Sécurisation  du WiFi

Le Wi-Fi (Wireless Fidelity)

Wi-Fi, marque de la Wi-Fi Alliance

Protocole de communications sans fil

Norme IEEE 802.11

Réseau sur 2 fréquences : 2,4 GHz et 5 GHz

WiFi a : 5 Mbps -> 50 m

WiFi b : 11 Mbps -> 300 m

WiFi g : 54 Mbps -> 500 m

WiFi n : 450 Mbps MIMO

WiFi ac : 1,3 Gbps MIMO

La sécurisation du WiFi avec clé de sécurité

Les débuts

Réseau hotspot ou communautaire

ouvert, en clair, aucune sécurité 🔓

Réseau privé ou invité 🔐

- WEP (Wired Equivalent Privacy) basé sur chiffrement RCA (1999) surnommé Weak Encryption Protocol

🗝️ clé de chiffrement de sécurité à 40 caractères hexadécimaux ou 23 caractères ASCII

⚠️🚫(durée de résistance d'une clé WEP🗝️ : < 3 minutes 📎)

La sécurisation du WiFi avec clé de sécurité

l'actuel

Réseau privé ou invité 🔐

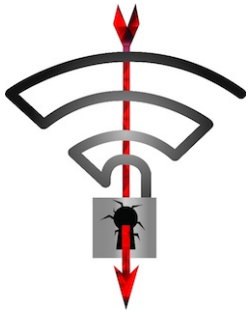
- **WPA** (Wi-Fi Protected Access) basé sur chiffrement TKIP (2003)

⚠️🚫(durée de résistance d'une clé WPA 🗝️ : > 10 heures 📎)

- **WPA2** (Wi-Fi Protected Access 2) basé sur chiffrement AES (2006)

🗝️ clé de chiffrement avec phrase secrète (> 6 caractères ASCII)

Soudain, KRACK (Key Reinstallation AttaCK)



Le 16 Octobre 2017, des chercheurs ont dévoilé une série de failles dans le fonctionnement de WPA 2, découverte depuis Mai 2017.

Sont susceptibles d'être affectés :

- Clients WiFi : ordinateurs (Windows, Mac, Linux,…), smartphones, tablettes (Android, iOS, Windows Mobile,…)
- Point d'accès Wifi : routeurs WiFi, Box (Freebox, Livebox, BBox, La Box de SFR,…), mode partage de connexion

Non réellement affectés : Linksys, Freebox, Livebox

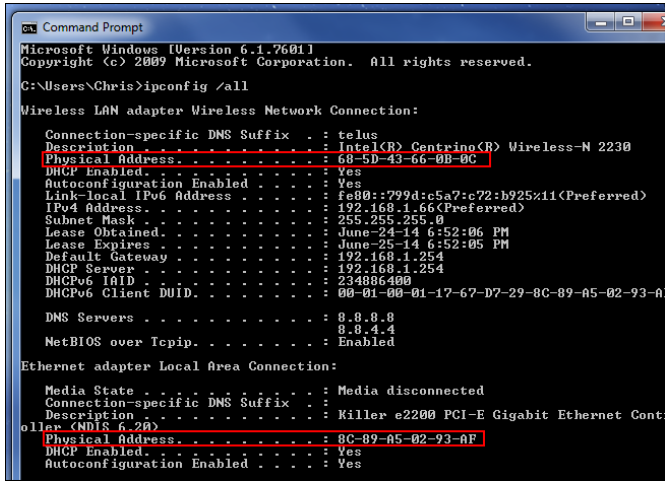
Correctifs en cours de déploiement : Windows (octobre), Apple (correctifs prêts en attente de déploiement), Linux (package wpa_supplicant mis à jour), Android (novembre)

La sécurisation du Wi-Fi par liste d'adresses MAC

Adresse Internet Protocol (IPv4 ou IPv6)
adresse d'identification sur les réseaux

Adresse physique ou MAC (Media Access Control)
adresse d'identification du matériel
unique pour chaque carte réseau (Ethernet, Wi-Fi, USB,…)

Filtrage avec liste blanche
Association pour ajouter un nouvel appareil

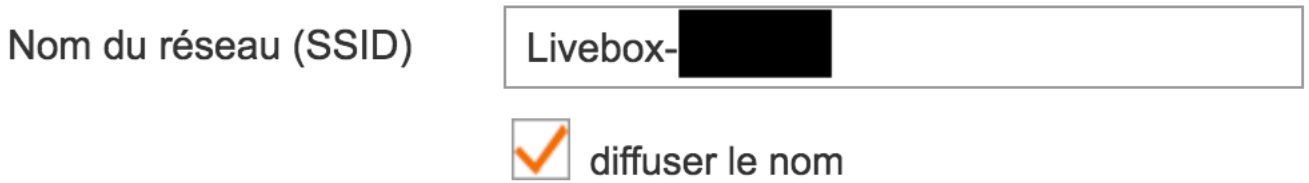


La non-diffusion du nom de réseau (SSID)

Les points d'accès WiFi peuvent diffuser avec le signal WiFi **un nom de réseau** (le SSID ou Service Set IDentifier) pour les identifier par rapport à un autre réseaux.

Par défaut, la diffusion du nom du réseau est activé. La désactivation s'effectue via un paramètre de configuration du point d'accès.

Seuls les appareils WiFi connaissant **le nom exacte** (avec casse des caractères) peuvent se connecter au réseau.

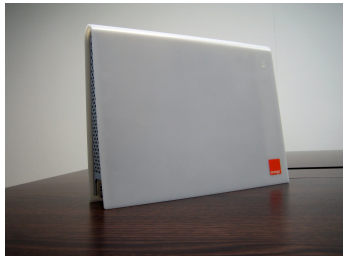


Le matériel : les box

WEP + Filtrage MAC

Livebox 1, 1.1

Neufbox Trio2 et Trio3C



WPA

Freebox v3 et v4

WPA + Filtrage MAC

Livebox 1.2/Mini

Neufbox Sagem ou Cegetel-Box

Le matériel : les box

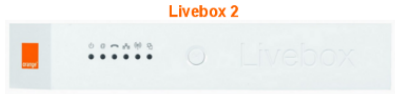
WPA 2

Livebox 2, 3 (Play), 4

Freebox v5 (Crystal 1), Alicebox Initial, Freebox Server, Freebox Server Mini

La Box de SFR (Neufbox v4, v6), La Box Plus de SFR (Neufbox v7), LaBox de Numericable, La Box La Poste Mobile

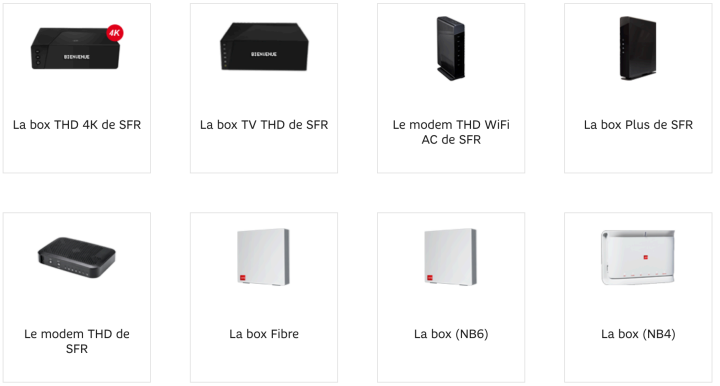
BBox, BBox Sensation, BBox Miami



Freebox Crystal

Freebox Mini 4K

Freebox Revolution



NordnetBox Impulsion

Sagemcom 2704

NordnetBox Séduction

NordnetBox Passion

NordnetBox Tentation

Les autres solutions de protection

Le chiffrement des données transmises

- HTTPS (navigateur)
- VPN (Réseau privé d'ordinateur)

La solution physique

- La câble Ethernet (RJ 45 Cat 5+)
- Le Courant Porteur en Ligne (CPL)

Question.Question.Question.Question.
Question, question: did I