Technologies sans fils

PREAMBULE

Ce cours vous présente les différents réseaux sans fils avec les problématiques rencontrées et les solutions utilisées. Il aborde également l'internet des objets via les différentes offres du marché.

Pour mettre en œuvre le tutoriel sur le wifi 802.1x, je vous invite à lire les cours Windows, et authentification et chiffrement.

Réseaux personnels sans fils (pwan)

Le réseau personnel sans fils (Wireless Personal Area Network) concerne les réseaux de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, PDA…) à un ordinateur ou bien à permettre la liaison sans fils entre deux machines très peu distantes.

- Le **ZigBee** (IEEE 802.15.4) permet d'obtenir des liaisons sans fils faible prix et faible consommation d'énergie, il est utilisé dans les petits appareils électroniques (appareils électroménagers, hifi, jouets…)
- L'**infrarouge** Cette technologie est largement utilisée pour les télécommandes. L'association irDA (infrared data association) s'occupe de la normalisation.
- **Bluetooth** (802.15) Ce standard est basé sur un mode de fonctionnement maître/esclave. Son objectif principal est de relier entre eux des périphériques (imprimantes, téléphones portables, appareils domestiques, oreillettes, souris, clavier, etc.) sans utiliser de liaison filaire.

Réseaux Métropolitains sans fils (MWAN)

Le réseau métropolitain sans fils (Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio. La BLR est principalement une technologie utilisée par les opérateurs de télécommunication.

Le **WiMAX (802.16)** s'adresse notamment au marché des réseaux métropolitains, mais elle est là également pour couvrir la zone dite du « dernier kilomètre », c'est-à-dire fournir un accès à internet haut débit aux zones non couvertes par les technologies filaires classiques (lignes xDSL, câble ou encore les lignes spécialisées) Une autre possibilité consiste à utiliser le WiMAX comme réseau de collecte entre des réseaux locaux sans fils.

Les réseaux étendus sans fils WWAN

Ces technologies sont surtout utilisées dans le cadre de la téléphonie mobile.

- **GSM** (Global System for Mobile Communication) propose un débit de 9.6 Kb/s
- **GPRS** (General Packet Radio Service) offre un débit de 115 Kb/s
- **EDGE** (Enhanced Data rate for GSM Evolution) est une solution medium en le GPRS et l'UMTS. Elle offre un débit de 384 Kb/s
- **UMTS** (Universal Mobile Telecommunication System) ou 3G de 384 kbits/s
- **HSDPA** (High Speed Downlink Packet Access ou 3G+) propose un débit de 1,8 à 14 Mbits/s
- **LTE** (Long Term Evolution ou 4G) permet des débits compris entre 100 Mb/s et 1 Gb/s)
- **LTE B** ou 5G permet des débits théoriques de 50 Gb/s
- **VSAT** (Very Small Aperture Terminal) ce système par satellite consiste à installer chez l'utilisateur une petite antenne qui reçoit des informations diffusées depuis un satellite géostationnaire pour un débit de 40 à 80 Mb/s)

Réseaux locaux sans fils (WLAN)

Le réseau local sans fils (Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Cette possibilité permet aux opérateurs de proposer des points d'accès appelés
hot spots dans les gares, aéroports, hôtels, trains.

Le WIFI

Le wifi utilise des bandes de fréquence variées : les bandes 2.4Ghz, les bandes 5Ghz et les bandes de 60Ghz.

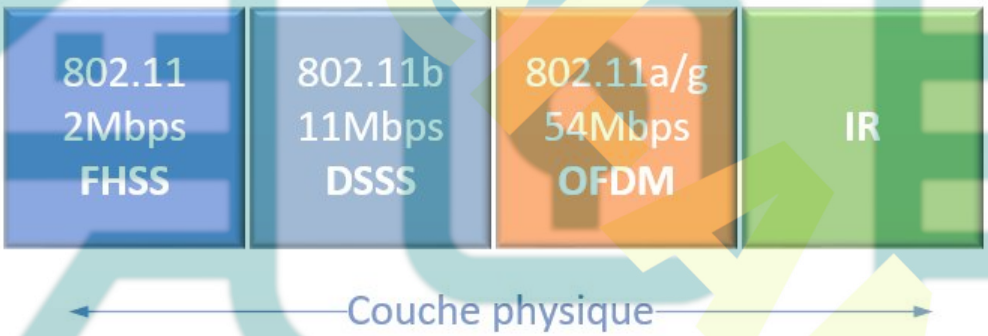
L'utilisation de ces bandes étant régie par chaque pays (ARCEP pour la France), on utilise les bandes libres sans licences mais dont la puissance est limitée.

