Caractéristiques principales :

Interopérabilité

Les normes IEEE 802.11 garantissent une interopérabilité entre les équipements de différents fabricants certifiés par la Wi-Fi Alliance.

Portée

Varie en fonction des conditions environnementales et des bandes utilisées (environ 30 à 90 mètres en intérieur pour 2,4 GHz).

Applications

Réseaux domestiques, réseaux d'entreprise, lieux publics (hôtels, cafés, aéroports), et IoT (Internet des objets).

Conclusion

IEEE 802.11 est une norme essentielle pour les communications sans fil modernes. Ses évolutions successives répondent aux besoins croissants en termes de vitesse, d'efficacité et de sécurité, rendant le Wi-Fi omniprésent dans les environnements personnels et professionnels.

3. Etude comparative des différents protocoles de sécurité WIFI

3.1. Comparaison synthétique des protocoles

Protocole	Algorithme de chiffrement	Points forts	Points faibles	Statut actuel
WEP	RC4	Simple, universel à l'époque	Très faible sécurité, facilement cassable	Obsolète
WPA	RC4 + TKIP	Amélioration de WEP, dynamique	Vulnérable aux attaques modernes	Dépassé
WPA2	AES	Sécurisé, largement adopté	Failles comme KRACK	Standard courant
WPA3	AES + SAE	Très sécurisé, protection des réseaux ouverts	Compatibilité limitée	Standard recommandé

Les protocoles de sécurité Wi-Fi sont conçus pour protéger les données transmises sur un réseau sans fil et empêcher tout accès non autorisé. Voici une comparaison des principaux protocoles utilisés depuis la naissance du Wi-Fi.

3.2. WEP (Wired Equivalent Privacy)

Introduit en 1997 (avec IEEE 802.11).

Caractéristiques principales :
Utilise une clé de chiffrement RC4 de 40 ou 104 bits.
Les clés sont statiques (ne changent pas automatiquement).
Simple à configurer mais peu sécurisé.

Forces :
Compatibilité universelle avec les premiers équipements Wi-Fi.
Facile à configurer.

Faiblesses :
Vulnérabilités majeures dues à la répétition des clés IV (Initialization Vectors).
Le chiffrement RC4 est obsolète et facilement cassé.
Peut être compromis en quelques minutes à l'aide d'outils gratuits.

Statut actuel :
Déprécié et déconseillé.

3.3. WPA (Wi-Fi Protected Access)

Introduit en 2003.

Caractéristiques principales :
Utilise le protocole TKIP (Temporal Key Integrity Protocol) pour le chiffrement.
Introduction d'une vérification d'intégrité pour détecter les modifications non autorisées des données.
Amélioration du chiffrement dynamique par rapport à WEP.

Forces :
Compatibilité avec les anciens équipements Wi-Fi via une mise à jour.
Introduit des clés temporaires pour chaque session.

Faiblesses :
TKIP reste basé sur RC4, ce qui le rend vulnérable aux attaques modernes.
Moins sécurisé que les versions ultérieures comme WPA2.

Statut actuel :
Remplacé par WPA2.

3.4. WPA2 (Wi-Fi Protected Access 2)

Introduit en 2004.

Caractéristiques principales :
Utilisation obligatoire de l'algorithme de chiffrement AES (Advanced Encryption Standard).

Supporte deux modes :
Personnel (PSK) : Basé sur une clé partagée, pour les réseaux domestiques.
Entreprise (EAP) : Authentification basée sur un serveur RADIUS, pour les environnements professionnels.

Forces :
AES est beaucoup plus sécurisé que RC4.
Compatible avec presque tous les équipements récents.
Fiabilité et sécurité accrues par rapport à WPA.

Faiblesses :
Vulnérable à des attaques spécifiques (exemple : KRACK en 2017, une faille dans le protocole de négociation des clés).

Statut actuel :
Standard largement utilisé pour la sécurité Wi-Fi.

3.5. WPA3 (Wi-Fi Protected Access 3)

Introduit en 2018.

Caractéristiques principales :
Protège contre les attaques par force brute grâce au protocole SAE (Simultaneous Authentication of Equals).
Chiffrement des données même sur les réseaux ouverts (OWE, Opportunistic Wireless Encryption).
Introduit le 192-bit security suite pour les environnements professionnels nécessitant une sécurité élevée.

Forces :
SAE empêche la réutilisation des clés et renforce la sécurité des mots de passe faibles.
Protection accrue contre les attaques passives et actives.
Compatibilité avec les anciens équipements en mode transition WPA2/WPA3.

Faiblesses :
Pas encore universellement adopté (nécessite des équipements compatibles).
Les attaques de type downgrade (forcer un passage à WPA2) peuvent encore exister si les deux protocoles sont activés.

Statut actuel :
Recommandé pour les nouveaux réseaux, en particulier dans les environnements critiques.

4. Présentation du fonctionnement d'une solution RADIUS et certificats

Le protocole RADIUS (Remote Authentication Dial-In User Service) centralise l'authentification, l'autorisation, et la gestion des comptes d'accès dans un réseau. Il est souvent utilisé pour sécuriser l'accès Wi-Fi dans des environnements professionnels.