مثال تكوين شبكة وحدة تحكم الشبكة المحلية اللاسلكية (LAN)

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
نقطة الوصول من الشبكة العنكبوتية الخارجية خفيفة الوزن Cisco Aironet 1510 Series
نقطة الوصول من أعلى السطح (RAP)
نقطة الوصول من أعلى العمود (PAP)
الميزات غير مدعومة على شبكات الشبكة المعشقة
تسلسل بدء تشغيل نقطة الوصول
التكوين
تمكين التكوين بدون لمس (تمكين بشكل افتراضي)
إضافة MIC إلى قائمة تخويل AP
تكوين معلمات التوصيل لنقاط الوصول
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يقدم هذا المستند مثالا أساسيا للتكوين حول كيفية إنشاء إرتباط جسر من نقطة إلى نقطة باستخدام حل الشبكة العنكبوتية. يستخدم هذا المثال نقطتي وصول خفيفة الوزن (LAPs). تعمل نقطة وصول واحدة كنقطة وصول على السطح (RAP)، وتعمل نقطة الوصول في الوضع LAP) Lightweight) الأخرى كنقطة وصول على سطح العمود (PAP)، ويتم توصيلها بوحدة تحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco. يتم توصيل RAP ب WLC من خلال محول Cisco Catalyst.

يرجى الرجوع إلى مثال تكوين شبكة وحدة تحكم الشبكة المحلية اللاسلكية للإصدارات 5.2 والإصدارات الأحدث لمركز التحكم في الشبكة المحلية اللاسلكية (LAN) الإصدار 5.2 والإصدارات الأحدث

المتطلبات الأساسية

- تم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للتشغيل الأساسي.
- يتم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في وضع الطبقة 3.
- تم تكوين محول عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- المعرفة الأساسية بتكوين نقاط LAP ووحدات WLC من Cisco
- معرفة أساسية ببروتوكول نقطة الوصول في الوضع Lightweight (LWAPP).
- معرفة تكوين خادم DHCP خارجي و/أو خادم اسم المجال (DNS)
- معرفة التكوين الأساسية لمحولات Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco 4402 Series WLC الذي يشغل البرنامج الثابت 3.2.150.6
- 2 (2) نقاط الوصول في الوضع Lightweight من السلسلة Cisco Aironet 1510 Series LAPs
- محول الطبقة 2 من Cisco

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.

معلومات أساسية

نقطة الوصول من الشبكة العنكبوتية الخارجية خفيفة الوزن Cisco Aironet 1510 Series

نقطة الوصول من السلسلة Cisco Aironet 1510 Series للشبكة العنكبوتية الخارجية خفيفة الوزن هي جهاز لاسلكي مصمم خصيصا للوصول إلى العميل اللاسلكي والربط من نقطة إلى نقطة، والربط من نقطة إلى عدة نقاط، والاتصال اللاسلكي للشبكة العنكبوتية من نقطة إلى عدة نقاط. نقطة الوصول الخارجية هي وحدة مستقلة يمكن تثبيتها على جدار أو جسر، أو على عمود سطح أو على عمود إنارة شارع.

تعمل نقطة الوصول AP1510 باستخدام وحدات تحكم لتوفير إدارة مركزية وقابلة للتطوير وأمان فائق وقابلية التنقل. نظرا لتصميمها لدعم عمليات النشر التي تتم دون تهيئة، تنضم نقطة الوصول طراز AP1510 بسهولة وأمان إلى شبكة الشبكة المعشقة، كما تتوفر لإدارة الشبكة ومراقبتها من خلال واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم.

كما أن نقطة الوصول AP1510 مزودة بجهازين لاسلكيين يعملان في آن واحد: جهاز لاسلكي يعمل بتردد 2. 4 جيجاهرتز يستخدم للوصول إلى الزبون وجهاز لاسلكي يعمل بتردد 5 جيجاهرتز يستخدم لنقل البيانات إلى نقطة وصول أخرى بتردد 1510. تمر حركة مرور عميل شبكة LAN اللاسلكية من خلال راديو نقل الشبكة الخاص بنقطة الوصول أو يتم إرسالها عبر نقاط الوصول الأخرى AP1510S حتى تصل إلى اتصال إيثرنت لوحدة التحكم.

نقطة الوصول من أعلى السطح (RAP)

تحتوي نقاط الوصول عن بعد (RAP) على اتصال سلكي بمحول Cisco WLC. وهم يستخدمون الواجهة اللاسلكية لنقل البيانات للاتصال ببروتوكولات PAP المجاورة. نقاط الوصول عن بعد (RAP) هي العقدة الأصلية لأي جسر أو شبكة شبكة وتوصيل جسر أو شبكة شبكة بالشبكة السلكية. لذلك، لا يمكن أن يكون هناك إلا RAP واحد لأي مقطع شبكة جسر أو شبكة.

ملاحظة: عند إستخدام حل شبكات الشبكة العنكبوتية للربط بين الشبكة المحلية (LAN) وشبكة LAN، لا تقم بتوصيل بروتوكول RAP مباشرة إلى وحدة Cisco WLC. يلزم وجود محول أو موجه بين Cisco WLC و RAP لأن Cisco WLCs لا تقوم بإعادة توجيه حركة مرور الإيثرنت التي تأتي من منفذ تم تمكين LWAPP عليه. يمكن أن تعمل نقاط الوصول عن بعد (RAP) في وضع LWAPP للطبقة 2 أو الطبقة 3.

نقطة الوصول من أعلى العمود (PAP)

لا تحتوي قوائم التحكم في الوصول الخاصة بالمنفذ (PAP) على اتصال سلكي ب Cisco WLC. ويمكن أن تكون لاسلكية بالكامل، كما تدعم العملاء الذين يتصلون بأجهزة PAP أو RAP الأخرى، أو يمكن إستخدامها للاتصال بأجهزة طرفية أو شبكة سلكية. الإيثرنت أعجزت ميناء افتراضيا لأسباب أمن، غير أن أنت ينبغي مكنت هو ل PAPs.

