

WPA نيوكت ىلع ةمراع ةرظان

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [النظرية الأساسية](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [EAP للشبكة أو مصادقة مفتوحة باستخدام EAP](#)
- [تكوين واجهة سطر الأوامر \(CLI\)](#)
- [تكوين GUI](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [إجراء أكتشاف الأخطاء وإصلاحها](#)
- [أوامر استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يزود هذا وثيقة عينة تشكيل ل (WPA Protected Access (Wi-Fi)، المؤقت أمن معيار أن أعضاء تحالف Wi-Fi يستعملون.

المتطلبات الأساسية

المتطلبات

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

- معرفة دقيقة بالشبكات اللاسلكية ومشكلات الأمان اللاسلكي
- معرفة طرق أمان بروتوكول المصادقة المتوسع (EAP)

المكونات المستخدمة

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

- نقاط الوصول (AP) المستندة إلى البرامج (APs) إلى Cisco IOS ©
- برنامج IOS الإصدار JA(15)12.2 من Cisco أو إصدار أحدث **ملاحظة:** يفضل استخدام أحدث إصدار من برنامج Cisco IOS Software، حتى وإن كان WPA مدعوماً في برنامج Cisco IOS الإصدار JA(11)12.2 والإصدارات الأحدث. للحصول على أحدث إصدار من برنامج Cisco IOS Software، ارجع إلى [التنزيلات](#) ([للعلماء](#)) المسجلين

فقط).

- بطاقة واجهة الشبكة (NIC) المتوافقة مع WPA وبرنامج العميل المتوافق مع WPA الخاص بها 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.

النظرية الأساسية

تتسم ميزات الأمان في شبكة لاسلكية بالضعف، مثل WEP. استحدثت مجموعة صناعة تحالف واي فاي (أو WECA) الجيل التالي من معايير الأمان المؤقتة للشبكات اللاسلكية. ويوفر المعيار الدفاع ضد نقاط الضعف إلى أن تصدق منظمة المعهد الدولي لبحوث الطاقة على المعيار 802.11i.

يعتمد هذا النظام الجديد على مصادقة EAP/802.1x الحالية وإدارة المفاتيح الديناميكية وبضيف تشفير تشفير أقوى. بعد أن يشكل الجهاز العميل وخادم المصادقة اقتران EAP/802.1x، يتم التفاوض على إدارة مفتاح WPA بين نقطة الوصول وجهاز العميل المتوافق مع WPA.

كما توفر منتجات نقطة الوصول من Cisco تكويننا هجيناً يعمل فيه كل من عملاء EAP السابقين الذين يستندون إلى WEP (مع الإدارة القديمة أو بدون إدارة المفاتيح) بالاقتران مع عملاء WPA. ويشار إلى هذا التكوين باسم وضع الترحيل. يسمح وضع الترحيل بنهج مرحلي للترحيل إلى WPA. لا يغطي هذا المستند وضع الترحيل. يقدم هذا المستند مخطط تفصيلي لشبكة مؤمنة WPA خالصة.

بالإضافة إلى المخاوف الأمنية على مستوى المؤسسات أو المؤسسات، توفر WPA أيضاً نسخة مفتاح مشترك مسبقاً (WPA-PSK) معدة للاستخدام في المكاتب الصغيرة أو المكاتب المنزلية (SOHO) أو الشبكات اللاسلكية المنزلية. لا تدعم الأداة المساعدة لعميل WPA-PSK (ACU) Cisco Aironet. تدعم الأداة المساعدة Wireless Zero Configuration من Microsoft Windows WPA-PSK لمعظم البطاقات اللاسلكية، كما تفعل الأدوات المساعدة التالية:

- عميل Aegis من MeetingHub Communications **ملاحظة:** ارجع إلى [إعلان نهاية العمر الافتراضي \(EOS\)](#) ونقطة نهاية العمر الافتراضي (EEGIS) [لخط متحدثات الاجتماعات](#).
- عميل Odyssey من برنامج Funk **ملاحظة:** ارجع إلى [مركز دعم عملاء شبكات Juniper](#).
- أدوات مساعدة العملاء لمصنعي المعدات الأصلية (OEM) من بعض المصنعين يمكنك تكوين WPA-PSK عندما:

- أنت تعرف التشفير أسلوب مثل تشفير بروتوكول سلامة المفاتيح المؤقتة (TKIP) في صفحة مدير التشفير.
 - أنت تحدد نوع المصادقة، واستخدام إدارة المفاتيح المصدق عليها، والمفتاح المشترك مسبقاً في علامة التبويب إدارة معرف مجموعة الخدمة (SSID) في واجهة المستخدم الرسومية.
 - لا يلزم وجود تكوين في علامة التبويب "مدير الخادم".
- دخلت in order to مكنت WPA-PSK من خلال ال ligne قارن (CLI)، هذا أمر. البدء من وضع التكوين:

```
AP(config)#interface dot11Radio 0
AP(config-if)#encryption mode ciphers tkip
AP(config-if)#ssid ssid_name
AP(config-if-ssid)#authentication open
AP(config-if-ssid)#authentication key-management wpa
AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

ملاحظة: يقدم هذا القسم التكوين ذي الصلة فقط ب WPA-PSK. التشكيل في هذا قسم فقط أن يمنحك فهم على كيف أن يمكن WPA-PSK ولا يكون التركيز من هذا وثيقة. يشرح هذا المستند كيفية تكوين WPA.

الاصطلاحات

التكوين

يعتمد WPA على طرق EAP/802.1x الحالية. يفترض هذا المستند أن لديك تكوين EAP خفيف (LEAP) أو EAP أو Protected EAP (PEAP) يعمل قبل إضافة التكوين لإشراك WPA.

يقدم هذا القسم معلومات تكوين الميزات الموضحة في هذا المستند.

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

EAP للشبكة أو مصادقة مفتوحة باستخدام EAP

في أي أسلوب مصادقة يستند إلى EAP/802.1x، قد تتساءل عن الاختلافات بين EAP-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 رغبتهم في إجراء مصادقة EAP لاحقاً في عملية الاقتران. تعين Cisco القيمة بشكل مختلف، من بداية الاقتران بعلامة EAP للشبكة.

أستخدم طريقة المصادقة التي تشير إليها هذه القائمة إذا كانت شبكتك تحتوي على عملاء:

- أستخدم عملاء Cisco Network-EAP.
- عملاء الطرف الثالث (والتي تتضمن ملحقات متوافقة مع سيسكو [CCX] منتجات متوافقة مع EAP) - استخدام المصادقة المفتوحة مع EAP.
- مزيج من كل من عملاء Cisco والأطراف الخارجية - أختار كلا من شبكة EAP والمصادقة المفتوحة مع EAP.

تكوين واجهة سطر الأوامر (CLI)

يستخدم هذا المستند التكوينات التالية:

- تكوين LEAP موجود ويعمل
- برنامج IOS الإصدار JA(15)12.2 من Cisco لـ APs المستندة إلى برنامج Cisco IOS

أسوشيتد برس

```
ap1#show running-config
...Building configuration
.
.
.
aaa new-model
!
aaa group server radius rad_eap
server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
```

```

no ip address
no ip route-cache
!
encryption mode ciphers tkip
This defines the cipher method that WPA uses. The ---!
TKIP !--- method is the most secure, with use of the Wi-
Fi-defined version of TKIP. ! ssid WPAlabap1200
authentication open eap eap_methods
This defines the method for the underlying EAP when ---!
third-party clients !--- are in use. authentication
network-eap eap_methods
This defines the method for the underlying EAP when ---!
Cisco clients are in use. authentication key-
management wpa
This engages WPA key management. ! speed basic-1.0 ---!
basic-2.0 basic-5.5 basic-11.0 rts threshold 2312
channel 2437 station-role root bridge-group 1 bridge-
group 1 subscriber-loop-control bridge-group 1 block-
unknown-source no bridge-group 1 source-learning no
bridge-group 1 unicast-flooding bridge-group 1 spanning-
disabled . . . interface FastEthernet0 no ip address no
ip route-cache duplex auto speed auto bridge-group 1 no
bridge-group 1 source-learning bridge-group 1 spanning-
disabled ! interface BVI1 ip address 192.168.2.108
255.255.255.0 !--- This is the address of this unit. no
ip route-cache ! ip default-gateway 192.168.2.1 ip http
server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable R0 snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-
port 1646 key shared_secret !--- This defines where the
RADIUS server is and the key between the AP and server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end ! end

```

تكوين GUI

أتمت هذا steps in order to شكلت ال AP ل WPA:

1. أكمل الخطوات التالية لإعداد مدير التشفير: تمكين التشفير ل TKIP. امسح القيمة في مفتاح التشفير 1. تعيين مفتاح التشفير 2 كمفتاح الإرسال. **#radio** يطبق

Cisco Systems
Cisco 1200 Access Point

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

RADIO0-802.11B RADIO1-802.11A

Hostname ldap1200p102 16:10:59 Tue Apr 6 2004

Security: Encryption Manager - Radio0 802.11B

Encryption Modes

None

WEP Encryption Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Cipher

Encryption Keys

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

Global Properties

Broadcast Key Rotation Interval: Disable Rotation
 Enable Rotation with Interval: (10-10000000 sec)

WPA Group Key Update: Enable Group Key Update On Membership Termination
 Enable Group Key Update On Member's Capability Change

Apply-Radio0 Apply-All Cancel

Close Window Copyright (c) 1993-2004 by Cisco Systems, Inc.

2. أكمل الخطوات التالية لإعداد إدارة SSID: حدد SSID المطلوب من قائمة SSID الحالية. اختر طريقة مصادقة مناسبة. بناء هذا القرار على نوع بطاقات العملاء التي تستخدمها. راجع قسم [EAP للشبكة أو مصادقة مفتوحة مع EAP](#) في هذا المستند للحصول على مزيد من المعلومات. إذا عمل EAP قبل إضافة WPA، ربما لا يكون التغيير ضرورياً. أتمت هذا steps in order to مكن المفتاح إدارة: اختر إلزامي من القائمة المنسدلة "إدارة المفاتيح". حدد خانة الاختيار WPA. طقطقة يطبق-radio#

The screenshot displays the configuration interface for a Cisco 1200 Access Point. The main configuration area is titled 'Security: SSID Manager - Radio 802.11B'. Under 'SSID Properties', the 'Current SSID List' shows a single entry 'WPA1abep1200'. The 'Authentication Settings' section includes 'Methods Accepted' with 'Open Authentication' and 'Network EAP' checked. 'Server Priorities' are set to 'Use Defaults' for both EAP and MAC Authentication Servers. In the 'Authenticated Key Management' section, 'Key Management' is set to 'Mandatory' and 'WPA' is checked, both of which are circled in red. The 'WPA Pre-shared Key' field is empty, and 'ASCII' is selected for the key format.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر `show`.

• `show dot11 association mac_address` — يعرض هذا الأمر معلومات حول عميل مرتبط محدد التعريف. تحقق من أن العميل يفاوض على إدارة المفاتيح ك WPA والتشفير ك TKIP.

