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

Contenu

Introduction

Ce document décrit comment à utiliser-et configurez le Confidentialité équivalente aux transmissions par fil (WEP) sur un point d'accès autonome de Cisco (AP).

Conditions préalables

Conditions requises

Ce document suppose que vous pouvez établir un rapport administratif aux périphériques WLAN, et que les périphériques fonctionnent normalement dans un environnement décrypté. Afin de configurer un 40-bit standard WEP, vous devez avoir deux unités par radio ou plus qui communiquent les uns avec les autres.

Composants utilisés

Les informations dans ce document sont basées sur des 1140 AP qui exécutent le Cisco IOS® Release15.2JB.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le WEP est l'algorithme de chiffrement établi dans la norme de 802.11 (WiFi). Le WEP utilise le chiffrement de flux RC4 pour la confidentialité, et la somme de contrôle cyclique de la Redondance Check-32 (CRC-32) pour l'intégrité.

Le WEP 64-bit standard utilise un bit 40 principal (également connu comme WEP-40), qui est concaténé avec 24-bit un vecteur d'initialisation (iv) afin de former la clé RC4. Une clé WEP 64-bit est habituellement écrite comme chaîne de 10 (base 16) caractères hexadécimaux (zéro à neuf et à A-F). Chaque caractère représente quatre bits, et chiffres des dizaines de quatre bits chacun égale 40 bits ; si vous ajoutez le 24-bit IV, il produit la clé WEP 64-bit complète.

Une clé WEP 128-bit est habituellement écrite comme chaîne de 26 caractères hexadécimaux. Vingt-six chiffres de quatre bits bits chaque equals104 ; si vous ajoutez le 24-bit IV, il produit la clé WEP 128-bit complète. La plupart des périphériques permettent à l'utilisateur pour introduire la clé en tant que 13 caractères ASCII.

Méthodes d'authentification

Deux méthodes d'authentification peuvent être utilisées avec le WEP : Authentification Système ouvert et authentification principale partagée.

Avec l'authentification Système ouvert, le client WLAN n'a pas besoin de fournir des qualifications à AP pour l'authentification. N'importe quel client peut authentifier avec AP, et puis tente de s'associer. En effet, aucune authentification ne se produit. Ultérieurement, des clés WEP peuvent être utilisées afin de chiffrer des trames de données. En ce moment, le client doit avoir les clés correctes.

Avec l'authentification principale partagée, la clé WEP est utilisée pour l'authentification dans un à quatre phases, prise de contact de défi-réponse :

1. Le client envoie une demande d'authentification à AP.
2. AP répond avec un défi de libellé.
3. Le client chiffre le texte de défi avec la clé WEP configurée, et répond avec une autre demande d'authentification.
4. AP déchiffre la réponse. Si la réponse apparie le texte de défi, AP 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 le RC4.

Au premier regard, il pourrait sembler comme si l'authentification principale partagée est plus sécurisé qu'authentification Système ouvert, puisque ce dernier n'offre aucune vraie authentification. Cependant, l'inverse est vrai. Il est possible de dériver le flot de clés utilisé pour la prise de contact si vous capturez les trames de défi dans l'authentification principale partagée. Par conséquent, il est recommandé d'utiliser l'authentification Système ouvert pour l'authentification WEP, plutôt que l'authentification principale partagée.

Le Protocole TKIP (Temporal Key Integrity Protocol) a été créé afin d'aborder ces questions WEP. Semblable au WEP, le TKIP utilise le cryptage RC4. Cependant, le TKIP améliore le WEP en plus des mesures telles que le hachage de clé de par-paquet, la rotation principale du Message Integrity Check (MIC), et de l'émission afin d'adresser des vulnérabilités connues WEP. Le TKIP utilise le chiffrement du flux RC4 avec les clés 128-bit pour le cryptage et les clés 64-bit pour l'authentification.

Configurez

Cette section fournit les configurations GUI et CLI pour le WEP.

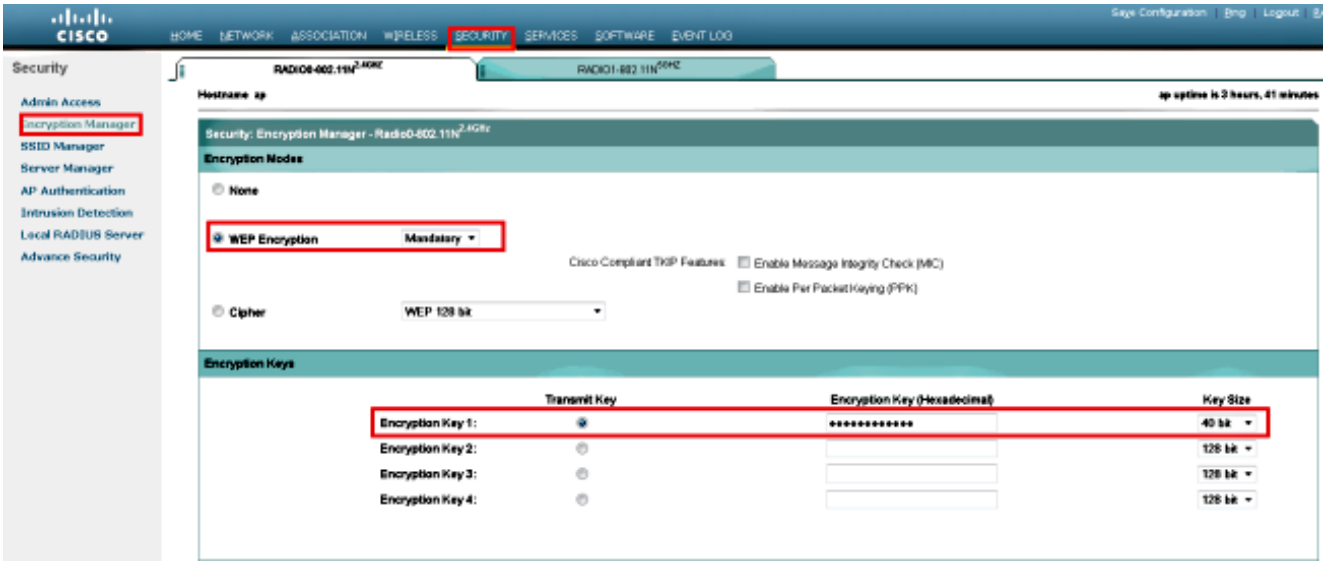
Configuration de la GUI

Terminez-vous ces étapes afin de configurer le WEP avec le GUI.

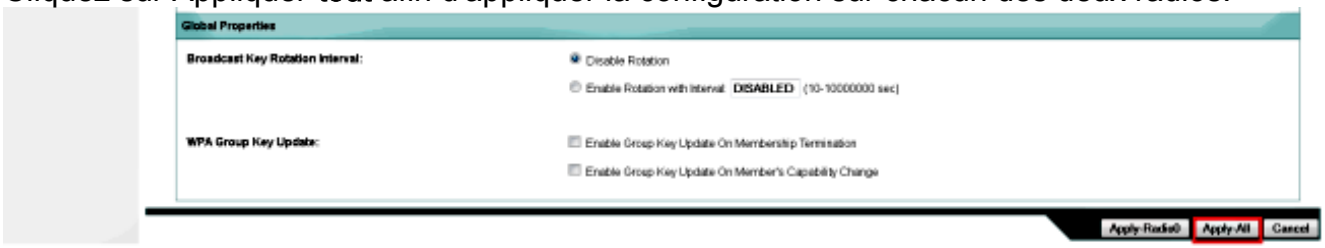
1. Connectez à AP par le GUI.
2. Du menu Security du côté gauche de la fenêtre, choisissez le **gestionnaire de cryptage** pour l'interface par radio à laquelle vous voulez configurer vos clés WEP statiques.
3. Sous des modes de chiffrement, cliquez sur le **cryptage WEP**, et sélectionnez **obligatoire du** menu déroulant pour le client.

   Les modes de chiffrement utilisés par la station sont :
   Par défaut (aucun cryptage) - Exige des clients de communiquer avec AP sans n'importe quel chiffrement de données. Cette configuration n'est pas recommandée.**Facultatif** - Permet à des clients pour communiquer avec AP l'un ou l'autre avec ou sans le chiffrement de données. Typiquement, vous utilisez cette option quand vous avez des périphériques de client qui ne peuvent pas établir un rapport WEP, tel que des clients de non-Cisco dans un environnement 128-bit WEP.**Obligatoire (chiffrement complet)** - Exige des clients d'utiliser le chiffrement de données quand ils communiquent avec AP. On ne permet pas aux des clients qui n'utilisent pas le chiffrement de données pour communiquer. Cette option est recommandée si vous souhaitez maximiser la Sécurité de votre WLAN.
4. Sous des clés de chiffrement, sélectionnez la case d'option de **touche de transmission**, et introduisez la clé de l'hexadécimal 10-digit. Assurez-vous que la taille de clé est fixée au **bit 40**.

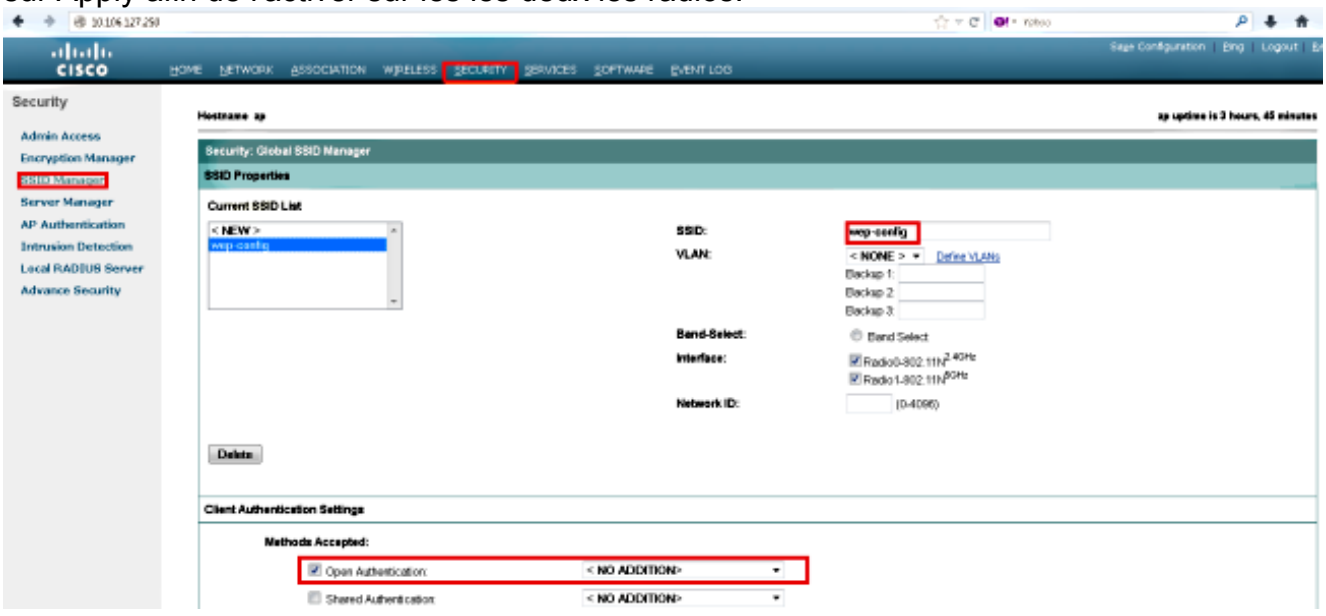
   Écrivez 10 chiffres hexadécimaux pour les clés WEP 40-bit, ou 26 chiffres hexadécimaux pour les clés WEP 128-bit. Les clés peuvent être n'importe quelle combinaison de ces chiffres :
   0 à 9a à fA à
   F



5. Cliquez sur Appliquer-**tout** afin d'appliquer la configuration sur chacun des deux radios.



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



7. Naviguez vers le réseau, et permettez aux radios pour **2.4 gigahertz** et **5 gigahertz** afin de les obtenir exécution.

Configuration CLI

Employez cette section afin de configurer le WEP avec le CLI.

```
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
```

Vérifiez

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

```
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
```

Dépannez

Utilisez cette section afin de dépanner votre configuration.

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Ces commandes de **débogage** sont utiles afin de dépanner la configuration :

- **événements de debug dot11** - Active le débogage pour tous les événements de dot1x.
- **paquets de debug dot11** - Active le débogage pour tous les paquets de dot1x.

Voici un exemple du log qui affiche quand le client s'associe avec succès au WLAN :

```
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
```

Quand le client introduit la clé fausse, des affichages de cette erreur :

```
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
```