الكشف المخادع بموجب الشبكات اللاسلكية الموحدة

المحتويات

المقدمة

توسع الشبكات اللاسلكية الشبكات السلكية وتزيد من إنتاجية العاملين والوصول إلى المعلومات. ومع ذلك، تمثل الشبكة اللاسلكية غير المصرح بها طبقة إضافية من المخاوف الأمنية. مع تقليل التفكير في أمان المنفذ على الشبكات السلكية، تعد الشبكات اللاسلكية امتدادا سهلا للشبكات السلكية. وبالتالي، فإن الموظف الذي يجلب نقطة الوصول (AP) الخاصة به من Cisco إلى بنية أساسية لاسلكية أو سلكية آمنة بشكل جيد ويسمح للمستخدمين غير المصرح لهم بالوصول إلى هذه الشبكة التي كانت لولا ذلك آمنة يمكن أن يخل بسهولة بشبكة آمنة.

يتيح الكشف المخادع لمسؤول الشبكة إمكانية مراقبة مشكلة الأمان هذه والقضاء عليها. توفر بنية الشبكة الموحدة من Cisco طريقتين للكشف المخادع اللتين تتيحان حلا كاملا للتعريف والاحتواء المخادعين دون الحاجة إلى شبكات وأدوات تغشية مكلفة يصعب تبريرها.

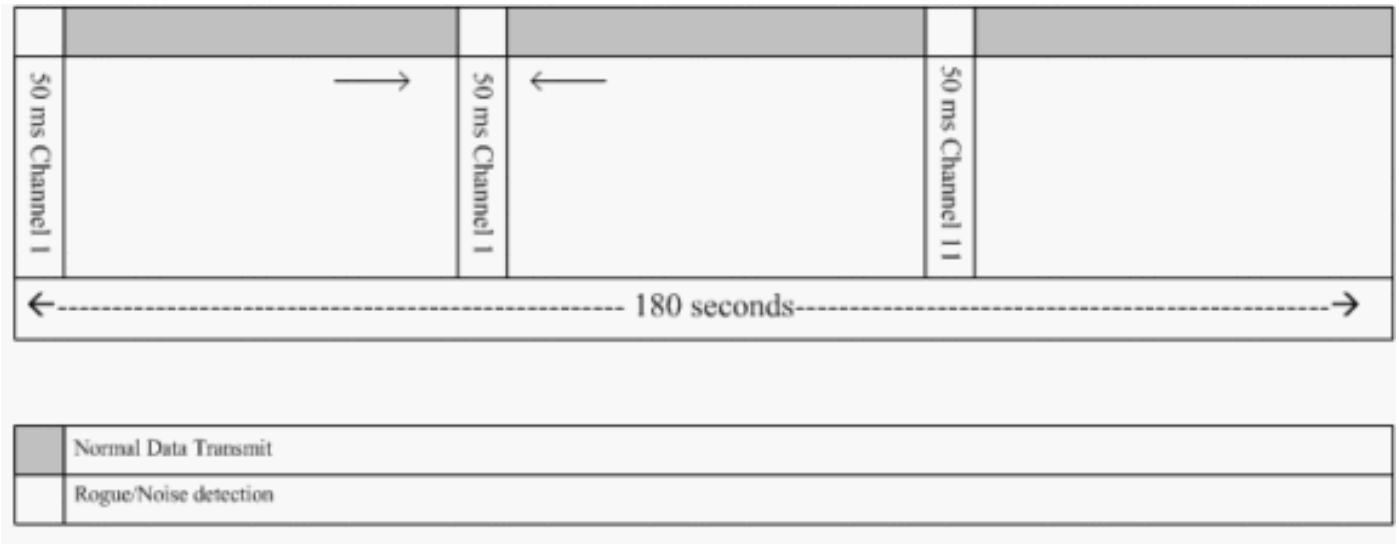
نظرة عامة على الميزة

لا يلتزم الكشف عن المجرمين بأي قواعد تنظيمية ولا يلزم الالتزام القانوني بتنفيذه. ومع ذلك، فإن الاحتواء المخادع عادة ما يطرح مسائل قانونية يمكن أن تضع مقدم البنية التحتية في وضع غير مريح إذا ما ترك للعمل تلقائيا. تعتبر Cisco حساسة للغاية لمثل هذه المشاكل وتوفر هذه الحلول. يتم تكوين كل وحدة تحكم باسم مجموعة RF.بمجرد تسجيل نقطة وصول من الوزن الخفيف بوحدة تحكم، فإنها تقوم بدمج **عنصر معلومات المصادقة (IE)** المحدد لمجموعة RF التي تم تكوينها على وحدة التحكم في جميع إطارات الاستجابة المزودة بأجهزة التوجيه/المسبار الخاصة بها. عندما تسمع نقطة الوصول في الوضع Lightweight إطارات الاستجابات من نقطة وصول (AP) إما دون **IE** هذا أو مع **IE خطأ**، فعندئذ تقوم نقطة الوصول في الوضع Lightweight بالإعلام عن نقطة الوصول (AP) كجهة مارقة وتسجيل BSSID الخاصة بها في جدول مخادع وإرسال الجدول إلى وحدة التحكم. هناك طريقتان، هما بروتوكول اكتشاف الموقع الدوار (RLDP) والتشغيل السلبي، ويتم شرحهما بالتفصيل؛ راجع قسم تحديد المخادع النشطة.

الاستكشاف المخادع للبنية الأساسية

قد يكون الاكتشاف المخادع في بيئة لاسلكية نشطة مكلفا. تتطلب هذه العملية نقطة الوصول الموجودة في الخدمة (أو الوضع المحلي) أن تتوقف عن الخدمة، وتستمع للضوضاء، وتقوم بالكشف عن المخادع. يقوم مسؤول الشبكة بتكوين القنوات للمسح الضوئي، ويقوم بتكوين الفترة الزمنية التي يتم فيها فحص جميع المحطات. وتستمع نقطة الوصول إلى 50 مللي ثانية لإرشادات العميل الدخيلة، ثم ترجع إلى القناة التي تم تكوينها من أجل خدمة العملاء مرة أخرى. يحدد هذا المسح الضوئي النشط، مقرونا برسائل مجاورة، نقاط الوصول التي هي مخادع وأي نقاط وصول هي صحيحة وجزء من الشبكة. من أجل تكوين القنوات التي تم مسحها ضوئيا وفترة وقت المسح الضوئي، استعرض إلى **شبكة لاسلكية > 802.11b/g** (إما **b/g**" أو "**a**" حسب متطلبات الشبكة) وحدد زر **التردد اللاسلكي التلقائي** في الزاوية العلوية اليمنى من نافذة المستعرض.

يمكنك التمرير لأسفل إلى **قنوات مراقبة الضوضاء/التداخل/المخادع** لتكوين القنوات التي سيتم مسحها ضوئيا بحثا عن المخادعين والضوضاء. الخيارات المتاحة هي: جميع القنوات (من 1 إلى 14) أو قنوات البلدان (من 1 إلى 11) أو قنوات اقتران القنوات الديناميكية (DCA) (بشكل افتراضي 1 و 6 و 11). يمكن تكوين فترة وقت المسح من خلال هذه القنوات في نفس النافذة، تحت **فواصل الشاشة (من 60 إلى 3600 ثوان)** مع فاصل قياس التشويش. بشكل افتراضي، يكون الفاصل الزمني للإصغاء لضجيج و مخادع خارج القناة هو 180 ثانية. هذا يعني أن كل قناة يتم مسحها ضوئيا كل 180 ثانية. هذا مثال على قنوات DCA التي يتم مسحها ضوئيا كل 180 ثانية:



كما هو موضح، فإن العدد الكبير من القنوات التي تم تكوينها ليتم مسحها ضوئيا مع الفواصل الزمنية القصيرة للمسح الضوئي، يترك وقتا أقل لنقطة الوصول حتى تقوم فعليا بخدمة عملاء البيانات.

تنتظر نقطة الوصول في الوضع Lightweight من أجل تسمية العملاء ونقاط الوصول (AP) بالفاسدين لأنه من المحتمل ألا يتم الإبلاغ عن هذه الفاسقات من قبل نقطة وصول أخرى حتى يتم إكمال دورة أخرى. تتحرك نقطة الوصول نفسها إلى نفس القناة مرة أخرى من أجل مراقبة نقاط الوصول (AP) المارقة والعملاء، بالإضافة إلى الضوضاء والتداخل. إذا تم الكشف عن نفس العملاء و/أو نقاط الوصول (APs)، فسيتم سردها على أنها مخادع في وحدة التحكم مرة أخرى. يبدأ جهاز التحكم الآن في تحديد ما إذا كان هؤلاء الفاسدون ملحقين بالشبكة المحلية أو مجرد نقطة وصول (AP) مجاورة. في كلتا الحالتين، تعتبر نقطة الوصول التي لا تشكل جزءا من الشبكة اللاسلكية المحلية المدارة دخيلة.

التفاصيل المخادعة

تذهب نقطة وصول (AP) خفيفة الوزن خارج القناة لمدة 50 مللي ثانية للاستماع إلى العملاء المخادعين والمراقبة بحثا عن الضوضاء وتداخل القنوات. يتم إرسال أي عملاء أو نقاط وصول (AP) مخادعين تم اكتشافهم إلى وحدة التحكم، والتي تجمع المعلومات التالية:

- عنوان MAC لنقطة الوصول المخادعة
- اسم نقطة الوصول المخادع
- عنوان MAC الخاص بالعميل (العملاء) المتصل المخادع
- ما إذا كانت الإطارات محمية باستخدام WPA أو WEP

- الديباجة
- نسبة الإشارة إلى الضوضاء (SNR)
- مؤشر قوة إشارة المستقبل (RSSI)

نقطة وصول جهاز الكشف عن المخادع

يمكنك جعل نقطة الوصول تعمل كمكتشف مخادع، مما يسمح بوضعها على منفذ خط اتصال حتى يمكنها سماع جميع شبكات VLAN المتصلة بالجانب السلكي. ينتقل البحث عن العميل على الشبكة الفرعية السلكية على جميع شبكات VLAN. تستمع نقطة الوصول المخادعة إلى حزم بروتوكول تحليل العنوان (ARP) لتحديد عناوين الطبقة 2 للعملاء المخادعين أو نقاط الوصول المخادعة المحددة التي تم إرسالها بواسطة وحدة التحكم. إذا تم العثور على عنوان من الطبقة 2 مطابق، تقوم وحدة التحكم بإنشاء تنبيه يحدد نقطة الوصول أو العميل المخادع كتهديد. يشير هذا الإنذار إلى أن الوغد قد شوهد على الشبكة السلكية.

تحديد الفاسقين الفاعلين

يجب "مشاهدة" نقاط الوصول المخادعة مرتين قبل إضافتها كمخادع من قبل وحدة التحكم. لا تعتبر نقاط الوصول المخادعة تهديدا إذا لم تكن متصلة بالجزء السلكي من شبكة الشركة. ولتحديد ما إذا كان الوغد نشيطا، تستعمل أساليب متنوعة. وتشمل هذه النهج الإدارة الريفية.

بروتوكول اكتشاف المواقع الدخيلة (RLDP)

RLDP هو نهج نشط، والذي يتم إستخدامه عندما لا توجد نقطة وصول (AP) مخادعة مكونة لمصادقة (مصادقة مفتوحة). يرشد هذا الوضع، والذي يتم تعطيله بشكل افتراضي، نقطة وصول (AP) نشطة للانتقال إلى القناة المخادعة والاتصال بالمخالف كعميل. خلال هذا الوقت، ترسل نقطة الوصول النشطة رسائل إلغاء المصادقة إلى جميع العملاء المتصلين ثم تقوم بإيقاف تشغيل واجهة الراديو. بعد ذلك، سوف ترتبط بنقطة الوصول المخادعة كعميل.

ثم تحاول نقطة الوصول الحصول على عنوان IP من نقطة الوصول المخادعة وإعادة توجيه حزمة بروتوكول مخطط بيانات المستخدم (UDP) (المنفذ 6352) التي تحتوي على نقطة الوصول المحلية ومعلومات الاتصال المخادعة إلى وحدة التحكم من خلال نقطة الوصول المخادعة. إذا كانت وحدة التحكم تتلقى هذه الحزمة، فإنه يتم تعيين التنبيه لإعلام مسؤول الشبكة بأنه تم اكتشاف نقطة وصول مخادعة على الشبكة السلكية باستخدام ميزة RLDP.

ملاحظة: أستخدم الأمر **debug dot11 rldp enable** للتحقق من ما إذا كانت نقطة الوصول في الوضع Lightweight ترتبط باستلام عنوان DHCP من نقطة الوصول المخادعة. يعرض هذا الأمر أيضا حزمة UDP التي يتم إرسالها من قبل نقطة الوصول في الوضع Lightweight إلى وحدة التحكم.

يتم عرض عينة من حزمة UDP (المنفذ الوجهة 6352) التي يتم إرسالها بواسطة نقطة الوصول في الوضع Lightweight هنا:

```
0a 01 01 0d 0a 01 .......(.*..... 0030 01 1e 00 07 85 92 78 01 00 000000000 0020
......x......... 0040 000 0000000000000
```

تحتوي وحدات البايت الخمس الأولى من البيانات على عنوان DHCP المعطى لنقطة الوصول في الوضع المحلي بواسطة نقطة الوصول المخادعة. ال 5 بايت التالية هي عنوان IP لوحدة التحكم، متبوعة ب 6 بايت تمثل عنوان MAC لنقطة الوصول المخادعة. ثم هناك 18 بايت من الأصفار.

التشغيل السلبي:

يستخدم هذا الأسلوب عندما يكون لنقطة الوصول المخادعة شكل من أشكال المصادقة، إما WEP أو WPA. عندما يتم تكوين نموذج مصادقة على نقطة وصول (AP) مخادعة، لا يمكن لنقطة الوصول في الوضع Lightweight الاقتران لأنها لا تعرف المفتاح الذي تم تكوينه على نقطة الوصول المخادعة. تبدأ العملية بوحدة التحكم عند تمريرها على قائمة

عناوين MAC الخاصة بالعميل المخادع إلى نقطة وصول يتم تكوينها كمكتشف مخادع. يقوم المكتشف المخادع بفحص جميع الشبكات الفرعية المتصلة والمهيئة لطلبات ARP، ويبحث ARP عن عنوان طبقة 2 مطابق. إذا تم اكتشاف تطابق، يقوم وحدة التحكم بإخطار مسؤول الشبكة بأنه يتم اكتشاف وغد على الشبكة الفرعية السلكية.

إحتواء نشط للمارقين

بمجرد اكتشاف عميل مخادع على الشبكة السلكية، يمكن لمسؤول الشبكة إحتواء كل من نقاط الوصول المخادعة والعملاء المخادعين. ويمكن تحقيق ذلك لأن حزم إلغاء المصادقة 802.11 يتم إرسالها إلى العملاء المرتبطين بنقاط الوصول المارقة حتى يتم تخفيف التهديد الذي تحدثه مثل هذه الفتحة. في كل مرة يتم فيها محاولة إحتواء نقطة الوصول المخادعة، يتم إستخدام ما يقرب من 15٪ من مورد نقطة الوصول في الوضع Lightweight. لذلك، يقترح تحديد موقع نقطة الوصول المخادعة وإزالتها فعليا بمجرد احتواؤها.

