

# ةيكل لسا لال لاجملا تامدخ نيوكت

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[خدمات المجال اللاسلكية](#)

[دور جهاز WDS](#)

[دور نقاط الوصول باستخدام جهاز WDS](#)

[التكوين](#)

[تعين نقطة وصول كمعرف فئة المورد \(WDS\)](#)

[تعين WLSM ك WDS](#)

[تعين نقطة وصول كجهاز بنية أساسية](#)

[تحديد أسلوب مصادقة العميل](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[أوامر استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## المقدمة

يقدم هذا المستند مفهوم خدمات المجال اللاسلكي (WDS). يصف المستند أيضا كيفية تكوين نقطة وصول (AP) واحدة أو الوحدة النمطية لخدمات شبكة LAN اللاسلكية (WLSM) كشبكة WDS وأخرى على الأقل كنقطة وصول للبنية الأساسية. يرشدك الإجراء الوارد في هذا المستند إلى WDS الذي يعمل ويسمح للعملاء بالاقتران إما بنقطة الوصول WDS أو بنقطة الوصول (AP) للبنية الأساسية. يهدف هذا المستند إلى إنشاء أساس يمكنك من خلاله تكوين [التحويل الآمن السريع](#) أو تقديم [محرك حلول شبكة LAN اللاسلكية](#) (WLSE) في الشبكة، حتى يمكنك استخدام الميزات.

## المتطلبات الأساسية

### المتطلبات

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

- لديهم معرفة كاملة بشبكات LAN اللاسلكية ومشكلات الأمان اللاسلكي.
- معرفة طرق أمان بروتوكول المصادقة المتوسع (EAP) الحالي.

### المكونات المستخدمة

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

- نقاط الوصول مع برنامج Cisco IOS ©
  - برنامج IOS الإصدار JA2(2)12.3 أو إصدار أحدث من Cisco
  - الوحدة النمطية Catalyst 6500 Series Wireless LAN Services Module
- تم إنشاء المعلومات المقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي) وعنوان IP على الواجهة BVI1، لذلك يمكن الوصول إلى الوحدة من واجهة المستخدم الرسومية (GUI) لبرنامج Cisco IOS software أو واجهة سطر الأوامر (CLI). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الاصطلاحات

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

## خدمات المجال اللاسلكية

WDS سمة جديد ل APs في cisco ios برمجية والأساس من المادة حفازة WLSM 6500 sery. إن WDS وظيفة أساسية تتيح ميزات أخرى مثل:

- التجوال الآمن السريع
- تفاعل WLSE
- إدارة الراديو

يجب عليك إنشاء علاقات بين نقاط الوصول التي تشارك في WDS و WLSM، قبل أن تعمل أي ميزات أخرى تستند إلى WDS. من مقاصد WDS تقليل الحاجة إلى خادم المصادقة للتحقق من مسوغات المستخدم وتقليل الوقت اللازم لمصادقة العميل.

in order to استعملت WDS، أنت ينبغي عينت واحد ap أو ال WLSM بما أن ال WDS. يجب أن تستخدم نقطة الوصول إلى WDS اسم مستخدم وكلمة مرور WDS لإنشاء علاقة مع خادم مصادقة. يمكن أن يكون خادم المصادقة إما خادم RADIUS خارجي أو ميزة خادم RADIUS المحلي في نقطة الوصول WDS. يجب أن يكون WLSM علاقة مع خادم المصادقة، حتى وإن لم يكن WLSM بحاجة إلى المصادقة إلى الخادم.

تتصل نقاط وصول أخرى، تسمى نقاط الوصول للبنية الأساسية، مع WDS. قبل حدوث التسجيل، يجب أن تصادق نقاط الوصول (APs) للبنية الأساسية على WDS. تحدد مجموعة خوادم البنية الأساسية الموجودة على WDS مصادقة البنية الأساسية هذه.

توجد مجموعة واحدة أو أكثر من مجموعات خوادم العملاء على WDS تعرف مصادقة العميل.

عندما يحاول عميل الاقتران بنقطة وصول للبنية الأساسية، تمرر نقطة الوصول للبنية الأساسية بيانات اعتماد المستخدم إلى WDS للتحقق من الصحة. إذا رأت WDS بيانات الاعتماد لأول مرة، فإن WDS يلتفت إلى خادم المصادقة للتحقق من صحة بيانات الاعتماد. ثم يقوم WDS بتخزين بيانات الاعتماد مؤقتًا، لإزالة الحاجة إلى العودة إلى خادم المصادقة عند محاولة نفس المستخدم المصادقة مرة أخرى. وتتضمن أمثلة إعادة المصادقة ما يلي:

- إعادة صياغة
  - تجوال
  - عندما يقوم المستخدم بتشغيل جهاز العميل
- يمكن إنشاء قنوات عبر بروتوكول مصادقة EAP القائم على RADIUS من خلال WDS مثل:

- EAP خفيف الوزن (LEAP)
- EAP محمي (PEAP)
- أمان طبقة النقل-EAP (EAP-TLS)

• مصادقة EAP المرنة من خلال الاتصال النفقي الآمن (EAP-FAST)  
كما يمكن لمصادقة عنوان MAC النفق إما إلى خادم مصادقة خارجي أو مقابل قائمة محلية إلى نقطة وصول WDS.  
لا يدعم WLSM مصادقة عنوان MAC.

