تكوين WEP على نقاط الوصول والجسور Aironet

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
تكوين WEP على نقاط الوصول Aironet
نقاط وصول Aironet التي تشغل نظام تشغيل VxWorks
إعدادات VxWorks
نقاط الوصول Aironet APs التي تشغل برنامج Cisco IOS Software
تكوين جسور Aironet
إعدادات VxWorks
تكوين مهايئات عميلة
تعيين مفاتيح WEP
تمكين WEP
تكوين جسور مجموعة العمل
الإعدادات
معلومات ذات صلة

المقدمة

يزود هذا وثيقة طريقة أن يشكل سلكي مكافئ خصوصية (WEP) على cisco Aironet لاسلكي lan مكون (WLAN).

ملاحظة: راجع قسم مفاتيح الويب الثابتة في الفصل 6 - تكوين شبكات WLAN للحصول على مزيد من المعلومات حول تكوين WEP على وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs).

WEP هو خوارزمية التشفير المضمنة في مقياس 802.11 (Wi-Fi). يستخدم تشفير WEP تشفير الدفق الخاص بالرمز 4 (RC4) مع مفاتيح 40-بت أو 104-بت ومتجه تهيئة 24-بت (IV).

وكما يحدد المعيار، يستخدم WEP خوارزمية RC4 مع مفتاح 40-بت أو 104-بت و 24-بت IV. RC4 هو خوارزمية متماثلة لأنه يستخدم نفس المفتاح لتشفير البيانات وفك تشفيرها. لدى تمكين WEP يحتوي كل "محطة" راديو على مفتاح. يستخدم المفتاح لخردة البيانات قبل إرسال البيانات عبر موجات الهواء. إذا تلقت المحطة حزمة لم يتم تشتيتها باستخدام المفتاح المناسب، يتم تجاهل الحزمة ولا يتم تسليمها أبدا إلى المضيف.

يمكن إستخدام WEP في المقام الأول للمكاتب المنزلية أو المكاتب الصغيرة التي لا تتطلب تأمينا قويا جدا.

تنفيذ Aironet WEP موجود في الجهاز. لذلك يكون للأداء أدنى حد من التأثير عندما تستخدم WEP.

ملاحظة: هناك بعض المشاكل المعروفة في WEP مما يجعله ليس أسلوب تشفير قوي. القضايا هي:

- هناك قدر كبير من النفقات الإدارية الإضافية للحفاظ على مفتاح WEP مشترك.
- يحتوي WEP على نفس المشكلة الموجودة في كافة الأنظمة التي تعتمد على المفاتيح المشتركة. أي سر يعطى لشخص واحد يصبح علنيا بعد فترة من الزمن.
- يتم إرسال خوارزمية WEP الناشئة في نص واضح.
- المجموع الاختباري ل WEP خطي ويمكن التنبؤ به.

وقد تم إنشاء بروتوكول سلامة المفاتيح المؤقتة (TKIP) لمعالجة مشاكل WEP هذه. وكما هو الحال مع WEP، يستخدم TKIP تشفير RC4. ومع ذلك، فإن TKIP يحسن WEP بإضافة تدابير مثل تجزئة مفتاح كل حزمة، وفحص سلامة الرسائل (MIC)، وتدوير مفتاح البث لمعالجة نقاط الضعف المعروفة ل WEP. يستخدم TKIP تشفير تدفق RC4 مع مفاتيح 128-بت للتشفير ومفاتيح 64-بت للمصادقة.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أنه يمكنك إجراء اتصال إداري بأجهزة شبكة WLAN وأن الأجهزة تعمل بشكل طبيعي في بيئة غير مشفرة.

من أجل تكوين WEP قياسي 40-بت، يجب أن يكون لديك وحدتين راديو أو أكثر تتواصلان مع بعضهما البعض.

ملاحظة: يمكن لمنتجات Aironet إنشاء إتصالات WEP من فئة 40 بت بمنتجات غير متوافقة مع IEEE 802.11b من Cisco. لا يتناول هذا المستند تكوين الأجهزة الأخرى.

لإنشاء إرتباط WEP من فئة 128 بت، لا تتفاعل منتجات Cisco إلا مع منتجات Cisco الأخرى.

المكونات المستخدمة

أستخدم هذه المكونات مع هذا المستند:

- وحدتان أو أكثر من وحدات الراديو التي تتواصل مع بعضها البعض
- اتصال إداري بجهاز WLAN