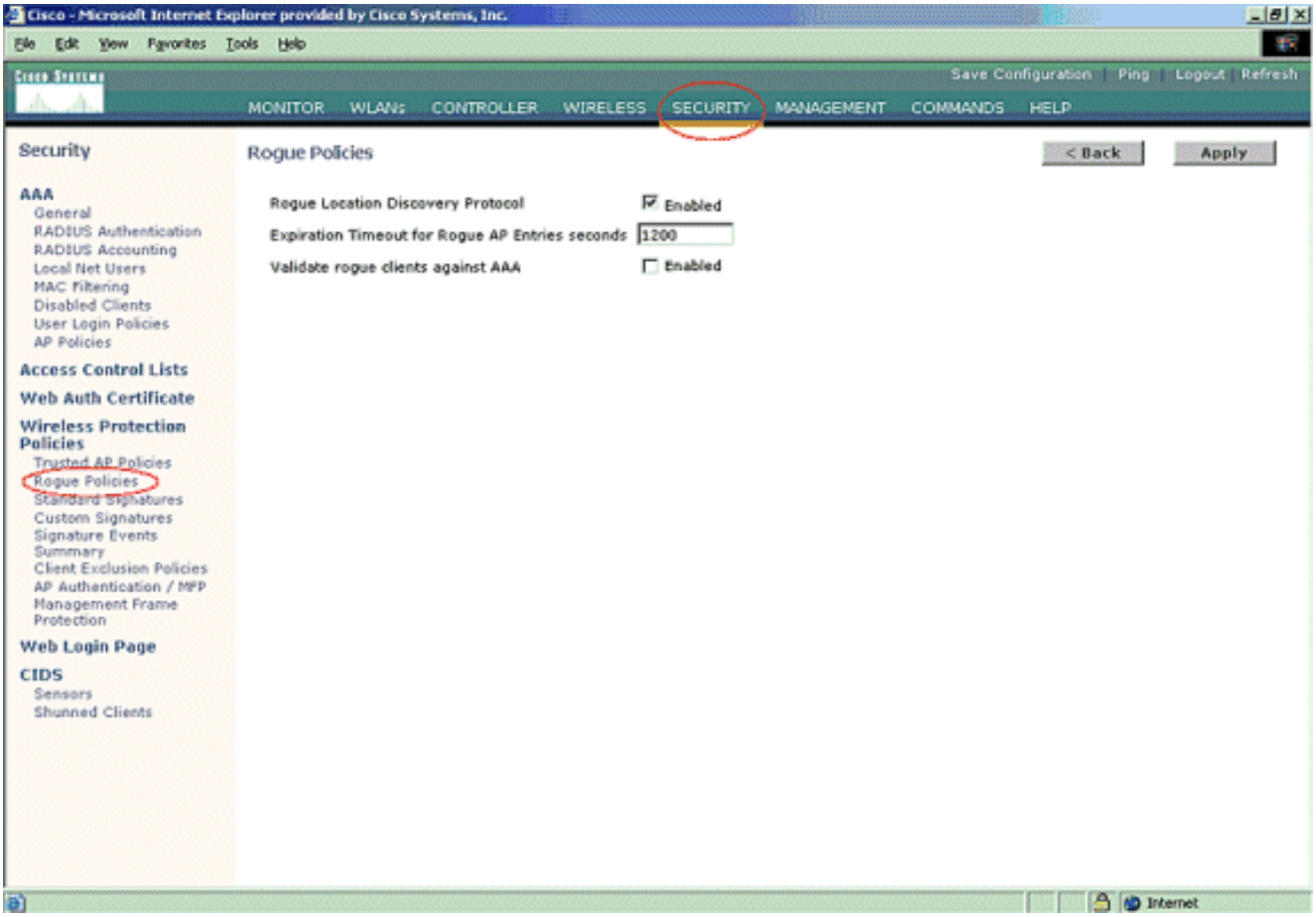
ملاحظة: من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الإصدار 5.2.157.0، بمجرد اكتشاف الموجه، يمكنك الآن إختيار إما أن تحتوي يدويا أو تلقائيا على الخداع الذي تم اكتشافه. في إصدارات برامج وحدات التحكم قبل 5.2.157.0، الاحتواء اليدوي هو الخيار الوحيد.

الكشف عن المخادع - خطوات التكوين

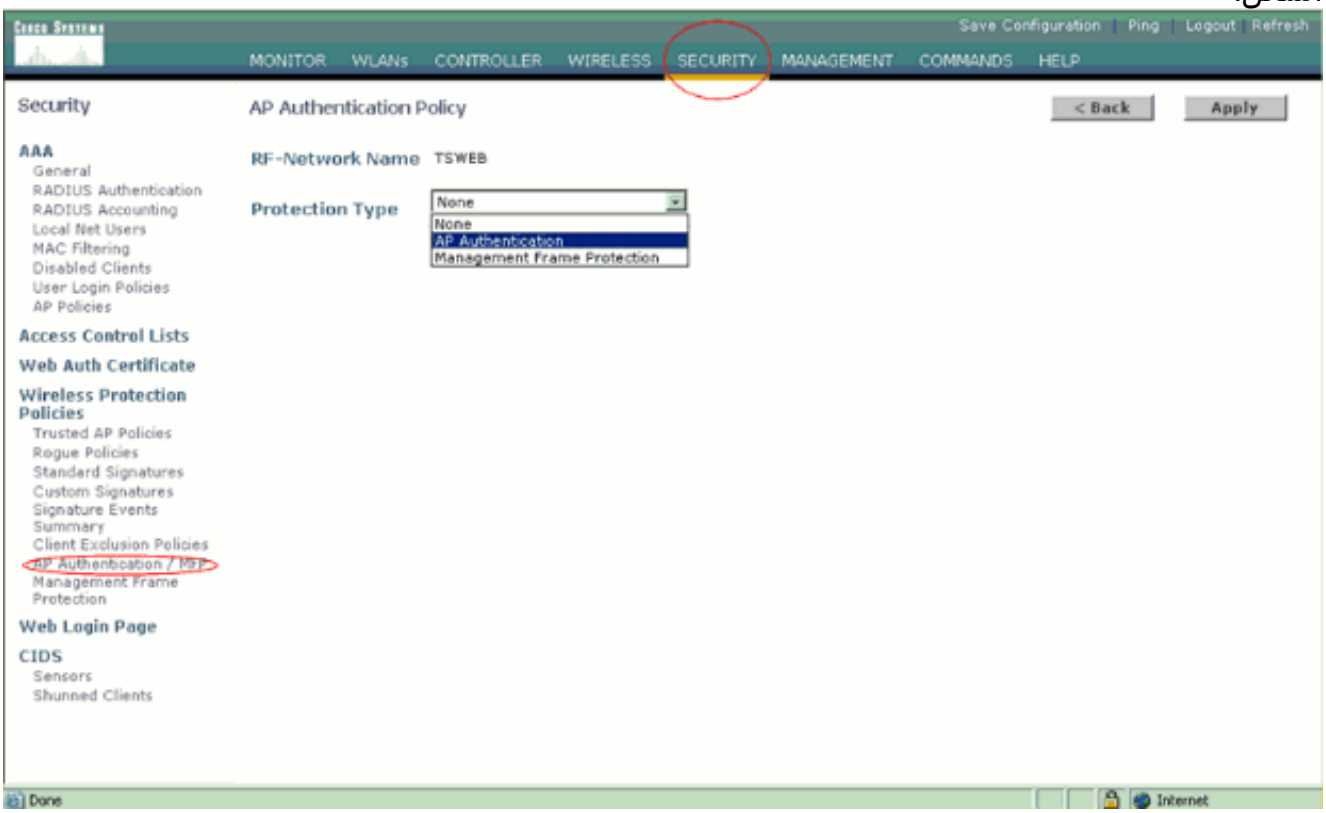
يتم تمكين تكوين الكشف عن المخادع بالكامل بشكل افتراضي للسماح بأكبر قدر ممكن من أمان الشبكة بمجرد إخراج الجهاز من عبوته. تفترض خطوات التكوين هذه أنه لم يتم إعداد كشف مارق على وحدة التحكم من أجل توضيح معلومات الكشف عن المخادعين المهمة.

من أجل إعداد الكشف عن المخادع، أكمل الخطوات التالية:

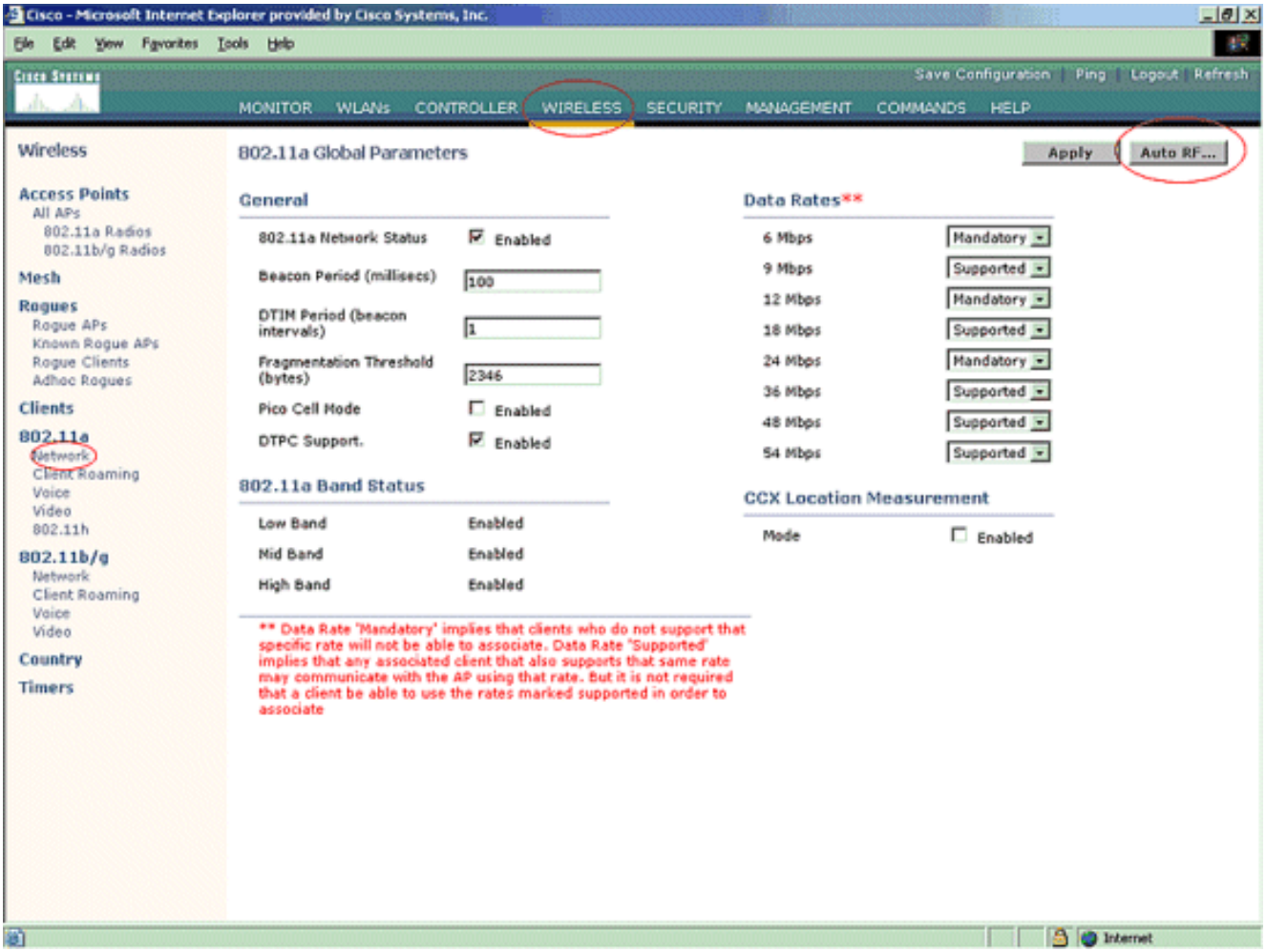
1. تأكد من تشغيل بروتوكول اكتشاف المواقع المخادعة. لتشغيله، أختر **الأمان > السياسات المخادعة** وانقر فوق **تمكين** في **بروتوكول اكتشاف الموقع المخادع** كما هو موضح في الشكل.**ملاحظة:** إذا لم يتم سماع نقطة وصول مخادعة لفترة زمنية معينة، تتم إزالتها من وحدة التحكم. هذه هي **مهلة انتهاء الصلاحية** لنقطة الوصول المخادعة، والتي تم تكوينها أسفل خيار RLDP.