تتصل WDS ونقاط الوصول للبنية الأساسية عبر بروتوكول بث متعدد يسمى بروتوكول التحكم في سياق WLAN (WLCCP). لا يمكن توجيه رسائل البث المتعدد هذه، لذلك يجب أن تكون WDS ونقاط الوصول للبنية الأساسية المقترنة في شبكة IP الفرعية نفسها وعلى مقطع الشبكة المحلية (LAN) نفسه. بين WDS و WLSE، يستخدم WLCCP TCP وبروتوكول مخطط بيانات المستخدم (UDP) على المنفذ 2887. عندما يكون WDS و WLSE على شبكات فرعية مختلفة، لا يمكن لبروتوكول مثل ترجمة عنوان الشبكة (NAT) ترجمة الحزم.

نقطة وصول تم تكوينها كجهاز WDS تدعم ما يصل إلى 60 نقطة وصول مشاركة. يدعم موجه الخدمات المدمجة (ISR) الذي تم تكوينه كأجهزة WDS ما يصل إلى 100 نقطة وصول (AP) مشاركة. كما يدعم محول مزود بتقنية WLSM ما يصل إلى 600 نقطة وصول مشتركة وما يصل إلى 240 مجموعة قابلة للتنقل. نقطة وصول واحدة تدعم ما يصل إلى 16 مجموعة قابلة للتنقل.

**ملاحظة:** توصي Cisco بأن تقوم نقاط الوصول للبنية الأساسية بتشغيل نفس إصدار IOS الخاص بجهاز WDS. إذا كنت تستخدم إصدارًا قديمًا من IOS، فقد تفشل نقاط الوصول في المصادقة على جهاز WDS. وبالإضافة إلى ذلك، توصي Cisco باستخدام أحدث إصدار من IOS. يمكنك العثور على أحدث إصدار من IOS في صفحة [التنزيلات اللاسلكية](#).

## دور جهاز WDS

يقوم جهاز WDS بالعديد من المهام على الشبكة المحلية اللاسلكية لديك:

- يعلن عن قدرات WDS ويشارك في إختيار أفضل جهاز WDS للشبكة المحلية اللاسلكية لديك. عندما تقوم بتكوين شبكة LAN اللاسلكية ل WDS، فإنك تقوم بإعداد جهاز واحد كمرشح WDS الرئيسي وجهاز إضافي واحد أو أكثر كمرشحين للنسخ الاحتياطي ل WDS. إذا كان جهاز WDS الرئيسي خارج الخط، فإن أحد أجهزة WDS الاحتياطية يحل محله.
- مصادقة جميع نقاط الوصول في الشبكة الفرعية وإنشاء قناة اتصال آمنة مع كل منها.
- يجمع بيانات الراديو من نقاط الوصول في الشبكة الفرعية، ويجمع البيانات، ويعيد توجيهها إلى جهاز WLSE على الشبكة الخاصة بك.
- يعمل كتمرير لجميع أجهزة العملاء 802.1x التي تتم مصادقتها والمرتبطة بنقاط الوصول المشاركة.
- تسجيل جميع أجهزة العميل في الشبكة الفرعية التي تستخدم ميزة الكي الديناميكي وإنشاء مفاتيح جلسات عمل لها وتخزين بيانات اعتماد الأمان الخاصة بها مؤقتًا. عندما يقوم العميل بالتجوال إلى نقطة وصول أخرى، يقوم جهاز WDS بإعادة توجيه بيانات اعتماد أمان العميل إلى نقطة الوصول الجديدة.

## دور نقاط الوصول باستخدام جهاز WDS

تتفاعل نقاط الوصول (APs) على الشبكة المحلية اللاسلكية مع جهاز WDS في هذه الأنشطة:

- اكتشاف جهاز WDS الحالي وتعبه وإعادة ترحيل إعلانات WDS إلى الشبكة المحلية اللاسلكية.
- المصادقة مع جهاز WDS وإنشاء قناة اتصال آمنة إلى جهاز WDS.
- تسجيل أجهزة العميل المقترنة بجهاز WDS.
- إرسال بيانات الراديو إلى جهاز WDS.

## التكوين

يعرض WDS التكوين بطريقة منظمة. فكل مفهوم يعتمد على المفهوم الذي يسبق. يحذف WDS عناصر التكوين

الأخرى مثل كلمات المرور والوصول عن بعد وإعدادات الراديو من أجل الوضوح والتركيز على الموضوع الأساسي.  
يقدم هذا القسم المعلومات اللازمة لتكوين الميزات الموضحة في هذا المستند.

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

## [تعيين نقطة وصول كمعرف فئة المورد \(WDS\)](#)

تتمثل الخطوة الأولى في تعيين نقطة وصول كمعرف فئة WDS. نقطة الوصول WDS هي الوحيدة التي تتصل بخادم المصادقة.

