

LEAP و Cisco Access Registrar نيوكت

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[تكوين Cisco LEAP \(Cisco Wireless EAP-Cisco\)](#)

[التعليمات بالتفصيل](#)

[تمكين Cisco LEAP \(Cisco EAP-Cisco\) على AP](#)

[التعليمات بالتفصيل](#)

[تكوين ACU 6.00](#)

[التعليمات بالتفصيل](#)

[آثار من Cisco AR](#)

[معلومات ذات صلة](#)

المقدمة

يدعم مسجل الوصول لخدمات الشبكات (AR) 3.0 بروتوكول المصادقة المتوسع الخفيف (EAP-Cisco) (LEAP Wireless). يوضح هذا المستند كيفية تكوين أدوات مساعدة العميل Aironet اللاسلكية و نقاط الوصول من السلسلة Cisco Aironet 340 أو 350 أو 1200 (Series APs) لمصادقة LEAP إلى AR من Cisco.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

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

- نقاط الوصول اللاسلكية Cisco Aironet® 340 أو 350 أو Series 1200
- البرنامج الثابت لنقطة الوصول 11.21 أو إصدار أحدث ل Cisco LEAP
- بطاقات واجهة الشبكة (NIC) من Cisco Aironet 340 أو Series 350
- إصدارات البرنامج الثابت 4.25.30 أو الأحدث ل Cisco LEAP
- مواصفات واجهة برنامج تشغيل الشبكة (8.2.3) (NDIS) أو إصدار أحدث ل Cisco LEAP
- (ACU) (Aironet Client Utilities) الإصدارات 5.02 أو الأحدث
- يلزم توفر Cisco Access Registrar 3.0 أو إصدار أحدث لتشغيل ومصادقة طلبات مصادقة Cisco LEAP و MAC

تم إنشاء المعلومات المقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

تكوين (EAP-Cisco Wireless (Cisco LEAP

يغطي هذا القسم التكوينات الأساسية ل Cisco LEAP على خادم Cisco AR و AP ومختلف العملاء.

التعليمات بالتفصيل

اتبع هذه التعليمات لتكوين LEAP:

1. قم بتغيير المنفذ على خادم Cisco AR. ترسل نقطة الوصول معلومات RADIUS عن منافذ بروتوكول مخطط بيانات المستخدم (1812 UDP (المصادقة) و 1813 (المحاسبة). بما أن Cisco AR يستمع على UDP ميناء 1645 و 1646 افتراضياً، أنت ينبغي شكلت ال Cisco AR أن يستمع على UDP ميناء 1812 و 1813. قم بإصدار الأمر `cd /radius/advanced/ports`. قم بإصدار الأمر `add 1812` لإضافة منفذ 1812. إذا كنت تخطط لإجراء عملية محاسبة، فعليك إصدار الأمر `add 1813` لإضافة المنفذ 1813. قم بحفظ التكوين، ثم أعد تشغيل الخدمات.
2. لإضافة نقطة الوصول إلى خادم Cisco AR، قم بإصدار الأوامر التالية: **القرص المضغوط**
`RADIUS/ العملاء إضافة AP350-1 نقطة الوصول AP350-1 من 171.69.89.1 ipaddress CDset ضبط`
`SharedSecret Cisco`
3. لتكوين مهلة جلسة عمل مفتاح الخصوصية المكافئة للتوصيل السلبي (WEP)، قم بإصدار الأوامر التالية: **ملاحظة:** يحدد معيار 802.1x خيار إعادة المصادقة. تستخدم خوارزمية Cisco LEAP هذا الخيار لانتهاج صلاحية مفتاح جلسة WEP الحالي للمستخدم وإصدار مفتاح جلسة WEP جديد. **القرص المضغوط**
`RADIUS/ توصيفات إضافة ملف تعريف نقطة وصول ملف تعريف القرص المضغوط`
`asطوانة set session-timeout 600`
4. لإنشاء مجموعة مستخدمين يستخدمون التوصيفات المضافة في الخطوة 3، قم بإصدار الأوامر التالية: **القرص المضغوط**
`RADIUS/ مجموعات المستخدمين إضافة AP-group CD ap-group ضبط ملف تعريف أساسيات المستخدمين في مجموعة المستخدمين هذه ملف التعريف ويستلمون بدورهم مهلة جلسة العمل.`
5. لإنشاء مستخدمين في قائمة مستخدمين وإضافة مستخدمين إلى مجموعة المستخدمين المعرفة في الخطوة 4، قم بإصدار الأوامر التالية: **القرص المضغوط**
`RADIUS/ قوائم المستخدمين إضافة مستخدم AP مستخدم AP للقرص المضغوط إضافة مستخدم 1 مستخدم 1 ضبط كلمة مرور Cisco تعيين مجموعة ap-group`
6. لإنشاء خدمة مصادقة وتفويض محلية لاستخدام "ap-userService" "UserService" ولتعيين نوع الخدمة على "eap-leap"، قم بإصدار هذه الأوامر: **القرص المضغوط**
`RADIUS/ الخدمات إضافة AP-localservice CD ap-localservice تعيين EAP-LEAP النوع UserService ap-userService`
7. لإنشاء خدمة مستخدم "ap-userService" لاستخدام قائمة المستخدم المحددة في الخطوة 5، قم بإصدار الأوامر التالية: **القرص المضغوط**
`RADIUS/ الخدمات إضافة AP-localservice CD ap-userService تعيين النوع المحليتين مستخدم ap-list المستخدمين`
8. لتعيين خدمة المصادقة والتفويض الافتراضية التي يستخدمها Cisco AR إلى الخدمة المحددة في الخطوة 6، قم بإصدار الأوامر التالية: **قرص مضغوط** / **نصف قطر**
`set defaultAuthenticationservice ap-localservice تعيين AP-localservice الافتراضي`
9. لحفظ التكوين وإعادة تحميله، قم بإصدار الأوامر التالية: **حفظ إعادة تحميل**

