and its BSS.

Process:

1. The station tunes its radio to a specific channel (e.g., channel 1 in the 2.4 GHz band).

2. It waits for a predefined period, typically at least one **Beacon Interval** (default is 100 TU, or 102.4 ms), to receive Beacon frames from APs on that channel.
3. The station records details from each Beacon frame, such as:
   - **SSID**: Network name.
   - **BSSID**: AP’s MAC address.
   - **Channel**: Operating channel.
   - **Supported Rates**: Data rates supported by the AP.
   - **TIM (Traffic Indication Map)**: Indicates buffered frames for power-saving stations.
   - **Security Parameters**: Encryption types (e.g., WPA2, WPA3).
   - **QoS Capabilities**: Support for IEEE 802.11e or other enhancements.
4. The station switches to the next channel and repeats the process until all relevant channels are scanned.
5. After scanning, the station evaluates the collected data to select an AP.

Advantages:

- **Power Efficient**: No transmission is required, reducing power consumption, which is ideal for battery-powered devices.
- **Stealthy**: Does not reveal the station’s presence, enhancing privacy.
- **Regulatory Compliance**: Suitable in environments where active transmissions are restricted (e.g., certain regulatory domains).

Disadvantages:

- **Slower**: Waiting for Beacon frames on each channel can take significant time, especially if the Beacon Interval is long or multiple channels are scanned.
- **Incomplete Information**: May miss APs with hidden SSIDs (suppressed in Beacon frames) or those with infrequent Beacons.
- **Channel Congestion**: In dense environments, overlapping Beacon frames may cause delays or missed detections.

Use Cases:

- Initial network discovery for power-constrained devices (e.g., IoT devices, smartphones in low-power mode).
- Environments with strict regulatory restrictions on probe transmissions.
- Scenarios where stealth is preferred to avoid detection.

2. Active Scanning

In **active scanning**, the station actively solicits information by transmitting **Probe Request frames** and listening for **Probe Response frames** from APs. This is a more proactive approach compared to passive scanning.

Process:

1. The station tunes its radio to a specific channel.
2. It broadcasts a **Probe Request frame**, which may include:
    - **SSID**: Specific SSID to query a particular network, or a wildcard SSID (empty) to discover all networks.
    - **Supported Rates**: Rates the station supports.
    - **Capabilities**: Additional features (e.g., QoS, security protocols).
3. APs on the channel that match the Probe Request criteria respond with **Probe Response frames**, which contain similar information to Beacon frames:
    - SSID, BSSID, channel, supported rates, security settings, TIM, QoS parameters, etc.
4. The station waits for a short period (e.g., **MinChannelTime** to detect responses and **MaxChannelTime** if responses are received) to collect Probe Responses.
5. The station moves to the next channel and repeats the process until all desired channels are scanned.
6. The station evaluates the collected Probe Responses to select an AP.

Advantages:

- **Faster**: Stations can quickly discover APs without waiting for Beacon intervals, as Probe Responses are sent immediately.
- **Comprehensive**: Can discover APs with hidden SSIDs (if the specific SSID is included in the Probe Request) and gather detailed network information.
- **Efficient in Dense Networks**: Reduces scanning time in environments with many APs, as stations actively solicit responses.

Disadvantages:

- **Power Intensive**: Transmitting Probe Requests consumes more power than listening passively.
- **Increased Airtime Usage**: Probe Requests and Responses add to channel congestion, especially in dense environments.
- **Privacy Concerns**: Broadcasting Probe Requests may reveal the station's presence and preferred SSIDs, potentially exposing it to tracking or attacks.

Use Cases:

- Fast network discovery for devices prioritizing speed over power efficiency (e.g., laptops, smartphones during active use).
- Roaming scenarios where stations need to quickly identify a new AP.
- Environments with hidden SSIDs, where active probing with specific SSIDs is required.