Configurer le protocole WEP 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 : Reportez-vous à la section Clés Web statiques du Chapitre 6 - Configuration des WLAN pour plus d'informations sur la configuration WEP sur les contrôleurs LAN sans fil (WLC).

WEP est l'algorithme de chiffrement intégré à la norme 802.11 (Wi-Fi). Le chiffrement WEP utilise le chiffrement de flux Ron Code 4 (RC4) avec des clés 40 ou 104 bits et un vecteur d'initialisation 24 bits (IV).

Comme le spécifie la norme, WEP utilise l'algorithme RC4 avec une clé 40 bits ou 104 bits et une clé IV 24 bits. RC4 est un algorithme symétrique car il utilise la même clé pour le chiffrement et le déchiffrement des données. Lorsque WEP est activé, chaque station radio possède 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 rejeté et n'est jamais remis à l'hôte.

WEP peut être utilisé principalement pour un bureau à domicile ou un petit bureau qui ne

nécessite pas une sécurité très élevée.

L'implémentation WEP d'Aironet se trouve dans le matériel. Par conséquent, un impact minimal sur les performances est obtenu lorsque vous utilisez WEP.

Remarque : Il existe des problèmes connus avec le protocole WEP, ce qui en fait une méthode de cryptage peu fiable. Les problèmes sont les suivants :

- La gestion d'une clé WEP partagée implique de nombreuses tâches administratives.
- WEP présente le même problème que tous les systèmes basés sur des clés partagées. Tout secret donné à une personne devient public après un certain temps.
- L'IV qui initie l'algorithme WEP est envoyé en texte clair.
- La somme de contrôle WEP est linéaire et prévisible.

Le protocole TKIP (Temporal Key Integrity Protocol) a été créé pour traiter ces problèmes WEP. Tout comme WEP, TKIP utilise le chiffrement RC4. Cependant, TKIP améliore le WEP en ajoutant des mesures telles que le hachage de clé par paquet, le contrôle d'intégrité des messages (MIC) et la rotation des clés de diffusion pour répondre aux vulnérabilités connues du WEP. TKIP utilise le chiffrement de flux RC4 avec des clés de 128 bits pour le chiffrement et des clés de 64 bits pour l'authentification.

Conditions préalables

Conditions requises

Ce document suppose que vous pouvez établir une connexion administrative aux périphériques WLAN et que ces périphériques fonctionnent normalement dans un environnement non chiffré.

Pour configurer le WEP 40 bits standard, vous devez disposer de deux unités radio ou plus qui communiquent entre elles.

Remarque : les produits Aironet peuvent établir des connexions WEP 40 bits avec des produits non Cisco conformes à la norme IEEE 802.11b. Ce document ne traite pas de la configuration des autres périphériques.

Pour la création d'une liaison WEP 128 bits, les produits Cisco interagissent uniquement avec d'autres produits Cisco.

Components Used

Utilisez ces composants avec ce document :

- Deux unités radio ou plus communiquant entre elles
- Une connexion administrative au périphérique WLAN

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.

Conventions

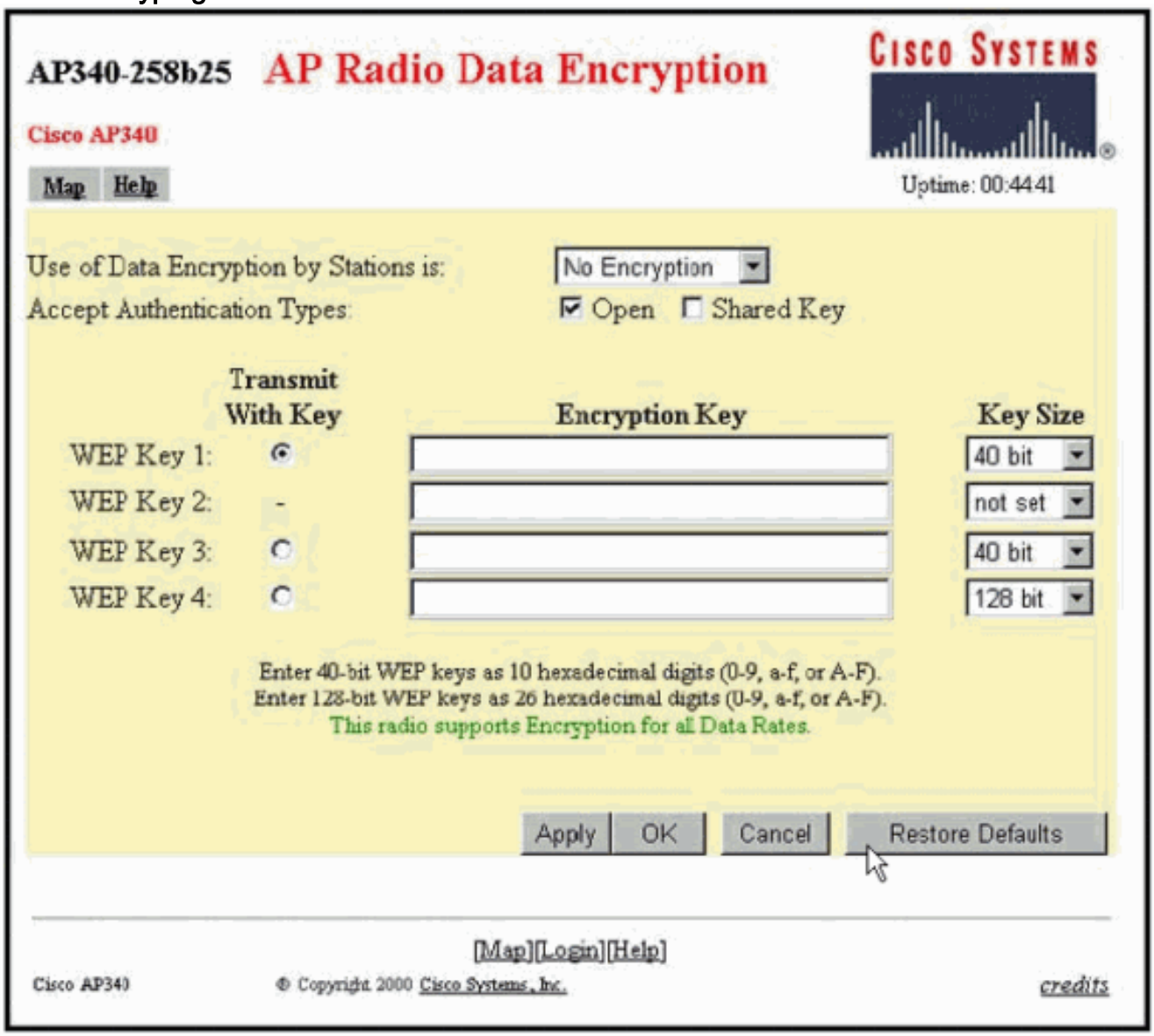
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration du protocole WEP sur les points d'accès Aironet

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

Procédez comme suit :

1. Établir une connexion au point d'accès (AP).
2. Naviguez jusqu'au menu de cryptage radio AP.Utilisez l'un des chemins suivants :**État résumé > Configuration > Radio/Matériel AP > Cryptage des données radio (WEP) > Chiffrement des données radio APÉtat récapitulatif > Configuration > Sécurité > Configuration de la sécurité : Cryptage des données radio (WEP) > Cryptage des données radio APRemarque :** Pour apporter des modifications à cette page, vous devez être un administrateur doté de fonctionnalités d'identification et d'écriture.**Vue du navigateur Web du menu de cryptage des données radio AP**



Paramètres VxWorks

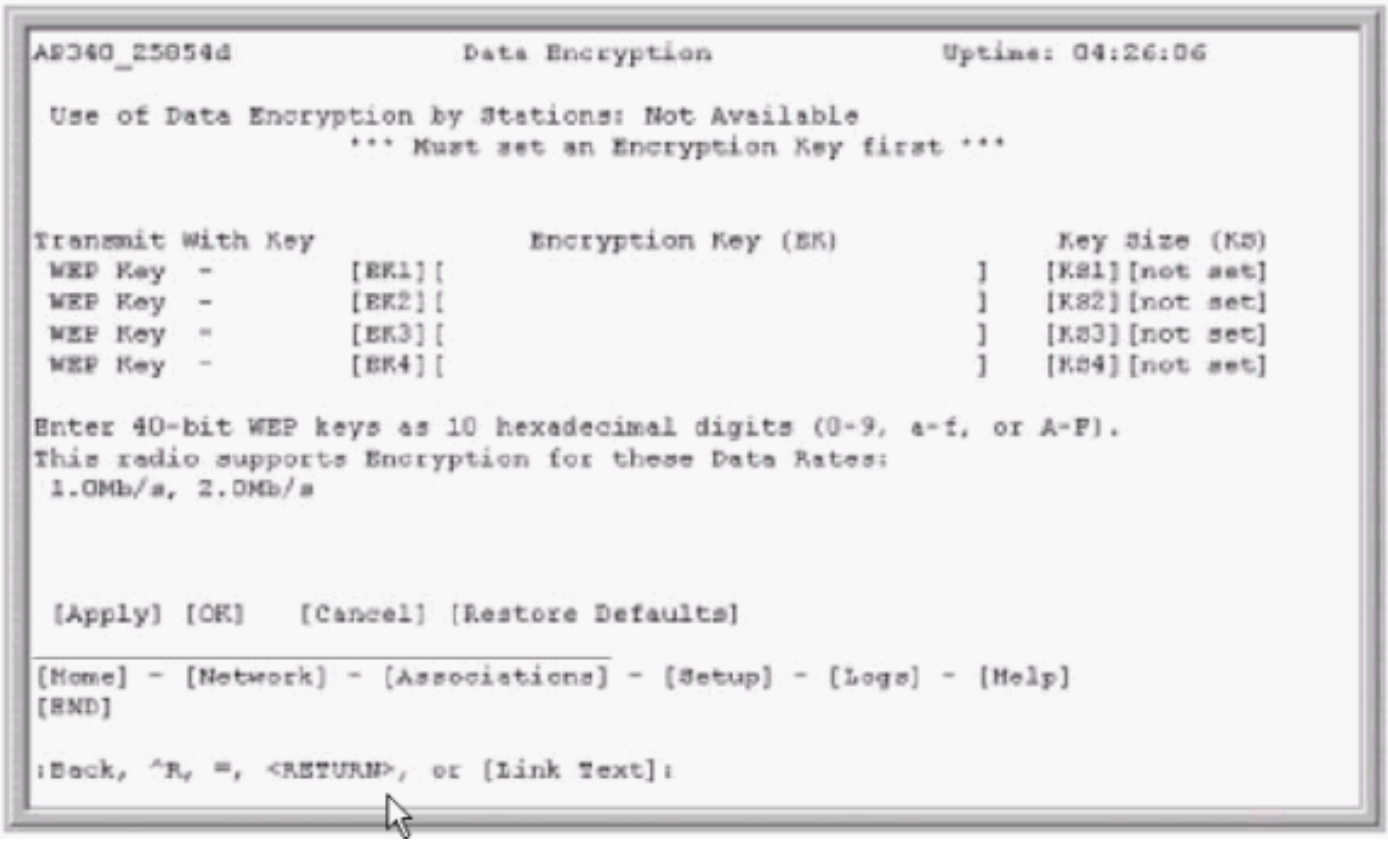
La page AP Radio Data Encryption présente une variété d'options à utiliser. Certaines options sont obligatoires pour WEP. Cette section indique ces options obligatoires. D'autres options ne sont pas nécessaires pour que WEP fonctionne, mais elles sont recommandées.

- **L'utilisation du chiffrement des données par stations est la suivante :**Utilisez ce paramètre afin de choisir si les clients doivent utiliser le chiffrement des données lorsqu'ils communiquent avec le point d'accès. Le menu déroulant répertorie trois options :**No Encryption (No Encryption) (No Encryption (par défaut)** : nécessite que les clients communiquent avec le point d'accès sans aucun chiffrement des données. Ce paramètre n'est pas recommandé.**Facultatif** : permet aux clients de communiquer avec le point d'accès avec ou sans chiffrement de données. Généralement, 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.**Cryptage complet (RECOMMANDÉ)** : exige que les clients utilisent le chiffrement 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.**Remarque :** Vous devez définir une clé WEP avant d'activer l'utilisation du chiffrement. Reportez-vous à la section **Clé de chiffrement (OBLIGATOIRE)** de cette liste.
- **Accepter les types d'authentification**Vous pouvez choisir Open, Shared Key, ou les deux options afin de définir les authentifications que le point d'accès reconnaîtra.**Open (RECOMMANDÉ)** : ce paramètre par défaut permet à tout périphérique, quelles que soient ses clés WEP, de s'authentifier et de tenter de s'associer.**Shared Key** : ce paramètre indique au point d'accès d'envoyer une requête de clé partagée en texte clair à tout périphérique qui tente de s'associer au point d'accès.**Remarque :** Cette requête peut laisser le point d'accès ouvert à une attaque en texte connu par des intrus. Par conséquent, ce paramètre n'est pas aussi sécurisé que le paramètre Open.
- **Transmettre avec clé**Ces boutons vous permettent de sélectionner la clé que le point d'accès utilise lors de la transmission des données. Vous ne pouvez sélectionner qu'une seule clé à la fois. Toutes les clés définies peuvent être utilisées pour recevoir des données. Vous devez définir la clé avant de la spécifier en tant que clé de transmission.
- **Clé de chiffrement (OBLIGATOIRE)**Ces champs vous permettent d'entrer les clés WEP. Saisissez 10 chiffres hexadécimaux pour les clés WEP 40 bits ou 26 chiffres hexadécimaux pour les clés WEP 128 bits. Les touches peuvent être n'importe quelle combinaison de ces chiffres :0 à 9a à fA à FAfin de protéger la sécurité des clés WEP, les clés WEP existantes n'apparaissent pas en texte brut dans les champs d'entrée. Dans les versions récentes des points d'accès, vous pouvez supprimer des clés existantes. Cependant, vous ne pouvez pas modifier les clés existantes.**Remarque :** Vous devez configurer les clés WEP pour votre réseau, vos points d'accès et vos périphériques clients de la même manière. Par exemple, si vous définissez la clé WEP Key 3 sur votre AP sur 0987654321 et sélectionnez cette clé comme clé active, vous devez également définir la clé WEP Key 3 sur le périphérique client sur la même valeur.
- **Taille de clé (OBLIGATOIRE)**Ce paramètre définit les clés sur WEP 40 bits ou 128 bits. Si « not set » apparaît pour cette sélection, la clé n'est pas définie.**Remarque :** Vous ne pouvez pas supprimer une clé en sélectionnant « non défini ».
- **Boutons d'action**Quatre boutons d'action contrôlent les paramètres. Si JavaScript est activé sur votre navigateur Web, une fenêtre contextuelle de confirmation apparaît après avoir cliqué sur un bouton, sauf Annuler.**Apply** : ce bouton active les nouveaux paramètres de valeur. Le navigateur reste sur la page.**OK** : ce bouton applique les nouveaux paramètres et redirige le