تمكين (Cisco LEAP) (EAP-Cisco) على AP

التعليمات بالتفصيل

اتبع الخطوات التالية لتمكين Cisco LEAP على AP:

1. تصفح إلى نقطة الوصول.
2. من صفحة حالة الملخص، انقر فوق إعداد.
3. في قائمة الخدمات، انقر على التأمين < خادم المصادقة.
4. حدد إصدار 802.1x الذي سيتم تشغيله على نقطة الوصول هذه في القائمة المنسدلة 802.1x Protocol Version.
5. قم بتكوين عنوان IP الخاص بأثر Cisco AR في مربع اسم الخادم/نص IP.
6. تحقق من تعيين القائمة المنسدلة نوع الخادم على RADIUS.
7. قم بتغيير مربع نص المنفذ إلى 1812. هذا هو رقم منفذ IP الصحيح الذي سيتم استخدامه مع تقرير ما بعد التصرف (AR) من Cisco.
8. قم بتكوين مربع النص "سر مشترك" باستخدام القيمة المستخدمة على تقرير الوصول عن بعد (AR) من Cisco.
9. حدد خانة الاختيار مصادقة EAP.
10. قم بتعديل مربع نص المهلة إذا كان ذلك مطلوباً. هذه هي قيمة المهلة لطلب مصادقة ل Cisco AR.
11. انقر فوق موافق للعودة إلى شاشة إعداد الأمان. إذا كنت تقوم أيضاً بمحاسبة RADIUS، فتتحقق من أن المنفذ على صفحة إعداد المحاسبة يوافق على المنفذ الذي تم تكوينه في Cisco AR (تم تعيينه ل 1813).
12. انقر على تشفير البيانات اللاسلكية (WEP).
13. قم بتكوين مفتاح WEP للبت بالكتابة في قيمة مفتاح 40-بت أو 128-بت في مربع نص مفتاح 1 WEP.
14. حدد أنواع المصادقة المراد استخدامها. تأكد من تحديد خانة الاختيار Network-EAP على أقل تقدير.
15. تحقق من تعيين القائمة المنسدلة استخدام تشفير البيانات على تشفير اختياري أو كامل. يسمح اختياري باستخدام عملاء غير WEP و WEP على نفس نقطة الوصول. كن على علم بأن هذا وضع غير آمن للعملية. استخدم التشفير الكامل عند الإمكان.
16. طغطة ok أن ينهي.

