Wireless Enterprise Standard

**Status: Draft**

**Wireless Day0, 1 and 2 Tasks**

**Monitoring**:

* AP/client health dashboards
* Channel utilization and interference
* Rogue AP detection & alerts

**Optimization**:

* Dynamic RF adjustments (or manual tuning)
* Adjustments to SSID load balancing, minimum bitrate settings

**Security**:

* Firmware upgrades
* WPA3 rollout, segmentation enforcement
* Guest traffic isolation

**Change management**:

* Adding new APs or sites
* Adjusting RF or network profiles

**Analytics/Reporting**:

* Usage reports
* Application performance
* Client behavior/location tracking

**Wi-Fi Survey by Project Phase**

|  |  |  |
| --- | --- | --- |
| **Project Phase** | **Survey Type** | **Purpose** |
| **Plan & Design** | *Wi-Fi Predictive Design* | Design RF coverage before deployment using building floor plans and RF modeling tools. |
| **Pre-Deployment** | *Wi-Fi Pre-deployment Survey* | Validate predictive designs onsite using test APs to measure real-world attenuation and interference. |
| **Deployment Validation** | *Wi-Fi Deployment Validation Survey* | Post-installation survey to confirm coverage, signal quality, and validate that the design has been implemented successfully. |
| **Operations / Troubleshooting** | *Wi-Fi Diagnostic Survey* | Performed when users report issues; it identifies RF problems, interference, misconfigurations, or performance bottlenecks. |

**802.1X** is the gold standard for **port-based network access control** in enterprise Wi-Fi

**802.1X Authentication Flow in Wi-Fi**

1. **Supplicant connects to AP** (SSID using 802.1X)
2. **AP (Authenticator)** forwards request to RADIUS server
3. **RADIUS Server** checks identity & authentication policy
4. If successful:
   * Port is opened
   * Role/VLAN/DACLs may be pushed
5. If failed:
   * Access denied or fallback to guest VLAN

**Common EAP Types in 802.1X Wi-Fi**

|  |  |  |
| --- | --- | --- |
| **EAP Type** | **Description** | **Use Case** |
| **EAP-TLS** | Cert-based mutual auth | Highly secure, for corporate devices |
| **PEAP-MSCHAPv2** | Username/password in tunnel | Easy to deploy, common with AD |
| **EAP-TTLS** | Tunnel with varied auth | Flexible for mixed environments |
| **EAP-FAST** | Cisco proprietary | Legacy Cisco environments |

**Core Components of 802.1X in Wi-Fi**

**1. Supplicant (Client Device)**

* The software or device **requesting access** to the network.
* Usually built into OS (Windows, macOS, iOS, Android, Linux).
* Examples:
  + Laptops, phones, tablets
  + IoT devices (may require certificate-based auth or MAC bypass)
* Can use:
  + EAP-TLS (cert-based)
  + PEAP/MSCHAPv2 (username/password)

**2. Authenticator (Access Point or Controller)**

* **Wireless access point (AP)** or **wireless controller** that acts as the middleman between the supplicant and the authentication server.
* Controls port access (open or restrict) based on authentication result.
* Common examples:
  + Cisco Catalyst/Meraki, Aruba, Juniper Mist APs

**3. Authentication Server (RADIUS Server)**

* Validates the **credentials or certificates** received via the authenticator.
* Often integrates with identity stores like:
  + Microsoft Active Directory
  + LDAP
  + Azure AD (via extensions)
* Common RADIUS solutions:
  + Cisco ISE
  + Aruba ClearPass
  + FreeRADIUS
  + Windows NPS

**Supporting Components**

**4. Certificate Authority (CA)**

* Required for **EAP-TLS**, **PEAP**, or **TTLS** to issue and manage digital certificates.
* Can be:
  + Microsoft AD Certificate Services
  + Public CAs (for BYOD use cases)
  + Internal PKI

**5. Identity Store**

* Backend user directory (e.g., AD, LDAP) used by the RADIUS server to validate user/device credentials.

**6. Policy Engine (optional but common)**

* Provides **role-based access**, VLAN assignments, downloadable ACLs.
* Can apply differentiated access based on user group, device posture, time of day, etc.

Examples: Cisco ISE or Aruba ClearPass

Tools

Wi-Fi SSID Overhead Calculator: revolution wifi

|  |
| --- |
| **ASSUMPTIONS:** |
| 802.11b Long Preamble used for 1 Mbps;  Short Preamble used for 2, 5.5, 11 Mbps |
| 802.11g short slot time is assumed, with no 802.11b clients within range |
| WMM is enabled and beacons are transmitted using Best Effort AC |

|  |  |
| --- | --- |
| **VARIABLES:** | |
| **Beacon Data Rate (Mbps)** | **802.11a 12 Mbps** |
| **Beacon Frame Size (Bytes)** | **330** |
| **Beacon Interval (ms)** | **102.4** |

**Amount of Overhead:**

|  |  |  |  |
| --- | --- | --- | --- |
| 0-10% Low | 10-20% Medium | 20-50% High | >50% Very High |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Number of APs on Channel\*** | **Number of SSIDs** | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |

A white text with black text

AI-generated content may be incorrect.

Standards

A screenshot of a computer security trends

AI-generated content may be incorrect.

**Channel Planning**

<https://www.ekahau.com/blog/channel-planning-best-practices-for-better-wi-fi/>

<http://revolutionwifi.blogspot.com/2013/03/80211ac-channel-planning.html>

wireless-enterprise-authentication-802-1x

**WPA Authentication Protocols – Overview & Comparison**

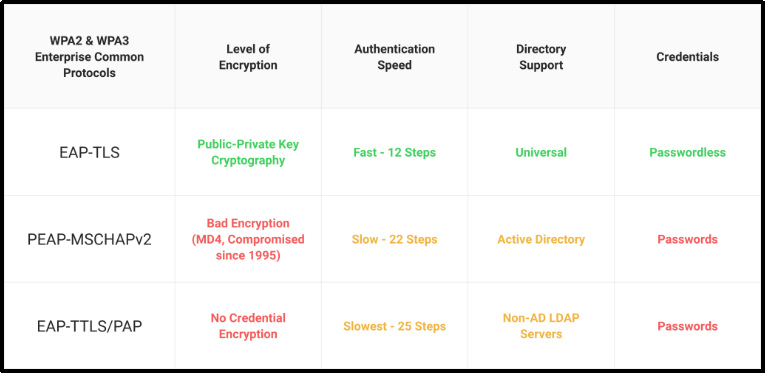
|  |  |  |  |
| --- | --- | --- | --- |
| **Protocol** | **Authentication Type** | **Security Level** | **Typical Use Case** |
| **WPA2-PSK** | Shared Password | Moderate | Small businesses, guest Wi-Fi |
| **WPA3-PSK (SAE)** | Shared Password | Stronger | Newer guest networks |
| **WPA2-Enterprise** | 802.1X + RADIUS | Strong | Standard for enterprise |
| **WPA3-Enterprise** | 802.1X + RADIUS + 192-bit crypto | Highest | High security/government |

|  |  |  |
| --- | --- | --- |
| **Mode** | **Uses 802.1X?** | **How Authentication Works** |
| **WPA2-Enterprise** | Yes | Auth via 802.1X + RADIUS + EAP (PEAP, EAP-TLS, etc.) |
| **WPA3-Enterprise** | Yes | Same as above but with enhanced encryption (192-bit) |
| **WPA2-PSK** | No | Shared password (no identity, no 802.1X) |
| **WPA3-PSK (SAE)** | No | Shared password with improved security (still no 802.1X) |

What 802.1X brings to the table:

* Per-user/device authentication (identity-aware access)
* Integration with RADIUS servers (e.g., Cisco ISE, Cloud RADIUS)
* Enables dynamic VLAN assignment, NAC, posture checks
* Supports EAP types (e.g., PEAP, EAP-TLS for cert-based auth)

So in short:  
Enterprise = 802.1X + RADIUS + identity-based access  
PSK = just a password, no identity layer



WPA authentication protocols in different modes:

* WPA2-Enterprise
* WPA3-Enterprise
* WPA2-PSK
* WPA3-PSK

Enterprise setting, customers must establish a secure connection with an authentication server before entering their credentials.

**What Enterprises Typically Do**

|  |  |  |
| --- | --- | --- |
| **SSID Type** | **Recommended Protocol** | **Why** |
| Corporate Devices | WPA2-Enterprise / WPA3-Enterprise | Identity-based, cert-based, VLAN support |
| BYOD/Contractors | WPA2-Enterprise + SCEP | PKI-based onboarding via Intune or Jamf |
| Guest Wi-Fi | WPA3-PSK (or open + captive portal) | Secure but frictionless access |
| IoT Devices | WPA2-PSK with MAB fallback | Simplified provisioning, isolated VLAN |

**Summary**

* Use **WPA2/WPA3-Enterprise** for any **internal/corporate SSID**.
* Use **PSK (preferably WPA3-PSK)** for **guest or IoT** where 802.1X is not viable.
* Futureproof with WPA3 **only** if your device fleet supports it.

## Meraki Specifics

Meraki Campus Design

A diagram of a cloud computing system

AI-generated content may be incorrect.

A diagram of a security system

AI-generated content may be incorrect.

A diagram of a cloud monitoring

AI-generated content may be incorrect.

Simple Onboarding and Access

• Order can have a single or multiple device/license

• Power up devices and they pull config from dashboard

Role Base Access (RBAC) with Meraki Dashboard

A green and orange squares with white text

AI-generated content may be incorrect.

Using tags for additional Flexibility

A close-up of a diagram

AI-generated content may be incorrect.

Integration at scale with APIs

<http://developer.cisco.com/meraki/>

A green and white background with text

AI-generated content may be incorrect.

Wireless Firmware Upgrades

Intelligent firmware rollout that constantly monitors firmware globally

A diagram of a software company

AI-generated content may be incorrect.

A close-up of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Meraki Tags: Overview**

There are two main types of tags:

|  |  |  |
| --- | --- | --- |
| **Tag Type** | **Applies To** | **Purpose** |
| **Network Tags** | Entire network org/site | Organize and filter networks for templates, firmware, settings |
| **Device Tags** | Individual APs, switches, MX | Group devices within networks for policy, SSID, VLAN or firewall overrides |

**Network Tags**

* **Defined in:** Meraki Dashboard > Organization > Overview
* **Used for:** Binding **configuration templates** to groups of networks (e.g., HQ, Branch, Retail)
* **Use Cases:**
  + Assign specific firmware versions
  + Apply common template to tagged branches (e.g., all retail-store-\*)
  + Filter networks in bulk actions or dashboard views

**Device Tags**

* **Defined in:** Device details or inventory
* **Used for:**
  + **Per-device policy assignment**, especially for wireless SSIDs and firewall rules
  + Overriding settings within a template-bound network
* **Use Cases:**
  + Only advertise a specific SSID on tagged APs (e.g., only lobby-ap)
  + Assign VLAN or RF profile to tagged APs
  + Enable local breakouts only on certain devices (e.g., sd-wan-primary)

**Day 0 / Day 1 / Day 2 Use Cases**

|  |  |
| --- | --- |
| **Phase** | **Use of Tags** |
| **Day 0** (Planning) | - Define **network tags** for branches/sites types (e.g., store, warehouse, hq) - Decide tagging schema and automation triggers - Design **template hierarchy** based on network tags |
| **Day 1** (Deployment) | - Apply **device tags** to APs or switches for specific SSIDs, RF profiles, VLANs - Use network tags to bind to templates - Set RADIUS VLAN assignment overrides using tags |
| **Day 2** (Operations) | - Automate firmware upgrades or configuration updates by tag - Bulk assign or audit device configurations - Filter alerts, events, and logs based on tags - Trigger Ansible/automation workflows per tag group |

**Tags + Ansible**

With Meraki’s API + Ansible modules, tags help:

* Dynamically apply configs (SSID, VLANs, templates)
* Roll out changes to specific groups (e.g., ap-north-zone)
* Perform config drift detection per tag group

**Roaming**

Exec Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Description** | **Pros** | **Cons** |
| **1. Stretched VLAN via L2 Trunking** | Extend same VLAN across buildings using physical L2 trunk links | Simple design; native Meraki support | STP/scalability limits; requires contiguous switching domain |
| **2. Meraki Layer 3 Roaming with Central NAT** | Meraki feature that keeps client IP via tunnel to anchor AP | Seamless roaming: no L2 extension needed | Slight overhead; configuration per SSID |
| **3. VXLAN Overlay (Hybrid)** | Use Catalyst VXLAN/SD-Access fabric to stretch VLANs over IP | Scalable; modern campus core integration | Requires Catalyst core; not native to Meraki MS switches |
| **4. RADIUS + Dynamic VLAN Assignment** | Central auth assigns same VLAN at all sites (requires pre-provisioned VLAN) | Policy-driven; identity aware | VLAN must exist in all sites; does not eliminate L2 constraint |

Comparing Option 2: Meraki L3 Roaming with Central NAT vs. Option 4: Dynamic VLAN via RADIUS

|  |  |  |
| --- | --- | --- |
| **Factor** | **Option 2: Meraki L3 Roaming w/ Central NAT** | **Option 4: Dynamic VLAN Assignment via RADIUS** |
| **Roaming Experience** | Seamless — user keeps same IP across APs, even across subnets | Not seamless across buildings unless VLAN exists in both areas |
| **Authentication Flow** | No re-auth needed when roaming — session is preserved via tunnel anchor | Re-authentication may occur when moving between VLANs/sites |
| **IP Address Preservation** | ✅ Yes — IP address is centrally anchored, no DHCP renewal | ❌ No — if VLAN changes across buildings, new DHCP lease is issued |
| **Application Impact** | Minimal — apps like VoIP, VPN, video conferencing remains stable | Risk of session drop or latency as IP stack resets during re-auth |
| **User Disruption** | Near-zero — users roam invisibly across infrastructure | Moderate — short outage or disconnect may be observed during reassociation |
| **Configuration Complexity** | Moderate — Meraki-specific config per SSID | Moderate — requires consistent RADIUS policies + pre-defined VLANs per site |
| **Operational Overhead** | Low once configured — no VLAN sprawl required | Higher — requires VLAN planning and provisioning across all locations |
| **Ideal For** | Seamless experience across multi-building campuses | Policy-driven access with centralized control (e.g., role-based VLANs) |

**Summary Recommendations:**

* **Option 2 (Meraki L3 Roaming with Central NAT)**  
  ✅ **Best for user experience** in campus environments — users roam without dropping IP or session.  
  Ideal for **real-time apps** (VoIP, Zoom, Citrix, Teams).
* **Option 4 (Dynamic VLAN via RADIUS)**  
  ⚠️ **More suitable for policy control**, but less ideal for roaming continuity.  
  Use where **identity-based segmentation** is more important than session persistence.

**Client-Side Roaming Optimization by OS**

|  |  |  |  |
| --- | --- | --- | --- |
| **OS / Platform** | **Optimization** | **Layer 2 or Layer 3 Benefit** | **Admin Action Needed** |
| **Windows 10/11** | - Enable **Fast Roaming (802.11r)** support via Group Policy - Enable **Aggressive roaming** (Roaming Aggressiveness = High) - Configure WLAN profiles via Intune/GPO - Use native **WLAN AutoConfig** behaviors properly | L2 & L3 (Fast reassociation and PMK caching) | Yes – via GPO, Intune, or manual regedit |
| **macOS (Monterey+)** | - macOS supports **802.11r**, **802.11k**, **802.11v** natively - Use **Jamf** or MDM to enforce known networks - Disable power save modes aggressively in roaming-prone environments | L2 roaming (best case with Meraki Fast Roaming) | Moderate – Jamf Pro profile enforcement |
| **iOS/iPadOS** | - Native support for **802.11r/k/v** - MDM-based Wi-Fi config to optimize SSID selection - Background scanning on roaming candidates | L2 roaming | No extra config needed beyond MDM |
| **Android (11+)** | - Varies by OEM; enforce **roaming parameters** using Android Enterprise - Some support for **802.11k/r/v** but inconsistently - Disable Wi-Fi sleep/power save on critical apps | L2 roaming (if supported) | OEM/MDM-dependent |
| **Windows (legacy)** | - Roaming delay due to lack of 802.11r/OKC - Use **driver updates** from Intel/Qualcomm - Avoid GPOs that restrict wireless profile flexibility | May degrade roaming unless patched | Requires manual tuning or OS upgrade |

**General Client-Side Best Practices**

* **Use certificate-based authentication (EAP-TLS)**: avoids interactive prompts during reassociation.
* **Limit SSID count per AP**: fewer SSIDs = faster scans = quicker roaming decisions.
* **Driver Updates**: ensure Wi-Fi adapter drivers (Intel, Broadcom, etc.) are up to date — many roaming fixes are vendor-specific.
* **Avoid power-save modes** on critical roaming clients (VoIP handsets, thin clients).
* **Fast Transition (FT/802.11r)** should be explicitly supported in the SSID — most enterprise clients benefit greatly.

**For Meraki Networks Specifically:**

Meraki supports:

* **802.11r** (Fast BSS Transition)
* **802.11k** (Neighbor reporting)
* **802.11v** (BSS Transition Management)

**Clients must support these as well** for them to function — so **platform tuning + Meraki config go hand-in-hand**.

**BYOD Self-Provisioning with Cisco ISE (WPA2/WPA3-Enterprise)**

**SSID**: BYOD-WiFi  
**Security Type**: WPA2-Enterprise or WPA3-Enterprise  
**Use Case**: Staff/contractor personal devices that need secure corporate access but are not fully managed.

**Trust Enforcement Logic**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stage** | **Function** | **Enforced By** | **Notes** |
| Connect to Onboarding SSID | User connects to open or pre-auth SSID (BYOD-Onboard) | Meraki AP | Triggers redirection |
| Device Identity Check | ISE portal identifies device as unmanaged | Cisco ISE | MAC and browser fingerprinting |
| Self-Service Portal | User logs in with corporate SSO | Cisco ISE Portal | Enforced via SAML or LDAP |
| Certificate Provision | ISE issues personal certificate via SCEP | ISE + ISE Internal CA or External CA | Cert includes user/device identity |
| Network Switch | ISE dynamically redirects to BYOD-WiFi SSID | ISE + Meraki RADIUS change-of-authorization (CoA) | Enforces WPA2/3-Enterprise with EAP-TLS |
| Role-Based Access | Assign VLAN/ACL based on identity group | ISE + Meraki Group Policy | Personal devices restricted from privileged apps |

**Optional Enhancements:**

* **Posture assessment** via ISE Agent or browser-based scan (e.g., AV installed, updates current).
* **MDM enrollment redirect** if corporate ownership changes.
* **Guest fallback**: If identity fails, redirect to Guest-WiFi.

**MDM Policy Enforcement Logic – EAP-TLS Workflow (Zero Trust Aligned)**

**Objective**: Ensure only MDM-enrolled corporate devices with valid certificates can join the enterprise SSID.

**Trust Policy Flow:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stage** | **Function** | **Enforced By** | **Notes** |
| Device Enrollment | Device registers with MDM (e.g., Intune, JAMF) | MDM Platform | Tagged as corporate asset |
| Certificate Issuance | Unique client certificate issued (EAP-TLS) | SCEP/NDES or MDM CA | Includes device identifier (UDID, hostname) |
| Wi-Fi Join Attempt | Device attempts WPA3-Enterprise connection | Meraki AP | Triggers 802.1X |
| Identity Validation | Certificate checked (CN, SAN, expiry) | Cisco ISE / RADIUS | Policy matched via certificate attributes |
| Posture Check (optional) | Validate compliance (OS version, antivirus, disk encryption) | Cisco ISE + MDM API | Can assign different VLANs or deny access |
| Network Access | VLAN assigned + group policy enforced | Meraki + RADIUS | Access granted only if policy matches |

**Zero Trust Design Principles Supported:**

* **Strong Identity Assurance**: Device + User identity bound to cert
* **Least Privilege**: Dynamic VLANs and ACLs per posture
* **Continuous Evaluation**: ISE can revalidate posture during session

**WPA3-Personal Guest Wi-Fi – Zero Trust Guest Access Logic**

**SSID**: Guest-WiFi  
**Security Type**: WPA3-Personal (SAE)  
**Use Case**: Short-term guest users with simplified access and basic isolation.

**Trust Enforcement Logic**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stage** | **Function** | **Enforced By** | **Notes** |
| Broadcast SSID | Guest-WiFi with WPA3-Personal (SAE) | Meraki AP | Transition mode optional for legacy support |
| Pre-shared Key Entry | User inputs dynamic or rotating PSK | User Device | Optional PSK rotation via automation |
| DHCP Assignment | Guest IP assigned from DMZ/guest VLAN | Meraki or upstream DHCP | VLAN segmentation ensures traffic isolation |
| Content & URL Filtering | Limit access to corporate or sensitive assets | Meraki L7 firewall rules | Can integrate with Umbrella or firewall content filters |
| Session Tracking | Optional splash page agreement or click-through | Meraki Captive Portal | No identity, but legal/log compliance enforced |

**Optional Enhancements:**

* Use **sponsored guest registration portals** (Meraki or ISE) for known guests.
* Integrate with **Umbrella DNS Filtering** for outbound DNS control.
* Rotate PSKs on schedule via **Meraki API**.