Exemple de configuration du protocole WEP (Wired Equivalent Privacy) sur les points d'accès et les ponts Aironet

Contenu

Introduction

Ce document propose des méthodes pour configurer le Wired Equivalent Privacy (WEP) sur les composants du réseau local sans fil (WLAN) de Cisco Aironet.

Remarque: Référez-vous à la section statique de clés de Web du chapitre 6 - configurer des WLAN pour plus d'informations sur la configuration WEP sur les contrôleurs LAN Sans fil (WLCs).

Le WEP est l'algorithme de chiffrement établi dans la norme de 802.11 (WiFi). Le cryptage WEP utilise le chiffrement de flux du code 4 de Ron (RC4) avec 40- ou clés 104-bit et 24-bit un vecteur d'initialisation (iv).

Pendant que la norme spécifie, le WEP utilise l'algorithme RC4 avec une clé 40-bit ou 104-bit et un 24-bit IV. RC4 est un algorithme symétrique parce qu'il utilise la même clé pour le cryptage et le déchiffrement des données. Quand le WEP est activé, chaque « station » par radio a une clé. La clé est utilisée pour brouiller les données avant la transmission des données par les ondes hertziennes. Si une station reçoit un paquet qui n'est pas brouillé avec la clé appropriée, le paquet est jeté et pas livré jamais à l'hôte.

Le WEP peut être principalement utilisé pour un bureau à domicile ou un petit bureau qui n'exige pas très la forte sécurité.

L'implémentation de l'Aironet WEP est dans le matériel. Par conséquent, l'incidence des performances minimale résulte quand vous utilisez le WEP.

Remarque: Il y a quelques problèmes connus avec le WEP, qui lui fait pas une méthode de cryptage fort. Les questions sont :

- Il y a beaucoup de frais d'administration pour mettre à jour une clé WEP partagée.
- Le WEP a le même problème que tous les systèmes basés sur des clés partagées. N'importe quel secret donné à une personne devient public après une période.
- L'IV qui injecte l'algorithme WEP est introduit le texte clair.
- La somme de contrôle WEP est Linéaire et prévisible.

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

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 40-bit standard WEP, vous devez avoir deux unités par radio ou plus qui communiquent les uns avec les autres.

Remarque: Les produits Aironet peuvent établir des connexions 40-bit WEP avec des Produits d'IEEE 802.11b-compliant non-Cisco. Ce document n'adresse pas la configuration d'autres périphériques.

Pour la création d'un lien 128-bit WEP, les Produits Cisco interagissent seulement avec d'autres Produits Cisco.

Composants utilisés

Utilisez ces composants avec ce document :

- Deux unités par radio ou plus qui communiquent les uns avec les autres
- Une connexion administrative au périphérique WLAN

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.

