PROJET ASSURMER

2025

AUTEURS :

DE CARVALHO LOPES Bruno
BELAHA Sidahmed
LE CLAINCHE Killian

DATE :

07/01/2025

I. La norme IEEE802.11

La norme **IEEE 802.11** est une norme définie par l'**Institute of Electrical and Electronics Engineers (IEEE)** pour les réseaux locaux sans fil (Wi-Fi). Elle spécifie les protocoles, les fréquences et les méthodes d'accès utilisées pour établir et gérer des connexions sans fil entre appareils.

1. Objectif et Portée

L'IEEE 802.11 vise à définir des mécanismes standardisés pour permettre des communications sans fil à courte portée dans un réseau local (WLAN). Les réseaux basés sur cette norme sont utilisés dans des environnements variés comme les maisons, les entreprises, les espaces publics, etc.

2. Structure Générale de la Norme

La norme est organisée en plusieurs sous-normes, désignées par des lettres (par exemple, 802.11a, 802.11b, 802.11g, etc.), chacune apportant des améliorations ou des spécifications pour des besoins particuliers.

Composants principaux :

- **Couche Physique (PHY)** : Définit les méthodes de transmission, comme la modulation et la fréquence.
- **Couche de Contrôle d'Accès au Médium (MAC)** : Gère l'accès au réseau, la sécurité, et les mécanismes d'accès partagés.

3. Évolution et Versions

Chaque version de la norme apporte des améliorations en termes de débit, portée, ou gestion du spectre. Voici les versions les plus importantes :

a) IEEE 802.11 (1997)

- Première version de la norme.
- Débit maximal de 2 Mbps.
- Utilise les bandes 2,4 GHz.

b) IEEE 802.11b (1999)

- Débit maximal de 11 Mbps.
- Fonctionne dans la bande 2,4 GHz.
- Large adoption en raison de son coût réduit.

c) IEEE 802.11a (1999)

- Débit maximal de 54 Mbps.
- Utilise la bande 5 GHz, réduisant les interférences.

- Moins populaire en raison de coûts plus élevés.

d) IEEE 802.11g (2003)

- Combine les avantages de 802.11a et 802.11b.
- Débit de 54 Mbps dans la bande 2,4 GHz.

e) IEEE 802.11n (2009)

- Introduit la technologie **MIMO** (Multiple Input Multiple Output).
- Débits théoriques jusqu'à 600 Mbps.
- Fonctionne sur les bandes 2,4 GHz et 5 GHz.

f) IEEE 802.11ac (2013)

- Débits allant jusqu'à 6,93 Gbps.
- Fonctionne principalement sur la bande 5 GHz.
- Introduit le concept de MU-MIMO (Multi-User MIMO).

g) IEEE 802.11ax (Wi-Fi 6, 2019)

- Optimisé pour les environnements à haute densité.
- Débits théoriques jusqu'à 9,6 Gbps.
- Fonctionne sur les bandes 2,4 GHz et 5 GHz (et parfois 6 GHz avec Wi-Fi 6E).
- Introduit l'OFDMA (Orthogonal Frequency Division Multiple Access) pour une meilleure gestion des ressources.

4. Bandes de Fréquences

La norme IEEE 802.11 utilise principalement deux bandes :

- **2,4 GHz** : Plus grande portée, mais sujet aux interférences (partagé avec d'autres appareils comme les micro-ondes).
- **5 GHz** : Plus rapide et moins sujet aux interférences, mais portée réduite.
- **6 GHz** (introduite avec Wi-Fi 6E) : Offrant davantage de canaux pour réduire la congestion.

5. Sécurité

La norme a évolué pour améliorer la sécurité :

- **WEP (Wired Equivalent Privacy)** : Premier mécanisme, aujourd'hui obsolète.
- **WPA (Wi-Fi Protected Access)** et **WPA2** : Introduisent des améliorations significatives en sécurité.
- **WPA3** : Dernière version offrant une sécurité accrue.

6. **Applications**

- **Domestiques** : Streaming, jeux en ligne, IoT.
- **Professionnelles** : Bureaux, entreprises, entrepôts.
- **Publics** : Hotspots Wi-Fi dans les cafés, aéroports, etc.

7. **Avantages et Limites**

Avantages :

- Facilité d'installation.
- Mobilité.
- Évolutivité avec les versions successives.

Limites :

- Interférences et congestion dans les bandes 2,4 GHz.
- Sécurité (si mal configurée ou avec des mécanismes obsolètes).
- Portée réduite comparée aux réseaux filaires.

II. Serveur RADIUS :

Le **serveur RADIUS** (Remote Authentication Dial-In User Service) est un protocole standardisé utilisé pour fournir des services d'authentification, d'autorisation et de comptabilité (AAA). Il est couramment utilisé dans les environnements réseau pour garantir un accès sécurisé aux ressources informatiques, comme le Wi-Fi, les VPN, ou d'autres services réseau.

A) Rôles principaux :

Authentification :
- Vérifie l'identité de l'utilisateur ou du périphérique via des identifiants (nom d'utilisateur, mot de passe, certificat).

Autorisation :
- Contrôle les droits d'accès, en permettant ou refusant l'accès aux ressources en fonction des règles définies.

Comptabilité :
- Suivi et enregistrement des sessions utilisateur (durée, adresse IP utilisée, données échangées, etc.).

B) Fonctionnement général :

- **Lorsqu'un utilisateur tente de se connecter à un réseau sécurisé (par exemple, une borne Wi-Fi configurée), le périphérique client envoie une requête au client RADIUS (borne Wi-Fi, contrôleur).**
- **Le client RADIUS relaie la requête d'authentification au serveur RADIUS.**
- **Le serveur RADIUS valide l'identité de l'utilisateur en se basant sur une base de données locale ou distante (par exemple, un annuaire LDAP ou Active Directory).**
- **Si l'authentification réussit, le serveur RADIUS renvoie une réponse d'autorisation au client RADIUS, permettant l'accès au réseau.**

1. Fonctionnement de RADIUS

Le serveur RADIUS fonctionne selon un processus bien défini basé sur les principes AAA : **Authentification**, **Autorisation**, et **Comptabilité**.

A) Les rôles dans l'architecture RADIUS :

Client RADIUS :

- Un périphérique réseau (ex. borne Wi-Fi, routeur, switch) qui relaie les demandes d'accès des utilisateurs au serveur RADIUS.

Serveur RADIUS :
- Valide les informations d'identification des utilisateurs et renvoie une réponse (acceptation ou rejet).

Base de données des utilisateurs :
- Contient les informations nécessaires pour authentifier et autoriser les utilisateurs (ex. Active Directory, LDAP, fichier local).

B) Processus de communication RADIUS

Demande d'accès :

- L'utilisateur tente de se connecter au réseau sécurisé via un périphérique (ordinateur, smartphone, etc.).
- Les informations d'identification (nom d'utilisateur, mot de passe, ou certificat) sont envoyées au **client RADIUS**.

Transmission de la requête :

- Le client RADIUS encapsule ces informations dans un **paquet RADIUS** et l'envoie au serveur RADIUS via un canal sécurisé (UDP généralement sur les ports 1812 ou 1645).

Validation des informations :

- Le serveur RADIUS vérifie les informations reçues en interrogeant une **base de données** (locale ou distante).
  - Si les identifiants sont corrects, le serveur RADIUS génère une réponse d'**acceptation**.
  - Si les identifiants sont incorrects ou manquent, une réponse de **rejet** est renvoyée.

Autorisation :

- En cas d'acceptation, le serveur RADIUS peut transmettre des **paramètres d'autorisation** spécifiques (ex. VLAN assigné, temps de session maximum).

Connexion établie :

- Le client RADIUS applique les paramètres transmis et permet ou bloque l'accès au réseau.

Comptabilité (optionnelle) :

- Une fois la session établie, le client RADIUS peut envoyer des rapports sur l'utilisation du réseau au serveur RADIUS (ex. durée, données consommées).

2. Sécurisation des échanges

- Les paquets RADIUS sont protégés par une **clé secrète partagée** entre le client et le serveur.
- Lorsque des protocoles comme **EAP-TLS** sont utilisés, des certificats numériques assurent une authentification forte et chiffrée.

3. Certificats et Sécurisation

A) Rôle des certificats dans l'authentification

Un **certificat numérique** est un document électronique délivré par une autorité de certification (CA) qui permet de garantir l'identité des entités (serveurs ou utilisateurs).

- **Objectifs principaux des certificats :**
  - **Authentification mutuelle :** Vérification des identités entre le client et le serveur.
  - **Chiffrement des échanges :** Protection des données transmises contre toute interception.
  - **Établissement de la confiance :** Validation par une autorité de certification reconnue.
- **Composants principaux d'un certificat :**
  - Le nom de l'entité (ex. le serveur RADIUS ou l'utilisateur).

- La clé publique pour le chiffrement.
- Une signature numérique de l'autorité de certification.

B) Protocoles d'authentification sécurisée utilisés avec RADIUS

RADIUS peut utiliser différents protocoles d'authentification sécurisée reposant sur les certificats. Voici les plus courants :

EAP-TLS (Transport Layer Security):
- Basé sur un certificat délivré à la fois au client (utilisateur) et au serveur.
- Offre une authentification forte grâce à l'échange de certificats.
- Avantage : Très sécurisé, mais nécessite une infrastructure à clé publique (PKI).

PEAP (Protected EAP) :
- Encapsule les échanges dans un tunnel TLS sécurisé.
- Nécessite un certificat uniquement pour le serveur RADIUS.
- Avantage : Réduit la complexité tout en offrant une bonne sécurité.

EAP-TTLS (Tunneled TLS) :
- Similaire à PEAP, mais plus flexible en supportant des méthodes d'authentification héritées (ex. identifiants simples).
- Utilisé lorsque des certificats clients ne sont pas pratiques à déployer.

C) Étapes pour la sécurisation avec des certificats

Émission des certificats :
- Les certificats sont générés par une autorité de certification (CA).
- Le serveur RADIUS reçoit un certificat pour établir sa légitimité auprès des clients.
- Les utilisateurs (ou périphériques) peuvent également recevoir des certificats pour une authentification mutuelle (dans le cas d'EAP-TLS).

Configuration du serveur RADIUS :
- Importation du certificat délivré par la CA.
- Configuration pour utiliser un protocole comme EAP-TLS ou PEAP.

Configuration des clients :
- Installation de la CA racine pour valider le certificat du serveur.
- Configuration des clients pour exiger une connexion sécurisée via le serveur RADIUS.

Échanges sécurisés :
- Lorsqu'un utilisateur tente de se connecter, un tunnel chiffré est établi grâce au certificat du serveur.
- Les données d'authentification sont transmises dans un format sécurisé, empêchant les attaques par interception.

4. **Sécurisation supplémentaire avec les clés partagées**

- En plus des certificats, les paquets RADIUS utilisent une **clé secrète partagée** entre le client RADIUS (par exemple, une borne Wi-Fi) et le serveur RADIUS.
- Cette clé garantit que seuls les périphériques autorisés peuvent interagir avec le serveur.

A) Avantages de l'utilisation des certificats

Sécurité accrue :
- Les certificats réduisent considérablement les risques de vol d'identité ou de mots de passe.

Confiance renforcée :
- Les certificats délivrés par une CA reconnue établissent une confiance entre les entités.

Chiffrement des données sensibles :
- Toutes les communications sont protégées contre l'interception et la modification.

III. Etude comparative des différents protocoles de sécurité wifi

1. Introduction

Le Wi-Fi est une technologie omniprésente qui connecte des milliards d'appareils dans le monde. Cependant, sa nature sans fil l'expose à des risques importants, notamment :

- **Intrusions non autorisées** : Accès à un réseau par des attaquants non légitimes.
- **Vol de données** : Interception des communications entre un appareil et le point d'accès.
- **Déni de service (DoS)** : Saturation du réseau par des attaquants.

Cette étude vise à analyser et comparer les principaux protocoles de sécurité Wi-Fi pour identifier les options les plus adaptées selon les besoins spécifiques.

2. Protocoles de sécurité Wi-Fi analysés

Les protocoles Wi-Fi ont évolué au fil des ans pour répondre aux nouvelles menaces :

WEP (Wired Equivalent Privacy) : Premier protocole standardisé pour la sécurité des réseaux Wi-Fi.

WPA (Wi-Fi Protected Access) : Une solution transitoire pour corriger les failles de WEP.

WPA2 (Wi-Fi Protected Access 2) : Une amélioration majeure apportant des algorithmes de chiffrement robustes.

WPA3 (Wi-Fi Protected Access 3) : Le protocole actuel, conçu pour offrir une sécurité avancée adaptée aux nouveaux usages.

3. Critères de comparaison

Voici les critères d'analyse retenus pour cette étude :

Chiffrement et authentification : Algorithmes et processus utilisés pour sécuriser les données.

Vulnérabilités connues : Failles d'exploitation publiées ou détectées.

Performance : Impact sur les ressources matérielles et la vitesse de transmission.

Compatibilité : Prise en charge par les appareils récents et anciens.

Facilité de mise en œuvre : Simplicité pour les utilisateurs finaux ou les administrateurs.

Cas d'utilisation recommandé : Contextes où le protocole est le plus pertinent.

4. Analyse détaillée des protocoles

A) WEP (Wired Equivalent Privacy)

- **Résumé historique** : Introduit en 1997 avec la norme IEEE 802.11 pour offrir une sécurité équivalente à celle des réseaux filaires.
- **Technologie utilisée** :
    - Chiffrement basé sur RC4.
    - Longueur des clés : 40 bits (standard) ou 104 bits (amélioré).
    - Utilisation d'un vecteur d'initialisation (IV) de 24 bits.
- **Forces** :
    - Compatibilité étendue, même sur les équipements très anciens.
    - Facile à configurer.
- **Faiblesses** :
    - Le chiffrement RC4 est obsolète et vulnérable.
    - Le vecteur d'initialisation est trop court, entraînant des collisions fréquentes.
    - Vulnérabilités : FMS (Fluhrer, Mantin et Shamir), cracking rapide avec des outils comme Aircrack-NG.
- **Statut actuel** : Complètement abandonné par la Wi-Fi Alliance et déconseillé dans tous les cas.

B) WPA (Wi-Fi Protected Access)

- **Résumé historique** : Introduit en 2003 comme une solution temporaire à WEP.
- **Technologie utilisée** :
    - Chiffrement TKIP (Temporal Key Integrity Protocol) basé sur RC4.
    - Mise à jour dynamique des clés pour empêcher les attaques de rejouement.
- **Forces** :
    - Corrige certaines failles de WEP, notamment les collisions d'IV.
    - Relativement facile à déployer sur les équipements WEP avec mise à jour logicielle.
- **Faiblesses** :
    - Le protocole RC4 reste faible par conception.
    - Vulnérable à des attaques comme Michael (exploit des checksum) et attaques par dictionnaire.

- **Vulnérabilités majeures** :
    - Vulnérable aux attaques par brute force sur le protocole PSK (Pre-Shared Key).
    - Man-in-the-Middle et attaques par replay possibles.
- **Statut actuel** : Obsolète, bien que toujours en usage sur des équipements anciens.

C) WPA2 (Wi-Fi Protected Access 2)

- **Résumé historique** : Standard depuis 2004, introduisant des améliorations majeures.
- **Technologie utilisée** :
    - Chiffrement AES (Advanced Encryption Standard) avec CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).
    - Deux modes d'utilisation : **PSK** (clé partagée) pour les environnements domestiques et **EAP** (Extensible Authentication Protocol) pour les entreprises.
- **Forces** :
    - Protection contre les attaques par replay.
    - AES est une norme de chiffrement robuste et largement adoptée.
    - Adapté aux environnements professionnels et domestiques.
- **Faiblesses** :
    - Vulnérable à certaines attaques (exemple : KRACK - Key Reinstallation Attack, découvert en 2017).
    - Les clés PSK faibles (courtes ou simples) peuvent être crackées via brute force.
- **Statut actuel** : Toujours utilisé, mais en transition vers WPA3.

D) WPA3 (Wi-Fi Protected Access 3)

- **Résumé historique** : Lancement en 2018 pour répondre aux failles de WPA2.
- **Technologie utilisée** :
    - Chiffrement renforcé basé sur SAE (Simultaneous Authentication of Equals).
    - Chiffrement individualisé pour chaque session utilisateur (chiffrement opportuniste).
    - Améliorations pour les appareils IoT via Wi-Fi Easy Connect.
- **Forces** :
    - Résistance accrue aux attaques par force brute (avec SAE, une attaque réussie nécessite d'attaquer chaque mot de passe individuellement).

- Protection contre les attaques de désauthentification.
- Adapté aux environnements modernes (domotique, IoT).

- **Faiblesses** :
  - Moins de compatibilité avec les anciens appareils.
  - Coût potentiellement plus élevé pour la mise à niveau des infrastructures.
- **Statut actuel** : Recommandé pour toutes les nouvelles installations.

5. Tableau comparatif

Protocole	Année	Chiffrement	Forces	Faiblesses	Statut actuel
WEP	1997	RC4	Simplicité, Compatibilité	Extrêmement vulnérable	Abandonné
WPA	2003	TKIP/RC4	Corrige WEP, clé dynamique	Faible sécurité, attaques possibles	Dépassé
WPA2	2004	AES/CCMP	Sécurité fiable, largement adopté	Vulnérabilités comme KRACK	Standard courant
WPA3	2018	AES/SAE	Sécurité avancée	Compatibilité limitée, plus coûteux	Standard recommandé

6. Conclusion

- **WEP** et **WPA** sont à éviter en raison de leur obsolescence et de leur faible sécurité.
- **WPA2** reste adapté à de nombreux contextes, mais il est impératif de l'utiliser avec des mots de passe robustes et de déployer des correctifs pour les vulnérabilités connues (ex. KRACK).
- **WPA3** est la meilleure option pour les nouvelles installations, offrant des améliorations substantielles en termes de sécurité et d'efficacité.