ملاحظة: تدعم نقاط الوصول في الوضع LAPs) Lightweight) الخاصة بالحافة البعيدة من Cisco Aironet 1030 عمليات نشر أحادية الخطوة، بينما تدعم نقاط الوصول في الوضع الخارجي خفيفة الوزن من السلسلة Cisco Aironet 1500 Series عمليات النشر أحادية ومتعددة الخطوات. على هذا النحو، يمكن إستخدام نقاط الوصول من السلسلة Cisco Aironet 1500 Series خفيفة الوزن الخارجية كنقاط وصول من سطح المكتب وكنقاط وصول (PAPs) لخطوة واحدة أو أكثر من الخطوات من Cisco WLC.

الميزات غير مدعومة على شبكات الشبكة المعشقة

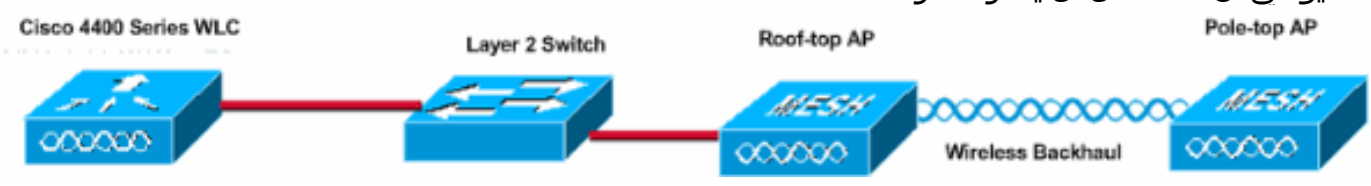
لا تكون ميزات وحدات التحكم هذه مدعومة على شبكات الشبكة:

- الدعم متعدد البلدان
- CAC القائم على التحميل (تدعم شبكات الشبكة فقط CAC القائمة على عرض النطاق الترددي، أو الثابتة.)
- الإتاحة العالية (مؤقت ربط الاكتشاف الأساسي ونبضات القلب السريعة)
- مصادقة EAP-FASTv1 و 802.1X
- مصادقة EAP-FASTv1 و 802.1X
- شهادة ذات دلالة محلية
- الخدمات المستندة إلى الموقع

تسلسل بدء تشغيل نقطة الوصول

تصف هذه القائمة ما يحدث عند بدء تشغيل كل من RAP و PAP:

- كل حركة مرور تتنقل عبر ال RAP و ال cisco WLC قبل أن يتم إرسالها إلى الشبكة المحلية LAN.
- عندما يأتي الراب، يتم ربط PAPs به تلقائيا.
- يستخدم الارتباط المتصل سرا مشتركا لإنشاء مفتاح يتم إستخدامه لتوفير معيار التشفير المتقدم (AES) للارتباط.
- وبمجرد اتصال نقطة الوصول (PAP) البعيدة ب RAP، يمكن لنقاط الوصول الخاصة بالشبكة العنكبوتية تمرير حركة مرور البيانات.
- يمكن للمستخدمين تغيير السر المشترك أو تكوين نقاط الوصول إلى الشبكة باستخدام واجهة سطر أوامر Cisco CLI))، أو واجهة مستخدم الويب لوحدة التحكم، أو نظام التحكم اللاسلكي من cisco. Cisco (Cisco WCS) يوصى أن أنت تعدل ال يشارك سر.



التكوين

أتمت هذا steps in order to شكلت ال WLC و APs ل يجسر من نقطة إلى نقطة.

1. قم بتمكين التكوين بدون لمس على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
2. أضف الميكروفون إلى قائمة تخويل نقطة الوصول.
3. تكوين معلمات التوصيل لنقاط الوصول.
4. التحقق من التكوين.

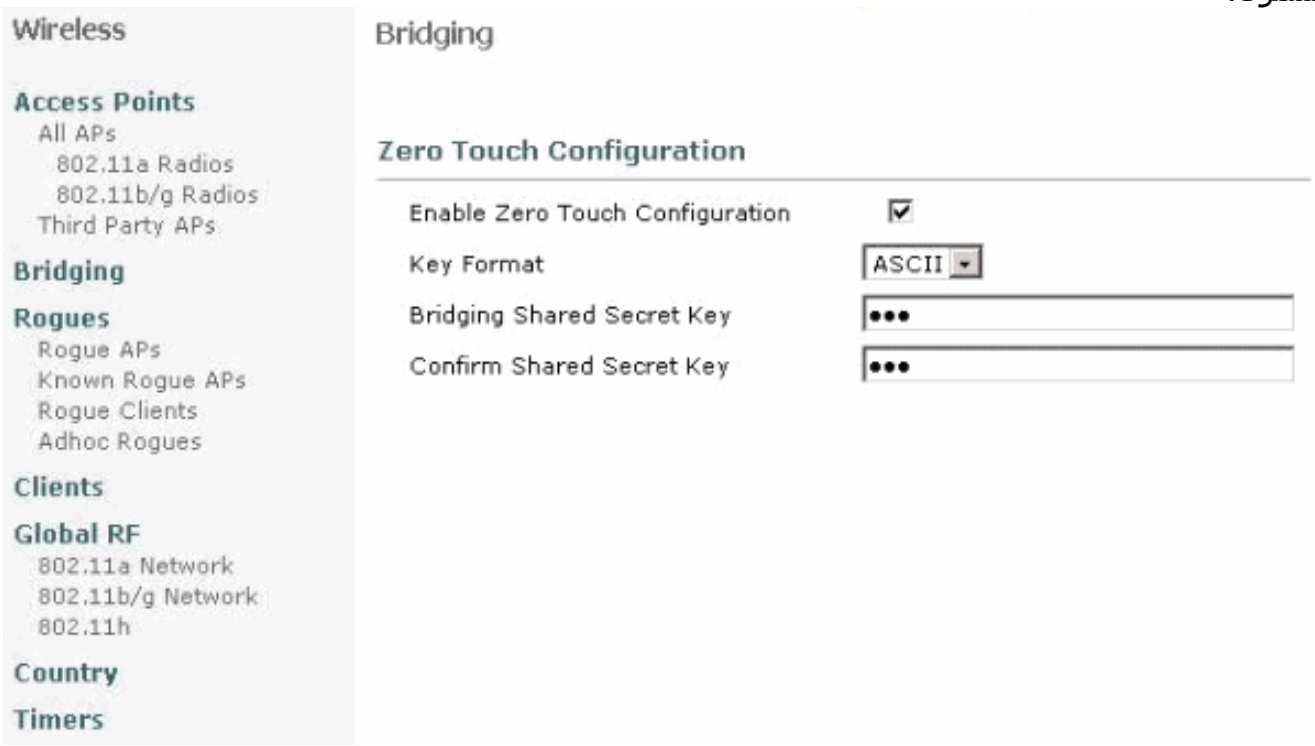
تمكين التكوين بدون لمس (تمكين بشكل افتراضي)

تكوين GUI

يمكن تمكين "التكوين دون لمس" نقاط الوصول (APs) من الحصول على المفتاح السري المشترك من وحدة التحكم عند تسجيله مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). إذا قمت بإلغاء تحديد هذا المربع، فإن وحدة التحكم لا توفر المفتاح السري المشترك، وتستخدم نقاط الوصول مفتاح افتراضي مشترك مسبقا للاتصال الآمن. تم تمكين القيمة الافتراضية (أو تحديدها). أتمت هذا steps من ال WLC GUI:

ملاحظة: لا يوجد اعتماد للتكوين دون لمس في الإصدار 4.1 من WLC والإصدارات اللاحقة.

1. أخترت **لاسلكي > يجسر** وطقطقة **يمكن لا لمس تشكيل**.
2. حدد تنسيق المفتاح.
3. أدخل المفتاح السري المشترك الذي يجسر.
4. أدخل المفتاح السري المشترك الذي يجسر مرة أخرى في المفتاح تأكيد سر مشترك.



تكوين واجهة سطر الأوامر (CLI)

أتمت هذا steps من ال CLI:

1. قم بإصدار الأمر **config network zero-config enable** لتمكين التكوين الذي بدون لمس.

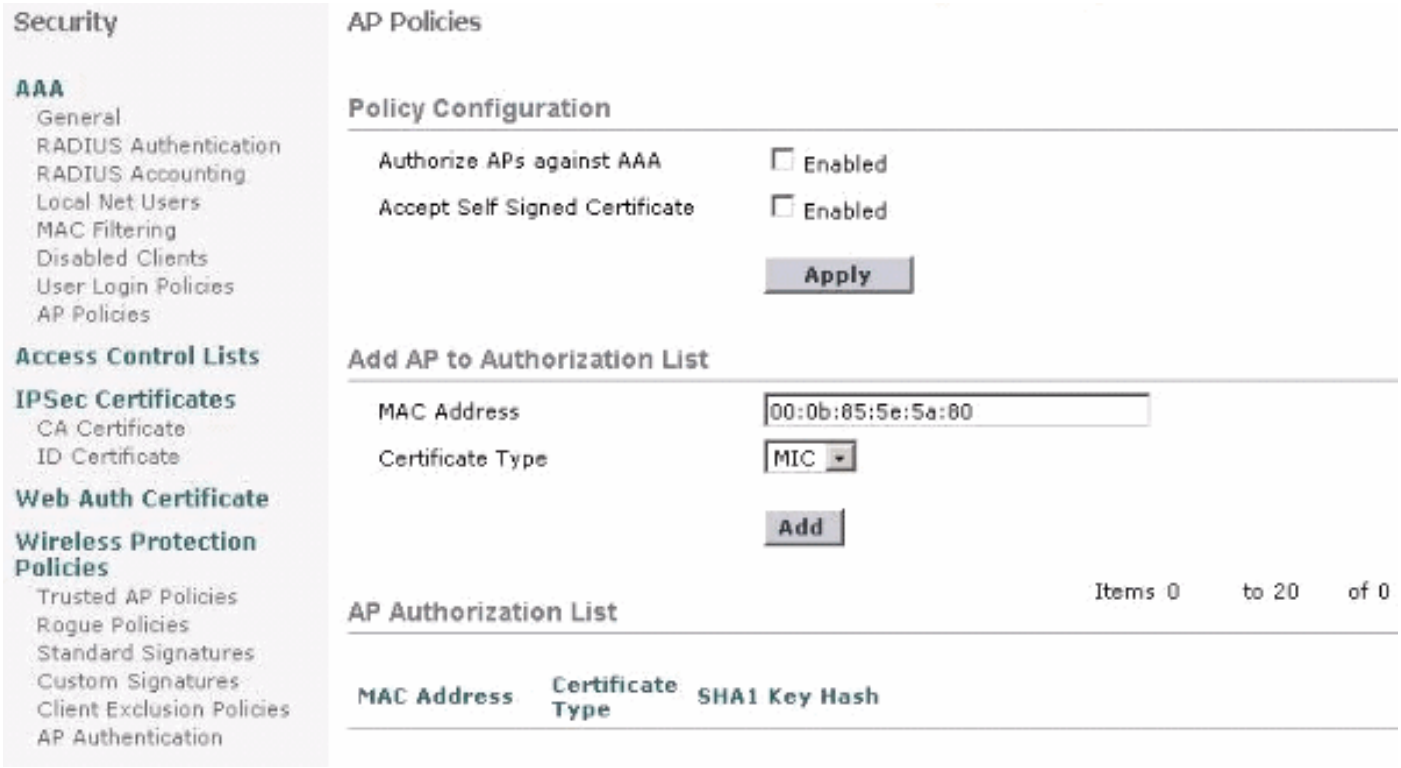
```
Cisco Controller) >config network zero-config enable)
```