Conventions

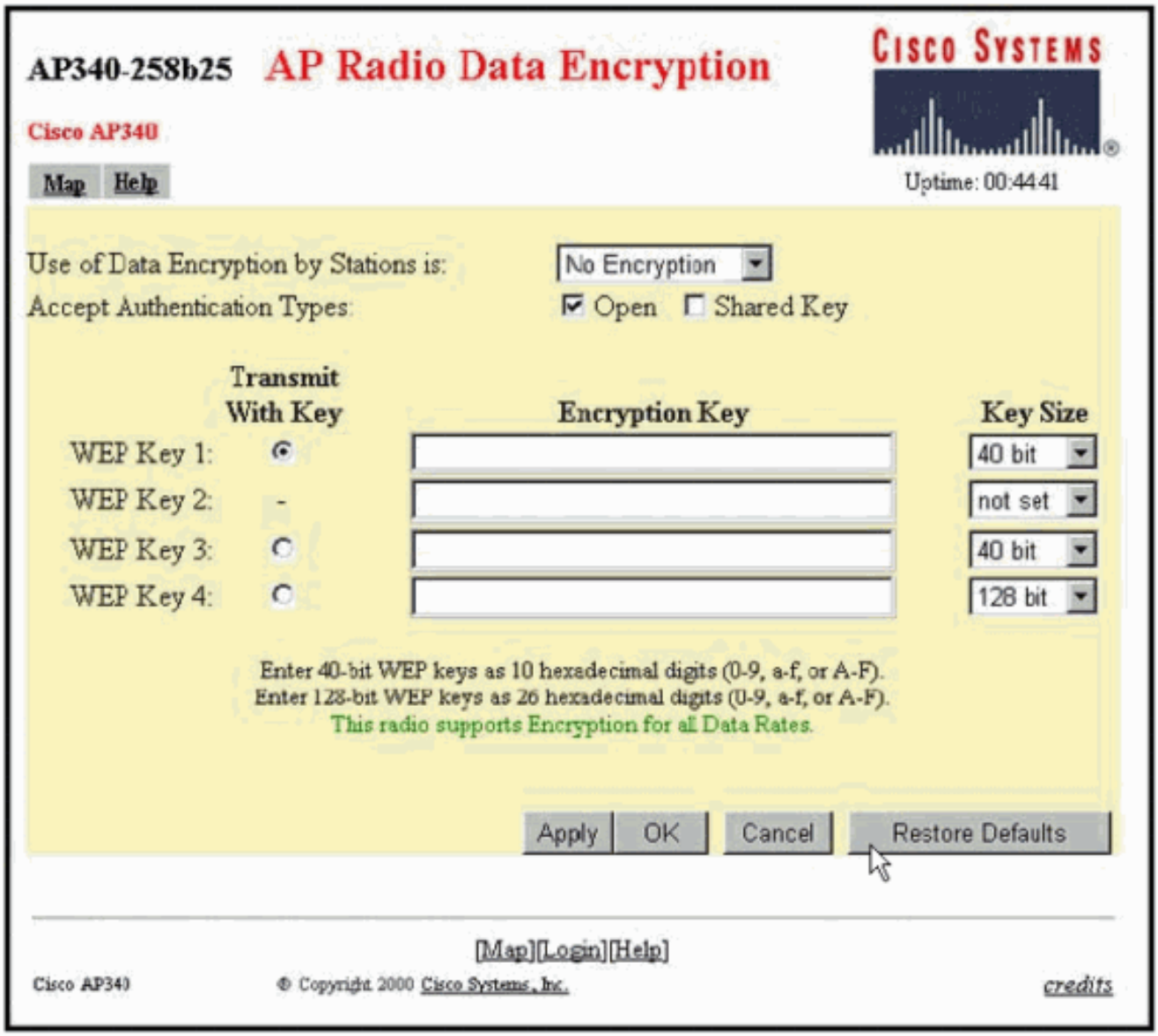
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez le WEP sur des points d'accès Aironet

Points d'accès Aironet qui exécutent le système d'exploitation de VxWorks

Procédez comme suit :

1. Établissez un rapport au Point d'accès (AP).
2. Naviguez vers le menu de chiffrement de radio AP.Utilisation une de ces chemins :**L'état récapitulatif > a installé > radio AP/matériel > chiffrement de données de radio (WEP) > le chiffrement de données par radio APÉtat récapitulatif > installé > Sécurité > configuration de la sécurité : Chiffrement de données par radio (WEP) > chiffrement de données de radio APRemarque:** Afin d'apporter des modifications à cette page, vous devez être un administrateur avec l'identité et écrire des capacités.**Vue de navigateur Web du menu de chiffrement de données de radio AP**