أتمت هذا steps in order to عينت ap ك WDS:

1. أخترت in order to شكلت المصادقة نادل على ال WDS ap، أمن نادل مدير أن يذهب إلى الخادم مدير علامة تبويب: تحت خوادم الشركة، اكتب عنوان IP الخاص بخادم المصادقة في حقل الخادم. حدد السر المشترك والمنافذ. تحت أولويات الخادم الافتراضية، قم بتعيين حقل الأولوية 1 إلى عنوان IP الخاص بالخادم هذا ضمن نوع المصادقة المناسب.

**Cisco 1200 Access Point**

SERVER MANAGER GLOBAL PROPERTIES

Hostname WDS\_AP 16:09:43 Fri Apr 23 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:  (Hostname or IP Address)

Shared Secret:

Authentication Port (optional):  (0-65536)

Accounting Port (optional):  (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:  <NONE >

Priority 2:  <NONE >

Priority 3:  <NONE >

Proxy Mobile IP Authentication

Priority 1:  <NONE >

Priority 2:  <NONE >

Priority 3:  <NONE >

Apply Cancel

بدلا من ذلك، أصدرت هذا أمر من ال CLI:

2. تتمثل الخطوة التالية في تكوين نقطة الوصول (WDS) في خادم المصادقة كعميل المصادقة والتفويض والمحاسبة (AAA). ولهذا، يلزمك إضافة نقطة الوصول إلى WDS كعميل AAA. أكمل الخطوات التالية: ملاحظة: يستخدم هذا المستند خادم ACS الآمن من Cisco كخادم مصادقة. في خادم التحكم في الوصول الآمن (ACS) من Cisco، يحدث هذا في صفحة [تكوين الشبكة](#) حيث تقوم بتعريف هذه السمات لنقطة الوصول (AP) إلى WDS: الاسم عنوان IP مشترك أسلوب المصادقة Cisco Aironet RADIUS فريق عمل هندسة الإنترنت ل [IETF] RADIUS انقر فوق إرسال. للحصول على خوادم مصادقة أخرى غير ACS، ارجع إلى الوثائق من

الشركة  
المصنعة.

**Cisco Systems Network Configuration**

**Edit**

### Add AAA Client

AAA Client Hostname: WDS\_AP

AAA Client IP Address: 10.0.0.102

Key: sharedsecret

Authenticate Using: RADIUS (Cisco Aironet)

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

Submit Submit + Restart Cancel

**Help**

- [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](#)

**AAA Client Hostname**

The AAA Client Hostname is the name assigned to the AAA client.

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

**AAA Client IP Address**

The AAA Client IP Address is the IP address assigned to the AAA client.

أيضا، في Cisco Secure ACS، تأكد من تكوين ACS لتنفيذ مصادقة LEAP على [تكوين النظام](#) - صفحة إعداد المصادقة العالمية. انقر أولا على تكوين النظام، ثم انقر على إعداد المصادقة العامة.

**Cisco Systems System Configuration**

**Select**

- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [CiscoSecure Database Replication](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [IP Pools Server](#)
- [IP Pools Address Recovery](#)
- [ACS Certificate Setup](#)
- [Global Authentication Setup](#)

[Back to Help](#)

**Help**

- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [CiscoSecure Database Replication](#)
- [RDBMS Synchronization](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [IP Pools Address Recovery](#)
- [IP Pools Server](#)
- [VoIP Accounting Configuration](#)
- [ACS Certificate Setup](#)
- [Global Authentication Configuration](#)

**Service Control**

Select to open the page from which you can stop or restart Cisco Secure ACS services.

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

انزلق إلى أسفل الصفحة إلى إعداد LEAP. عندما تضع علامة في المربع، يصادق ACS

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

**Edit** **Help**

**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:

Retired master key TTL:

PAC TTL:

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](#)

**Help**

- [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*

3. اخترت in order to شملت ال WDS عملية إعداد على ال WDS ap، لاسلكي خدمات WDS على ال WDS ap، وطققة على العامة setup لسان. قم بإجراء هذه الخطوات: تحت WDS-Wireless Domain Services

- خصائص عامة، حدد استخدام نقطة الوصول هذه كخدمات مجال لاسلكية. قم بتعيين قيمة حقل أولوية خدمات المجال اللاسلكي إلى قيمة مقدارها 254 تقريباً، لأن هذا هو الحقل الأول. أنت تستطيع شكلت one or much APs أو مفتاح كمرشح أن يزود WDS. يوفر الجهاز ذو الأولوية العليا WDS.

The screenshot displays the Cisco 1200 Access Point configuration page. The left sidebar contains navigation options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, AP, WDS, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Cisco 1200 Access Point' and has tabs for 'WDS STATUS', 'SERVER GROUPS', and 'GENERAL SET-UP'. The 'GENERAL SET-UP' tab is active, showing the hostname 'WDS\_AP' and the date '16:22:14 Fri Apr 23 2004'. Under 'Wireless Services: WDS/WNM - General Set-Up', the 'WDS - Wireless Domain Services - Global Properties' section is expanded. It includes a checked checkbox for 'Use this AP as Wireless Domain Services', a text input field for 'Wireless Domain Services Priority' set to '254' (with a range of '1-255' in parentheses), and an unchecked checkbox for 'Use Local MAC List for Client Authentication'. Below this, the 'WNM - Wireless Network Manager - Global Configuration' section is also expanded, showing an unchecked checkbox for 'Configure Wireless Network Manager' and a text input field for 'Wireless Network Manager IP Address' set to 'DISABLED' (with '(IP Address)' in parentheses). 'Apply' and 'Cancel' buttons are located at the bottom right.

بدلاً من ذلك، أصدرت هذا الأمر من الـ CLI:  
4. اختر خدمات لاسلكية < WDS، وانتقل إلى علامة التبويب مجموعات الخوادم: قم بتحديد اسم مجموعة خوادم يصادق نقاط الوصول الأخرى، وهي مجموعة بنية أساسية. قم بتعيين الأولوية 1 على خادم المصادقة الذي تم تكوينه مسبقاً. انقر على الزر استخدام المجموعة ل: مصادقة البنية الأساسية. تطبيق الإعدادات على معرفات مجموعة الخدمة (SSIDs) ذات الصلة.



Cisco Systems

## Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS\_AP 16:26:44 Fri Apr 23 2004

Wireless Services: WDS - Server Groups

Server Group List

< NEW >  
Infrastructure

Delete

Server Group Name: Infrastructure

Group Server Priorities: [Define Servers](#)

Priority 1: 10.0.0.3

Priority 2: < NONE >

Priority 3: < NONE >

Use Group For:

Infrastructure Authentication

Client Authentication

Authentication Settings

EAP Authentication

LEAP Authentication

MAC Authentication

Default (Any) Authentication

SSID Settings

Apply to all SSIDs

Restrict SSIDs (Apply only to listed SSIDs)

SSID: DISABLED Add

Remove

Apply Cancel

بدلاً من ذلك، أصدرت هذا الأمر من الـ CLI:

5. قم بتكوين اسم مستخدم وكلمة مرور WDS كمستخدم في خادم المصادقة الخاص بـ Cisco ACS. للحصول الآمن، يحدث هذا على صفحة [إعداد المستخدم](#)، حيث تقوم بتعريف اسم مستخدم وكلمة مرور WDS. للحصول على خوادم مصادقة أخرى غير ACS، ارجع إلى الوثائق من الشركة المصنعة. **ملاحظة:** لا تضع مستخدم WDS في مجموعة تم تعيين العديد من الحقوق والامتيازات لها - تتطلب WDS مصادقة محدودة فقط.

**CISCO SYSTEMS** User Setup

**Edit**

**User: WDSUser (New User)**

Account Disabled

**Supplementary User Info** ?

Real Name

Description

**User Setup** ?

Password Authentication:  

  
 CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)  
 Password   
 Confirm Password

**Help**

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

6. أخترت خدمات لاسلكي < AP، وطققة يمكن ل المشاركة في SWAN بنية أساسية خيار. ثم اكتب اسم مستخدم وكلمة مرور WDS. يجب تحديد اسم مستخدم وكلمة مرور WDS على خادم المصادقة لجميع الأجهزة التي تقوم بتعيين أعضاء في WDS.

**Cisco Systems**

## Cisco 1200 Access Point

Hostname: WDS\_AP 16:00:29 Fri Apr 23 2004

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
SECURITY +  
SERVICES +  
**WIRELESS SERVICES**  
AP  
WDS  
SYSTEM SOFTWARE +  
EVENT LOG +

**Wireless Services: AP**

Participate in SWAN Infrastructure:  Enable  Disable

WDS Discovery:  Auto Discovery  
 Specified Discovery:  (IP Address)

Username:   
Password:   
Confirm Password:

L3 Mobility Service via IP/GRE Tunnel:  Enable  Disable

Apply Cancel

بدلاً من ذلك، أصدرت هذا الأمر من الـ CLI:

7. أختبر خدمات لاسلكية < WDS. على علامة التبويب حالة WDS AP WDS، تحقق مما إذا كانت نقطة الوصول WDS تظهر في منطقة معلومات WDS، في الحالة النشطة. يجب أن تظهر نقطة الوصول أيضاً في منطقة معلومات نقطة الوصول، مع الحالة كمسجلة. إذا لم تظهر نقطة الوصول مسجلة أو نشطة، فتتحقق من خادم المصادقة بحثاً عن أي أخطاء أو محاولات مصادقة فاشلة. عندما يتم تسجيل نقطة الوصول بشكل مناسب، أضف نقطة وصول للبنية الأساسية لاستخدام خدمات WDS.

Cisco 1200 Access Point

WDS STATUS SERVER GROUPS GENERAL SET-UP

Hostname WDS\_AP 16:30:08 Fri Apr 23 2004

Wireless Services: WDS - Wireless Domain Services - Status

**WDS Information**

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

**WDS Registration**

APs: 1 Mobile Nodes: 0

**AP Information**

MAC Address	IP Address	State
0005.9a38.429f	10.0.0.102	REGISTERED

**Mobile Node Information**

MAC Address	IP Address	State	SSID	VLAN ID	BSSID

**Wireless Network Manager Information**

IP Address	Authentication Status

Refresh

بدلا من ذلك، أصدرت هذا أمر من ال CLI: ملاحظة: لا يمكنك إختبار اقترانات العملاء لأن مصادقة العميل لا تتضمن أحكاما بعد.

## تعين WLSM ك WDS

يشرح هذا القسم كيفية تكوين WLSM ك WDS. WDS هو الجهاز الوحيد الذي يتصل بخادم المصادقة.

**ملاحظة:** قم بإصدار هذه الأوامر في موجه أوامر enable ل WLSM، وليس من Supervisor Engine 720. أصدرت in order to ذهبت إلى الأمر رسالة حث من ال WLSM، هذا أمر في enable أمر رسالة حث في المشرف محرك 720:

```
c6506#session slot x proc 1
In this command, x is the slot number where the ---!
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
<Password: <enable password
#wlan
```

**ملاحظة:** لاستكشاف أخطاء WLSM لديك وإصلاحها وصيانتها بسهولة أكبر، قم بتكوين الوصول عن بعد إلى WLSM عن بعد إلى برنامج Telnet. ارجع إلى [تكوين الوصول عن بعد إلى Telnet](#).

من أجل تعيين WLSM على أنه WDS:

1. من ال CLI من ال WLSM، أصدرت هذا أمر، وأنشأت علاقة مع المصادقة نادل: **ملاحظة:** لا يوجد تحكم أولوية في WLSM. إذا كانت الشبكة تحتوي على وحدات WLSM متعددة، فإن WLSM يستخدم **تكوين التكرار** لتحديد الوحدة النمطية الأساسية.

2. قم بتكوين WLSM في خادم المصادقة كعميل AAA في Cisco Secure ACS، يحدث هذا على صفحة **تكوين الشبكة** حيث تقوم بتعريف هذه السمات ل WLSM: الاسم عنوان IP مشترك أسلوب المصادقة RADIUS Cisco Aironet RADIUS IETF للحصول على خوادم مصادقة أخرى غير ACS، ارجع إلى الوثائق من الشركة المصنعة.

أيضا، في Cisco Secure ACS، قم بتكوين ACS لإجراء مصادقة LEAP على **تكوين النظام** - صفحة **إعداد المصادقة العالمية**. انقر أولا على **تكوين النظام**، ثم انقر على **إعداد المصادقة العامة**.

**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> <hr/> <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>

انزلق إلى أسفل الصفحة إلى إعداد LEAP. عندما تضع علامة في المربع، يصادق ACS LEAP.

**CISCO SYSTEMS** System Configuration

**Edit** **Help**

### 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:

Retired master key TTL:

PAC TTL:

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

**Help**

- [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*

3. على ال WLSM، عينت طريقة أن يصادق الآخر APs (بنية أساسية نادل مجموعة).
4. على ال WLSM، عينت طريقة أن يصادق الزبون أداة (زبون نادل مجموعة) وما EAP نوع أن يستعمل زبون. ملاحظة: تؤدي هذه الخطوة إلى إزالة الحاجة إلى عملية [تعريف أسلوب مصادقة العميل](#).

5. عينت VLAN فريد بين المشرف محرك 720 وال WLSM in order to سمحت ال WLSM أن يتصل مع كيان خارجي مثل APs ومصادقة نادل. هذه شبكة VLAN غير مستخدمة في أي مكان آخر أو لأي غرض آخر على الشبكة. خلقت ال VLAN على المشرف محرك 720 أولاً، بعد ذلك أصدرت هذا أمر: على Supervisor Engine (المحرك المشرف) 720: WLSM.
6. دقت الدالة من ال WLSM مع هذا أمر: على Supervisor Engine (المحرك المشرف) 720:

### تعيين نقطة وصول كجهاز بنية أساسية

بعد ذلك، يجب عليك تعيين نقطة وصول واحدة على الأقل للبنية الأساسية وربط نقطة الوصول ب WDS. يرتبط العملاء بنقاط الوصول (APs) للبنية الأساسية. تطلب نقاط الوصول للبنية الأساسية نقطة الوصول إلى WDS أو WLSM لإجراء المصادقة لها.

أتمت هذا steps in order to أضفت بنية أساسية ap أن يستعمل الخدمات من ال WDS:

**ملاحظة:** ينطبق هذا التكوين فقط على نقاط الوصول (APs) للبنية الأساسية وليس على نقطة الوصول (WDS).

1. اختر خدمات لاسلكية < AP. في نقطة الوصول للبنية الأساسية، حدد تمكين لخيار الخدمات اللاسلكية. ثم اكتب اسم مستخدم وكلمة مرور WDS. يجب تحديد اسم مستخدم وكلمة مرور WDS على خادم المصادقة لجميع الأجهزة التي يجب أن تكون أعضاء في WDS.

بدلاً من ذلك، أصدرت هذا أمر من ال CLI:

2. اختر خدمات لاسلكية < WDS. على علامة التبويب "حالة WDS AP WDS"، تظهر نقطة الوصول للبنية الأساسية الجديدة في منطقة معلومات WDS، مع ظهور الحالة كنشطة، وفي منطقة معلومات نقطة الوصول، مع ظهور الحالة كمسجلة. إذا لم تظهر نقطة الوصول نشطة و/أو مسجلة، تحقق من خادم المصادقة بحثاً عن أي أخطاء أو محاولات مصادقة فاشلة. بعد أن تظهر نقطة الوصول نشطة و/أو مسجلة، أضف أسلوب مصادقة عميل



**Cisco 1200 Access Point**

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS\_AP 10:02:01 Mon Apr 26 2004

Wireless Services: WDS - Wireless Domain Services - Status

**WDS Information**

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

**WDS Registration**

APs: 2 Mobile Nodes: 0

**AP Information**

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

**Mobile Node Information**

MAC Address	IP Address	State	SSID	VLAN ID	BSSID

**Wireless Network Manager Information**

IP Address	Authentication Status

Refresh

بدلاً من ذلك، قم بإصدار هذا الأمر من واجهة سطر الأوامر: بدلاً من ذلك، قم بإصدار هذا الأمر من WLSM: بعد ذلك، قم بإصدار هذا الأمر على نقطة الوصول (AP) للبنية الأساسية: ملاحظة: لا يمكنك اختبار اقترانات العملاء لأن مصادقة العميل لا تتضمن أحكاماً بعد.

## تحديد أسلوب مصادقة العميل

وأخيراً، قم بتعريف طريقة مصادقة العميل.

أكمل هذه الخطوات لإضافة أسلوب مصادقة العميل:

1. أختَر خدمات لاسلكية < WDS. قم بإجراء هذه الخطوات على علامة التبويب WDS AP Server Groups: قم بتحديد مجموعة خوادم تقوم بمصادقة العملاء (مجموعة عملاء). قم بتعيين الأولوية 1 على خادم المصادقة الذي تم تكوينه مسبقاً. ضبط النوع القابل للتطبيق من المصادقة (MAC، EAP، LEAP، وهكذا دواليك). تطبيق الإعدادات على SSIDs ذات الصلة.

**Cisco Systems**

## Cisco 1200 Access Point

10:23:43 Mon Apr 26 2004

WDS STATUS    SERVER GROUPS    GENERAL SET-UP

Hostname WDS\_AP

### Wireless Services: WDS - Server Groups

**Server Group List**

< NEW >
Infrastructure
Client

Delete

**Server Group Name:** Client

**Group Server Priorities:** [Define Servers](#)

Priority 1: 10.0.0.3

Priority 2: < NONE >

Priority 3: < NONE >

**Use Group For:**

Infrastructure Authentication

**Client Authentication**

**Authentication Settings**

EAP Authentication

LEAP Authentication

MAC Authentication

Default (Any) Authentication

**SSID Settings**

**Apply to all SSIDs**

Restrict SSIDs (Apply only to listed SSIDs)

SSID: DISABLED    Add

Remove

Apply    Cancel

بدلاً من ذلك، أصدرت هذا الأمر من الـ CLI: **ملاحظة:** تم تخصيص مثال نقطة الوصول WDS ولا يقبل اقترانات العملاء. **ملاحظة:** لا تتم بتكوين نقاط الوصول (APs) للبنية الأساسية لمجموعات الخوادم لأن نقاط الوصول (APs) للبنية الأساسية تقوم بإعادة توجيه أي طلبات إلى WDS لمعالجتها.

2. في نقاط الوصول (AP) أو نقاط الوصول (APs) للبنية الأساسية: تحت عنصر قائمة التأمين < مدير التشغيل، انقر على تشفير WEP أو تشفير، كما هو مطلوب من بروتوكول المصادقة الذي تستخدمه.

**Cisco Systems**

## Cisco 1200 Access Point

RADIO0-802.11B    RADIO1-802.11A

Hostname Infrastructure\_AP    10:36:59 Mon Apr 26 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: Encryption Manager - Radio0-802.11B

#### Encryption Modes

None

WEP Encryption Mandatory

Cisco Compliant TKIP Features:  Enable MIC  Enable Per Packet Keying

Cipher WEP 128 bit

#### Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	<input type="text" value="A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>
Encryption Key 2:	<input type="radio"/>	<input type="text" value="A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>
Encryption Key 3:	<input type="radio"/>	<input type="text" value="A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>
Encryption Key 4:	<input type="radio"/>	<input type="text" value="A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>

تحت عنصر قائمة تأمين < مدير SSID، حدد طرق المصادقة كما هو مطلوب من بروتوكول المصادقة الذي تستخدمه.

**Cisco Systems**

## Cisco 1200 Access Point

RADIO0-802.11B    RADIO1-802.11A

Hostname Infrastructure\_AP    10:38:39 Mon Apr 26 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 >  
infraSSID

SSID: infraSSID  
VLAN: < NONE > [Define VLANs](#)  
Network ID: (0-4096)

Delete-Radio0    Delete-All

### Authentication Settings

Methods Accepted:

Open Authentication: with EAP  
 Shared Authentication: < NO ADDITION >  
 Network EAP: < NO ADDITION >

3. أنت تستطيع الآن بنجاح إختبار ما إذا كان زبون يصدق إلى بنية أساسية APs. تشير نقطة الوصول الخاصة ب WDS في علامة التبويب حالة WDS (أسفل الخدمات اللاسلكية < عنصر قائمة WDS) إلى أن العميل يظهر في منطقة معلومات عقدة Mobile في حالة مسجلة. إذا لم يظهر العميل، فتتحقق من خادم المصادقة بحثاً عن أي أخطاء أو محاولات مصادقة فاشلة من قبل العملاء.

**Cisco Systems**

## Cisco 1200 Access Point

10:49:24 Mon Apr 26 2004

Hostname WDS\_AP

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
SECURITY +  
SERVICES +  
WIRELESS SERVICES  
AP  
WDS  
SYSTEM SOFTWARE +  
EVENT LOG +

Wireless Services: WDS - Wireless Domain Services - Status

**WDS Information**

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

**WDS Registration**

APs: 2 | Mobile Nodes: 1

**AP Information**

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

**Mobile Node Information**

MAC Address	IP Address	State	SSID	VLAN ID	BSSID
0030.6527.74a	10.0.0.25	REGISTERED	infraSSID	-	0007.85b4.113b

**Wireless Network Manager Information**

IP Address	Authentication Status

Refresh

بدلا من ذلك، أصدرت هذا أمر من ال CLI: ملاحظة: إذا كنت بحاجة إلى تصحيح أخطاء المصادقة، فتأكد من تصحيح أخطائك على نقطة الوصول WDS، لأن نقطة الوصول WDS هي الجهاز الذي يتصل بخادم المصادقة.

## التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. تعرض هذه القائمة بعض الأسئلة الشائعة المتعلقة بأمر WDS من أجل توضيح فائدة هذه الأوامر بشكل أكبر:

- السؤال: في نقطة الوصول WDS، ما هي الإعدادات الموصى بها لهذه العناصر؟ مهلة خادم RADIUS وقت انتهاء صلاحية خادم RADIUS وقت تسليم فشل التحقق من سلامة الرسائل (MIC) لبروتوكول سلامة المفاتيح المؤقتة (TKIP) وقت تسليم العميل الفاصل الزمني لإعادة مصادقة EAP أو MAC انتهاء مهلة عميل EAP (إختياري) جواب: من المقترح أن تحتفظ بالتكوين بالإعدادات الافتراضية المتعلقة بهذه الإعدادات الخاصة، وتستخدمهم فقط عندما تكون هناك مشكلة تتعلق بالتوقيت. هذه هي الإعدادات الموصى بها لنقطة الوصول (AP) إلى WDS: تعطيل مهلة خادم radius. هذا هو عدد الثواني التي ينتظرها نقطة الوصول للرد على طلب RADIUS قبل أن تقوم بإعادة الطلب. الافتراضي هو 5 ثواني. تعطيل Radius-server Deadtime. يتم تخطي RADIUS بطلبات إضافية لمدة دقائق ما لم يتم وضع علامة "معطل" على جميع الخوادم. يتم تمكين وقت تسليم فشل TKIP MIC بشكل

افتراضي إلى 60 ثانية. إذا قمت بتمكين وقت التسليم، يمكنك إدخال الفاصل الزمني بالثواني. إذا اكتشفت نقطة الوصول عطلتى ميكروفون في غضون 60 ثانية، فإنها تمنع جميع عملاء TKIP على تلك الواجهة لفترة التسليم المحددة هنا. يجب تعطيل وقت تسليم العميل بشكل افتراضي. إذا قمت بتمكين التسليم، فأدخل عدد الثواني التي يجب على نقطة الوصول انتظارها بعد فشل المصادقة قبل معالجة طلب مصادقة لاحق. يتم تعطيل الفاصل الزمني لإعادة مصادقة EAP أو MAC بشكل افتراضي. إن يمكن أنت reauthentication، أنت تستطيع عينت الفاصل الزمني أو قبلت الفاصل الزمني يعطى بخادم المصادقة. إن يختار أنت أن يعين الفاصل الزمني، دخلت الفاصل الزمني بالثواني أن ال AP ينتظره قبل أن يجبر هو زبون أن يصدق. مهلة عميل EAP (إختياري) هي 120 ثانية بشكل افتراضي. أدخل مقدار الوقت الذي يجب على نقطة الوصول انتظاره للعملاء اللاسلكيين للاستجابة لطلبات مصادقة EAP.

- سؤال: بالنسبة لوقت التسليم في TKIP، فقد قرأت أنه يجب تعيين هذا إلى 100 ميلي ثانية و ليس 60 ثانية. أفترض أنه تم تعيينه لثانية واحدة من المستعرض لأنه أقل رقم يمكنك إختياره؟ جواب: لا توجد توصية محددة بتعيينها على 100 ميلي ثانية ما لم يتم الإبلاغ عن فشل حيث يكون الحل الوحيد هو الزيادة هذه المرة. و ثانية واحدة هي أقل عملية إعداد.
- السؤال: هل يساعد هذان الأمران مصادقة العميل بأي طريقة وهل هما مطلوبان على WDS أو نقطة الوصول (AP) للبنية الأساسية؟ سمة خادم RADIUS 6 on-for-login-auth سمة خادم radius 6 دعم متعدد جواب: لا تساعد هذه الأوامر عملية المصادقة ولا تكون مطلوبة على WDS أو نقطة الوصول.
- سؤال: في نقطة الوصول للبنية الأساسية، أفترض أنه لا توجد حاجة إلى أي من إعدادات "إدارة الخادم" و"خصائص عمومية" لأن نقطة الوصول تتلقى معلومات من WDS. هل هناك أي من هذه الأوامر المحددة مطلوبة لنقطة الوصول (AP) للبنية الأساسية؟ سمة خادم RADIUS 6 on-for-login-auth سمة خادم radius 6 دعم متعدد مهلة خادم RADIUS وقت انتهاء صلاحية خادم RADIUS الإيجابية: لا توجد حاجة إلى وجود إدارة خادم وخصائص عمومية لنقاط الوصول (APs) للبنية الأساسية. تتولى WDS هذه المهمة ولا حاجة إلى وجود هذه الإعدادات: سمة خادم RADIUS 6 on-for-login-auth سمة خادم radius 6 دعم متعدد مهلة خادم RADIUS وقت انتهاء صلاحية خادم RADIUS يبقى إعداد سمة خادم radius 32 تنسيق تضمين in-access-req %h بشكل افتراضي وهو مطلوب.

نقطة الوصول هي جهاز من الطبقة 2. لذلك، لا تدعم نقطة الوصول تنقل الطبقة 3 عند تكوين نقطة الوصول للعمل كجهاز WDS. أنت تستطيع حققت طبقة 3 حركية فقط عندما أنت تشكل ال WLSM بما أن ال WDS أداة. أحلت [الطبقة 3 حركية بنية](#) قسم من [cisco مادة حفازة sery 6500 لاسلكي lan خدمات وحدة نمطية: تقرير](#) ل كثير معلومة.

لذلك، عندما تقوم بتكوين نقطة وصول كجهاز WDS، لا تستخدم الأمر `mobility network-id`. يطبق هذا أمر على طبقة 3 حركية وأنت تحتاج أن يتلقى WLSM مثل ك WDS أداة in order to شكلت بشكل صحيح طبقة 3 حركية. إذا كنت تستخدم الأمر `mobility network-id` بشكل غير صحيح، فيمكنك رؤية بعض هذه الأعراض:

- يتعذر على العملاء اللاسلكيين الاقتران بنقطة الوصول.
- يمكن للعملاء اللاسلكي الاقتران بنقطة الوصول، ولكن لا يتلقون عنوان IP من خادم DHCP.
- لا تتم مصادقة الهاتف اللاسلكي عندما يكون لديك صوت عبر نشر شبكة WLAN.
- لا تحدث مصادقة EAP. باستخدام معرف شبكة التنقل الذي تم تكوينه، تحاول نقطة الوصول إنشاء نفق تضمين توجيه عام (GRE) لإعادة توجيه حزم EAP. إذا لم يتم إنشاء نفق، فإن الحزم لا تذهب إلى أي مكان.
- لا تعمل نقطة الوصول التي تم تكوينها كجهاز WDS كما هو متوقع، ولا يعمل تكوين WDS. ملاحظة: لا يمكنك تكوين نقطة الوصول Cisco Aironet 1300 AP/Bridge كمدير WDS. لا يدعم AP/Bridge 1300 هذه الوظيفة. يمكن أن يشارك ال AP/Bridge 1300 في شبكة WDS كجهاز بنية أساسية يتم فيه تكوين بعض AP أو WLSM الأخرى كمدير WDS.

## [أوامر استكشاف الأخطاء وإصلاحها](#)

تدعم [أداة مترجم الإخراج \(للملاء المسجلين فقط\)](#) بعض أوامر `show`. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرَج الأمر `show`.

ملاحظة: ارجع إلى [معلومات مهمة حول أوامر التصحيح](#) قبل استخدام أوامر `debug`.

- بيدي مصدق Debug dot11 aaa all — المفاوضات المختلفة التي يمر بها العميل على هيئة شركاء ومصادقة من خلال عملية 802.1x أو EAP. تم إدخال تصحيح الأخطاء هذا في برنامج Cisco IOS الإصدار 12.2(15)JA. يقوم هذا الأمر بتعطيل debug dot11 aaa dot1x الكل في ذلك والإصدارات اللاحقة.
- debug aaa authentication — يعرض عملية المصادقة من منظور AAA عام.
- debug wlcgp ap — يعرض مفاوضات WLCCP المعنية بما أن ap ينضم إلى WDS.
- debug wlcgp packet — يعرض المعلومات التفصيلية حول مفاوضات WLCCP.
- debug wlcgp leap-client — يعرض التفاصيل بينما ينضم جهاز بنية أساسية إلى WDS.

## معلومات ذات صلة

- [تكوين WDS والتجوال الآمن السريع وإدارة الراديو](#)
- [ملاحظة تكوين الوحدة النمطية Catalyst 6500 Series Wireless LAN Services Module](#)
- [تكوين مجموعات التشفير و WEP](#)
- [تكوين أنواع المصادقة](#)
- [صفحات دعم شبكة LAN اللاسلكية](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا