

# RADIUS مداخل عم EAP ةق داصم

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [EAP للشبكة أو مصادقة مفتوحة باستخدام EAP](#)
- [تعريف خادم المصادقة](#)
- [تحديد أساليب مصادقة العميل](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [إجراء استكشاف الأخطاء وإصلاحها](#)
- [أوامر استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

## المقدمة

يقدم هذا المستند نموذجا لتكوين نقطة وصول تستند إلى Cisco IOS® لمصادقة بروتوكول المصادقة المتوسع (EAP) للمستخدمين اللاسلكيين مقابل قاعدة بيانات يتم الوصول إليها بواسطة خادم RADIUS.

ونظرا للدور السلبي الذي تلعبه نقطة الوصول في EAP (الذي يقوم بجسر الحزم اللاسلكية من العميل إلى الحزم السلكية الموجهة إلى خادم المصادقة، والعكس بالعكس)، يتم استخدام هذا التكوين مع جميع أساليب EAP تقريبا. وتتضمن هذه الأساليب (ولكنها لا تقتصر على) LEAP، و EAP المحمي (PEAP-MS-Challenge Authentication) (CHAP Protocol) الإصدار 2، وبطاقة الرمز المميز العامة (PEAP) (GTC)، والمصادقة المرنة EAP عبر الاتصال النفقي الآمن (FAST)، وأمان طبقة النقل (TLS)، و (EAP-Tunneled TLS) (TTLS). يجب عليك تكوين خادم المصادقة بشكل مناسب لكل من طرق EAP هذه.

يغطي هذا المستند كيفية تكوين نقطة الوصول (AP) وخادم RADIUS، وهو Cisco ACS الآمن في مثال التكوين في هذا المستند.

## المتطلبات الأساسية

### المتطلبات

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

- أنت على دراية بواجهة مستخدم Cisco IOS GUI أو CLI.
- أنت على دراية بالمفاهيم الكامنة وراء مصادقة EAP.

## المكونات المستخدمة

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

- منتجات Cisco Aironet AP التي تعمل بنظام التشغيل Cisco IOS.
- افتراض شبكة LAN افتراضية واحدة فقط (VLAN) في الشبكة.
- منتج خادم مصادقة RADIUS يتم دمج بنجاح في قاعدة بيانات المستخدم. هذه هي خوادم المصادقة المدعومة لكل من Cisco LEAP و EAP-FAST: خادم التحكم في الوصول الآمن (ACS) من Cisco مسجل الوصول (CAR) من Cisco نصف قطر المنحدر الفولاذي يستحق الترابط هذه هي خوادم المصادقة المدعومة الخاصة بالإصدار 2 من Microsoft PEAP-MS-CHAP و PEAP-GTC: خدمة مصادقة الإنترنت من Microsoft (IAS) مصدر المحتوى الإضافي الآمن من Cisco نصف قطر المنحدر الفولاذي يستحق الترابط يمكن أن تخول Microsoft أي خادم مصادقة إضافي. ملاحظة: يتطلب GTC أو كلمات المرور لمرة واحدة خدمات إضافية تتطلب برامج إضافية على كل من العميل والخادم، بالإضافة إلى أجهزة أو مولدات رموز برمجية. راجع مصنع متطلب العميل للحصول على تفاصيل حول خوادم المصادقة المدعومة بمنتجاتها من أجل EAP-TLS و EAP-TTLS وأساليب EAP الأخرى.

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 تلمحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## التكوين

يصف هذا التكوين كيفية تكوين مصادقة EAP على نقطة وصول مستندة إلى IOS. في المثال في هذا المستند، يتم استخدام LEAP كطريقة لمصادقة EAP مع خادم RADIUS.

**ملاحظة:** أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

كما هو الحال مع معظم خوارزميات المصادقة المستندة إلى كلمة المرور، يكون Cisco LEAP عرضة لهجمات القاموس. لا يعد هذا هجوماً جديداً أو نقطة ضعف جديدة خاصة ب Cisco LEAP. يعد إنشاء سياسة كلمة مرور قوية أكثر الطرق فعالية لتخفيف هجمات القاموس. ويتضمن ذلك استخدام كلمات مرور قوية وانتهاء صلاحية كلمات المرور بشكل دوري. راجع [هجوم القاموس على Cisco LEAP](#) للحصول على مزيد من المعلومات حول هجمات القاموس وكيفية منعها.

يستعمل هذا وثيقة هذا تشكيل ل على حد سواء GUI و CLI:

- عنوان IP لنقطة الوصول هو 10.0.0.106.
- عنوان IP الخاص بخادم (RADIUS ACS) هو 10.0.0.3.

## EAP للشبكة أو مصادقة مفتوحة باستخدام EAP

في أي أسلوب مصادقة يستند إلى EAP/802.1x، يمكنك التساؤل عن الاختلافات بين EAP على الشبكة والمصادقة المفتوحة مع EAP. تشير هذه العناصر إلى القيم الموجودة في حقل خوارزمية المصادقة في رؤوس حزم الإدارة والاقتران. يحدد معظم مصنعي العملاء اللاسلكيين هذا الحقل بالقيمة 0 (المصادقة المفتوحة) ثم يشيرون إلى الرغبة في إجراء مصادقة EAP لاحقاً في عملية الاقتران. تعين Cisco القيمة بشكل مختلف، من بداية الاقتران بعلامة EAP للشبكة.

إذا كانت شبكتك تحتوي على عملاء:

- أستخدم عملاء Cisco Network-EAP.
- عملاء الطرف الثالث (بما في ذلك المنتجات المتوافقة مع CCX)—إستخدام مفتوحة مع EAP.
- مزيج من كل من عملاء Cisco وعملاء الجهات الخارجية - أختار كلا من بروتوكول Network-EAP وافتح باستخدام EAP.

## تعريف خادم المصادقة

تتمثل الخطوة الأولى في تكوين EAP في تعريف خادم المصادقة وإنشاء علاقة معه.

1. في علامة التثبيت إدارة خادم نقطة الوصول (أسفل التأمين < عنصر قائمة إدارة الخادم)، أكمل الخطوات التالية: أدخل عنوان IP الخاص بخادم المصادقة في حقل الخادم. حدد السر المشترك والمنفذ. انقر فوق **تطبيق** لإنشاء التعريف وملء القوائم المنسدلة. ثبت ال EAP صحة هوية نوع أولوية 1 مجال إلى الخادم عنوان تحت تقصير نادل أولوية. طقطقة  
يطبق.

**Cisco Systems** Cisco 1200 Access Point

SERVER MANAGER GLOBAL PROPERTIES

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP  
ASSOCIATION  
NETWORK INTERFACES  
SECURITY  
Admin Access  
Encryption Manager  
SSID Manager  
Server Manager  
Local RADIUS Server  
Advanced Security  
SERVICES  
WIRELESS SERVICES  
SYSTEM SOFTWARE  
EVENT LOG

Hostname AP 12:18:46 Mon Sep 20 2004

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)  
Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

RADIUS

< NEW >  
10.0.0.3

Delete

Server: 10.0.0.3 (Hostname or IP Address)  
Shared Secret:

Authentication Port (optional): 1645 (0-65536)  
Accounting Port (optional): 1646 (0-65536)

Apply Cancel

Default Server Priorities

EAP Authentication  
Priority 1: 10.0.0.3  
Priority 2: < NONE >  
Priority 3: < NONE >

MAC Authentication  
Priority 1: < NONE >  
Priority 2: < NONE >  
Priority 3: < NONE >

Accounting  
Priority 1: < NONE >  
Priority 2: < NONE >  
Priority 3: < NONE >

Admin Authentication (RADIUS)  
Priority 1: < NONE >  
Priority 2: < NONE >  
Priority 3: < NONE >

Admin Authentication (TACACS+)  
Priority 1: 10.0.0.3  
Priority 2: < NONE >  
Priority 3: < NONE >

Proxy Mobile IP Authentication  
Priority 1: < NONE >  
Priority 2: < NONE >  
Priority 3: < NONE >

Apply Cancel

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc.

