7 WLAN sécurisés

Vidéo – WLAN sécurisés

Cette vidéo présentera les points suivants :

- Masquage SSID
- Filtrage d'adresses MAC
- Systèmes d'authentification et de cryptage (authentification ouverte et authentification à clé partagée)

Masquage SSID et filtrage des adresses MAC

Pour faire face aux menaces de garder les intrus sans fil à l'extérieur et de protéger les données, deux premières fonctions de sécurité ont été utilisées et sont toujours disponibles sur la plupart des routeurs et des points d'accès:

Masquage SSID

- Les points d'accès et certains routeurs sans fil permettent de désactiver la trame de balise SSID. Les clients sans fil doivent être configurés manuellement avec le SSID pour se connecter au réseau.

Filtrage d'adresses MAC

- Un administrateur peut autoriser ou refuser manuellement l'accès sans fil des clients en fonction de leur adresse matérielle MAC physique. Dans la figure, le routeur est configuré pour autoriser deux adresses MAC. Les appareils avec des adresses MAC différentes ne pourront pas rejoindre le WLAN 2,4 GHz.

Méthodes d'authentification d'origine du 802.11

La meilleure façon de sécuriser un réseau sans fil est d'utiliser des systèmes d'authentification et de cryptage. Deux types d'authentification ont été introduits avec la norme 802.11 d'origine:

L'authentification de système ouvert,

- Aucun mot de passe requis. Généralement utilisé pour fournir un accès Internet gratuit dans les espaces publics comme les cafés, les aéroports et les hôtels.
- Le client est responsable d'assurer la sécurité, par exemple via un VPN.

Authentification par clé partagée

- Fournit des mécanismes, tels que WEP, WPA, WPA2 et WPA3 pour authentifier et crypter les données entre un client sans fil et AP. Cependant, le mot de passe doit être pré-partagé entre les deux parties pour se connecter.

Méthodes d'authentification par clé partagée

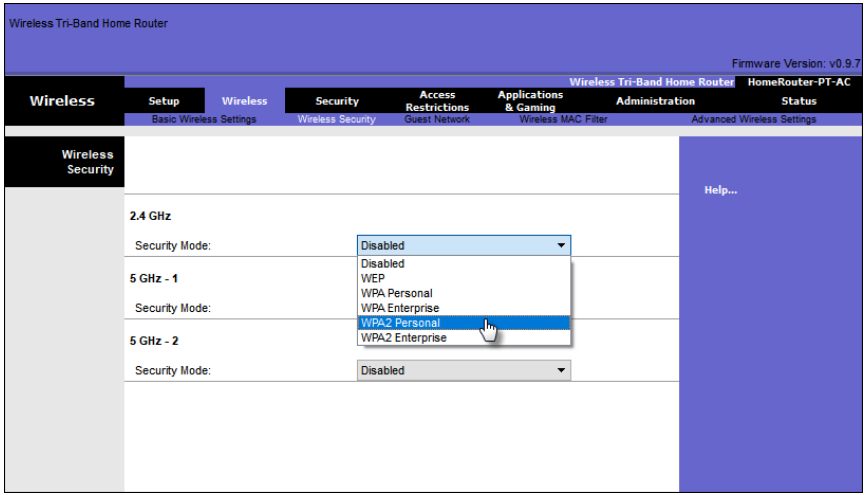
Il existe quatre techniques d'authentification par clé partagée, comme décrit dans le tableau.

Méthode d'authentification	Description
WEP (Wired Equivalent Privacy)	La spécification 802.11 originale conçue pour sécuriser les données à l'aide de la méthode de chiffrement Rivest Cipher 4 (RC4) avec une clé statique. Le WEP n'est plus recommandé et ne doit jamais être utilisé.
Fonction WPA (Wi-Fi Protected Access)	Une norme de l'Alliance Wi-Fi qui utilise le protocole WEP mais sécurise les données grâce à l'algorithme de cryptage TKIP (Temporal Key Integrity Protocol), beaucoup plus puissant. Le protocole TKIP modifie la clé pour chaque paquet, rendant très difficile son piratage.
WPA2	Il utilise le standard de cryptage avancé (AES) pour le cryptage. Le mode de chiffrement AES est actuellement considéré comme étant le protocole de chiffrement le plus puissant.
WPA3	Il s'agit de la prochaine génération de sécurité Wi-Fi. Tous les appareils compatibles WPA3 utilisent les dernières méthodes de sécurité, interdisent les protocoles hérités obsolètes et nécessitent l'utilisation de cadres de gestion protégés (PMF).

Authentification d'un Utilisateur à Domicile

Les routeurs domestiques ont généralement deux choix pour l'authentification: WPA et WPA2.

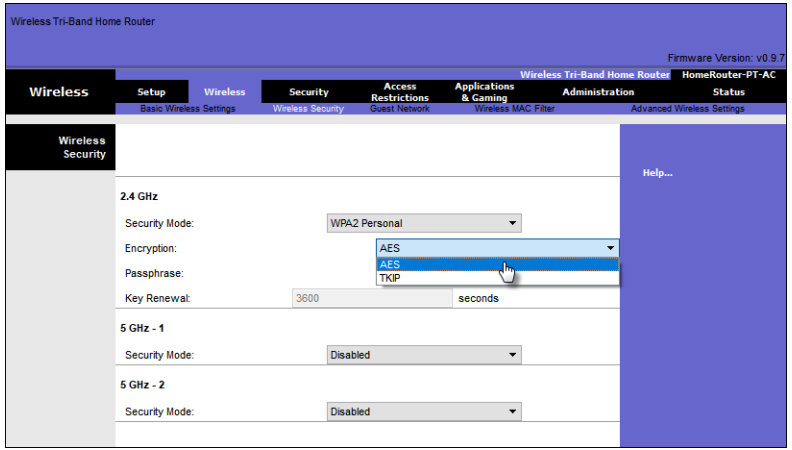
- **Personnel** - Destiné aux réseaux domestiques ou de petites entreprises, les utilisateurs s'authentifient à l'aide d'une clé pré-partagée (PSK). Les clients sans fil s'authentifient auprès du routeur sans fil à l'aide d'un mot de passe pré-partagé. Aucun serveur d'authentification spécial n'est requis.
- **Entreprise** - Destiné aux réseaux d'entreprise. Nécessite un serveur d'authentification RADIUS (Remote Authentication Dial-In User Service). Le périphérique doit être authentifié par le serveur RADIUS, puis les utilisateurs doivent s'authentifier à l'aide de la norme 802.1X, qui utilise le protocole EAP (Extensible Authentication Protocol) pour l'authentification.



Méthodes de Cryptage

WPA et WPA2 incluent deux protocoles de chiffrement:

- **Protocole d'Intégrité de Clé Temporelle (TKIP)** – Utilisé par WPA et prend en charge les équipements WLAN hérités. Utilise WEP mais chiffre la charge utile de couche 2 à l'aide de TKIP.
- **Norme de Cryptage Avancée (AES)** - Utilisé par WPA2 et utilise le mode de chiffrement du compteur avec le protocole CCMP (Block Chaining Message Authentication Code Protocol) qui permet aux hôtes de destination de reconnaître si les bits cryptés et non cryptés ont été altérés.

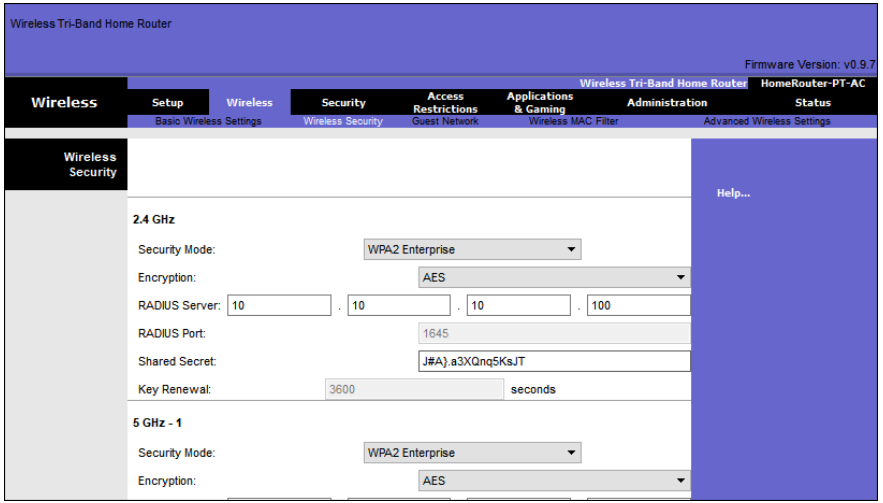


Authentification dans l'Entreprise

Le choix du mode de sécurité d'entreprise nécessite un serveur RADIUS d'authentification, d'autorisation et de comptabilité (AAA).

Des informations sont nécessaires:

- **Adresse IP du serveur RADIUS** - Adresse IP du serveur.
- **Numéros de port UDP** - Ports UDP 1812 pour l'authentification RADIUS et 1813 pour la comptabilité RADIUS, mais peuvent également fonctionner à l'aide des ports UDP 1645 et 1646.
- **Clé partagée** - Utilisée pour authentifier l'AP avec le serveur RADIUS.



Remarque: l'authentification et l'autorisation des utilisateurs sont gérées par la norme 802.1X, qui fournit une authentification centralisée sur serveur des utilisateurs finaux.

WPA 3

Parce que WPA2 n'est plus considéré comme sécurisé, WPA3 est recommandé lorsqu'il est disponible. WPA3 comprend quatre fonctionnalités:

- **WPA3 - Personnel:** Déjoue les attaques par force brute en utilisant l'authentification simultanée des égaux (SAE).
- **WPA3 - Entreprise:** Utilise l'authentification 802.1X / EAP. Cependant, il nécessite l'utilisation d'une suite cryptographique 192 bits et élimine le mélange des protocoles de sécurité pour les normes 802.11 précédentes.
- **Réseaux ouverts:** N'utilise aucune authentification. Cependant, ils utilisent le chiffrement sans fil opportuniste (OWE) pour chiffrer tout le trafic sans fil.
- **IoT Onboarding:** Utilise le protocole DPP (Device Provisioning Protocol) pour intégrer rapidement les appareils IoT.