Corporate WLAN Configuration Guide

1. Introduction

This guide outlines the standard configuration steps and settings required to deploy a secure and efficient corporate WLAN environment.

2. Prerequisites

- Wireless Access Points (APs) with latest firmware
- WLAN controller (if applicable)
- Networking cables and power source for APs
- Network switch configured for VLANs
- SSID and authentication requirements

3. Network Topology Example

Device	IP Address	Role
WLAN Controller	192.168.50.10	Manages APs
Access Point 1	192.168.50.101	Broadcasts SSID
Access Point 2	192.168.50.102	Broadcasts SSID

4. WLAN SSID Configuration

1. Log in to the WLAN controller or AP management interface.
2. Create a new SSID (e.g., `Corp-WiFi`).
3. Choose WPA2-Enterprise security.
4. Configure RADIUS server settings:

```
RADIUS Server IP:   192.168.50.20
Port:               1812
Shared Secret:      [your_secret_key]
```

5. Enable VLAN assignment if needed (e.g., VLAN 20 for wireless clients).
6. Save and apply configuration.

5. Access Point Deployment Steps

1. Physically place APs for optimal coverage (minimum overlap, minimal interference).
2. Connect APs to switch ports configured for the WLAN VLAN.
3. Power on and ensure connectivity to the controller.
4. Adopt or register APs on the WLAN controller interface.
5. Verify SSID broadcast across all APs.

6. Client Connection Example

```
SSID:           Corp-WiFi
Security:       WPA2-Enterprise (802.1X)
Username:       corporate_user
Password:       [user_password]
```

7. Troubleshooting

- Verify AP LEDs for connectivity status.
- Check controller logs for authentication failures.
- Ensure correct VLAN tagging on switch ports.
- Ping RADIUS server from AP/controller to confirm reachability.

8. Documentation

- Record all SSIDs, VLAN IDs, and encryption methods used.
- Maintain a list of AP locations with IP addresses.
- Document RADIUS server credentials and backup procedures.