WiFi Training Program 2025

Name: Aswath S

University: VIT Vellore

Reg.No: 21BEC2188

Question-8:

What are challenges if deploying autonomous APs (more than 50) in large network like university

Deploying Autonomous APs (also called Standalone APs) across a large network like a university presents several challenges, mainly due to lack of central management and coordination.

Key Challenges:

1. Scalability Issues

- **Configuration Overhead: Each AP must be manually configured, managed, and monitored.**
- **Firmware Updates: Updating firmware individually on 50+ APs is time-consuming and prone to errors.**
- **No Centralized Authentication: Implementing consistent security policies (e.g., WPA3, 802.1X) is difficult.**

2. Lack of Centralized Management

- **Inconsistent Configuration: APs may have conflicting SSIDs, security policies, or radio settings if configured separately.**
- **No Unified Monitoring: Troubleshooting network-wide issues (e.g., interference, client load balancing) is complex.**
- **Rogue AP Detection: No centralized detection system for unauthorized devices on the network.**

3. Roaming Problems

- **Non-Seamless Roaming: Devices moving across campus may experience connectivity drops or re-authentication delays.**
- **Disjointed Network Experience: Clients need to re-establish connections when moving between APs with different SSIDs or security settings.**

4. Security Concerns

- **Lack of Centralized Policy Enforcement: Each AP needs to be configured separately with access control lists (ACLs) and authentication mechanisms.**
- **Vulnerability to Attacks: Without a central controller, detecting and mitigating attacks (e.g., deauthentication attacks, spoofing) is challenging.**

5. Network Performance Issues

- **No Load Balancing: Overloading of some APs while others remain underutilized.**

- **Channel Interference: Without coordination, APs may operate on overlapping channels causing performance degradation.**
- **Bandwidth Inefficiencies: No traffic prioritization (QoS) for critical applications.**

6. Maintenance Complexity

- **No Remote Management: Every AP must be accessed physically or via individual IP addresses for maintenance.**
- **Manual Troubleshooting: Identifying issues like packet loss, latency, or interference becomes tedious.**

7. High Operational Cost

- **Human Resources: More network administrators are required to manage 50+ APs individually.**
- **Increased Downtime: Lack of quick troubleshooting tools leads to longer downtime during outages.**