navigateur vers la page principale de configuration.**Annuler** : ce bouton annule les modifications de paramètre et retourne les paramètres aux valeurs précédemment stockées. Vous revenez ensuite à la page principale de configuration.**Restore Defaults** : ce bouton rétablit les paramètres d'usine par défaut de tous les paramètres de cette page.

Remarque : Dans les versions récentes de Cisco IOS® des points d'accès, seuls les boutons de contrôle **Appliquer** et **Annuler** sont disponibles pour cette page.

Vue Émulateur de terminal du menu Chiffrement de données



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

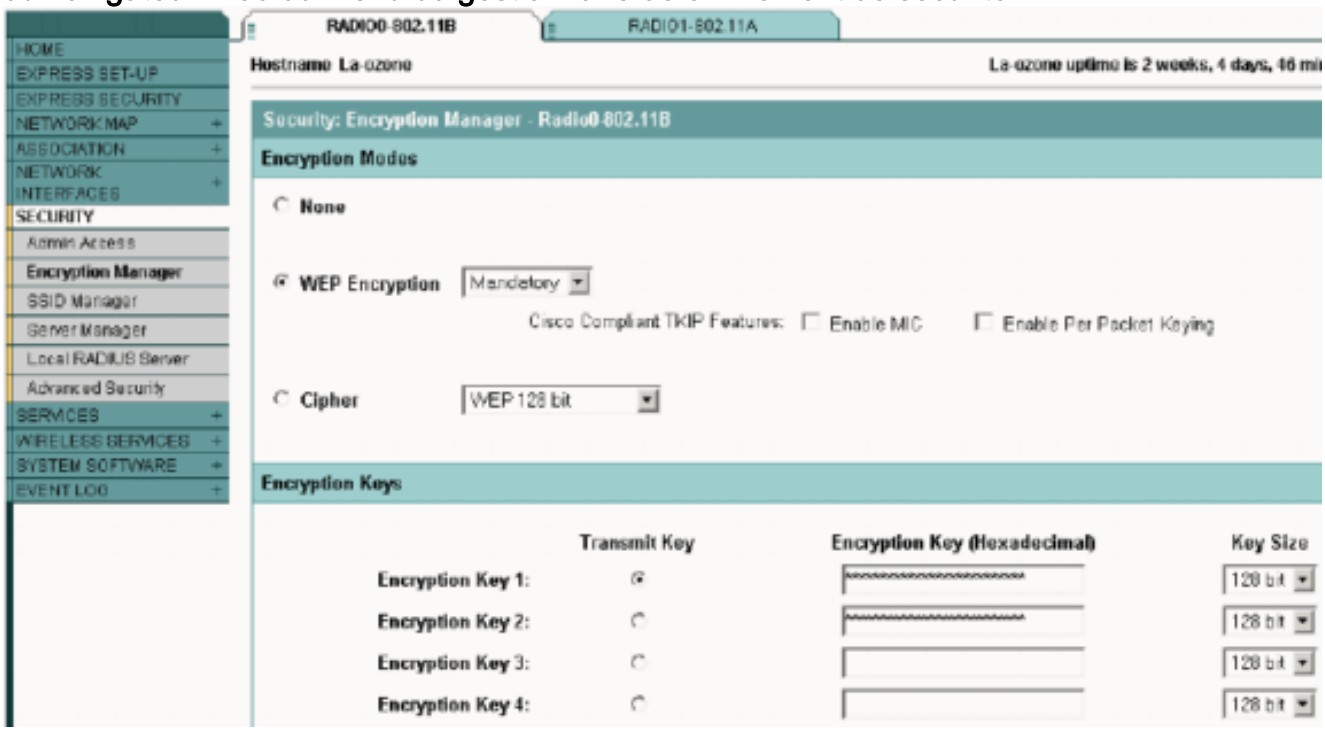
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

Points d'accès Aironet qui exécutent le logiciel Cisco IOS

Procédez comme suit :

1. Établir une connexion au point d'accès.
2. Dans l'option de menu SÉCURITÉ située à gauche de la fenêtre, sélectionnez **Encryption**

Manager pour l'interface radio à laquelle vous voulez configurer vos clés WEP statiques.**Vue du navigateur Web du menu du gestionnaire de chiffrement de sécurité AP**



Configurer les ponts Aironet

Si vous utilisez VxWorks, procédez comme suit :

1. Connectez-vous au pont.
2. Accédez au menu Confidentialité.Choisissez **Main Menu > Configuration > Radio > I80211 > Privacy**.Le menu Confidentialité contrôle l'utilisation du chiffrement sur le paquet de données transmis par les radios. L'algorithme RSA RC4 et l'une des quatre clés connues au maximum sont utilisés pour chiffrer les paquets. Chaque noeud de la cellule radio doit connaître toutes les clés utilisées, mais toutes les clés peuvent être sélectionnées pour transmettre les données.**Vue 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 à Configuration des suites de chiffrement et WEP - Pont de la gamme 1300 et Configuration des fonctionnalités WEP et WEP - Pont de la gamme 1400 pour plus d'informations sur la configuration de WEP dans les ponts de la gamme 1300 et 1400 via le mode CLI.

Afin d'utiliser l'interface utilisateur graphique pour configurer les ponts des gammes 1300 et 1400, suivez la même procédure expliquée dans la section AP Aironet qui exécutent le logiciel Cisco IOS de ce document.

Paramètres VxWorks

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

Cette section présente les options de menu dans l'ordre dans lequel elles apparaissent dans la vue émulateur de terminal du menu Confidentialité. Cependant, configurez les options dans cet ordre :

1. Key (Clé)
2. Transmission
3. authentification
4. Client
5. Chiffrement

La configuration dans cet ordre garantit que les conditions préalables nécessaires sont configurées lors de la configuration de chaque paramètre.

Voici les options :

- **Clé (OBLIGATOIRE)**L'option Key (Clé) programme les clés de chiffrement dans le pont. Vous êtes invité à définir l'une des quatre clés. Vous êtes invité à entrer la clé deux fois. Pour définir la clé, vous devez saisir 10 ou 26 chiffres hexadécimaux, selon que la configuration Bridge est pour les clés 40 bits ou 128 bits. Utilisez n'importe quelle combinaison de ces chiffres :0 à 9a à fA à FLes clés doivent correspondre dans ***tous les*** noeuds de la cellule radio et vous devez entrer les clés dans le même ordre. Vous n'avez pas besoin de définir les quatre clés, à condition que le nombre de clés corresponde dans chaque périphérique du WLAN.
- **Transmission**L'option Transmit indique à la radio quelles clés utiliser pour transmettre des paquets. Chaque radio peut décrypter les paquets reçus qui sont envoyés avec l'une des quatre clés.
- **authentification**Vous utilisez l'option Auth sur les ponts de répéteur afin de déterminer le mode d'authentification que l'unité utilise pour se connecter à son parent. Les valeurs autorisées sont Open ou Shared Key. Le protocole 802.11 spécifie une procédure dans laquelle un client doit s'authentifier auprès d'un parent avant que le client puisse s'associer.**Open (RECOMMANDÉ)** : ce mode d'authentification est essentiellement une opération nulle. Tous les clients sont autorisés à s'authentifier.**Shared Key** : ce mode permet au parent d'envoyer au client un texte de demande de confirmation, que le client chiffre et retourne au parent. Si le parent décrypte correctement le texte de la demande de confirmation, le client est authentifié.**Attention :** N'utilisez pas le mode Clé partagée. Lorsque vous l'utilisez, une version en texte brut et chiffrée des mêmes données est transmise en direct. Cela ne rapporte rien. Si la clé utilisateur est incorrecte, l'unité ne déchiffre pas les paquets et les paquets ne peuvent pas accéder au réseau.
- **Client**L'option Client détermine le mode d'authentification que les noeuds clients utilisent pour s'associer à l'unité. Voici les valeurs autorisées :**Open (RECOMMANDÉ)** : ce mode d'authentification est essentiellement une opération nulle. Tous les clients sont autorisés à s'authentifier.**Shared Key** : ce mode permet au parent d'envoyer au client un texte de demande de confirmation, que le client chiffre et retourne au parent. Si le parent décrypte correctement le texte de la demande de confirmation, le client est authentifié.**Two** : ce mode permet au client d'utiliser l'un ou l'autre des modes.