تكوين ACU 6.00

التعليمات بالتفصيل

اتبع الخطوات التالية لتكوين وحدة التحكم في الوصول (ACU):

1. افتح ACU.
2. انقر على مدير ملف التخصيص على شريط الأدوات.
3. انقر على إضافة لإنشاء توصيف جديد.
4. أدخل اسم ملف التخصيص في مربع النص، ثم انقر موافق.
5. أدخل معرف مجموعة الخدمة (SSID) المناسب في مربع نص SSID1.
6. انقر على أمان الشبكة.
7. حدد LEAP من القائمة المنسدلة نوع أمان الشبكة.
8. طغطة بشكل.
9. شكلت الكلمة عملية إعداد حسب الحاجة.
10. وانقر فوق OK.
11. طغطة ok على الشبكة أمن شاشة.

قم بإصدار الأمر `trace /r 5` للحصول على إخراج تتبع على Cisco AR. إن يحتاج أنت ap تصحيح، أنت يستطيع ربطت إلى ال ap عن طريق telnet وأصدر ال `eap_diag1_on` و `eap_diag2_on` أمر.

```
P1121: Packet received from 10.48.86.230 :16:31:49 06/28/2004
P1121: Checking Message-Authenticator :16:31:49 06/28/2004
P1121: Trace of Access-Request packet :16:31:49 06/28/2004
      P1121: identifier = 5 :16:31:49 06/28/2004
            P1121: length = 146 :16:31:49 06/28/2004
                  :P1121 :16:31:49 06/28/2004
reqauth = e5:4f:91:27:0a:91:82:6b:a4:81:c1:cc:c8:11:86:0b
      P1121: User-Name = user1 :16:31:49 06/28/2004
P1121: NAS-IP-Address = 10.48.86.230 :16:31:49 06/28/2004
      P1121: NAS-Port = 37 :16:31:49 06/28/2004
P1121: Service-Type = Login :16:31:49 06/28/2004
      P1121: Framed-MTU = 1400 :16:31:49 06/28/2004
P1121: Called-Station-Id = 000d29e160f2 :16:31:49 06/28/2004
P1121: Calling-Station-Id = 00028adc8f2e :16:31:49 06/28/2004
      P1121: NAS-Identifier = frinket :16:31:49 06/28/2004
P1121: NAS-Port-Type = Wireless - IEEE 802.11 :16:31:49 06/28/2004
P1121: EAP-Message = 02:02:00:0a:01:75:73:65:72:31 :16:31:49 06/28/2004
                  :P1121 :16:31:49 06/28/2004
Message-Authenticator = f8:44:b9:3b:0f:33:34:a6:ed:7f:46:2d:83:62:40:30
      P1121: Cisco-AVPair = ssid=blackbird :16:31:49 06/28/2004
(P1121: Using Client: ap1200-1 (10.48.86.230) :16:31:49 06/28/2004
P1121: Using Client ap1200-1 (10.48.86.230) as the NAS :16:31:49 06/28/2004
      P1121: Authenticating and Authorizing with :16:31:49 06/28/2004
            Service ap-localservice
,P1121: Response Type is Access-Challenge :16:31:49 06/28/2004
      .skipping Remote Session Management
,P1121: Response Type is Access-Challenge :16:31:49 06/28/2004
      .skipping Local Session Management
P1121: Adding Message-Authenticator to response :16:31:49 06/28/2004
P1121: Trace of Access-Challenge packet :16:31:49 06/28/2004
      P1121: identifier = 5 :16:31:49 06/28/2004
            P1121: length = 61 :16:31:49 06/28/2004
                  :P1121 :16:31:49 06/28/2004
reqauth = 60:ae:19:8d:41:5e:a8:dc:4c:25:1b:8d:49:a3:47:c4
      = P1121: EAP-Message :16:31:49 06/28/2004
c3:47:d6:be:b3:67:75:73:65:72:31:01:02:00:15:11:01:00:08:66:27
      = P1121: Message-Authenticator :16:31:49 06/28/2004
      d2:bc:ec:8d:85:36:0b:3a:98:b4:90:cc:af:16:2f:59
P1121: Sending response to 10.48.86.230 :16:31:49 06/28/2004
P1123: Packet received from 10.48.86.230 :16:31:49 06/28/2004
P1123: Checking Message-Authenticator :16:31:49 06/28/2004
P1123: Trace of Access-Request packet :16:31:49 06/28/2004
      P1123: identifier = 6 :16:31:49 06/28/2004
            P1123: length = 173 :16:31:49 06/28/2004
                  :P1123 :16:31:49 06/28/2004
reqauth = ab:f1:0f:2d:ab:6e:b7:49:9e:9e:99:00:28:0f:08:80
      P1123: User-Name = user1 :16:31:49 06/28/2004
P1123: NAS-IP-Address = 10.48.86.230 :16:31:49 06/28/2004
      P1123: NAS-Port = 37 :16:31:49 06/28/2004
P1123: Service-Type = Login :16:31:49 06/28/2004
      P1123: Framed-MTU = 1400 :16:31:49 06/28/2004
P1123: Called-Station-Id = 000d29e160f2 :16:31:49 06/28/2004
P1123: Calling-Station-Id = 00028adc8f2e :16:31:49 06/28/2004
      P1123: NAS-Identifier = frinket :16:31:49 06/28/2004
P1123: NAS-Port-Type = Wireless - IEEE 802.11 :16:31:49 06/28/2004
```

= P1123: EAP-Message :16:31:49 06/28/2004
:02:02:00:25:11:01:00:18:5e:26:d6:ab:3f:56:f7:db:21:96:f3:b0:fb:ec:6b
a7:58:6f:af:2c:60:f1:e3:3c:75:73:65:72:31
= P1123: Message-Authenticator :16:31:49 06/28/2004
da:35:89:30:1e:e1:d6:18:0a:4f:3b:96:f4:f8:eb:21
P1123: Cisco-AVPair = ssid=blackbird :16:31:49 06/28/2004
(P1123: Using Client: ap1200-1 (10.48.86.230 :16:31:49 06/28/2004
P1123: Using Client ap1200-1 (10.48.86.230) as the NAS :16:31:49 06/28/2004
P1123: Authenticating and Authorizing :16:31:49 06/28/2004
with Service ap-localservice
P1123: Calling external service ap-userservice :16:31:49 06/28/2004
for authentication and authorization
P1123: Getting User user1's UserRecord :16:31:49 06/28/2004
from UserList ap-users
P1123: User user1's MS-CHAP password matches :16:31:49 06/28/2004
P1123: Processing UserGroup ap-group's check items :16:31:49 06/28/2004
P1123: User user1 is part of UserGroup ap-group :16:31:49 06/28/2004
P1123: Merging UserGroup ap-group's BaseProfiles :16:31:49 06/28/2004
into response dictionary
P1123: Merging BaseProfile ap-profile :16:31:49 06/28/2004
into response dictionary
:P1123: Merging attributes into the Response Dictionary :16:31:49 06/28/2004
P1123: Adding attribute Session-Timeout, value = 600 :16:31:49 06/28/2004
P1123: Merging UserGroup ap-group's Attributes :16:31:49 06/28/2004
into response Dictionary
:P1123: Merging attributes into the Response Dictionary :16:31:49 06/28/2004
P1123: Removing all attributes except for :16:31:49 06/28/2004
EAP-Message from response - they will be sent back in the Access-Accept
,P1123: Response Type is Access-Challenge :16:31:49 06/28/2004
.skipping Remote Session Management
,P1123: Response Type is Access-Challenge :16:31:49 06/28/2004
.skipping Local Session Management
P1123: Adding Message-Authenticator to response :16:31:49 06/28/2004
P1123: Trace of Access-Challenge packet :16:31:49 06/28/2004
P1123: identifier = 6 :16:31:49 06/28/2004
P1123: length = 44 :16:31:49 06/28/2004
:P1123 :16:31:49 06/28/2004
reqauth = 28:2e:a3:27:c6:44:9e:13:8d:b3:60:01:7f:da:8b:62
P1123: EAP-Message = 03:02:00:04 :16:31:49 06/28/2004
= P1123: Message-Authenticator :16:31:49 06/28/2004
2d:63:6a:12:fd:91:9e:7d:71:9d:8b:40:04:56:2e:90
P1123: Sending response to 10.48.86.230 :16:31:49 06/28/2004
P1125: Packet received from 10.48.86.230 :16:31:49 06/28/2004
P1125: Checking Message-Authenticator :16:31:49 06/28/2004
P1125: Trace of Access-Request packet :16:31:49 06/28/2004
P1125: identifier = 7 :16:31:49 06/28/2004
P1125: length = 157 :16:31:49 06/28/2004
:P1125 :16:31:49 06/28/2004
reqauth = 72:94:8c:34:4c:4a:ed:27:98:ba:71:33:88:0d:8a:f4
P1125: User-Name = user1 :16:31:49 06/28/2004
P1125: NAS-IP-Address = 10.48.86.230 :16:31:49 06/28/2004
P1125: NAS-Port = 37 :16:31:49 06/28/2004
P1125: Service-Type = Login :16:31:49 06/28/2004
P1125: Framed-MTU = 1400 :16:31:49 06/28/2004
P1125: Called-Station-Id = 000d29e160f2 :16:31:49 06/28/2004
P1125: Calling-Station-Id = 00028adc8f2e :16:31:49 06/28/2004
P1125: NAS-Identifier = frinket :16:31:49 06/28/2004
P1125: NAS-Port-Type = Wireless - IEEE 802.11 :16:31:49 06/28/2004
= P1125: EAP-Message :16:31:49 06/28/2004
01:02:00:15:11:01:00:08:3e:b9:91:18:a8:dd:98:ee:75:73:65:72:31
= P1125: Message-Authenticator :16:31:49 06/28/2004
8e:73:2b:a6:54:c6:f5:d9:ed:6d:f0:ce:bd:4f:f1:d6
P1125: Cisco-AVPair = ssid=blackbird :16:31:49 06/28/2004
(P1125: Using Client: ap1200-1 (10.48.86.230 :16:31:49 06/28/2004

