Dossier de projet n°9 :

Mise en place d'une solution Wi-Fi sécurisée

Dylan CHAU
Axel BAUGÉ

2A-SISR

ASSURMER

Date de création : 17/01/2023
Version : 1.0
Pour validation : DSI
A destination : DSI
Mode de diffusion : Intranet Nombre de pages : 86

Métadonnées

Diff ısion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau et Axel Baugé	1.0	Initialisation du document

Validation			
Rédacteur		Validateur	
Nom	Date	Nom	Date
Dylan Chau et Axel Baugé	14/02/2023	DSI	14/02/2023
Date d'application : 14/02/2023			

Table des matières

1. Qu'est-ce que le Wi-Fi ?

Le Wi-Fi (de l'anglais Wireless Fidelity) est une technologie de réseau sans fil permettant aux périphériques tels que les ordinateurs, les périphériques mobiles et les équipements divers (imprimantes, caméras) d'accéder à Internet mais également de communiquer entre eux sans besoin de connexion filaire.

Cette technologie permet la transmission de données grâce des ondes électromagnétiques et radioélectriques en haut-débit garantissant une liberté de mouvement au sein de la zone couverte par le réseau sans fil.

L'appellation Wi-Fi est à la base une marque déposée qui, à l'origine, désignait le nom de la certification donnée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), organisme ayant pour mission de spécifier l'interopérabilité entre les matériels conformes à la norme 802.11 et de vendre le label « Wi-Fi » aux matériels répondant à ses spécifications.

Plus simple à retenir, le nom Wi-Fi est désormais aussi utilisé dans la vie de tous les jours pour désigner un réseau répondant la norme IEEE 802.11. Dans certains pays, on utilise également le terme « WLAN ».

2. Les composantes

a) La porteuse

Afin de transporter les ondes électromagnétiques, il est nécessaire d'utiliser une « porteuse ». L'onde est modifiée pour transporter et transmettre l'information et sert de fondement à la communication sans fil entre un appareil et un réseau WiFi. Elle permet ainsi d'encoder les données à transmettre, en modulant la fréquence ou l'amplitude, où différentes valeurs du signal représentent différentes données numériques.

La porteuse, avec une fréquence spécifique (Le plus souvent en GHz : nombre de périodes du signal pendant une seconde), est essentielle pour la transmission et la réception efficaces des données dans un environnement Wi-Fi.

Plus la fréquence est élevée, plus le débit que l'on souhaite obtenir pourra être élevé.

b) L'antenne

Afin de guider la porteuse, il est nécessaire d'avoir un guide d'ondes, que l'on désigne par le terme « antenne ».

Elle est utilisée pour émettre, mais aussi de réceptionner les ondes électromagnétiques. Divers types de données, y compris des informations informatiques peuvent alors être transmises. Cette capacité permet une utilisation quotidienne plus flexible sans nécessité d'une connexion filaire.

Selon sa forme et sa longueur, les ondes sont diffusées de différentes manières. Les deux types d'antennes Wi-Fi les plus courants sont les modèles :

- Omnidirectionnels (couverture à 360°), très répandues.
    - Dipôle (En tige, sur certains équipements comme les caméras)
    - Colinéaire (Sur les toits)
    - Patch (Principalement dans les smartphones)
- Directionnels (faisceau focalisé).

c) Les normes

Afin d'assurer l'interopérabilité entre les différents systèmes équipés de carte WiFi, la norme IEEE802.11 établit les bases des réseaux Wi-Fi.

Elle introduite pour la première fois en 1997 par l'Institut des Ingénieurs électriciens et électroniciens (IEEE). Elle a révolutionné la manière dont nous accédons à Internet en permettant la connexion sans fil à des réseaux locaux. Elle permet de choisir une fréquence porteuse entre 14 canaux différents afin de réduire les interférences, optimiser l'utilisation de la bande-passante et la flexibilité dans des environnements denses.

Depuis sa création, elle a connu de nombreuses évolutions afin d'être amélioré en termes de vitesse de transmission, portée et sécurité des connexions sans fil.

Tableau récapitulatif des principales normes IEEE 802.11 utilisées :

IEEE 802.11n (Wi-Fi 4)	Introduit en 2009, le Wi-Fi 4 a permis de supporter les bandes de fréquences de 2,4 GHz et 5 GHz et introduire le Multiple Input Multiple Output (MIMO) afin d'améliorer la vitesse de transmission et réduire les erreurs. Avec des débits pouvant atteindre 600 Mbit/s, cette norme a permis une utilisation plus large des réseaux WLAN en remplacement des réseaux filaires.
IEEE 802.11ac (Wi-Fi 5)	Lancée en 2013, la norme Wi-Fi 5 a permis d'atteindre des débits allant jusqu'à 3,5 Gbit/s grâce à une bande passante plus large, l'ajout de canaux supplémentaires, une meilleure modulation, et l'extension des capacités MIMO. Cette norme a fonctionné exclusivement sur la bande des 5 GHz, offrant ainsi des vitesses gigabit et réduisant les interférences avec d'autres appareils.
IEEE 802.11ax (Wi-Fi 6)	Le Wi-Fi 6, publié en 2021, se concentre sur l'amélioration de l'efficacité spectrale et la gestion de la densité du réseau. Bien que sa vitesse théorique atteigne 9,6 Gbit/s, l'objectif principal de cette norme est de gérer efficacement le trafic dans des zones à forte densité de Wi-Fi, grâce à des mécanismes multi-utilisateurs et à l'amélioration de la portée et de la consommation d'énergie pour les opérations extérieures.
IEEE 802.11be (Wi-Fi 7)	Le Wi-Fi 7 lancé en 2024 représente la norme la plus récente, prévu pour offrir des vitesses quatre fois plus rapides que le Wi-Fi 6, avec des débits théoriques d'environ 40 Gbit/s. Cette norme promet également de doubler la largeur de bande à 320 MHz et d'apporter des améliorations significatives en termes de latence, de prise en charge des appareils et de performances dans des environnements Wi-Fi encombrés.

Les bornes Wi-Fi d'ASSURMER fonctionnent avec les normes IEEE 802.11n et 802.11ac.

3. Les protocoles de sécurité Wi-Fi : étude comparative

Afin d'assurer la protection du réseau en matière de Wi-Fi, les données qui transitent entre deux machines d'un même réseau sont chiffrées à l'aide de protocoles de sécurité.

Pour rendre les réseaux sans fil plus sûrs et plus efficaces, ces protocoles font régulièrement l'objet de modifications et mises à jour pour faire face à de nouvelles failles de sécurité.

Ainsi, plusieurs protocoles de sécurité ont été développés et sont WEP, WPA, WPA2, WPA3. Ils ont le même objectif, mais leur fonctionnement est bien différent.

WEP (Wired Equivalent Privacy)

Introduit en 1999, le WEP a été la première solution de chiffrement pour protéger les réseaux Wi-Fi.

Fonctionnement : Le protocole utilise l'algorithme de chiffrement RC4 pour l'authentification et le chiffrement. Elle combine une clé de chiffrement prédéfinie de 64 bits ou 128 bits avec un vecteur d'initialisation (IV) de 24 bits pour renforcer le chiffrement.

Sécurité : Considéré comme faible en raison de la petite taille de l'IV et de la gestion des clés statiques qui permet un échange avec une clé unique, elle rend le réseau vulnérable aux attaques. L'information transite en clair sur le réseau. En raison des nombreuses failles que le WEP présente, il a été abandonné depuis 2004. En outre, il est très facile de casser la clé WEP avec aircrack-ng.

WPA (Wi-Fi Protected Access)

Régi par la norme IEEE802.11i et introduit en 2003, le WPA est une amélioration du WEP en corrigeant la majorité de ses problèmes.

Fonctionnement : Le protocole introduit l'utilisation du protocole TKIP (Temporal Key Integrity Protocol) pour améliorer la sécurité par rapport au WEP. TKIP utilise des clés de 256 bits, le mélange de clés par paquet, et une vérification d'intégrité du message. Le protocole WPA dispose également de 2 modes de fonctionnement : WPA-Personal et WPA-Enterprise, proposant ainsi 2 méthodes d'authentification différente, PSK (Pre-Shared Key) et EAP (Extensible Authentication Protocol).

Sécurité : Plus sûr que le WEP, TKIP est également considéré comme vulnérable en raison de son utilisation continue de l'algorithme RC4 et de sa rétrocompatibilité avec WEP.

WPA2

Introduit en 2004, le WPA2 est une amélioration du WPA et suit la continuité de la norme IEEE802.11i.

Fonctionnement : L'amélioration la plus significative est le remplacement du RC4/TKIP par l'AES (Advanced Encryption Standard) qui est un protocole de chiffrement symétrique et CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), offrant une meilleure sécurité et intégrité des données. Le WPA2 utilise AES, mais peut également utiliser TKIP pour une rétrocompatibilité (pour qu'il puisse accepter les connexions WPA). Il propose également les 2 modes de fonctionnement du WPA.

Sécurité : Considéré comme très sécurisé, le protocole a été compromis en 2017 par la vulnérabilité KRACK (Key Reinstallation Attacks) qui exploitait une faiblesse dans la procédure de handshake quatre voies.

WPA3

Introduit en 2018 et en réponse à la vulnérabilité KRACK, il s'agit du successeur du WPA2, introduisant des fonctionnalités et une couche de sécurité supplémentaire à la fois pour l'usage personnel et pour les entreprises.

Fonctionnement : Le protocole ajoute une meilleure protection contre les attaques par force brute grâce au protocole SAE (Simultaneous Authentication of Equals) basé sur Diffie–Hellman key exchange et utilise un chiffrement individuel des données avec des clés plus longues (jusqu'à 256 bits pour le mode entreprise).

Sécurité : Considéré comme le protocole le plus sécurisé à ce jour, il adresse les faiblesses des protocoles précédents et offre des protections supplémentaires contre les attaques modernes. Malheureusement, une faille (Dragonblood) a déjà mis à mal ce protocole sans pour autant le condamner.

Tableau récapitulatif :

Protocole	Chiffrement	Authentification	Remarques
WEP	RC4 (64 ou 128 bits)	Clés statiques	Facilement piratable, désormais considéré comme obsolète.
WPA (Personal et Enterprise)	TKIP (128 bits)	PSK ou EAP	Plus sûr que le WEP, néanmoins vulnérable à des attaques par « injection de paquets ».
WPA2 (Personal et Enterprise)	AES (128 ou 256 bits)	PSK ou EAP	Standard actuel, offre une bonne sécurité et performance, vulnérable à KRACK.
WPA3	AES (192 ou 256 bits)	SAE	Plus sécurisé, protège contre les attaques par force brute, encore émergent.

Pour un dispositif moderne, il est recommandé d'utiliser WPA2 ou WPA3 pour assurer une sécurité optimale du réseau Wi-Fi.

WPA2 est actuellement le protocole le plus répandu et supporté par la plupart des appareils, tandis que WPA3 offre une meilleure sécurité nécessitant du matériel compatible plus récent (Obligatoire sur les équipements Wifi 6).

/!\ WEP et WPA sont considérés comme moins sécurisés et doivent être évités absolume