مصادقة التصحيح

المحتويات

المقدمة

يستخدم الاتصال اللاسلكي المصادقة بعدة طرق. أكثر أنواع المصادقة شيوعا هو بروتوكول المصادقة المتوسع (EAP) في الأنواع والنماذج المختلفة. وتتضمن أنواع المصادقة الأخرى مصادقة عنوان MAC والمصادقة الإدارية. يصف هذا وثيقة كيف أن يضبط ويفسر الإنتاج من تصحيح الأخطاء مصادقات. تكون المعلومات الواردة من عمليات تصحيح الأخطاء هذه قيمة عندما تقوم باستكشاف أخطاء التثبيتات اللاسلكية وإصلاحها.

ملاحظة: تستند أجزاء هذا المستند التي تشير إلى منتجات غير تابعة لشركة Cisco إلى تجربة المؤلف، وليس إلى التدريب الرسمي. إنها مصممة لراحتك وليس كدعم فني. للحصول على دعم فني موثوق به على منتجات غير تابعة ل Cisco، اتصل بالدعم التقني لذلك المنتج.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- المصادقة من حيث علاقتها بالشبكات اللاسلكية
- واجهة سطر الأوامر (CLI) لبرنامج Cisco IOS®
- تكوين خادم RADIUS

المكونات المستخدمة

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

- المنتجات اللاسلكية المستندة إلى برنامج IOS من Cisco من أي طراز وإصدار
- هيلغرايف هايبر تيرمينت

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.

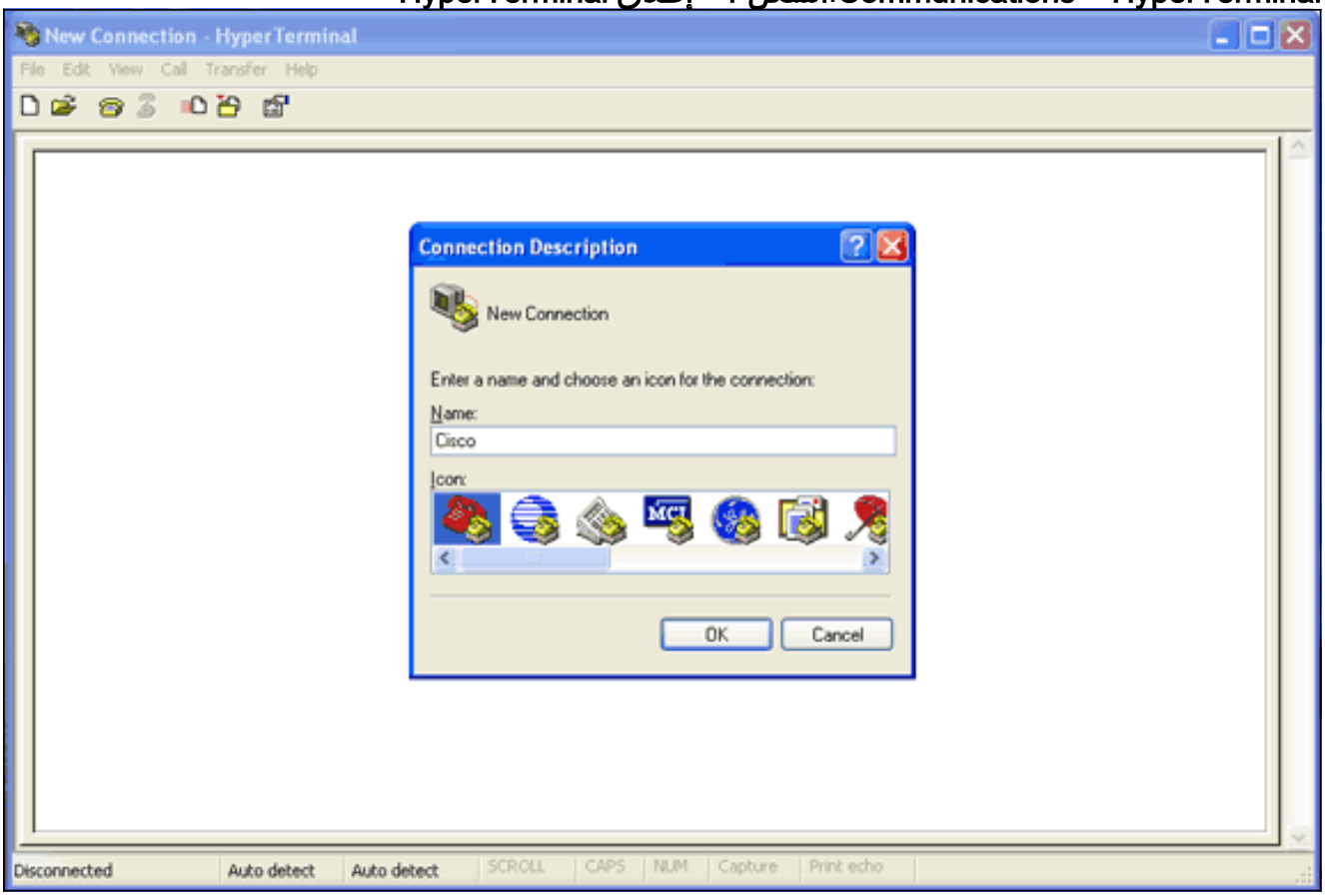
تصحيح أخطاء الالتقاط

إذا تعذر عليك التقاط معلومات تصحيح الأخطاء وتحليلها، فإن المعلومات غير مفيدة. تعتبر أسهل طريقة لالتقاط هذه البيانات هي من خلال وظيفة التقاط الشاشة المدمجة في تطبيق Telnet أو تطبيق الاتصالات.

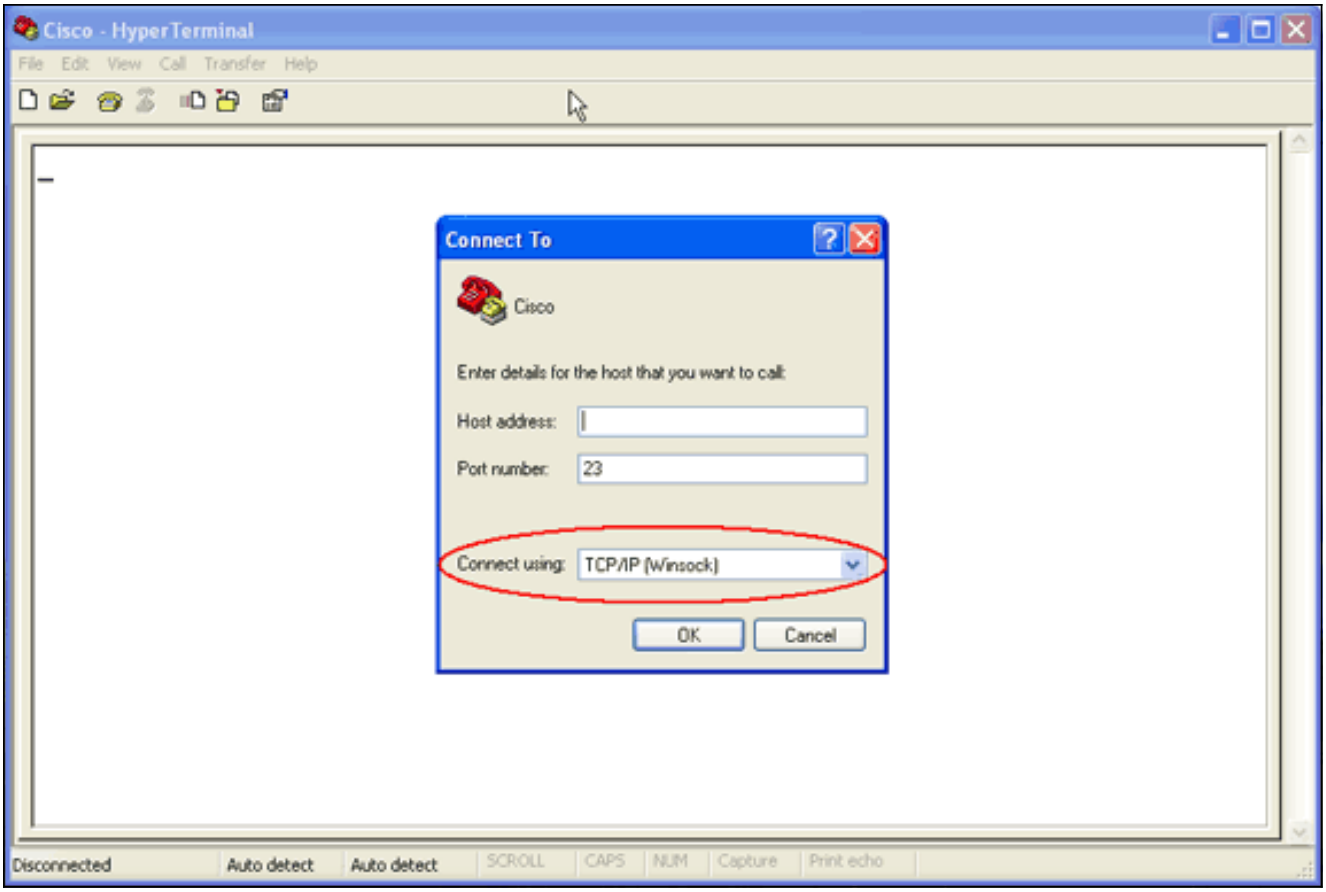
يوضح هذا المثال كيفية التقاط الإخراج باستخدام تطبيق HyperTerminal من Hilgraeve. تتضمن معظم أنظمة التشغيل Microsoft Windows برنامج HyperTerminal، ولكن يمكنك تطبيق المفاهيم على أي تطبيق محاكاة طرفية. لمزيد من المعلومات الكاملة حول التطبيق، ارجع إلى Hilgraeve .

