### Q8)Challenges of Deploying Autonomous APs (50+) in a Large University Network

Autonomous APs (standalone APs) operate independently without a central controller. While simple for small setups, they introduce significant challenges in large-scale deployments like universities:

**1. Management & Configuration Complexity**

* **Manual Configuration:** Each AP must be configured individually (SSIDs, security, VLANs).
* **Inconsistent Policies:** Risk of misconfigurations due to human error.
* **No Central Dashboard:** Hard to monitor all APs at once.

**Impact:**  
✔ Time-consuming maintenance.  
✔ Higher IT workload.

**2. Poor Roaming Performance**

* **No Centralized Handoff:** Autonomous APs don’t coordinate client roaming.
* **Sticky Clients:** Devices cling to weak signals instead of switching to closer APs.

**Impact:**  
✔ Dropped VoIP/Zoom calls when moving across campus.  
✔ Slow Wi-Fi for mobile users.

**3. Security Risks**

* **Inconsistent Security Policies:** Some APs might use weaker encryption (WPA2 vs. WPA3).
* **Hard to Enforce Compliance:** Difficult to push updates (e.g., patching WPA3 vulnerabilities).
* **Rogue AP Detection:** No automated way to detect unauthorized APs.

**Impact:**  
✔ Higher vulnerability to attacks (e.g., Evil Twin APs).

**4. Scalability Issues**

* **Limited Visibility:** No single view of network health.
* **Channel Interference:** APs don’t auto-adjust channels/power (unlike controller-based systems).

**Impact:**  
✔ Congested Wi-Fi in high-density areas (lecture halls, dorms).

**5. Troubleshooting Difficulties**

* **Logs Scattered Across APs:** Hard to diagnose issues without centralized logs.
* **No Analytics:** Can’t track client behavior, RF interference, or performance trends.

**Impact:**  
✔ Longer downtime during outages.

**6. Firmware & Updates**

* **Manual Upgrades:** Must update each AP individually.
* **Risk of Version Mismatch:** Some APs may run outdated firmware.

**Impact:**  
✔ Security vulnerabilities persist longer.

**7. Lack of Load Balancing**

* **Clients May Overload Certain APs:** No intelligence to distribute devices evenly.

**Impact:**  
✔ Unstable performance in crowded areas.

**Comparison: Autonomous APs vs. Controller-Based (SplitMAC)**

|  |  |  |
| --- | --- | --- |
| Challenge | Autonomous APs | Controller-Based (SplitMAC) |
| Management | Manual per AP | Centralized (WLC/Cloud) |
| Roaming | Poor | Seamless (802.11k/v/r) |
| Security | Inconsistent | Uniform policies |
| Scalability | Difficult (>50 APs) | Easy (1000+ APs) |
| Updates | Manual | Push to all APs at once |