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**

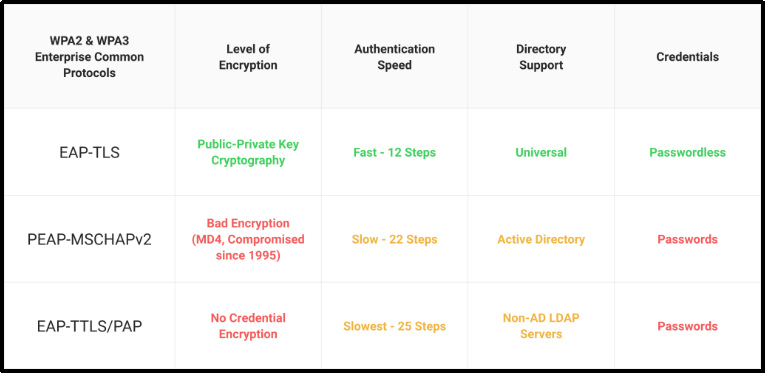
|  |  |  |  |
| --- | --- | --- | --- |
| **Protocol** | **Authentication Type** | **Security Level** | **Typical Use Case** |
| **WPA2-PSK** | Shared Password | Moderate | Small businesses, guest Wi-Fi |
| **WPA3-PSK (SAE)** | Shared Password | Stronger | Newer guest networks |
| **WPA2-Enterprise** | 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.