- **ChiffrementDésactivé** - Si vous définissez l'option de chiffrement sur Désactivé, aucun chiffrement n'est effectué. Les données sont transmises en clair.**On (OBLIGATOIRE)** : si vous définissez l'option Encryption sur On, tous les paquets de données transmis sont chiffrés et tous les paquets reçus non chiffrés sont ignorés.**Mixed** : en mode Mixed, un pont racine ou un pont répéteur accepte l'association des clients dont le chiffrement est activé ou désactivé. Dans ce cas, seuls les paquets de données entre les noeuds pris en charge sont chiffrés. Les paquets de multidiffusion sont envoyés en clair. Tous les noeuds peuvent voir les paquets.**Attention :** N'utilisez pas le mode Mixed. Si un client dont le chiffrement est activé envoie un paquet de multidiffusion à son parent, le paquet est chiffré. Le parent déchiffre le paquet et le retransmet en clair à la cellule, et d'autres noeuds peuvent voir le paquet. La possibilité de voir un paquet sous forme chiffrée ou non peut contribuer à casser une clé. L'inclusion du mode Mixed est uniquement compatible avec d'autres fournisseurs.

Configurer les adaptateurs client

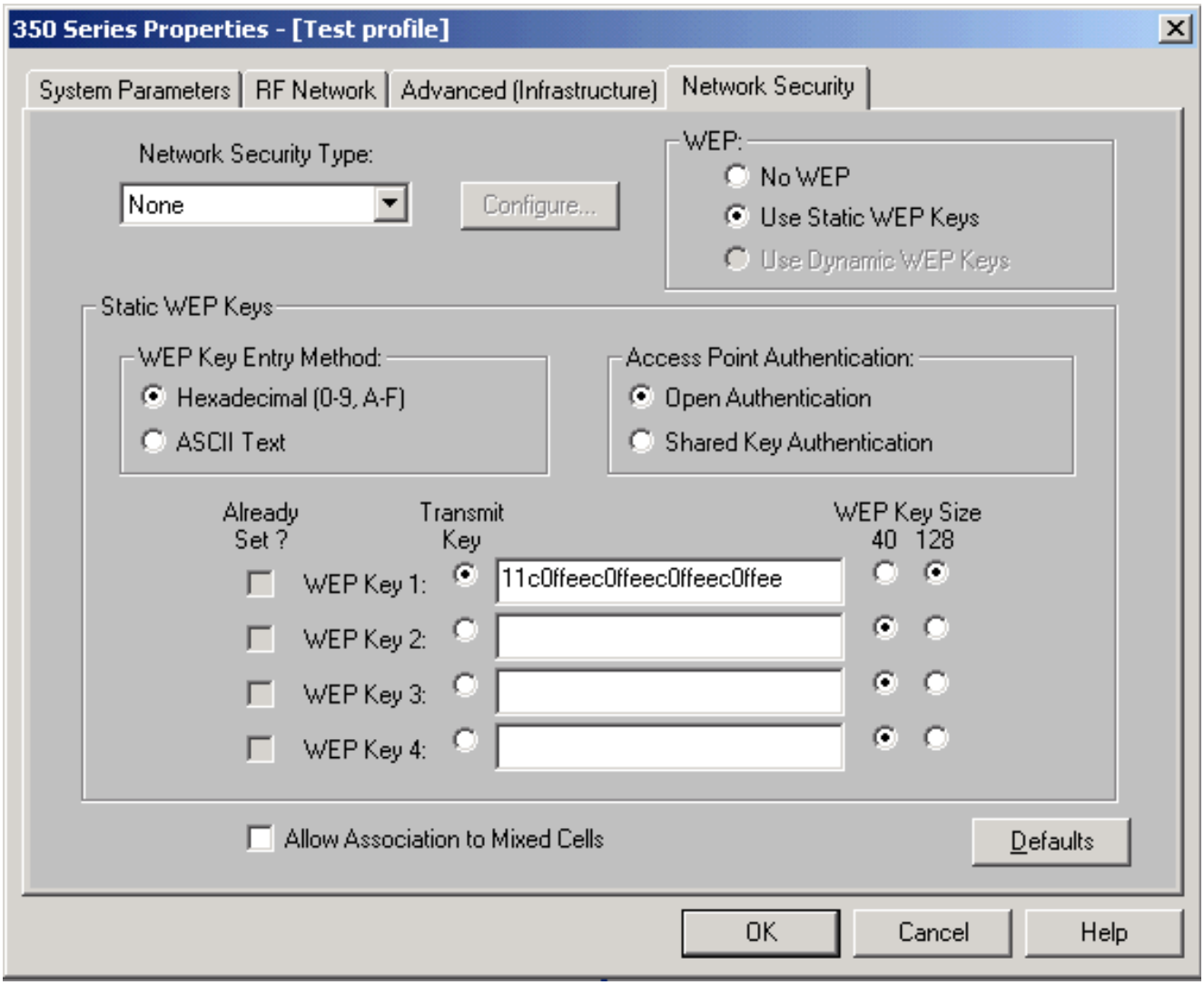
Vous devez effectuer deux étapes principales afin de configurer WEP sur l'adaptateur client Aironet :

1. Configurez la/les clé(s) WEP dans Client Encryption Manager.
2. Activez WEP dans l'utilitaire client Aironet (ACU).

Définir les clés WEP

Complétez ces étapes afin de configurer les clés WEP sur les adaptateurs client :

1. Ouvrez ACU et sélectionnez **Profile Manager**.
2. Choisissez le profil dans lequel vous voulez activer WEP et cliquez sur **Modifier**.
3. Cliquez sur l'onglet **Sécurité réseau** afin d'afficher les options de sécurité, puis cliquez sur **Utiliser les clés WEP statiques**.Cette action active les options de configuration WEP qui sont estompées lorsque Aucun WEP n'est
sélectionné.



4. Pour la clé WEP à créer, choisissez **40** bits ou **128** bits sous Taille de clé WEP sur le côté droit de la fenêtre.**Remarque :** les adaptateurs client 128 bits peuvent utiliser des clés 40 bits ou 128 bits. Mais les adaptateurs 40 bits ne peuvent utiliser que des clés 40 bits.**Remarque :** La clé WEP de votre adaptateur client doit correspondre à la clé WEP utilisée par les autres composants WLAN avec lesquels vous communiquez.Lorsque vous définissez plusieurs clés WEP, vous devez affecter les clés WEP aux mêmes numéros de clé WEP pour tous les périphériques. Les clés WEP doivent être composées de caractères hexadécimaux et doivent contenir 10 caractères pour les clés WEP 40 bits ou 26 caractères pour les clés WEP 128 bits. Les caractères hexadécimaux peuvent être :0 à 9a à fA à F**Remarque :** les clés WEP en texte ASCII ne sont pas prises en charge sur les AP Aironet. Par conséquent, vous devez choisir l'option hexadécimale (0-9, A-F) si vous prévoyez d'utiliser votre adaptateur client avec ces points d'accès.**Remarque :** après avoir créé la clé WEP, vous pouvez l'écrire. Mais vous ne pouvez pas le modifier ou le supprimer.**Remarque :** Si vous utilisez une version ultérieure de l'utilitaire de bureau Aironet (ADU) au lieu d'ACU comme utilitaire client, vous pouvez également supprimer la clé WEP créée et la remplacer par une nouvelle clé.
5. Cliquez sur le bouton **Transmit Key** situé à côté de l'une des clés que vous avez créées.Avec cette action, vous indiquez que cette clé est la clé que vous voulez utiliser pour transmettre des paquets.
6. Cliquez sur **Persistent** sous WEP Key Type.Cette action permet à l'adaptateur client de conserver cette clé WEP, même lorsque l'adaptateur est mis hors tension ou au redémarrage de l'ordinateur sur lequel la clé est installée. Si vous choisissez Temporaire pour cette option, la clé WEP est perdue lorsque l'adaptateur client est hors tension.

7. Click OK.

Activer WEP

Procédez comme suit :

1. Ouvrez ACU et sélectionnez **Modifier les propriétés** dans la barre de menus.
2. Cliquez sur l'onglet **Sécurité réseau** afin d'afficher les options de sécurité.
3. Cochez la case **Activer WEP** afin d'activer WEP.

Référez-vous à Configuration de WEP dans ADU pour connaître les étapes de configuration de WEP en utilisant ADU comme utilitaire client.

Configurer les ponts de groupe de travail

Il existe des différences entre le pont de groupe de travail Aironet 340 et le pont Aironet 340. Cependant, la configuration du pont de groupe de travail pour utiliser WEP est presque identique à celle du pont. Reportez-vous à la section Configurer les ponts Aironet pour la configuration du pont.

1. Connectez-vous au pont de groupe de travail.
2. Accédez au menu Confidentialité.Choisissez **Main > Configuration > Radio > I80211 > Privacy** afin d'accéder au menu Privacy VxWorks.

Paramètres

Le menu Confidentialité présente les paramètres répertoriés dans cette section. Configurez les options sur le pont de groupe de travail dans l'ordre suivant :

1. Key (Clé)
2. Transmission
3. authentification
4. Chiffrement

Voici les options :

- **Key (Clé)**L'option Key (Clé) établit la clé WEP que le pont utilise pour recevoir des paquets. La valeur doit correspondre à la clé utilisée par le point d'accès ou autre périphérique avec lequel le pont de groupe de travail communique. La clé comprend jusqu'à 10 caractères hexadécimaux pour le chiffrement à 40 bits ou 26 caractères hexadécimaux pour le chiffrement à 128 bits. Les caractères hexadécimaux peuvent être n'importe quelle combinaison de ces chiffres :0 à 9a à fA à F
- **Transmission**L'option Transmit (Transmission) établit la clé WEP que le pont utilise pour transmettre des paquets. Vous pouvez choisir d'utiliser la même clé que celle utilisée pour l'option Clé. Si vous choisissez une autre clé, vous devez établir une clé correspondante sur l'AP.Une seule clé WEP peut être utilisée à la fois pour les transmissions. La clé WEP que vous utilisez pour transmettre des données doit avoir la même valeur sur votre pont de groupe de travail et sur les autres périphériques avec lesquels il communique.
- **Authentification (Auth)**Le paramètre Auth détermine la méthode d'authentification utilisée par le système. Les options sont les suivantes :**Open (RECOMMANDÉ)** : le paramètre Open par

défaut permet à n'importe quel point d'accès, quels que soient ses paramètres WEP, de s'authentifier, puis de tenter de communiquer avec le pont.**Shared Key** : ce paramètre demande au pont d'envoyer une requête de clé partagée en texte clair aux points d'accès afin de tenter de communiquer avec le pont. Le paramètre Shared Key (Clé partagée) peut laisser le pont ouvert à une attaque en texte connu par des intrus. Par conséquent, ce paramètre n'est pas aussi sécurisé que le paramètre Open.

- **Chiffrement**L'option Encryption définit les paramètres de chiffrement sur tous les paquets de données, à l'exception des paquets d'association et de certains paquets de contrôle. Il existe quatre options :**Remarque :** Le chiffrement doit être actif sur l'AP et une clé doit être définie correctement.**Désactivé** : paramètre par défaut. Tout le chiffrement est désactivé. Le pont de groupe de travail ne communique pas avec un point d'accès avec l'utilisation de WEP.**On (RECOMMANDÉ)** : ce paramètre nécessite le chiffrement de tous les transferts de données. Le pont de groupe de travail communique uniquement avec les points d'accès qui utilisent WEP.**Mixed on** : ce paramètre signifie que le pont utilise toujours WEP afin de communiquer avec l'AP. Cependant, le point d'accès communique avec tous les périphériques, qu'ils utilisent WEP ou non.**Mixed off** : ce paramètre signifie que le pont n'utilise pas WEP pour communiquer avec l'AP. Cependant, le point d'accès communique avec tous les périphériques, qu'ils utilisent WEP ou non.**Attention :** Si vous sélectionnez On ou Mixed on comme catégorie WEP et que vous configurez le pont par le biais de sa liaison radio, la connectivité au pont est perdue si vous définissez la clé WEP de manière incorrecte. Assurez-vous d'utiliser exactement les mêmes paramètres lorsque vous définissez la clé WEP sur le pont de groupe de travail et la clé WEP sur les autres périphériques de votre WLAN.

Informations connexes

- Association de normes IEEE
- Produits LAN sans fil de la gamme Aironet 340
- Ressources de prise en charge sans fil
- Page Wireless LAN Support
- Guide de configuration du logiciel Cisco IOS pour les points d'accès Cisco Aironet
- Guide de configuration du logiciel Cisco IOS pour le pont/point d'accès extérieur de la gamme Cisco Aironet 1300
- Guide de configuration logicielle de points d'accès Cisco Aironet pour VxWorks
- Guide de configuration du logiciel du pont de la gamme Cisco Aironet 1400
- Guides de configuration des adaptateurs client LAN sans fil Cisco Aironet
- Présentation de la sécurité des LAN sans fil Cisco
- Sécurisation des réseaux sans fil (mobilité)
- 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