

**Chapitre 09****Concevoir et sécuriser un WLAN****1. Concepts des réseaux WLAN****1.1. Définition de WLAN**

- Les réseaux sans fil peuvent offrir la mobilité client, une connexion au réseau quels que soient le lieu et le moment et une connexion en itinérance.
- Le réseau local sans fil (**WLAN**, Wireless Local Area Network) est une sous-catégorie de réseau sans fil couramment utilisée par les particuliers, dans les bureaux et les environnements de campus.
- Bien qu'il utilise les fréquences radio en lieu et place de câbles, ce type de réseau est fréquemment implémenté dans un environnement de réseau commuté et son format de trame est similaire à celui d'Ethernet.

**1.2. Avantages des technologies sans fil**

- L'accès sans fil au réseau offre une productivité accrue et permet au personnel d'une entreprise d'être plus détendu.
- La mise en place d'un réseau sans fil peut également réduire les coûts.
- Le réseau sans fil offre une adaptabilité face aux fluctuations des besoins et des technologies ; l'ajout de nouveaux équipements se fait de manière assez transparente dans le cas d'un réseau sans fil.

**1.3. Technologies sans fil**

<b>Bluetooth</b>	Norme <b>WPAN IEEE 802.15</b> . Elle utilise un processus d'appariement des périphériques pour communiquer sur des distances allant jusqu'à 100 m.
<b>Wi-Fi</b>	Norme <b>WLAN IEEE 802.11</b> . Le Wireless Fidelity est couramment déployée pour assurer l'accès au réseau des utilisateurs domestiques et professionnels, avec un trafic de données, voix et vidéo, sur des distances allant jusqu'à 300 m.
<b>WiMAX</b>	Norme <b>WWAN IEEE 802.16</b> . Elle offre un accès sans fil à haut débit jusqu'à 50 km de distance. Elle est une alternative aux connexions câblées et d'ADSL haut débit.
<b>Haut débit cellulaire</b>	Elle offre une connectivité au réseau mobile en haut débit. Elle a été utilisée à ses débuts avec les téléphones portables de 2 <sup>ème</sup> génération (2G), en 1991, puis avec les technologies de communication mobile de 3G et de 4G.
<b>Haut débit satellite</b>	Elle offre un accès réseau aux sites distants via une antenne parabolique directionnelle alignée sur un satellite à orbite géostationnaire (GEO). Elle est généralement plus coûteuse et requiert une visibilité directe.

#### 1.4. Normes IEEE WLAN 802.11


Norme IEEE	Débit maximal	Fréquence	Rétrocompatibilité
802.11	2 Mbit/s	2,4 GHz	—
802.11 a	54 Mbit/s	5 GHz	—
802.11 b	11 Mbit/s	2,4 GHz	—
802.11 g	54 Mbit/s	2,4 GHz	802.11 b
802.11 n	600 Mbit/s	2,4 GHz et 5 GHz	802.11 a/b/g
802.11 ac	1,3 Gbit/s (1 300 Mbit/s)	5 GHz	802.11 a/n
802.11 ad	7 Gbit/s (7 000 Mbit/s)	2,4 GHz, 5 GHz et 60 GHz	802.11 a/b/g/n/ac

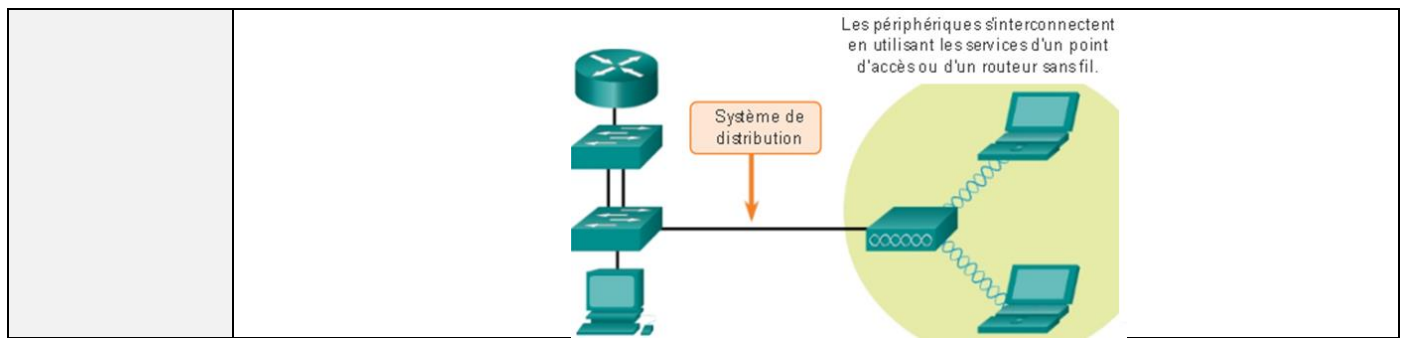
#### 1.5. Comparaison entre WLAN et LAN

Caractéristique	WLAN 802.11	LAN Ethernet 802.3
Couche physique	Fréquence radio ou radiofréquence (RF)	Câble
Accès multimédias	Evitement de collision	Détection de collisions
Disponibilité	Quiconque équipé d'une carte réseau radio dans la portée d'émission d'un point d'accès	Connexion par câble requise
Signaux parasites	Oui	Sans conséquence
Réglementation	Réglementation supplémentaire par les autorités nationales	Norme IEEE

#### 1.6. Topologies WLAN 802.11

- Les WLAN peuvent accueillir plusieurs topologies réseau.
- La norme 802.11 identifie deux principaux modes de topologie sans fil :

<b>Mode ad hoc</b>	<p>Un réseau sans fil ad hoc est composé de deux périphériques sans fil qui communiquent en mode P2P (peer-to-peer), sans utiliser de points d'accès ou de routeurs sans fil. Par exemple, un poste de travail client doté d'une fonctionnalité sans fil peut être configuré pour fonctionner en mode ad hoc, ce qui permet à un autre périphérique de s'y connecter. Le <b>Bluetooth</b> et <b>Wi-Fi Direct</b> sont des exemples de mode ad hoc.</p> 
<b>Mode d'infrastructure</b>	<p>Dans ce mode, l'interconnexion entre les clients sans fil se fait via un <b>point d'accès</b> ou un <b>routeur sans fil</b>. Les points d'accès se connectent à l'infrastructure du réseau par le biais du système de distribution par câble (DS), tel qu'Ethernet.</p>



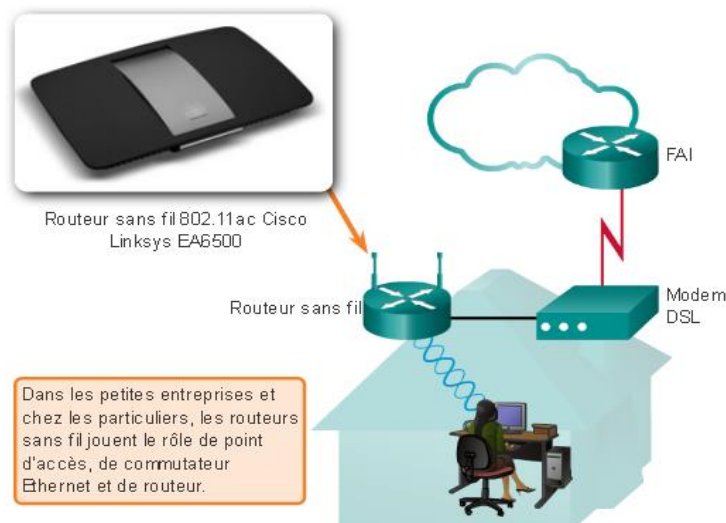
## 2. Composants de WLAN

### 2.1. Cartes réseaux sans fil

- Pour la communication sans fil, les périphériques finaux doivent posséder une carte réseau sans fil intégrant un émetteur/récepteur radio ainsi que le pilote logiciel requis pour la rendre opérationnelle.
- Les ordinateurs portables, les tablettes et les smartphones sont aujourd'hui tous équipés d'une carte réseau sans fil intégrée. Toutefois, lorsqu'un périphérique ne dispose pas d'une telle carte, il est possible d'utiliser un adaptateur sans fil USB.

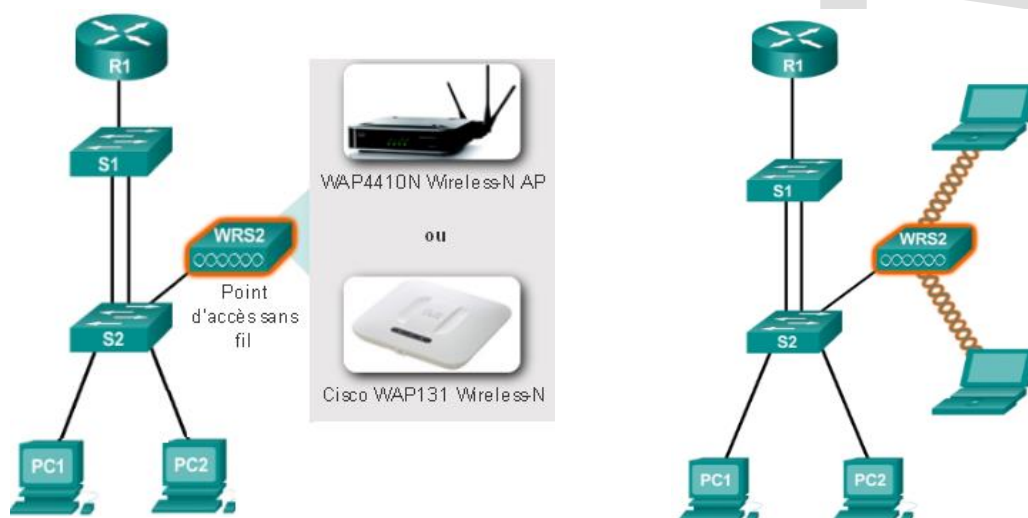
### 2.2. Routeur domestique sans fil

- Le type de périphérique d'infrastructure auquel un périphérique final s'associe et s'authentifie varie en fonction de la taille et des critères d'exigence du WLAN.
- Par exemple, les petites entreprises et les particuliers interconnectent généralement des périphériques sans fil à l'aide d'un petit routeur sans fil intégré qui sert à la fois de :
  - **Point d'accès** : ils fournissent l'accès sans fil 802.11a/b/g/n/ac.
  - **Commutateur** : ils jouent le rôle de commutateur Ethernet 10/100/1000, à quatre ports et bidirectionnel simultané, pour les périphériques filaires connectés.
  - **Routeur** : ils offrent une passerelle par défaut pour la connexion à d'autres infrastructures de réseau.



### 2.3. Solutions professionnelles sans fil

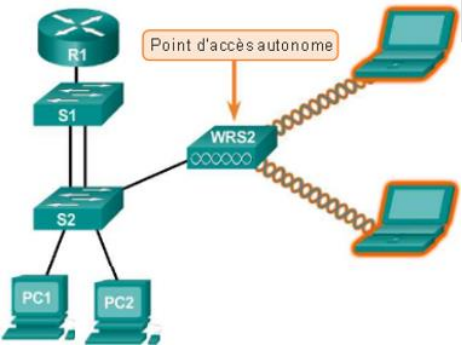
- Les organisations qui fournissent une connectivité sans fil à leurs utilisateurs ont besoin d'une infrastructure WLAN pour proposer des options de connectivité complémentaires.
- La norme IEEE 802.11 fait référence au client sans fil sous le nom de **station (STA)**. Le terme **client sans fil** est souvent utilisé pour décrire un périphérique doté de fonctionnalités sans fil.
- Par exemple, le réseau de petite entreprise suivant est un LAN Ethernet 802.3. Chaque client (PC1 et PC2) est connecté à un commutateur par le biais d'un câble réseau. Le point d'accès sans fil est également connecté au commutateur. Il est possible d'utiliser un point d'accès Cisco WAP4410N AP ou WAP131 AP pour assurer la connectivité du réseau sans fil.



