



LES RÉSEAUX SANS FIL





16.1. Introduction aux réseaux sans fil

16.1.1. Avantages des réseaux sans fil :

- ➔ La mobilité ➔ Flexibilité de déplacement et du travail à distance.
- ➔ Les coûts réduits : pas de câbles nécessaires.



16.1.2. Types de réseau sans fil :

 <p>Bluetooth zigbee</p> <p>WPAN (6 à 9 M)</p> <p>Norme 802.15</p> <p>Bande de fréquence : 2,4 GHz</p>  <p>WMAN (Jusqu'à 50 KM)</p> <p>Norme 802.16</p> <p>Fréquences sous licences spécifiques</p>	 <p>WLAN (Jusqu'à 100 M)</p> <p>Norme 802.11</p> <p>Bandes de fréquence : 2,4 GHz et 5 GHz</p>  <p>WWAN (Nationale et mondiale)</p> <p>Normes GSM, 3G, 4G, 5G, etc.</p> <p>Fréquences sous licences spécifiques</p>
--	---

- ➔ **WPAN** (Wireless **P**ersonal **A**rea **N**etwork) : Réseau personnel sans fil
- ➔ **WLAN** (Wireless **L**ocal **A**rea **N**etwork) : Réseau local sans fil
- ➔ **WMAN** (Wireless **M**etropolitan **A**rea **N**etwork) : Réseau métropolitain sans fil
- ➔ **WWAN** (Wireless **W**ide **A**rea **N**etwork) : Réseau étendu sans fil

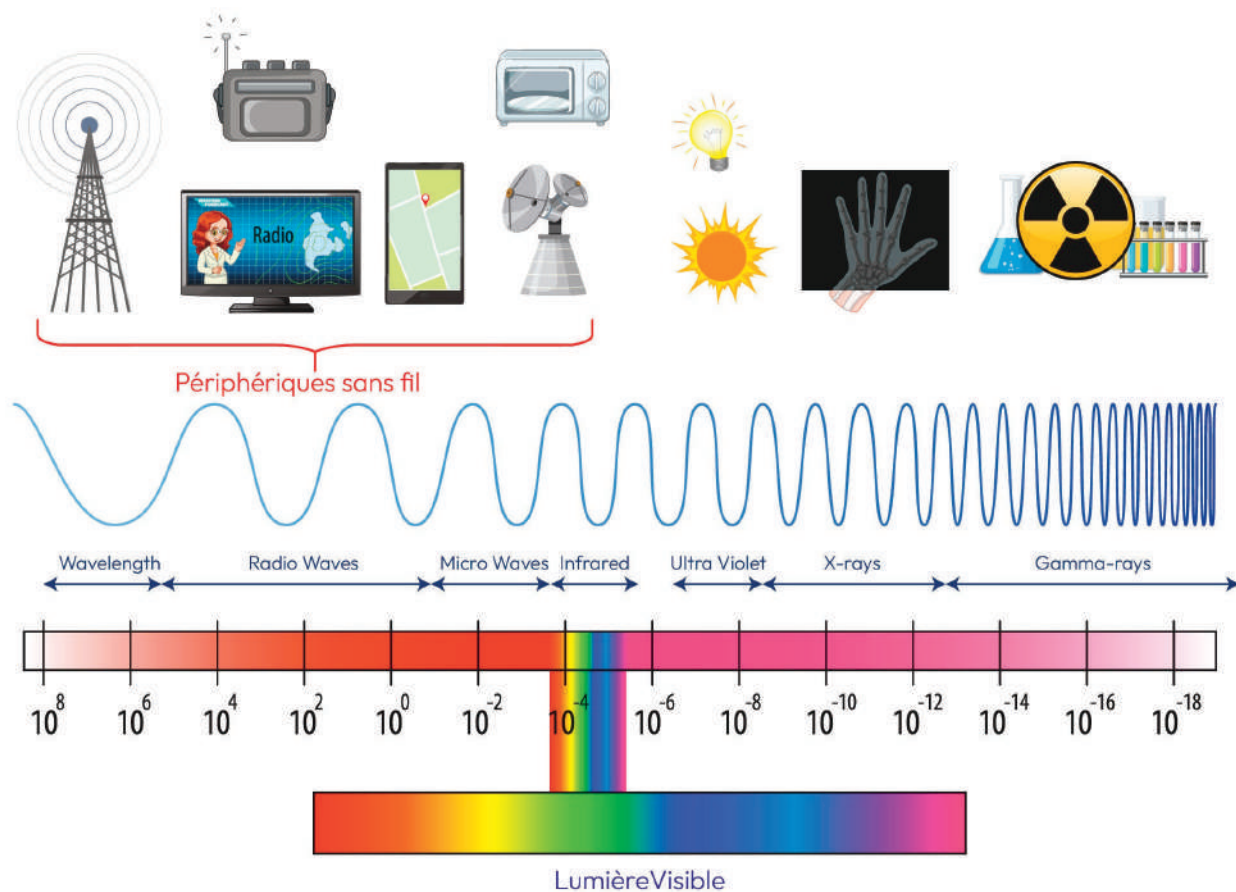
WLAN (**W**ireless **L**ocal **A**rea **N**etwork) est un réseau local sans fil, qui permet aux utilisateurs de se connecter à un réseau à l'aide de dispositifs sans fil tels que des ordinateurs portables, des smartphones ou des tablettes.

Il utilise des technologies telles que le Wi-Fi pour transmettre des données à travers l'air, éliminant ainsi la nécessité de câbles physiques pour connecter les dispositifs.

Les WLANs sont souvent utilisés dans les environnements domestiques, les petites entreprises et les organisations afin de permettre aux utilisateurs de se connecter à Internet et aux ressources réseau sans fil.

Les WLANs peuvent également être utilisés dans les environnements professionnels pour connecter des dispositifs tels que des terminaux mobiles, des imprimantes et des appareils IoT à un réseau.




16.1.3. Les ondes radio :



Les réseaux locaux sans fil WLAN utilisent les bandes de fréquences suivantes :

- ➡ 2,4 GHz (**UHF** : **Ultra High Frequencies**) - 802.11b/g/n/ax
- ➡ 5 GHz (**SHF** : **Super High Frequencies**) - 802.11a/n/ac/ax

16.1.4. Organisations des normes sans fil :

ACRONYME	NOM	LOGO	DESCRIPTION
IEEE	Institute of Electrical and Electronics Engineers		Spécifier la manière dont les fréquences sont modulées pour transporter l'information.
ITU-R	International Telecommunication Union - Radiocommunication		Réglementer l'attribution du spectre fréquentiel.
Wi-Fi Alliance	Wi-Fi alliance		Assurer l'interopérabilité des produits basés sur la norme 802.11

16.1.5. Normes 802.11 :

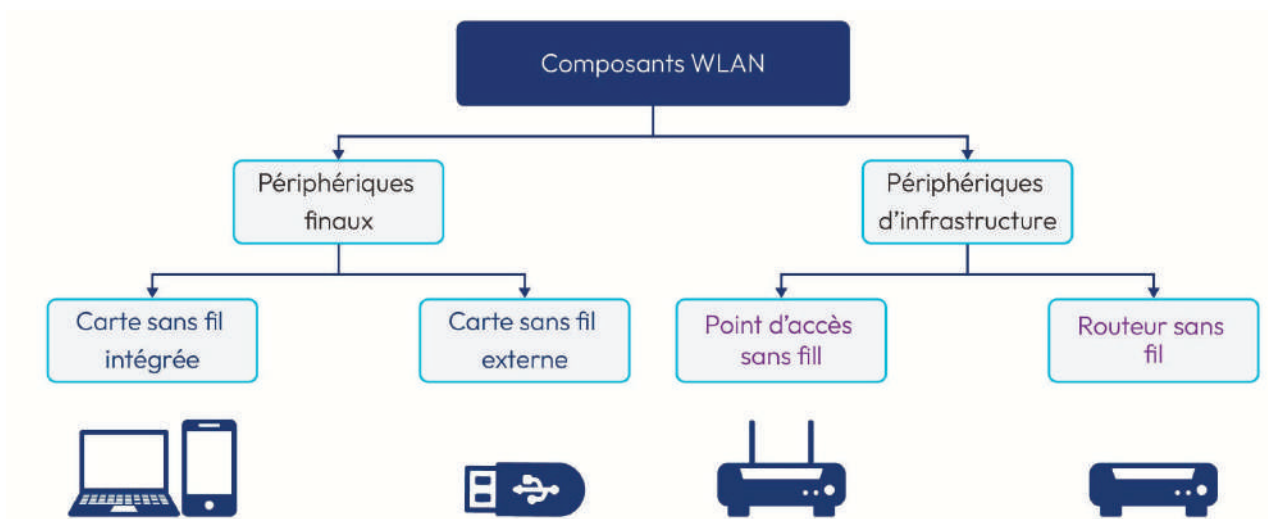
NORME IEEE WLAN	BANDE DE FRÉQUENCE	DESCRIPTION
802.11	2,4 GHz	<ul style="list-style-type: none"> Vitesses allant jusqu'à 2 Mb/s
802.11a	5 GHz	<ul style="list-style-type: none"> Vitesses allant jusqu'à 54 Mb/s Petite zone de couverture Moins efficace pour pénétrer les structures des bâtiments Non interopérable avec les 802.11b et 802.11g

NORME IEEE WLAN	BANDE DE FRÉQUENCE	DESCRIPTION
802.11b	2,4 GHz	<ul style="list-style-type: none"> • Vitesses allant jusqu'à 11 Mb/s • Portée plus longue que 802.11a • Mieux à même de pénétrer les structures des bâtiments
802.11g	2,4 GHz	<ul style="list-style-type: none"> • Vitesses allant jusqu'à 54 Mb/s • Rétrocompatible avec 802.11b avec une capacité de bande passante réduite
802.11n	2,4 GHz 5 GHz	<ul style="list-style-type: none"> • Débits de données varient de 150 Mb/s à 600 Mb/s avec une plage de distance jusqu'à 70 m (230 pieds) • Les points d'accès et les clients sans fil ont besoin de plusieurs antennes utilisant la technologie MIMO • Rétrocompatibilité avec les appareils 802.11a/b/g à débit de données limité
802.11ac	5 GHz	<ul style="list-style-type: none"> • Débits de données allant de 450 Mb/s à 1,3 Gb/s (1300 Mbps) utilisant la technologie MIMO • jusqu'à huit antennes peuvent être prises en charge • Rétrocompatible avec les appareils 802.11a / n avec limitation des débits de données
802.11ax	2,4 GHz 5 GHz	<ul style="list-style-type: none"> • Publié en 2019 - dernière norme • Également connue sous le nom de High-Efficiency Wireless (HEW) • Débits de données plus élevés • Capacité accrue • Gère de nombreux appareils connectés • Efficacité énergétique améliorée • Capabilité 1 GHz et 7 GHz, lorsque ces fréquences seront disponibles • Recherchez Wi-Fi Génération 6 sur Internet pour plus d'informations

16.1.6. Comparaison entre LAN et WLAN :

	LAN	WLAN
Connexions physiques	Utilisation des câbles	Ondes radio
Couche liaison de données	CSMA/CD	CSMA/CA
	Carrier Sense Multiple Access / Collision Detection	Carrier Sense Multiple Access / Collision Avoidance
Problèmes de signaux parasites	Non	Oui
Mobilité	Non	Oui

16.2. Composants WLAN :



16.2.1. Périphériques finaux :

Les périphériques finaux fournissent une interface à l'utilisateur final.

- ➔ Périphériques avec carte réseau sans fil intégrée : Ordinateur portable, Téléphone, Tablette, imprimante, etc.
- ➔ Périphériques avec carte réseau sans fil externe : Ordinateur de bureau, etc.

16.2.2. Périphériques d'infrastructure :

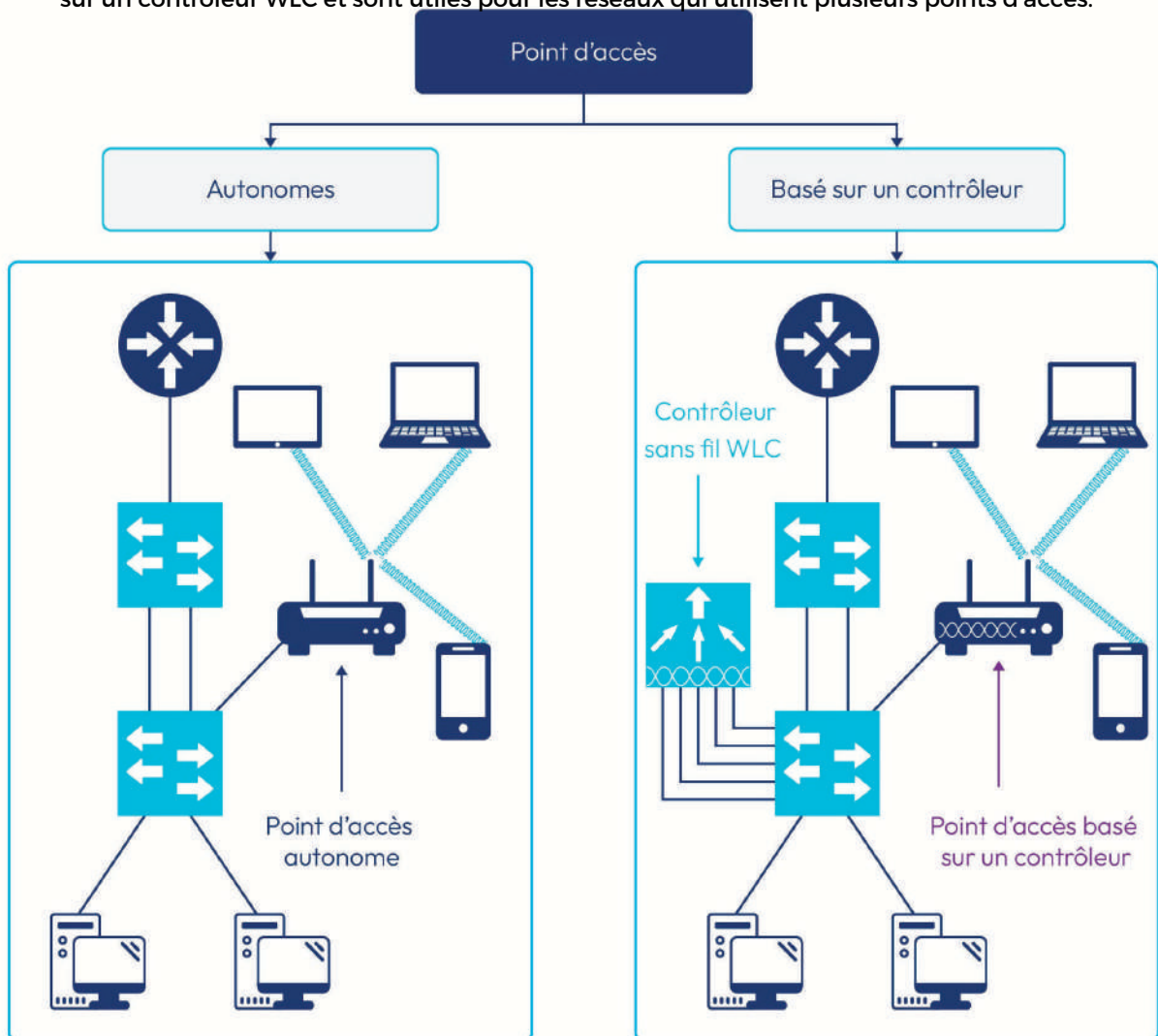
POINT D'ACCÈS :

Un point d'accès sans fil fournit une connectivité locale au réseau sans fil WLAN.

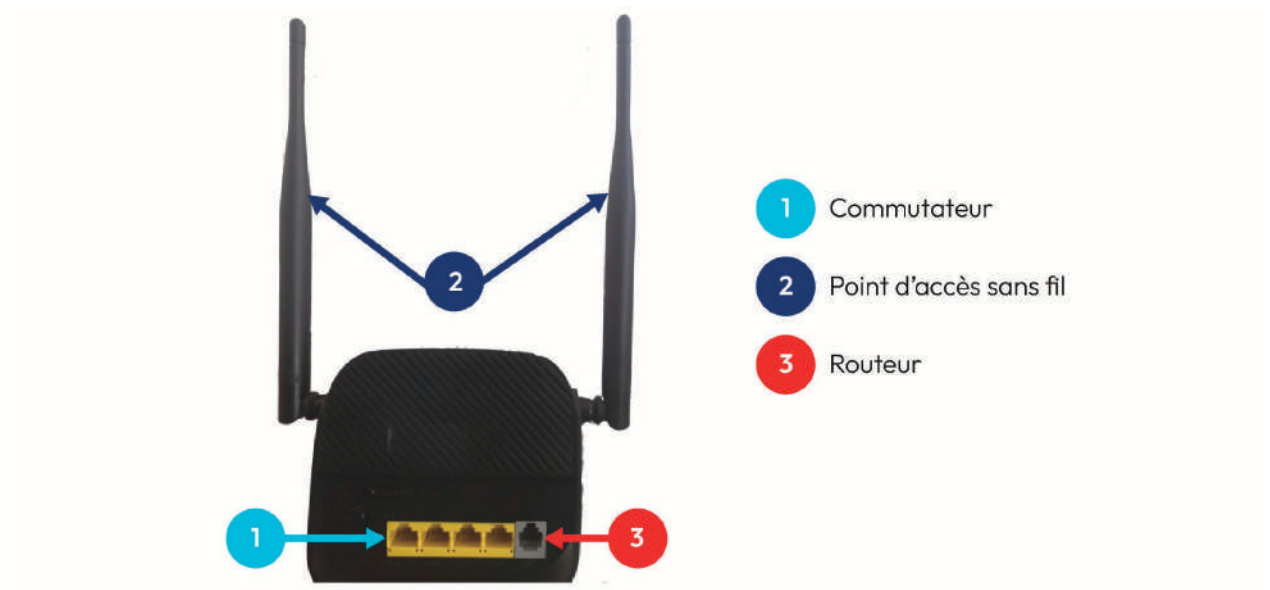
Il existe deux types de point d'accès sans fil :

➔ **Points d'accès autonomes** : Ils sont configurés manuellement et sont utiles pour les petits réseaux.

➔ **Points d'accès basés sur un contrôleur LWAPP (Lightweight Access Point Protocol)** : Ils sont basés sur un contrôleur WLC et sont utiles pour les réseaux qui utilisent plusieurs points d'accès.



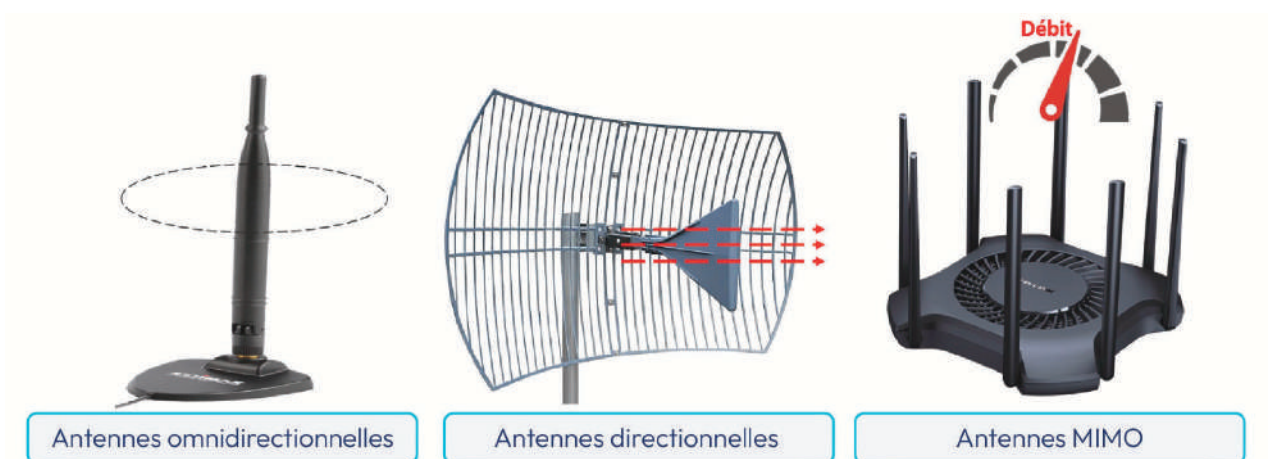
ROUTEUR DOMESTIQUE SANS FIL :



Un routeur domestique sans fil a 3 fonctions principales :

- ➔ **Commutateur** : Joue le rôle d'un commutateur filaire LAN
- ➔ **Point d'accès sans fil** : Fournit une connectivité locale au réseau WLAN
- ➔ **Routeur** : Joue le rôle de passerelle par défaut pour se connecter aux réseaux Internet

16.2.3. Antenne sans fil :



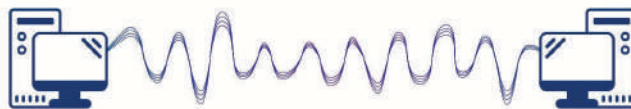
Il existe 3 types d'antennes :

- **Antennes omnidirectionnelles** : Elles offrent une couverture à 360 degrés.
- **Antennes directionnelles** : Elles focalisent le signal dans une direction donnée.
- **Antennes MIMO** : Elles utilisent plusieurs antennes pour augmenter le débit pour les réseaux sans fil IEEE 802.11n / ac / ax.

16.3. Fonctionnement d'un réseau sans fil :

16.3.1. Modes de topologies sans fil :

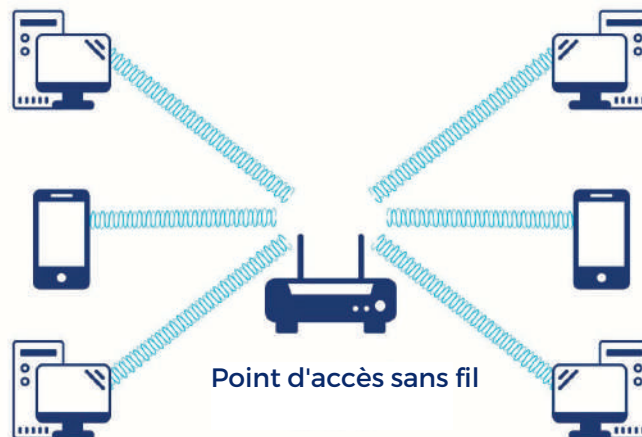
MODE « ADHOC » :



Le mode « **Adhoc** » consiste à connecter deux périphériques finaux sans fil, **sans utiliser un périphérique d'infrastructure** comme un point d'accès sans fil, par exemple.

MODE « INFRASTRUCTURE » :

Le mode « **Infrastructure** » consiste à connecter plusieurs périphériques finaux sans fil en utilisant **un périphérique d'infrastructure**.



MODE « PARTAGE DE CONNEXION » :

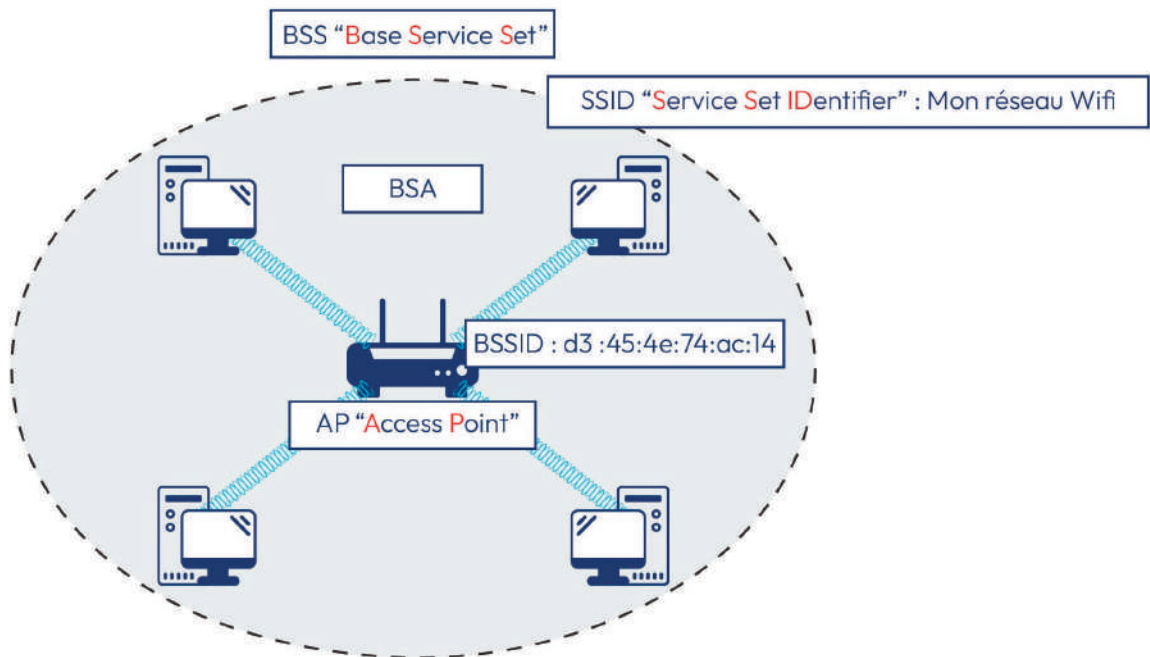
Le mode « **Partage de connexion** » est une variante du mode Adhoc qui consiste à activer un téléphone avec accès aux données cellulaires pour créer un **point d'accès personnel**.



16.3.2. Topologies sans fil :

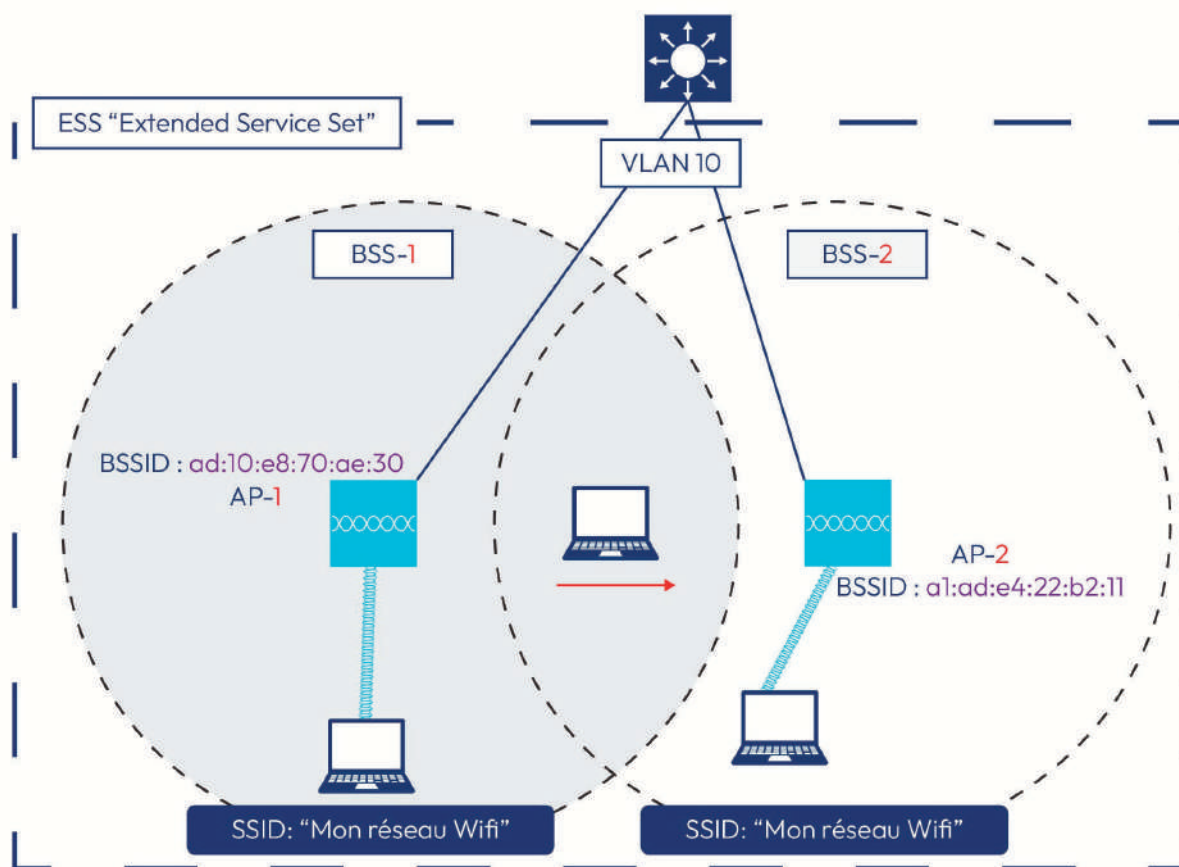
TOPOLOGIE BSS :

- ➔ Un **BSS** ou « **ensemble de service de base** » (**B**asic **S**ervice **S**et) consiste à utiliser **un seul point d'accès** qui interconnecte tous les clients sans fil associés.
- ➔ La zone de couverture est appelée « **zone de service de base** » **BSA** (**B**asic **S**ervice **A**rea).
- ➔ Une zone BSA est identifiée par un **BSSID** (**b**asic **s**ervice **s**et **i**dentifier).



TOPOLOGIE ESS :

- ➔ Un **ESS** ou « **ensemble de service étendu** » (**E**xtended **S**ervice **S**et) consiste à joindre **deux ou plusieurs BSS**, via un système de distribution.
- ➔ La zone de couverture est appelée « **zone de service étendu** » **ESA** (**E**xtended **S**ervice **A**rea).
- ➔ Une zone ESA est identifiée par un **SSID** qui permet un passage transparent entre les différentes zones BSA de la même ESA.



16.3.3. Structure d'une trame 802.11 :



Contrôle de trame	Identifie le type de la trame, etc.
Durée	La durée restante pour recevoir la transmission de trame suivante.
Adresse 1	L'adresse MAC de l'appareil sans fil ou AP récepteur.
Adresse 2	L'adresse MAC de l'appareil sans fil ou AP de transmission.
Adresse 3	L'adresse MAC de la destination, telle que l'interface du routeur (passerelle par défaut) à laquelle l'AP est connecté.
Contrôle de séquence	Les numéros d'ordre et les numéros des fragments.
Adresse 4	Utilisée en mode Adhoc.
Données utiles	Le paquet.
FCS	Le contrôle des erreurs de transmission.

16.3.4. Types de trames :

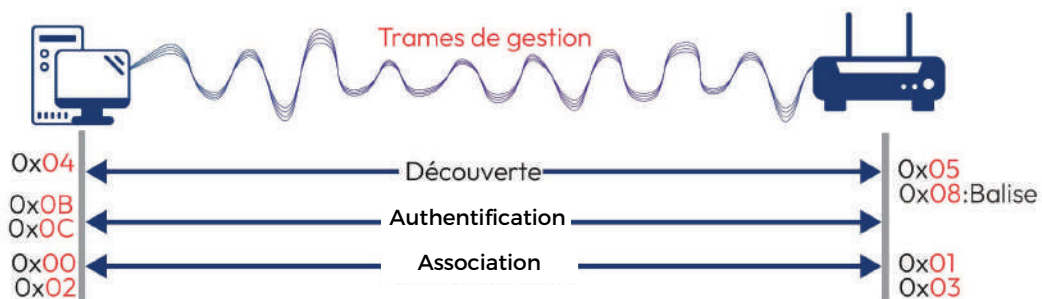
Il existe 3 grands types de trame :

- ➡ **Trames de gestion (0x0)**
- ➡ **Trames de contrôle (0x1)**
- ➡ **Trames de données (0x2)**

TRAMES DE GESTION :

Les trames de gestion sont utilisées pour :

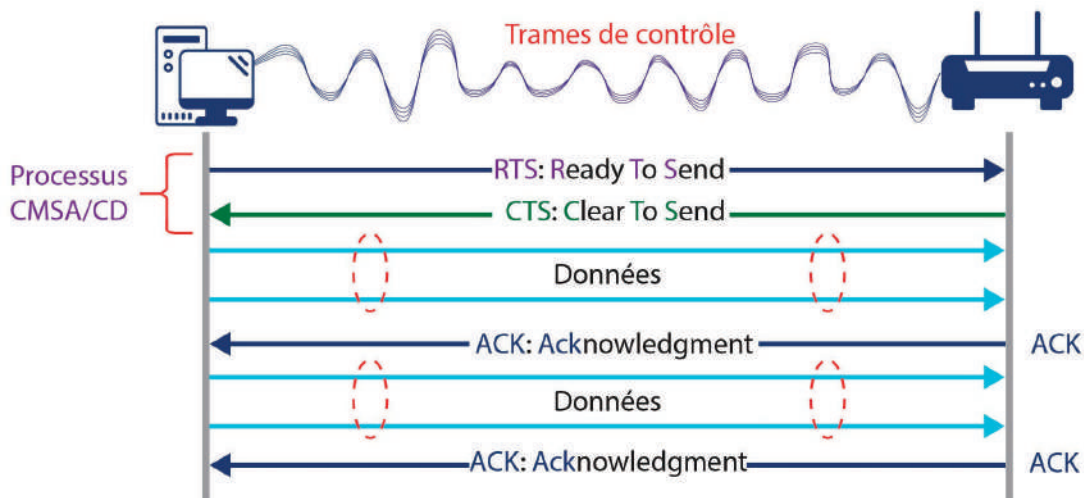
- ➔ La **découverte** du point d'accès en utilisant l'un des deux modes :
 - **Mode passif** : Le point d'accès diffuse le SSID en utilisant des trames de « **Balise** »
 - **Mode actif** : Le client sans fil doit connaître le SSID, car le point d'accès ne diffuse pas les trames de balise.
- ➔ L'**authentification** d'un périphérique sans fil auprès du point d'accès sans fil
- ➔ L'**association** du périphérique sans fil au point d'accès sans fil



TRAMES DE CONTRÔLE ET TRAMES DE DONNÉES :

Les trames de contrôle sont utilisées pour :

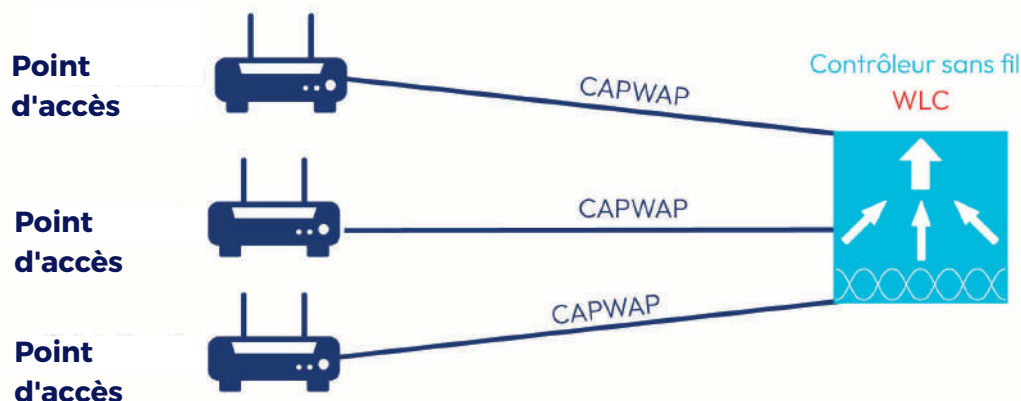
- ➔ Le processus de contrôle de support CSMA/CA
- ➔ Confirmer la réception des trames de données.



16.3.5. Fonctionnement du protocole CAPWAP :

RÔLE DU CAPWAP :

Le protocole **CAPWAP** (**C**ontrol **A**nd **P**rovisioning of **W**ireless **A**ccess **P**oints) est un protocole qui permet à un contrôleur sans fil (WLC) de gérer plusieurs points d'accès sans fil (AP).

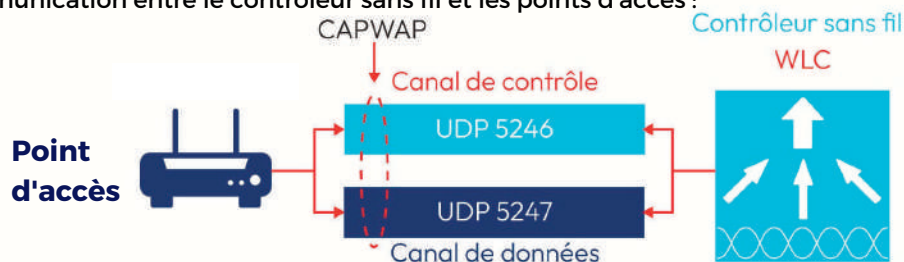


LA SÉCURITÉ AVEC CAPWAP :

Le protocole **CAPWAP** (**C**ontrol and **P**rovisioning of **W**ireless **A**ccess **P**oints, ou contrôle et approvisionnement des points d'accès sans fil en français), est un protocole de communication utilisé pour gérer et configurer les points d'accès sans fil dans les réseaux informatiques.

Il permet aux administrateurs de réseau de configurer et de gérer les points d'accès sans fil à distance, ce qui facilite l'installation et la gestion de ces équipements dans les grandes entreprises ou les installations avec de nombreux points d'accès.

Le protocole **CAPWAP** utilise une option de sécurité **DTLS** (**D**atagram **T**ransport **L**ayer **S**ecurity) pour chiffrer la communication entre le contrôleur sans fil et les points d'accès :



Par défaut, le chiffrement DTLS est activé pour le canal de contrôle et désactivé pour le canal de données

LE CONTRÔLE D'ACCÈS MULTIMÉDIA PARTAGÉ :

Le protocole **CAPWAP** utilise le concept d'un contrôle d'accès multimédia partagé (**MAC partagé**) qui consiste à définir les fonctions du point d'accès et celles du contrôleur :

FONCTIONS MAC DU POINT D'ACCÈS	FONCTIONS MAC DU CONTRÔLEUR SANS FIL
Trames de découverte du point d'accès	Authentification
Accusé de réception et retransmissions	Association et réassociation de clients
Qualité de service	Traduction de trame vers d'autres protocoles
Chiffrement et déchiffrement des données	Arrêt du trafic 802.11 sur une interface filaire

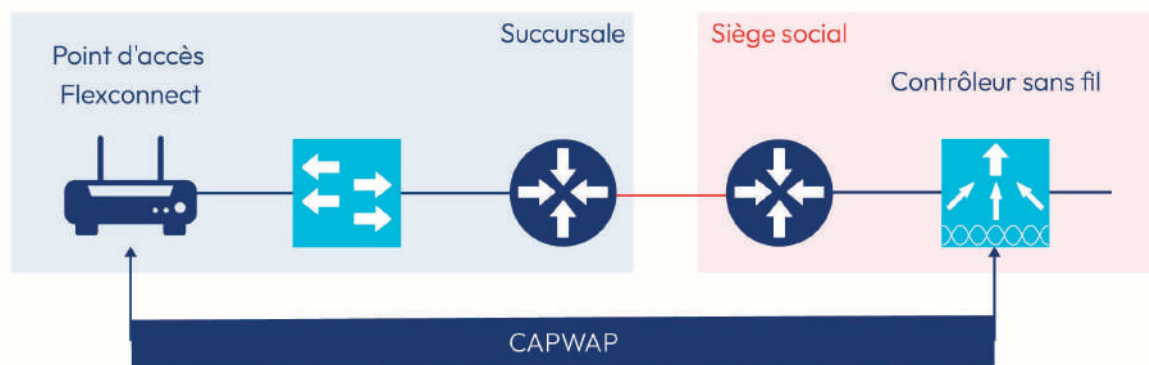
CAPWAP ET LA COUCHE RÉSEAU :

Le protocole **CAPWAP** peut fonctionner avec IPv4 et IPv6 en utilisant les numéros de protocoles :

- ➡ 17 pour IPv4
- ➡ 136 pour IPv6

LES POINTS D'ACCÈS FLEXCONNECT :

FlexConnect est une solution qui permet de contrôler les points d'accès des succursales à partir du siège social en utilisant une connexion WAN.



Il existe deux modes de fonctionnement :

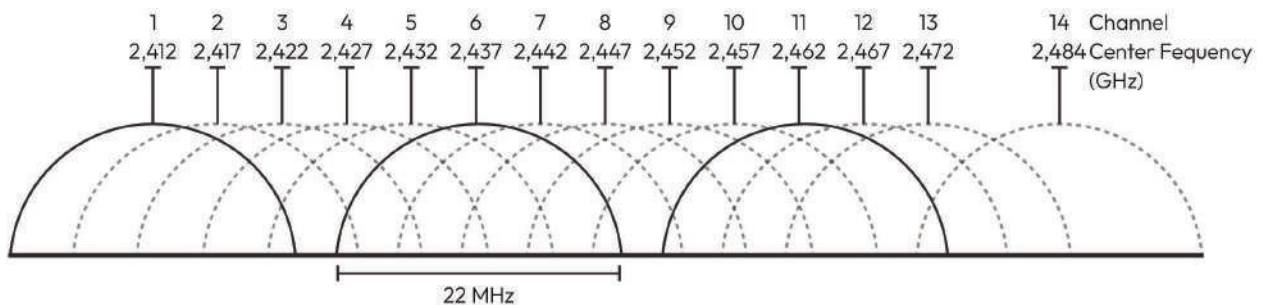
- ➔ **Mode connecté** : Le WLC est accessible. Dans ce mode, le FlexConnect AP a une connectivité CAPWAP avec son WLC.
- ➔ **Mode autonome** : Le WLC est inaccessible. Dans ce mode, un AP FlexConnect peut assurer certaines des fonctions du WLC localement comme l'authentification.

16.3.6. La gestion des canaux :

LES BANDES DE FRÉQUENCES :

Le réseau sans fil utilise les deux bandes de fréquences :

La bande 2,4 GHz :



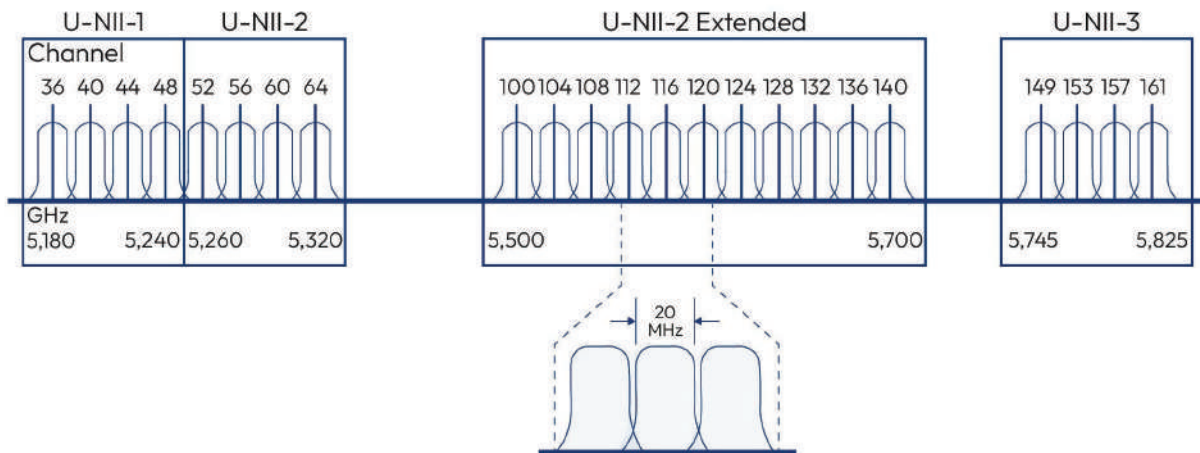
S'il y a 3 points d'accès adjacents, on peut utiliser les 3 canaux 1, 6 et 11, car il n'y a pas de chevauchement.

Remarque :

RÉGION	NOMBRE DE CANAUX
Amérique du Nord	11
Europe	13
Japon	14

La bande 5 GHz :

La bande 5GHz est divisée en 3 sections.



La bande 5 GHz peut fournir une transmission de données plus rapide aux clients sans fil grâce à la quantité de canaux **qui ne se chevauchent pas**

Les bandes de fréquence **2.4GHz et 5GHz** sont utilisées pour la transmission de données sans fil dans les réseaux WiFi.

La bande de fréquence 2.4GHz est utilisée depuis longtemps et est compatible avec une grande variété d'appareils sans fil. Par conséquent, elle est plus largement utilisée.

Cependant, la bande de fréquence 2.4GHz est davantage encombrée en raison de l'utilisation simultanée de nombreux appareils sans fil tels que les téléphones, les ordinateurs portables, les routeurs et les appareils domestiques intelligents.

La bande de fréquence 5GHz, quant à elle, est moins utilisée, mais offre des débits de données plus rapides et une meilleure portée.

Elle est également moins encombrée, ce qui permet une meilleure performance pour les applications exigeant de grandes bandes passantes telles que la diffusion vidéo en continu.

Pour résumer :

La bande de fréquence 2.4GHz est plus largement utilisée et compatible avec une grande variété d'appareils, mais est davantage encombrée et offre des débits de données moins élevés.

La bande de fréquence 5GHz offre des débits de données plus rapides et une meilleure performance pour les applications exigeant de grandes bandes passantes, mais est moins utilisée et compatible avec moins d'appareils.

16.4. La sécurité des réseaux sans fil :

16.4.1. Menaces de sécurité d'un WLAN :

ATTAQUES DE DÉNI DE SERVICE :

Une attaque **DoS** (**D**enial **o**f **S**ervice) est une attaque qui vise à rendre le WLAN indisponible. Une attaque DoS peut-être à cause de :

- ➡ Un appareil mal configuré
- ➡ Interférences intentionnelles ou accidentelles

POINTS D'ACCÈS NON AUTORISÉS :

Un point d'accès non autorisé est un point d'accès installé d'une manière malveillante pour permettre l'accès à une ressource sécurisée.

Il peut provoquer le fait de :

- ➡ Capturer les données des utilisateurs : Adresses MAC, etc.
- ➡ Lancer une attaque **MITM** (**M**an **I**n **T**he **M**iddle : L'homme du milieu)

ATTAQUE D'HOMME AU MILIEU (MITM) :

Une **attaque MITM** est une attaque qui consiste à se positionner entre deux entités légitimes pour pouvoir lire ou modifier des données qui circulent entre elles.

Un exemple d'une attaque MITM est l'attaque « **AP maléfique jumelle** », qui utilise un point d'accès non autorisé avec le même SSID et avec une authentification ouverte.

16.4.2. Mesures de sécurité des WLAN :

MASQUAGE SSID :

Le masquage du SSID consiste à empêcher le point d'accès sans fil d'envoyer des trames de balise.

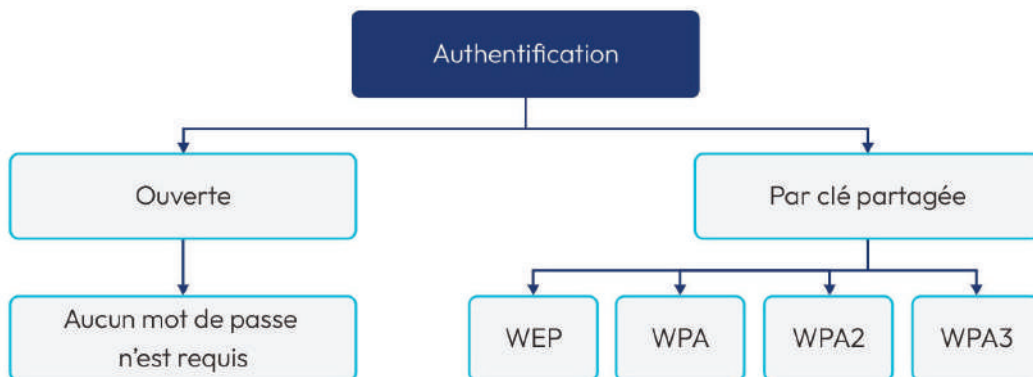
FILTRAGE DES ADRESSES MAC

Le filtrage des adresses MAC consiste à empêcher des appareils qui possèdent certaines adresses MAC de se connecter au point d'accès sans fil.

UTILISATION DES MÉTHODES D'AUTHENTIFICATION 802.11

Il existe deux types d'authentification :

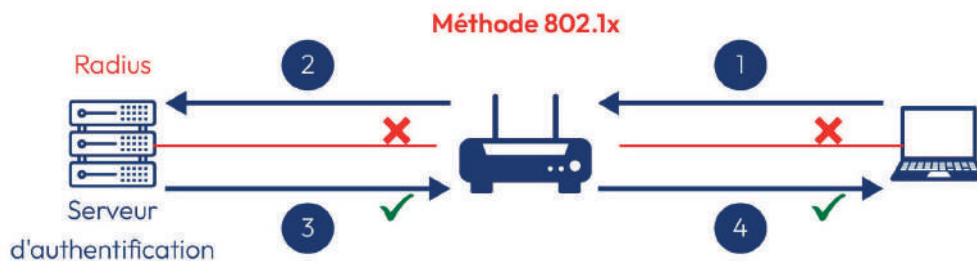
- ➔ **Authentification ouverte** : aucun mot de passe n'est requis pour se connecter au point d'accès sans fil.
- ➔ **Authentification par clé partagée** : le client doit entrer une clé (mot de passe Wi-Fi) pour se connecter au point d'accès sans fil.



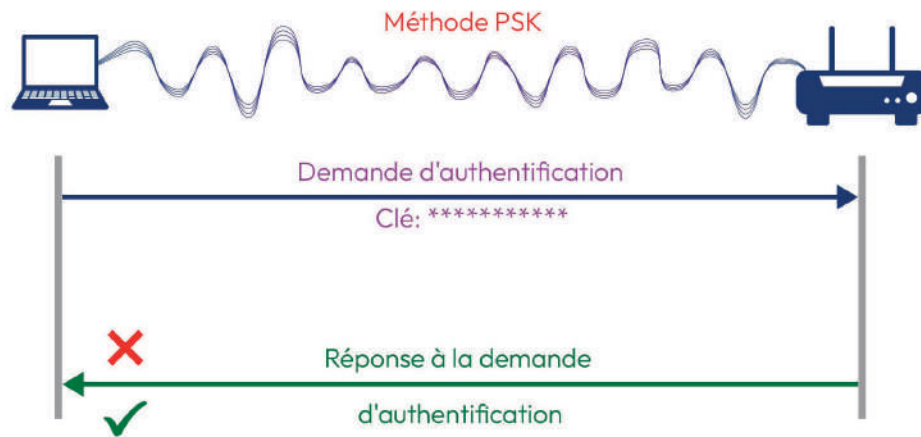
Méthodes d'authentification :

Il existe deux méthodes d'authentification :

Entreprise : 802.1x



Personnelle : Par clé prépartagée **PSK (Pre-Shared Key)**



Protocoles d'authentification par clé partagée :

PROTOCOLE D'AUTHENTIFICATION	DESCRIPTION
WEP	Méthode d'authentification: Clé partagée Chiffrement : RC4 avec une clé statique. Intégrité : CRC-32
WPA	Méthode d'authentification: Clé partagée ou 802.1x Chiffrement : Le WEP avec TKIP (Clé temporaire) Intégrité : MIC
WPA2 (802.11i)	Méthode d'authentification: Clé partagée ou 802.1x Chiffrement : AES Intégrité : CCMP
WPA3	La prochaine génération de sécurité Wi-Fi. 4 fonctionnalités : <ul style="list-style-type: none"> • WPA3-Personnel • WPA3-Entreprise • Réseaux ouverts • Intégration de l'Internet des objets (IoT)

16.5. Configuration des réseaux sans fil :

16.5.1. Configuration du réseau :



L'onglet « **Setup** » permet de configurer :

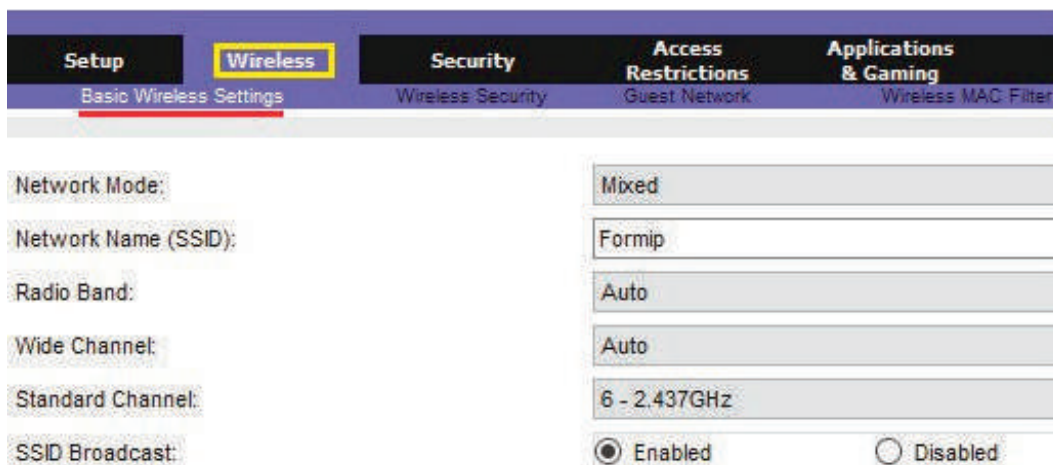
- ➔ Modifier l'adresse de l'interface WAN : à l'aide du DHCP ou d'une manière statique.
- ➔ Modifier l'adresse de l'interface LAN.
- ➔ Modifier la configuration du serveur DHCP.

16.5.2. Configuration du réseau sans fil :

L'onglet « **Wireless** » permet de configurer :

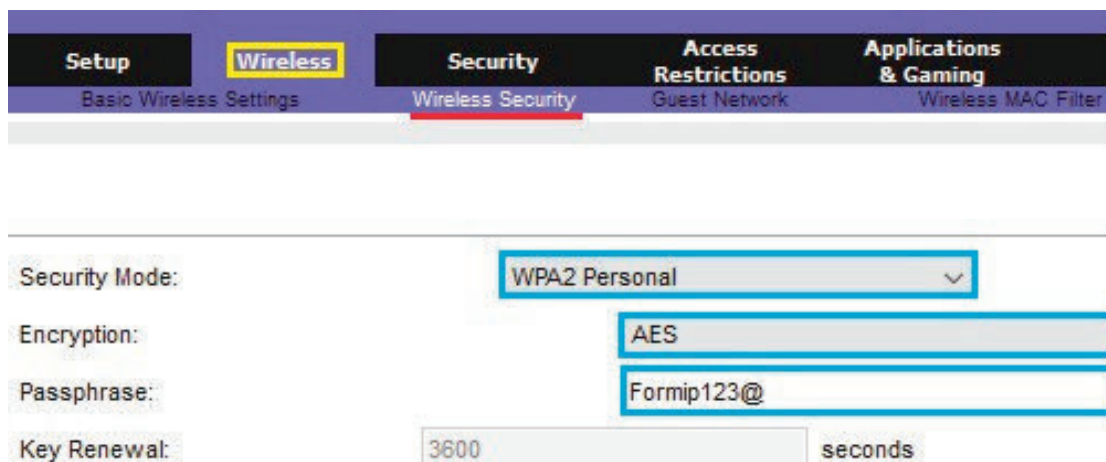
LES PARAMÈTRES DE BASE DU RÉSEAU SANS FIL :

- ➔ La norme Wi-Fi (Network Mode)
- ➔ Le SSID et sa diffusion (Activée ou désactivée)
- ➔ Le canal



LA SÉCURITÉ DU RÉSEAU SANS FIL

- ➔ Mode de sécurité
- ➔ Algorithme de chiffrement et clé pré-partagée



The screenshot shows the 'Wireless Security' configuration page. The 'Security Mode' is set to 'WPA2 Personal'. The 'Encryption' is set to 'AES'. The 'Passphrase' is 'Formip123@'. The 'Key Renewal' is set to '3600 seconds'.

Setup	Wireless	Security	Access Restrictions	Applications & Gaming
Basic Wireless Settings		Wireless Security	Guest Network	Wireless MAC Filter

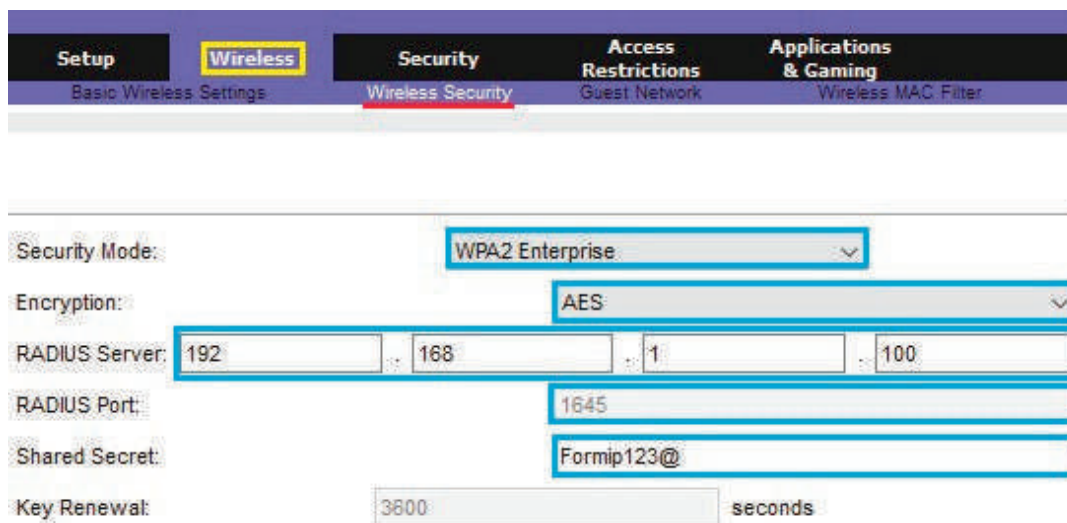
Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Formip123@

Key Renewal: 3600 seconds

- ➔ Avec le mode « Entreprise », il est possible de rentrer des informations pour un serveur RADIUS.



The screenshot shows the 'Wireless Security' configuration page with 'WPA2 Enterprise' selected. It includes fields for 'RADIUS Server' (192.168.1.100), 'RADIUS Port' (1645), and 'Shared Secret' (Formip123@). The 'Key Renewal' is set to '3600 seconds'.

Setup	Wireless	Security	Access Restrictions	Applications & Gaming
Basic Wireless Settings		Wireless Security	Guest Network	Wireless MAC Filter

Security Mode: WPA2 Enterprise

Encryption: AES

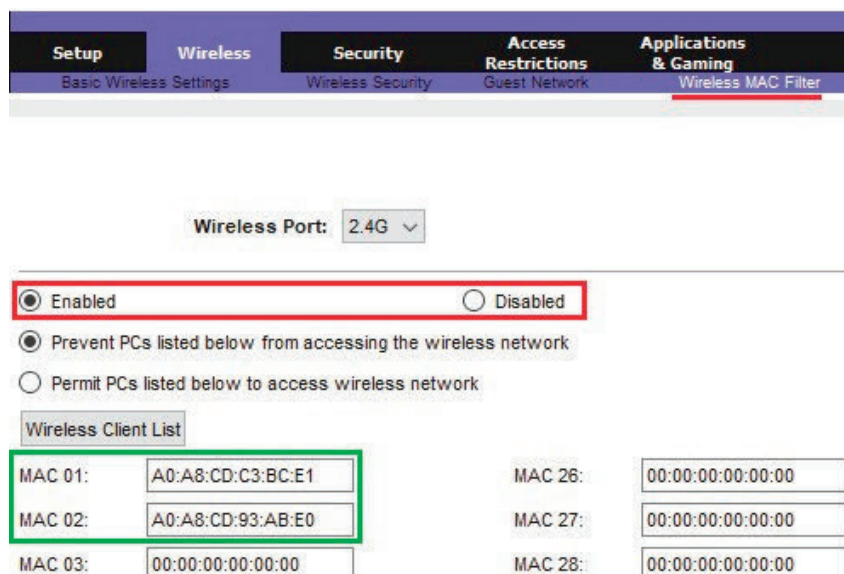
RADIUS Server: 192.168.1.100

RADIUS Port: 1645

Shared Secret: Formip123@

Key Renewal: 3600 seconds

LE FILTRAGE DES ADRESSES MAC



Wireless Port: 2.4G

☒ Enabled ☐ Disabled

☒ Prevent PCs listed below from accessing the wireless network

☐ Permit PCs listed below to access wireless network

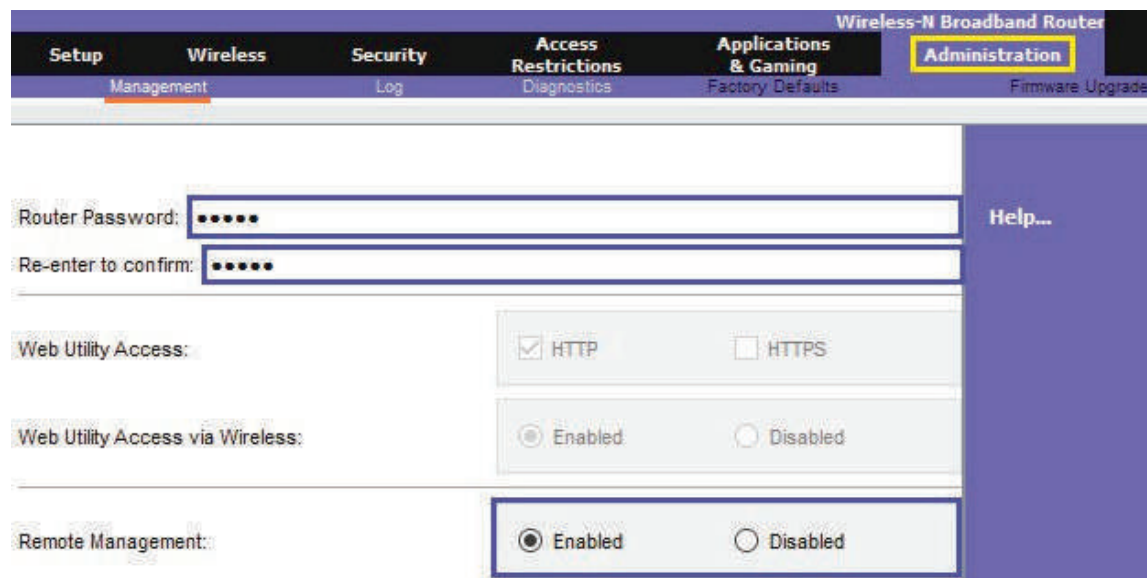
Wireless Client List

MAC 01:	A0:A8:CD:C3:BC:E1	MAC 26:	00:00:00:00:00:00
MAC 02:	A0:A8:CD:93:AB:E0	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00

16.5.3. Administration du routeur sans fil :

Dans l'onglet « **Administration** », on peut configurer :

- ➔ Le mot de passe de gestion pour l'accès au routeur
- ➔ Activation ou la désactivation de l'accès distant



Router Password:

Re-enter to confirm:

Web Utility Access: ☒ HTTP ☐ HTTPS

Web Utility Access via Wireless: ☒ Enabled ☐ Disabled

Remote Management: ☒ Enabled ☐ Disabled

Help...