L'organisme IEEE a décidé de normaliser les réseaux sans fils sous le nom de groupe 802.11 pour créer des standards. Il faut noter qu'à l'époque une norme européenne voyait le jour sous le nom **HiperLan** mais l'organisme IEEE l'a emporté.

> Les normes 802.11**b**, 802.11**g** et 802.11**n** utilisent les bandes 2.4Ghz
> Les normes 802.11**a** et 802.11**n** utilisent quant à elles les bandes à 5Ghz.

Courant 2019 devrait apparaître le 802.11**ay** utilisant des bandes de fréquences de 8Ghz. Cependant, il est à noter que les bandes de fréquences les plus élevées sont plus sensibles aux atténuations liées aux obstacles.

La couche physique



Mode communication

Le mode infrastructure

Chaque ordinateur se connecte à un point d'accès via une liaison sans fils. L'ensemble formé par le point d'accès et les stations est appelé ensemble de services de base (BBS) et constitue une cellule.

Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits) qui correspond à l'adresse MAC du point d'accès. Il est possible de relier plusieurs BSS entre eux afin de constituer un ensemble de services étendu (ESS)

1. Fonctionnement de l'AP (Access Point)

Il va régulièrement envoyer des trames de management (trames **beacon**) qui contiennent des informations permettant de décrire le service set et l'ensemble des caractéristiques de ce service set.

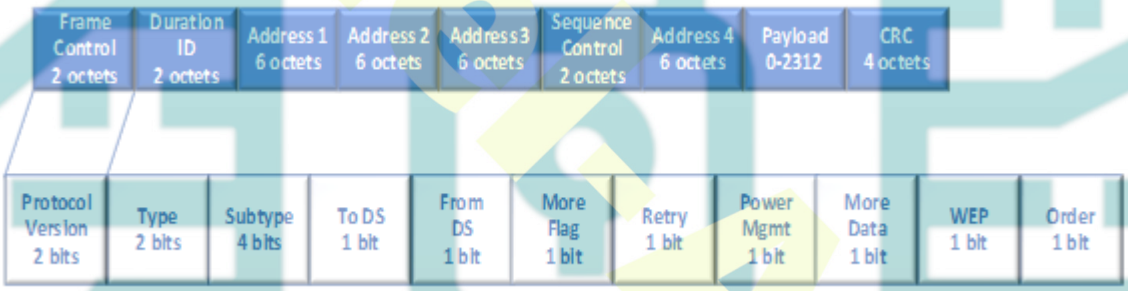
2. Fonctionnement de la station

Lorsqu'elle va arriver, dans la zone de couverture, la station va sonder le réseau, via un message **Probe Request** et les AP vont répondre un **Probe Response** puis la station va s'authentifier auprès du point d'accès pour s'associer au réseau.

Le mode ad hoc

Les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point.

Trame WIFI



- Contrôle de la trame (détaillé plus bas)
- **Durée/ID** – Ce champ peut avoir deux sens différents : pour les trames de polling en mode d'économie d'énergie, c'est l'identifiant de la station. Pour les autres trames, c'est la valeur de la durée de vie pendant laquelle le canal sera occupé.
- **4 champs d'adresses** – les deux premières adresses représentent l'adresse de la station destination, et de la station source. L'adresse 3 est l'adresse de la station source originale (si le flag From DS du champ de contrôle est à 1) ou est l'adresse du terminal de destination. L'adresse 4 est utilisée lorsqu'une trame est transmise d'un point d'accès à un autre à travers le système de distribution. Les bits To DS et From DS sont alors tous les deux à 1 et il faut renseigner à la fois la source et la destination.
- **Contrôle de séquence** – pour spécifier l'ordre des fragments d'une trame fragmentée.
- **Charge utile** qui peut aller jusqu'à 2312 octets.
- **Un champ CRC** pour le contrôle d'erreur.

Le champ contrôle de trame sur 32 bits

- Version de protocole.
- D'un Type et d'un sous-type qui représentent les 3 sortes de trames et leurs fonctions
- Les bits : ToDS et From DS (pour indiquer que la trame est envoyée vers le système de distribution ou si elle vient du DS)
- More Fragments est mis à 1 lorsque d'autres fragments suivent.
- Le bit Retry indique une retransmission d'un fragment ou d'une trame précédemment transmise.
- Bit Power Management est utilisé pour la gestion de l'énergie. Il indique que la station passe en mode d'économie d'énergie juste après la fin de la transmission de la trame en cours.
- Le bit More Data est utilisé par l'AP pour indiquer que des trames sont stockées pour une station. La station peut demander à recevoir les autres trames ou bien passer en mode actif.

Les normes WIFI

802.11b

La norme 802.11b permet d'obtenir un débit théorique de 11 Mbps, pour une portée d'environ une cinquantaine de mètres en intérieur et 200 mètres en extérieur (et même au-delà avec des antennes directionnelles) Elle utilise la bande de fréquence 2,4 Ghz

802.11a

La norme 802.11a permet d'obtenir un débit théorique de 54 Mbps pour une portée d'environ une trentaine de mètres sur une bande de fréquence 5 Ghz

802.11g

La norme 802.11g permet d'obtenir un débit de 54 Mbps pour une portée d'environ une cinquantaine de mètres en intérieur. Dans la mesure où la norme 802.11g utilise la bande de fréquence 2,4 Ghz, elle est compatible avec les matériels 802.11b

802.11h

Elle vise à rapprocher la norme 802.11 du standard Européen (Hiperlan 2, d'où le « h » de 802.11h) pour être en conformité avec la réglementation européenne en matière de fréquences et d'économie d'énergie

802.11n

La norme 802.11n propose un débit théorique de 300 Mbit/s grâce aux

technologies MIMO (Multiple-Input Multiple-Output) Le 802.11n a été conçu pour pouvoir utiliser les fréquences 2,4 Ghz ou 5 Ghz. Le 802.11n peut combiner jusqu'à 8 canaux non superposés, ce qui permet en théorie d'atteindre une capacité totale de d'un gigabit par seconde

802.11ac

Cette norme propose un débit théorique de 433 à 1300 Mbts/s en technologie MIMO et peut utiliser les bandes de fréquences de 2,4 à 5Ghz. Elle permet la mise en œuvre de vlan sur les bornes WIFI

802.11ad

Bande de fréquence en 60 Ghz, offrant un débit jusqu'à 6,75 Gbit/s

802.11ah

Bande de fréquence en 8 Ghz, offrant un débit jusqu'à 8 Mbit/s

802.11ax

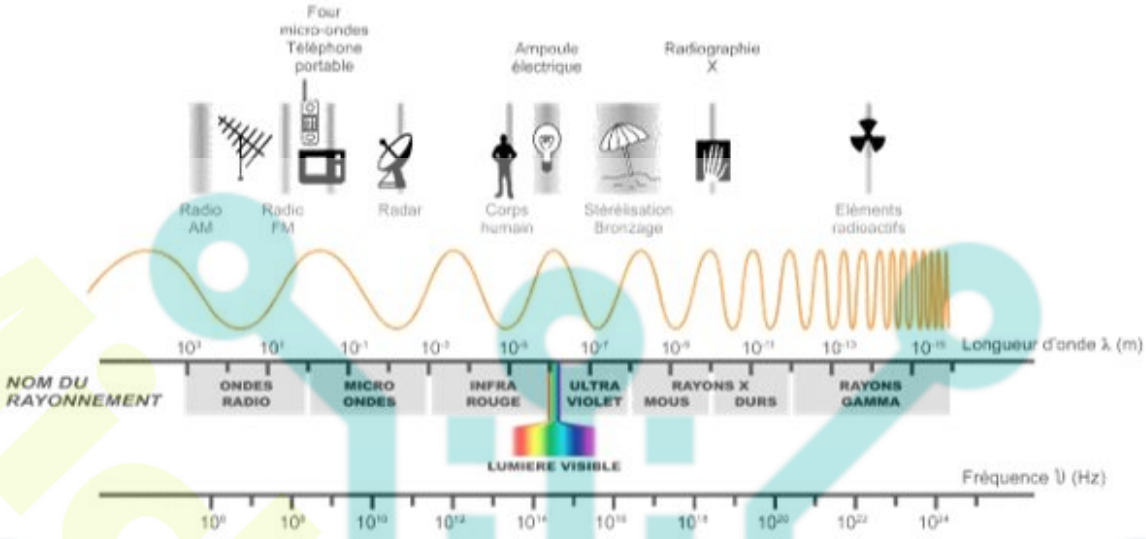
Bande de fréquence en 2/5 Ghz, offrant un débit jusqu'à 10 Gbits/s

802.11e

Elle ajoute deux nouvelles méthodes d'accès : EDCF et HCF pour la qualité de services en proposant 8 classes différentes.

Le Li-Fi

Light Fidelity est une technologie de communication sans fils basée sur l'utilisation de la lumière visible comprise entre la couleur bleue et la couleur rouge. Contrairement au Wi-Fi qui utilise le spectre électromagnétique, le Li-Fi utilise le spectre optique.



La connexion Li-Fi est opérationnelle dans la limite du cône de lumière que projette l'éclairage généralement situé au plafond afin d'offrir une couverture le plus large possible.

Fonctionnement

Un routeur LiFi alimente le système d'éclairage en courant et en données.
Un décodeur LiFi sur le terminal mobile décrypte le signal lumineux.

Avantages de la technologie LIFI

Une bande de fréquences entièrement libre et sans licence à l'échelle mondiale.
Absence d'interférences avec les ondes radio et le brouillage électromagnétique.
Sécurisation accrue de la communication (les ondes optiques ne traversent

pas les murs)
Communications sans fils à très haut-débit avec une limite théorique de 1 Gbits/s par LED émettrice.
Omniprésence des LEDs dans l'éclairage domestique, industriel, dans les displays et les signalétiques urbaines.
Possibilité de se géolocaliser à l'intérieur des bâtiments sans GSM et sans WiFi.

L'internet des objets

les domaines d'applications

Les domaines d'application de l'internet des objets sont nombreux. Il s'agit principalement de l'automobile, des services de santé, des réseaux d'énergie, du smart metering (mesures), du smart home, des smarts cities, de l'industrie 4.0 et de l'agriculture.

Allant des simples montres aux voitures connectés, les services demandés requièrent de nouvelles façons de concevoir les réseaux. L'association des opérateurs de télécommunication, prévoit que le nombre de connexions IoT devrait pour approcher les 25 milliards au niveau mondial en 2025.

En effet, les besoins d'autonomie, de portée, de débits font naitre de nouvelles technologies et de nouvelles normes.

C'est là qu'interviennent différentes solutions concurrentes.

- D'un côté, les technologies de réseaux basse consommation et à longue distance LPWAN (pour Low Power Wide Area Network), parmi lesquelles figurent entre autres les solutions Sigfox et LoRaWAN (dites LoRa).

- De l'autre, les opérateurs mobiles via des solutions IoT reposant sur des réseaux cellulaires existants, à l'image des offres LTE-M et NB-IoT développées respectivement par Orange Business Service et SFR Business.

Les défis proposés vont du passage à l'échelle, à la gestion de l'hétérogénéité des équipements et des services jusqu'aux besoins de sécurité.

	Non cellulaire	Non Cellulaire	Cellulaire	Cellulaire
	LoRa WAN	**Sigfox**	**NB-IoT**	**LTE-M**
Localisation	Oui	Oui	Oui	Oui
Débits	10Kb/s	600b/s	250Kb/s	5Mb/s
Capacité	40 000	1 Million	200 000	1 Million
Durée batterie	15 ans	15 ans	10 ans	10 ans
Sécurité	AES 128	AES 128	3GPP 256	3GPP 256
Distance	20 Km	40 Km	10 Km	–

Comparatif des technologies

La bataille pour s'arroger le marché de l'IoT risque donc d'être longue et de plus en plus acharnée dans les années à venir.

Les réseaux Wifi 802.11ah (HaLow)

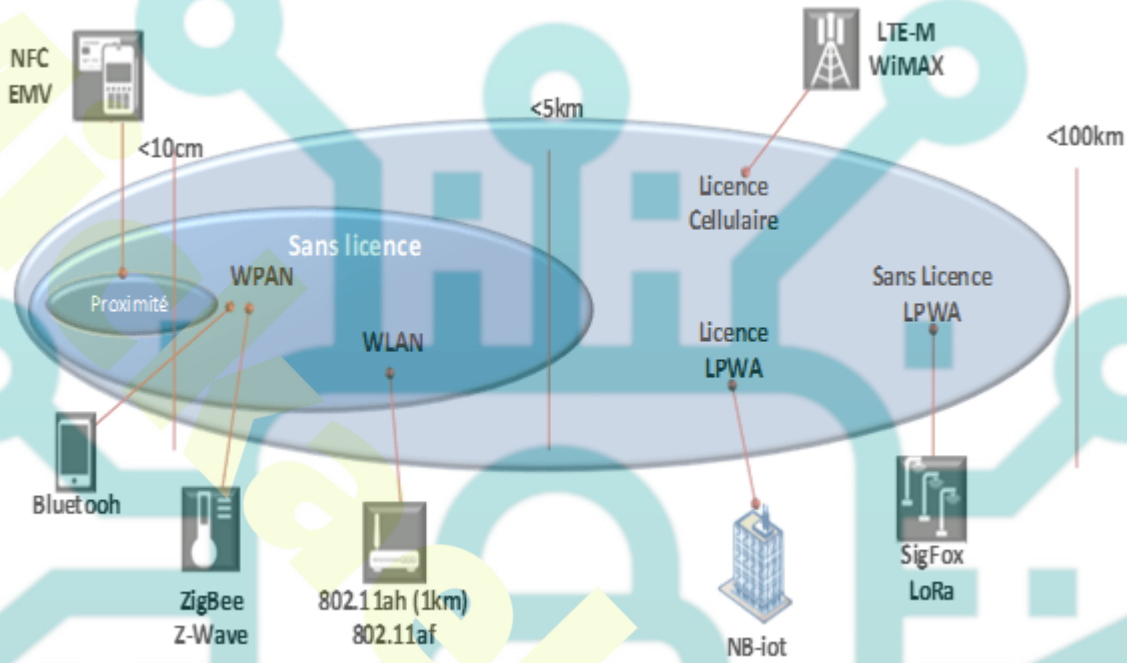
L'organisme de normalisation IEEE a annoncé la disponibilité du standard 802.11ah qui étend l'usage des réseaux locaux radio sans fils aux bandes de fréquence situées sous le gigahertz.

Le Wi-Fi HaLow, est réservé aux marchés des communications de machine à machine (M2M), de l'Internet des objets, du smart grid (réseau électrique intelligent), de la télé-santé, des appareils domotiques et des dispositifs électroniques portés sur soi.

Le standard 802.11ah doit garantir une longue autonomie des dispositifs alimentés sur piles ou batteries et desservir un grand nombre de nœuds d'extrémités grâce à une couche MAC qui promet une mise à l'échelle, une éco-efficacité et un fonctionnement en mode relai.

https://www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1181267-les-reseaux-iot

Choisir un protocole



Les problèmes de sécurités des réseaux sans fils

Les ondes radioélectriques ont tendances à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint.
La principale conséquence est la facilité pour une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fils est déployé.

Le souci vient du fait qu'un réseau sans fils peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant ! Il suffit en effet à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues "publiques" dans le rayon de couverture du point d'accès.

Le War-driving

Étant donné qu'il est très facile d'écouter des réseaux sans fils, une pratique venue tout droit des États-Unis consiste à circuler dans la ville avec un matériel équipé d'une connectique sans fils, de logiciels spécialisés à la recherche de réseaux à pirater.

L'interception de données

Par défaut un réseau sans fils est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour une entreprise l'enjeu stratégique peut être très important.

L'intrusion réseau

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fils non sécurisé représente de cette façon un point d'entrée royal au réseau interne d'une entreprise ou une organisation.

Le brouillage radio

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fils.

Le déni de service

Les méthodes d'accès au réseau et d'association étant connues, il est simple pour un pirate d'envoyer des paquets pour inonder le réseau sans fils.

La sécurisation des réseaux sans fils

Une infrastructure adaptée

La première chose à faire lors de la mise en place d'un réseau sans fils consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir.

Éviter les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Il est donc vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (broadcast) de ce dernier sur le réseau.

Le filtrage des adresses MAC

Les points d'accès permettent généralement de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fils.

La protection des échanges

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre différents mécanismes.

WEP (Obsolète)

Le WEP fait partie du standard 802.11 et a pour but d'assurer l'authentification.

- L'accès n'est autorisé qu'à ceux ayant connaissance de la clé WEP.
- La confidentialité est assurée par le chiffrement WEP (basé sur RC4) et l'intégrité des flux (CRC)
- Le WEP utilise une clé courte (40 bits), partagée par tous et entrée manuellement dans les équipements (points d'accès ou stations)

WPA (Obsolète)

WPA (Wi-Fi Protected Access) a pour objectif de pallier les problèmes posés par le WEP sans attendre la ratification de la norme 802.11i tout en conservant les matériels existants.

- Concernant les méthodes de chiffrement, le WPA utilise le protocole TKIP qui se base, comme le WEP, sur l'algorithme RC4.
- Le WPA élimine les failles du WEP en changeant périodiquement la clef. Il renforce l'intégrité des messages en y ajoutant un code d'intégrité de message.

802.11i (WPA2)

Cette norme a pour objet l'amélioration de la sécurité des réseaux 802.11

- Le WPA2 implante essentiellement le protocole CCMP. Avec ce protocole, WPA2 amène une grande innovation en se basant sur le chiffrement symétrique par bloc au lieu du chiffrement par flot.
- Il a remplacé le RC4 par l'AES qui est beaucoup plus robuste.
- L'algorithme CBC-Mac est appliqué sur les différents blocs d'un message pour générer un code d'authenticité qui assure l'intégrité des messages.

WPA3

Le WPA3 utilise des procédés de chiffrement modernes par poignée de mains (SAE) pour assurer entre autres un niveau de sécurité accru contre les « attaques par dictionnaire » et empêcher efficacement l'essai systématique automatisé de mots de passe pour accéder au Wi-Fi. D'autres caractéristiques de sécurité deviennent obligatoires, comme par exemple les trames de gestion protégées (Protected Management Frames, PMF) qui assurent un échange sûr durant la phase de connexion entre le périphérique Wi-Fi et la base Wi-Fi.

Mise en œuvre du 802.1x (RADIUS)

La norme IEEE 802.1X propose un moyen d'authentifier les équipements connectés sur un port avant de leur donner l'accès au réseau.

Elle utilise EAP (Extensible Authentication Protocol) un protocole générique qui permet de transporter divers protocoles d'authentification. L'encapsulation de chaque protocole d'authentification dans EAP étant défini à part.

Le principe de l'authentification 802.1X consiste en ce que l'équipement d'accès au réseau (commutateur filaire ou point d'accès sans fils) relaye les trames EAP entre le poste client et un serveur d'authentification (un serveur RADIUS), sans avoir à connaître le protocole d'authentification utilisé.
Si le protocole d'authentification comprend la génération de clés de session, celles-ci sont transmises à l'équipement d'accès et utilisées pour le chiffrement de la session.

	WPA	WPA 2	WPA 3
Chiffrement	Protocole d'intégrité des clés temporelles (TKIP) avec RC4	CCMP et Norme de Cryptage Avancéé (AES)	Norme de Cryptage Avancée (AES)
Taille clé	128 - bits	128 - bits	128-bits (Personal) 192-Bits (entreprise)
Type de chiffrement	Stream	Bloc	Bloc
Intégrité	Code d'intégrité des messages	CBC-MAC	algorithme de hachage sécurisé
Gestion des clés	Mécanisme 4-Way hanshake	Mécanisme 4-Way hanshake	l'authentification simultanée d'égal à égal
Authentification	Clé pré-partagée (PSK) et 802.1x avec variante EAP	Clé pré-partagée (PSK) et 802.1x avec variante EAP	Simultaneous Authentication of Equals (SAE) & 802.1x avec variante EAP