PROS Lilian
Aldin Music
Yannick BISSIELO

La norme Wi-Fi ou 802.11

Qu'est ce que la norme 802.11 ou WiFi ?

Définition : L'IEEE 802.11 est un ensemble de normes définies par l'Institute of Electrical and Electronics Engineers (IEEE) pour les réseaux locaux sans fil (WLAN).

Présentation du WiFi (802.11)

La norme IEEE 802.11 (ISO/*IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom Wi-Fi (Wireless Fidelity) correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau WiFi est en réalité un réseau répondant à la norme 802.11.

Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fils à haut débit pour que l'ordinateur à connecter ne soit pas trop distante par rapport au point d'accès. Dans la pratique, le WiFi permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (PDA) ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres en intérieur et à plusieurs centaines de mètres en environnement ouvert.

Ainsi, des opérateurs commencent à irriguer des zones à fortes concentration d'utilisateurs (gares, aéroports, hotels, trains, ...) avec des réseaux sans fils. Ces zones d'accès sont appelées « hot spots ». Dispose d'un menu contextuel.

Objectif : Fournir une communication sans fil pour les appareils et les réseaux informatiques.

Quels sont ses points clés ?

1. **Versions :** Plusieurs versions existent, comme 802.11a, 802.11b, 802.11g, 802.11n, et 802.11ac, chacune avec ses propres spécifications de vitesse et de fréquence.
2. **Portée et Vitesse :** La portée et la vitesse varient en fonction de la version spécifique. Par exemple, 802.11ac offre des vitesses plus élevées que 802.11b. (voir tableaux)
3. **Compatibilité :** Les appareils récents sont généralement compatibles avec plusieurs versions pour assurer une meilleure connectivité.

PROS Lilian
Aldin Music
Yannick BISSIELO

Protocole	Date de publication	Fréquence	Taux de transfert (Typ)	Taux de transfert (Max)	Portée théorique intérieure	Portée théorique extérieure
Initiale	1997	2,5 GHz	1 Mbit/s	2 Mbit/s	20 m	100 m
802.11a	1999	5 GHz	25 Mbit/s	54 Mbit/s	35 m	120 m
802.11b	1999	2,5 GHz	6,5 Mbit/s	11 Mbit/s	35 m	140 m
802.11g	2003	2,5 GHz	25 Mbit/s	54 Mbit/s	38 m	140 m
802.11n	2009	2,5/5 GHz	200 Mbit/s	600 Mbit/s	70 m (2,4 GHz) 12-35 m (5 GHz)	250 m
802.11ac	2013	5 GHz	433 Mbit/s	1300 Mbit/s	12-35 m	300 m
802.11ax	2021	2,5/5/6 GHz	-	10,54 bit/s	12-35 m	300 m

Réseaux locaux 802.11 : standards physiques [masquer]

Protocole 802.11	date[8]	Fréquence (GHz)	largeur de bande (MHz), (GHz)	Débit binaire[9] (Mbit/s), (Gbit/s)	Nombre maximum de flux MIMO	Codage / Modulation	Portée Intérieur (mètres)	Portée Extérieur (mètres)
802.11-1997 (d'origine)	juin 1997[8]	2,4	79 ou 22[10] MHz	1, 2 Mbit/s	NC	FHSS, DSSS	20 m	100 m
802.11a (Wi-Fi 2)	sept 1999[8]	5 3,7[A](US)	20 MHz	6 Mbit/s à 54 Mbit/s	1	OFDM	35 m	120 m (5 GHz) 5 000 m[A] (3,7 GHz)
802.11b (Wi-Fi 1)	sept 1999[8]	2,4	22 MHz	1 Mbit/s à 11 Mbit/s	1	DSSS	35 m	140 m
802.11g (Wi-Fi 3)	juin 2003[8]	2,4	20 MHz	6 Mbit/s à 54 Mbit/s	1	OFDM	38 m	140 m
802.11n (Wi-Fi 4)	oct 2009[8]	2,4 5	20, 40 MHz	6,5 à 150 Mbit/s Mbit/s[B]	4	OFDM	70 m (2.4 GHz) 35 m (5 GHz)	250 m[11]
802.11ac (Wi-Fi 5)	déc 2013[8]	5	20, 40, 80, 160 MHz	6,5 Mbit/s à 3,4 Gbit/s	8	OFDM	12-35 m	300 m
802.11ad	déc 2012[8]	57 à 71	1,7 à 2,16 GHz	jusqu'à 6,75 Gbit/s[12]	NC	OFDM ou porteuse unique	10 m[13]	10 m
802.11af (en)	fév 2014[8]	0,054 à 0,79	6 à 8 MHz	1,8 à 568,9 Mbit/s	4	OFDM	100 m	1 000 m
802.11ah	mai 2017[8]	0,9	1 à 8 MHz	0,6 à 8,6 Mbit/s[14]	4	OFDM	100 m	100 m
802.11ax (Wi-Fi 6 et 6E)	fév 2021[15]	1 à 7,1[16]	20, 40, 80, 160 MHz	8 Mbit/s à 10,5 Gbit/s	8	OFDM, OFDMA	12-35 m	300 m
802.11ay (en)	mars 2021[15]	58,3 à 70,2	2,16 à 8,64 GHz	20 à 176 Gbit/s	4[17]	OFDM ou *single carrier*	100 m	500 m

Comment obtenir cette certification ?

1. Conception et Développement

- **Respect des Spécifications :** Concevez votre produit (comme un routeur, une carte réseau, etc.) en suivant les spécifications techniques de la norme IEEE 802.11 appropriée.
- **Mise à jour Technologique :** Assurez-vous que votre produit est compatible avec les dernières versions de la norme, si cela est pertinent.

2. Test et Certification

- **Tests Internes :** Effectuez des tests internes pour vous assurer que votre produit répond aux exigences de la norme.
- **Laboratoires de Test Certifiés :** Faites tester votre produit par un laboratoire de test certifié IEEE pour la conformité aux normes 802.11. Ces laboratoires effectueront une série de tests pour vérifier la conformité aux normes techniques.

3. Certification Wi-Fi Alliance (Optionnel mais Recommandé)

- **Certification Wi-Fi :** Bien que ce ne soit pas obligatoire pour la conformité à la norme IEEE 802.11, la certification Wi-Fi Alliance ajoute de la crédibilité à votre produit. Elle assure que votre produit est compatible avec d'autres produits certifiés Wi-Fi.
- **Processus de Certification :** Soumettez votre produit à la Wi-Fi Alliance pour la certification. Ce processus comprend des tests de performance, de sécurité, et d'interopérabilité.

4. Marquage et Commercialisation

- **Marquage :** Une fois certifié, vous pouvez marquer votre produit avec la désignation IEEE 802.11 et, si certifié, le logo Wi-Fi.
- **Commercialisation :** Vous pouvez maintenant commercialiser votre produit comme étant conforme à la norme IEEE 802.11 et, si applicable, certifié Wi-Fi.

5. Maintien de la Conformité

- **Mises à Jour :** Soyez attentif aux mises à jour des normes et procédez à des mises à jour de votre produit au besoin.
- **Tests Continus :** Effectuez des tests réguliers pour assurer le maintien de la conformité.

Avantages/Inconvénients

Avantages

1. **Mobilité :** Permet aux utilisateurs de se déplacer tout en restant connectés au réseau.
2. **Installation Facile :** Moins de câblage nécessaire, facilitant l'installation et la reconfiguration des réseaux.
3. **Flexibilité :** Compatible avec une grande variété d'appareils.

Inconvénients

1. **Sécurité :** Les réseaux sans fil peuvent être moins sécurisés que les réseaux filaires, bien que cela puisse être atténué avec des protocoles de sécurité adéquats.
2. **Interférences :** Sensible aux interférences d'autres appareils électroniques et aux obstructions physiques.
3. **Portée Limitée :** La portée est souvent limitée par rapport aux réseaux filaires.

Les risques en matière de sécurité :

- L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil
- Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à internet
- Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences
- Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices

Approfondir nos connaissances sur les réseaux Wi-Fi :

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

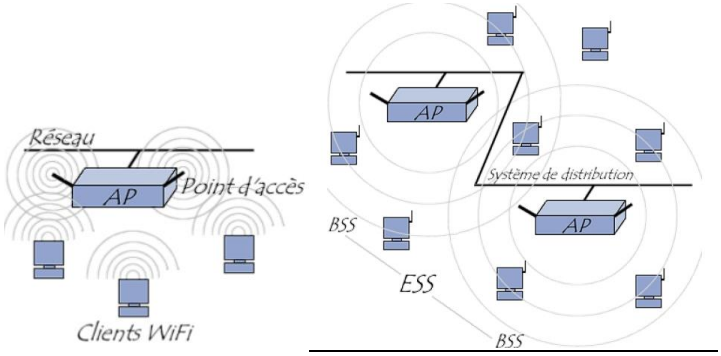
- La **couche physique** (notée parfois couche PHY), proposant trois types de codages de l'information
- La **couche de liaison** de données, constitué de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC)

La couche physique définit la modulation des ondes **radioélectriques** et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bis de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. La norme 802.11 propose réalité 3 couche physique, définissant les modes de transmissions alternatifs

Couche de liaison de données (MAC)	**802.2**		
	802.11		
Couche Physique	**DSSS**	**FHSS**	**Infrarouges**

Le mode Infrastructure

En mode infrastructure chaque ordinateur station (notée STA) se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone couverture est appelé ensemble de services de base (en anglais Basic Service Set noté BSS) et continue une cellule. Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.



Une infrastructure adaptée

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir. Il n'est pas rare que la zone réellement couverte soit moins grande que souhaitée, dans ce cas il est possible de réduire la puissance de votre borne d'accès afin de l'adapter à votre zone à couvrir.

Le filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique unique (appelée adresse MAC). Cette adresse se présente sous la forme de de 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. Les points d'accès permettent dans leur interface de configuration de gérer une liste de droit d'accès (ACL) basée sur les adresses MAC des équipements s'étant déjà connecté sur le réseau sans fil.

Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. En contrepartie cela ne résous pas le problème de la confidentialité des échanges.

WEP – Wired Equivalent Privacy

Pour régler les problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP.

IL s'agit d'un protocole de chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 bits ou 128 bits. LE principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou128 bits. Cette clé secrète doit être déclarée au niveau du point d'accès et des clients. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre le nombre pseudo-aléatoire et la trame.

La clé de session partagé par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.

De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

Dans le cas de la clé de 40 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener le pirate à trouver la clé de session. De plus une faille décelée par Scott Fluhrer, Itsik Mantin et Adi Shamir concernant la génération de la chaîne pseudo-aléatoire rend possible la découverte de la clé de session en stockant 100 Mo à 1 Go de trafics créés intentionnellement.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en oeuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

WPA (WiFi Protected Acces)

Le WPA est une solution de sécurisation de réseau WiFi reposant sur des protocoles d'authentification et un algorithme de cryptage robuste : **TKIP** (Temporary Key Integrity Protocol). Le protocole TKIP permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes, pour plus de sécurité. WPA2 supporte aussi l'AES (Advanced Encryption Standard) qui est beaucoup plus sécurisé.

Améliorer l'authentification

Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs (en anglais **AAA** pour *Authentication, Authorization, and Accounting*) il est possible de recourir à un serveur RADIUS (*Remote Authentication Dial-In User Service*). Le protocole *RADIUS* (défini par les RFC 2865 et 2866), est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

Mise en place d'un VPN

Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel (**VPN**).