أكمل الخطوات التالية لتكوين HyperTerminal للاتصال بنقطة الوصول (AP) أو الجسر:

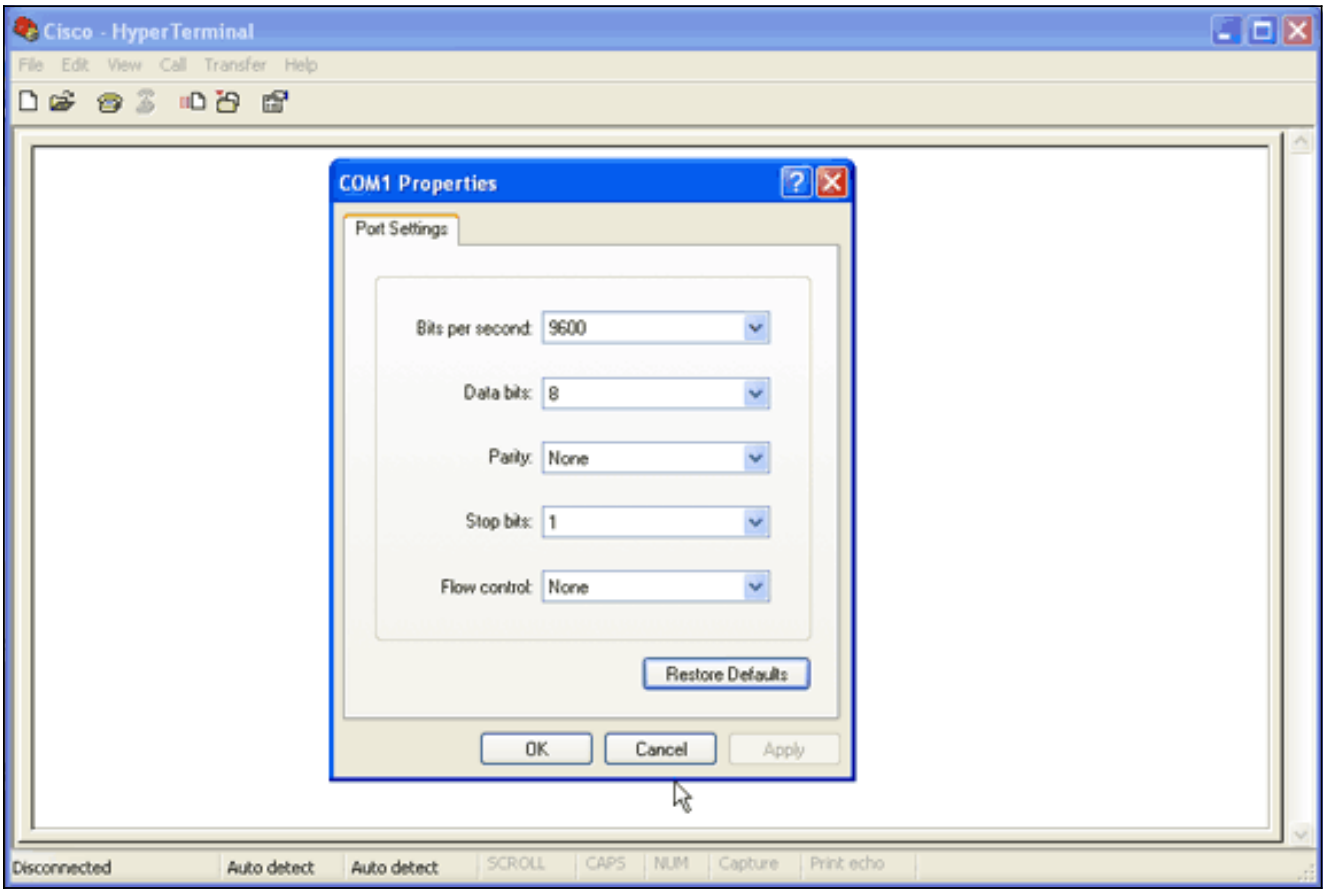
1. لفتح HyperTerminal، أختر **Start (ابدأ) > Programs (البرامج) > System Tools (أدوات النظام) > Communications > HyperTerminal**.**الشكل 1 - إطلاق HyperTerminal**



2. عند فتح HyperTerminal، أكمل الخطوات التالية:أدخل اسما للاتصال.أختر أيقونة.وانقر فوق **OK**.
3. لاتصالات Telnet، أكمل الخطوات التالية:من قائمة الاتصال باستخدام القائمة المنسدلة، أختر **TCP/IP**.أدخل عنوان IP الخاص بالجهاز حيث تريد تشغيل تصحيح الأخطاء.وانقر فوق **OK**.**شكل 2 - اتصال Telnet**

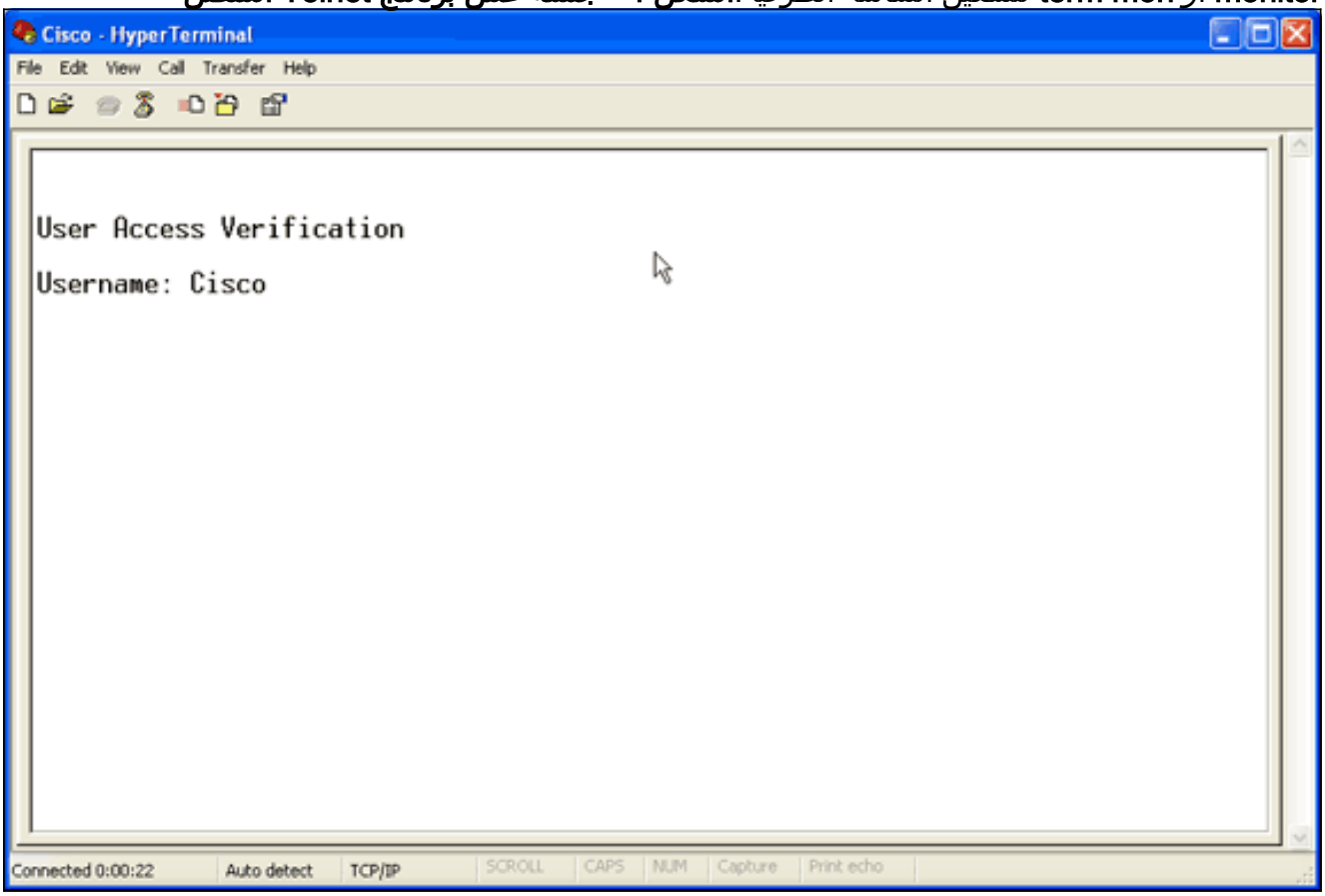


4. لاتصالات وحدة التحكم، أكمل الخطوات التالية:من قائمة الاتصال باستخدام القائمة المنسدلة، أختر منفذ COM حيث يتم توصيل كبل وحدة التحكم.وانقر فوق **OK**.تظهر صفحة الخصائص الخاصة بالاتصال.قم بتعيين سرعة الاتصال بمنفذ وحدة التحكم.طقطقت in order to أحيات التقصير ميناء عملية إعداد، **إستعادة تقصير.ملاحظة:** تتبع معظم منتجات Cisco إعدادات المنفذ الافتراضية.إعدادات المنفذ الافتراضية هي:بت في الثانية - 9600وحدات بت البيانات—8الندية—بلاإيقاف البت—1التحكم في التدفق — لا شيء**الشكل 3 - خصائص COM1**

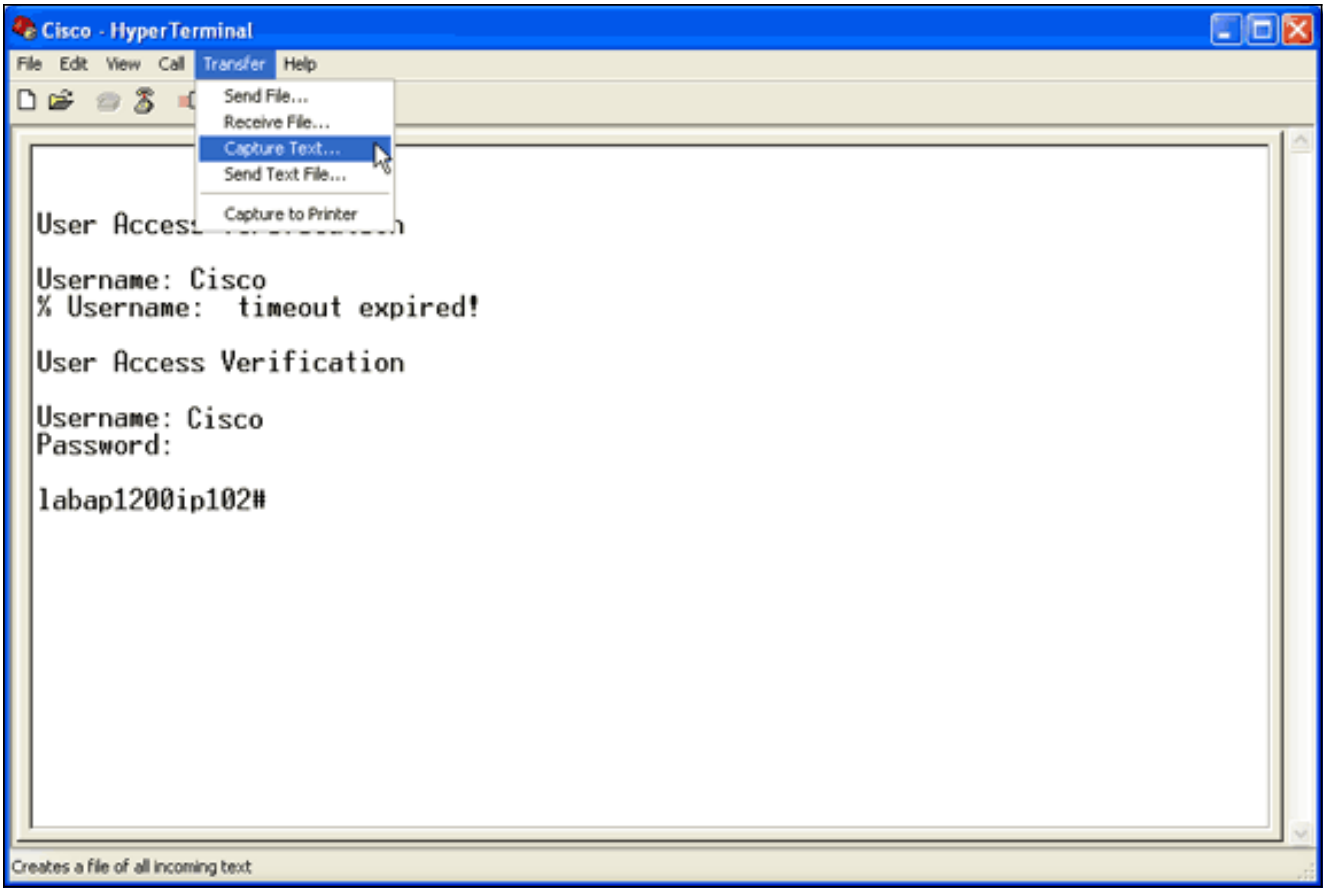


عند هذه النقطة، يؤسس Telnet أو وحدة طرفية للتحكم اتصال، وأنت حضضت على اسم مستخدم وكلمة مرور.**ملاحظة:** تعين أجهزة Cisco Aironet كلا من اسم المستخدم الافتراضي وكلمة المرور ل *Cisco* (حساس لحالة الأحرف).

5. لتشغيل تصحيح الأخطاء، أكمل الخطوات التالية:أصدرت **ال enable** أمر in order to دخلت أسلوب ذو امتياز.دخلت ال enable كلمة.**ملاحظة:** تذكر أن كلمة المرور الافتراضية لمعدات Aironet هي *Cisco* (حساس لحالة الأحرف).**ملاحظة:** لعرض مخرجات تصحيح الأخطاء من جلسة عمل Telnet، أستخدم الأمر **terminal monitor** أو **term mon** لتشغيل الشاشة الطرفية.**الشكل 4 - جلسة عمل برنامج Telnet المتصل**

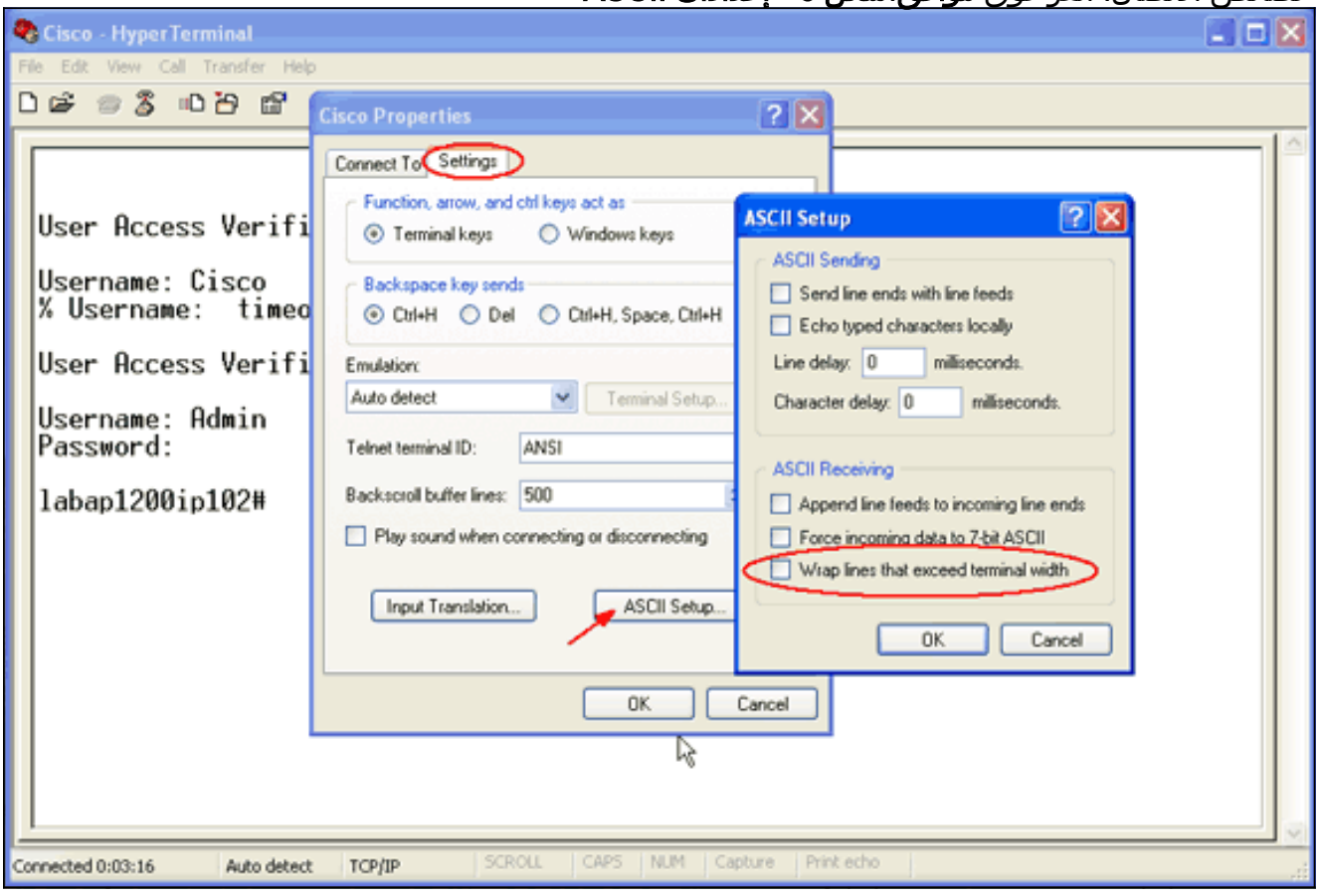


6. بعد إنشاء اتصال، أكمل الخطوات التالية لتجميع التقاط شاشة:أختر **التقاط نص** من قائمة النقل.**الشكل 5 - حفظ التقاط الشاشة**



عندما تفتح شاشة تطلب منك اسم ملف للإخراج، قم بإدخال اسم ملف.

7. أتمت هذا steps in order to أعجزت الشاشة التفاف:**ملاحظة:** يمكنك قراءة تصحيح الأخطاء بسهولة أكبر عندما تقوم بتعطيل التفاف الشاشة.من قائمة HyperTerminal، أختر **ملف**.أختر **الخصائص**.في صفحة خصائص التوصيل، انقر على علامة التبويب **إعدادات**.انقر على **إعداد ASCII**.قم بإلغاء تحديد **خطوط الالتفاف التي تتجاوز عرض الوحدة الطرفية**.طقطقت in order to أغلقت ال ascii عملية إعداد، **ok**.لإغلاق صفحة خصائص الاتصال، انقر فوق **موافق**.**شكل 6 - إعدادات ASCII**



الآن بعد أن أصبح بإمكانك التقاط أي مخرج شاشة إلى ملف نصي، فإن تصحيح الأخطاء التي تقوم بتشغيلها تعتمد على ما يتم التفاوض عليه. تصف الأقسام التالية من هذا المستند نوع الاتصال الذي تم التفاوض عليه بواسطة تصحيح الأخطاء.

EAP

تكون هذه الأخطاء هي الأكثر فائدة لمصادقة EAP:

- **debug radius authentication**—تبدأ مخرجات هذا تصحيح الأخطاء بهذه الكلمة: RADIUS.
- **عملية مصدق debug dot11 aaa**— تبدأ مخرجات تصحيح الأخطاء هذا بهذا النص: _dot11_auth_dot1x.
- يبدأ **debug dot11 aaa authenticator state-machine**—تبدأ مخرجات تصحيح الأخطاء هذا مع هذا النص: dot11_auth_dot1x_run_rfsm.

تظهر هذه الأخطاء:

- ما يتم الإبلاغ عنه أثناء أجزاء RADIUS من مربع حوار المصادقة
- الإجراءات التي يتم إتخاذها أثناء حوار المصادقة هذا
- الحالات المختلفة التي يتم من خلالها تحويل حوار المصادقة

يوضح هذا المثال مصادقة EAP خفيفة (LEAP) ناجحة:

مثال مصادقة EAP الناجحة

```
Apr  8 17:45:48.208: dot11_auth_dot1x_start: in the
                                dot11_auth_dot1x_start
                                  Apr  8 17:45:48.208:
                :dot11_auth_dot1x_send_id_req_to_client
   sending identity request for 0002.8aa6.304f Apr 8
  17:45:48.208: dot11_auth_dot1x_send_id_req_to_client:
          Started timer client_timeout 30 seconds Apr 8
    17:45:48.210: dot11_auth_parse_client_pak: Received
   EAPOL packet from 0002.8aa6.304f Apr 8 17:45:48.210:
                   dot11_auth_dot1x_run_rfsm: Executing
      Action(CLIENT_WAIT,EAP_START) for 0002.8aa6.304f
                                  Apr  8 17:45:48.210:
                :dot11_auth_dot1x_send_id_req_to_client
   sending identity request for 0002.8aa6.304f Apr 8
  17:45:48.210: dot11_auth_dot1x_send_id_req_to_client:
          Started timer client_timeout 30 seconds Apr 8
    17:45:48.212: dot11_auth_parse_client_pak: Received
   EAPOL packet from 0002.8aa6.304f Apr 8 17:45:48.212:
   dot11_auth_parse_client_pak: id is not matching req-
id:1resp-id:2, waiting for response Apr 8 17:45:48.213:
dot11_auth_parse_client_pak: Received EAPOL packet from
                     0002.8aa6.304f Apr 8 17:45:48.213:
                   dot11_auth_dot1x_run_rfsm: Executing
    Action(CLIENT_WAIT,CLIENT_REPLY) for 0002.8aa6.304f
                                  Apr  8 17:45:48.214:
             :dot11_auth_dot1x_send_response_to_server
 Sending client 0002.8aa6.304f data to server Apr 8
17:45:48.214: dot11_auth_dot1x_send_response_to_server:
           tarted timer server_timeout 60 seconds Apr 8
   17:45:48.214: RADIUS: AAA Unsupported [248] 14 Apr 8
 17:45:48.214: RADIUS: 6C 61 62 61 70 31 32 30 30 69 70
      31 [labap1200ip1] Apr 8 17:45:48.215: RADIUS: AAA
                Unsupported [150] 2 Apr 8 17:45:48.215:
   RADIUS(0000001C): Storing nasport 17 in rad_db Apr 8
        17:45:48.215: RADIUS(0000001C): Config NAS IP:
```

```
10.0.0.102 Apr 8 17:45:48.215: RADIUS/ENCODE(0000001C):
                acct_session_id: 28 Apr 8 17:45:48.216:
      RADIUS(0000001C): Config NAS IP: 10.0.0.102 Apr 8
          17:45:48.216: RADIUS(0000001C): sending Apr 8
 17:45:48.216: RADIUS(0000001C): Send Access-Request to
 10.0.0.3:1645 id 21645/93, len 139 Apr 8 17:45:48.216:
RADIUS: authenticator 92 26 A8 31 ED 60 6A 88 - 84 8C 80
B2 B8 26 4C 04 Apr 8 17:45:48.216: RADIUS: User-Name [1]
 9 "aironet" Apr 8 17:45:48.216: RADIUS: Framed-MTU [12]
    6 1400 Apr 8 17:45:48.217: RADIUS: Called-Station-Id
    [30] 16 "0005.9a39.0374" Apr 8 17:45:48.217: RADIUS:
       Calling-Station-Id [31] 16 "0002.8aa6.304f" Apr 8
17:45:48.217: RADIUS: Service-Type [6] 6 Login [1] Apr 8
 17:45:48.217: RADIUS: Message-Authenticato[80] 18 * Apr
      8 17:45:48.217: RADIUS: EAP-Message [79] 14 Apr 8
 17:45:48.218: RADIUS: 02 02 00 0C 01 61 69 72 6F 6E 65
 74 [?????aironet] Apr 8 17:45:48.218: RADIUS: NAS-Port-
    Type [61] 6 802.11 wireless [19] Apr 8 17:45:48.218:
   RADIUS: NAS-Port [5] 6 17 Apr 8 17:45:48.218: RADIUS:
     NAS-IP-Address [4] 6 10.0.0.102 Apr 8 17:45:48.218:
   RADIUS: Nas-Identifier [32] 16 "labap1200ip102" Apr 8
         17:45:48.224: RADIUS: Received from id 21645/93
           10.0.0.3:1645, Access-Challenge, len 69 Apr 8
17:45:48.224: RADIUS: authenticator C8 6D 9B B3 67 60 44
29 - CC AB 39 DE 00 A9 A8 CA Apr 8 17:45:48.224: RADIUS:
EAP-Message [79] 25 Apr 8 17:45:48.224: RADIUS: 01 43 00
                17 11 01 00 08 63 BB E7 8C 0F AC EB 9A
 [?C??????c???????] Apr 8 17:45:48.225: RADIUS: 61 69 72
      6F 6E 65 74 [aironet] Apr 8 17:45:48.225: RADIUS:
   Session-Timeout [27] 6 20 Apr 8 17:45:48.225: RADIUS:
       Message-Authenticato[80] 18 * Apr 8 17:45:48.226:
       RADIUS(0000001C): Received from id 21645/93 Apr 8
 17:45:48.226: RADIUS/DECODE: EAP-Message fragments, 23,
                      total 23 bytes Apr 8 17:45:48.226:
        dot11_auth_dot1x_parse_aaa_resp: Received server
    response: GET_CHALLENGE_RESPONSE Apr 8 17:45:48.226:
dot11_auth_dot1x_parse_aaa_resp: found eap pak in server
                            response Apr 8 17:45:48.226:
  dot11_auth_dot1x_parse_aaa_resp: found session timeout
   20 sec Apr 8 17:45:48.227: dot11_auth_dot1x_run_rfsm:
          Executing Action(SERVER_WAIT,SERVER_REPLY) for
                                        0002.8aa6.304f
                                   Apr  8 17:45:48.227:
              :dot11_auth_dot1x_send_response_to_client
  Forwarding server message to client 0002.8aa6.304f
                                   Apr 8 17:45:48.227:
 dot11_auth_dot1x_send_response_to_client: Started timer
          client_timeout 20 seconds Apr 8 17:45:48.232:
 dot11_auth_parse_client_pak: Received EAPOL packet from
                      0002.8aa6.304f Apr 8 17:45:48.232:
            dot11_auth_dot1x_run_rfsm: Executing Action
          (CLIENT_WAIT,CLIENT_REPLY) for 0002.8aa6.304f
                                   Apr  8 17:45:48.232:
              :dot11_auth_dot1x_send_response_to_server
  Sending client 0002.8aa6.304f data to server Apr 8
 17:45:48.232: dot11_auth_dot1x_send_response_to_server:
          Started timer server_timeout 60 seconds Apr 8
   17:45:48.233: RADIUS: AAA Unsupported [248] 14 Apr 8
 17:45:48.234: RADIUS: 6C 61 62 61 70 31 32 30 30 69 70
      31 [labap1200ip1] Apr 8 17:45:48.234: RADIUS: AAA
                Unsupported [150] 2 Apr 8 17:45:48.234:
     RADIUS(0000001C): Using existing nas_port 17 Apr 8
         17:45:48.234: RADIUS(0000001C): Config NAS IP:
 10.0.0.102 Apr 8 17:45:48.234: RADIUS/ENCODE(0000001C):
```

acct_session_id: 28 Apr 8 17:45:48.234: RADIUS(0000001C): Config NAS IP: 10.0.0.102 Apr 8 17:45:48.234: RADIUS(0000001C): sending Apr 8 17:45:48.234: RADIUS(0000001C): Send Access-Request to 10.0.0.3:1645 id 21645/94, len 166 Apr 8 17:45:48.235: RADIUS: authenticator 93 B5 CC B6 41 97 A0 85 - 1B 4D 13 0F 6A EE D4 11 Apr 8 17:45:48.235: RADIUS: User-Name [1] 9 "aironet" Apr 8 17:45:48.235: RADIUS: Framed-MTU [12] 6 1400 Apr 8 17:45:48.236: RADIUS: Called-Station-Id [30] 16 "0005.9a39.0374" Apr 8 17:45:48.236: RADIUS: Calling-Station-Id [31] 16 "0002.8aa6.304f" Apr 8 17:45:48.236: RADIUS: Service-Type [6] 6 Login [1] Apr 8 17:45:48.236: RADIUS: Message-Authenticato[80] 18 * Apr 8 17:45:48.236: RADIUS: EAP-Message [79] 41 Apr 8 17:45:48.236: RADIUS: 02 43 00 27 11 01 00 18 30 9F 55 AF 05 03 71 7D [?C?'????0?U???q}] Apr 8 17:45:48.236: RADIUS: 25 41 1B B0 F4 A9 7C EE F5 51 24 9A FC 6D 51 6D [?A????|??Q$??mQm] Apr 8 17:45:48.237: RADIUS: 61 69 72 6F 6E 65 74 [aironet] Apr 8 17:45:48.237: RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19] Apr 8 17:45:48.237: RADIUS: NAS-Port [5] 6 17 Apr 8 17:45:48.238: RADIUS: NAS-IP-Address [4] 6 10.0.0.102 Apr 8 17:45:48.238: RADIUS: Nas-Identifier [32] 16 "labap1200ip102" Apr 8 17:45:48.242: RADIUS: Received from id 21645/94 10.0.0.3:1645, Access-Challenge, len 50 Apr 8 17:45:48.243: RADIUS: authenticator 59 2D EE 24 CF B2 87 AF - 86 D0 C9 00 79 BE 6E 1E Apr 8 17:45:48.243: RADIUS: EAP-Message [79] 6 Apr 8 17:45:48.243: RADIUS: 03 43 00 04 [?C??] Apr 8 17:45:48.244: RADIUS: Session-Timeout [27] 6 20 Apr 8 17:45:48.244: RADIUS: Message-Authenticato[80] 18 * Apr 8 17:45:48.244: RADIUS(0000001C): Received from id 21645/94 Apr 8 17:45:48.244: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes Apr 8 17:45:48.244: dot11_auth_dot1x_parse_aaa_resp: *Received server response: GET_CHALLENGE_RESPONSE* Apr 8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp: found eap pak in server response Apr 8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp: found session timeout 20 sec Apr 8 17:45:48.245: dot11_auth_dot1x_run_rfsm: (Executing Action(**SERVER_WAIT,SERVER_REPLY** for 0002.8aa6.304f Apr 8 17:45:48.245: :dot11_auth_dot1x_send_response_to_client *Forwarding server message to client 0002.8aa6.304f* Apr 8 17:45:48.246: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 20 seconds Apr 8 17:45:48.249: dot11_auth_parse_client_pak: Received EAPOL packet from 0002.8aa6.304f Apr 8 17:45:48.250: dot11_auth_dot1x_run_rfsm: Executing Action(**CLIENT_WAIT,CLIENT_REPLY**) for 0002.8aa6.304f Apr 8 17:45:48.250: :dot11_auth_dot1x_send_response_to_server *Sending client 0002.8aa6.304f data to server* Apr 8 17:45:48.250: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds Apr 8 17:45:48.250: RADIUS: AAA Unsupported [248] 14 Apr 8 17:45:48.251: RADIUS: 6C 61 62 61 70 31 32 30 30 69 70 31 [labap1200ip1] Apr 8 17:45:48.251: RADIUS: AAA Unsupported [150] 2 Apr 8 17:45:48.251: RADIUS(0000001C): Using existing nas_port 17 Apr 8 17:45:48.252: RADIUS(0000001C): Config NAS IP: 10.0.0.102 Apr 8 17:45:48.252: RADIUS/ENCODE(0000001C):

acct_session_id: 28 Apr 8 17:45:48.252:
RADIUS(0000001C): Config NAS IP: 10.0.0.102 Apr 8
17:45:48.252: RADIUS(0000001C): sending Apr 8
17:45:48.252: RADIUS(0000001C): Send Access-Request to
10.0.0.3:1645 id 21645/95, len 150 Apr 8 17:45:48.252:
RADIUS: authenticator 39 1C A5 EF 86 9E BA D1 - 50 FD 58
80 A8 8A BC 2A Apr 8 17:45:48.253: RADIUS: User-Name [1]
9 "aironet" Apr 8 17:45:48.253: RADIUS: Framed-MTU [12]
6 1400 Apr 8 17:45:48.253: RADIUS: Called-Station-Id
[30] 16 "0005.9a39.0374" Apr 8 17:45:48.253: RADIUS:
Calling-Station-Id [31] 16 "0002.8aa6.304f" Apr 8
17:45:48.254: RADIUS: Service-Type [6] 6 Login [1] Apr 8
17:45:48.254: RADIUS: Message-Authenticato[80] 18 * Apr
8 17:45:48.254: RADIUS: EAP-Message [79] 25 Apr 8
17:45:48.254: RADIUS: 01 43 00 17 11 01 00 08 50 9A 67
2E 7D 26 75 AA [?C??????P?g.}&u?] Apr 8 17:45:48.254:
RADIUS: 61 69 72 6F 6E 65 74 [aironet] Apr 8
17:45:48.254: RADIUS: NAS-Port-Type [61] 6 802.11
wireless [19] Apr 8 17:45:48.254: RADIUS: NAS-Port [5] 6
17 Apr 8 17:45:48.255: RADIUS: NAS-IP-Address [4] 6
10.0.0.102 Apr 8 17:45:48.255: RADIUS: Nas-Identifier
[32] 16 "labap1200ip102" Apr 8 17:45:48.260: RADIUS:
Received from id 21645/95 10.0.0.3:1645, Access-Accept,
len 206 Apr 8 17:45:48.260: RADIUS: authenticator 39 13
3C ED FC 02 68 63 - 24 13 1B 46 CF 93 B8 E3 Apr 8
17:45:48.260: RADIUS: Framed-IP-Address [8] 6
255.255.255.255 Apr 8 17:45:48.261: RADIUS: EAP-Message
[79] 41 Apr 8 17:45:48.261: RADIUS: 02 00 00 27 11 01 00
18 FA 53 D0 29 6C 9D 66 8E [???'?????S?)l?f?] Apr 8
17:45:48.262: RADIUS: C4 A3 CD 54 08 8C 35 7C 74 0C 6A
EF D4 6D 30 A4 [???T??5|t?j??m0?] Apr 8 17:45:48.262:
RADIUS: 61 69 72 6F 6E 65 74 [aironet] Apr 8
17:45:48.262: RADIUS: Vendor, Cisco [26] 59 Apr 8
17:45:48.262: RADIUS: Cisco AVpair [1] 53 "leap:session-
key=G:3asil;mwerAEJNYH-JxI," Apr 8 17:45:48.262: RADIUS:
Vendor, Cisco [26] 31 Apr 8 17:45:48.262: RADIUS: Cisco
AVpair [1] 25 "auth-algo-type=eap-leap" Apr 8
17:45:48.262: RADIUS: Class [25] 31 Apr 8 17:45:48.263:
RADIUS: 43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 64 36
[CISCOACS:00001d6] Apr 8 17:45:48.263: RADIUS: 33 2F 30
61 30 30 30 30 36 36 2F 31 37 [3/0a000066/17] Apr 8
17:45:48.263: RADIUS: Message-Authenticato[80] 18 * Apr
8 17:45:48.264: RADIUS(0000001C): Received from id
21645/95 Apr 8 17:45:48.264: RADIUS/DECODE: EAP-Message
fragments, 39, total 39 bytes Apr 8 17:45:48.264: found
leap session key Apr 8 17:45:48.265:
dot11_auth_dot1x_parse_aaa_resp: *Received server
response: PASS* Apr 8 17:45:48.265:
dot11_auth_dot1x_parse_aaa_resp: *found eap pak in server
response* Apr 8 17:45:48.265:
dot11_auth_dot1x_parse_aaa_resp: *found leap session key
in server response* Apr 8 17:45:48.265:
dot11_auth_dot1x_parse_aaa_resp: leap session key length
16 Apr 8 17:45:48.266: dot11_auth_dot1x_run_rfsm:
Executing Action(**SERVER_WAIT,SERVER_PASS**) for
0002.8aa6.304f
Apr 8 17:45:48.266:
:dot11_auth_dot1x_send_response_to_client
Forwarding server message to client 0002.8aa6.304f
Apr 8 17:45:48.266:
dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 20 seconds Apr 8 17:45:48.266: %DOT11-6-
ASSOC: Interface Dot11Radio0, Station RKIBBE-W2K4
[0002.8aa6.304f Associated KEY_MGMT[NONE

لاحظ التدفق في تصحيح أخطاء . وهناك تقدم عبر العديد من الدول:

1. EAP_Start
2. Client_WAIT
3. _
4. Server_WAIT
5. **ملاحظة:** مع وجود التفاوض بين الاثنين، يمكن أن يكون هناك عدة تكرارات من CLIENT_WAIT وCLIENT_REPLY، بالإضافة إلى SERVER_WAIT وSERVER_REPLY.
6. Server_PASS

يعرض تصحيح أخطاء كل خطوة فردية خلال كل حالة. تظهر تصحيح أخطاء RADIUS المحادثة الفعلية بين خادم المصادقة والعميل. إن أسهل طريقة للعمل مع تصحيح أخطاء EAP هي مراقبة تطور رسائل آلة الحالة خلال كل حالة.

وعندما يفشل شيء ما في التفاوض، تظهر تصحيح أخطاء سبب توقف العملية. شاهد الرسائل المماثلة لهذه الأمثلة:

- - تشير هذه الحالة إلى أن العميل لم يستجب خلال فترة زمنية مناسبة. قد يحدث هذا الفشل في الاستجابة لأحد هذه الأسباب:توجد مشكلة في برنامج العميل.انتهت صلاحية قيمة مهلة عميل EAP (من علامة التبويب الفرعية لمصادقة EAP تحت الأمان المتقدم).بعض EAP، خاصة EAP المحمي (PEAP)، يستغرق أكثر من 30 ثانية لإكمال المصادقة. قم بتعيين هذا المؤقت إلى قيمة أعلى (بين 90 و 120 ثانية).هذا مثال على محاولة :**ملاحظة:** مراقبة أي رسائل خطأ نظام مماثلة لهذه الرسالة:

```
DOT11-4-MAXRETRIES: Packet to client xxxx.xxxx.xxxx reached%
                    max retries, removing the client
```

ملاحظة: يمكن أن تشير رسائل الخطأ هذه إلى مشكلة في تردد الراديو (RF).
- **عدم تطابق سري مشترك بين نقطة الوصول وخادم RADIUS**—في سجل المثال هذا، لا يقبل خادم RADIUS طلب المصادقة من نقطة الوصول. تستمر نقطة الوصول في إرسال الطلب إلى خادم RADIUS، ولكن خادم RADIUS يرفض الطلب لأن السر المشترك غير متطابق.لحل هذه المشكلة، تأكد من أن السر المشترك على نقطة الوصول هو نفسه المستخدم في خادم RADIUS.
- **server_timeout** — تشير هذه الحالة إلى أن خادم المصادقة لم يستجب خلال فترة زمنية مناسبة. يحدث هذا الفشل في الاستجابة بسبب مشكلة على الخادم. تحقق من صحة هذه الحالات:تحتوي نقطة الوصول على اتصال IP بخادم المصادقة.**ملاحظة:** يمكنك إستخدام الأمر **ping** للتحقق من الاتصال.أرقام منافذ المصادقة والمحاسبة صحيحة للخادم.**ملاحظة:** يمكنك التحقق من أرقام المنافذ من علامة التبويب "مدير الخادم".خدمة المصادقة قيد التشغيل وتعمل.هذا مثال على محاولة server_timeout:
- **server_fail** — تشير هذه الحالة إلى أن الخادم قدم إستجابة مصادقة غير ناجحة بناء على مسوغات المستخدم. يظهر تصحيح RADIUS الذي يسبق هذا الفشل اسم المستخدم الذي تم تقديمه إلى خادم المصادقة. تأكد من التحقق من سجل "المحاولات الفاشلة" في خادم المصادقة للحصول على تفاصيل إضافية حول سبب رفض الخادم لوصول العميل.هذا مثال على محاولة server_fail:
- **لا توجد إستجابة من العميل**—في هذا المثال، يرسل خادم RADIUS رسالة مرور إلى نقطة الوصول التي تقوم نقطة الوصول بتوجيهها ثم تقوم بعد ذلك بالاتصال بالعميل. لا يستجيب العميل لنقطة الوصول في نهاية المطاف. لذلك، يصادق ال ap هو بعد أن يصل إلى الحد الأقصى إعادة محاولة.تقوم نقطة الوصول بإعادة توجيه إستجابة التحدي من نصف القطر إلى العميل. لا يستجيب العميل ويبلغ الحد الأقصى لعمليات إعادة المحاولة التي تتسبب في فشل EAP والنقطة الوصول لإلغاء مصادقة العميل.يرسل RADIUS رسالة مرور إلى نقطة الوصول، ويرسل نقطة الوصول رسالة المرور إلى العميل، ولا يستجيب العميل. تقوم نقطة الوصول بإلغاء مصادقتها بعد وصولها إلى الحد الأقصى من عمليات إعادة المحاولة. بعد ذلك يحاول العميل طلب هوية جديد إلى نقطة الوصول، ولكن نقطة الوصول ترفض هذا الطلب لأن العميل قد وصل بالفعل إلى الحد الأقصى من عمليات إعادة المحاولة.

تظهر عمليات تصحيح أخطاء و/أو radius التي *تسبق* مباشرة رسالة جهاز الحالة تفاصيل الفشل.

أحلت ل كثير معلومة على كيف أن يشكل EAP، EAP صحة هوية مع RADIUS نادل.

مصادقة MAC

تعد عمليات تصحيح الأخطاء هذه الأكثر فائدة لمصادقة MAC:

- **debug radius authentication**—عند إستخدام خادم مصادقة خارجي، تبدأ مخرجات هذا تصحيح الأخطاء بهذه الكلمة: RADIUS.
- يبدأ **debug dot11 aaa authenticator mac-authen**— مخرجات تصحيح الأخطاء هذا مع هذا النص: _dot11_auth_dot1x.

تظهر هذه الأخطاء:

- ما يتم الإبلاغ عنه أثناء أجزاء RADIUS من مربع حوار المصادقة
- المقارنة بين عنوان MAC الذي يتم توفيره وعنوان MAC الذي تتم مصادقته مقابل

عند إستخدام خادم RADIUS خارجي مع مصادقة عنوان MAC، يتم تطبيق تصحيح أخطاء RADIUS. تتمثل نتيجة هذا الاقتران في عرض المحادثة الفعلية بين خادم المصادقة والعميل.

عندما يتم إنشاء قائمة من عناوين MAC محليا إلى الجهاز كقاعدة بيانات اسم مستخدم وكلمة مرور، تظهر فقط تصحيح أخطاء **MAC-authen** المخرجات. عندما يتم تحديد مطابقة العنوان أو عدم تطابق، يتم عرض هذه المخرجات.

ملاحظة: أدخل دائما أي حروف أبجدية في عنوان MAC في الحروف الصغيرة.

توضح هذه الأمثلة مصادقة MAC ناجحة مقابل قاعدة بيانات محلية:

مثال مصادقة MAC الناجح

```
Apr  8 19:02:00.109: dot11_auth_mac_start: method_list:
                                                mac_methods
Apr  8 19:02:00.109: dot11_auth_mac_start: method_index:
                                    0x4500000B, req: 0xA7626C
     Apr  8 19:02:00.109: dot11_auth_mac_start: client-
                                        >unique_id: 0x28
Apr  8 19:02:00.110: dot11_mac_process_reply: AAA reply
                                    for 0002.8aa6.304f PASSED
         Apr  8 19:02:00.145: %DOT11-6-ASSOC: Interface
                          Dot11Radio0, Station RKIBBE-W2K4
            [0002.8aa6.304f Associated KEY_MGMT[NONE
```

توضح هذه الأمثلة مصادقة MAC فاشلة مقابل قاعدة بيانات محلية:

فشل مثال مصادقة MAC

```
Apr  8 19:01:22.336: dot11_auth_mac_start: method_list:
                                                mac_methods
Apr  8 19:01:22.336: dot11_auth_mac_start: method_index:
                                                ,0x4500000B
                                        req: 0xA7626C
     Apr  8 19:01:22.336: dot11_auth_mac_start: client-
                                        >unique_id: 0x27
          :Apr  8 19:01:22.337: dot11_mac_process_reply
                AAA reply for 0002.8aa6.304f FAILED
            :Apr  8 19:01:22.337: %DOT11-7-AUTH_FAILED
        Station 0002.8aa6.304f Authentication failed
```

عندما تفشل مصادقة عنوان MAC، تحقق من دقة الحروف التي يتم إدخالها في عنوان MAC. تأكد من أنك قمت بإدخال أي حروف هجائية في عنوان MAC في الحروف الصغيرة.

لمزيد من المعلومات حول كيفية تكوين مصادقة MAC، ارجع إلى تكوين أنواع المصادقة (دليل تكوين برنامج Cisco IOS لنقاط الوصول Cisco Aironet، 12.2(13)JA).

WPA

على الرغم من أن وصول Wi-Fi المحمي (WPA) ليس نوع مصادقة، إلا أنه بروتوكول يخضع للتفاوض.

- يفاوض WPA بين نقطة الوصول وبطاقة العميل.
- تتفاوض إدارة مفتاح WPA بعد مصادقة العميل بنجاح بواسطة خادم مصادقة.
- يفاوض WPA كلا من مفتاح Pairwise المؤقت (PTK) ومفتاح GroupWise المؤقت (GTK) في مصافحة رباعية الإتجاه.

ملاحظة: لأن WPA يتطلب نجاح EAP الأساسي، تحقق من أن العملاء يمكنهم المصادقة بنجاح مع EAP هذا قبل الدخول في WPA.

هذه الأخطاء هي الأكثر فائدة لمفاوضات WPA:

- **عملية مصدق debug dot11 aaa**— تبدأ مخرجات تصحيح الأخطاء هذا بهذا النص: `_dot11_auth_dot1x`.
- يبدأ **debug dot11 aaa authenticator state-machine**—تبدأ مخرجات تصحيح الأخطاء هذا مع هذا النص: `.dot11_auth_dot1x_run_rfsm`

بالنسبة للمصادقة الأخرى في هذا المستند، تكون تصحيح أخطاء WPA سهلة القراءة والتحليل. ينبغي إرسال رسالة PTK واستلام رد مناسب. وبعد ذلك، ينبغي إرسال رسالة GTK واستلام رد مناسب آخر.

إن لا يرسل ال PTK أو GTK رسالة، التشكيل أو برمجية مستوى على ال ap يستطيع كنت على خطأ. إذا لم يتم إستلام استجابات PTK أو GTK من العميل، فتحقق من التكوين أو مستوى البرنامج على طالب WPA لبطاقة العميل.

مثال تفاوض WPA الناجح

```
labap1200ip102#
:Apr  7 16:29:57.908: dot11_dot1x_build_ptk_handshake
        building PTK msg 1 for 0030.6527.f74a
:Apr  7 16:29:59.190: dot11_dot1x_verify_ptk_handshake
      verifying PTK msg 2 from 0030.6527.f74a
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header:
                                                  :Warning
       Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header:
                                                  :Warning
          (Invalid key len (exp=0x20, act=0x0
:Apr  7 16:29:59.192: dot11_dot1x_build_ptk_handshake
        building PTK msg 3 for 0030.6527.f74a
:Apr  7 16:29:59.783: dot11_dot1x_verify_ptk_handshake
      verifying PTK msg 4 from 0030.6527.f74a
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header:
                                                  :Warning
       Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header:
                                                  :Warning
          (Invalid key len (exp=0x20, act=0x0
:Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake
        building GTK msg 1 for 0030.6527.f74a
:Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake
     dot11_dot1x_get_multicast_key len 32 index 1
      :Apr  7 16:29:59.788: dot11_dot1x_hex_dump: GTK
CA 88 7D 03 D9 C4 61 FD 4B BE 71 EC F7 43 B5 82 27
                                                93 57 83
:Apr  7 16:30:01.633: dot11_dot1x_verify_gtk_handshake
      verifying GTK msg 2 from 0030.6527.f74a
:Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header
  Warning: Invalid key info (exp=0x391, act=0x301
```

```
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header:
                                                  :Warning
                (Invalid key len (exp=0x20, act=0x0
Apr  7 16:30:01.633: %DOT11-6-ASSOC: Interface
                                                 ,Dot11Radio0
[Station  0030.6527.f74a Associated KEY_MGMT[WPA
                                               labap1200ip102#
```

أحلت ل كثير معلومة على كيف أن يشكل WPA، WPA تشكيل نظرة عامة.

المصادقة الإدارية/HTTP

يمكنك تقييد الوصول الإداري إلى الجهاز للمستخدمين المدرجين في قاعدة بيانات اسم مستخدم وكلمة مرور محلية أو في خادم مصادقة خارجي. ويتم دعم الوصول الإداري باستخدام كل من RADIUS وTACACS+.

تعد عمليات تصحيح الأخطاء هذه الأكثر فائدة للمصادقة الإدارية:

- **تصحيح أخطاء مصادقة** RADIUS أو **تصحيح أخطاء مصادقة tacacs**—تبدأ مخرجات تصحيح الأخطاء هذا بإحدى هذه الكلمات: RADIUS أو TACACS.
- **تصحيح أخطاء المصادقة والتفويض والمحاسبة** (AAA)—تبدأ مخرجات تصحيح الأخطاء هذا بالنص: AAA/AUTHEN.
- **تفويض تصحيح الأخطاء AAA**—تبدأ مخرجات تصحيح الأخطاء هذا بهذا النص: AAA/AUTHOR.

تظهر هذه الأخطاء:

- ما يتم الإبلاغ عنه أثناء أجزاء RADIUS أو TACACS من مربع حوار المصادقة
- المفاوضات الفعلية للمصادقة والتفويض بين الجهاز وخادم المصادقة

يوضح هذا المثال مصادقة إدارية ناجحة عند تعيين سمة RADIUS على Administrative:

مثال المصادقة الإدارية الناجح مع سمة نوع الخدمة

```
Apr 13 19:43:08.030: AAA: parse name=tty2 idb type=-1
                                                  tty=-1
Apr 13 19:43:08.030: AAA: name=tty2 flags=0x11 type=5
                                       shelf=0 slot=0
                          adapter=0 port=2 channel=0
 Apr 13 19:43:08.031: AAA/MEMORY: create_user (0xA1BB6C)
                                'user='NULL' ruser='NULL
             ds0=0 port='tty2' rem_addr='10.0.0.25'
                          authen_type=ASCII service=LOGINN
    Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540):
                                                'port='tty2
                  list='' action=LOGIN service=LOGIN
    Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540):
                                      using "default" list
    :(Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540
     Method=tac_admin (tacacs+) Apr 13 19:43:08.032:
TAC+: send AUTHEN/START packet ver=192 id=3200017540 Apr
   13 19:43:08.032: AAA/AUTHEN(3200017540): Status=ERROR
     Apr 13 19:43:08.032: AAA/AUTHEN/START (3200017540):
          Method=rad_admin (radius) Apr 13 19:43:08.032:
           AAA/AUTHEN(3200017540): Status=GETUSER Apr 13
             19:43:08.032: AAA/AUTHEN/CONT (3200017540):
    continue_login (user='(undef)') Apr 13 19:43:08.032:
           AAA/AUTHEN(3200017540): Status=GETUSER Apr 13
  19:43:08.032: AAA/AUTHEN(3200017540): Method=rad_admin
   (radius) Apr 13 19:43:08.032: AAA/AUTHEN(3200017540):
```

```
Status=GETPASS Apr 13 19:43:08.033: AAA/AUTHEN/CONT
(3200017540): continue_login (user='aironet') Apr 13
19:43:08.033: AAA/AUTHEN(3200017540): Status=GETPASS Apr
13 19:43:08.033: AAA/AUTHEN(3200017540):
Method=rad_admin (radius) Apr 13 19:43:08.033: RADIUS:
Pick NAS IP for u=0xA1BB6C tableid=0 cfg_addr=10.0.0.102
best_addr=0.0.0.0 Apr 13 19:43:08.033: RADIUS: ustruct
sharecount=1 Apr 13 19:43:08.034: Radius:
radius_port_info() success=1 radius_nas_port=1 Apr 13
19:43:08.034: RADIUS(00000000): Send Access-Request to
10.0.0.3:1645 id 21646/48, len 76 Apr 13 19:43:08.034:
RADIUS: authenticator 91 A0 98 87 C1 FC F2 E7 - E7 E4 57
DF 20 D0 82 27 Apr 13 19:43:08.034: RADIUS: NAS-IP-
Address [4] 6 10.0.0.102 Apr 13 19:43:08.034: RADIUS:
NAS-Port [5] 6 2 Apr 13 19:43:08.035: RADIUS: NAS-Port-
Type [61] 6 Virtual [5] Apr 13 19:43:08.035: RADIUS:
User-Name [1] 9 "aironet" Apr 13 19:43:08.035: RADIUS:
Calling-Station-Id [31] 11 "10.0.0.25" Apr 13
19:43:08.035: RADIUS: User-Password [2] 18 * Apr 13
19:43:08.042: RADIUS: Received from id 21646/48
10.0.0.3:1645, Access-Accept, len 62 Apr 13
19:43:08.042: RADIUS: authenticator C9 32 E7 8F 97 5F E6
4C - 6B 90 71 EE ED 2C 2B 2B Apr 13 19:43:08.042:
RADIUS:  Service-Type        [6]   6
[Administrative            [6
Apr 13 19:43:08.042: RADIUS:  Framed-IP-Address   [8]
6   255.255.255.255
Apr 13 19:43:08.042: RADIUS:  Class               [25]
30
Apr 13 19:43:08.043: RADIUS:   43 49 53 43 4F 41 43 53
3A 30 30 30 30 33 36 36
[CISCOACS:0000366]
Apr 13 19:43:08.043: RADIUS:   39 2F 30 61 30 30 30 30
36 36 2F 32
[9/0a000066/2]
Apr 13 19:43:08.044: RADIUS: saved authorization data
for user A1BB6C at B0C260
Apr 13 19:43:08.044: AAA/AUTHEN(3200017540): Status=PASS
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147):
Port='tty2' list='' service=EXEC Apr 13 19:43:08.044:
AAA/AUTHOR/HTTP: tty2(1763745147) user='aironet' Apr 13
19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147): send AV
service=shell Apr 13 19:43:08.044: tty2
AAA/AUTHOR/HTTP(1763745147): send AV cmd* Apr 13
19:43:08.045: tty2 AAA/AUTHOR/HTTP(1763745147): found
list "default" Apr 13 19:43:08.045: tty2
AAA/AUTHOR/HTTP(1763745147): Method=tac_admin (tacacs+)
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147):
user=aironet Apr 13 19:43:08.045: AAA/AUTHOR/TAC+:
(1763745147): send AV service=shell Apr 13 19:43:08.045:
AAA/AUTHOR/TAC+: (1763745147): send AV cmd* Apr 13
19:43:08.046: AAA/AUTHOR (1763745147): Post
authorization status = ERROR Apr 13 19:43:08.046: tty2
AAA/AUTHOR/HTTP(1763745147): Method=rad_admin (radius)
Apr 13 19:43:08.046: AAA/AUTHOR (1763745147): Post
authorization status = PASS_ADD Apr 13 19:43:08.443:
AAA/MEMORY: free_user (0xA1BB6C) user='aironet'
ruser='NULL' port='tty2' rem_addr='10.0.0.25'
authen_type=ASCII service=LOGIN
```

يوضح هذا المثال مصادقة إدارية ناجحة عند إستخدام سمات خاصة بالمورد لإرسال عبارة "priv-level":

مثال المصادقة الإدارية الناجح مع السمة الخاصة بالمورد

```
Apr 13 19:38:04.699: RADIUS: cisco AVPair ""shell:priv-
                                                ""lvl=15
                                not applied for shell
      Apr 13 19:38:04.699: AAA/AUTHOR (380584213): Post
                                     authorization status
                                          PASS_ADD =
  Apr 13 19:38:04.802: AAA/MEMORY: free_user (0xAA0E38)
                                          'user='aironet
      ruser='NULL' port='tty3' rem_addr='10.0.0.25'
                                       authen_type=ASCII
                                       service=LOGIN
  Apr 13 19:38:04.901: AAA: parse name=tty3 idb type=-1
                                                tty=-1
  Apr 13 19:38:04.901: AAA: name=tty3 flags=0x11 type=5
                                       shelf=0 slot=0
                          adapter=0  port=3 channel=0
Apr 13 19:38:04.902: AAA/MEMORY: create_user (0xAA23BC)
                                            'user='NULL
'ruser='NULL' ds0=0 port='tty3' rem_addr='10.0.0.25
                     authen_type=ASCII service=LOGIN
    Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140):
                                     ''=port='tty3' list
                          action=LOGIN service=LOGIN
    Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140):
                                     using "default" list
    Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140):
  Method=tac_admin (tacacs+) Apr 13 19:38:04.902: TAC+:
  send AUTHEN/START packet ver=192 id=1346300140 Apr 13
 19:38:04.902: AAA/AUTHEN(1346300140): Status=ERROR Apr
        13 19:38:04.902: AAA/AUTHEN/START (1346300140):
         Method=rad_admin (radius) Apr 13 19:38:04.902:
          AAA/AUTHEN(1346300140): Status=GETUSER Apr 13
            19:38:04.903: AAA/AUTHEN/CONT (1346300140):
   continue_login (user='(undef)') Apr 13 19:38:04.903:
          AAA/AUTHEN(1346300140): Status=GETUSER Apr 13
 19:38:04.903: AAA/AUTHEN(1346300140): Method=rad_admin
  (radius) Apr 13 19:38:04.904: AAA/AUTHEN(1346300140):
    Status=GETPASS Apr 13 19:38:04.904: AAA/AUTHEN/CONT
   (1346300140): continue_login (user='aironet') Apr 13
19:38:04.904: AAA/AUTHEN(1346300140): Status=GETPASS Apr
               13 19:38:04.904: AAA/AUTHEN(1346300140):
  Method=rad_admin (radius) Apr 13 19:38:04.904: RADIUS:
Pick NAS IP for u=0xAA23BC tableid=0 cfg_addr=10.0.0.102
  best_addr=0.0.0.0 Apr 13 19:38:04.904: RADIUS: ustruct
              sharecount=1 Apr 13 19:38:04.904: Radius:
   radius_port_info() success=1 radius_nas_port=1 Apr 13
  19:38:04.925: RADIUS(00000000): Send Access-Request to
   10.0.0.3:1645 id 21646/3, len 76 Apr 13 19:38:04.926:
RADIUS: authenticator 0C DD 2B B7 CA 5E 7C B9 - 46 90 FD
     7A FD 56 3F 07 Apr 13 19:38:04.926: RADIUS: NAS-IP-
   Address [4] 6 10.0.0.102 Apr 13 19:38:04.926: RADIUS:
 NAS-Port [5] 6 3 Apr 13 19:38:04.926: RADIUS: NAS-Port-
    Type [61] 6 Virtual [5] Apr 13 19:38:04.926: RADIUS:
  User-Name [1] 9 "aironet" Apr 13 19:38:04.926: RADIUS:
          Calling-Station-Id [31] 11 "10.0.0.25" Apr 13
     19:38:04.926: RADIUS: User-Password [2] 18 * Apr 13
          19:38:04.932: RADIUS: Received from id 21646/3
            10.0.0.3:1645, Access-Accept, len 89 Apr 13
19:38:04.933: RADIUS: authenticator FA A4 31 49 51 87 9D
       CA - 9D F7 B3 9B EF C2 8B 7E Apr 13 19:38:04.933:
      RADIUS: Vendor, Cisco [26] 27 Apr 13 19:38:04.933:
      RADIUS:   Cisco AVpair     [1]   21  ""shell:priv-
```

```
                                                        ""lvl=15
  Apr 13 19:38:04.934: RADIUS:  Service-Type        [6]
                                      [6   Login       [1
  Apr 13 19:38:04.934: RADIUS:  Framed-IP-Address   [8]
                                      6   255.255.255.255
 Apr 13 19:38:04.934: RADIUS:  Class               [25]
                                                       30
 Apr 13 19:38:04.934: RADIUS:   43 49 53 43 4F 41 43 53
                                3A 30 30 30 30 33 36 33
                                 [CISCOACS:0000363]
 Apr 13 19:38:04.934: RADIUS:   61 2F 30 61 30 30 30 30
                                              36 36 2F 33
                                    [a/0a000066/3]
    Apr 13 19:38:05.634: AAA/AUTHOR (3854191802): Post
   authorization status = PASS_ADD Apr 13 19:38:05.917:
        AAA/MEMORY: free_user (0xA9D054) user='aironet'
          ruser='NULL' port='tty2' rem_addr='10.0.0.25'
                 authen_type=ASCII service=LOGIN priv=0
```

المشكلة الأكثر شيوعا مع المصادقة الإدارية هي الفشل في تكوين خادم المصادقة لإرسال سمات مستوى الامتياز أو نوع الخدمة الإدارية المناسبة. فشل هذا المثال في المصادقة الإدارية بسبب عدم إرسال سمات مستوى الامتياز أو سمات نوع الخدمة الإدارية:

بدون سمات خاصة بالمورد أو نوع الخدمة

```
 Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065):
                                              'Port='tty3
                                  list='' service=EXEC
 Apr 13 20:02:59.516: AAA/AUTHOR/HTTP: tty3(2007927065)
                                           'user='aironet
 Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065):
                                     send AV service=shell
 Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065):
                                              *send AV cmd
 Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065):
                                       "found list "default
 Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065):
                                 (+Method=tac_admin (tacacs
    Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065):
                                              user=aironet
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send
                                        AV service=shell
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send
                                              *AV cmd
     Apr 13 20:02:59.516: AAA/AUTHOR (2007927065): Post
                              authorization status = ERROR
 Apr 13 20:02:59.517: tty3 AAA/AUTHOR/HTTP(2007927065):
                                 (Method=rad_admin (radius
    Apr 13 20:02:59.517: AAA/AUTHOR (2007927065): Post
                           authorization status = PASS_ADD
  Apr 13 20:02:59.561: AAA/MEMORY: free_user (0xA756E8)
                                           'user='aironet
      ruser='NULL' port='tty2' rem_addr='10.0.0.25'
                                       authen_type=ASCII
                  (service=LOGIN priv=0  vrf= (id=0
  Apr 13 20:02:59.620: AAA/MEMORY: free_user (0x9E5B04)
                                           'user='aironet
     ruser='NULL'  port='tty3' rem_addr='10.0.0.25'
                                       authen_type=ASCII
                   (service=LOGIN priv=0 vrf= (id=0
  Apr 13 20:03:04.501: AAA: parse name=tty2 idb type=-1
                                             tty=-1
```

```
   Apr 13 20:03:04.501: AAA: name=tty2 flags=0x11 type=5
                                  shelf=0 slot=0 adapter=0
                                     port=2 channel=0
 Apr 13 20:03:04.502: AAA/MEMORY: create_user (0xA9C7A4)
                                                  'user='NULL
 ruser='NULL' ds0=0 port='tty2' rem_addr='10.0.0.25'
                                           authen_type=ASCII
                                  service=LOGIN priv=0
      Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642):
                                       ''=port='tty2' list
                            action=LOGIN service=LOGIN
Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642): using
                                              "default" list
      Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642):
                                 (+Method=tac_admin (tacacs
     Apr 13 20:03:04.503: TAC+: send AUTHEN/START packet
                                    ver=192 id=377202642
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=ERROR
      Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642):
                                  (Method=rad_admin (radius
             Apr 13 20:03:04.503: AAA/AUTHEN(377202642):
                                              Status=GETUSER
       Apr 13 20:03:04.503: AAA/AUTHEN/CONT (377202642):
                           ('(continue_login (user='(undef
             Apr 13 20:03:04.503: AAA/AUTHEN(377202642):
                                              Status=GETUSER
             Apr 13 20:03:04.503: AAA/AUTHEN(377202642):
                                  (Method=rad_admin (radius
             Apr 13 20:03:04.503: AAA/AUTHEN(377202642):
                                              Status=GETPASS
       Apr 13 20:03:04.504: AAA/AUTHEN/CONT (377202642):
                           ('continue_login (user='aironet
             Apr 13 20:03:04.504: AAA/AUTHEN(377202642):
                                              Status=GETPASS
             Apr 13 20:03:04.504: AAA/AUTHEN(377202642):
                                  (Method=rad_admin (radius
 Apr 13 20:03:04.504: RADIUS: Pick NAS IP for u=0xA9C7A4
                                                tableid=0
               cfg_addr=10.0.0.102 best_addr=0.0.0.0
      Apr 13 20:03:04.505: RADIUS: ustruct sharecount=1
        Apr 13 20:03:04.505: Radius: radius_port_info()
                               success=1 radius_nas_port=1
    Apr 13 20:03:04.505: RADIUS(00000000): Send Access-
                                  Request to 10.0.0.3:1645
                                    id 21646/59, len 76
 Apr 13 20:03:04.505: RADIUS:  authenticator 0F BD 81 17
                                              8F C5 1C B4
                             1C 66 4D CF D4 96 03 84 -
  Apr 13 20:03:04.505: RADIUS:  NAS-IP-Address      [4]
                                              6   10.0.0.102
  Apr 13 20:03:04.506: RADIUS:  NAS-Port            [5]
                                                    6   2
 Apr 13 20:03:04.506: RADIUS:  NAS-Port-Type       [61]
                                   [6   Virtual           [5
  Apr 13 20:03:04.506: RADIUS:  User-Name           [1]
                                               "9   "aironet
 Apr 13 20:03:04.506: RADIUS:  Calling-Station-Id  [31]
                                           "11  "10.0.0.25
  Apr 13 20:03:04.507: RADIUS:  User-Password       [2]
                                                   *  18
 Apr 13 20:03:04.513: RADIUS: Received from id 21646/59
                                              ,10.0.0.3:1645
                                 Access-Accept, len 56
 Apr 13 20:03:04.513: RADIUS:  authenticator BB F0 18 78
```

```
                                                33 D0 DE D3
                                  8B E9 E0 EE 2A 33 92 B5 -
   Apr 13 20:03:04.513: RADIUS:  Framed-IP-Address   [8]
                                        6   255.255.255.255
  Apr 13 20:03:04.513: RADIUS:  Class               [25]
                                                       30
  Apr 13 20:03:04.514: RADIUS:   43 49 53 43 4F 41 43 53
                                 3A 30 30 30 30 33 36 38
                                  [CISCOACS:0000368]
  Apr 13 20:03:04.514: RADIUS:   33 2F 30 61 30 30 30 30
                                                 36 36 2F 32
                                     [3/0a000066/2]
   Apr 13 20:03:04.515: RADIUS: saved authorization data
                                for user A9C7A4 at A9C99C
 Apr 13 20:03:04.515: AAA/AUTHEN(377202642): Status=PASS
  Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138):
                                     ''=Port='tty2' list
                                        service=EXEC
  Apr 13 20:03:04.515: AAA/AUTHOR/HTTP: tty2(2202245138)
                                          'user='aironet
  Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138):
                                   send AV service=shell
  Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138):
                                           *send AV cmd
  Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138):
                                    "found list "default
  Apr 13 20:03:04.516: tty2 AAA/AUTHOR/HTTP(2202245138):
                                (+Method=tac_admin (tacacs
     Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138):
                                           user=aironet
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send
                                     AV service=shell
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send
                                                 *AV cmd
      Apr 13 20:03:04.517: AAA/AUTHOR (2202245138): Post
                          authorization status = ERROR
  Apr 13 20:03:04.517: tty2 AAA/AUTHOR/HTTP(2202245138):
                                (Method=rad_admin (radius
      Apr 13 20:03:04.517: AAA/AUTHOR (2202245138): Post
                                   authorization status
                                        PASS_ADD =
   Apr 13 20:03:04.619: AAA/MEMORY: free_user (0xA9C7A4)
                                           'user='aironet
       ruser='NULL' port='tty2' rem_addr='10.0.0.25'
                                      authen_type=ASCII
                           =service=LOGIN priv=0 vrf
```

أحلت ل كثير معلومة على كيف أن يشكل صحة هوية إدارية، بدير المنفذ نقطة (cisco ios برمجية تشكيل مرشد ل cisco Aironet نقاط الوصول، JA(13)12.2).

لمزيد من المعلومات حول كيفية تكوين الامتياز الإداري للمستخدمين على خادم المصادقة، ارجع إلى نموذج التكوين: المصادقة المحلية لمستخدمي خادم HTTP. تحقق من المقطع الذي يطابق بروتوكول المصادقة الذي تستخدمه.

معلومات ذات صلة

- دليل تكوين برنامج Cisco IOS Software لنقاط الوصول Cisco Aironet، الإصدار JA(13)12.2
- مصادقة EAP مع خادم RADIUS
- مصادقة LEAP مع خادم RADIUS المحلي
- الأسئلة المتداولة حول Cisco Aironet Wireless Security

- نقطة الوصول Wireless Domain Services AP كمثال لتكوين خادم AAA
- 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).