Q6)What’s the difference between Sniffer and Monitor mode ,use case for each mode?

**1. Sniffer Mode**

**What It Is:**

* A **dedicated diagnostic mode** where an AP **captures and forwards Wi-Fi packets** to a **Wireshark** or similar tool for analysis.
* Typically used in **enterprise Wi-Fi systems** (Cisco, Aruba, Ruckus).

**How It Works:**

* The AP **acts like a sensor**, capturing **802.11 frames** (management, control, data).
* Packets are **forwarded to a PC** running Wireshark via **CAPWAP** or **Ethernet**.
* Can filter specific channels, clients, or traffic types.

**Use Cases:**

✔ **Troubleshooting connectivity issues** (why is a client failing to authenticate?)  
✔ **Analyzing roaming behavior** (how long does handoff take between APs?)  
✔ **Debugging enterprise Wi-Fi issues** (QoS, interference, retries)

**Limitations:**

* **Not all APs support it** (usually enterprise-grade APs only).
* **Requires a WLC** (for CAPWAP-based sniffing).
* **Does not capture all raw RF data** (unlike Monitor Mode).

**2. Monitor Mode**

**What It Is:**

* A **low-level Wi-Fi interface mode** where a wireless NIC **captures all raw 802.11 frames** from the air.
* Used with **tools like Wireshark, Kismet, or Aircrack-ng**.

**How It Works:**

* The Wi-Fi card **disassociates from all networks** and listens to **all traffic** on a channel.
* Captures **unencrypted management/control frames** (even if data is encrypted).
* Can detect **hidden SSIDs, rogue APs, and packet retransmissions**.

**Use Cases:**

✔ **Security auditing** (detecting rogue APs, deauth attacks)  
✔ **Wireless penetration testing** (WPA cracking, packet injection)  
✔ **RF analysis** (signal strength, interference, channel utilization)

**Limitations:**

* **Cannot decrypt WPA/WPA2 traffic** (unless you have the key).
* **Requires compatible Wi-Fi adapters** (e.g., Atheros, Alfa cards).
* **No network connectivity** (NIC is in passive listening mode).

**Comparison Table**

|  |  |  |
| --- | --- | --- |
| Feature | Sniffer Mode | Monitor Mode |
| Device Used | Enterprise AP (Cisco, Aruba) | Wi-Fi NIC (Atheros, Alfa) |
| Packet Capture | Selective (via WLC) | All raw 802.11 traffic |
| Encrypted Traffic | Can decrypt if keys are known | Only sees encrypted data as-is |
| Use Case | Enterprise troubleshooting | Security analysis, hacking |
| Tools | Wireshark + CAPWAP | Wireshark, Aircrack-ng, Kismet |
| Connectivity | AP remains operational | Wi-Fi NIC cannot connect to networks |

**When to Use Which?**

**Use Sniffer Mode If:**

* Troubleshooting **enterprise Wi-Fi issues** (Cisco/Aruba networks).
* Need **Filtered, structured captures** (e.g., only client XYZ’s traffic).
* Access to **a supported AP and WLC**.

**Use Monitor Mode If:**

* Doing **security research or pentesting**.
* Need **raw RF-level data** (e.g., detecting Wi-Fi jammers).
* Using **a Kali Linux machine with a compatible Wi-Fi card**.