# دليل نشر الشبكة المعشقة في الأماكن المغلقة

## المحتويات

## المقدمة

نقطة الوصول Lightweight 1242/1131 هي جهاز بنية أساسية Wi-Fi مزدوج اللاسلكية يستخدم لعمليات النشر الداخلية المحددة. إنه منتج قائم على بروتوكول نقطة الوصول في الوضع Lightweight (LWAPP). وهو يوفر راديو 2. 4 جيجاهيرتز وراديو 5. 8 جيجاهيرتز متوافقين مع 802. 11b/g و 802. 11a. يمكن إستخدام أحد أجهزة الراديو للوصول المحلي (العميل) لنقطة الوصول (AP) ويمكن تكوين جهاز الراديو الثاني لنقل البيانات اللاسلكية. يدعم LAP1242/LAP1131 P2P و P2MP ونوع الشبكات من البنى.

تأكد من القراءة من خلال الدليل قبل محاولة أي من التثبيتات.

يصف هذا المستند نشر الشبكة اللاسلكية للمؤسسة للشبكة الداخلية. هذا المستند سيمكن المستخدمين النهائيين اللاسلكيين من فهم أساسيات الشبكة الداخلية وأماكن تكوين الشبكة الداخلية وكيفية تكوين الشبكة الداخلية. الشبكة الداخلية هي مجموعة فرعية من شبكة Cisco Enterprise اللاسلكية يتم نشرها باستخدام وحدات التحكم اللاسلكية ونقاط الوصول في الوضع Lightweight.

الشبكة الداخلية هي مجموعة فرعية من بنية شبكة المؤسسة يتم نشرها على البنية اللاسلكية الموحدة. الشبكة المغلقة مطلوبة اليوم. باستخدام شبكة داخلية، يتم إستخدام أحد أجهزة الراديو (عادة 802.11b/g) و/أو إرتباط إيثرنت السلكي للاتصال بالعملاء، بينما يتم إستخدام جهاز الراديو الثاني (عادة 802.11a) لنقل حركة مرور العملاء. قد تكون حركة الشبكة خطوة واحدة أو عبر نقلات متعددة. الشبكة الداخلية تجلب لك هذه القيم:

- عدم الاضطرار إلى تشغيل أسلاك إيثرنت لكل نقطة وصول.
- منفذ محول إيثرنت غير مطلوب لكل نقطة وصول.
- اتصال الشبكة حيث يتعذر على الأسلاك توفير الاتصال.
- المرونة في النشر - لا تقتصر على 100 متر من محول إيثرنت.
- سهولة نشر شبكة لاسلكية أقران.

ينجذب تجار التجزئة في الصناديق الكبيرة إلى الشبكات الداخلية نظرا لوفر التكاليف على الأسلاك وكذلك للأسباب المذكورة آنفا.

ويستخدمه الاختصاصيون في الجرد عند إجراء عمليات الجرد لتجار التجزئة، مصانع التصنيع، وشركات أخرى. فهم يريدون نشر شبكة Wi-Fi مؤقتة بسرعة في موقع أحد العملاء لتمكين الاتصال في الوقت الفعلي بأجهزتهم المحمولة. الندوات التعليمية، المؤتمرات، التصنيع، والضيافة هي بعض الاماكن حيث تلزم الهندسة المعمارية داخل المباني.

عندما تنتهي من قراءة هذا الدليل، ستفهم أين تستخدمه وكيف يمكنك تكوين الشبكة الداخلية. ستفهم أيضا أن الشبكة الداخلية في حاويات NEMA ليست بديلا للشبكة الخارجية. علاوة على ذلك، ستفهم أيضا تفوق الشبكة الداخلية على مرونة دور الارتباط (شبكة الخطوة الواحدة) التي تستخدمها نقاط الوصول (APs) المستقلة.

**الافتراضات:**

لديك معرفة بشبكة Cisco اللاسلكية الموحدة وبنائها وبنيتها. لديك معرفة بمنتجات الشبكات الخارجية من Cisco وبعض المصطلحات المستخدمة لشبكات الشبكة العنكبوتية.

| مسرد المختصرات | |
|---|---|
| LWAPP | بروتوكول نقطة الوصول في الوضع Lightweight - بروتوكول التحكم ونفق البيانات بين نقاط |

| | |
|---|---|
| | الوصول ووحدة التحكم في الشبكة المحلية اللاسلكية. |
| وحدة التحكم /وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) | وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية - أجهزة Cisco التي تعمل على تمركز إدارة الشبكة لشبكة محلية لاسلكية (WLAN) وتبسيطها عن طريق تقليص عدد كبير من نقاط النهاية المدارة إلى نظام واحد موحد، مما يسمح بنظام شبكة WLAN موحد للمعلومات الذكية. |
| راب | نقطة الوصول الجذر/ نقطة الوصول إلى السقف - تعمل أجهزة Cisco اللاسلكية كجسر بين وحدة التحكم ونقاط الوصول اللاسلكية الأخرى. نقاط الوصول (AP) المتصلة بوحدة التحكم. |
| خريطة | نقاط الوصول للشبكة العنكبوتية - جهاز لاسلكي من Cisco يتصل ببروتوكول RAP أو خريطة عبر الهواء على راديو 802.11a ويقدم أيضا الخدمات للعملاء على راديو 802.11b/g. |
| والد | نقطة وصول (إما عبر بروتوكول RAP/MAP) توفر الوصول إلى نقاط وصول (AP) أخرى عبر الهواء على راديو 802. 11a. |
| جار | جميع نقاط الوصول في شبكة شبكة شبكة متداخلة ولها جيران. لا يوجد جار ل RAP كما هو متصل بوحدة التحكم. |
| طفل | دائما ما تكون نقطة الوصول البعيدة عن وحدة التحكم تابعة. سيكون للطفل والد واحد والعديد من الجيران في شبكة عنكبوتية. إذا توفي الوالد، سيتم إختيار الجار التالي الذي لديه أفضل قيمة سهلة. |
| SNR | نسبة الإشارة إلى الضجيج |
| BGN | اسم مجموعة الجسر |
| EAP | بروتوكول المصادقة المتوسع |
| PSK | المفتاح المشترك مسبقا |
| AWPP | بروتوكول المسار اللاسلكي القابل للتكيف |

## نظرة عامة

نقطة وصول شبكة الاتصال المعشقة الداخلية من Cisco هي جهاز بنية Wi-Fi أساسي مزدوج اللاسلكية لعمليات النشر الداخلية المحددة. إنه منتج قائم على بروتوكول نقطة الوصول في الوضع Lightweight (LWAPP). وهو يوفر

راديو 2. 4 جيجاهيرتز وراديو 5. 8 جيجاهيرتز متوافقين مع معايير 802. 11a ،802. 11b/g. يمكن إستخدام أحد أجهزة الراديو (802.11b/g) للوصول المحلي (العميل) لنقطة الوصول (AP) ويمكن تكوين جهاز الراديو الثاني (802.11a) لنقل البيانات لاسلكيا. فهي توفر بنية شبكة داخلية، حيث تتحدث العقد المختلفة (الأجهزة اللاسلكية) مع بعضها البعض من خلال نقل حركة الشبكة، فضلا عن أنها توفر إمكانية وصول العملاء المحليين. كما يمكن إستخدام نقطة الوصول هذه لبنى التوصيل من نقطة إلى نقطة ومن نقطة إلى عدة نقاط. يعتبر حل الشبكة اللاسلكية الداخلية المعشقة حلا مثاليا للتغطية الداخلية الكبيرة حيث يمكنك الحصول على معدلات بيانات عالية وموثوقية جيدة مع الحد الأدنى من البنية الأساسية. هذه هي الميزات الأساسية البارزة التي تم تقديمها مع الإصدار الأول من هذا المنتج:

- يستخدم في بيئة داخلية لعدد 3 نقلات. الحد الأقصى 4.
- عقدة ترحيل ومضيف لعملاء المستخدم النهائي. يستخدم راديو 802.11a كواجهة نقل حركة مرور واستقبال 802.11b/g لخدمة العملاء.
- أمان نقاط الوصول داخل الشبكة - دعم EAP و PSK.
- تتصل خرائط LWAPP في بيئة شبكة مع وحدات التحكم بنفس الطريقة مقارنة بنقاط الوصول المتصلة بشبكة إيثرنت.
- الربط اللاسلكي من نقطة إلى نقطة.
- الربط اللاسلكي من نقطة إلى عدة نقاط.
- تحديد أصلي مثالي. SNR و Easy و BGN
- تحسينات BGN. الوضع الافتراضي والخالي.
- الوصول المحلي.
- القائمة السوداء الأصل. قائمة الاستبعاد.
- الشفاء الذاتي من خلال AWPP.
- الربط بين إيثرنت.
- دعم أساسي للصوت من نسخة 4. 0.
- تحديد التردد الديناميكي.
- مكافحة الغرابة - تجاوز فشل BGN و DHCP الافتراضيين.

**ملاحظة:** لن يتم دعم هذه الميزات:

- قناة السلامة العامة 4.9 جيجاهيرتز
- التوجيه حول التداخل
- مسح الخلفية
- وصول عالمي
- دعم جسر مجموعة العمل

**برمجيات شبكة داخلية**

يعتبر برنامج الشبكة المعشقة في الأماكن المغلقة إصدارا خاصا نظرا لتركيزه على نقاط الوصول (AP) الداخلية، وخاصة الشبكة الداخلية. في هذا الإصدار، لدينا كل من نقاط الوصول (AP) الداخلية التي تعمل في الوضع المحلي وأيضا في وضع الجسر. لم يتم تنفيذ بعض الميزات المتوفرة في الإصدار 4.1.171.0 في هذا الإصدار. تم إجراء تحسينات على واجهة سطر الأوامر (CLI) وواجهة المستخدم الرسومية (GUI - مستعرض الويب) وعلى جهاز الحالة نفسه. إن الهدف من هذه التحسينات هو الحصول على معلومات قيمة من وجهة نظرك فيما يتعلق بهذا المنتج الجديد وبقدرته على البقاء من الناحية الوظيفية.

تحسينات محددة للشبكة العنكبوتية الداخلية:

- **البيئة الداخلية** - يتم تنفيذ الشبكة الداخلية باستخدام LAP1242s و LAP1131. ويتم تنفيذ ذلك في البيئات الداخلية حيث لا يتوفر كبل الإيثرنت. ويجري التنفيذ بسهولة وسرعة لتوفير تغطية لاسلكية للمناطق النائية داخل المبنى (على سبيل المثال، مراكز توزيع البيع بالتجزئة، والتعليم للندوات/المؤتمرات، والتصنيع، والضيافة).
- **تحسينات اسم مجموعة الجسر (BGN)** - للسماح لمسؤول الشبكة بتنظيم شبكة من نقاط الوصول (APs) إلى قطاعات محددة من قبل المستخدم، توفر Cisco آلية تسمى اسم مجموعة الجسر، أو BGN. يتسبب BGN، وهو بالفعل اسم القطاع، في أن تتصل نقطة وصول بنقاط وصول أخرى بنفس BGN. في حالة عدم العثور على أي

قطاع مناسب يطابق BGN الخاص بها، تعمل نقطة الوصول في الوضع الافتراضي، وتختار أفضل والد يستجيب ل BGN الافتراضي. وقد تلقت هذه الميزة بالفعل الكثير من التقدير من الحقل حيث إنها تحارب شروط نقطة الوصول (إذا قام شخص ما بتكوين BGN بشكل غير صحيح). في إصدار البرنامج 4.1.171.0، لا تعمل نقاط الوصول (APs)، عند إستخدام شبكة BGN الافتراضية، كعقدة شبكة داخلية ولا تتوفر على أي وصول إلى العميل. وهو في وضع الصيانة للوصول عبر وحدة التحكم، وإذا لم يقم المسؤول بإصلاح شبكة BGN، فستقوم نقطة الوصول بإعادة التمهيد بعد 30 دقيقة.

- **تحسينات الأمان** - يتم تكوين أمان رمز الشبكة الداخلية بشكل افتراضي ل EAP (بروتوكول المصادقة المتوسع). ويتم تحديد هذا في RFC3748. وعلى الرغم من أن بروتوكول EAP لا يقتصر على الشبكات المحلية اللاسلكية ويمكن إستخدامه لمصادقة الشبكة المحلية السلكية، إلا أنه غالبا ما يستخدم في الشبكات المحلية اللاسلكية. عندما يتم إستدعاء EAP بواسطة جهاز NAS (خادم الوصول إلى الشبكة) تم تمكين 802.1X مثل نقطة الوصول اللاسلكية 802.11 a/b/g، فإن طرق EAP الحديثة يمكن أن توفر آلية مصادقة آمنة وتتفاوض على مفتاح PMK آمن (مفتاح رئيسي مزدوج الحكمة) بين العميل و NAS. ويمكن بعد ذلك إستخدام PMK لجلسة عمل التشفير اللاسلكي التي تستخدم تشفير TKIP أو CCMP (استنادا إلى تشفير AES).قبل إصدار برنامج 4.1.171.0، أستخدمت نقاط الوصول من الشبكة الخارجية PMK/BMK للانضمام إلى وحدة التحكم. كانت هذه عملية ثلاثية الدورات. الآن تقلصت الدورات للحصول على تقارب أسرع.إن الهدف العام من الأمن الشبكي الداخلي هو توفير:تكوين دون لمس لتوفير الأمان.الخصوصية والمصادقة لإطارات البيانات.مصادقة متبادلة بين الشبكة والعقد.القدرة على إستخدام طرق EAP القياسية لمصادقة عقد AP للشبكة المعشقة الداخلية.فصل LWAPP وأمان الشبكة الداخلية.يتم تحسين آليات الاكتشاف والتوجيه والمزامنة من البنية الحالية لاستيعاب العناصر المطلوبة لدعم بروتوكولات الأمان الجديدة.تكتشف نقاط الوصول الخاصة بالشبكات الداخلية نقاط وصول أخرى للشبكات عن طريق المسح الضوئي والاستماع إلى التحديثات المجاورة المجانية من نقاط الوصول الخاصة بالشبكات الأخرى. تعلن أي من خرائط RAP أو MAPs الداخلية المتصلة بالشبكة عن معلمات الأمان الأساسية في إطارات NEIGH_UPD الخاصة بها (والتي تشبه كثيرا إطارات الإرشاد عبر شبكة 802.11).وبمجرد انتهاء هذه المرحلة، يتم إنشاء إرتباط منطقي بين نقطة الوصول الخاصة بشبكة داخلية ونقطة الوصول (AP) الجذرية.
- **تحسينات WCS**تمت إضافة تنبيهات الشبكة داخل المباني.يمكن إنشاء تقارير شبكة داخلية تظهر عدد الخطوات وأسوأ SNR، وما إلى ذلك.يمكن تشغيل إختبار الارتباط (من الأصل إلى الطفل ومن الطفل إلى الأصل) بين العقد التي تظهر معلومات ذكية للغاية.معلومات نقطة الوصول المعروضة أكبر بكثير من المعلومات السابقة.فالمرء لديه خيار أيضا أن ينظر إلى الجيران المحتملين.كما تم تحسين المراقبة الصحية والوصول إليها بشكل أكثر سهولة.

## الأجهزة والبرامج المدعومة

يوجد حد أدنى من متطلبات المعدات والبرامج للشبكة المعشقة في الأماكن المغلقة:

- تدعم نقاط الوصول من Cisco LWAPP AIR-LAP1242AG-A-K9 و AIR-LAP1131AG-A-K9 تكوين الشبكة الداخلية.
- يدعم برنامج Cisco Mesh الإصدار 2 شبكة Enterprise (منتجات داخلية وخارجية). يمكن تثبيت هذا على وحدة التحكم من Cisco، و Cisco 440x/210x، و WISMs فقط.
- يمكن تنزيل برنامج Cisco Enterprise Mesh الإصدار 2 من Cisco.com.

## الداخل مقابل الخارج

هذه بعض الفروق البارزة بين الشبكة الداخلية والخارجية:

| | **شبكة داخلية** | **شبكة عنكبوتية خارجية** |
|---|---|---|
| البيئة | تم تصنيف الأجهزة داخل المنزل فقط | في المناطق الخارجية فقط، |

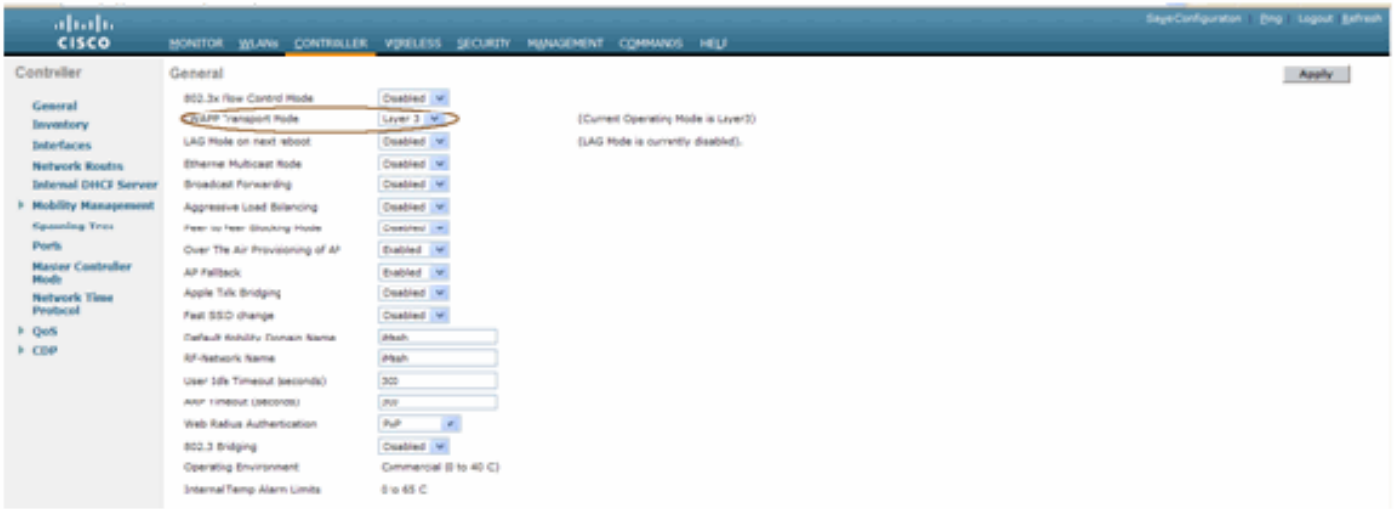
| | | |
|---|---|---|
| | | أجهزة فائقة القوة |
| الأجهزة | نقطة وصول داخلية باستخدام LAP1242 و LAP1131AG | نقطة وصول خارجية باستخدام LAP15xx و LAP152x |
| مستويات الطاقة | 2.4 جيجاهرتز:20 ديسيبل لكل ميللي وات بسرعة 5.8 جيجاهرتز:17 ديسيبل لكل ميللي وات | 2.4 جيجاهرتز:28 ديسيبل لكل ميللي وات بسرعة 5.8 جيجاهرتز:28 ديسيبل لكل ميللي وات |
| أحجام الخلايا | تقريبا 150 قدما | تقريبا 1000 قدم |
| إرتفاع التنفيذ | على بعد 12 قدما من الأرض | 30-40 قدما من الأرض |

## التكوين

تأكد من مراجعة الدليل بدقة قبل بدء أي تنفيذ، خاصة إذا كنت قد تلقيت أجهزة جديدة.

### وضع وحدة التحكم L3

يمكن نشر نقاط الوصول من الشبكة الداخلية كشبكة L3.



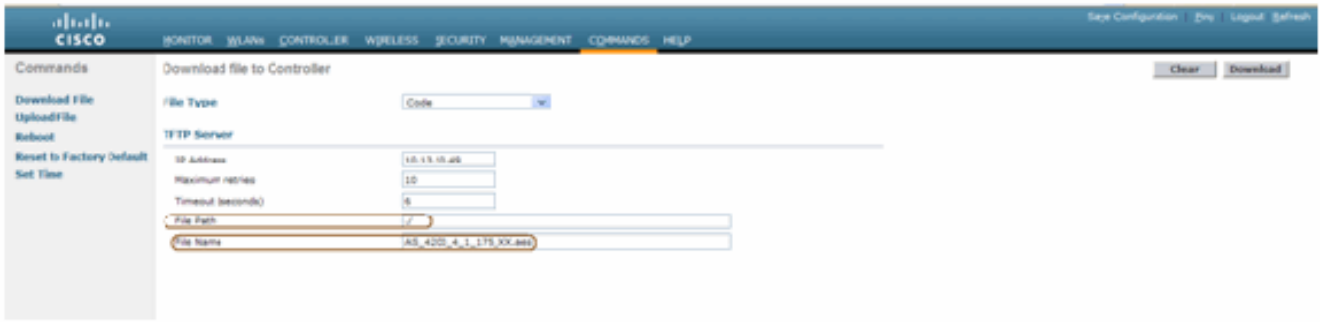

### ترقية وحدة التحكم إلى أحدث رمز

أكمل الخطوات التالية:

1. لترقية الإصدار 2 من الشبكة العنكبوتية على شبكة شبكة داخلية، يجب أن تكون شبكتك تعمل على الإصدار 4.1.185.0 أو إصدار الشبكة 1، متاح على Cisco.com.
2. قم بتنزيل أحدث رمز لوحدة التحكم إلى خادم TFTP. من واجهة واجهة المستخدم الرسومية (GUI) الخاصة

بوحدة التحكم، انقر فوق **الأوامر** > **تنزيل الملف**.

3. حدد نوع الملف **كرمز** وأعط عنوان IP لخادم TFTP الخاص بك. قم بتعريف المسار واسم الملف.




**ملاحظة:** أستخدم خادم TFTP الذي يدعم عمليات نقل حجم الملفات التي تزيد عن 32 ميجابايت. على سبيل المثال، **tftpd32**. تحت مسار الملف، ضع **"/"** كما هو موضح.

4. عند الانتهاء من تثبيت البرنامج الثابت الجديد، أستخدم الأمر **show sysinfo** في واجهة سطر الأوامر (CLI) للتحقق من تثبيت البرنامج الثابت الجديد.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

**ملاحظة:** رسميا، لا تدعم Cisco الخفض لوحدات التحكم.

## عنوان MAC

هو إلزامي أن يستعمل ماك ييصفي. لقد صنعت هذه الميزة حل شبكة Cisco الداخلية ك "Zero Touch" حقيقي. بخلاف الإصدارات السابقة، لن يكون لشاشة الشبكة خيار تصفية MAC بعد الآن.


**ملاحظة:** يتم تمكين تصفية MAC بشكل افتراضي.

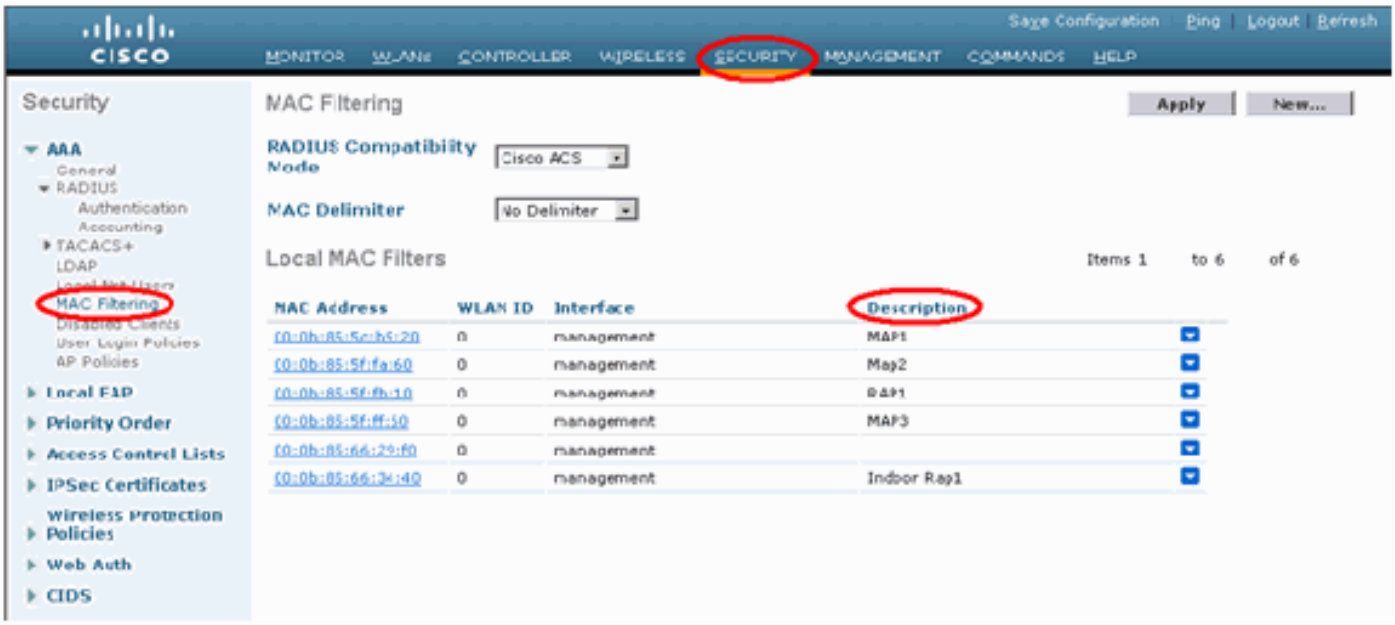
## تسجيل عنوان MAC إلى أجهزة الراديو

في ملف نصي، قم بتسجيل عناوين MAC الخاصة بكل أجهزة الراديو AP الخاصة بالشبكة الداخلية التي تقوم بنشرها في شبكتك. يمكن العثور على عنوان MAC في الجزء الخلفي من نقاط الوصول. هذا يساعدك على الاختبار في المستقبل، بما أن معظم أوامر CLI تتطلب إدخال عنوان MAC لنقاط الوصول أو الأسماء مع الأمر. يمكنك أيضا تغيير اسم نقاط الوصول إلى شيء يسهل تذكره، مثل، "بناء رقم-pod رقم-ap نوع: آخر أربعة حروف سداسية عشرية لعنوان MAC".

## أدخل عنوان MAC وأسماء أجهزة الراديو في وحدة التحكم

تحتفظ وحدة التحكم في Cisco بقائمة عناوين MAC للتخويل الخاص بنقطة الوصول (AP) الداخلية. تستجيب وحدة التحكم فقط لطلبات الاكتشاف الواردة من أجهزة الراديو الداخلية التي تظهر في قائمة التخويل. أدخل عناوين MAC لجميع أجهزة الراديو التي تميل إلى إستخدامها في الشبكة على وحدة التحكم.

على واجهة واجهة المستخدم الرسومية (GUI) لوحدة التحكم، انتقل إلى **الأمان**، وانقر على **تصفية MAC** على الجانب الأيسر من الشاشة. طقطقت **جديد** in order to دخلت ماك عنوان كما هو موضح هنا:




أدخل أيضا أسماء أجهزة الإرسال اللاسلكي لتسهيل الاستخدام بموجب **الوصف** (مثل الموقع، AP #، وما إلى ذلك). يمكن إستخدام الوصف أيضا في حالة تثبيت أجهزة الراديو للرجوع إليها بسهولة في أي وقت.

## تمكين تصفية MAC

تصفية MAC ممكنة بشكل افتراضي.

كما يمكن إختيار وضع التأمين مثل EAP أو PSK في نفس الصفحة.

