**6. What's the difference between Sniffer and monitor mode, use case for each mode.**

Sniffer mode and monitor mode are both used to capture wireless traffic, but the way they work and where they’re used is different.

**Sniffer Mode:**

* In sniffer mode, the access point captures wireless packets and sends them to a tool like Wireshark for analysis.
* It usually focuses on a specific channel and SSID, so it’s more targeted.
* This mode is useful when there's a need to check what’s going wrong with a particular client or network issue.
* It’s mostly used in enterprise networks where everything is managed by a controller.

**Use Cases:** For troubleshooting client connectivity problems, checking VoIP call quality, monitoring how specific applications perform over the network, and making sure policies like QoS and firewall rules are actually working. It's also helpful to track how clients roam between access points. This mode fits well in setups where a centralized controller manages the wireless network.

**Monitor Mode:**

* Monitor mode is more passive. It just listens to everything happening on a particular channel.
* It doesn’t connect to any network or transmit anything. It just captures all wireless frames, even from networks it’s not part of.
* This mode is useful when a complete picture of the wireless environment is needed.

**Use Cases:** For wireless security testing, spotting rogue access points, capturing hidden SSIDs, and checking how crowded each channel is. It's also useful during site surveys to map signal strength, detect any intrusions, and perform packet injection tests while doing ethical hacking.