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

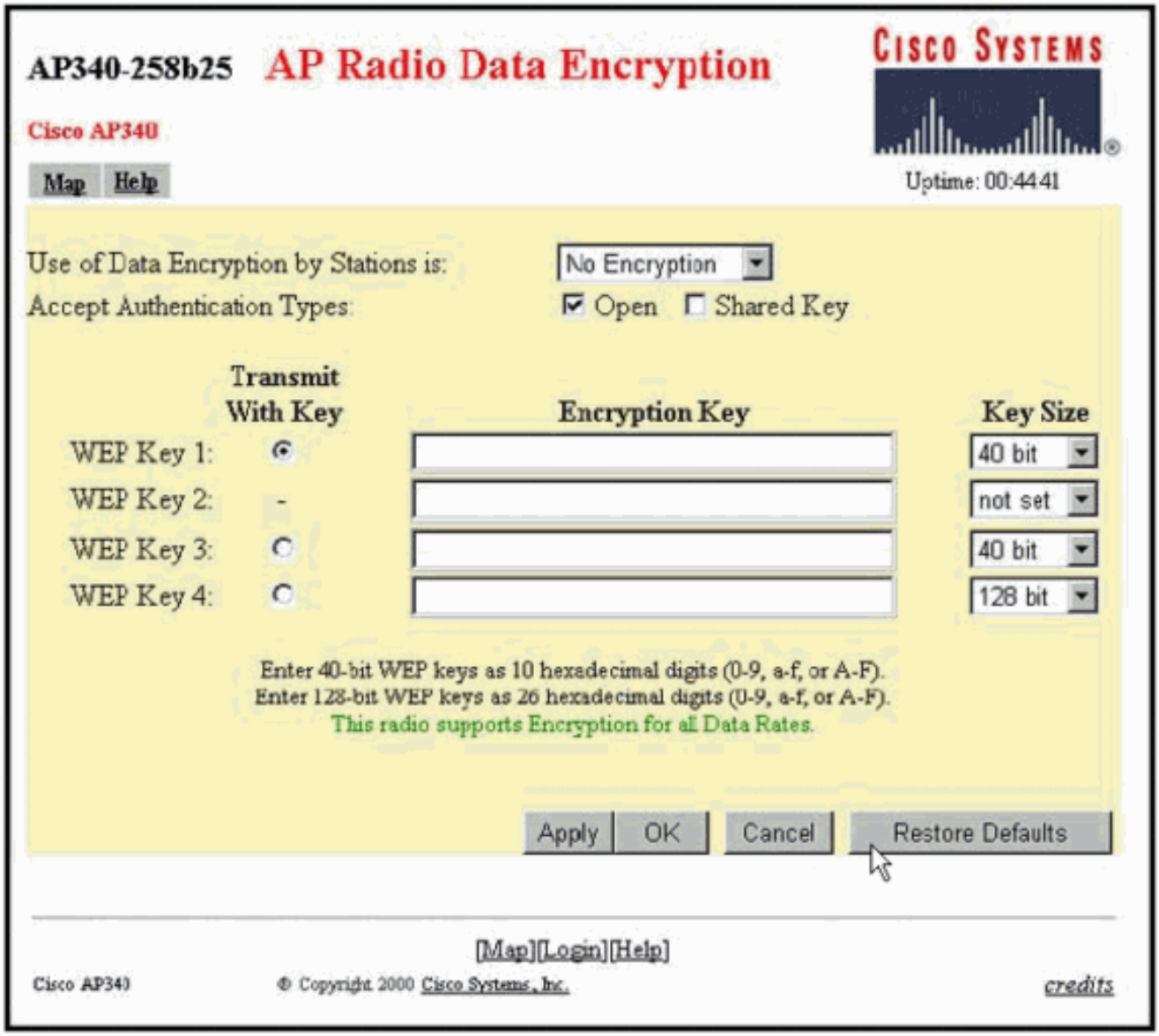
تكوين WEP على نقاط الوصول Aironet

نقاط وصول Aironet التي تشغل نظام تشغيل VxWorks

أكمل الخطوات التالية:

1. إجراء اتصال بنقطة الوصول (AP).
2. انتقل إلى قائمة AP للتشفير اللاسلكي.أستخدم أحد المسارات التالية:**حالة الملخص > إعداد > راديو/أجهزة AP**

> تشفير البيانات اللاسلكي (WEP) > تشفير بيانات الراديو لـ APحالة الملخص > إعداد > التأمين > إعداد التأمين: تشفير البيانات اللاسلكية (WEP) > تشفير بيانات الراديو لنقطة الوصولملاحظة: لإجراء تغييرات على هذه الصفحة، يجب أن تكون مسؤولا يتمتع بإمكانيات الهوية والكتابة.**عرض مستعرض الويب لقائمة تشفير البيانات اللاسلكية لنقطة الوصول (AP)**



إعدادات VxWorks

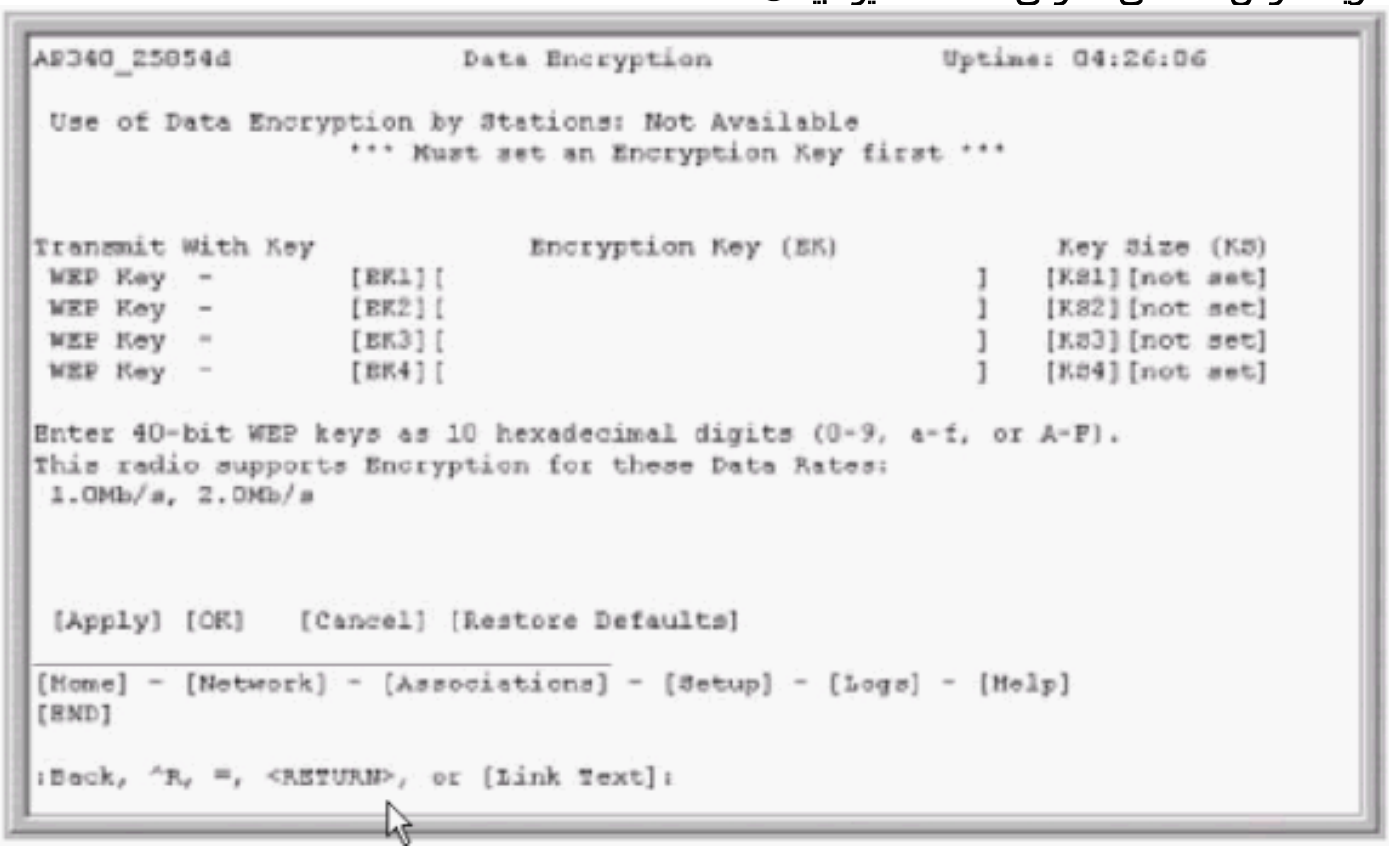
تقدم صفحة تشفير البيانات اللاسلكية لنقطة الوصول مجموعة متنوعة من الخيارات لاستخدامها. تكون بعض الخيارات إلزامية لـ WEP. يلاحظ هذا القسم هذه الخيارات الإلزامية. لا يلزم وجود خيارات أخرى لكي يعمل WEP، ولكن يوصى بها.

- **إستخدام تشفير البيانات حسب المحطات هو:**أستخدم هذا الإعداد لاختيار ما إذا كان يجب على العملاء إستخدام تشفير البيانات عند إتصالهم بنقطة الوصول. تسرد القائمة المنسدلة ثلاثة خيارات:**لا يوجد تشفير (افتراضي)**—يتطلب من العملاء الاتصال بنقطة الوصول دون أي تشفير للبيانات. لا يوصى بهذا الإعداد.**إختياري**—يسمح للعملاء بالتواصل مع نقطة الوصول إما بتشفير البيانات أو بدونه. وعادة ما تستخدم هذا الخيار عندما يكون لديك أجهزة عميل لا يمكنها إجراء اتصال WEP، مثل العملاء من غير Cisco في بيئة WEP 128-بت.**التشفير الكامل (مستحسن)**—يتطلب من العملاء إستخدام تشفير البيانات عند إتصالهم بنقطة الوصول. غير مسموح للعملاء الذين لا يستخدمون تشفير البيانات بالاتصال. يوصى بهذا الخيار إذا كنت ترغب في زيادة أمان شبكة WLAN الخاصة بك إلى الحد الأقصى.**ملاحظة:** يجب عليك تعيين مفتاح WEP قبل تمكين إستخدام التشفير. راجع قسم **مفتاح التشفير (إلزامي)** في هذه القائمة.

- **قبول أنواع المصادقة**يمكنك إختيار مفتاح مفتوح أو مشترك أو كلا من هذين الخيارين لتعيين المصادقة التي يتعرف عليها نقطة الوصول.**فتح (مستحسن)**—يسمح هذا الإعداد الافتراضي لأي جهاز، بغض النظر عن مفاتيح WEP الخاصة به، بالمصادقة ومحاولة الاقتران.**مفتاح مشترك**— يقول هذا الإعداد لنقطة الوصول أن يرسل استعلام مفتاح مشترك نص عادي إلى أي جهاز يحاول الاقتران بنقطة الوصول.**ملاحظة:** يمكن أن يترك هذا الاستعلام نقطة الوصول مفتوحة لهجوم نص معروف من الدخلاء. لذلك، فإن هذا الإعداد غير آمن مثل الإعداد "فتح".
- **الإرسال باستخدام المفتاح**تتيح لك هذه الأزرار تحديد المفتاح الذي تستخدمه نقطة الوصول أثناء نقل البيانات. يمكنك تحديد مفتاح واحد فقط في كل مرة. يمكن إستخدام أي من مفاتيح المجموعة أو كلها لتلقي البيانات. يجب تعيين المفتاح قبل تعيينه كمفتاح إرسال.
- **مفتاح التشفير (إلزامي)**تتيح لك هذه الحقول إدخال مفاتيح WEP. أدخل 10 أرقام سداسية عشرية لمفاتيح WEP ذات 40-بت أو 26 رقما سداسية عشرية لمفاتيح WEP ذات 128-بت. يمكن أن تكون المفاتيح أي تركيب لهذه الأرقام:من 0 إلى 9من أ إلى ومن A إلى Fالحماية أمان مفتاح WEP، لا تظهر مفاتيح WEP الموجودة في النص العادي في حقول الإدخال. في الإصدارات الأخيرة من نقاط الوصول، يمكنك حذف المفاتيح الموجودة. ومع ذلك، لا يمكنك تحرير المفاتيح الموجودة.**ملاحظة:** يجب عليك إعداد مفاتيح WEP لشبكتك ونقاط الوصول (AP) وأجهزة العميل بالطريقة نفسها تماما. على سبيل المثال، إذا قمت بضبط مفتاح WEP 3 على نقطة الوصول إلى 0987654321 وحدد هذا المفتاح كمفتاح نشط، فيجب عليك أيضا تعيين مفتاح WEP 3 على جهاز العميل إلى نفس القيمة.
- **حجم المفتاح (إلزامي)**يضبط هذا الإعداد المفاتيح على -40 WEPبت أو 128-بت. إذا ظهر "لم يتم تعيينه" لهذا التحديد، فلن يتم تعيين المفتاح.**ملاحظة:** لا يمكنك حذف مفتاح عن طريق تحديد "غير معين".
- **أزرار الإجراءات**إعدادات التحكم في أربعة أزرار إجراءات. إذا كان JavaScript متاحا على متصفح الويب الخاص بك، تظهر نافذة تأكيد منبثقة بعد أن تنقر أي زر، ما عدا إلغاء الأمر.**تطبيق**—ينشط هذا الزر إعدادات القيمة الجديدة. يبقى المستعرض على الصفحة.**موافق**—يطبق هذا الزر الإعدادات الجديدة وينقل المستعرض مرة أخرى إلى صفحة الإعداد الرئيسية.**إلغاء الأمر**- يقوم هذا الزر بإلغاء تغييرات الإعداد وإرجاع الإعدادات إلى القيم التي تم تخزينها مسبقا. ثم ارجع إلى صفحة "الإعداد" الرئيسية.**إستعادة الافتراضيات**- يغير هذا الزر كل الإعدادات في هذه الصفحة إلى إعدادات المصنع الافتراضية.

ملاحظة: في الإصدارات الأخيرة من نقاط الوصول من Cisco IOS®، يتوفر فقط أزرار التحكم **تطبيق** و**إلغاء الأمر** لهذه الصفحة.

طريقة عرض المحاكى الطرفى لقائمة تشفير البيانات



عرض المحاكي الطرفي لتسلسل تكوين مفتاح WEP (برنامج 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#
```

نقاط الوصول Aironet APs التي تشغل برنامج Cisco IOS Software

أكمل الخطوات التالية:

1. إجراء اتصال بنقطة الوصول.
2. من خيار قائمة التأمين الموجود على الجانب الأيسر من النافذة، أختر **مدير التشفير** لواجهة الراديو التي تريد تكوين مفاتيح WEP الثابتة الخاصة بك.**عرض مستعرض الويب لقائمة مدير تشفير أمان نقطة الوصول**

تكوين جسور Aironet

إذا كنت تستخدم VxWorks، أكمل الخطوات التالية:

1. قم بإجراء اتصال بالجسر.
2. انتقل إلى قائمة الخصوصية.أختر **القائمة الرئيسية > التكوين > الراديو > i80211 > الخصوصية**.تتحكم قائمة الخصوصية في إستخدام التشفير على حزمة البيانات التي يتم إرسالها عبر الهواء بواسطة أجهزة الراديو. يتم إستخدام خوارزمية RSA RC4 وأحد المفاتيح التي تصل إلى أربعة مفاتيح معروفة لتشفير الحزم. يجب أن تعرف كل عقدة في خلية الراديو كل المفاتيح المستخدمة، لكن يمكن تحديد أي من المفاتيح لنقل البيانات.**عرض**

المحاكي الطرفي لقائمة الخصوصية

```
        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
>_
```

راجع تكوين مجموعات التشفير و WEP - جسر Series 1300 وتكوين ميزات WEP و WEP - جسر Series 1400 للحصول على معلومات حول كيفية تكوين WEP في 1300 و 1400 Series Bridge من خلال وضع CLI.

in order to استعملت GUI أن يشكل 1300 و 1400 sery جسر، أتمت ال نفسه إجراء يفسر في أن Aironet APs شوط cisco ios برمجية قسم من هذا وثيقة.

إعدادات VxWorks

تعرض قائمة الخصوصية مجموعة من الخيارات التي يجب تكوينها. تكون بعض الخيارات إلزامية ل WEP. يلاحظ هذا القسم هذه الخيارات الإلزامية. لا يلزم وجود خيارات أخرى لكي يعمل WEP، ولكن يوصى بها.

يعرض هذا القسم خيارات القائمة بالترتيب الذي تظهر به في طريقة عرض المحاكي الطرفي لقائمة الخصوصية. ومع ذلك، قم بتكوين الخيارات في هذا الترتيب:

1. المفتاح
2. إرسال
3. Auth
4. العميل
5. تشفير

يضمن التكوين في هذا الأمر إعداد الشروط المسبقة الضرورية عند تكوين كل إعداد.

هذه هي الخيارات:

- **المفتاح (إلزامي)**يقوم خيار المفتاح برمجة مفاتيح التشفير في الجسر. يطلب منك تعيين أحد المفاتيح الأربعة. يطلب منك مرتين إدخال المفتاح. in order to عينت المفتاح، أنت ينبغي دخلت إما 10 أو 26 رقم سداسي عشر، أي يعتمد على ما إذا الجسر تشكيل ل 40-بت أو 128-بت مفتاح. أستخدم أي تركيبة من هذه الأرقام:من 0 إلى 9من أ إلى ومن A إلى Fيجب أن تتطابق المفاتيح في ***كل*** عقد في خلية الراديو، ويجب عليك إدخال المفاتيح بنفس الترتيب. أنت لا تحتاج أن يعين كل المفاتيح الأربعة، ما دام عدد المفاتيح مطابق في كل أداة في ال WLAN.
- **إرسال**يعلم خيار الإرسال الراديو أي المفاتيح سيتم إستخدامه لإرسال الحزم. يمكن لكل جهاز لاسلكي فك تشفير الحزم المستلمة التي يتم إرسالها مع أي من المفاتيح الأربعة.
- **Auth**تستخدم خيار المصادقة على جسور مكرر لتحديد وضع المصادقة الذي تستخدمه الوحدة للاتصال بأولادها. القيم المسموح بها هي مفتاح مفتوح أو مشترك. يحدد بروتوكول 802.11 إجراء يجب على العميل بموجبه المصادقة مع أحد الوالدين قبل أن يتمكن العميل من الاقتران.**فتح (مستحسن)**— هذا الوضع من المصادقة هو عملية خالية بشكل أساسي. يسمح لجميع العملاء بالمصادقة.**المفتاح المشترك**—يسمح هذا الوضع للأب بإرسال نص التحدي إلى العميل، والذي يقوم العميل بتشفيره وإعادته إلى الأصل. إذا قام الأصل بفك تشفير نص التحدي بنجاح، تتم مصادقة العميل.**تحذير:** لا تستخدم وضع المفتاح المشترك. عندما تستخدمه، يتم إرسال نسخة مشفرة و ذات نص عادي من نفس البيانات في الهواء. وهذا لا يكسب شيئا. إذا كان مفتاح المستخدم غير صحيح، فإن

الوحدة لا تقوم بفك تشفير الحزم، ولا يمكن للحزم الوصول إلى الشبكة.

- **العميل**يحدد خيار العميل وضع المصادقة الذي تستخدمه عقد العميل لإقرانه بالوحدة. هذه هي القيم المسموح بها:**فتح (مستحسن)**— هذا الوضع من المصادقة هو عملية خالية بشكل أساسي. يسمح لجميع العملاء بالمصادقة.**المفتاح المشترك**—يسمح هذا الوضع للأب بإرسال نص التحدي إلى العميل، والذي يقوم العميل بتشفيره وإعادته إلى الأصل. إذا قام الأصل بفك تشفير نص التحدي بنجاح، تتم مصادقة العميل.**كلاهما**—يسمح هذا الوضع للعميل باستخدام أي من الوضعين.
- **تشفيرإيقاف**— إذا قمت بضبط خيار التشفير على إيقاف التشغيل، فلن يتم إجراء أي تشفير. ترسل البيانات في الخفاء.**قيد التشغيل (إلزامي)**— إذا قمت بضبط خيار التشفير على تشغيل، فسيتم تشفير جميع حزم البيانات المرسلة ويتم تجاهل أي حزم مستلمة غير مشفرة.**مختلط**—في الوضع المختلط، يقبل جسر الجذر أو مكرر الاقتران من العملاء الذين لديهم تشفير قيد التشغيل أو إيقاف التشغيل. في هذه الحالة، يتم تشفير حزم البيانات فقط بين العقد التي تدعم كلتيهما. يتم إرسال حزم البث المتعدد في الخلاء. يمكن أن ترى كل العقد الحزم.**تحذير:** لا تستخدم الوضع المختلط. إذا قام العميل الذي تم تمكين التشفير بإرسال حزمة بث متعدد إلى أصله، فسيتم تشفير الحزمة. يقوم الأصل بفك تشفير الحزمة ويرسل الحزمة في المسح إلى الخلية، ويمكن للعقد الأخرى أن ترى الحزمة. يمكن أن تساهم القدرة على عرض حزمة في كل من النموذج المشفر وغير المشفر في كسر مفتاح. يتم تضمين الوضع المختلط فقط للتوافق مع الموردين الآخرين.

تكوين مهايئات عميلة

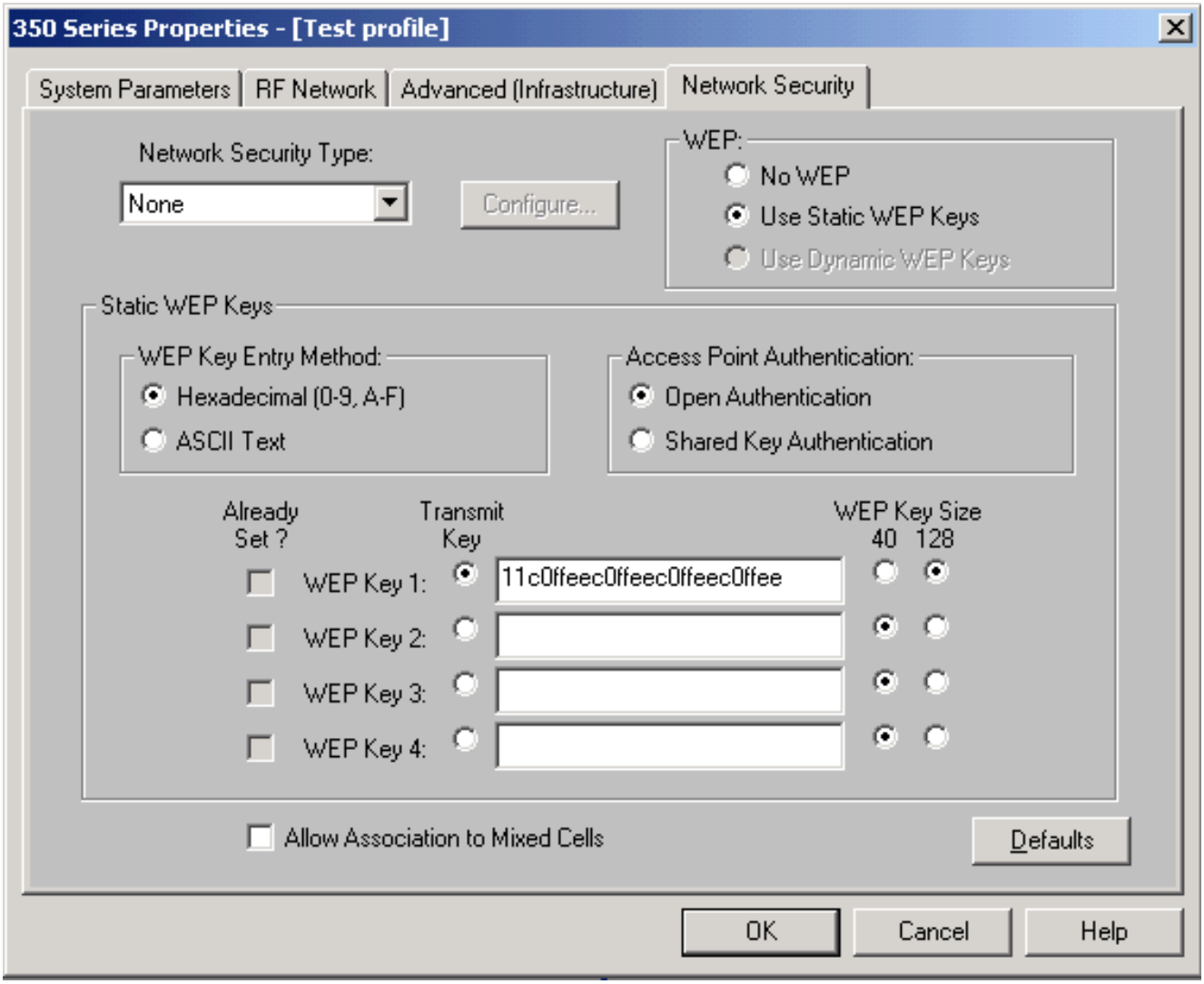
يجب عليك إكمال خطوتين رئيسيتين لإعداد WEP على مهايئ عميل Aironet:

1. قم بتكوين مفتاح/مفاتيح WEP في إدارة تشفير العميل.
2. تمكين WEP في الأداة المساعدة لعميل Aironet (ACU).

تعيين مفاتيح WEP

أكمل الخطوات التالية لإعداد مفاتيح WEP على مهايئات العميل:

1. افتح وحدة التحكم في الوصول (ACU) واختر **مدير ملف التعريف**.
2. أختر التوصيف الذي تريد تمكين WEP فيه ثم انقر على **تحرير**.
3. انقر على علامة التبويب **أمان الشبكة** لعرض خيارات الأمان، وانقر على **إستخدام مفاتيح WEP الثابتة**.يؤدي هذا الإجراء إلى تنشيط خيارات تكوين WEP غير نشطة عند عدم تحديد WEP.



4. لمفتاح WEP الذي تريد إنشائه، أختر إما **40** بت أو **128** بت تحت حجم مفتاح WEP على الجانب الأيمن من النافذة.**ملاحظة:** يمكن لمهايئات الأجهزة العميلة إصدار 128 بت إستخدام مفاتيح إصدار 40 بت أو 128 بت. إلا أنه لا يمكن للمهايئات ذات 40 بت إلا إستخدام مفاتيح 40 بت.**ملاحظة** يجب أن يتطابق مفتاح WEP لمهايئ العميل مع مفتاح WEP الذي تستخدمه مكونات WLAN الأخرى التي تتصل بها.عندما تقوم بضبط أكثر من مفتاح WEP واحد، يجب عليك تعيين مفاتيح WEP إلى نفس أرقام مفاتيح WEP لجميع الأجهزة. يجب أن تتكون مفاتيح WEP من الحروف السداسية العشرية ويجب أن تحتوي على 10 حروف لمفاتيح WEP ذات 40 بت أو 26 حرفا لمفاتيح WEP ذات 128 بت. يمكن أن تكون الحروف السداسية العشرية:من 0 إلى 9من أ إلى ومن A إلى F**ملاحظة:** مفاتيح WEP-text ل ASCII غير مدعومة على نقاط الوصول (APs) من Aironet. لذلك، يجب عليك إختيار الخيار السداسي عشر (0-9، A-F) إذا كنت تخطط لاستخدام مهايئ العميل مع نقاط الوصول (APs) هذه.**ملاحظة** بعد أن تقوم بإنشاء مفتاح WEP، يمكنك الكتابة فوقه. ولكن لا يمكنك تحريره أو حذفه.**ملاحظة:** إذا كنت تستخدم إصدارا أحدث من Aironet Desktop Utility (ADU) بدلا من ACU كأداة عميل مساعدة، فيمكنك أيضا حذف مفتاح WEP الذي تم إنشاؤه واستبداله بمفتاح جديد.
5. انقر فوق زر **إرسال مفتاح** بجانب أحد المفاتيح التي قمت بإنشائها.مع هذا الإجراء، تشير إلى أن هذا المفتاح هو المفتاح أن أنت تريد أن يستعمل أن يبث ربط.
6. انقر على **متواصل** ضمن نوع مفتاح WEP.يسمح هذا الإجراء لمهايئ العميل بالاحتفاظ بمفتاح WEP هذا، حتى عند إزالة طاقة المحول أو عند إعادة تشغيل الكمبيوتر الذي تم تثبيت المفتاح فيه. إذا أخترت مؤقت لهذا الخيار، يفقد مفتاح WEP عند إزالة الطاقة من محول العميل.
7. وانقر فوق **OK**.

تمكين WEP

أكمل الخطوات التالية:

1. افتح وحدة التحكم بالوصول (ACU) واختر **تحرير الخصائص** من شريط القائمة.
2. انقر على علامة التبويب **أمان الشبكة** لعرض خيارات الأمان.
3. حدد خانة الاختيار **تمكين WEP** لتنشيط WEP.

راجع تكوين WEP في ADU للاطلاع على خطوات تكوين WEP باستخدام ADU كأداة مساعدة عميل.

تكوين جسور مجموعة العمل

هناك إختلافات بين جسر مجموعة العمل Aironet 340 Series وجسر Aironet 340 Series. ومع ذلك، فإن تكوين جسر مجموعة العمل لاستخدام WEP يكاد يكون مطابقا لتكوين الجسر. رأيت ال configure Aironet جسر قسم ل التشكيل من الجسر.

1. الاتصال بجسر مجموعة العمل.
2. انتقل إلى قائمة الخصوصية.أخترت **رئيسي>تشكيل>لاسلكي>i80211>خصوصية** in order to نفذت الخصوصية vxWorks قائمة.

الإعدادات

تعرض قائمة الخصوصية الإعدادات التي يسردها هذا القسم. تكوين الخيارات على جسر مجموعة العمل بهذا الترتيب:

1. المفتاح
2. إرسال
3. Auth
4. تشفير

هذه هي الخيارات:

- **المفتاح**يحدد خيار المفتاح مفتاح WEP الذي يستخدمه الجسر لتلقي الحزم. يجب أن تتطابق القيمة مع المفتاح الذي تستخدمه نقطة الوصول (AP) أو أي جهاز آخر يتصل به جسر مجموعة العمل. يتكون المفتاح من 10 حروف سادس عشرية للتشفير 40-بت أو 26 حرف سادس عشري للتشفير 128-بت. يمكن أن تكون الحروف السداسية العشرية أي تركيب لهذه الأرقام:من 0 إلى 9من أ إلى ومن A إلى F
- **إرسال**يؤسس خيار الإرسال مفتاح WEP الذي يستخدمه الجسر لإرسال الحزم. يمكنك إختيار إستخدام نفس المفتاح الذي أستخدمته لخيار المفتاح. إذا أخترت مفتاحا مختلفا، فيجب عليك إنشاء مفتاح مطابق على نقطة الوصول.يمكن إستخدام مفتاح WEP واحد فقط في وقت واحد لعمليات الإرسال. يجب تعيين مفتاح WEP الذي تستخدمه لإرسال البيانات إلى نفس القيمة على Workgroup Bridge والأجهزة الأخرى التي يتصل بها.
- **المصادقة (المصادقة)**تحدد معلمة المصادقة طريقة المصادقة التي يستخدمها النظام. الخيارات هي:**فتح (مستحسن)**- يسمح الإعداد الافتراضي لفتح أي نقطة وصول، بغض النظر عن إعدادات WEP الخاصة بها، بالمصادقة ثم محاولة الاتصال بالجسر.**مفتاح مشترك**- يرشد هذا الإعداد الجسر لإرسال استعلام مفتاح مشترك نص عادي إلى نقاط الوصول في محاولة للاتصال بالجسر. يمكن أن يترك إعداد "المفتاح المشترك" الجسر مفتوحا لهجوم نص معروف من الدخلاء. لذلك، فإن هذا الإعداد غير آمن مثل الإعداد "فتح".
- **تشفير**يعمل خيار التشفير على تعيين معلمات التشفير على جميع حزم البيانات، باستثناء حزم الاقتران وبعض حزم التحكم. هناك أربعة خيارات:**ملاحظة:** يجب أن يكون لنقطة الوصول تشفير نشط وتعيين مفتاح بشكل صحيح.**إيقاف التشغيل** — هذا هو الإعداد الافتراضي. تم إيقاف تشغيل كافة عمليات التشفير. لا يتصل جسر مجموعة العمل بنقطة وصول باستخدام WEP.**قيد التشغيل (مستحسن)**—يتطلب هذا الإعداد تشفير جميع عمليات نقل البيانات. يتصل "جسر مجموعة العمل" فقط بنقاط الوصول التي تستخدم WEP.**تشغيل مختلط**—يعني هذا الإعداد أن الجسر يستخدم WEP دائما للاتصال بنقطة الوصول. ومع ذلك، تتصل نقطة الوصول بجميع الأجهزة، سواء أستخدمت WEP أو لم تستخدم WEP.**إيقاف مختلط**- يعني هذا الإعداد أن الجسر لا يستخدم WEP للاتصال بنقطة الوصول. ومع ذلك، تتصل نقطة الوصول بجميع الأجهزة، سواء أستخدمت WEP أو لم تستخدم WEP.**تحذير:** إذا قمت بتحديد تشغيل أو إختلاط في فئة WEP وقمت بتكوين الجسر من خلال

رابط الراديو الخاص به، يتم فقد الاتصال بالجسر إذا قمت بضبط مفتاح WEP بشكل غير صحيح. تأكد من إستخدام نفس الإعدادات تماما عند ضبط مفتاح WEP على جسر مجموعة العمل ومفتاح WEP على الأجهزة الأخرى على الشبكة المحلية اللاسلكية (WLAN).

معلومات ذات صلة

- رابطة معايير IEEE
- منتجات الشبكات المحلية اللاسلكية Aironet 340 Series
- موارد الدعم اللاسلكي
- صفحة دعم شبكة LAN اللاسلكية
- دليل تكوين برنامج Cisco IOS Software لنقاط الوصول Cisco Aironet
- دليل تكوين برنامج Cisco IOS Software لنقطة الوصول الخارجية/Bridge سلسلة Cisco Aironet 1300
- دليل تكوين برنامج نقطة الوصول Cisco Aironet ل VxWorks
- دليل تكوين برنامج Cisco Aironet 1400 Series Bridge Software
- أدلة تكوين مهايئات عميلة للشبكة المحلية (LAN) اللاسلكية Aironet من Cisco
- نظرة عامة على أمان شبكة LAN اللاسلكية من Cisco
- الشبكات اللاسلكية الآمنة (المتنقلة)
- نقطة الوصول كمثال لتكوين جسر مجموعة العمل
- الأسئلة المتداولة حول جسر مجموعة عمل Aironet من Cisco
- إجراء إسترداد كلمة المرور لمعدات Cisco Aironet
- الأسئلة المتداولة حول نقطة وصول Cisco Aironet
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).