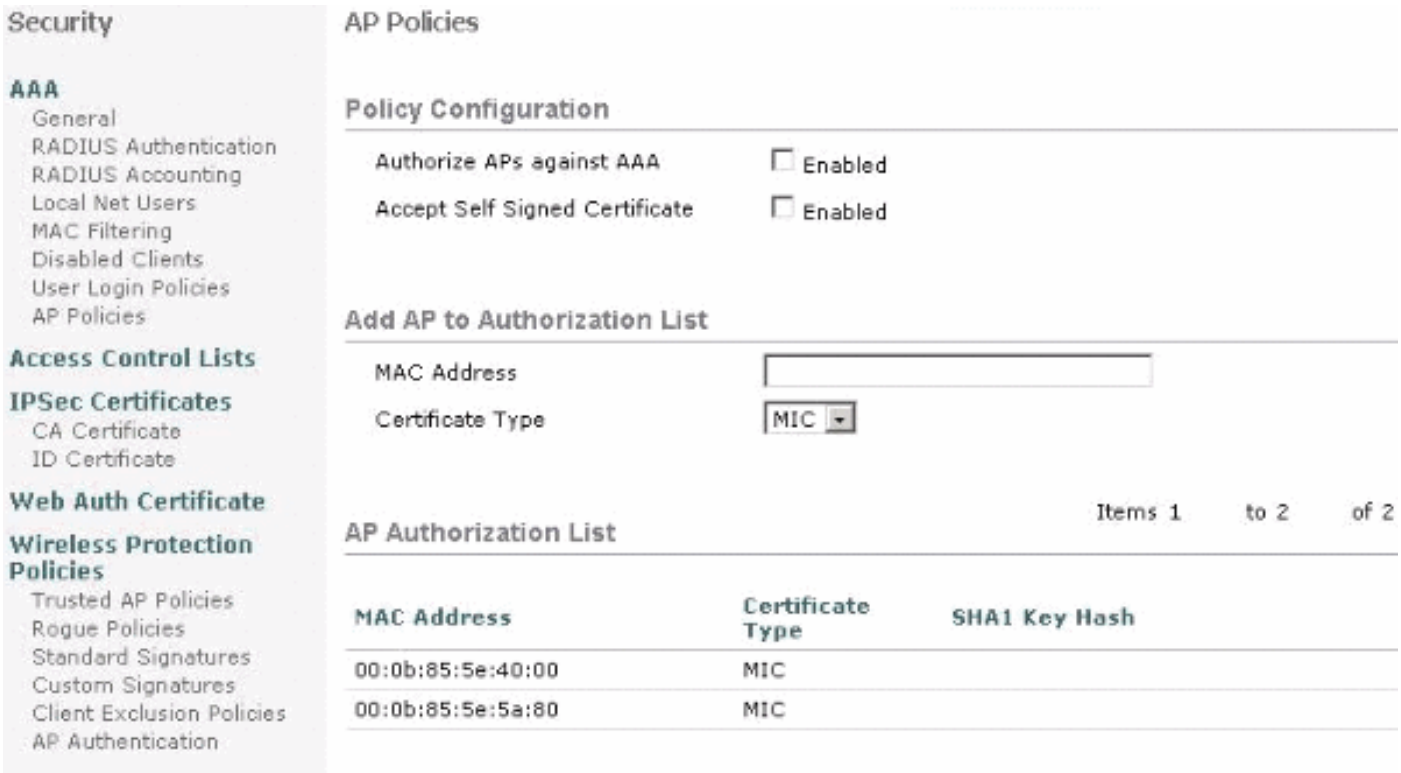
قم بإصدار الأمر config network bridging-shared-secret <string>لإضافة المفتاح السري المشترك الذي2. يجسر.

```
Cisco Controller) >config network bridging-shared-secret Cisco)
```

إضافة MIC إلى قائمة تخويل AP

تتمثل الخطوة التالية في إضافة نقطة الوصول إلى قائمة التخويل في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). أخترت in order to أتمت هذا، **تأمين > سياسات AP**، دخلت ال mac address{upper} ap تحت إضافة ap إلى التخويل قائمة وطقطقة **يضيف**.





في هذا المثال، تتم إضافة كل من نقاط الوصول (RAP و PAP) إلى قائمة تخويل نقطة الوصول (AP) على وحدة التحكم.

تكوين واجهة سطر الأوامر (CLI)

قم بإصدار الأمر **config auth-list add mic <ap mac>**لإضافة الميكروفون إلى قائمة التخويل.

```
Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00)
Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80)
```

التكوين

يستعمل هذا وثيقة هذا تشكيل:

Cisco WLC 4402

```
                    Cisco Controller) >show run-config)

                            ...Press Enter to continue

                                          System Inventory
 Switch Description.............................. Cisco
                                                Controller
       Machine Model.................................
                                                WLC4402-12
       Serial Number.................................
                                                FLS0943H005
       Burned-in MAC Address.........................
                                             00:0B:85:40:CF:A0
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
       Power Supply 2................................
                                                Present, OK

             Press Enter to continue Or <Ctl Z> to abort

                                        System Information
 Manufacturer's Name............................. Cisco
                                              Systems, Inc
 Product Name.................................... Cisco
                                                Controller
       Product Version...............................
                                                3.2.150.6
       RTOS Version..................................
                                                3.2.150.6
       Bootloader Version............................
                                                3.2.150.6
Build Type...................................... DATA +
                                                WPS

       System Name...................................
                                          lab120wlc4402ip100
       .................................System Location
       .................................System Contact
       System ObjectID...............................
                                    1.3.6.1.4.1.14179.1.1.4.3
       IP Address....................................
```

```
                                                    192.168.120.100
System Up Time................................... 0 days
                                          1 hrs 4 mins 6 secs

Configured Country.............................. United
                                                          States
      Operating Environment.....................
                                        (Commercial (0 to 40 C
 Internal Temp Alarm Limits...................... 0 to
                                                           65 C
 Internal Temperature............................ +42 C

      State of 802.11b Network.....................
                                                       Disabled
      State of 802.11a Network.....................
                                                       Disabled
    Number of WLANs................................ 1
      3rd Party Access Point Support...............
                                                       Disabled
    Number of Active Clients....................... 0

            Press Enter to continue Or <Ctl Z> to abort

                                             Switch Configuration
      802.3x Flow Control Mode.....................
                                                        Disable
 Current LWAPP Transport Mode..................... Layer
                                                           3
 LWAPP Transport Mode after next switch reboot.... Layer
                                                           3
      FIPS prerequisite features..................
                                                       Disabled

            Press Enter to continue Or <Ctl Z> to abort

                                          Network Information
RF-Network Name............................. airespacerf
     Web Mode................................... Enable
     Secure Web Mode............................ Enable
     Secure Shell (ssh)......................... Enable
     Telnet..................................... Enable
    Ethernet Multicast Mode..................... Disable
                                                 Mode: Ucast
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
   ARP Unicast Mode............................ Disabled
    Cisco AP Default Master..................... Disable
     Mgmt Via Wireless Interface................ Enable
     Bridge AP Zero Config...................... Enable
           Bridge Shared Secret.....................
                                               youshouldsetme
    Allow Old Bridging Aps To Authenticate...... Disable
    Over The Air Provisioning of AP's.......... Disable
    Mobile Peer to Peer Blocking................ Disable
    Apple Talk ................................. Disable
     AP Fallback ............................... Enable
         Web Auth Redirect Ports ................... 80
   Fast SSID Change ........................... Disabled

            Press Enter to continue Or <Ctl Z> to abort

                                               Port Summary
     STP   Admin   Physical   Physical   Link
                                             Link    Mcast
```

```
    Pr  Type   Stat   Mode     Mode      Status   Status
                                  Trap   Appliance   POE
--- ------ ---------- ---------- ------- ---- ------- --
                                  ------- --------- ----
       Normal  Forw Enable  Auto       1000 Full  Up  1
                                 Enable  Enable     N/A
       Normal  Forw Enable  Auto       1000 Full  Up  2
                                 Enable  Enable     N/A

                                 Mobility Configuration
 Mobility Protocol Port.......................... 16666
      Mobility Security Mode.....................
                                                Disabled
      Default Mobility Domain.....................
                                              airespacerf
    Mobility Group members configured.............. 3

              Switches configured in the Mobility Group
    MAC Address          IP Address         Group Name
       <00:0b:85:33:a8:40    192.168.5.70       <local
       <00:0b:85:40:cf:a0    192.168.120.100    <local
   00:0b:85:43:8c:80    192.168.5.40       airespacerf

                                Interface Configuration
  Interface Name................................. ap-
                                                manager
      IP Address.....................................
                                          192.168.120.101
      IP Netmask.....................................
                                            255.255.255.0
      IP Gateway.....................................
                                            192.168.120.1
      VLAN...........................................
                                                untagged
    Active Physical Port........................... 1
    Primary Physical Port.......................... 1
      Backup Physical Port.....................
                                              Unconfigured
      Primary DHCP Server.....................
                                              192.168.1.20
      Secondary DHCP Server.....................
                                              Unconfigured
      ACL.....................................
                                              Unconfigured
  AP Manager..................................... Yes

      Interface Name.....................
                                                management
      MAC Address.....................................
                                          00:0b:85:40:cf:a0
      IP Address.....................................
                                            192.168.120.100
      IP Netmask.....................................
                                            255.255.255.0
      IP Gateway.....................................
                                            192.168.120.1
      VLAN...........................................
                                                untagged
    Active Physical Port........................... 1
    Primary Physical Port.......................... 1
      Backup Physical Port.....................
                                              Unconfigured
      Primary DHCP Server.....................
                                              192.168.1.20
```

```
       Secondary DHCP Server.....................
                                              Unconfigured
       ACL.......................................
                                              Unconfigured
    AP Manager..................................... No

       Interface Name............................
                                              service-port
       MAC Address...............................
                                        00:0b:85:40:cf:a1
       IP Address................................
                                        192.168.250.100
       IP Netmask................................
                                        255.255.255.0
       DHCP Protocol.............................
                                              Disabled
    AP Manager..................................... No

       Interface Name............................
                                              virtual
       IP Address................................
                                              1.1.1.1
       Virtual DNS Host Name.....................
                                              Disabled
    AP Manager..................................... No

                                     WLAN Configuration

     WLAN Identifier.............................. 1
       Network Name (SSID).......................
                                     lab120wlc4402ip100
       Status....................................
                                              Enabled
       MAC Filtering.............................
                                              Enabled
       Broadcast SSID............................
                                              Enabled
       AAA Policy Override.......................
                                              Disabled
     Number of Active Clients..................... 0
    Exclusionlist Timeout......................... 60
                                              seconds
  Session Timeout................................ 1800
                                              seconds
       Interface.................................
                                              management
       WLAN ACL..................................
                                              unconfigured
       DHCP Server...............................
                                              Default
Quality of Service............................. Silver
                                              ((best effort
       WMM.......................................
                                              Disabled
       802.11e...................................
                                              Disabled
       Dot11-Phone Mode (7920)...................
                                              Disabled
  Wired Protocol................................ None
       IPv6 Support..............................
                                              Disabled
   Radio Policy.................................. All
                                     Radius Servers
       Authentication...........................
```

```
                                                192.168.1.20 1812
                                                        Security

  Authentication:....................... Open 802.11
                                                          System
       Static WEP Keys.............................
                                                         Enabled
Key Index:.....................................
                                                               1
Encryption:....................................
                                                 104-bit WEP
       802.1X.....................................
                                                        Disabled
       Wi-Fi Protected Access (WPA1).................
                                                        Disabled
       Wi-Fi Protected Access v2 (WPA2).............
                                                        Disabled
       IP Security................................
                                                        Disabled
       IP Security Passthru.......................
                                                        Disabled
       L2TP.......................................
                                                        Disabled
       Web Based Authentication.....................
                                                        Disabled
       Web-Passthrough............................
                                                        Disabled
       Auto Anchor................................
                                                        Disabled
       Cranite Passthru...........................
                                                        Disabled
       Fortress Passthru..........................
                                                        Disabled

                                             RADIUS Configuration
       Vendor Id Backward Compatibility.............
                                                        Disabled
       Credentials Caching........................
                                                        Disabled
    Call Station Id Type.......................... IP
                                                         Address
       Administrative Authentication via RADIUS.....
                                                         Enabled
       Keywrap....................................
                                                        Disabled

                                           Load Balancing Info
       Aggressive Load Balancing....................
                                                         Enabled
     Aggressive Load Balancing Window.............. 0
                                                         clients

                                          Signature Policy
       Signature Processing.......................
                                                         Enabled

                         Spanning Tree Switch Configuration

     STP Specification..................... IEEE 802.1D
                  STP Base MAC Address.................
                                              00:0B:85:40:CF:A0
          Spanning Tree Algorithm.............. Disable
            STP Bridge Priority................... 32768
               STP Bridge Max. Age (seconds).......... 20
```

