**Wireless Enterprise Services,**

**Solution Architecture Deliverable (SAD)**

This SAD outline flexible architecture patterns and building blocks for delivering secure, scalable, and high-performing enterprise wireless services. It focuses on providing multiple architecture options and identity service paths, suitable for a broad range of enterprise scenarios.

While vendor-agnostic in nature, it supports comparative evaluation across vendors in the appendix to facilitate downstream decisions.

The SAD is intended to support:

* Planning and governance for greenfield wireless rollouts.
* Cross-functional collaboration between network, security, and identity teams.
* Future phases such as HLD and LLD creation.

**Assumptions**

**Network Architecture**

* **Centralized Data Plane Architecture**: Data tunnelled back to controller or cloud gateway (e.g., Cisco Catalyst 9800, Aruba Mobility Conductor, or Meraki Cloud).
* **Distributed Data Plane Architecture**: Data locally bridged at AP (e.g., Meraki local breakout, Aruba Instant mode).

**Identity Architecture**

* **Enterprise client hybrid AD = Yes**: Integration with on-prem AD synced with Azure AD; supports on-prem certificate authority and conditional access.
* **Enterprise client hybrid AD = No (AAD Only)**: Modern device identity only via Intune + Microsoft Cloud PKI or third-party cloud RADIUS services.

**Technical Requirements**

**Requirements Areas**

* Corporate, guest, and IoT wireless segmentation
* Support for Zero Trust principles (ZTNA-ready)
* Alignment with Wi-Fi 6/6E adoption strategy

**Capacity Requirements**

* User concurrency forecasts
* High-density coverage (e.g., meeting rooms, auditoriums)
* Bandwidth and RF utilization monitoring

**Application Requirements**

* **Latency/Jitter/Packet Loss**: <150ms latency, <30ms jitter, <1% packet loss for real-time apps
* **Bandwidth**: Per-app profiling (VoIP, video conferencing, SaaS)

**Devices (LCMI)**

* Least Capable: Barcode scanners, VoIP handsets, IoT devices
* Most Important: Executive laptops, mobile endpoints, UC devices

**VoIP Requirements**

* Fast BSS transition (802.11r), CAC, DSCP marking
* Layer 3 roaming support

**Location-Based Services**

* Support for BLE beacons, AP location triangulation
* APIs for integration with RTLS platforms

**AP Choice**

* Wi-Fi 6E APs with tri-band capability
* External antenna options for harsh environments

**Security & Monitoring**

* 802.1X support with certificate-based EAP-TLS
* WPA3-Enterprise with fallback to WPA2
* Full telemetry via syslog/API to SIEM
* Integration with NAC (Cisco ISE, Aruba ClearPass, or RADIUS-as-a-Service)

**Redundancy Requirements**

* Dual switch uplinks, link aggregation (LAG)
* Redundant RADIUS/PKI/NAC services
* High availability for cloud controllers (if applicable)

**Minimum Data Rate**

* Default minimum: 12 Mbps (adjusted per site RF design)

**Certificate Requirements**

* Cloud or on-prem PKI
* Certificate enrolment via SCEP, Intune, or MDM

**WLAN Configuration**

* Segmented SSIDs per use case
* RF tuning based on site surveys (channel/power plan)
* Adaptive QoS and fast roaming features

**Authentication Requirements**

* 802.1X EAP-TLS for corporate
* PSK or MAC-based auth for IoT
* Guest captive portal integration (sponsored/anonymous access)

**Key Sections**

**Architecture Components**

* Access Points, Edge Switches, Identity Services (NAC/PKI)
* Wireless Controllers (on-prem/cloud)
* Integration with RADIUS, DHCP, DNS, and NTP
* Wired Core and Distribution layers

**Current vs. Target State**

* **Current State**: Fragmented WLAN deployments, legacy WPA2-PSK auth, limited telemetry
* **Target State**: Unified enterprise WLAN, centralized identity, telemetry-driven operations, ZTNA-aligned

**RF Design Philosophy**

* **Coverage-first** (e.g. warehouses, outdoor): APs placed for signal continuity
* **Capacity-first** (e.g. offices, auditoriums): Focus on density, interference mitigation

**Architectural Principles**

* **Redundancy**: Active/standby RADIUS and controller clusters
* **Scalability**: Cloud-native management, API-driven automation
* **Security**: Full-stack encryption, 802.1X, posture-based access

**Security Architecture**

* Identity store (AAD, AD, LDAP)
* RADIUS with certificate-based auth
* MDM posture checks and NAC policies
* SSO via SAML/OIDC where applicable

**WLAN Services**

* Layer 3 roaming (anchor or local breakout)
* Multicast support (multicast-to-unicast conversion)
* Guest VLAN segmentation
* VoIP QoS and prioritization

**Integration with Wired Core and Edge**

* Wired switch support for 802.1X (MAC bypass for IoT)
* PoE for APs
* Uplink redundancy with LAG or RSTP/MSTP
* VLAN pooling and dynamic VLAN assignment from RADIUS

**Appendix**

1/ Vendor comparison (Cisco, Meraki, Aruba, Juniper) to be provided as part of the HLD.

2/ **Options Analysis – Meraki Wireless Architecture**

It is intended to support decision-making and planning during enterprise wireless network design. Each option is evaluated based on applicability, architectural fit, operational considerations, and required network services.

**Option 1: Centralised Data Plane Architecture**

**Use Case Fit:** University campuses, medium/large enterprise headquarters, research institutions

|  |  |
| --- | --- |
| **Design Element** | **Characteristics** |
| **Traffic Flow** | Centralized traffic forwarding to core controller and services |
| **Controller Use** | Optional Catalyst 9800 for enhanced telemetry and QoS |
| **Management Model** | Meraki Dashboard + possible hybrid visibility via Catalyst |
| **Authentication & Identity** | Centralized RADIUS/NAC (e.g., Cisco ISE) |
| **DHCP/DNS** | Provided centrally in the campus data center |
| **Roaming** | Layer 2 roaming with PMK caching, OKC, 802.11r |
| **RF Design** | Capacity-first design with AP overlap and RF tuning |
| **Network Dependency** | High – core-dependent for services |
| **Security Integration** | Full posture-based access via NAC, 802.1X, MDM |
| **Operational Complexity** | High – multiple services and tight coordination required |
| **Resilience/HA** | Controller and switch stack HA, campus-wide redundancy |
| **Recommended Services** | ISE/NPS, SIEM, PKI, campus DNS/DHCP, firewall clusters |

**Option 2: Distributed Data Plane Architecture**

**Use Case Fit:** Retail branches, distributed enterprise sites, regional offices, small campuses

|  |  |
| --- | --- |
| **Design Element** | **Characteristics** |
| **Traffic Flow** | Local breakout from AP or access switch |
| **Controller Use** | None – traffic flows directly; Meraki Cloud controls management |
| **Management Model** | 100% Meraki Dashboard cloud-managed |
| **Authentication & Identity** | Cloud RADIUS or proxy to central auth (e.g., SecureW2, Portnox) |
| **DHCP/DNS** | Local gateway or cloud-relayed services |
| **Roaming** | Minimal roaming – per site L2 domains |
| **RF Design** | Coverage-first with AI-RRM for channel/power |
| **Network Dependency** | Low – minimal core reliance |
| **Security Integration** | Group policy via tags; lightweight posture checks |
| **Operational Complexity** | Low – templated configuration, simplified site setup |
| **Resilience/HA** | Meraki cloud HA, AP config caching, dual uplinks |
| **Recommended Services** | Cloud NAC/PKI, local DHCP, lightweight SIEM, secure internet edge |

This options analysis informs the selection of a preferred wireless architecture based on organizational goals, existing infrastructure, and operational capabilities. Each option has strengths and trade-offs, and may be mixed in hybrid deployments across different business units.

**Summary Recommendation Table**

|  |  |  |
| --- | --- | --- |
| **Dimension** | **Option 1: Centralised** | **Option 2: Distributed** |
| **Scale** | Suited to 1000s of APs, campus | Scales horizontally across sites |
| **Best For** | High-density, high-roaming users | Retail, branch, lightweight ops |
| **Identity Complexity** | Full NAC, MDM integration | Simpler cert or PSK-based auth |
| **Operational Overhead** | Higher (more components) | Lower (single dashboard) |
| **Resilience Model** | Controller HA + campus switches | Cloud-managed HA + AP fallback |
| **IT Resource Dependency** | Requires skilled campus IT | Deployable by lean IT teams |

**Meraki Wireless Design Decisions**

1. Cloud Management Strategy
2. Configuration Templates
3. Network and Device Tagging
4. Wireless Firmware Lifecycle Management
5. AI-RRM (AI-Driven Radio Resource Management)
6. Zero Wait DFS
7. Client Roaming Optimization
8. Distributed vs. Centralized Data Plane
9. Multicast & VLAN Override Design
10. DHCP and Subnet Sizing
11. Security & Identity Integration (802.1X, RADIUS, SGT)
12. Client Load Balancing
13. API Automation & Ecosystem Integration
14. Roaming Domain Planning
15. AAA Load Balancer Recommendation

**Meraki Wireless Design Decision Table (Landscape View)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Design Decision** | **Description** | **Key Features** | **Implications** |
| **1. Cloud Management Strategy** | Use Meraki Dashboard for centralized cloud-based network management. | 99.99% uptime SLA, multi-region redundancy, RBAC, remote access | Simplifies ops, needs reliable internet for management access. |
| **2. Configuration Templates** | Apply standard configs across networks via templates. | Global settings for SSIDs, VLANs, RF; local overrides allowed | Speeds up deployment; requires careful planning to avoid override conflicts. |
| **3. Network & Device Tagging** | Tag networks/devices to organize policies and filtering. | Dynamic policy assignment, visibility filtering, tag-driven config templates | Must define tag naming standards for scalability and clarity. |
| **4. Firmware Lifecycle Management** | Plan and schedule firmware upgrades across device groups. | Staged updates, test groups, firmware channel control | Prevents disruptions; must track firmware branches. |
| **5. AI-RRM (Radio Resource Management)** | Optimize channel and power via historical RF analytics. | AI-driven channel planning, busy-hour RF logic, improved coverage models | Reduces interference and improves performance in high-density areas. |
| **6. Zero Wait DFS** | Seamless DFS scanning without disassociating clients. | Off-channel DFS scan, real-time monitoring | Uses DFS channels without impact; requires supported AP models. |
| **7. Client Roaming Optimization** | Enhance roaming via L2 design and fast roaming protocols. | 802.11r, OKC, PMK caching | Faster transitions; design subnet boundaries carefully to avoid L3 roaming pitfalls. |
| **8. Centralized vs. Distributed Data Plane** | Select data path handling model: cloud-local breakout or controller-based. | Distributed = local breakout; centralized = traffic tunneled | Distributed fits Meraki well; centralized needed for security-sensitive apps. |
| **9. Multicast & VLAN Override Design** | Design how multicast traffic is handled per VLAN. | Multicast-to-unicast conversion, IGMP proxying | Enhances streaming/voice support; VLANs must be designed per site. |
| **10. DHCP & Subnet Sizing** | Right-size IP scopes based on user density and lease times. | Shorter leases for guest/retail; subnet design per roaming domain | Avoids DHCP exhaustion; needs scope segmentation per AP group. |
| **11. Security & Identity Integration** | Use 802.1X + RADIUS + NAC/ISE/ClearPass for auth and policy. | EAP-TLS, AAA override, VLAN or SGT assignment, CWA | Enables identity-driven access; requires NAC and cert infra. |
| **12. Client Load Balancing** | Distribute clients across APs based on signal and utilization. | Passive (probe-based), active (802.11v) balance | May impact client performance if tuning is off; recommended off in high-density unless optimized. |
| **13. API Automation & Ecosystem** | Use Meraki APIs for provisioning, alerting, integration. | Dashboard API, Webhooks, MQTT, location analytics, captive portal API | Enables full automation; requires API security and lifecycle governance. |
| **14. Roaming Domain Planning** | Define L2 roaming boundaries based on client scale and RF. | Max 200 APs/roaming domain, 8k clients/switch (hardware dependent) | Ensures performance; VLAN pools and ARP handling need careful planning. |
| **15. AAA Load Balancer Recommendation** | Use a load balancer when deploying >3 AAA servers. | Sticky sessions, failover, central RADIUS routing | Boosts auth resilience and load distribution in large-scale wireless deployments. |