Configurations de VxWorks

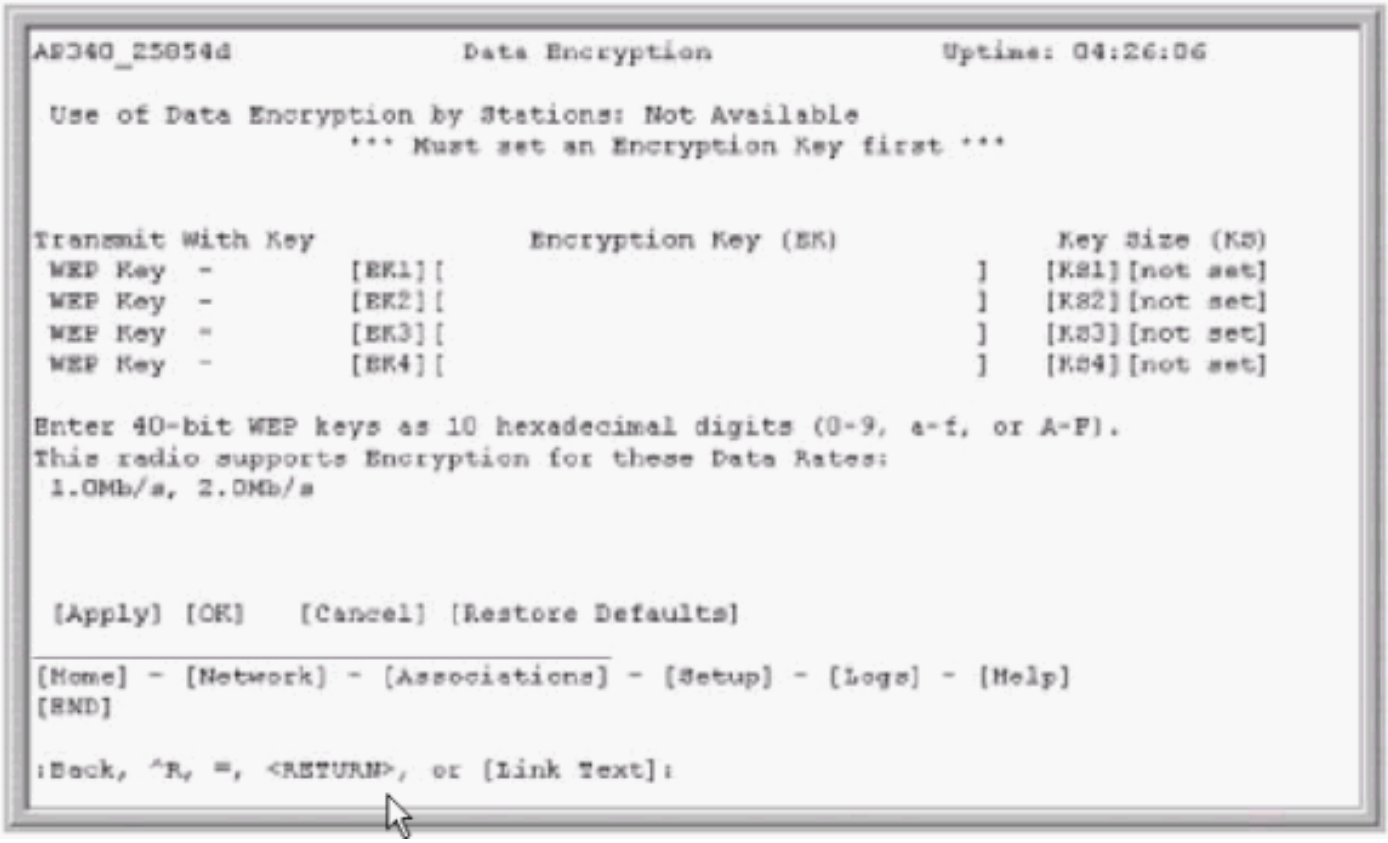
La page de chiffrement de données de radio AP présente un grand choix d'options de utiliser. Quelques options sont obligatoires pour le WEP. Cette section note ces options obligatoires. D'autres options ne sont pas nécessaires pour que le WEP fonctionne, mais elles sont recommandées.

- **L'utilisation du chiffrement de données par des stations est :**Utilisez ce établissement afin de choisir si les clients doivent utiliser le chiffrement de données quand ils communiquent avec AP. Le menu déroulant répertorie trois options :**Aucun cryptage (par défaut)** — 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.**(recommandé) de 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.**Remarque:** Vous devez placer une clé WEP avant que vous activiez l'utilisation de cryptage. Voyez la section **(OBLIGATOIRE) de clé de chiffrement de** cette liste.
- **Recevez les types d'authentification**Vous pouvez choisir la clé ouverte et partagée, ou chacun des deux options afin de placer les authentifications qu'AP identifiera.**Ouvrez le (recommandé)** — Cette valeur par défaut permet à n'importe quel périphérique, indépendamment de ses clés WEP, pour authentifier et tenter pour s'associer.**Clé partagée** — Cette configuration indique AP envoyer un texte brut, requête principale partagée à n'importe quel périphérique qui tente de s'associer avec AP.**Remarque:** Cette requête peut laisser AP ouvert d'attaque de texte connue des intrus. Par conséquent, cette configuration n'est pas aussi sécurisée que le paramètre Ouvert.
- **Transmettez par la clé**Ces boutons te permettent pour sélectionner la clé qu'AP utilise pendant la transmission de données. Vous pouvez sélectionner seulement une clé à la fois. Tout ou une partie des clés de positionnement peut être utilisé pour recevoir des données. Vous devez placer la clé avant que vous la spécifiiez comme touche de transmission.
- **Clé de chiffrement (OBLIGATOIRE)**Ces champs te permettent pour introduire les clés WEP. 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 FAfin de protéger la Sécurité de clé WEP, les clés WEP existantes n'apparaissent pas en texte brut dans les domaines d'entrée. Dans des versions récentes des aps, vous pouvez supprimer des clés existantes. Cependant, vous ne pouvez pas éditer les clés existantes.**Remarque:** Vous devez installer les clés WEP pour votre réseau, aps, et périphériques de client de la même manière. Par exemple, si vous placez la clé WEP 3 sur votre AP à 0987654321 et sélectionnez cette clé comme clé active, vous devez également placer la clé WEP 3 sur le périphérique de client à la même valeur.
- **Taille de clé (OBLIGATOIRE)**Cette configuration place les clés à 40-bit ou à 128-bit WEP. Si « non réglé » apparaît pour cette sélection, la clé n'est pas placée.**Remarque:** Vous ne pouvez pas supprimer une clé en sélectionnant « non réglé ».
- **Boutons d'action**Quatre configurations de contrôle de boutons d'action. Si le Javascript est activé sur votre navigateur Web, une fenêtre contextuelle de confirmation apparaît après que vous cliquiez sur n'importe quel bouton, excepté l'annulation.**Appliquez** — Ce bouton lance les nouvelles configurations de valeur. Le navigateur demeure à la page.**OK** — Ce bouton

applique les nouveaux paramètres et déplace le navigateur de nouveau à la page de configuration principale.**Annulation** — Ce bouton annule des modifications de configuration et renvoie les configurations aux valeurs précédemment enregistrées. Vous revenez alors à la page de configuration principale.**Par défaut de restauration** — Ce bouton change toutes les configurations à cette page de nouveau aux paramétrages d'usine.

Remarque: Dans des versions récentes de Cisco IOS® des aps, les boutons de commande seulement d'**application** et d'**annulation** sont disponibles pour cette page.

Vue de l'émulateur de terminal du menu de chiffrement de données



Vue de l'émulateur de terminal de l'ordre de configuration de clé WEP (logiciel de Cisco IOS®)

```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
  transmit-key  Set the key as transmit key
  <cr>

La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee transmit-key
La-ozone(config-if)#end
La-ozone#
*Mar 19 00:42:13.893: %SYS-5-CONFIG_I: Configured from console by console
La-ozone#
La-ozone#
```

Aironet aps qui exécutent le logiciel de Cisco IOS

Procédez comme suit :

1. Établissez un rapport à AP.

2. De l'option de 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.**Vue de navigateur Web du menu de gestionnaire de cryptage de Sécurité AP**

Configurez les ponts Aironet

Si vous utilisez VxWorks, terminez-vous ces étapes :

1. Établissez un rapport à la passerelle.
2. Naviguez vers le menu Confidentialité.Choisissez le **menu principal > la configuration > la radio > l'I80211 > l'intimité**.Les contrôles de menu Confidentialité l'utilisation du cryptage sur le paquet de données qui est transmis au-dessus de l'air par les radios. L'algorithme RSA RC4 et celui de jusqu'à quatre clés connues sont utilisés pour chiffrer les paquets. Chaque noeud dans la cellule radio doit connaître toutes les clés en service, mais des clés l'unes des peuvent être sélectionnées pour transmettre les données.**Vue de l'émulateur de terminal du menu Confidentialité**

```
        Configuration Radio I80211 Privacy Menu
      Option          Value      Description
1 - Encryption    [ off  ]    - Encrypt radio packets
2 - Auth          [ open ]    - Authentication mode
3 - Client        [ open ]    - Client authentication modes allowed
4 - Key                       - Set the keys
5 - Transmit                  - Key number for transmit
 Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

Référez-vous aux suites de configuration de chiffrement et au WEP - passerelle de gamme 1300 et caractéristiques de configuration WEP et WEP - passerelle de gamme 1400 pour les informations sur la façon dont configurer WEP en 1300 et passerelles de gamme 1400 par le mode CLI.

Afin d'utiliser le GUI pour configurer des passerelles de gammes 1300 et 1400, remplissez la

même procédure expliquée dans l'Aironet aps que section de logiciel de Cisco IOS de passage de ce document.

Configurations de VxWorks

Le menu Confidentialité présente un ensemble d'options que vous devez configurer. Quelques options sont obligatoires pour le WEP. Cette section note ces options obligatoires. D'autres options ne sont pas nécessaires pour que le WEP fonctionne, mais elles sont recommandées.

Cette section présente les options du menu dans la commande qu'elles apparaissent dans la vue de l'émulateur de terminal du menu Confidentialité. Cependant, configurez les options dans cette commande :

1. Clé
2. Transmettez
3. Authentique
4. Client
5. Cryptage

La configuration dans cette commande s'assure que des conditions préalables nécessaires sont installées pendant que vous configurez chaque configuration.

Ce sont les options :

- **Clé (OBLIGATOIRE)**L'option de clé programme les clés de chiffrement dans la passerelle. Vous êtes incité à placer une des quatre clés. Vous êtes incité deux fois à introduire la clé. Afin de définir la clé, vous devez écrire 10 ou 26 chiffres hexadécimaux, qui dépend de si la configuration de pont est pour les clés 40-bit ou 128-bit. Utilisez n'importe quelle combinaison de ces chiffres :0 à 9a à fA à FLes clés doivent s'assortir dans ***tous les*** Noeuds dans la cellule radio, et vous devez introduire les clés dans la même commande. Vous n'avez pas besoin de définir chacune des quatre clés, tant que le nombre de clés s'assortissent dans chaque périphérique dans le WLAN.
- **Transmettez**L'option de transmission indique à la radio quelles clés aux utiliser afin de transmettre des paquets. Chaque radio peut déchiffrer les paquets reçus qui sont envoyés avec des quatre clés l'unes des.
- **Authentique**Vous employez l'option authentique sur des ponts-répéteur afin de déterminer quelle authentication mode l'unité l'utilise pour connecter à son parent. Les valeurs permises sont clé ouverte ou partagée. Le protocole de 802.11 spécifie une procédure dans laquelle un client doit authentifier avec un parent avant que le client puisse s'associer.**Ouvrez le (recommandé)** — Ce mode de l'authentification est essentiellement une exécution nulle. On permet à tous les clients pour authentifier.**Clé partagée** — Ce mode permet au parent pour envoyer au client un texte de défi, que le client chiffre et renvoie au parent. Si le parent déchiffre avec succès le texte de défi, le client est authentifié.**Attention** : N'utilisez pas le mode principal partagé. Quand vous l'utilisez, un texte brut et une version chiffrée des mêmes données transmet sur l'air. Ceci ne gagne rien. Si la clé d'utilisateur est erronée, l'unité ne déchiffre pas les paquets, et les paquets ne peuvent pas accéder au réseau.
- **Client**L'option Client détermine l'authentication mode que les noeuds client les utilisent pour associer à l'unité. Ce sont les valeurs qui sont permises :**Ouvrez le (recommandé)** — Ce mode de l'authentification est essentiellement une exécution nulle. On permet à tous les clients pour authentifier.**Clé partagée** — Ce mode permet au parent pour envoyer au client un

texte de défi, que le client chiffre et renvoie au parent. Si le parent déchiffre avec succès le texte de défi, le client est authentifié.**Chacun des deux** — Ce mode permet au client pour utiliser l'un ou l'autre de mode.

- **CryptageOutre de** — Si vous placez l'option de chiffrement à hors fonction, aucun cryptage n'est fait. Les données transmettent en clair.**Sur (OBLIGATOIRE)** — Si vous placez l'option de chiffrement à en fonction, tous les paquets de données transmises sont chiffrés et tous les paquets reçus décryptés sont jetés.**Mélangé** — Dans le mode mixte, une racine ou un pont-répéteur reçoit l'association des clients qui ont le cryptage tourné l'un ou l'autre "Marche/Arrêt". Dans ce cas, seulement des paquets de données entre les Noeuds que chacun des deux les prennent en charge sont chiffrés. Des paquets de multidiffusion sont envoyés en clair. Tous les Noeuds peuvent voir les paquets.**Attention** : N'utilisez pas le mode mixte. Si un client qui fait activer le cryptage envoie un paquet de multidiffusion à son parent, le paquet est chiffré. Le parent déchiffre le paquet et retransmet le paquet en clair à la cellule, et d'autres Noeuds peuvent voir le paquet. La capacité de visualiser un paquet dans chiffré et forme non chiffrée peut contribuer à casser une clé. L'intégration du mode mixte est seulement pour la compatibilité avec d'autres constructeurs.

Configurez les adaptateurs de client

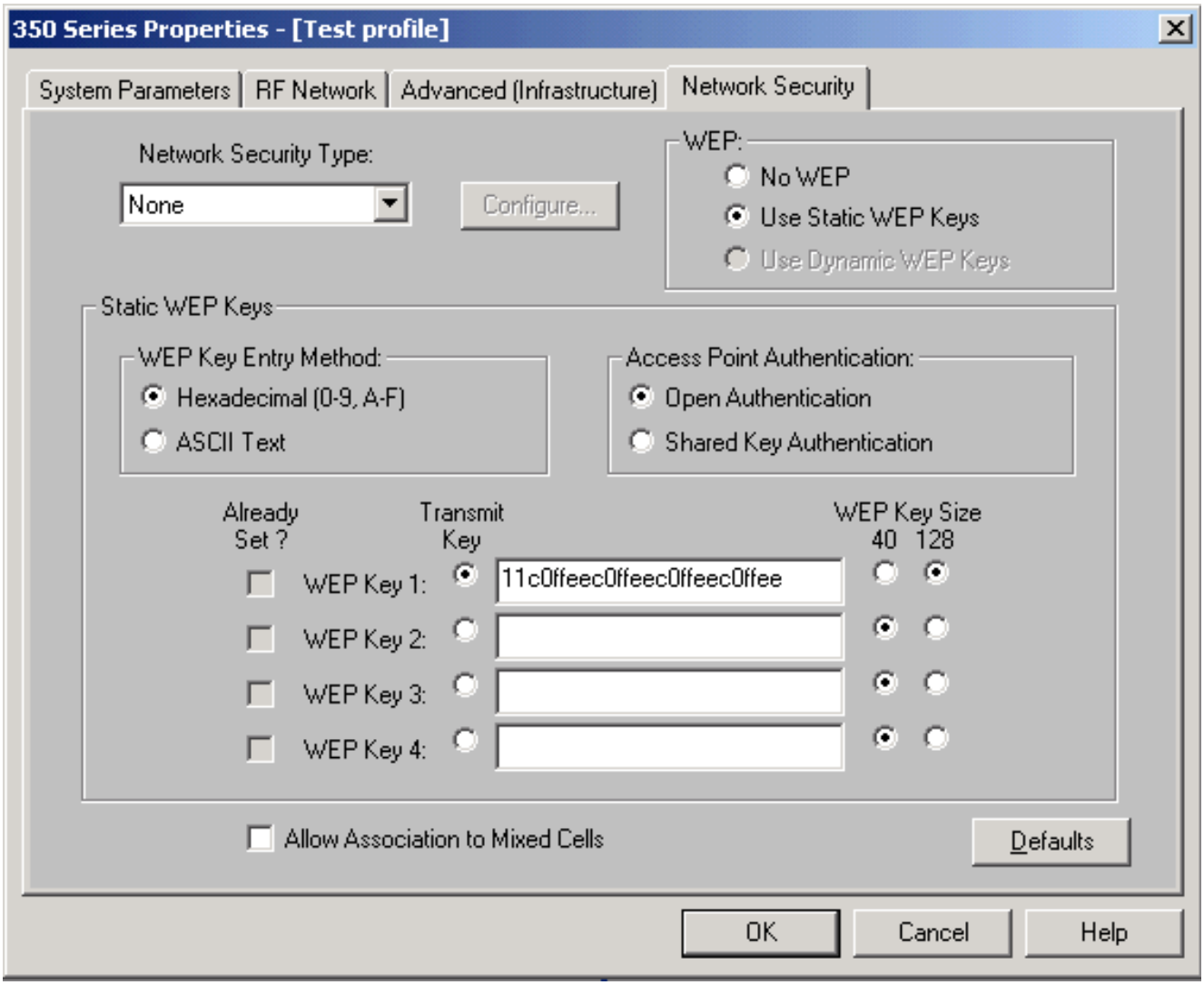
Vous devez se terminer deux étapes principales afin d'installer le WEP sur l'adaptateur client Aironet :

1. Configurez la clé WEP/clés dans le Client Encryption Manager.
2. Enable WEP dans l'Aironet Client Utility (ACU).

Placez les clés WEP

Terminez-vous ces étapes afin d'installer des clés WEP sur les adaptateurs de client :

1. Ouvrez l'ACU et choisissez le **gestionnaire de profil**.
2. Choisissez le profil où vous voulez activer le WEP et cliquer sur Edit.
3. Cliquez sur l'**onglet Sécurité réseau** afin de présenter les options de Sécurité, et cliquez sur les **clés WEP statiques d'utilisation**.Cette action lance les options de configuration WEP qui sont obscurcies quand aucun WEP n'est
sélectionné.



4. Pour la clé WEP que vous voulez créer, choisissez **40** bits ou **128** bits sous la taille de clé WEP du côté droit de la fenêtre.**Remarque:** les adaptateurs du client 128-bit peuvent utiliser les clés 40-bit ou 128-bit. Mais les adaptateurs 40-bit peuvent seulement utiliser les clés 40-bit.**Remarque:** Votre clé WEP d'adaptateur de client doit apparier la clé WEP qui les autres composants WLAN avec lesquels vous communiquez l'utilisation.Quand vous placez plus d'une clé WEP, vous devez assigner les clés WEP aux mêmes nombres de clé WEP pour tous les périphériques. Des clés WEP doivent être composées des caractères hexadécimaux et doivent contenir 10 caractères pour les clés WEP 40-bit ou 26 caractères pour les clés WEP 128-bit. Les caractères hexadécimaux peuvent être :0 à 9a à fA à F**Remarque:** des clés WEP d'ASCII-texte ne sont pas prises en charge sur l'Aironet aps. Par conséquent, vous devez choisir (0-9, A-F) l'option hexadécimale si vous prévoyez d'utiliser votre adaptateur de client avec ces aps.**Remarque:** Après que vous créiez la clé WEP, vous pouvez écrire au-dessus de elle. Mais vous ne pouvez pas l'éditer ou supprimer.**Remarque:** Si vous utilisez une version ultérieure d'Aironet Desktop Utility (ADU) au lieu de l'ACU comme utilitaire client, vous pouvez également supprimer la clé WEP créée et la remplacer par un neuf.
5. Cliquez sur le bouton de **touche de transmission** qui est près d'une des clés que vous avez créées.Avec cette action, vous indiquez que cette clé est la clé que vous voulez employer pour transmettre des paquets.
6. Type de dessous **persistant de** clé WEP de clic.Cette action permet à votre adaptateur de client pour retenir cette clé WEP, même lorsque l'alimentation à l'adaptateur est coupée ou à la réinitialisation de l'ordinateur en lequel la clé est installée. Si vous choisissez provisoire pour cette option, la clé WEP est perdue quand l'alimentation est coupée de votre adaptateur

de client.
7. Cliquez sur **OK**.

Enable WEP

Procédez comme suit :

1. Ouvrez l'ACU et choisissez **éditent Properties de la** barre de menus.
2. Cliquez sur l'**onglet Sécurité réseau** afin de présenter les options de Sécurité.
3. Cochez la case de l'**enable WEP** afin de lancer le WEP.

Référez-vous à configurer le WEP dans l'ADU pour que les étapes configurent le WEP utilisant l'ADU comme utilitaire client.

Configurez les ponts de groupe de travail

Il y a des différences entre le pont de groupe de travail de gamme 340 d'Aironet et la passerelle de gamme 340 d'Aironet. Cependant, la configuration du pont de groupe de travail pour utiliser le WEP est presque identique à la configuration de la passerelle. Voyez la section de ponts Aironet de configurer pour la configuration de la passerelle.

1. Connectez au pont de groupe de travail.
2. Naviguez vers le menu Confidentialité.Choisissez la **canalisation > la configuration > la radio > l'I80211 > l'intimité** afin d'accéder au menu de VxWorks d'intimité.

Configurations

Le menu Confidentialité présente les configurations que cette section répertorie. Configurez les options sur le pont de groupe de travail dans cette commande :

1. Clé
2. Transmettez
3. Authentique
4. Cryptage

Ce sont les options :

- **Clé**L'option principale établit la clé WEP qui les utilisations de passerelle afin de recevoir des paquets. La valeur doit apparier la clé qui AP ou tout autre périphérique avec lesquels le pont de groupe de travail communique des utilisations. La clé se compose de jusqu'à 10 caractères hexadécimaux pour le cryptage 40-bit ou de 26 caractères hexadécimaux pour le cryptage 128-bit. Les caractères hexadécimaux peuvent être n'importe quelle combinaison de ces chiffres :0 à 9a à fA à F
- **Transmettez**L'option de transmission établit la clé WEP qui les utilisations de passerelle afin de transmettre des paquets. Vous pouvez choisir d'utiliser la même clé que vous avez utilisée pour l'option principale. Si vous choisissez une clé différente, vous devez établir une clé assortie sur AP.Seulement une clé WEP peut être utilisée en même temps pour des transmissions. La clé WEP que vous utilisez pour transmettre des données doit être placée à la même valeur sur votre pont de groupe de travail et d'autres périphériques avec lesquels elle communique.

- **Authentification (authentique)**Le paramètre authentique détermine quelle méthode d'authentification le système utilise. Les options sont :**Ouvrez le (recommandé)** — Le paramètre Ouvert par défaut permet à n'importe quel AP, indépendamment de ses configurations WEP, pour authentifier et puis tenter pour communiquer avec la passerelle.**Clé partagée** — Cette configuration demande à la passerelle pour envoyer un texte brut, requête principale partagée aux aps afin d'essayer de communiquer avec la passerelle. Le paramétrage de clé partagée peut laisser la passerelle ouverte d'attaque de texte connue des intrus. Par conséquent, cette configuration n'est pas aussi sécurisée que le paramètre Ouvert.
- **Cryptage**L'option de chiffrement place des paramètres de chiffrement sur tous les paquets de données, excepté des paquets d'association et quelques paquets de contrôle. Il y a quatre options :**Remarque:** AP doit avoir le cryptage actif et une clé réglée correctement.**Outre de** — C'est la valeur par défaut. Tout le cryptage est arrêté. Le pont de groupe de travail ne communique pas avec AP avec l'utilisation du WEP.**Sur le (recommandé)** — Cette configuration exige le cryptage de tous les transferts des données. Le pont de groupe de travail communique seulement avec les aps qui utilisent le WEP.**Mélangé en fonction** — Cette configuration signifie que la passerelle emploie toujours le WEP afin de communiquer avec AP. Cependant, AP communique avec tous les périphériques, s'ils utilisent le WEP ou n'utilisent pas le WEP.**Mélangé hors fonction** — Cette configuration signifie que la passerelle n'emploie pas le WEP afin de communiquer avec AP. Cependant, AP communique avec tous les périphériques, s'ils utilisent le WEP ou n'utilisent pas le WEP.**Attention** : Si vous sélectionnez en fonction ou mélangé en fonction pendant que la catégorie et vous WEP configurent la passerelle par sa liaison radio, la Connectivité à la passerelle est perdue si vous placez la clé WEP inexactement. Assurez-vous que vous utilisez exactement les mêmes configurations quand vous placez la clé WEP sur le pont de groupe de travail et la clé WEP sur d'autres périphériques sur votre WLAN.

Informations connexes

- Association de normes ieees
- Produits LAN sans fil de gamme 340 d'Aironet
- Ressources de prise en charge sans fil
- Page de support technique sur LAN sans fil
- Guide de configuration du logiciel de Cisco IOS pour des Points d'accès de Cisco Aironet
- Guide de configuration du logiciel de Cisco IOS pour le Point d'accès extérieur de Gamme Cisco Aironet 1300/passerelle
- Guide de configuration logicielle de points d'accès Cisco Aironet pour VxWorks
- Guide de configuration du logiciel de passerelle de Gamme Cisco Aironet 1400
- Guides de configuration d'Adaptateurs client LAN sans fil Cisco Aironet
- Aperçu Sans fil de Sécurité LAN de Cisco
- Radio (mobilité) sécurisant des réseaux sans fil
- Exemple de configuration d'un point d'accès en tant que pont de groupe de travail
- Ponts de groupe de travail Cisco Aironet - FAQ
- Procédure de récupération de mot de passe pour l'équipement Cisco Aironet
- Points d'accès Cisco Aironet - FAQ
- Support et documentation techniques - Cisco Systems