أنت يستطيع أيضا أصدرت هذا أمر من ال CLI:  
AP#configure terminal

.Enter configuration commands, one per line. End with CNTL/Z

AP(config)#aaa group server radius rad\_eap

AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646

```
AP(config-sg-radius)#exit
```

```
AP(config)#aaa new-model
```

```
AP(config)#aaa authentication login eap_methods group rad_eap
```

```
AP(config)#radius-server host 10.0.0.3 auth-port 1645  
acct-port 1646 key labap1200ip102
```

```
AP(config)#end
```

```
AP#write memory
```

2. يجب تكوين نقطة الوصول في خادم المصادقة كعميل AAA. على سبيل المثال، في Cisco Secure ACS، يحدث ذلك في صفحة [تكوين الشبكة](#) حيث يتم تحديد اسم نقطة الوصول وعنوان IP والسر المشترك وطريقة المصادقة (RADIUS Cisco IOS/PIX أو RADIUS Cisco Aironet). ارجع إلى الوثائق من الشركة المصنعة الخاصة بخوادم المصادقة الأخرى غير الخاصة بـ ACS.

The screenshot shows the Cisco Network Configuration web interface. The main content area is titled "AAA Client" and contains the following fields and options:

- AAA Client Hostname: AP
- AAA Client IP Address: 10.0.0.106
- Key: sharedsecret
- Authenticate Using: RADIUS (Cisco IOS/PIX) (selected from a dropdown menu)

Below these fields are several checkboxes for logging and accounting options:

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom of the form are three buttons: "Submit", "Submit + Restart", and "Cancel".

On the right side, there is a "Help" section with a list of links:

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

Below the links, there is a section titled "AAA Client Hostname" with the text: "The AAA Client Hostname is the name assigned to the AAA client." and a [Back to Top](#) link.

تأكد من تكوين خادم المصادقة لتنفيذ أسلوب مصادقة EAP المطلوب. على سبيل المثال، بالنسبة لـ ACS الآمن من Cisco الذي يعمل LEAP، قم بتكوين مصادقة LEAP على [تكوين النظام](#) - صفحة [إعداد المصادقة العالمية](#). انقر على [تكوين النظام](#)، ثم انقر على [إعداد المصادقة العامة](#). أحلت التوثيق من الصانع لخدمات مصادقة أخرى غير ACS أو أساليب EAP أخرى.

**CISCO SYSTEMS** **System Configuration**

Select	Help
<ul style="list-style-type: none"> <li>User Setup</li> <li>Group Setup</li> <li>Shared Profile Components</li> <li>Network Configuration</li> <li>System Configuration</li> <li>Interface Configuration</li> <li>Administration Control</li> <li>External User Databases</li> <li>Reports and Activity</li> <li>Online Documentation</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Service Control</a></li> <li><a href="#">Logging</a></li> <li><a href="#">Date Format Control</a></li> <li><a href="#">Local Password Management</a></li> <li><a href="#">CiscoSecure Database Replication</a></li> <li><a href="#">ACS Backup</a></li> <li><a href="#">ACS Restore</a></li> <li><a href="#">ACS Service Management</a></li> <li><a href="#">IP Pools Server</a></li> <li><a href="#">IP Pools Address Recovery</a></li> <li><a href="#">ACS Certificate Setup</a></li> <li><a href="#">Global Authentication Setup</a></li> </ul> <p style="text-align: center;"><a href="#">Back to Help</a></p>
	<ul style="list-style-type: none"> <li><a href="#">Service Control</a></li> <li><a href="#">Logging</a></li> <li><a href="#">Date Format Control</a></li> <li><a href="#">Local Password Management</a></li> <li><a href="#">CiscoSecure Database Replication</a></li> <li><a href="#">RDBMS Synchronization</a></li> <li><a href="#">ACS Backup</a></li> <li><a href="#">ACS Restore</a></li> <li><a href="#">ACS Service Management</a></li> <li><a href="#">IP Pools Address Recovery</a></li> <li><a href="#">IP Pools Server</a></li> <li><a href="#">VoIP Accounting Configuration</a></li> <li><a href="#">ACS Certificate Setup</a></li> <li><a href="#">Global Authentication Configuration</a></li> </ul> <p><b>Service Control</b></p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p><a href="#">[Back to Top]</a></p>

تعرض هذه الصورة Cisco Secure ACS الذي تم تكوينه ل PEAP و EAP-FAST و EAP-TLS و LEAP و EAP-MD5.

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

## Global Authentication Setup

### EAP Configuration

#### PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

#### EAP-FAST

Allow EAP-FAST

Active master key TTL:  months

Retired master key TTL:  months

PAC TTL:  weeks

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

#### EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

#### LEAP

Allow LEAP (For Aironet only)

#### EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds):

### MS-CHAP Configuration

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

Submit

Submit + Restart

Cancel

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

#### PEAP

*Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have*

بمجرد أن تعرف نقطة الوصول أين ترسل طلبات مصادقة العميل، قم بتكوينها لقبول هذه الأساليب.

ملاحظة هذه التعليمات خاصة بالتثبيت الذي يستند إلى WEP. للحصول على WPA (الذي يستخدم التشفير بدلا من WEP)، راجع [نظرة عامة على تكوين WPA](#).

1. في علامة تبويب مدير تشفير نقطة الوصول (ضمن التأمين < عنصر قائمة مدير التشفير)، أكمل الخطوات التالية: حدد أنك تريد استخدام تشفير WEP. حدد أن WEP إلزامي. تحقق من تعيين حجم المفتاح على 128-بت. طقطقة **يطبق**.

The screenshot displays the Cisco 1200 Access Point configuration page. The left sidebar shows navigation options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Cisco 1200 Access Point' and shows configuration for 'RADIO0-802.11B'. The 'Security: Encryption Manager - Radio0.802.11B' section is active, showing 'Encryption Modes' with 'WEP Encryption' selected and 'Mandatory' in a dropdown menu. Below this, 'Cisco Compliant TKIP Features' includes 'Enable MIC' and 'Enable Per Packet Keying'. The 'Encryption Keys' section has a table with columns for 'Transmit Key', 'Encryption Key (Hexadecimal)', and 'Key Size'. The 'Global Properties' section includes 'Broadcast Key Rotation Interval' (set to 'Disable Rotation') and 'WPA Group Key Update' options.

Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1: <input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2: <input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3: <input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4: <input type="radio"/>	<input type="text"/>	128 bit

Buttons at the bottom: Apply-Radio0, Apply-All, Cancel.

أنت تستطيع أيضا أصدرت هذا أمر من ال CLI:  
AP#configure terminal



.Enter configuration commands, one per line. End with CNTL/Z

```
AP(config)#interface dot11radio 0
```

```
AP(config-if)#encryption mode wep mandatory
```

```
AP(config-if)#end
```

```
AP#write memory
```

2. أكمل الخطوات التالية على علامة تبويب إدارة SSID لنقطة الوصول (تحت التأمين < عنصر قائمة إدارة SSID): حدد SSID المطلوب. تحت "طرق المصادقة المقبولة"، حدد المربع المسمى فتح واستخدم القائمة المنسدلة للاختيار مع EAP. ضع علامة في المربع المسمى Network-EAP إذا كانت لديك بطاقات عميل Cisco. انظر المناقشة في [EAP للشبكة أو افتح المصادقة باستخدام قسم EAP](#). طقطقة يطبق.

RADIO0-802.11B

RADIO1-802.11A

Hostname AP

12:47:46 Mon Sep 20 2004

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY**
- Admin Access
- Encryption Manager
- SSID Manager**
- Server Manager
- Local RADIUS Server
- Advanced Security
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

## Security: SSID Manager - Radio0-802.11B

### SSID Properties

#### Current SSID List

< NEW >
labap1200

**SSID:**

**VLAN:**  [Define VLANs](#)

**Network ID:**  (0-4096)

Delete-Radio0

Delete-All

### Authentication Settings

#### Methods Accepted:

Open Authentication:

Shared Authentication:

Network EAP:

#### Server Priorities:

##### EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

##### MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

Portions of this image not relevant to the discussion have been edited for clarity

### Global Radio0-802.11B SSID Properties

**Set Guest Mode SSID:**

**Set Infrastructure SSID:**   Force Infrastructure Devices to associate only to this SSID

Apply

Cancel

أنت تستطيع أيضا أصدرت هذا أمر من ال CLI:

```
AP#configure terminal
```

```
.Enter configuration commands, one per line. End with CNTL/Z
```

```
AP(config)#interface dot11radio 0
```

```
AP(config-if)#ssid labap1200
```

```
AP(config-if-ssid)#authentication open eap eap_methods
```

```
AP(config-if-ssid)#authentication network-eap eap_methods
```

```
AP(config-if-ssid)#end
```

```
AP#write memory
```

وبمجرد تأكيد الوظيفة الأساسية بتكوين EAP أساسي، يمكنك إضافة ميزات إضافية وإدارة المفاتيح في وقت لاحق. تمتع بطبقة وظائف أكثر تعقيداً فوق المؤسسات الوظيفية لتسهيل عملية استكشاف الأخطاء وإصلاحها.

## التحقق من الصحة

يوفر هذا القسم معلومات يمكنك استخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر العرض بواسطة [أداة مترجم الإخراج \(العملاء المسجلون فقط\)](#)، والتي تتيح لك عرض تحليل إخراج أمر العرض.

• **show radius server-group all**—يعرض قائمة بجميع مجموعات خادم RADIUS التي تم تكوينها على نقطة الوصول.

## استكشاف الأخطاء وإصلاحها

### إجراء استكشاف الأخطاء وإصلاحها

أتمت هذا steps in order to تحريت تشكيك.

1. في الأداة المساعدة أو البرنامج من جانب العميل، قم بإنشاء توصيف جديد أو توصيل بالمعلومات نفسها أو المتماثلة لضمان عدم إتلاف أي شيء في تكوين العميل.
2. للقضاء على إمكانية حدوث مشاكل في التردد اللاسلكي تمنع المصادقة الناجحة، قم بتعطيل المصادقة مؤقتاً كما هو موضح في هذه الخطوات: من واجهة سطر الأوامر، استخدم الأوامر **no authentication open eap\_methods**، و**authentication open no authentication network-eap\_methods**. من واجهة المستخدم الرسومية (GUI)، في صفحة "مدير SSID"، قم بإلغاء تحديد **Network-EAP**، ثم تحقق من فتح، ثم قم بتعيين القائمة المنسدلة إلى **بدون إضافة**. في حالة اقتران العميل بنجاح، لا يساهم RF في مشكلة الاقتران.
3. تحقق من مزامنة كلمات المرور السرية المشتركة بين نقطة الوصول وخادم المصادقة. وإلا، يمكنك تلقي رسالة الخطأ هذه:

```
Invalid message authenticator in EAP request
```

من واجهة سطر الأوامر (CLI)، تحقق من الخط **Radius-server host x.x.x auth-port x access-port x**

من واجهة المستخدم الرسومية (GUI)، على صفحة مدير الخادم، قم بإعادة إدخال

السر المشترك للخادم المناسب في المربع المسمى "سر مشترك". يجب أن يحتوي الإدخال السري المشترك

لنقطة الوصول على خادم RADIUS على نفس كلمة المرور السرية المشتركة كتلك المذكورة سابقاً.

4. قم بإزالة أي مجموعات مستخدمين من خادم RADIUS. في بعض الأحيان قد تحدث تعارضات بين مجموعات

المستخدمين المعرفة بواسطة خادم RADIUS ومجموعات المستخدمين في المجال السفلي. تحقق من سجلات خادم RADIUS للمحاولات الفاشلة، والسبب وراء فشل هذه المحاولات.

## أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر العرض بواسطة أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر العرض.

توفر مصادقات تصحيح الأخطاء قدرًا كبيرًا من التفاصيل حول كيفية تجميع وتفسير مخرجات تصحيح الأخطاء المتعلقة بـ EAP.

ملاحظة: قبل إصدار أوامر debug، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

• **debug dot11 aaa** - جهاز الحالة—يعرض التقسيمات (أو الحالات) الرئيسية للتفاوض بين العميل وخادم المصادقة. فيما يلي مخرج من مصادقة ناجحة:

```
Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending*
                        identity request to 0040.96ac.dd05
:Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client*
                        0040.96ac.dd05 timer started for 30 seconds
Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing*
                        Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
:Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client*
                        (Sending identity request to 0040.96ac.dd05 (client
Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client*
                        0040.96ac.dd05 timer started for 30 seconds
Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing*
                        Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
:Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server*
                        Sending client 0040.96ac.dd05 data (User Name) to server
:Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server*
                        Started timer server_timeout 60 seconds
Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing*
                        Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
:Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client*
                        Forwarding server message(Challenge) to client 0040.96ac.dd05
:Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client*
                        Started timer client_timeout 20 seconds
Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing*
                        Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
:Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server*
                        Sending client 0040.96ac.dd05 data(User Credentials) to server
-----Lines Omitted for simplicity-----
:Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client*
                        Started timer client_timeout 20 seconds
Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action*
                        SERVER_WAIT,SERVER_PASS) for 0040.96ac.dd05)
:Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client*
                        Forwarding server message(Pass Message) to client
                        0040.96ac.dd05
:Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client*
                        Started timer client_timeout 30 seconds
,Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0*
Station TACWEB 0040.96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
                        (associated to the access point
```

ملاحظة: في إصدارات برنامج Cisco IOS Software قبل 12.2(15)JA، تكون صياغة الأمر debug هذا هي  
**debug dot11 aaa dot1x state-machine**

• **عملية مصادق debug dot11 aaa**—يعرض إدخالات الحوار الفردية للتفاوض بين العميل وخادم

المصادقة.ملاحظة: في إصدارات برنامج Cisco IOS software قبل 12.2(15)JA، تكون صياغة أمر تصحيح الأخطاء هذا هي `debug radius authentication`—يعرض مفاوضات RADIUS بين الخادم والعميل، وكلاهما، يتم توصيلهما بواسطة نقطة الوصول (AP). هذا مخرج للمصادقة الفاشلة:

- `debug radius authentication`—يعرض مفاوضات RADIUS بين الخادم والعميل، وكلاهما، يتم توصيلهما بواسطة نقطة الوصول (AP). هذا مخرج للمصادقة الفاشلة:

```
Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11*
Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5*
[Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi*
Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3*
[Mar 1 02:34:55.087: RADIUS: 32 [2*
Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106*
Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47*
Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106*
Mar 1 02:34:55.087: RADIUS(00000031): sending*
Mar 1 02:34:55.087: RADIUS(00000031): Send Access-Request*
to 10.0.0.3 :164 5 id 1645/61, len 130
- Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E*
A4 7E D3 C2 26 EB 77 56
"Mar 1 02:34:55.088: RADIUS: User-Name [1] 8 "wirels*
Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400*
"Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0*
"Mar 1 02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05*
[Mar 1 02:34:55.088: RADIUS: Service-Type [6] 6 Login [1*
Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18*
Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5*
[??4A AB 88 [s?Y??QS?XM??J
Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13*
"Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299*
Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106*
"Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap*
Mar 1 02:34:55.093: RADIUS: Received from id 1645/61*
Access-Challenge, len 79 ,1645: 10.0.0.3
- Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2*
9B B4 77 B8 973 49 87 84
-----Lines Omitted-----
Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106*
Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47*
Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106*
Mar 1 02:34:55.118: RADIUS(00000031): sending*
Mar 1 02:34:55.118: RADIUS(00000031): Send Access-Request to*
id 1645/62, len 168 5 164: 10.0.0.3
- Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7*
0F 4E 7C F4 C7 1F 24 07
"Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels*
Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400*
-----Lines Omitted-----
Mar 1 02:34:55.124: RADIUS: Received from id 1645/62*
Access-Reject, len 56 ,1645: 10.0.0.3
- Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25*
AD 01 26 11 9A F6 01 37
Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6*
[????] Mar 1 02:34:55.125: RADIUS: 04 15 00 04*
Mar 1 02:34:55.125: RADIUS: Reply-Message [18] 12*
Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D*
[??Rejected]
Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18*
Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62*
Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes*
Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes*
Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station*
0040.96ac.dd05 Authentication failed
```

- `debug aaa authentication`—يعرض مفاوضات AAA للمصادقة بين الجهاز العميل وخادم المصادقة.

## معلومات ذات صلة

- مصادقة التصحيح
- تكوين أنواع المصادقة
- مصادقة LEAP على خادم RADIUS محلي
- تكوين خوادم RADIUS و TACACS+
- تكوين مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows v3.2 باستخدام مصادقة جهاز PEAP-MS-CHAPv2
- مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows v3.2 المزود بمصادقة جهاز EAP-TLS
- تكوين PEAP/EAP على Microsoft IAS
- أستكشاف أخطاء Microsoft IAS وإصلاحها كخادم RADIUS
- عمل مصادقة Microsoft 802.1X
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا