Présentation d’une borne WI-FI

Auteur : Arthur GUILET
Reference : Assurmer
Date : 07/09/2022

DIFFUSION et VISAS

Diffusion				
Société / Entité	**Destinataires**	**Fonction**	**Diffusion**	**Pour info**
Assumer	Service IT	Présentation	Réseau	

Visas			
Société/Entité	**Nom**	**Fonction**	

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de pages
V1.0	11/01/2023	Arthur GUILET	Présentation du WI-FI	6

COORDONNEES

Contacts		
Nom	**E-mail**	**Téléphone**
Arthur GUILET	arthur.guilet@assurmer.fr	01.54.23.79.02

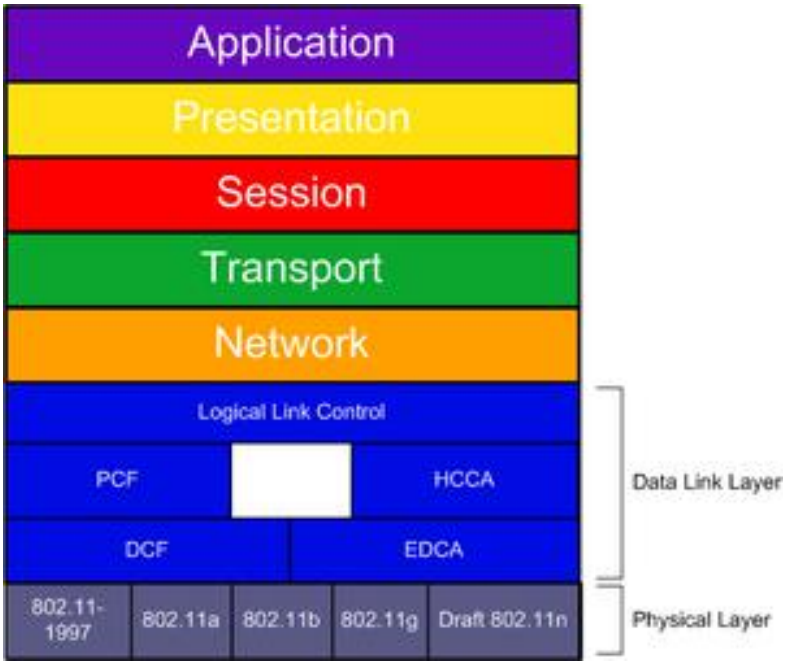
Table des matières

Le WI-FI

Le Wi-Fi est un ensemble de protocoles de communications sans-fil, avec la IEEE802.11ax (Wi-Fi 6 et 6E) pour la plus répandue et le plus récent février 2021. Il se base sur une des fréquences variables elle débute à 1GHz et peut monter jusqu'à 7Ghz, cette norme utilise

Du fait qu'il permet l'échange de données sur un réseau, il est devenu très vite nécessaire de le sécuriser. Ainsi est apparu le premier protocole de sécurisation par mot de passe d'un réseau Wi-FI en 1999 : le WEP. La plupart des protocoles se reposent sur un cryptage de la connexion au réseau par un mot de passe.

La norme 802.11 dans le modèle OSI



Le WEP

Le WEP est la première solution de cryptage de réseau Wi-Fi apparu en 1999. Il a été vite remplacé car il souffrait de nombreuses failles de sécurités. Son fonctionnement reposait sur l'utilisation d'une clé de 64, ou 128 bits. Ainsi, à l'heure actuelle il faut moins de 2 minutes pour cracker une clé WEP grâce à des outils spécialisés comme aircrack-ng.

Le WPA

Le WPA, apparu en 2003, est le successeur direct du WEP. Il est beaucoup plus efficace en termes de cryptage et évolutif dans son fonctionnement. Comme son prédécesseur il se base sur une clé 128 bits. Il fonctionnait avec un système dit de TKIP, qui est une méthode de cryptage qui mélange des paquets pour après les remettre dans l'ordre. Le TKIP a été instauré afin de ne pas rendre obsolète le matériel WEP. Cette méthode présentait de nombreuses failles dont une majeure découverte en 2008 permettant de pirater un réseau en moins de 15 minutes.
Le mode de fonctionnement du WPA le plus répandu est le WPA-Personnel (WPA-PSK), qui est le WPA destiné à un usage personnel ou de petite entreprise. Ici le mot de passe wifi est le même pour tous les utilisateurs et est stocké sur la machine cliente.
On le distingue du WPA-Enterprise (ou MGT) qui est relié à un serveur RADIUS permettant l'utilisation du plusieurs identifiants pour s'identifier.

Le WPA2

Évolution directe du WPA parue en 2004, le WPA2 remplace le TKIP par l'AES qui est un algorithme de chiffrement dis symétrique considéré comme plus performant et sécurisé que son prédécesseur. Cependant, le WPA2 peut aussi fonctionner en TKIP pour assurer une rétrocompatibilité et repose toujours sur une clé en 128 bits.
Le mode de fonctionnement du WPA2 le plus répandu est le WPA2-Personnel (WPA2-PSK), comme son prédécesseur l'authentification se déroulera alors grâce à une clé unique à tous les clients.
On le distingue lui aussi de son homologue catégorisé entreprise : le WPA2Enterprise, qui consiste lui aussi à utiliser un serveur d'authentification RADIUS qui permet d'autoriser ou non la connexion.
Le dispositif WPA2 possède lui aussi des failles dont la majeure nommée Krack découverte en 2016.

Le WPS

Le WPS n'est pas un standard à proprement parler, il a été instauré en 2007 et est un standard permettant de se connecter plus facilement aux réseaux WiFi sans entrer le mot de passe PSK. Le WPS se déclinait en 4 modes : le code PIN, le PBC (un bouton à appuyer sur le routeur et le client), le NFC, ou un branchement USB.
Cependant, 4 ans après de grave vulnérabilité ont été trouvée liées au WPS, permettant des piratages rapides. Il est conseillé de désactiver ce protocole.

Le WPA3

Afin de corriger la faille présente dans le WPA2, le WPA3 a été créé par la Wi-Fi Alliance en 2018. Il suppose un changement radical dans la sécurisation de l''authentification tout en gardant le principe d'unicité du mot de passe. Un des principaux problèmes liés au Wi-Fi auparavant étant la facilité d'effectuer des attaques par dictionnaire, le WPA3 instaure le remplacement du PSK par le SAE car il oblige aux attaquant de ne pouvoir faire qu'un seul essai de mot de passe hors ligne. Ainsi, si un attaquant veut faire du brute-force il devra être à proximité du réseau Wi-Fi et pourra se faire bloquer par le routeur. Une autre innovation implémentée est l'IDP, mettant en place une clé unique par clients, permettant aux clients de voir leur donnée protégée même si un attaquant récupère la clé. Enfin, le WPA3 met fin aux réseaux ouvert en mettant en place un chiffrement systématique grâce au système d'OWE. Enfin, le WPA3 instaure un successeur au WPS, le DPP, ce successeur corrige toutes les vulnérabilités du WPS.
Comme ses prédécesseurs, le WPA3 se décline en deux utilisations, la personnelle se basant sur une clé de chiffrement en 128 bits qui peut optionnellement être passée en 192 bits et la version Entreprise qui impose l'utilisation d'une clé en 192 bits.
Bien que le WPA3 soit extrêmement récent et très peu répandu, des failles ont déjà été trouvées en 2019 comme la Dragonblood.

La comparaison

	Cryptologie	Authentification
WPA-Personnel	Basée sur le TKIP, avec une clé en 128 bits	Par une clé unique pour tous les clients en utilisant le protocole PSK
WPA2-Personnel	Basée sur le protocole AES, avec une clé en 128 bits	Par une clé unique pour tous les clients en utilisant le protocole PSK
WPA-Enterprise	Basée sur le TKIP, avec une clé en 128 bits	Par un serveur d'authentification, permettant à chaque client d'avoir son mot de passe
WPA2-Enterprise	Basée sur le protocole AES, avec une clé en 128 bits	Par un serveur d'authentification, permettant à chaque client d'avoir son mot de passe
WPA3	Basée sur le protocole AES, avec une clé en 128 bits voir 196 bits	Par une clé unique pour tous les clients en utilisant le protocole SAE