P1125: Using Client ap1200-1 (10.48.86.230) as the NAS :16:31:49 06/28/2004
P1125: Authenticating and Authorizing :16:31:49 06/28/2004
with Service ap-localservice
:P1125: Merging attributes into the Response Dictionary :16:31:49 06/28/2004
P1125: Adding attribute Session-Timeout, value = 600 :16:31:49 06/28/2004
P1125: Restoring all attributes to response :16:31:49 06/28/2004
that were removed in the last Access-Challenge
.P1125: No default Remote Session Service defined :16:31:49 06/28/2004
P1125: Adding Message-Authenticator to response :16:31:49 06/28/2004
P1125: Trace of Access-Accept packet :16:31:49 06/28/2004
P1125: identifier = 7 :16:31:49 06/28/2004
P1125: length = 142 :16:31:49 06/28/2004
:P1125 :16:31:49 06/28/2004
reqauth = 71:f1:ef:b4:e6:e0:c2:4b:0a:d0:95:47:35:3d:a5:84
P1125: Session-Timeout = 600 :16:31:49 06/28/2004
= P1125: EAP-Message :16:31:49 06/28/2004
:02:02:00:25:11:01:00:18:86:5c:78:3d:82:f7:69:c7:96:70:35:31:bb:51:a7:ba:f8:48:8c
e8:3c:75:73:65:72:31:45:66:00
P1125: Message-Authenticator = :16:31:49 06/28/2004
7b:48:c3:17:53:67:44:f3:af:5e:17:27:3d:3d:23:5f
P1125: Cisco-AVPair = :16:31:49 06/28/2004
6c:65:61:70:3a:73:65:73:73:69:6f:6e:2d:6b:65:79:3d:04:f2:c5:2a:de:fb:4e:1e:8a:8d
b8:1b:e9:2c:f9:9a:3e:83:55:ff:ae:54:57:4b:60:e1:03:05:fd:22:95:4c:b4:62:
P1125: Sending response to 10.48.86.230 :16:31:49 06/28/2004

معلومات ذات صلة

- [صفحة دعم مسجل الوصول من Cisco](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل