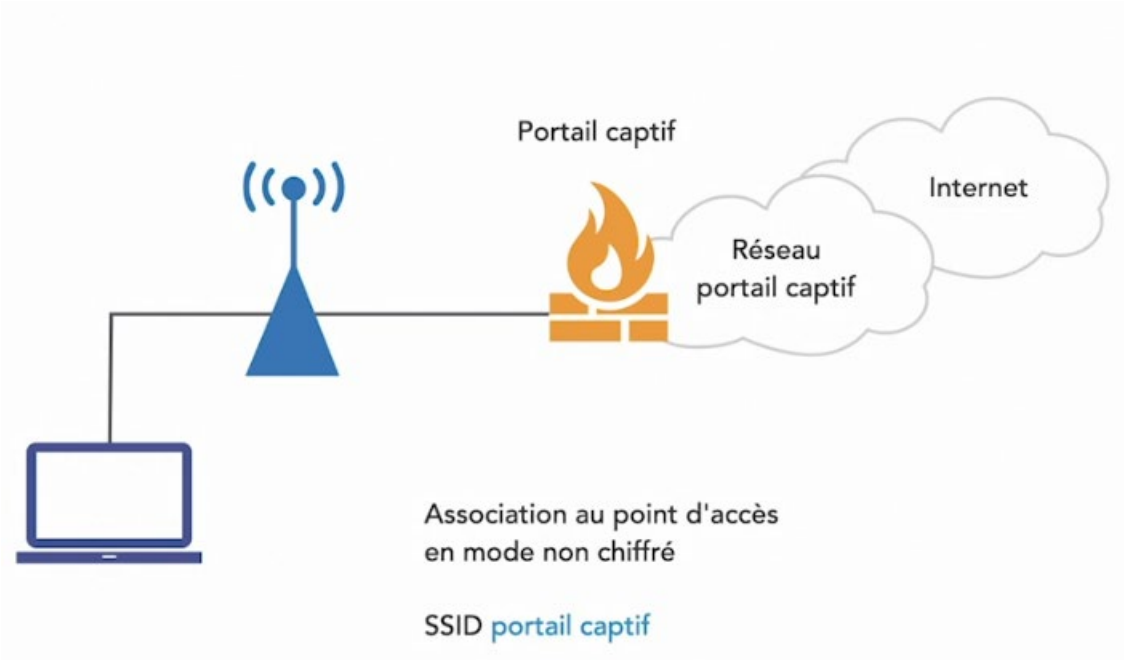
Mise en œuvre d'un réseau WiFi sécurisé

Sécuriser les réseaux wi-fi

OPEN AUTHENTICATION

- Authentification **Ouverte**
- Seule exigence : **Norme 802.11**
- **Pas de mot de passe**
- **Pas de contrôle de l'identité**
- Principalement utilisé dans **les lieux publics** (Aéroport, Hôtel…)



SOURCE: linkedin.com

WEP (WIRED EQUIVALENT PRIVACY)

- Défini par la norme **802.11** en 1999
- **Algorithme** de chiffrement **RC4**
- Méthode de sécurité **à clé partagée**
- L'outil de chiffrement est une **« phrase aléatoire »**
- Longueur de **40 ou 104 bits** = Chaine **de 10 ou 26** caractères hexadécimaux
- **Méthode faible pour sécuriser un LAN sans fil**

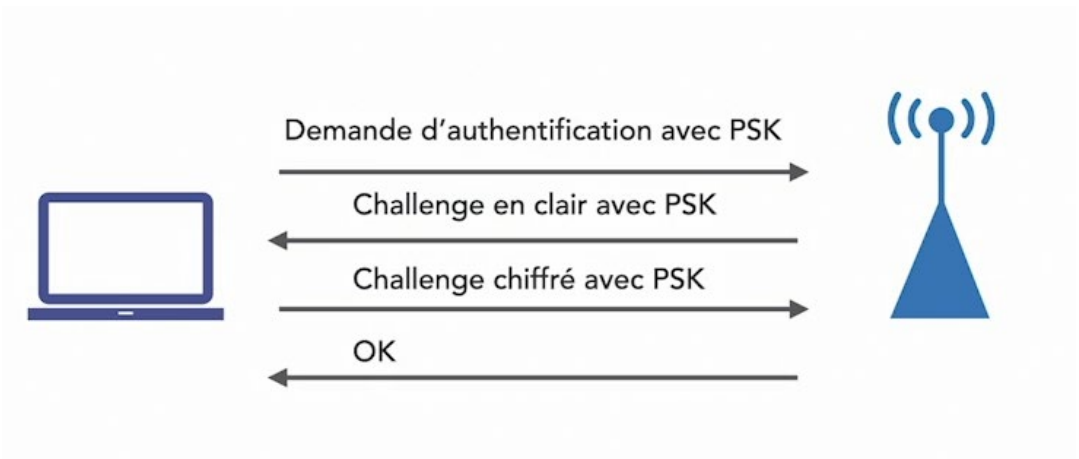
Clé WEP

128 bits = 104 bits + 24 bits vecteur d'initialisation (IV) + algorithme (RC4)

La clé WEP sert à la fois d'authentification et de chiffrement

Pre-shared key authentication

- Clé commune connue du client et de la borne
- À partir de 802.11a **W**ired **E**quivalent **P**rivacy



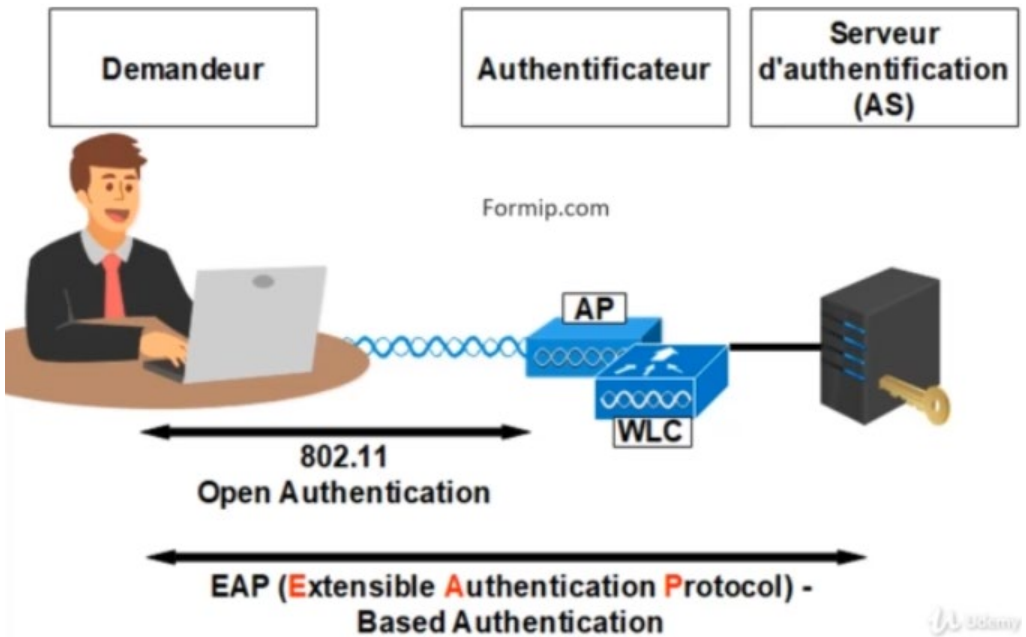
PSK (pre-shared key) = mot de passe

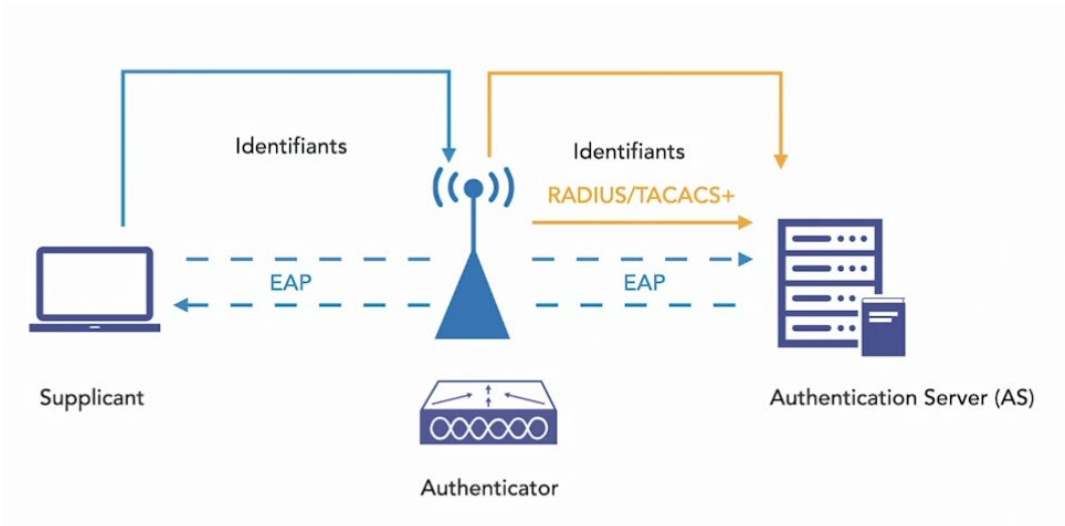
SOURCE: linkedin.com / udemy

Extensible Authentication Protocol (802.1X)

802.1X / EAP

- **Plus sécurisée** que le WEP
- Norme **802.1x** (juin 2001 par L'IEEE)
- **Authentification** par un serveur d'authentification
- Le **802.1x** repose sur le **protocole EAP** (Extensible Authentication Protocol)
- **Garde-barrière**





- Tunnel EAP (couche 2 OSI)
- AS interroge une base de données local / ou distant exemple : serveur AD

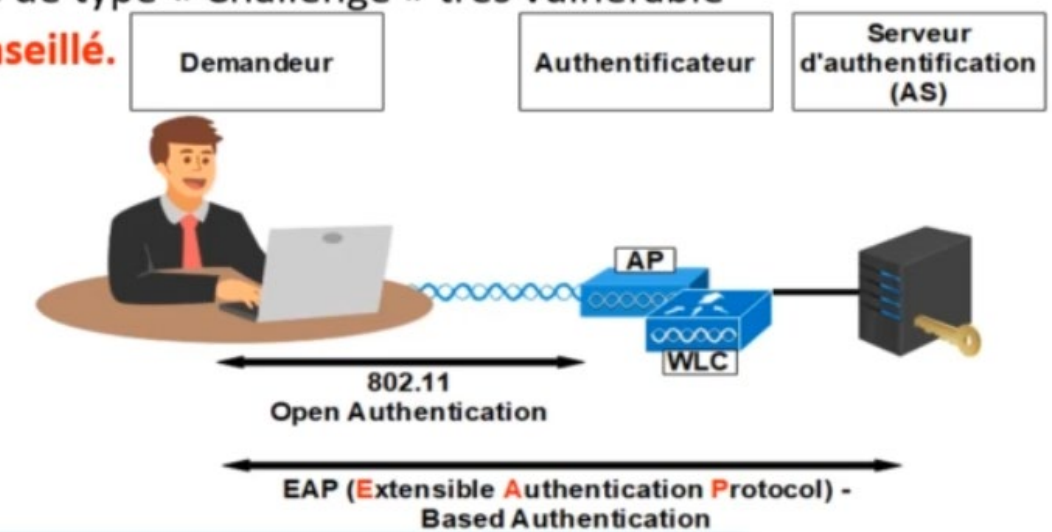
SOURCE: linkedin.com / udemy

Lightweight Extensible Authentication Protocol (LEAP)

- Propriétaire Cisco
- Authentification mutuelle
- Clés WEP dynamiques
- Déprécié

LEAP(Lightweight Extensible Authentication Protocol),

- Le client doit fournir un **nom d'utilisateur** et son **mot de passe.**
- Messages cryptés de type **« Challenge »**
- utilise des clés **WEP dynamiques**
- **Méthode cryptés** de type « Challenge » très vulnérable
- **Fortement déconseillé.**



SOURCE: linkedin.com / udemy

EAP-FAST

- Simple
- Sécurisé via tunnel TLS
- Tunnel établi via Protected Access Credential et clé prépartagée
- Certificats en option

EAP-FAST (EAP Flexible Authentication by Secure Tunneling)

- Crée par Cisco pour **pallier aux faiblesses du LEAP**
- Protection par **PAC** (Protected Access Credential)
  1. Le PAC est **généré et installé** sur le client
  2. Négociation d'un **tunnel TLS** (Transport Layer Security)
  3. Authentification par le **tunnel TLS**
- Demande un **serveur RADIUS**

SOURCE: linkedin.com / udemy

Protected Extensible Authentication Protocol (PEAP)

- Standard ouvert
- Établissement d'un tunnel TLS
- Authentification de l'AS via une PKI
- Authentification en 2 phases
    1. Authentification du serveur AS via PKI
    2. Établissement du tunnel TLS

PEAP (Protected EAP)

- **Authentification** interne et externe
- **Certificat numérique** pour s'identifier auprès du client
- Tunnel **TLS** (Transport Layer Security)

PKI : clé publique du serveur

SOURCE: linkedin.com

Extensible Authentication Protocol Transport Layer Security (EAP TLS)

- Sécurisé et complexe
- Standard ouvert
- Établissement d'un tunnel TLS
- Authentification de l'AS via une PKI
- Authentification du client par un certificat

EAP-TLS (EAP Transport Layer Security)

- Utilise la **couche transport** de sécurité, le TLS.
- Utilise **deux certificats** pour la création d'un tunnel sécurisé
  1. Certificat côté **serveur**
  2. Certificat côté **client**
- **Difficile et couteux**, de gérer 1 certificat par machines

Besoin d'un certificat sur chaque client (contrainte de gestion et configuration)

SOURCE: linkedin.com

Temporal Key Integrity Protocol (TKIP)

- Amélioration de WEP
- Chiffrement
  - Série de clés changeantes
  - Algorithme RC4
  - Une clé par paquet
- Intégrité
  - IV chiffré
  - Code MIC
- Spécification WPA2

TKIP (Temporal Key Integrity Protocol)

- développé pour **remplacer le WEP**
- Ajoute plusieurs fonctionnalités de **sécurité :**
  1. « **MIC** » (**M**essage **I**ntegrity **C**heck)
  2. « **time stamp** »
  3. « L'Adresse **MAC de l'expéditeur** »
  4. « **TKIP** sequence counter »
  5. « **Key mixing algorithm** »
  6. « **Longer initialization vectore** (IV) »
- **4 algorithmes** supplémentaires :
  1. **Code d'intégrité** de message
  2. Compteur pour les **vecteurs d'initialisation**
  3. Génération périodique **d'une nouvelle clé temporaire**
  4. Génération de **sous-clé (key mixing)**
- **Déconseillé dans la norme 802.11**

SOURCE: linkedin.com

Counter Mode CBC-MAC Protocol (CCMP)

- Remplacement de TKIP
- Chiffrement
  - Algorithme AES
  - Blocs et clés temporaires 128 bits
- Intégrité
  - IV unique
  - Code MAC (CBC-MAC)
- Spécification WPA2

CCMP (The Counter/CBC-MAC Protocol)

- **+ sûr** que le TKIP
- Se compose de **2 algorithmes** :
  1. Compteur de chiffrement **AES** (The Advanced Encryption Standard)
  2. Code **d'authentification des messages** (Cipher Block Chaining Message Authentication Code [CBC-MAC])
     - (Message Integrity Check [MIC])
- **Utilisé par le NIST** (U.S. National Institute of Standards and Technology) et le **gouvernement américain**
- Egalement très utilisée dans le **monde entier**
- Méthode de cryptage **la plus sécurisée**
- **Imposé sur la norme WPA2**

SOURCE: linkedin.com

Galois/Counter Mode Protocol (GCMP)

- En cours d'implémentation
- Chiffrement

  Algorithme AES 256
- Intégrité

  Code Galois
- Spécification WPA3

GCMP (Galois/Counter Mode Protocol)

- **+ sécurisé** et **plus efficace** que le CCMP
- Se compose de **deux algorithmes :**
  1. Chiffrement très rependu **AES** (The Advanced Encryption Standard)
  2. **Code d'authentification de message** (Galois Message Authentication Code [GMAC])
     - (Message Integrity Check [MIC])
- **Utilisé sur la norme WPA3**

SOURCE: linkedin.com

WPA, WPA2 ET WPA3

- « **Wi-Fi Alliance** » => http://wi-fi.org
- Certifications **WPA** (**W**i-Fi **P**rotected **A**ccess)
    1. **WPA** (Solution intermédiaire pour remplacer le WEP)
    2. **WPA2** (certifiée par l'Alliance Wi-Fi)
    3. **WPA3** (ajoute de meilleurs mécanismes de sécurité)
- **Le WPA3** propose un cryptage renforcé en s'appuyant sur le **chiffrement AES** (The **A**dvanced **E**ncryption **S**tandard) couplé avec le **protocole GCMP** (**G**alois/**C**ounter **M**ode **P**rotocol).
- **Le WPA3** utilise le **protocole PMF** (**P**rotected **M**anagement **F**rames)
- 2 modes **d'authentification client:**
    1. **La clé pré-partagée** (**P**re-**S**hared **K**ey [PSK])
       Mode Personnel
    2. **La norme 802.1x**
       Mode Entreprise

SOURCE: linkedin.com

Prise en charge de l'Authentification et du Cryptage	WPA	WPA2	WPA3
Authentification avec des clés pré-partagées ?	OUI	OUI	OUI
Authentification avec 802.1x?	OUI	OUI	OUI
Cryptage et MIC avec TKIP ?	OUI	NON	NON
Cryptage et MIC avec AES et CCMP ?	OUI	OUI	NON
Cryptage et MIC avec AES et GCMP ?	NON	NON	OUI

SOURCE: linkedin.com

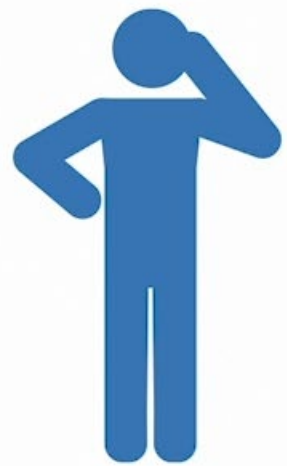
Niveaux de certification d'équipement

Certification	Apparition	Authentification	Norme
WPA	2004	TKIP	802.11i 802.1x possible
WPA2	2004-2005	CCMP + AES	802.11i 802.1x possible
WPA3	2018 – à présent	GCMP + Forward secrecy	802.1x possible

SOURCE: linkedin.com

TKIP

CCMP



WEP

EAP TLS

EAP

WPA 3

SOURCE: linkedin.com

Modes WPA

SOURCE: linkedin.com

- Mode WPA enterprise
- PEAP ou EAP-TLS
- WPA2 ou WPA3
- Clé à 14 caractères minimum

- WPA et WEP (bornes autonomes)
- Box opérateur

SOURCE: linkedin.com