```

Cisco - HyperTerminal
File Edit View Call Transfer Help
labap1200ip102#sho dot oss 0030.6527.f74a
Address      : 0030.6527.f74a      Name      :
IP Address   : 10.0.0.25           Interface : Dot11Radio 0
Device       : -                 Software  :
CCX Version  :
State        : EAP-Assoc         Parent    : self
SSID         : WPAlabap1200     VLAN     : 0
Hops to Infra : 1               Association Id : 4
Clients Associated: 0           Repeaters associated: 0
Tunnel Address : 0.0.0.0
Key Mgmt type : WPA              Encryption : TKIP
Current Rate  : 11.0            Capability :
Supported Rates : 1.0 2.0 5.5 11.0
Signal Strength : -61 dBm        Connected for : 797 seconds
Signal Quality : 88 %           Activity Timeout : 20 seconds
Power-save    : Off             Last Activity : 40 seconds ago

Packets Input : 57              Packets Output : 42
Bytes Input   : 10976           Bytes Output   : 6767
Duplicates Rcvd : 0            Data Retries  : 10
Decrypt Failed : 0              RTS Retries   : 0
MIC Failed    : 0
MIC Missing   : 0

labap1200ip102#

```

- كما يجب أن يشير إدخال جدول الاقتران لعمل معين إلى إدارة المفاتيح على أنها WPA والتشفير على أنه TKIP. في جدول الاقتران، انقر فوق عنوان MAC خاص لعمل للاطلاع على تفاصيل الاقتران لذلك العميل.

The screenshot shows the Cisco 1200 Access Point web interface. The main content area displays 'Association: Station View - Client' for the host name 'labap1200ip102'. A table provides detailed information about the associated client, with 'WPA' and 'TKIP' circled in red to match the terminal output above.

| Station Information and Status | | | |
|--------------------------------|---------------------|------------------------------|----------------|
| MAC Address | 0030.6527.f74a | Name | |
| IP Address | 0.0.0.0 | Class | |
| Device | | Software Version | |
| CCX Version | | | |
| State | EAP-Associated | Parent | self |
| SSID | WPAlabap1200 | VLAN | none |
| Hops To Infrastructure | 1 | Communication Over Interface | Radio0-802.11B |
| Clients Associated | 0 | Repeaters Associated | 0 |
| Key Mgmt type | WPA | Encryption | TKIP |
| Current Rate (Mb/sec) | 11.0 | Capability | |
| Supported Rates(Mb/sec) | 1.0, 2.0, 5.5, 11.0 | Association id | 4 |
| Signal Strength (dBm) | -64 | Connected For (sec) | 3 |
| Signal Quality (%) | 75 | Activity TimeOut (sec) | 59 |
| Power-save | Off | Last Activity (sec) | 1 |

[استكشاف الأخطاء وإصلاحها](#)

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إجراء استكشاف الأخطاء وإصلاحها

هذه المعلومات ذات صلة بهذا التكوين. أتمت هذا steps in order to تحريت تشكيك:

1. إذا لم يتم إختبار تهيئة LEAP أو EAP أو PEAP بدقة قبل تنفيذ WPA، فيجب عليك استكمال الخطوات التالية: تعطيل وضع تشفير WPA مؤقتاً. أعد تمكين EAP المناسب. تأكد من أن المصادقة تعمل.
2. تحقق من أن تكوين العميل يطابق تكوين نقطة الوصول. على سبيل المثال، عند تكوين نقطة الوصول ل WPA و TKIP، تأكد من تطابق الإعدادات التي تم تكوينها في العميل.

أوامر استكشاف الأخطاء وإصلاحها

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

تتضمن إدارة مفتاح WPA مصافحة رباعية بعد اكتمال مصادقة EAP بنجاح. يمكنك رؤية هذه الرسائل الأربع في تصحيح الأخطاء. إذا لم يتم EAP بمصادقة العميل بنجاح أو إذا لم يظهر لديك الرسائل، أكمل الخطوات التالية:

1. تعطيل WPA مؤقتاً.
 2. أعد تمكين EAP المناسب.
 3. تأكد من أن المصادقة تعمل.
- تصف هذه القائمة تصحيح الأخطاء:

- **debug dot11 aaa manager keys** — يعرض تصحيح الأخطاء هذا المصافحة التي تحدث بين نقطة الوصول وعميل WPA كمفاوضة المفتاح المؤقت (PTK) للمجموعة والمفتاح المؤقت (GTK). تم إدخال تصحيح الأخطاء هذا في برنامج Cisco IOS الإصدار JA(15)12.2. إذا لم تظهر أي مخرجات تصحيح أخطاء، فتتحقق من العناصر التالية: يتم تمكين مصطلح mon للمدرب الطرفي (إذا كنت تستخدم جلسة عمل Telnet). تم تمكين تصحيح الأخطاء. تم تكوين العميل بشكل مناسب ل WPA. إذا أظهر تصحيح الأخطاء أن مصافح PTK و/أو GTK تم بناؤها ولكن لم يتم التحقق منها، فتتحقق من برنامج مزود WPA للتكوين الصحيح والإصدار المحدث.
- **debug dot11 aaa** مصدق دولة-أداة— يعرض تصحيح الأخطاء هذا حالات المفاوضات المختلفة التي يمر بها العميل عندما يقترن ويصادق. تشير أسماء الولايات إلى هذه الحالات. تم إدخال تصحيح الأخطاء هذا في برنامج Cisco IOS الإصدار JA(15)12.2. ال debug يلغي ال **debug dot11 aaa dot1x** دولة-machine أمر في cisco ios برمجية إطلاق JA(15)12.2 وفيما بعد.
- **debug dot11 aaa dot1x state-machine** — يعرض تصحيح الأخطاء هذا حالات المفاوضات المختلفة التي يمر بها العميل عندما يقترن ويصادق. تشير أسماء الولايات إلى هذه الحالات. في إصدارات برنامج Cisco IOS software الأقدم من الإصدار JA(15)12.2 من برنامج Cisco IOS Software، يعرض تصحيح الأخطاء هذا أيضاً تفاوض إدارة مفتاح WPA.
- **عملية المصدق debug dot11 aaa** — يساعد تصحيح الأخطاء هذا كثيراً في تشخيص المشاكل المتعلقة بالاتصالات التي تم التفاوض عليها. وتبين المعلومات التفصيلية ما يرسله كل مشترك في التفاوض وتبين رد المشارك الآخر. يمكنك أيضاً استخدام تصحيح الأخطاء هذا بالاقتران مع أمر مصادقة **radius debug**. تم إدخال تصحيح الأخطاء هذا في برنامج Cisco IOS الإصدار JA(15)12.2. ال debug يلغي ال **debug dot11 aaa dot1x** عملية أمر في cisco ios برمجية إطلاق JA(15)12.2 وفيما بعد.
- **debug dot11 aaa dot1x** عملية— يساعد تصحيح الأخطاء هذا في تشخيص المشاكل المتعلقة بالاتصالات التي تم التفاوض عليها. وتبين المعلومات التفصيلية ما يرسله كل مشترك في التفاوض وتبين رد المشارك الآخر. يمكنك أيضاً استخدام تصحيح الأخطاء هذا بالاقتران مع أمر مصادقة **radius debug**. في إصدارات برنامج Cisco IOS software الأقدم من الإصدار JA(15)12.2 من برنامج Cisco IOS Software، يعرض تصحيح الأخطاء هذا تفاوض إدارة مفتاح WPA.

معلومات ذات صلة

- تكوين مجموعات التشفير و WEP
- تكوين أنواع المصادقة
- WPA2 - Wi-Fi Protected Access 2
- تكوين WPA 2 (Wi-Fi Protected Access 2)
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل