

Réseaux sans fil et Wi-Fi – Activité 9

Introduction au WLAN et aux réseaux sans fil

Définition de WLAN :

C'est un réseau local sur lequel peuvent se connecter plusieurs appareils via une connexion sans fil. À la différence des connexions filaires reliées à des ports, le WLAN transmet les données via des ondes radio, selon la norme Wi-Fi (IEEE 802.11).

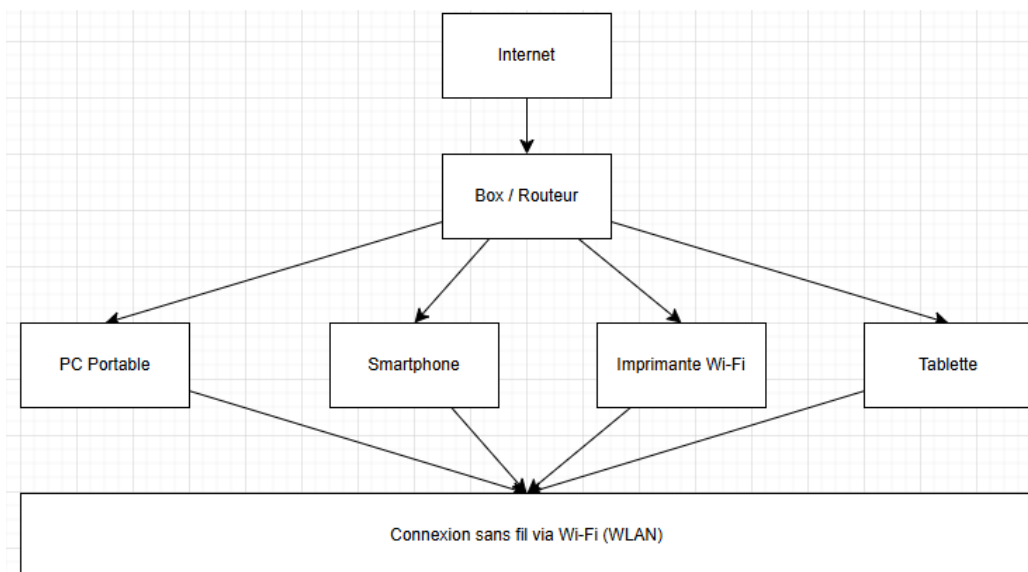
Comparaison LAN filaire et WLAN + Avantages et limites

Critère	LAN (filaire)	WLAN (sans fil)
Connexion	Par câble Ethernet	Par ondes radio (Wi-Fi)
Débit	Stable et élevé (1 Gbps ou +)	Variable, dépend de la distance et des interférences
Sécurité	Plus sécurisé (physique)	Moins sécurisé, nécessite chiffrement
Mobilité	Faible, poste fixe	Forte, déplacement libre
Installation	Complexe (câblage)	Simple et rapide
Fiabilité	Très fiable, peu d'interférences	Sensible aux perturbations
Coût initial	Plus élevé (matériel + câblage)	Moins coûteux

Note :

- LAN idéal pour la performance et la sécurité,
- WLAN idéal pour la flexibilité et les usages mobiles.

Schéma du WLAN lors d'utilisation concrète :



Normes Wi-Fi (IEEE 802.11)

Normes	Dates de sortie	Bande de fréquence utilisée (GHz)	Débits théoriques maximaux (Mbps)	Compatibilité ascendante/descendante	Obsolète
802.11a	1999	5	54	Non / Non	Oui
802.11b	1999	2.4	11	Non / Non	Oui
802.11g	2003	2.4	54	Oui / Oui	Oui
802.11n	2009	2.4 et 5	600	Oui / Oui	Non
802.11ac	2013	5	1300 à 6900	Oui / Oui	Non
802.11ax	2019	2.4, 5 et 6	Jusqu'à 9600	Oui / Oui	Non
802.11be	2024	2.4, 5 et 6	> 40000 (théorique)	Oui / Oui	Non

En norme Wi-Fi actuel pour un usage intensif c'est le Wi-Fi 6E (802.11ax étendu) et le Wi-Fi 7 (802.11be), car :

Critère	Wi-Fi 6E / Wi-Fi 7
Débit théorique	Jusqu'à 9.6 Gbps (Wi-Fi 6E) / > 40 Gbps (Wi-Fi 7)
Latence	Très faible, idéal pour le gaming et les appels vidéo
Bande de fréquence	Ajout du 6 GHz (moins encombrée, plus rapide)
Gestion des appareils	Optimisé pour les environnements multi-utilisateurs (OFDMA, MU-MIMO)
Sécurité	WPA3 intégré pour une meilleure protection
Stabilité	Moins de congestion, meilleure fluidité en streaming et cloud gaming

Note :

- OFDMA** : permet à plusieurs appareils de partager efficacement le Wi-Fi
- MU-MIMO** : envoie des données à plusieurs appareils en même temps
- WPA3** : renforce la sécurité des connexions sans fil

Sécurité des réseaux sans fil

Normes	Principes de fonctionnement	Faiblesse connues	Usages actuels	Différence dans l'utilisation	Sécurisé	Vulnérabilité
WEP	Chiffrement RC4 basique	Très facile à casser	Obsolète	Ancienne norme, peu utilisée	Très faible	Très élevée

WPA	Amélioration du WEP avec TKIP	Vulnérable aux attaques	Rare	Transition entre WEP et WPA2	Moyenne	Elevée
WPA2	Chiffrement AES + CCMP	Attaques KRACK possibles	Standard courant	Norme la plus répandue	Bonne	Moyenne
WPA3	Chiffrement renforcé + SAE	Compatibilité limitée	Nouveaux appareils	Remplace progressivement WPA2	Très bonne	Faible
RADIUS	Authentification centralisée	Complexité de mise en place	Réseaux pro	Utilisé avec 802.1X pour les réseaux d'entreprise	Bonne	Moyenne
802.1X	Contrôle d'accès réseau	Dépend du serveur d'authentification	Entreprises, écoles	Base pour les méthodes d'authentification comme EAP	Bonne	Moyenne
EAP	Méthode d'authentification extensible	Varie selon le type	Réseaux sécurisés	Utilisé avec 802.1X et RADIUS	Variable	Variable

Les différents rôles de ces technologies :

Composant	Rôle principal
WPA2/WPA3	Chiffre les données Wi-Fi
802.1X	Cadre d'authentification réseau
RADIUS	Serveur qui valide les identifiants
EAP	Méthode utilisée pour authentifier l'utilisateur

SSID et son rôle

Le **SSID** (Service Set Identifier) est le nom du réseau Wi-Fi. Il permet aux utilisateurs d'identifier et de se connecter à un réseau sans fil spécifique parmi plusieurs disponibles.

Ex : le nom inscrit dans la liste des réseaux Wi-Fi sur son appareil.

Diffusion ou masquage ?

- Par défaut, le SSID est diffusé par le point d'accès, ce qui permet aux appareils de le détecter facilement.
- Il est possible de masquer le SSID, ce qui empêche sa diffusion publique. Il est alors possible d'entrer manuellement le nom du réseau pour s'y connecter.

Sécurité illusoire du masque du SSID, une sécurité cosmétique ?

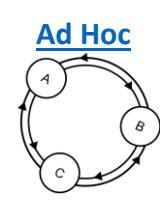
- Le réseau continue d'émettre des paquets, même sans diffuser son nom.
- Des outils comme Wireshark ou Kismet peuvent facilement détecter les SSID masqués en analysant le trafic.
- Cela n'empêche pas les attaques (ex : brute force), ni l'accès non autorisé si le mot de passe est faible.

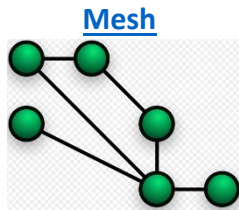
Cas concret avec 2 réseaux portant le même SSID :

On considère que les réseaux se nomment : DRAKE, le 1^{er} est l'entreprise et le 2nd est un réseau pirate, c'est le cas d'une attaque de type [Evil Twin](#).

Le résultat c'est que l'utilisateur peut se connecter au faux réseau sans le savoir, exposant ses données à une interception ou à une attaque de type [Man-in-the-Middle](#).

Topologies de réseaux sans fil

Type de réseau	Définition	Principe de fonctionnement	Exemple concret d'utilisation
	<p>Un réseau ad hoc est un réseau sans fil temporaire formé directement entre plusieurs appareils sans passer par un point d'accès central (comme une box ou un routeur).</p> <p>Chaque appareil joue à la fois le rôle de client et de routeur, ce qui permet aux données de circuler d'un appareil à l'autre de manière autonome.</p>	<p>Les appareils se connectent directement entre eux sans point d'accès central.</p> <p>Chaque appareil agit comme un émetteur et récepteur</p>	<p><u>Partage de fichiers</u> entre téléphones lors d'un événement sans Wi-Fi</p>

	<p>Architecture réseau dans laquelle chaque nœud (appareil) est connecté à plusieurs autres nœuds, voire à tous les autres. Cela crée un maillage dense et robuste, où les données peuvent circuler par plusieurs chemins.</p>	<p>Chaque nœud est connecté à plusieurs autres.</p> <p>Les données peuvent emprunter plusieurs chemins pour atteindre leur destination</p>	<p><u>Maison connectée</u> : objets domotiques (ampoules, thermostats, caméras) communiquant entre eux sans box centrale</p>
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------

La topologie Mesh est intéressante pour les grandes entreprises car elle garantit une connexion fiable, même en cas de panne, grâce à ses multiples chemins de communication. Elle permet aussi une couverture étendue et une intégration facile de nouveaux équipements, ce qui est idéal pour les villes connectées et les infrastructures complexes.

Extension des WLAN

Solution	Simplicité	Performance	Sécurité	Coût
Répéteur Wi-Fi	Très simple à installer	Débit réduit, réseau séparé	WPA2/WPA3 selon modèle	Faible (€)
Point d'accès (AP)	Moyennement simple (nécessite câblage)	Très bon débit, réseau stable	WPA2/WPA3 + VLAN possible	Moyen (€€)
Wi-Fi Mesh	Très simple via appli mobile	Bonne couverture, roaming fluide	WPA3, SSID unique	Elevé (€€€)
Solutions pro (contrôleur, VLAN, roaming)	Complexe (configuration réseau)	Optimale, gestion centralisée	Sécurité renforcée (802.1X, VLAN, WPA3)	Très élevé (€€€€)

Pour une PME à 2 étages ?

Il y a comme solution :

- **Installation de points d'accès câblés (AP)** pour chaque étage (ici 2), reliés au routeur via Ethernet
- **Utilisation d'un contrôleur centralisé** (type Omada SDN ou UniFI) pour gérer les AP, les VLAN et le roaming
- **Placement stratégique** : au centre de chaque étage (ici 2), loin des murs porteurs ou sources d'interférences

- **Option Mesh** (si câblage difficile) : système Wi-Fi Mesh pro (ex : TP-Link Omada Mesh) avec plusieurs nœuds.

Les avantages de ces solutions sont :

- Roaming fluide entre les étages (idéal pour les appels VoIP, visioconférences)
- Réseau segmenté par VLAN (ex : invités, employés, IoT)
- Sécurité renforcée (WPA3, filtrage MAC, portail captif)
- Gestion centralisée, évolutivité facile

Critère	Répéteur Wi-Fi	Point d'Accès câblé (AP)
Connexion	Sans fil, capte et répète le signal	Connecté en Ethernet au routeur
Performance	Débit réduit, latence possible	Débit optimal, stable
Installation	Très simple, plug and play	Nécessite câblage et configuration réseau
Sécurité	Basique (WPA2/WPA3 selon modèle)	Avancée (VLAN, WPA3, contrôle d'accès)
Coût	Faible	Moyen à élever selon modèle
Usage idéal	Maison, petites zones	PME, bureaux, environnements professionnels

De plus, le répéteur est une solution d'appoint alors le point d'accès câblé est une solution robuste et évolutive.

La conception d'un WLAN

Norme choisie : WPA3, Chiffrement renforcé

Topologie adaptée : Mesh et LAN câblé

Moyens de sécurité :

- Contrôleur Wi-Fi : pour gérer centralement les points d'accès, les VLAN et les politiques de sécurité.
- VLAN : segmentation du réseau (ex. : invités, employés, IoT) pour limiter les risques de propagation en cas d'intrusion.
- Roaming sécurisé : permet aux utilisateurs de se déplacer sans interruption de connexion, tout en maintenant l'authentification.

- Détection d'intrusion sans fil (WIDS/WIPS) : pour repérer et bloquer les points d'accès non autorisés ou les comportements suspects.
- 2FA
- Mot de passe fort
- Désactiver SSID Broadcast
- Filtrage d'adresses MAC
- Sécurité WPA3
- Utiliser VPN
- Désactiver l'administration à distance
- Changer le mot de passe par défaut
- Utiliser un firewall
- Désactiver UPnP
- Désactiver services inutiles

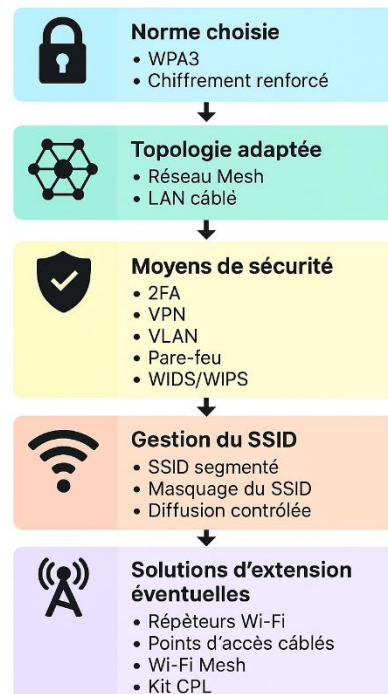
Gestion du SSID :

- Diffusion contrôlée : le SSID doit être identifiable mais non trop générique
- Segmentation par SSID : créer plusieurs SSID pour différents usages
- Masquage du SSID : peut être utilisé pour les réseaux sensibles, mais ne constitue pas une vraie mesure de sécurité

Solutions d'extensions éventuelles :

- Répéteurs Wi-Fi
- Points d'accès câblés (AP)
- Système Wi-Fi Mesh
- Kit CPL (Courant Porteur en Ligne)

SÉCURITÉ DES RÉSEAUX SANS FIL



Source : [GlobalSign by GMO](#)