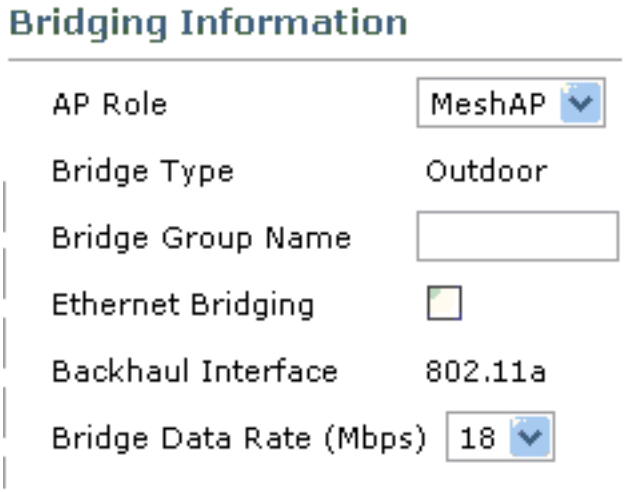
```
                STP Bridge Hello Time (seconds)........ 2
              STP Bridge Forward Delay (seconds)..... 15

                          Spanning Tree Port Configuration

        STP Port ID.............................. 8001
  STP Port State............................. Forwarding
      STP Port Administrative Mode............... 802.1D
         STP Port Priority.......................... 128
           STP Port Path Cost.......................... 4
        STP Port Path Cost Mode..................... Auto


        STP Port ID.............................. 8002
  STP Port State............................. Forwarding
      STP Port Administrative Mode............... 802.1D
         STP Port Priority.......................... 128
           STP Port Path Cost.......................... 4
        STP Port Path Cost Mode..................... Auto
```

تكوين معلمات التوصيل لنقاط الوصول

يقدم هذا القسم تعليمات حول كيفية تكوين دور نقطة الوصول في شبكة الشبكة العنكبوتية ومعلمات الربط ذات الصلة. أنت يستطيع شكلت هذا معلم يستعمل إما ال gui أو ال CLI.

1. طقطقة **لاسلكي** وبعد ذلك **كل APs** تحت نقاط الوصول. تظهر صفحة كل نقاط الوصول.
2. انقر فوق إرتباط **التفاصيل** لنقطة الوصول (AP1510) لديك للوصول إلى صفحة جميع نقاط الوصول > التفاصيل في هذه الصفحة، يتم تعيين وضع نقطة الوصول تحت عام تلقائيا على جسر لنقاط الوصول التي لها وظيفة جسر، مثل AP1510. تظهر هذه الصفحة أيضا هذه المعلومات تحت معلومات الربط. تحت يجسر معلومة، أختر واحد من هذا خيار in order to عينت الدور من هذا ap في الشبكة الشبكة:

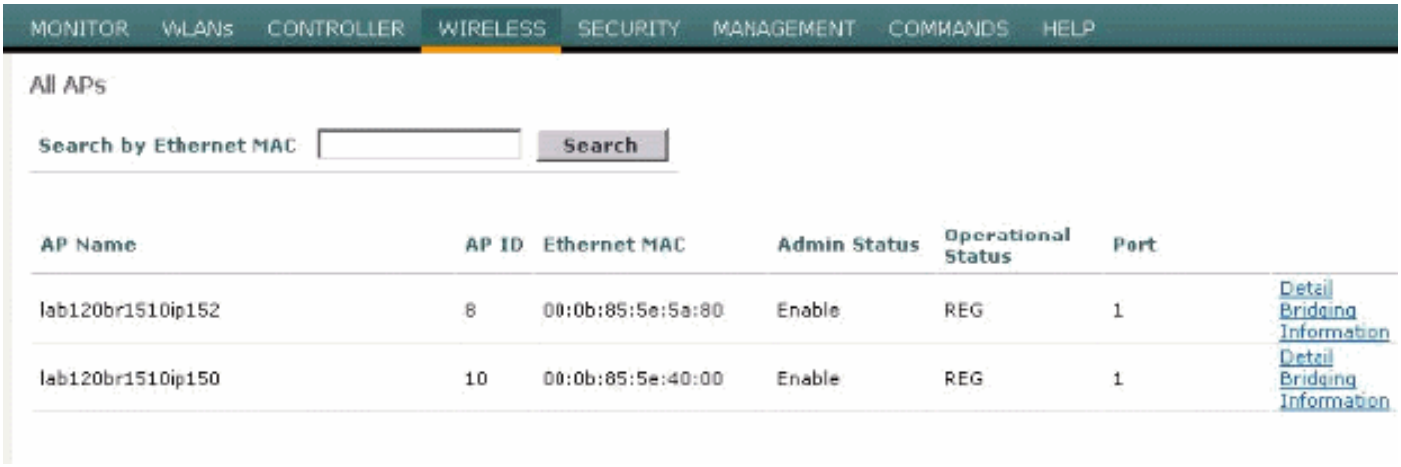
- **MeshAP**— أختر هذا الخيار إذا كان ل AP1510 توصيل لاسلكي بوحدة التحكم.
- **RootAP**— أختر هذا الخيار إذا كانت AP1510 تحتوي على اتصال سلكي بوحدة التحكم.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

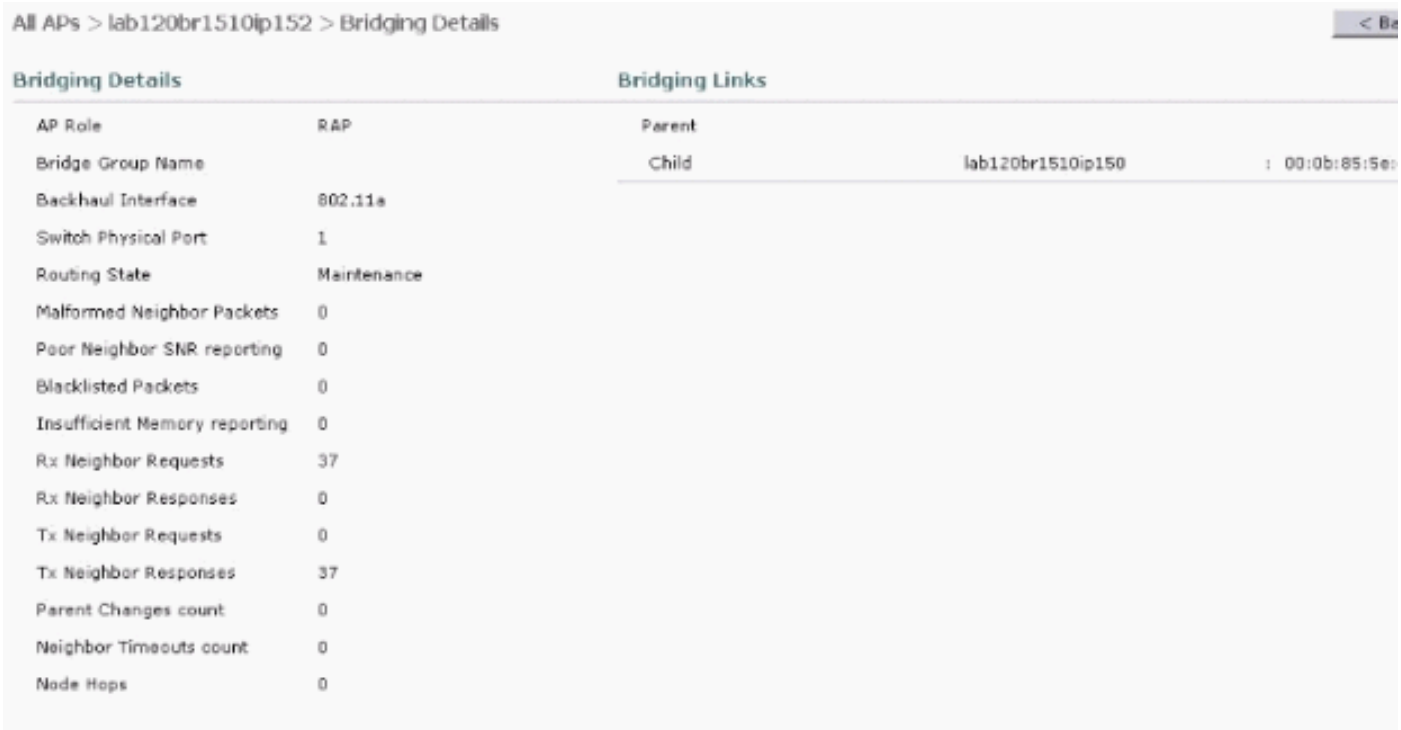
بعد تسجيل نقاط الوصول في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يمكنك عرضها أسفل علامة التبويب "لاسلكي" في أعلى واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC):



على واجهة سطر الأوامر (CLI)، يمكنك إستخدام الأمر **show ap summary** للتحقق من تسجيل نقاط الوصول في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC):

```
Cisco Controller) >show ap summary)

AP Name             Slots  AP Model     Ethernet MAC       Location         Port
----  ---------------  -----------------  ----------  -----  ------------------
  lab120br1510ip152    2     OAP1500     00:0b:85:5e:5a:80   default_location  1
  lab120br1510ip150    2     OAP1500     00:0b:85:5e:40:00   default_location  1

< (Cisco Controller)
```

طقطقة **يجسر تفاصيل** في ال gui in order to دقّقت الدور من ال ap:



على ال CLI، أنت يستطيع استعملت **العرض شبكة ممر <cisco ap>وأبديت شبكة <cisco ap>**أمر in order to دقّقت أن سجل ال APs مع ال WLC:

```
Cisco Controller) >show mesh path lab120br1510ip152)
00:0B:85:5E:5A:80 is RAP

Cisco Controller) >show mesh neigh lab120br1510ip152)

AP MAC : 00:0B:85:5E:40:00

FLAGS : 160 CHILD

worstDv 255, Ant 0, channel 0, biters 0, ppiters 10

Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0

adjustedEase 0, unadjustedEase 0

txParent 0, rxParent 0

poorSnr  0

(lastUpdate   1150103792 (Mon Jun 12 09:16:32 2006

parentChange 0

Per antenna smoothed snr values: 0 0 0 0

Vector through 00:0B:85:5E:40:00

< (Cisco Controller)
```

استكشاف الأخطاء وإصلاحها

الخاصة المعشقة مع (WLC) وهو أحد أكثر المشاكل شيوعا التي تظهر في نشر الشبكة المعشقة. أكمل التحققات التالية:

1. تحقق من إضافة عنوان MAC لنقطة الوصول في قائمة مرشح MAC في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). ويمكن ملاحظة ذلك تحت **التأمين > تصفية MAC**.
2. تحقق من السر المشترك بين "الراب" و"الخريطة". أنت يستطيع رأيت هذا رسالة في ال WLC عندما هناك حالة عدم توافق في المفتاح. "00:0b:85:68:c1:d0 LWAPP Join-Request AUTH_STRING_PAYLOAD " **ملاحظة:** حاول دائما إستخدام خيار **تمكين التكوين** دون لمس إذا كان متاحا للإصدار. يقوم هذا بتكوين المفتاح لنقاط الوصول في الشبكة المعشقة تلقائيا وتجنب التكوينات الخاطئة.
3. لا تقوم نقاط الوصول عن بعد (RAP) بإعادة توجيه أي رسائل بث على واجهة الراديو الخاصة بها. لذلك قم بتكوين خادم DHCP لإرسال عناوين IP من خلال البث الأحادي حتى يمكن للمخطط الحصول على عناوين IP الخاصة به التي تمت إعادة توجيهها بواسطة RAP. خلاف ذلك استعملت ساكن إستاتيكي ل الخريطة.
4. إما أن تترك اسم مجموعة الجسر بالقيم الافتراضية أو تأكد من تكوين أسماء مجموعات الجسر بالطريقة نفسها تماما على خرائط MAP و RAP المقابلة.

هذه مشاكل خاصة بنقاط وصول الشبكة المعشقة. بالنسبة لمشكلات الاتصال الشائعة بين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ونقطة وصول، ارجع إلى أستكشاف أخطاء نقطة الوصول في الوضع Lightweight واصلاحها التي لا تنضم إلى وحدة تحكم في الشبكة المحلية (LAN) اللاسلكية.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

أنت يستطيع استعملت هذا يضبط أمر أن يتحرى ال WLC:

- debug pem state enable — يستخدم لتكوين خيارات تصحيح أخطاء مدير نهج الوصول.
- debug pem events enable — يستخدم لتكوين خيارات تصحيح أخطاء مدير نهج الوصول.
- debug dhcp رسالة enable — يعرض تصحيح أخطاء رسائل DHCP التي يتم تبادلها إلى خادم DHCP ومنه.
- debug dhcp ربط enable — يعرض تصحيح أخطاء تفاصيل حزمة DHCP التي يتم إرسالها إلى خادم DHCP ومنه.

بعض أوامر **تصحيح الأخطاء** الإضافية التي يمكنك إستخدامها لاستكشاف الأخطاء وإصلاحها هي:

- **تمكين أخطاء lwapp**—يعرض تصحيح أخطاء LWAPP.
- **debug pm pki enable**— يعرض تصحيح أخطاء رسائل الشهادة التي يتم تمريرها بين نقطة الوصول و WLC.

يتيح **إخراج** أمر WLC هذا **debug lwapp events** أن يتم تسجيل نقاط الوصول في الوضع Lightweight في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC):

```
Cisco Controller) >debug lwapp events enable)

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 Received LWAPP JOIN REQUEST
'from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce
00:0B:85:40:CF:A0 rxNonce  00:0B:85:5E:40:00

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully added NPU Entry for
,AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101, Switch Port: 12223
intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop
MAC: 00:0b:85:5e:40:00

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of
LWAPP Join-Reply to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP
00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP
00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE REQUEST
from AP 00:0b:85:5e:40:00 to  00:0b:85:40:cf:a3

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00
static 1, 192.168.120.150/255.255.255.0, gtw 192.168.120.1 --

Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring
A regDfromCb -A-

Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring
A regDfromCb -A-

Mon Jun 12 09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret
airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Config-Message to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100'
```

```
Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100'

.Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00 associated
   Last AP failure was due to Link Failure, reason:     STATISTICS_INFO_RES

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Change-State-Event Response to AP 00:0b:85:5e:40:00

:Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext
Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for
!AP 00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Change-State-Event Response to AP 00:0b:85:5e:40:00

:Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext
Down LWAPP event for AP 00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP
!00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00
```

معلومات ذات صلة

- دليل نشر حلول شبكات Cisco
- دليل البدء السريع: نقاط وصول Cisco Aironet 1500 Series للشبكة العنكبوتية الخارجية خفيفة الوزن
- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 4.0 من Cisco
- صفحة الدعم 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).