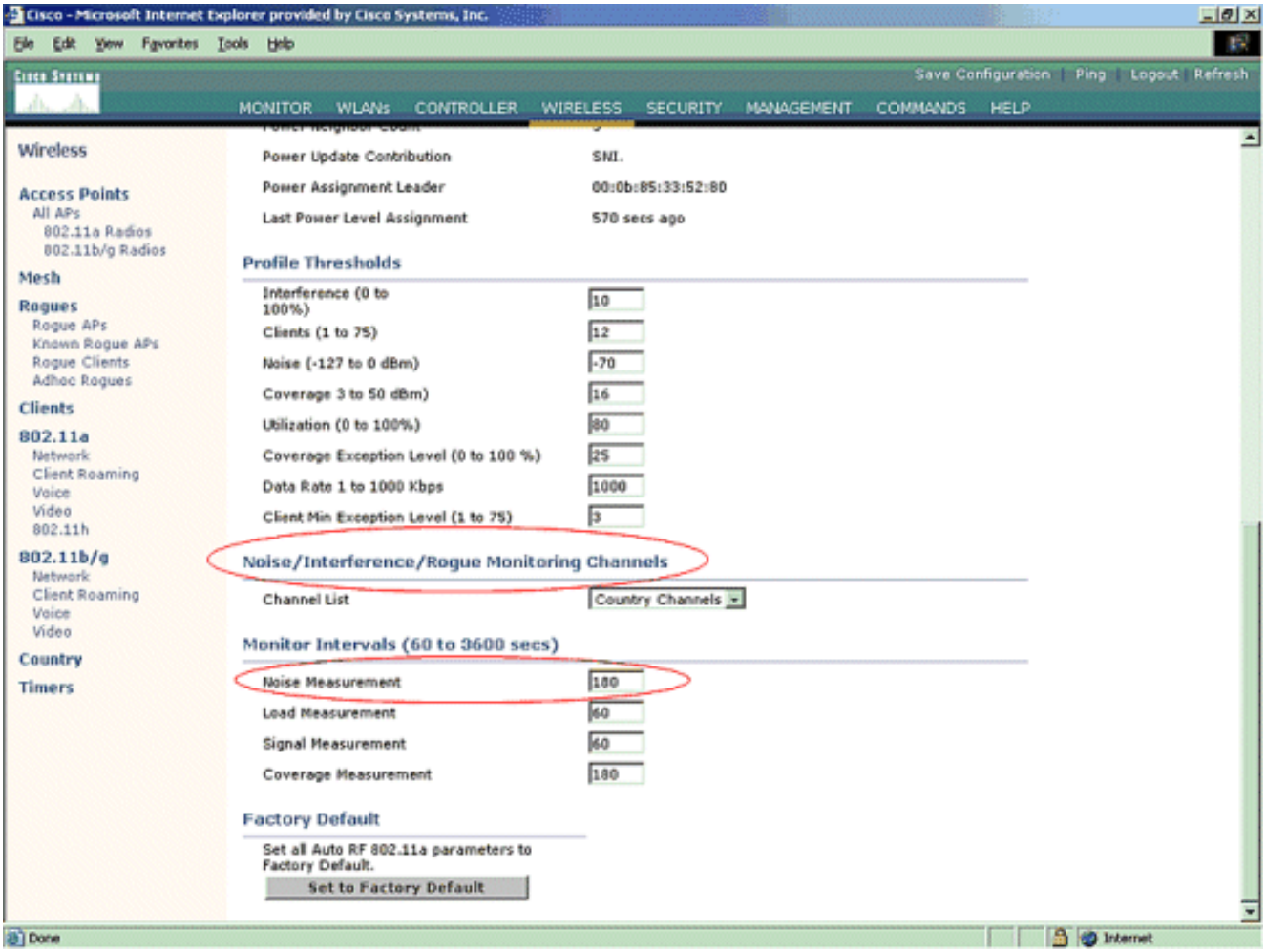
2. هذه خطوة إختيارية. عندما مكنت هذا سمة، ال APs يرسل RRM مجاور ربط مع مختلف **RF مجموعة** أسماء أبلغ عنه كخائن. وسيكون ذلك مفيدا في دراسة بيئة التردد اللاسلكي لديك. أخترت in order to مكنت هو، **أمن- > ap صحة هوية**. ثم أختر **مصادقة نقطة الوصول** كنوع حماية كما هو موضح في الشكل.



3. دققت القنوات أن يكون فحصت في هذا steps:حدد **لاسلكي > شبكة 802.11a**، ثم **تردد RF تلقائي** في الجانب الأيمن كما هو موضح في الشكل.



على صفحة **التردد اللاسلكي التلقائي**، قم بالتمرير إلى أسفل واختر **قنوات مراقبة التشويش/التداخل/المخادع**.



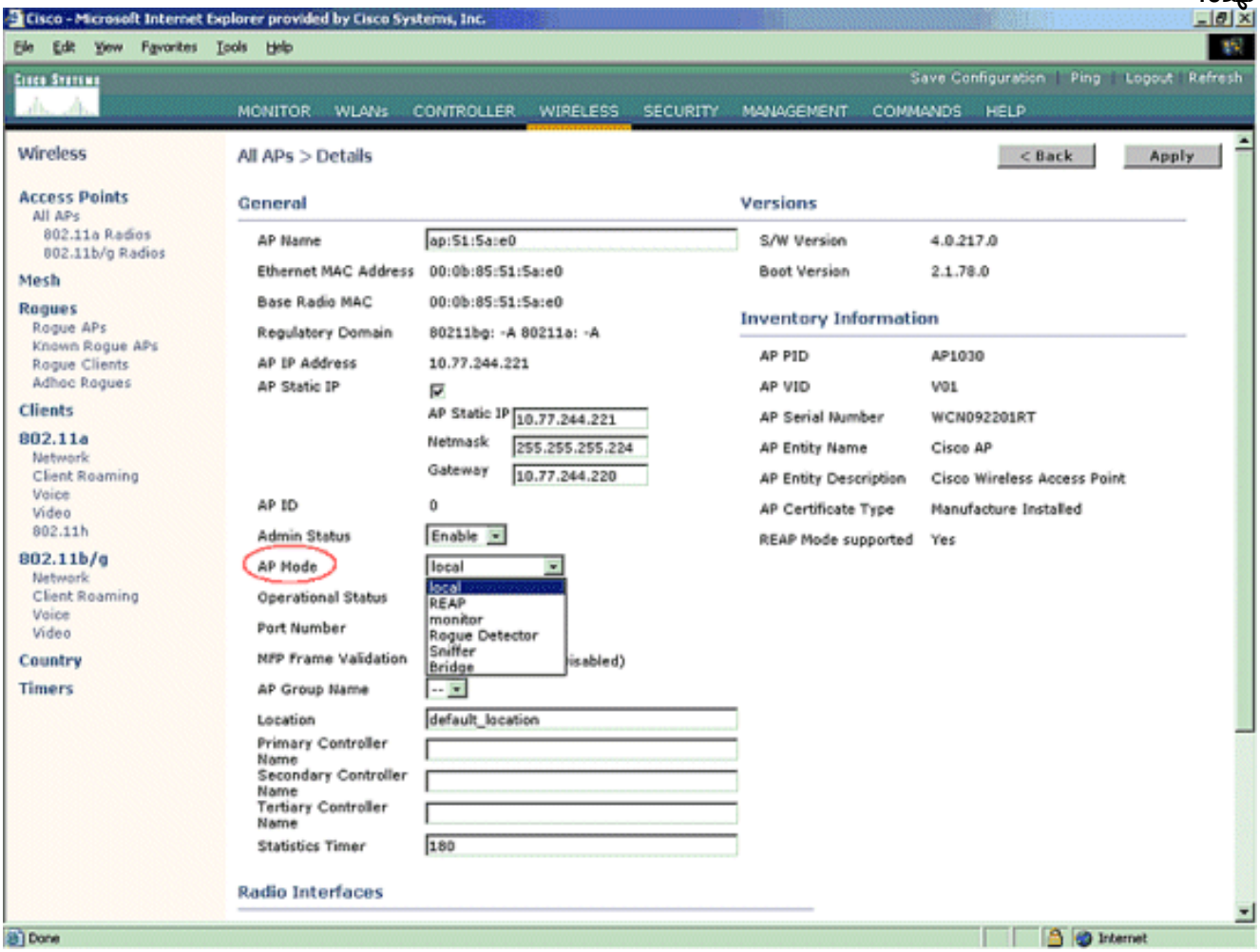
تعرض قائمة القنوات تفاصيل القنوات التي سيتم مسحها ضوئيا للمراقبة الدخيلة، بالإضافة إلى وظائف وحدات التحكم و AP الأخرى. ارجع إلى الأسئلة المتداولة حول نقطة الوصول في الوضع Lightweight للحصول على مزيد من المعلومات حول نقاط الوصول في الوضع Lightweight APs، وأستكشاف أخطاء وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) وإصلاحها للحصول على مزيد من المعلومات حول وحدات التحكم اللاسلكية.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. تعيين الفترة الزمنية لمسح القنوات المحددة:يتم تكوين مدة المسح الضوئي لمجموعة القنوات المحددة تحت **فواصل الشاشة > قياس التشويش**، والنطاق المسموح به هو من 60 إلى 3600 ثانية. إن ترك في التقصير من 180 ثاني، ال APs يمسح كل قناة في مجموعة القناة مرة واحدة، ل 50 ميللي ثانية، كل 180 ثانية. خلال هذه الفترة، يتغير راديو نقطة الوصول من قناة الخدمة الخاصة به إلى القناة المحددة، ويقوم بالاستماع إلى قيم السجلات لمدة 50 ملي ثانية، ثم يعود إلى القناة الأصلية. فوقت القفزة بالإضافة إلى وقت الخمول الذي يبلغ 50 ملي ثانية يؤدي إلى خروج نقطة الوصول عن القناة لمدة 60 ملي ثانية تقريبا في كل مرة. وهذا يعني أن كل نقطة وصول تنفق حوالي 840 ملي ثانية من إجمالي 180 ثانية في الاستماع للوسطاء الفاسدين.لا يمكن تعديل وقت "الاستماع" أو "الإقامة" ولا يتم تغييره مع تعديل قيمة قياس الضوضاء. إذا تم خفض مؤقت قياس الضوضاء، فإن عملية اكتشاف العثرات من المحتمل أن تجد المزيد من العثرات وأن تجدها بسرعة أكبر. ومع

ذلك، فإن هذا التحسن يأتي على حساب تكامل البيانات وخدمة العملاء. ومن ناحية أخرى، تسمح القيمة الأعلى بسلامة أفضل للبيانات ولكنها تقلل من القدرة على العثور على المخادعين بسرعة.

5. قم بتكوين وضع نقطة الوصول للعملية:يحدد وضع نقطة وصول في الوضع Lightweight دور نقطة الوصول. الأوضاع المتعلقة بالمعلومات المقدمة في هذا المستند هي:**محلي**— هذا هو التشغيل الطبيعي ل AP. يتيح هذا الوضع خدمة عملاء البيانات أثناء فحص القنوات التي تم تكوينها بحثا عن الضوضاء والأخطاء. في هذا الوضع من التشغيل، تنتقل نقطة الوصول خارج القناة ل 50 مللي ثانية وتستمع إلى المخادعين. هو يمر خلال كل قناة، واحد في كل مرة، للفترة المحددة تحت تشكيل آلي للتردد اللاسلكي.**مدرب**— هذا هو وضع إستقبال الراديو فقط، ويسمح لنقطة الوصول بمسح كل القنوات التي تم تكوينها كل 12 ثانية. لا ترسل إلا حزم إلغاء المصادقة في الهواء مع نقطة وصول مكونة بهذه الطريقة. يمكن لنقطة الوصول في وضع المراقبة اكتشاف المخادعين، ولكنها لا يمكنها الاتصال بخادع مشتبه به كعميل لإرسال حزم RLDP.**ملاحظة:** يشير DCA إلى القنوات غير المتداخلة القابلة للتكوين باستخدام الأوضاع الافتراضية.**الكاشف المخادع** — في هذا الوضع، يتم إيقاف راديو AP، وتستمع نقطة الوصول إلى حركة المرور السلكية فقط. يمرر جهاز التحكم نقاط الوصول التي تم تكوينها كأجهزة كشف مخادعة بالإضافة إلى قوائم بالعملاء المخادعين المشتبه فيهم وعناوين AP MAC. يقوم المكتشف المخادع بالاستماع إلى حزم ARP فقط، ويمكن توصيله بجميع مجالات البث من خلال إرتباط خط اتصال إذا كان ذلك مطلوبا.يمكنك تكوين وضع نقطة وصول فردي ببساطة، بمجرد توصيل نقطة الوصول في الوضع Lightweight بوحدة التحكم. لتغيير وضع نقطة الوصول، اتصل بواجهة الويب لوحدة التحكم وانتقل إلى **لاسلكي**. انقر على **التفاصيل** المجاورة لنقطة الوصول المرغوبة لعرض شاشة مماثلة لهذه:



أستخدم القائمة المنسدلة لوضع AP لتحديد وضع AP المطلوب للعملية.

أوامر استكشاف الأخطاء وإصلاحها

أنت يستطيع أيضا استعملت هذا أمر in order to تحريت تشكيلك على ال AP:

- **إظهار ملخص نقطة الوصول المخادعة**— يعرض هذا الأمر قائمة نقاط الوصول المخادعة التي تم اكتشافها بواسطة نقاط الوصول في الوضع Lightweight.
- **إظهار نقطة الوصول المخادعة بالتفصيل *<عنوان MAC لنقطة الوصول المخادعة>*** — أستخدم هذا الأمر لعرض تفاصيل حول نقطة وصول (AP) مخادعة فردية. هذا هو الأمر الذي يساعد على تحديد ما إذا كانت نقطة الوصول المخادعة متصلة بالشبكة السلكية.

القرار

يعد اكتشاف الأجهزة المخادعة واحتوائها داخل حل وحدات التحكم المركزية من Cisco الطريقة الأكثر فعالية والأقل تدخلا في هذه الصناعة. تتيح المرونة المتوفرة لمسؤول الشبكة إمكانية توفير ملائمة أكثر تخصيصا يمكنها إستيعاب أي متطلبات للشبكة.

معلومات ذات صلة

- نظرة عامة على مجموعات التردد اللاسلكي
- 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).