Exemple de configuration de WEP sur un point d'accès autonome

Table des matières

Introduction

Ce document décrit comment utiliser et configurer Wired Equivalent Privacy (WEP) sur un point d'accès autonome (AP) Cisco.

Conditions préalables

Exigences

Ce document suppose que vous pouvez établir une connexion administrative avec les périphériques WLAN et que ces périphériques fonctionnent normalement dans un environnement non chiffré. Pour configurer un WEP 40 bits standard, vous devez disposer d'au moins deux unités radio qui communiquent entre elles.

Composants utilisés

Les informations de ce document sont basées sur un point d'accès 1140 qui exécute Cisco IOS® version15.2JB.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

WEP est l'algorithme de chiffrement intégré à la norme 802.11 (Wi-Fi). WEP utilise le chiffrement de flux RC4 pour la confidentialité, et la somme de contrôle de redondance cyclique Check-32 (CRC-32) pour l'intégrité.

Le WEP 64 bits standard utilise une clé 40 bits (également appelée WEP-40), qui est concaténée avec un vecteur d'initialisation (IV) de 24 bits afin de former la clé RC4. Une clé WEP 64 bits est généralement saisie sous la forme d'une chaîne de 10 caractères hexadécimaux (base 16) (zéro à neuf et A à F). Chaque caractère représente quatre bits, et dix chiffres de quatre bits correspondent chacun à 40 bits ; si vous ajoutez la clé IV de 24 bits, elle produit la clé WEP complète de 64 bits.

Une clé WEP 128 bits est généralement saisie sous la forme d'une chaîne de 26 caractères hexadécimaux. Vingt-six chiffres de quatre bits correspondent chacun à 104 bits ; si vous ajoutez la clé IV de 24 bits, elle produit la clé WEP complète de 128 bits. La plupart des périphériques permettent à l'utilisateur d'entrer la clé sous la forme de 13 caractères ASCII.

Méthodes d'authentification

Deux méthodes d'authentification peuvent être utilisées avec WEP : Open System Authentication et Shared Key Authentication.

Avec Open System Authentication, le client WLAN n'a pas besoin de fournir des informations d'identification à l'AP pour l'authentification. Tout client peut s'authentifier auprès du point d'accès, puis tenter de s'associer. En effet, aucune authentification n'a lieu. Par la suite, des clés WEP peuvent être utilisées afin de chiffrer des trames de données. À ce stade, le client doit disposer des clés correctes.

Avec l'authentification par clé partagée, la clé WEP est utilisée pour l'authentification dans un échange de demande de confirmation/réponse en quatre étapes :

1. Le client envoie une demande d'authentification au point d'accès.
2. Le point d'accès répond par une demande en texte clair.
3. Le client chiffre le texte de demande de confirmation à l'aide de la clé WEP configurée et répond par une autre demande d'authentification.
4. Le point d'accès déchiffre la réponse. Si la réponse correspond au texte de défi, le point d'accès envoie une réponse positive.

Après l'authentification et l'association, la clé WEP pré-partagée est également utilisée afin de chiffrer les trames de données avec RC4.

À première vue, il peut sembler que l'authentification par clé partagée est plus sécurisée que l'authentification par système ouvert, car cette dernière n'offre aucune authentification réelle. Cependant, l'inverse est vrai. Il est possible de dériver le flux de clés utilisé pour la connexion si vous capturez les trames de demande de confirmation dans l'authentification par clé partagée. Par conséquent, il est conseillé d'utiliser l'authentification système ouverte pour l'authentification WEP, plutôt que l'authentification par clé partagée.

Le protocole TKIP (Temporal Key Integrity Protocol) a été créé pour résoudre ces problèmes

WEP. Tout comme le protocole WEP, TKIP utilise le cryptage RC4. Cependant, TKIP améliore le protocole WEP en ajoutant des mesures telles que le hachage de clé par paquet, le contrôle d'intégrité des messages (MIC) et la rotation de clé de diffusion afin de remédier aux vulnérabilités connues du protocole WEP. Le protocole TKIP utilise le chiffrement de flux RC4 avec des clés 128 bits pour le chiffrement et des clés 64 bits pour l'authentification.

Configurer

Cette section présente les configurations de l'interface graphique et de la CLI pour WEP.

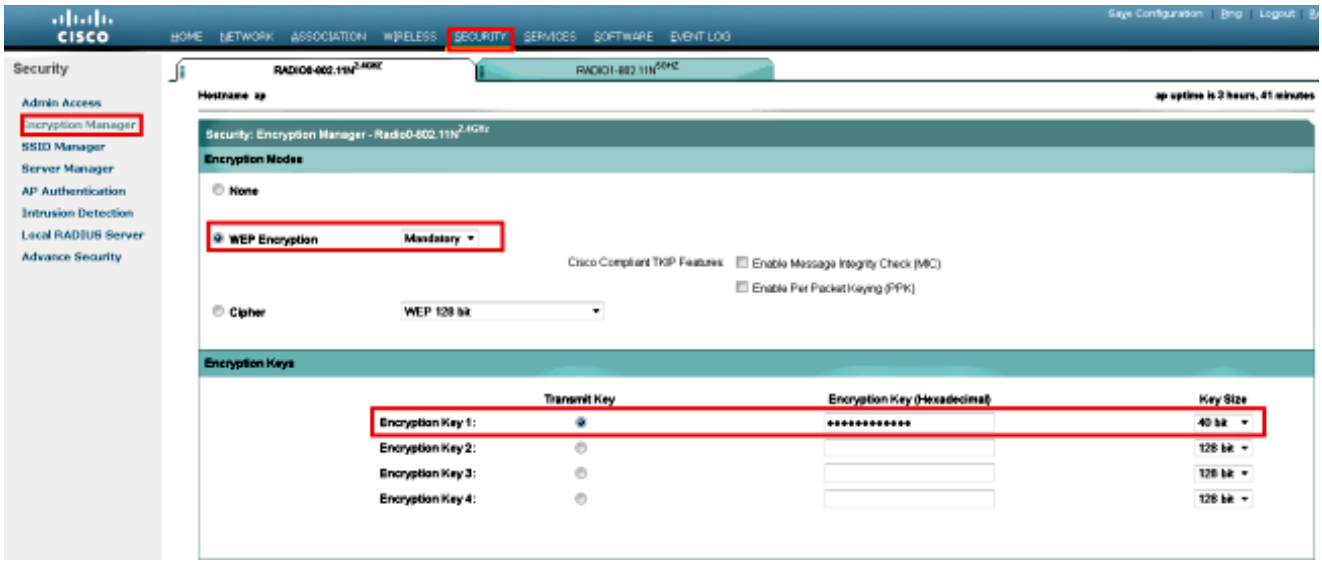
Configuration de la GUI

Complétez ces étapes afin de configurer WEP avec l'interface graphique utilisateur.

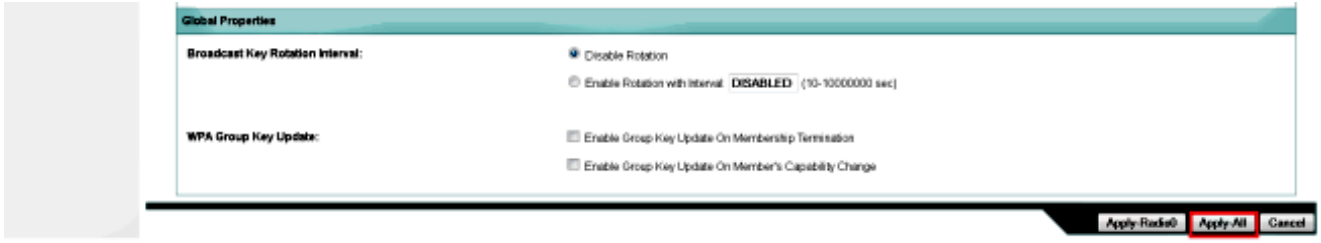
1. Connectez-vous au point d'accès via l'interface utilisateur graphique.
2. Dans le menu Security sur le côté gauche de la fenêtre, choisissez Encryption Manager pour l'interface radio vers laquelle vous voulez configurer vos clés WEP statiques.
3. Sous Encryption Modes, cliquez sur WEP Encryption, puis sélectionnez Mandatory dans le menu déroulant du client.

   Les modes de cryptage utilisés par la station sont les suivants :
   - Default (No Encryption) : requiert que les clients communiquent avec le point d'accès sans cryptage des données. Ce paramètre n'est pas recommandé.
   - Facultatif - Permet aux clients de communiquer avec le point d'accès avec ou sans cryptage des données. En général, vous utilisez cette option lorsque vous avez des périphériques clients qui ne peuvent pas établir de connexion WEP, tels que des clients non-Cisco dans un environnement WEP 128 bits.
   - Mandatory (Full Encryption) : exige que les clients utilisent le cryptage des données lorsqu'ils communiquent avec le point d'accès. Les clients qui n'utilisent pas le chiffrement des données ne sont pas autorisés à communiquer. Cette option est recommandée si vous souhaitez optimiser la sécurité de votre WLAN.
4. Sous Encryption Keys, sélectionnez la case d'option Transmit Key, puis entrez la clé hexadécimale à 10 chiffres. Assurez-vous que la taille de clé est définie sur 40 bits.

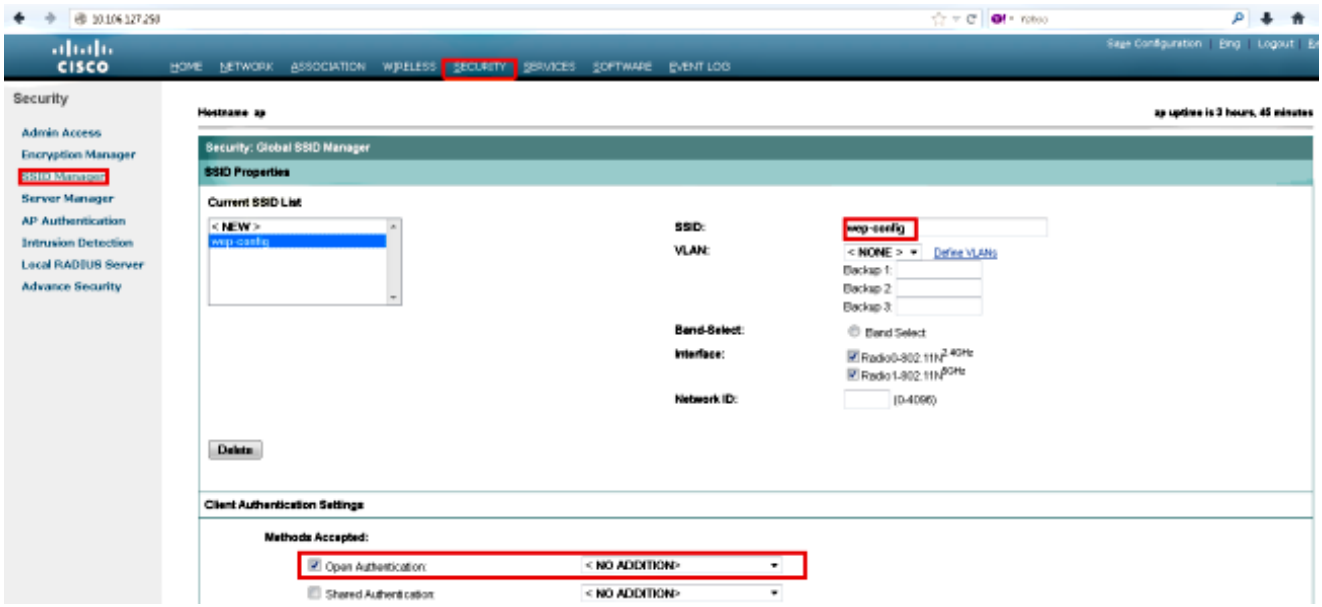
   Entrez 10 chiffres hexadécimaux pour les clés WEP 40 bits ou 26 chiffres hexadécimaux pour les clés WEP 128 bits. Les clés peuvent être n'importe quelle combinaison de ces chiffres :
   - 0 à 9
   - a à f
   - A à F



5. Cliquez sur Apply-All afin d'appliquer la configuration sur les deux radios.



6. Créez un SSID (Service Set Identifier) avec Open Authentication, et cliquez sur Apply afin de l'activer sur les deux radios.



7. Accédez au réseau et activez les radios pour 2,4 GHz et 5 GHz afin de les faire fonctionner.

Configuration CLI

Utilisez cette section afin de configurer WEP avec l'interface de ligne de commande.

<#root>

ap#

show run

```
Building configuration...

Current configuration : 1794 bytes
!
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
!
no aaa new-model
ip cef
!
!
!
dot11 syslog
!
  dot11 ssid wep-config
  authentication open
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
```

```
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1

 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
!
bridge 1 route ip
```

```
!
!
!
line con 0
line vty 0 4
login local
transport input all
!
end
```

Vérifier

Entrez cette commande afin de confirmer que votre configuration fonctionne correctement :

<#root>

ap#

show dot11 associations

```
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address    IP address      Device        Name           Parent         State
1cb0.94a2.f64c 10.106.127.251  unknown       -              self           Assoc
```

Dépannage

Utilisez cette section afin de dépanner votre configuration.

> Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

Ces commandes debug sont utiles afin de dépanner la configuration :

- debug dot11 events - Active le débogage pour tous les événements dot1x.
- debug dot11 packets - Active le débogage pour tous les paquets dot1x.

Voici un exemple de journal qui s'affiche lorsque le client s'associe avec succès au WLAN :

```
*Mar  1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
1cb0.94a2.f64c Associated KEY_MGMT[NONE]
```

Lorsque le client saisit la mauvaise clé, cette erreur s'affiche :

```
*Mar  1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key
mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c
*Mar  1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
Station 1cb0.94a2.f64c Reason: Sending station has left the BSS
*Mar  1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.