من ال gui قارن من المفتاح، استعملت هذا ممر:

مسار واجهة المستخدم الرسومية: **لاسلكي > شبكة داخلية**

لا يمكن التحقق من وضع الأمان إلا في CLI بواسطة هذا الأمر:

```
Cisco Controller) > show network)
```

```
(Cisco Controller) >show network

RF-Network Name.............................. iMesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Ucast
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk .................................. Disable
AP Fallback ................................. Enable
--More-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

## نشر الشبكة العنكبوتية الداخلية من المستوى الثالث

بالنسبة لشبكة شبكة L3 داخلية، قم بتكوين عناوين IP لأجهزة الراديو إذا لم ترغب في إستخدام خادم DHCP (داخلي أو خارجي).

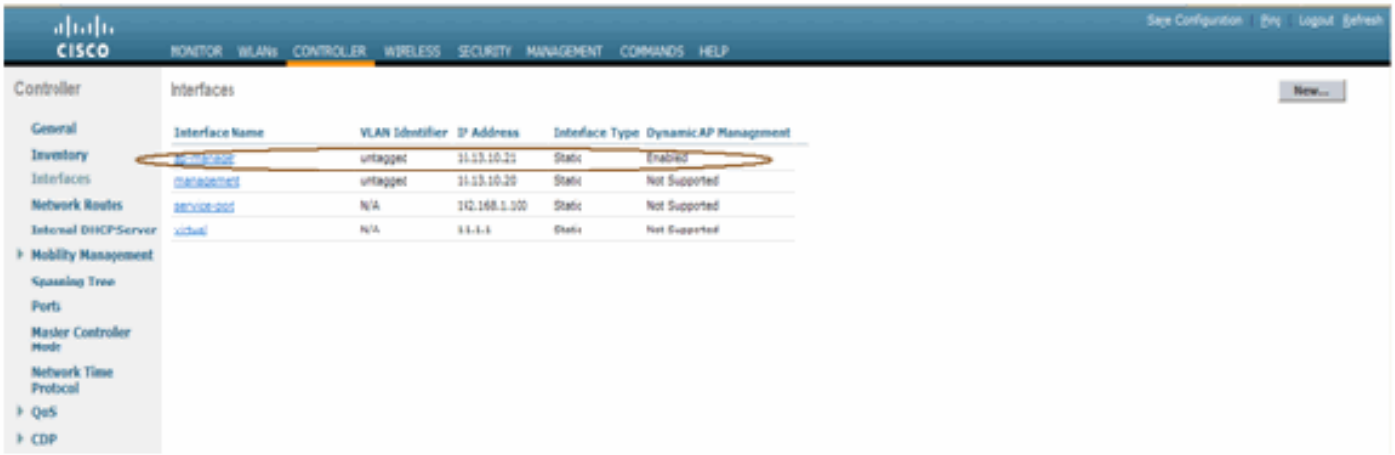
لشبكة شبكة L3 داخلية، إذا كنت تريد إستخدام خادم DHCP، قم بتكوين وحدة التحكم في وضع L3. قم بحفظ التكوين وإعادة تمهيد وحدة التحكم. تأكد من تكوين الخيار 43 على خادم DHCP. بعد إعادة تشغيل وحدة التحكم، ستتلقى نقاط الوصول المتصلة حديثا عنوان IP الخاص بها من خادم DHCP.

## تحديد الواجهات على وحدة التحكم

### مدير AP

بالنسبة لنشر من المستوى الثالث، يجب عليك تحديد **مدير نقطة الوصول**. يعمل مدير AP كعنوان IP للمصدر للاتصال من وحدة التحكم إلى نقاط الوصول.

المسار: **وحدة التحكم > الواجهات>AP-Manager>تحرير**.




يجب تعيين عنوان IP لواجهة **AP-Manager** في الشبكة الفرعية والشبكة المحلية الظاهرية (VLAN) نفسها الخاصة بواجهة الإدارة.


## أدوار الراديو

يمكن أن يكون لهذا الحل دوران رئيسيان للإرسال اللاسلكي:

- نقطة الوصول الجذر (RAP) - يقوم الراديو الذي تريد الاتصال به بوحدة التحكم (عبر المحول) بدور بروتوكول الوصول عن بعد (RAP). تحتوي نقاط الوصول عن بعد (RAP) على اتصال سلكي ممكن ل LWAPP بوحدة التحكم. إن RAP هي عقدة أصل لأي شبكة جسر أو شبكة شبكة داخلية. يمكن أن تحتوي وحدة التحكم على نقطة وصول RAP واحدة أو أكثر بحيث ينشأ لكل منها شبكات لاسلكية واحدة أو شبكات لاسلكية مختلفة. يمكن أن يكون هناك أكثر من بروتوكول RAP لنفس شبكة الشبكة داخل المباني للتكرار.
- نقطة وصول الشبكة المعشقة (MAP) الداخلية - يقوم الراديو الذي لا يوجد له اتصال سلكي بوحدة التحكم بدور نقطة وصول الشبكة المعشقة الداخلية. كانت نقطة الوصول هذه تسمى سابقا نقطة الوصول العليا للقطب. وللخرائط اتصال لاسلكي (من خلال واجهة نقل البيانات) ربما بمخططات أخرى وأخيرا بموجز RAP وبالتالي بوحدة التحكم. كما قد تحتوي MAPs على اتصال إيثرنت سلكي بشبكة LAN وتعمل كنقطة نهاية جسر لتلك الشبكة المحلية (باستخدام اتصال P2P أو P2MP). يمكن أن يحدث ذلك في وقت واحد، إذا تم تكوينه بشكل صحيح كجسر إيثرنت. لم يتم إستخدام عملاء خدمة MAPs على النطاق لواجهة نقل البيانات.

الوضع الافتراضي لنقطة الوصول هو MAP.

**ملاحظة:** يمكن تعيين أدوار الراديو عبر واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI). ستقوم نقاط الوصول بإعادة التمهيد بعد تغيير الدور.

**ملاحظة:** يمكنك إستخدام واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم للتكوين المسبق لأدوار الراديو على نقطة وصول (AP) شريطة أن تكون نقطة الوصول متصلة ماديا بالمحول أو يمكنك رؤية نقطة الوصول على المحول على أنها نقطة وصول (RAP) أو خريطة.

```
(Cisco Controller) >config ap role ?

rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?

<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

## اسم مجموعة الجسر

تتحكم أسماء مجموعات الجسر (BGN) في اقتران نقاط الوصول (APs). يمكن أن تقوم شبكات BGN بتجميع أجهزة الراديو منطقيا لتجنب اتصال شبكتين على نفس القناة ببعضهما البعض. يفيد هذا الإعداد أيضا إذا كان لديك أكثر من RAP واحد في شبكتك في نفس القطاع (المنطقة). BGN هي سلسلة من عشرة أحرف كحد أقصى.

يتم تعيين اسم مجموعة جسر مجموعة مجموعة المصنع في مرحلة التصنيع (قيمة خالية). ليس مرئيا بالنسبة لك. ونتيجة لذلك، فحتى في حالة عدم وجود شبكة BGN معرفة، يمكن لأجهزة الإرسال اللاسلكية الانضمام إلى الشبكة. إذا كان لديك حزمتي RAP في شبكتك في القطاع نفسه (للحصول على سعة أكبر)، يوصى بتكوين حزمتي RAP باستخدام شبكة BGN نفسها، ولكن على قنوات مختلفة.

**ملاحظة:** يمكن تعيين اسم مجموعة الجسر من واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم وواجهة المستخدم الرسومية (GUI).

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

بعد تكوين شبكة BGN، ستقوم نقطة الوصول بإعادة الضبط.

**ملاحظة:** يجب تكوين شبكة BGN بعناية فائقة على شبكة مباشرة. يجب أن تبدأ دائما من أبعد عقدة (آخر عقدة) وتتحرك نحو RAP. السبب هو أنه إذا بدأت تكوين BGN في مكان ما في وسط الخطوة المتعددة، فسيتم إسقاط العقد التي تتجاوز هذه النقطة حيث أن هذه العقد سيكون لها BGN مختلف (BGN القديم).

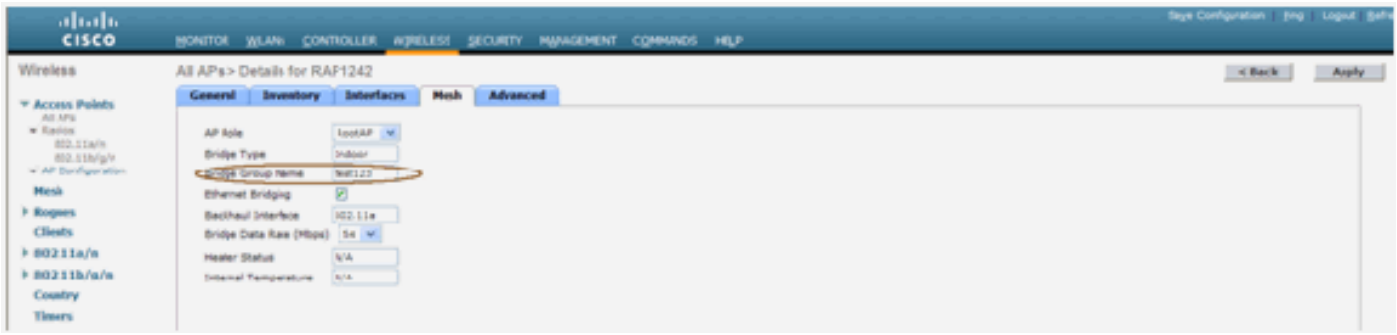
يمكنك التحقق من BGN بإصدار أمر CLI هذا:

```
Cisco Controller) > show ap config general)
```

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... RAP1242
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-AB     802.11a:-A3
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A     802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:18:74:fa:7d:1f
IP Address Configuration......................... DHCP
IP Address....................................... 10.13.13.11
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.13.13.10
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. J2106-1
Secondary Cisco Switch........................... 
Tertiary Cisco Switch............................ 
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
--More-- or (q)uit
AP Role ......................................... RootAP
Ethernet Bridging ............................... Enabled
Bridge GroupName ................................ test123
Public Safety ..................................  Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.175.19
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070808:082741)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3RH
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation........... Disabled
Console Login Name............................... 
Console Login State.............................. Unknown
AP Up Time....................................... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time................................. 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time............................... Sun Aug 19 11:59:07 2007

Join Taken Time.................................. 0 days, 00 h 00 m 24 s
Ethernet Port Duplex............................. Unknown
Ethernet Port Speed.............................. Unknown
```

أيضا، أنت يستطيع شكلت أو دققت ال BGN يستعمل الجهاز تحكم gui:

المسار: **لاسلكي > جميع نقاط الوصول > التفاصيل**.




يمكنك أن ترى أن معلومات AP البيئية معروضة أيضا مع هذا إصدار جديد.

## تكوين الأمان

الوضع الافتراضي لأمان الشبكة الداخلية هو EAP. وهذا يعني أنه ما لم تقم بتكوين هذه المعلمات على وحدة التحكم الخاصة بك، فلن تنضم خرائطك إلى:

### واجهة سطر الأوامر (CLI) لتكوين شبكة EAP الداخلية

```
(Cisco Controller) >config mesh local-auth enable

 enable Local Auth

(Cisco Controller) >config advanced eap ?

identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index      Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

إذا احتجت إلى البقاء في وضع PSK، فاستخدم هذا الأمر للعودة إلى وضع PSK:

```
(Cisco Controller) >config mesh security psk ?

(Cisco Controller) >config mesh security psk

 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)n
```

### أوامر عرض EAP للشبكة الداخلية

ضمن وضع EAP، يمكنك التحقق من أوامر **العرض** التالية للتحقق من مصادقة الخريطة:

```
(Cisco Controller) >show network

RF Network Name............................... jaggi123
Web Mode...................................... Disable
Secure Web Mode............................... Enable
Secure Shell (ssh)............................ Enable
Telnet........................................ Enable
Ethernet Multicast Mode....................... Disable   Mode: Mcast  224.1.1.1
Ethernet Broadcast Mode....................... Disable
User Idle Timeout............................. 300 seconds
ARP Idle Timeout.............................. 300 seconds
ARP Unicast Mode.............................. Disabled
Cisco AP Default Master....................... Disable
Mgmt Via Wireless Interface................... Enable
Mgmt Via Dynamic Interface.................... Disable
Bridge MAC filter Config...................... Disable
Bridge Security Mode.......................... EAP  otherwise PSK
Mesh Multicast Mode........................... 802.11b/g/n
Mesh Full Sector DFS.......................... Enable
Over The Air Provisioning of AP's............. Enable
Mobile Peer to Peer Blocking.................. Disable
AP Fallback .................................. Enable
Web Auth Redirect Ports ...................... 80
--More-- or (q)uit
Fast SSID Change ............................. Disabled
802.3 Bridging ............................... Disable
```

```
Cisco Controller) >show wlan 0)
```

```
(Cisco Controller) >show wlan 0

WLAN Identifier.................................. 0
Profile Name..................................... Mesh_profile
Network Name (SSID).............................. Mesh_ssid
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 2
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Allowed
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'prfMaP1500LlEAuth93')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                  Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ........................................... Disabled
   IP Security Passthru.......................... Disabled
   Web Based Authentication...................... Disabled
   Web-Passthrough............................... Disabled
   Conditional Web Redirect...................... Disabled
   Auto Anchor................................... Disabled
--More-- or (q)uit
   H-REAP Local Switching........................ Disabled
   Infrastructure MFP protection................. Enabled (Global Infrastructure MFP Disabled)
   Client MFP.................................... Optional
   Tkip MIC Countermeasure Hold-down Timer....... 60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

Cisco Controller) >**show local-auth config**)

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. 300

Configured EAP profiles:

EAP Method configuration:
    EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 436973636f0000000000000000000000
      Authority Information ..................... Cisco A-ID

(Cisco Controller) >show advanced eap


EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries........... 20
EAP Key-Index for Dynamic WEP.............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 1
EAP-Request Max Retries.................... 2
```

```
Cisco Controller) >show advanced eap)
```

### أوامر تصحيح أخطاء الشبكة الداخلية EAP

لتصحيح أخطاء أي مشاكل في وضع EAP، أستخدم الأوامر التالية في وحدة التحكم:

```
(Cisco Controller) >debug dot1x all enable

(Cisco Controller) >debug aaa all enable
```

## التثبيت

### المتطلبات الأساسية

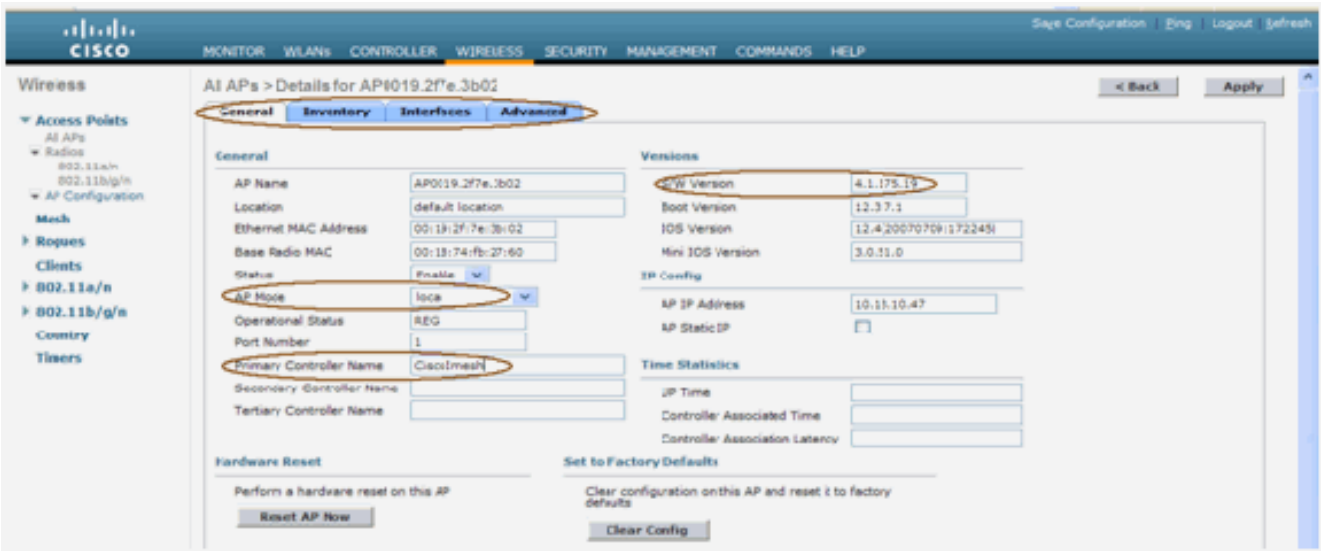
يجب أن تقوم وحدة التحكم بتشغيل الإصدار الموصى به من الرمز. انقر فوق **مراقبة** للتحقق من إصدار البرنامج. يمكن التحقق من الأمر نفسه عبر واجهة سطر الأوامر.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

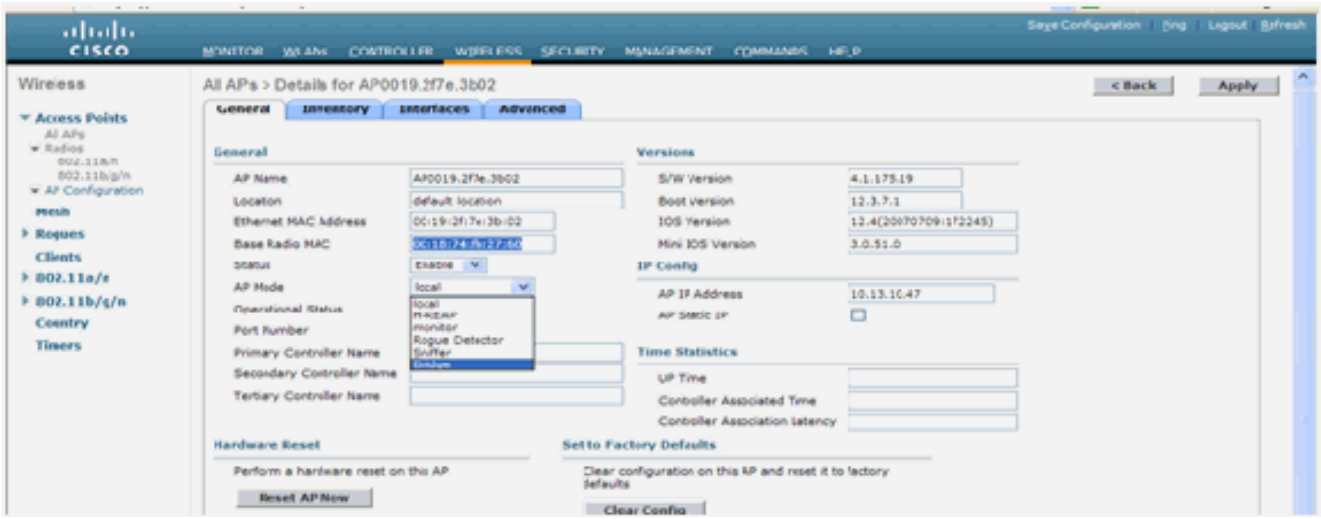
يجب الوصول إلى أنظمة مثل خادم DHCP وخادم ACS وخادم WCS.

### التثبيت

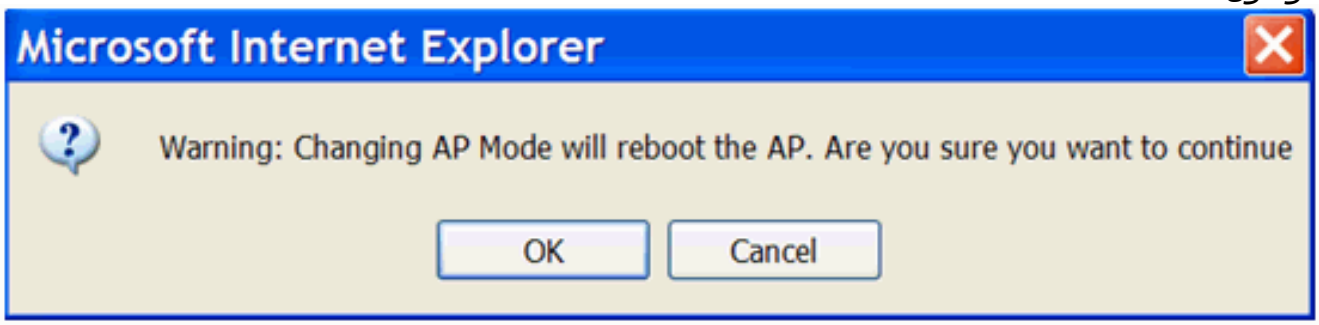
1. قم بتوصيل جميع نقاط الوصول في الوضع (Lightweight (LAPs) (1131AG/1242AG بشبكة من الطبقة 3 على الشبكة الفرعية نفسها الخاصة بعنوان IP الخاص بالإدارة. ستنضم جميع نقاط الوصول إلى وحدة التحكم كنقاط وصول في الوضع المحلي. في هذا الوضع، يتم وضع نقاط الوصول الأساسية باسم وحدة التحكم الأساسية واسم وحدة التحكم الثانوية واسم وحدة التحكم الثالثة.




2. التقط عنوان MAC للراديو الأساسي لنقطة الوصول (على سبيل المثال، 00:18:74: 27:60 :FB).
3. أضفت العنوان من ال ap ل ال ap أن يتلاقى في جسر أسلوب.
4. انقر فوق **الأمان > تصفية MAC > جديد**.
5. قم بإضافة عنوان MAC المنسوخ، ثم قم بتسمية نقاط الوصول في قائمة مرشح MAC وقائمة نقاط الوصول.
6. أخترت **جسر** من **ال ap أسلوب** قائمة.




7. سيطالبك بالتأكيد لأن هذا سيعيد تشغيل نقطة الوصول.




8. ستقوم نقطة الوصول بإعادة التمهيد والانضمام إلى وحدة التحكم في وضع الجسر. سيكون لنافذة AP الجديدة علامة تبويب إضافية: الشبكة. انقر علامة التبويب **الشبكة** (MESH) للتحقق من الدور ونوع الجسر واسم مجموعة الجسر وجسر إيثرنت وواجهة نقل البيانات الخلفية ومعدل بيانات الجسر، وما إلى ذلك.


9. في هذا الإطار، قم بالوصول إلى قائمة دور نقطة الوصول واختر الدور المناسب. في هذه الحالة، يكون الدور بشكل افتراضي هو MAP.اسم مجموعة الجسر فارغ بشكل افتراضي.واجهة نقل البيانات الخلفية هي 802.11a.معدل بيانات الجسر (معدل بيانات نقل البيانات الخلفي) يبلغ 24 ميجابت في الثانية.
10. قم بتوصيل نقطة الوصول (AP) التي تريدها ك RAP بوحدة التحكم. قم بنشر أجهزة الراديو (MAPs) في المواقع المطلوبة. شغل أجهزة الراديو. يجب أن تكون قادرا على رؤية جميع أجهزة الراديو على وحدة التحكم.

```
(Cisco Controller) >show ap summ

Number of APs.................................... 3

AP Name          Slots  AP Model             Ethernet MAC       Location         Port  Country
---------------  -----  -------------------  -----------------  ---------------  ----  -------
RAP1242          2      AIR-LAP1242AG-A-K9   00:18:74:fa:7d:1f  default location  1     US
LAP1242-1        2      AIR-LAP1242AG-A-K9   00:1b:2b:a7:ad:bf  default location  1     US
LAP1242-2        2      AIR-LAP1242AG-A-K9   00:14:1b:59:07:af  default location  1     US
```

11. حاول أن تكون هناك شروط لخط الرؤية بين العقد. في حالة عدم وجود شروط لخط الرؤية، قم بإنشاء تصاريح منطقة فرنل للحصول على شروط خط قريب من الموقع.
12. إذا كان لديك أكثر من وحدة تحكم متصلة بنفس شبكة الشبكة الداخلية، فيجب عليك تحديد اسم وحدة التحكم الأساسية على كل عقدة. وإلا فإن المراقب المالي الذي يرى أولا سوف يعتبر الجهاز الرئيسي.

## تهيئة الطاقة والقنوات

يمكن تكوين قناة نقل البيانات على بروتوكول الوصول عن بعد (RAP). سوف يتم ضبط MAPs إلى قناة RAP. يمكن تكوين الوصول المحلي بشكل مستقل ل MAPs.

من المفتاح gui، اتبع المسار: **لاسلكي>802.11a لاسلكي>يشكل**.


**ملاحظة:** مستوى طاقة Tx الافتراضي في نقل البيانات هو أعلى مستوى طاقة (المستوى 1) أما إدارة موارد الراديو (RRM) فهي في وضع إيقاف التشغيل بشكل افتراضي.

إذا كنت تقوم بتجميع نقاط الوصول عن بعد (RAP)، فإننا ننصحك باستخدام قنوات بديلة متجاورة على كل نقطة

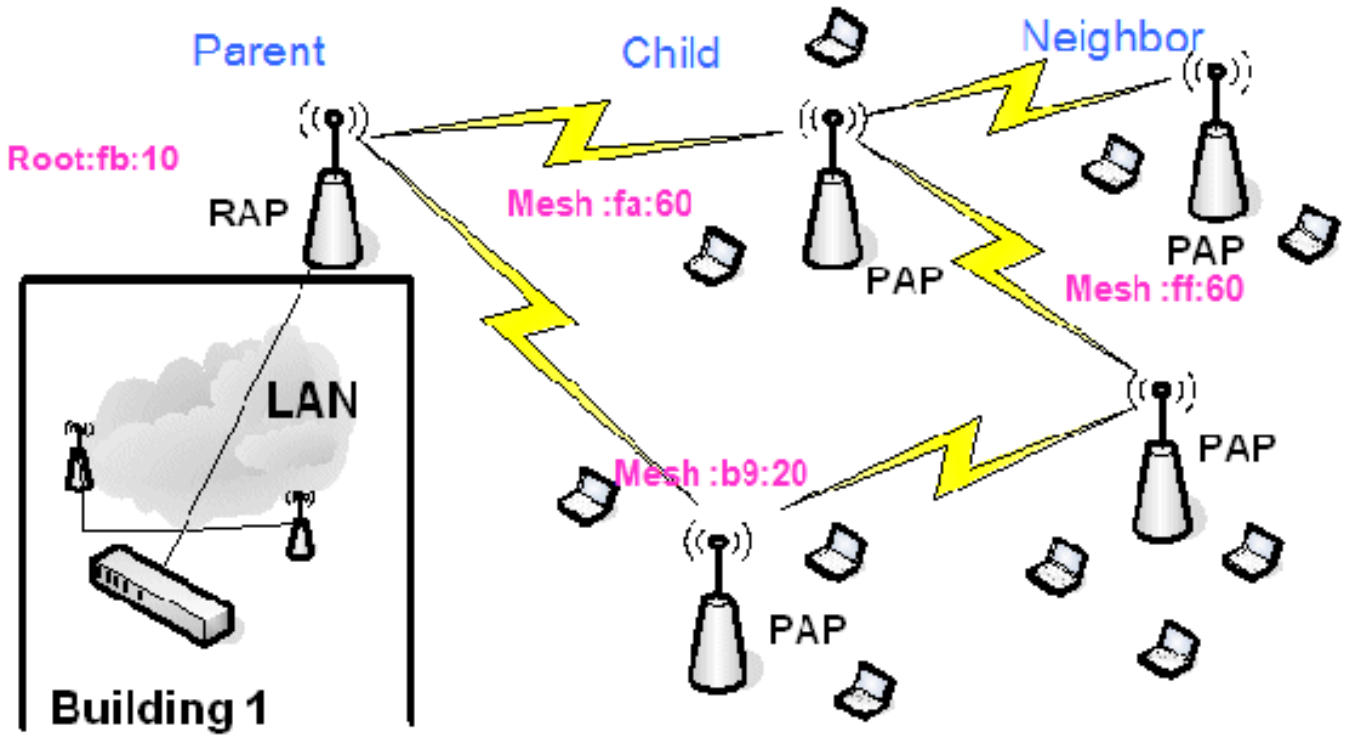
وصول عن بعد. وهذا سوف يقلل من تداخل القنوات المشتركة.

## فحص التردد اللاسلكي

في شبكة شبكة شبكة داخلية، يجب التحقق من العلاقة الأصل-التابع بين العقد. **HOP** هو إرتباط لاسلكي بين جهازي الراديو. تتغير علاقة الأصل-الطفل وأنت تسافر عبر الشبكة. يعتمد ذلك على وضعك في الشبكة المعشقة الداخلية.

الراديو الأقرب إلى وحدة التحكم في توصيل لاسلكي (hop) هو **أصل** للراديو على الجانب الآخر من النقلة. وفي نظام نقلات متعددة توجد بنية من نوع شجرة حيث تكون العقدة المتصلة بوحدة التحكم هي RAP (**الأصل**). العقدة المباشرة على الجانب الآخر من الخطوة الأولى هي **طفل**، والعقد التالية في الخطوة الثانية فصاعدا هي **جيران** لهذا الوالد المعين.

**شكل 1: شبكة نقطتين**




في الشكل 1، يتم ذكر أسماء نقاط الوصول (AP) للتسهيل. في لقطة الشاشة التالية، يتم التحقيق في **برنامج rap(fb:10)**. يمكن أن ترى هذه العقدة (في عملية النشر الفعلية) نقاط الوصول **إلى** الشبكة الداخلية **(fa:60 و b9:20)** على هيئة فروع و**MAP ff:60 على هيئة مجاور**.

من واجهة واجهة المستخدم الرسومية (GUI) للمحول، اتبع المسار: **لاسلكي > جميع نقاط الوصول > Rap1>معلومات الجوار**.


تأكد من تأسيس علاقات الأصل-الطفل وصيانتها بشكل صحيح من أجل شبكة الشبكة العنكبوتية الداخلية.

## التحقق من الارتباطات

show mesh هو أمر غني بالمعلومات للتحقق من الاتصال البيني في شبكتك.

يجب عليك إعطاء هذه الأوامر في كل عقدة (AP) باستخدام واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم، وتحميل النتائج في ملف Word أو نصي إلى موقع التحميل.

```
(Cisco Controller) >show mesh ?

env             Show mesh environment.
neigh           Show AP neigh list.
path            Show AP path.
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats  Show AP security stats.
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac             Show mesh cac.
```

في شبكتك المعشقة الداخلية، أختر رابط نقلات متعددة وأصدر تلك الأوامر بداية من نقطة الوصول السريع. قم بتحميل نتيجة الأوامر إلى موقع التحميل.

في القسم التالي، تم إصدار جميع هذه الأوامر لشبكة Hop Indoor Mesh الموضحة في الشكل 1.

## إظهار مسار الشبكة الداخلية

سيظهر هذا الأمر لك عناوين MAC وأدوار الراديو للعقد ونسب الإشارة إلى التشويش في dBs للوصلات/الارتباط الداخلي (SNRP و SNRDown) وربط SNR في dB لمسار معين.

```
(Cisco Controller) >show mesh path RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
RAP1242           is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-1           56      29     29       27       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242             56      41     32       34       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242           is a Root AP.
```

## إظهار ملخص جار الشبكة العنكبوتية في الأماكن المغلقة

سيظهر لك هذا الأمر عناوين MAC وعلاقات الأصل-التابع وعلاقات SNRs الوصلة/Downlink في dB.

```
(Cisco Controller) >show mesh neigh ?

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh  summary RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      0      0        0        0x860    BEACON
LAP1242-1           56      0      33       0        0x960    CHILD BEACON


(Cisco Controller) >show mesh neigh  summary LAP1242-1

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      30     29       28       0x961    UPDATED CHILD BEACON
RAP1242             56      43     46       31       0x86b    UPDATED NEIGH PARENT BEACON
```

وبحلول هذا الوقت، يجب أن تكون قادرا على رؤية العلاقات بين عقد الشبكة والتحقق من اتصال RF من خلال رؤية قيم SNR لكل إرتباط.

## أمان الوصول إلى وحدة تحكم AP

توفر هذه الميزة أمانا محسنا لوصول وحدة التحكم إلى نقطة الوصول (AP). مطلوب كبل وحدة تحكم لنقطة الوصول لاستخدام هذه الميزة.

وهذه البرامج مدعومة:

- واجهة سطر أوامر (CLI) لدفع مجموعة معرف المستخدم/كلمة المرور إلى نقطة الوصول المحددة:

```
(Cisco Controller) >config ap username Cisco password Cisco ?

all             Configures the Username/Password for all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

- أمر CLI لدفع مجموعة اسم المستخدم/كلمة المرور إلى جميع نقاط الوصول المسجلة إلى وحدة التحكم:

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

مع هذا أمر، ال userID/كلمة دفع من الجهاز تحكم ثابت عبر ال reload على ال APs. إذا تم مسح نقطة وصول من وحدة التحكم، فلا يوجد وضع وصول للأمان. تقوم نقطة الوصول بإنشاء ملائمة SNMP باستخدام تسجيل دخول ناجح. كما ستقوم نقطة الوصول بإنشاء ملائمة SNMP على فشل تسجيل الدخول إلى وحدة التحكم لثلاث مرات متتالية.

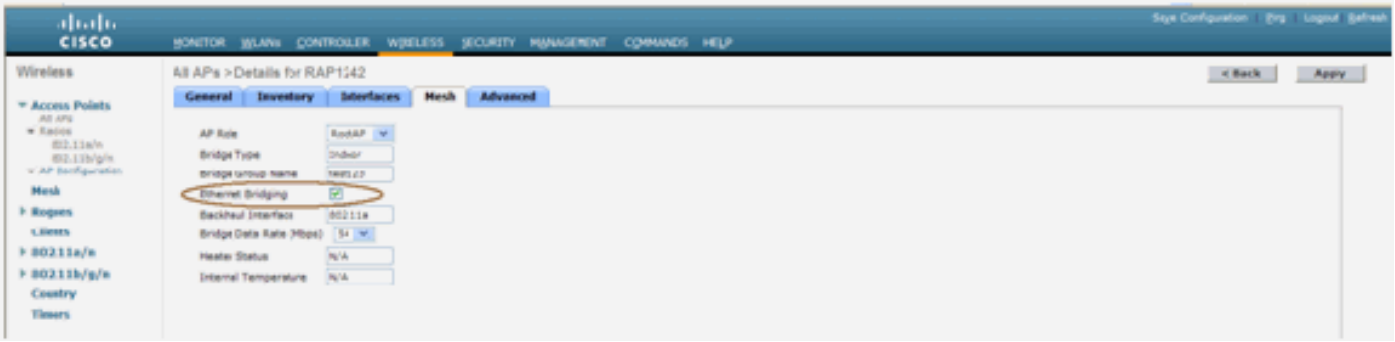
## الربط بين إيثرنت

لأسباب أمنية، أعجزت الإثرنيت ميناء على ال MAPs افتراضيا. ولا يمكن تمكينها إلا من خلال تكوين جسر الإيثرنت في بروتوكول الوصول عن بعد (RAP) والخرائط ذات الصلة.

ونتيجة لذلك، يجب تمكين جسر إيثرنت لسيناريوهين:

- عندما تريد إستخدام عقد الشبكة الداخلية كجسور.
- عند رغبتك في توصيل أي جهاز إيثرنت (مثل الكمبيوتر الشخصي/الكمبيوتر المحمول وكاميرا الفيديو وما إلى ذلك) على الخريطة باستخدام منفذ الإيثرنت الخاص به.

المسار: **لاسلكي** > انقر أي نقطة وصول > **الشبكة**.



هناك CLI أمر أن يستطيع كنت استعملت أن يشكل المسافة بين العقد يتم التوصيل. حاول توصيل جهاز إيثرنت مثل كاميرا الفيديو في كل خطوة وانظر إلى الأداء.

## تحسين اسم مجموعة الجسر

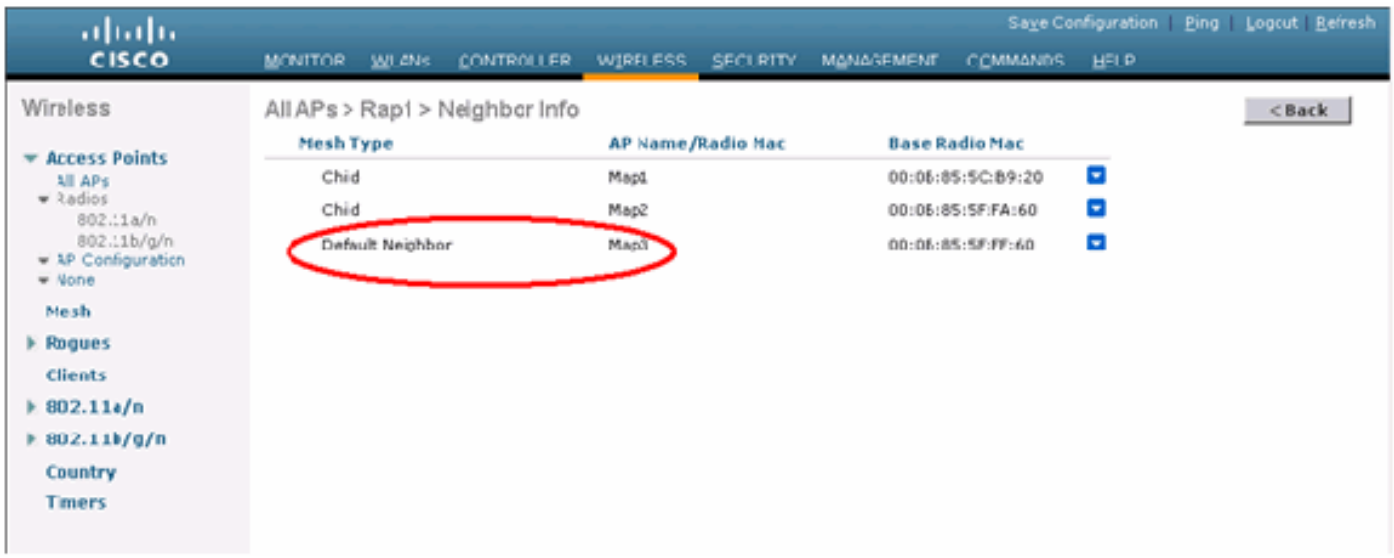
من المحتمل أن تكون نقطة الوصول مزودة بشكل غير صحيح ب "bridgeGroupName" لم يكن الغرض منها. اعتمادا على تصميم الشبكة، قد تكون نقطة الوصول هذه قادرة على الوصول إلى القطاع/الشجرة الصحيحة الخاصة بها والعثور عليها. وإذا لم يتمكن من الوصول إلى قطاع متوافق، فقد يصبح عالقا.

**لاسترداد نقطة وصول (AP) مجزأة كهذه، تم إدخال مفهوم BridgeGroupName "الافتراضي" مع رمز xx.x.3.2.**
الفكرة الأساسية أن ap أن يكون يستطيع لا يربط إلى أي آخر ap مع ال يشكل جسرGroupName، يحاول أن يربط مع "تقصير" (الكلمة) كجسرGroupName. تقبل جميع العقد التي تشغل الإصدار xx.x.3.2 والبرامج الأحدث عقد أخرى باستخدام اسم الجسر هذا.

كما يمكن أن تساعد هذه الميزة في إضافة عقدة جديدة أو عقدة تم تكوينها بشكل غير صحيح إلى شبكة قيد التشغيل.

إذا كانت لديك شبكة قيد التشغيل، فقم بأخذ نقطة وصول تم تكوينها مسبقا مع شبكة BGN مختلفة واجعلها تنضم إلى الشبكة. سترى نقطة الوصول هذه في وحدة التحكم باستخدام BGN "الافتراضي" بعد إضافة عنوان MAC الخاص بها في وحدة التحكم.

```
(CiscoController) >show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
 linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



**يمكن أن تعمل نقطة الوصول التي تستخدم شبكة BGN الافتراضية كنقطة وصول (AP) داخلية عادية تربط العملاء وتشكل علاقات فرعية أصلية للشبكة العنكبوتية الداخلية.**

في اللحظة التي تعثر فيها نقطة الوصول هذه التي تستخدم BGN الافتراضي على أصل آخر ذي BGN الصحيح، سيتم التبديل إليها.

## السجلات - الرسائل و sys و ap و trap

### سجلات الرسائل

قم بتمكين مستوى التقارير لسجلات الرسائل. من واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم، قم بإصدار هذا الأمر:

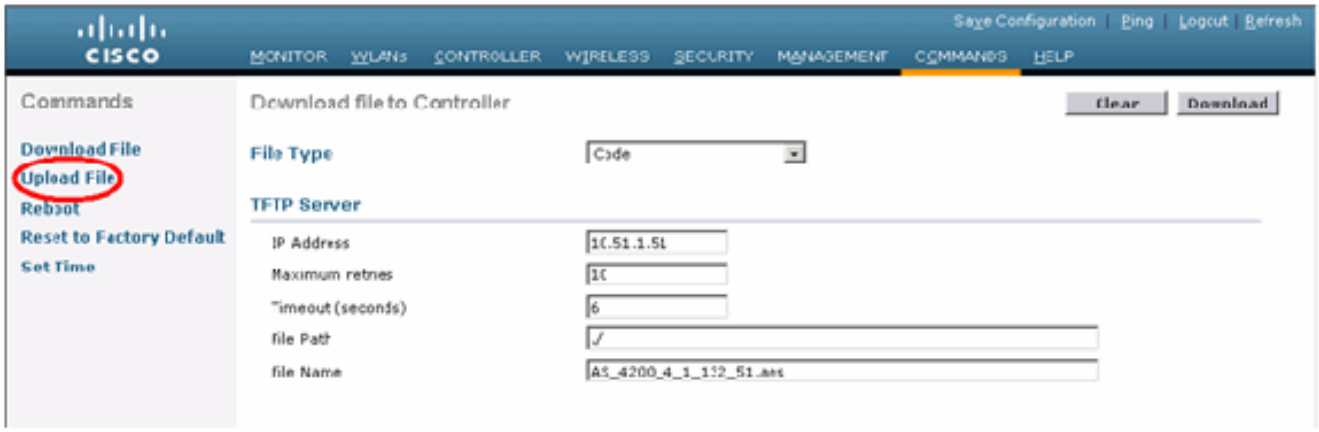
```
(Cisco Controller) >config msglog level ?

critical        Critical hardware or software Failure.
error           Non-Critical software error.
security        Authentication or security related error.
warning         Unexpected software events.
verbose         Significant system events.

(Cisco Controller) >config msglog level verbose
```

لعرض سجلات الرسائل، قم بإصدار هذا الأمر من واجهة سطر الأوامر (CLI) لوحدة التحكم:

```
(Cisco Controller) >show msglog

Message Log Severity Level ..... VERBOSE
Mon Jul 11 01:42:08 2005  [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul  8 06:12:02 2005  [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul  8 05:40:15 2005  [ERROR] spam_tmr.c 501: Did not receive hearbeat reply
 from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:45 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:40 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:14:00
Fri Jul  8 05:38:40 2005  Previous message occurred 5 times
Fri Jul  8 05:33:54 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:32:23 2005  [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul  8 05:32:17 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul  8 05:32:17 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul  8 05:32:16 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul  8 05:32:16 2005  Previous message occurred 2 times
Fri Jul  8 05:31:19 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake cal
```

لتحميل سجلات الرسائل، أستخدم واجهة المستخدم الرسومية (GUI) لوحدة التحكم:

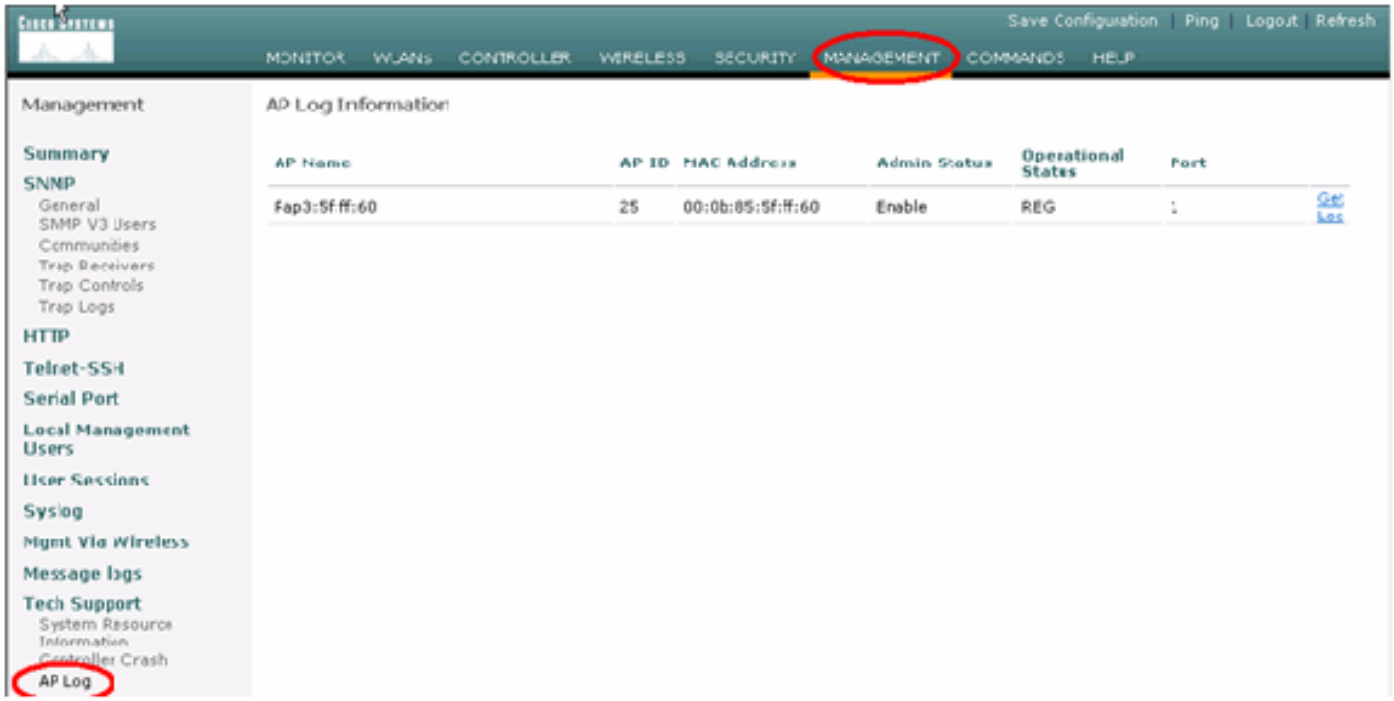
1. طقطقة
**أمر>تحميل**.




2. أدخل معلومات خادم TFTP. ستعطيك هذه الصفحة خيارات مختلفة للتحميل، وتريد إرسال هذه الملفات:سجل الرسائلسجل الأحداثسجل التراكبملف عطل (إن وجد)طقطقت in order to فحصت ل عطل مبرد، **إدارة>جهاز تحكم**
**عطل**.

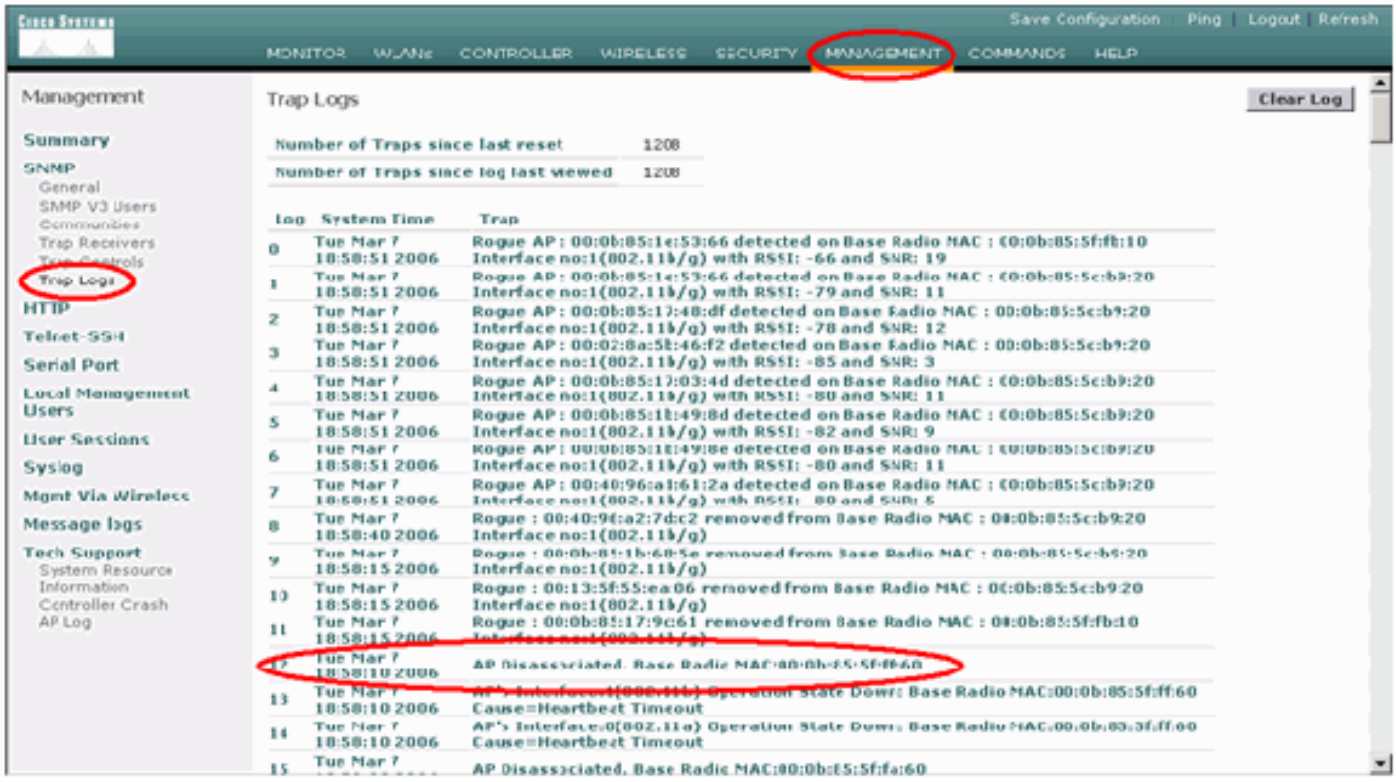

## سجلات نقطة الوصول

انتقل إلى صفحة واجهة المستخدم الرسومية هذه على وحدة التحكم للتحقق من سجلات نقطة الوصول لنقطة الوصول المحلية، إن وجدت:




## سجلات الملائمة

انتقل إلى صفحة واجهة المستخدم الرسومية هذه لوحدة التحكم وفحص سجلات الملائمة:




# الأداء

## إختبار تقارب بدء التشغيل

يمثل "التقارب" الوقت الذي يستغرقه بروتوكول RAP/MAP لإنشاء اتصال LWAPP مستقر باستخدام وحدة تحكم في الشبكة المحلية اللاسلكية (WLAN) بدءا من الوقت الذي تم فيه التمهيد لأول مرة كما هو مدرج هنا:

| إختبار التقارب | وقت التقارب (الحد الأدنى:الثانية) | | | |
|---|---|---|---|---|
| | راب | الخريط ة 1 | ماب 2 | الخريطة 3 |
| ترقية الصورة | 2:34 | 3:50 | 5:11 | 6:38 |
| إعادة تشغيل وحدة التحكم | 0:38 | 0:57 | 1:12 | 1:32 |
| تشغيل الشبكة العنكبوت ية الداخلية | 2:44 | 3:57 | 5:04 | 6:09 |
| إعادة تمهيد الراب | 2:43 | 3:57 | 5:04 | 6:09 |
| إعادة ربط الخريط ة | | 3:58 | 5:14 | 6:25 |
| تغيير خريطة الأصل (نفس القناة) | | 0:38 | | |

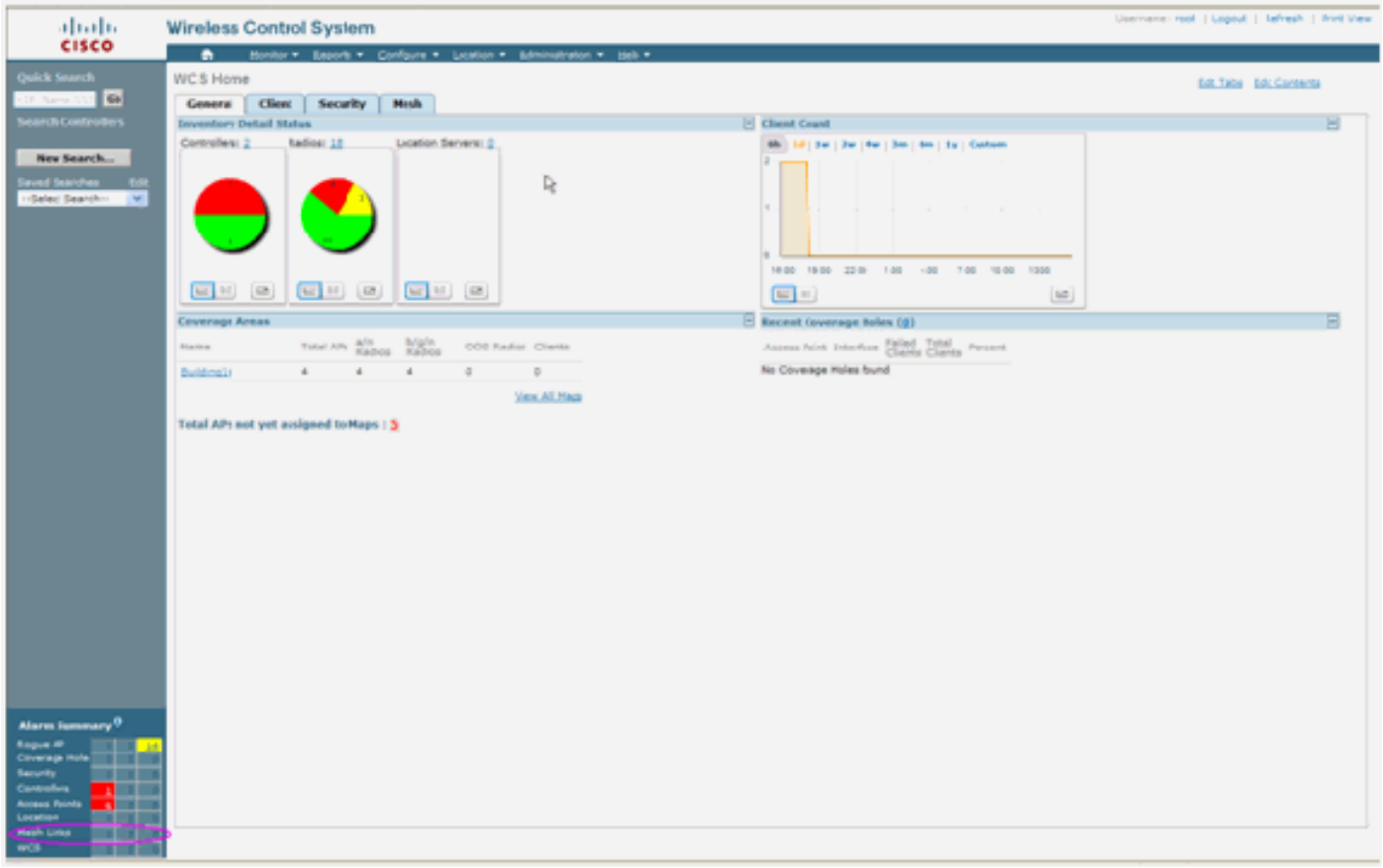
## WCS

### أجهزة إنذار الشبكة المعشقة في الأماكن المغلقة

سيولد WCS هذه الإنذارات والأحداث المتعلقة بشبكة الشبكة المعشقة الداخلية بناء على الملائمات من وحدة التحكم:

- Poor Link SNR
- تم تغيير الأصل
- نقل الطفل
- تخطيط التغييرات الأصل بشكل متكرر
- حدث منفذ وحدة التحكم
- فشل تفويض MAC
- حالات فشل المصادقة
- الأصل المستبعد التابع

انقر **روابط الشبكة**. سيظهر كل الإنذارات المتعلقة بالروابط الشبكية الداخلية.




تنطبق هذه الإنذارات على روابط الشبكات الداخلية:

- Poor Link SNR - يتم إنشاء هذا التنبيه إذا كان Link SNR أقل من 12db. يتعذر على المستخدم تغيير هذا الحد. إذا تم اكتشاف SNR ضعيف على إرتباط نقل البيانات للتابع/الأصل، فسيتم إنشاء الملائمة. سوف تحتوي الملائمة على قيمة SNR وعناوين MAC. خطورة التنبيه كبيرة. تعد نسبة SNR (من الإشارة إلى الضوضاء) مهمة لأن قوة الإشارة العالية لا تكفي لضمان أداء جهاز الاستقبال بشكل جيد. يجب أن تكون الإشارة الواردة أقوى من أي ضجيج أو تداخل موجود. فعلى سبيل المثال، من الممكن أن تكون قوة الإشارة عالية وأن يكون أداؤها اللاسلكي ضعيفا إذا كان هناك تداخل قوي أو مستوى ضوضاء مرتفع.
- تم تغيير الأصل - يتم إنشاء هذا التنبيه عند انتقال العنصر التابع إلى أصل آخر. عند فقد الأصل، سيضم العنصر التابع مع عنصر أصلي آخر، وسيرسل العنصر التابع ملائمة تحتوي على كل من عناوين MAC الخاصة بالأصل القديم والجدد إلى WCS. خطورة التنبيه: إعلامية.
- نقل الطفل - يتم إنشاء هذا التنبيه عندما يحصل WCS على فخ فقد الطفل. عندما كشفت نقطة الوصول الأصل عن فقدانها لطفل وعدم قدرتها على الاتصال بهذا الطفل، فإنها سترسل ملائمة فقد تابع إلى WCS. ستحتوي الملائمة على عنوان MAC التابع. خطورة التنبيه: إعلامية.
- يتغير أصل الخريطة بشكل متكرر - يتم إنشاء هذا التنبيه إذا قامت نقطة الوصول للشبكة الداخلية بتغيير أصلها بشكل متكرر. عندما يتجاوز عداد تغيير أصل الخريطة الحد المسموح به خلال مدة معينة، فإنه يرسل ملائمة إلى WCS. ستحتوي الملائمة على عدد مرات تغييرات الخريطة ومدة الوقت. على سبيل المثال، إذا كان هناك 5 تغييرات في غضون 2 دقيقة، عندئذ سيتم إرسال الملائمة. خطورة التنبيه: إعلامية.
- الأصل المستبعد التابع - يتم إنشاء هذا التنبيه عندما يقوم أحد الأطفال بإدراج أحد الوالدين في القائمة السوداء. يمكن أن يقوم العنصر التابع بإدراج أحد الوالدين في القائمة السوداء عندما فشل العنصر التابع في المصادقة في وحدة التحكم بعد عدد ثابت من المحاولات. يتذكر الطفل الأصل الموجود في القائمة السوداء وعندما ينضم الطفل إلى الشبكة، فإنه سيرسل الملائمة التي تحتوي على عنوان MAC الأصل الموجود في القائمة السوداء ومدة فترة القائمة السوداء.

تنبيهات بخلاف إرتباطات الشبكة داخل المباني:

- الوصول إلى منفذ وحدة التحكم - يوفر منفذ وحدة التحكم القدرة للعميل على تغيير اسم المستخدم وكلمة المرور لاسترداد نقطة الوصول الخارجية المجزأة. ومع ذلك، لمنع أي وصول مفوض من قبل المستخدم إلى نقطة

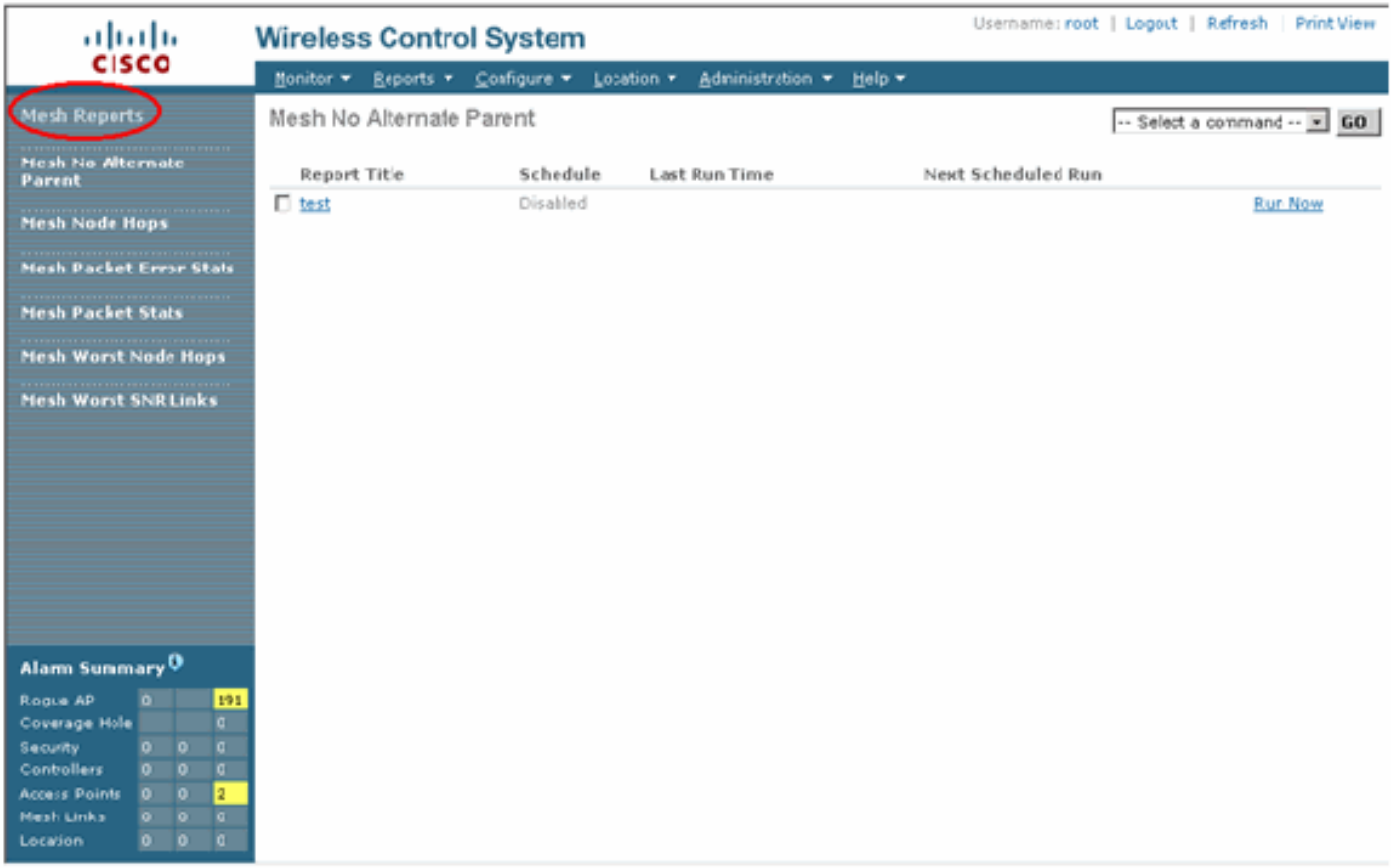
الوصول، يحتاج WCS إلى إرسال تنبيه عندما يحاول شخص ما تسجيل الدخول. هذا التنبيه مطلوب لتوفير الحماية لأن نقطة الوصول تكون ضعيفة جسديا أثناء وجودها في الأماكن المفتوحة. سيتم إنشاء هذا التنبيه إذا قام المستخدم بتسجيل الدخول بنجاح إلى منفذ وحدة تحكم AP، أو إذا فشل ثلاث مرات متتالية.

- فشل تفويض MAC - يتم إنشاء هذا التنبيه عندما تحاول نقطة الوصول الانضمام إلى الشبكة الداخلية لكنها تفشل في المصادقة لأنها ليست في قائمة مرشح MAC. سيتلقى WCS ملائمة من وحدة التحكم. سوف تحتوي الملائمة على عنوان MAC لنقطة الوصول التي فشلت في التخويل.

## تقرير الشبكة العنكبوتية وإحصاءاتها

ننقل التقرير المحسن والإطار الإحصائي من 4.1.185.0:

- لا يوجد مسار بديل
- نقلات عقد الشبكة
- حالات خطأ الحزم
- حالات الحزمة
- نقطة أسوأ
- أسوأ إرتباطات SNR




## لا يوجد مسار بديل

عادة ما يكون لنقطة الوصول الخاصة بالشباك الداخلي أكثر من جار واحد. في حالة فقد نقطة الوصول الخاصة بشبكة داخلية الارتباط الأصلي الخاص بها، فيجب أن تكون نقطة الوصول قادرة على العثور على الأصل البديل. في بعض الحالات إذا لم يكن هناك جيران ، فان الاسوشيتد برس لن تكون قادرة علي الذهاب إلى أي والد آخر إذا فقد الاباء. من المهم أن يعرف المستخدم نقاط الوصول التي ليس لها أبوان بديلان. يسرد هذا التقرير كل نقاط الوصول التي ليس لها أي جيران آخرين غير الأصل الحالي.

## نقلات عقد الشبكة العنكبوتية الداخلية

يوضح هذا التقرير عدد الخطوات البعيدة عن نقطة الوصول (RAP) الجذر. يمكنك إنشاء التقرير استنادا إلى المعايير التالية:

- نقطة الوصول (AP) حسب وحدة التحكم
- نقطة الوصول حسب الطابق

## معدلات أخطاء الحزمة

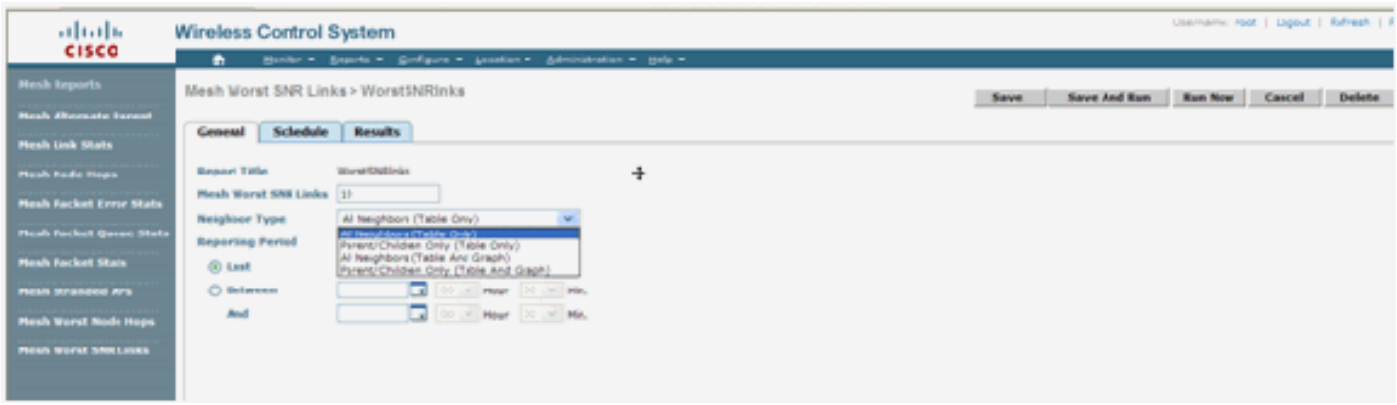
يمكن أن تحدث أخطاء الحزمة بسبب التداخل وعمليات إسقاط الحزم. يستند حساب معدل خطأ الحزمة إلى الحزم المرسلة والحزم المرسلة بنجاح. يتم قياس معدل خطأ الحزمة على إرتباط نقل البيانات وتجميع لكل من الجيران والوالد. ترسل نقطة الوصول معلومات الحزمة بشكل دوري إلى وحدة التحكم. بمجرد تغيير الأصل، ترسل نقطة الوصول معلومات خطأ الحزمة المجمعة إلى وحدة التحكم. يتم تعيين معلومات خطأ حزمة WCS من وحدة التحكم كل 10 دقائق بشكل افتراضي ويتم تخزينها في قاعدة البيانات لمدة تصل إلى 7 أيام. في WCS، الربط عرض خطأ معدل كرسم بياني. يعتمد الرسم البياني لخطأ الحزمة على البيانات التاريخية المخزنة في قاعدة البيانات.

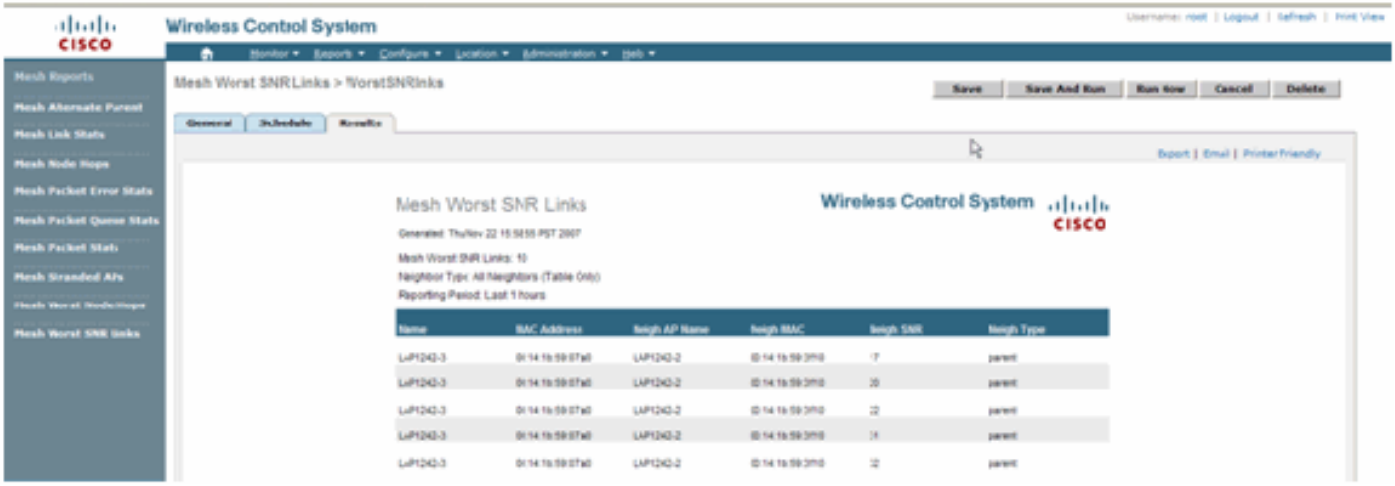
## حالات الحزمة

يوضح هذا التقرير قيم العداد الخاصة بحزم الإرسال المجاور وإجمالي الحزم المجاورة التي تم إرسالها بنجاح. يمكنك إنشاء التقرير استنادا إلى معايير معينة.

## أسوأ إرتباطات SNR

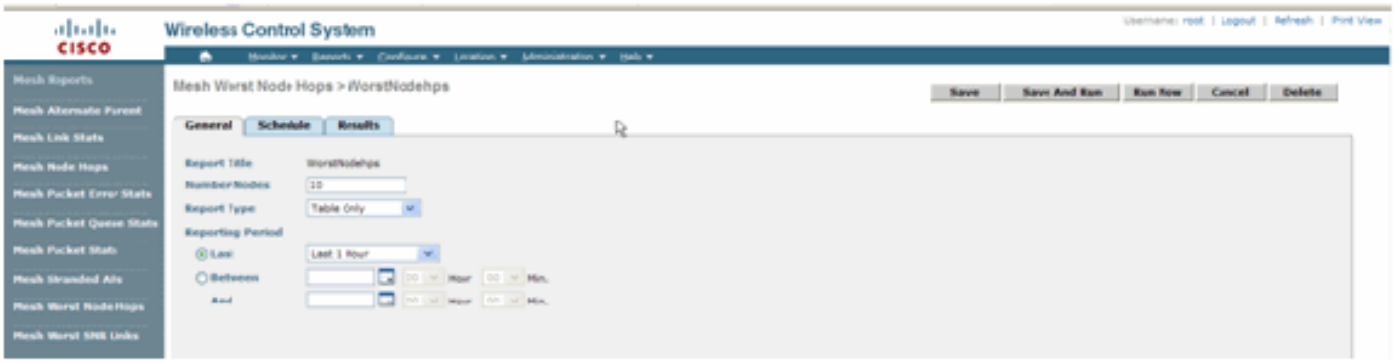
قد تحدث مشاكل الضوضاء في أوقات مختلفة وقد تزداد الضوضاء بمعدلات مختلفة أو قد تدوم لفترات زمنية مختلفة. يتيح الشكل التالي إمكانية إنشاء تقرير لكل من الراديو A و b/g بالإضافة إلى واجهات انتقائية. يسرد التقرير 10 إرتباطات SNR الأسوأ بشكل افتراضي. يمكنك الاختيار من بين 5 إلى 50 إرتباطات أسوأ. يمكن إنشاء التقرير خلال الساعة الأخيرة و 6 ساعات الأخيرة و 2 أيام الأخيرة و 7 أيام. يتم مسح البيانات كل 10 دقائق بشكل افتراضي. يتم الاحتفاظ بالبيانات في قاعدة البيانات لمدة سبعة أيام كحد أقصى. يمكن أن تكون معايير تحديد النوع المجاور هي كل الجيران، الأصل/التابع فقط.



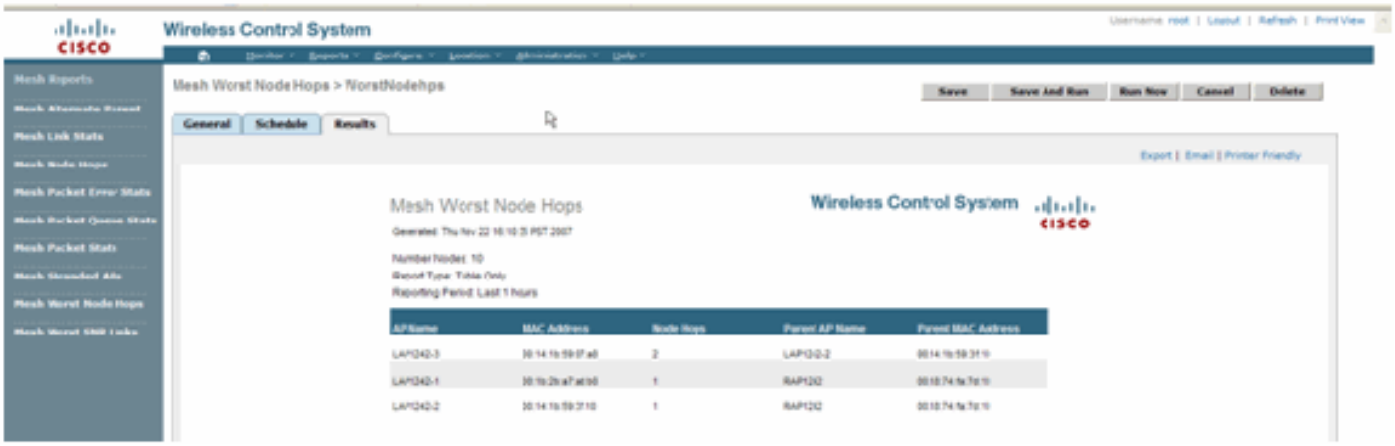



## نقلات العقد الأسوأ

يسرد هذا التقرير أسوء 10 نقاط وصول (APs) من التنقلات بشكل افتراضي. إذا كانت نقاط الوصول بعيدة عن عدد كبير جدا من الخطوات، فقد تكون الروابط ضعيفة للغاية. يمكن للمستخدم عزل نقاط الوصول (AP) التي تحتوي على العديد من التنقلات بعيدا عن نقطة الوصول (AP) الجذر واتخاذ الإجراء المناسب. يمكنك إختيار تغيير هذا **العدد من** معايير **العقد** بين 5 و 50. يمكن أن تكون معايير عامل تصفية **نوع التقرير** في هذا الشكل جدول فقط أو جدول ورسم بياني:




يوضح هذا الرقم نتيجة التقرير الأخير:




## إحصاءات الأمن

يتم عرض إحصائيات أمان الشبكة العنكبوتية الداخلية في صفحة تفاصيل نقطة الوصول ضمن قسم معلومات التوصيل. يتم إنشاء إدخال في جدول إحصائيات MeshNodeSecurity الداخلي عندما تقوم عقدة شبكة داخلية فرعية بالترابط أو المصادقة مع عقدة شبكة داخلية أصلية. تتم إزالة الإدخالات عندما تنفصل عقدة الشبكة الداخلية عن وحدة التحكم.

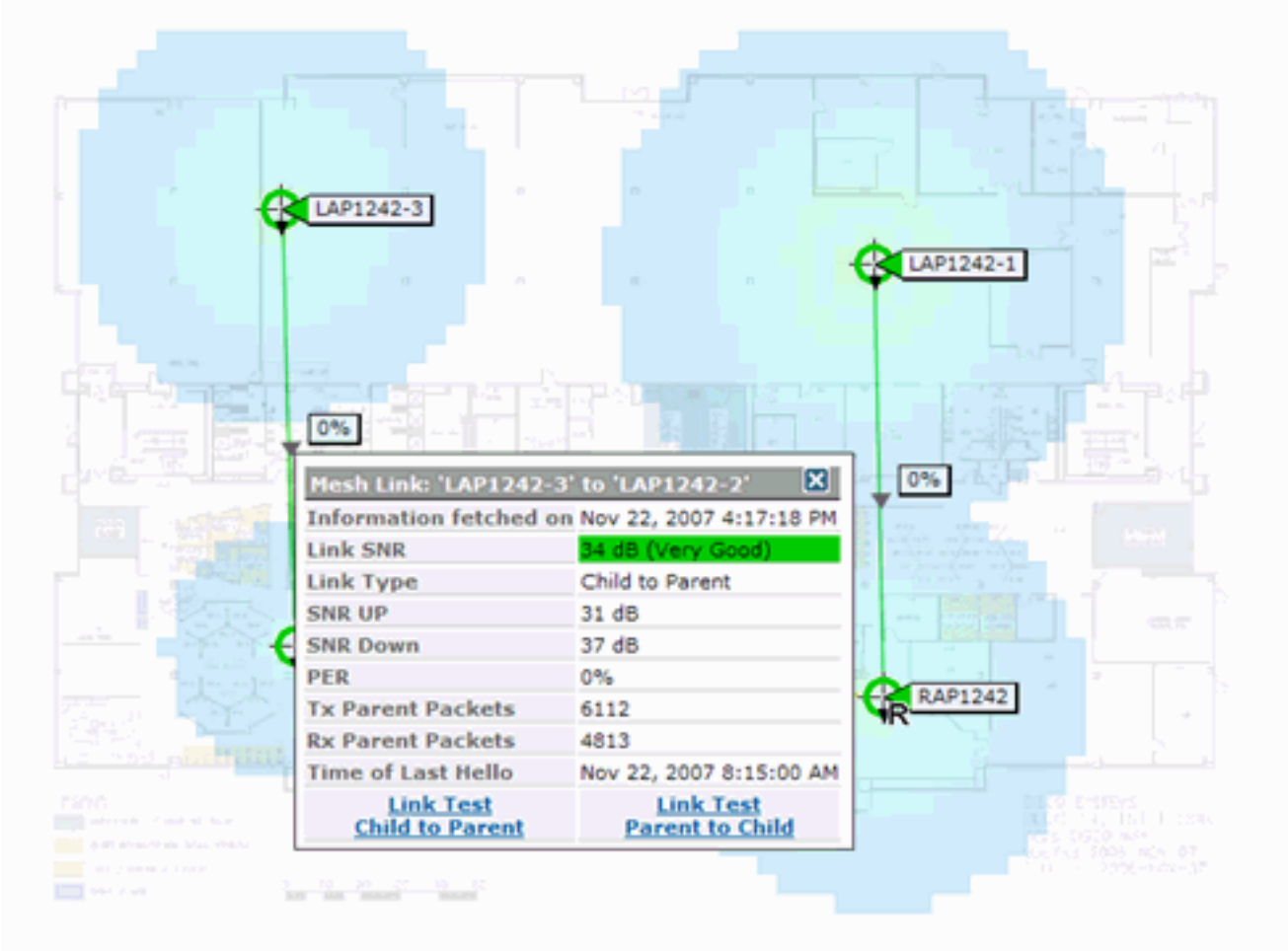
## إختبار الارتباط

يتم دعم إختبار إرتباط نقطة الوصول إلى نقطة الوصول على WCS. يمكن للمرء تحديد أي نقطتين من نقاط الوصول واستدعاء إختبار إرتباط بينهما.

إذا كانت نقاط الوصول هذه مجاورة للتردد اللاسلكي، فقد يؤدي إختبار الارتباط إلى نتيجة. يتم عرض النتيجة في مربع حوار على الخريطة نفسها بدون تحديث صفحة كامل. يمكن التخلص من مربع الحوار بسهولة.

ومع ذلك، إذا لم تكن نقطتا الوصول هاتين متجاورتين للتردد اللاسلكي، فلا يحاول WCS اكتشاف مسار بين نقطتي الوصول لإجراء إختبار إرتباط متعدد مجمعا.

عند تحريك الماوس فوق السهم على الارتباط بين العقدتين، تظهر هذه النافذة:




## إختبار إرتباط عقدة إلى عقدة

أداة إختبار الارتباط هي أداة حسب الطلب للتحقق من جودة الارتباط بين أي نقطتين APs. في WCS، تتم إضافة هذه الميزة في صفحة تفاصيل نقطة الوصول.

في صفحة تفاصيل نقطة الوصول، تحت علامة التبويب **إرتباط الشبكة الداخلية** حيث يتم سرد الارتباطات بجواره، هناك إرتباط لإجراء إختبار الارتباط.

تحتوي أداة إختبار إرتباط واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم على معلمات الإدخال الاختيارية: حجم الحزمة، إجمالي حزم إختبار الارتباط، مدة الاختبار، ومعدل إرتباط البيانات. يحتوي إختبار الارتباط على قيم افتراضية لهذه المعلمات الاختيارية. عناوين MAC للعقد هي معلمات الإدخال الإلزامية الوحيدة.

تختبر أداة إختبار الارتباط القوة، والحزمة المرسلة، والحزمة المستلمة بين العقد. يتم عرض إرتباط إختبار الارتباط في

تقرير تفاصيل نقطة الوصول. عند النقر فوق الارتباط، تظهر شاشة منبثقة نتائج إختبار الارتباط. سيتم تطبيق "إختبار الارتباط" فقط على Parent-Child وفيما بين الجيران.

يقوم إخراج إختبار الارتباط بإنشاء الحزم المرسلة، والحزم المستلمة، وحزم الأخطاء (الدلاء لأسباب مختلفة)، و SNR، وحد الضوضاء، و RSSI.

يوفر "إختبار الشبكة المحلية اللاسلكية" هذه التفاصيل حول واجهة المستخدم الرسومية (GUI) كحد أدنى:

- حزم إختبار الارتباط المرسلة
- حزم إختبار الارتباط المستلمة
- قوة الإشارة في dBM
- نسبة الإشارة إلى الضجيج

### إرتباطات جوار نقطة الوصول (AP) حسب الطلب

هذه ميزة جديدة في خريطة WCS. يمكنك النقر فوق نقطة وصول شبكة وتظهر نافذة منبثقة بها معلومات تفصيلية. يمكنك بعد ذلك النقر على **عرض جيران الشبكة**، والذي يجلب المعلومات المجاورة لنقطة الوصول المحددة ويعرض جدولا مع كل الجيران لنقطة الوصول ذات الشبكة الداخلية المحددة.

يعرض عرض رابط جوار الشبكة كل المتجاورين لنقطة الوصول المبرزة. تظهر هذه اللقطة جميع الجيران ونوع الجيران وقيمة SNR.

### إختبار بينغ

إختبار الاتصال هو أداة حسب الطلب تستخدم للاختبار بين وحدة التحكم و AP. أداة إختبار الاتصال متاحة في كل من صفحة تفاصيل نقطة الوصول وفي الخريطة. انقر فوق إرتباط **تشغيل إختبار الاتصال** في إما صفحة تفاصيل نقطة الوصول (AP) أو من معلومات نقطة الوصول (AP) الخاصة بالخريطة لبدء إختبار الاتصال من وحدة التحكم إلى نقطة الوصول الحالية.

## القرار

شبكة المؤسسة (أي الشبكة الداخلية) هي امتداد لتغطية Cisco اللاسلكية للأماكن التي لا يمكن فيها لشبكة إيثرنت السلكية توفير الاتصال. يتم تحقيق المرونة وسهولة الإدارة للشبكة اللاسلكية باستخدام شبكة المؤسسة.

يتم توفير معظم الميزات التي توفرها نقاط الوصول السلكية بواسطة طبولوجيا الشبكة الداخلية. كما يمكن أن تتواجد شبكة المؤسسة أيضا مع نقاط الوصول السلكية على وحدة التحكم نفسها.

## معلومات ذات صلة

- 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).