- Remarque** : les besoins sans fil d'une petite organisation diffèrent de ceux d'une organisation de grande taille. Les déploiements sans fil à grande échelle nécessitent du matériel sans fil supplémentaire, afin de simplifier l'installation et la gestion du réseau sans fil.

### 2.4. Points d'accès sans fil

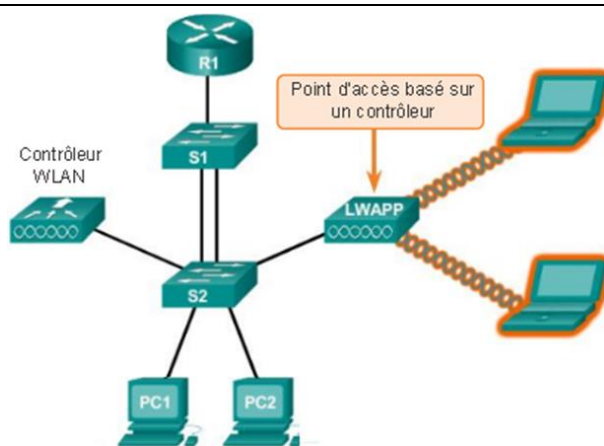
- Les points d'accès peuvent être divisés en deux catégories :

<p>Points d'accès autonomes</p>	<p>Parfois appelés <b>points d'accès intensifs</b>. Ce sont des périphériques indépendants configurés à l'aide de l'interface en ligne de commande Cisco ou d'une interface graphique utilisateur. Ils sont utiles dans les cas où seule une paire de points d'accès est nécessaire sur l'ensemble du réseau. A noter qu'un routeur domestique est un point d'accès autonome, car l'ensemble de la configuration de ce point d'accès se trouve sur le périphérique.</p> 
---------------------------------	---

### Points d'accès basés sur un contrôleur

Ce sont des périphériques dépendants d'un serveur, qui ne nécessitent aucune configuration initiale. Cisco propose deux solutions basées sur un contrôleur.

Ils sont utiles dans les cas où de nombreux points d'accès sont nécessaires sur l'ensemble du réseau. Chaque nouveau point d'accès ajouté est automatiquement configuré et géré par un contrôleur WLAN.



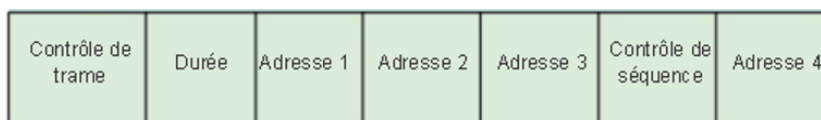
## 3. Fonctionnement du WLAN

### 3.1. Structure de trame 802.11

- La structure d'une trame WLAN 802.11 est la suivante :



- L'en-tête est composé des champs suivants :



Contrôle de trame	Il identifie le type de trame sans fil concerné (version du protocole, type de trame, etc).
Durée	Ce champ est utilisé pour indiquer le délai nécessaire avant transmission de trame suivante.
Adresse 1	Il contient généralement l'adresse MAC du point d'accès ou du périphérique sans fil de réception.
Adresse 2	Il contient généralement l'adresse MAC du point d'accès ou du périphérique sans fil d'émission.
Adresse 3	Il contient parfois l'adresse MAC de la destination, par exemple l'interface du routeur (passerelle par défaut) auquel le point d'accès est associé.
Contrôle de séquence	Il contient les sous-champs Sequence Number (Numéro d'ordre) et Fragment Number (Numéro de fragment). Le premier indique le numéro d'ordre de chaque trame. Le second indique le numéro de chaque trame envoyée dans le cas d'une trame fragmentée.

Adresse 4	Ce champ généralement absent car utilisé uniquement en mode ad hoc.
Données utiles	Il contient les données à transmettre.
FCS	Ce champ est utilisé pour le contrôle des erreurs de couche 2.

### 3.2. Méthode CSMA/CA

- Les WLAN IEEE 802.11 utilisent la méthode CSMA/CA avec le protocole MAC. Bien que le nom soit similaire à celui de la méthode CSMA/CD Ethernet, le concept est totalement différent.
- Pour plus de détails, veuillez consulter la section **CCNA3-4.2.2 Fonctionnement sans fil**

## 4. Configurer et sécuriser les réseaux WLAN

### 4.1. Configurer un routeur sans fil

- Avant d'implémenter des périphériques sans fil, il est recommandé de vérifier que le réseau filaire existant est opérationnel et que les hôtes filaires peuvent accéder aux services Internet.
- Une fois la fonctionnalité du réseau filaire confirmée, le plan d'implémentation suivant peut être appliqué :

Etape 1	Démarrer le processus d'implémentation WLAN avec un point d'accès et un client sans fil uniques, sans activer la sécurité sans fil.
Etape 2	Vérifier que le client a reçu une adresse IP DHCP et peut envoyer une requête ping au routeur filaire local par défaut, puis se connecter au réseau Internet externe.
Etape 3	Configurer la sécurité sans fil avec l'option WPA2/WPA Mixed Personal (WPA2/WPA mixte particulier). N'utiliser jamais la technologie WEP, sauf si aucune autre option n'est disponible.
Etape 4	Sauvegarder la configuration.

- Avant d'installer un routeur sans fil, tenez compte des paramètres suivants :

<b>SSID Name</b>	Nom SSID (c'est le nom du réseau WLAN).
<b>Network Password</b>	Mot de passe de réseau. Lorsque vous y êtes invité, ce mot de passe doit être saisi pour l'association et l'accès au SSID.
<b>Router Password</b>	Mot de passe du routeur (il est équivalent au mot de passe <i>enable secret</i> du mode d'exécution privilégié).
<b>Guest Network SSID Name</b>	Nom SSID du réseau invité. Pour des raisons de sécurité, les invités peuvent être isolés avec un SSID différent.
<b>Guest Network Password</b>	Mot de passe du réseau invité permettant d'accéder au réseau SSID invité.

<b>Linksys Smart Wi-Fi Username</b>	Nom d'utilisateur Linksys Smart Wi-Fi. Compte Internet nécessaire pour accéder au routeur à distance, depuis Internet.
<b>Linksys Smart Wi-Fi Password</b>	Mot de passe Linksys Smart Wi-Fi. Il est nécessaire pour accéder au routeur à distance.

#### **4.2. Configurer les clients WLAN**

- Lorsque le point d'accès ou le routeur sans fil a été configuré, la carte réseau sans fil du client doit à son tour être configurée pour lui permettre de se connecter au WLAN.
- L'utilisateur doit également vérifier que le client a pu se connecter sans problème au réseau sans fil souhaité, car il peut y avoir plusieurs WLAN disponibles à la connexion.

#### **4.3. Problème de sécurité pour les réseaux WLAN**

- La sécurité a toujours été une préoccupation majeure concernant le WLAN.
- Un WLAN est ouvert à toute personne située à proximité d'un point d'accès et disposant des données d'identification nécessaires pour s'y associer. Moyennant une carte réseau sans fil et une connaissance des techniques de piratage, un pirate n'a pas forcément besoin de pénétrer physiquement dans l'espace de travail pour pouvoir accéder à un réseau local sans fil.
- Les attaques peuvent être le fait de personnes extérieures à l'entreprise et d'employés mécontents, mais aussi la conséquence accidentelle de l'action d'un employé. Les réseaux sans fil sont particulièrement sensibles à certaines menaces, notamment :

<b>Intrusions sans fil</b>	Des utilisateurs non autorisés tentent d'accéder à des ressources réseau. La solution consiste à dissuader les intrus par l'authentification.
<b>Applications criminelles</b>	Des points d'accès non autorisés peuvent être installés par un utilisateur naïf ou délibérément, à des fins malveillantes. Utilisez un logiciel de gestion sans fil pour détecter les points d'accès non autorisés.
<b>Interception de données</b>	Les données dans fil peuvent être capturées facilement au moyen d'interceptions illicites. Utilisez le chiffrement pour protéger les données échangées entre les clients et les points d'accès.
<b>Attaques par déni de service</b>	Les services des WLAN peuvent être compromis accidentellement ou avec malveillance. Différentes solutions sont possibles, selon la source du DoS.

- Pour faire face aux menaces, tenir les intrus à distance et protéger les données, deux fonctions de sécurité préliminaires ont été appliquées :

<b>Masquage SSID</b>	Les points d'accès et certains routeurs sans fil permettent de masquer le SSID. Les clients sans fil doivent alors identifier manuellement le SSID pour se connecter au réseau.
<b>Filtrage des adresses MAC</b>	Un administrateur peut manuellement autoriser ou refuser l'accès à des clients sans fil, sur la base de l'adresse MAC.

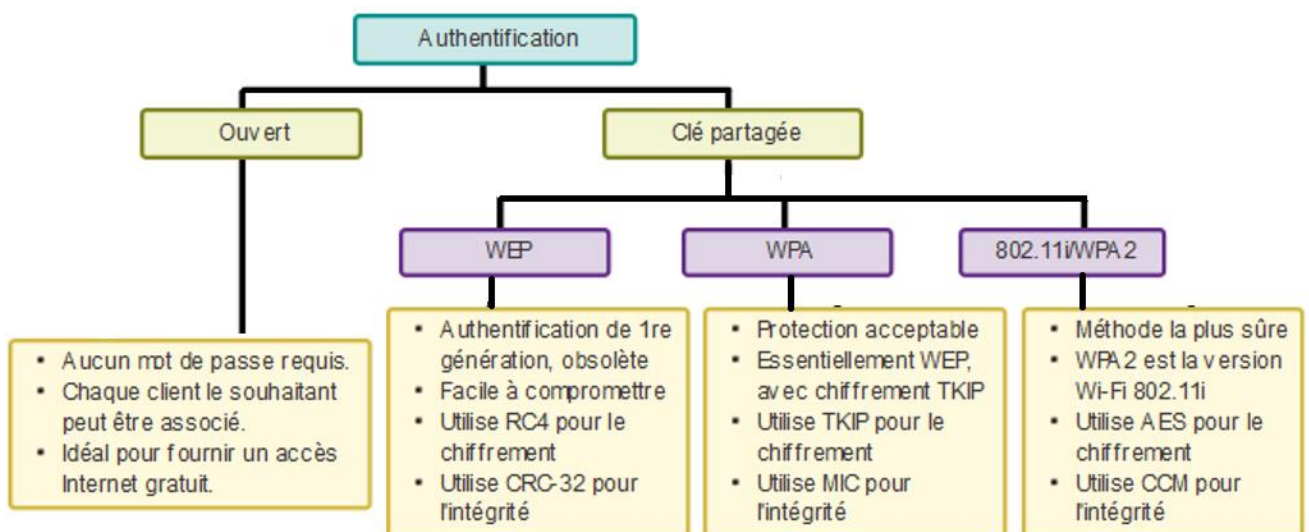
- **Remarque** : Les identifiants SSID sont faciles à trouver, même lorsque les points d'accès ne les diffusent pas ; et les adresses MAC peuvent être usurpées. Le meilleur moyen de sécuriser un réseau sans fil est d'utiliser des systèmes d'authentification et de chiffrement.

#### 4.4. Systèmes d'authentification

- La norme 802.11 d'origine avait établi deux types d'authentification :

<b>Authentification système ouverte</b>	Tous les clients sans fil peuvent se connecter facilement. Cette option est à utiliser uniquement lorsque la sécurité n'est pas une préoccupation (par exemple dans les endroits offrant un accès Internet gratuit, tels que les cafés et les hôtels).
<b>Authentification par clé partagée</b>	Fournit des mécanismes, tels que WEP, WPA et WPA2, pour authentifier et chiffrer les données entre un client sans fil et un point d'accès. Cependant, le mot de passe doit être partagé au préalable entre les deux parties à connecter.

	WEP	WPA	802.11i/WPA 2
<b>Méthode d'authentification</b>	Clé prépartagée	PSK ou 802.1x	PSK ou 802.1x
<b>Chiffrement</b>	RC4	TKIP	AES
<b>Intégrité des messages</b>	CRC-32	MIC	CCMP
<b>Sécurité</b>	Faible	Forte	Plus forte





#### 4.5. Méthodes de chiffrement

- Le chiffrement est une technique utilisée pour protéger les données. Si un intrus capture des données chiffrées, il sera incapable de les déchiffrer pendant un délai raisonnable.
- Les normes IEEE 802.11i, WPA et WPA2 utilisent les protocoles de chiffrement suivants :

<b>TKIP</b> (Temporal Key Integrity Protocol)	C'est la méthode de chiffrement utilisée par la norme WPA. Elle est basée sur la technique WEP, mais chiffre les données utiles de couche 2 en TKIP et effectue un contrôle MIC (Message Integrity Check) au niveau du paquet crypté pour s'assurer que le message n'a pas été altéré.
<b>AES</b> (Advanced Encryption Standard)	C'est la méthode de chiffrement préférée et utilisée par la norme WPA2. Elle exécute les mêmes fonctions que le protocole TKIP, mais offre un chiffrement bien plus solide qui permet aux hôtes de destination de savoir si les bits chiffrés et non chiffrés ont été altérés.

- Remarque** : choisissez toujours la norme WPA2 avec la technologie AES, lorsque cela est possible.

#### 4.6. Authentification d'un utilisateur domestique

- En général, les normes WPA et WPA2 prennent en charge deux types d'authentification :

<b>Particulier</b>	Destinée aux réseaux domestiques et de PME/PMI, les utilisateurs s'authentifient à l'aide d'une clé prépartagée (PSK). Les clients sans fil s'authentifient auprès du point d'accès à l'aide d'un mot de passe prépartagé. Aucun serveur d'authentification spécial n'est requis.
<b>Entreprise</b>	Destinée aux réseaux d'entreprise, elle requiert un serveur d'authentification <b>RADIUS</b> (Remote Authentication Dial-In User Service). Bien que plus compliquée à configurer, cette méthode offre une sécurité renforcée. Le périphérique doit être authentifié par le serveur RADIUS, puis les utilisateurs doivent s'authentifier à l'aide de la norme <b>802.1X</b> , qui utilise le protocole <b>EAP</b> (Extensible Authentication Protocol) pour l'authentification.

#### 4.7. Authentification au sein de l'entreprise

- Dans les réseaux présentant des besoins de sécurité très stricts, une authentification ou une identification supplémentaire est requise pour octroyer l'accès aux clients sans fil.
- Les options du mode de sécurité Entreprise nécessitent l'utilisation d'un serveur **RADIUS AAA** (Authentication, Authorization, and Accounting).