أخطاء وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) والأسئلة المتداولة حول رسائل النظام

المحتويات

المقدمة
الأسئلة المتداولة حول رسائل الخطأ
معلومات ذات صلة

المقدمة

يقدم هذا المستند معلومات حول الأسئلة الأكثر شيوعا (FAQ) حول رسائل الخطأ ورسائل النظام لوحدات التحكم في شبكة LAN اللاسلكية (WLCs) من Cisco.

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

الأسئلة المتداولة حول رسائل الخطأ

س. لقد بدأنا تحويل أكثر من 200 نقطة وصول (APs) من برنامج Cisco IOS® إلى بروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) باستخدام وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) طراز Cisco 4404. أكملنا تحويل 48 نقطة وصول وتتلقى رسالة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تفيد: [ERROR: spam_lrad.c 4212] .1 لماذا يحدث الخطأ؟

a. أنت ينبغي خلقت إضافي AP-manager قارن in order to ساندت أكثر من 48 APs. وإلا، فإنك تتلقى الخطأ الذي يبدو هكذا:

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
.the maximum number of APs on interface 1 is reached
```

قم بتكوين واجهات AP-Manager المتعددة وتكوين منافذ النسخ الاحتياطي/الأساسية التي لا تستخدمها واجهات AP-Manager الأخرى. أنت ينبغي خلقت ثان AP-manager قارن in order to جلبت إضافي APs. ولكن، تأكد من عدم تداخل تكوينات المنفذ الأساسي وميناء النسخ الاحتياطي لكل مدير. بمعنى أن، إن يستعمل 1 AP-Manager ميناء 1 كأساسي وميناء 2 كنسخة إحتياطية، 2 AP-Manager ينبغي استعملت ميناء 3 كأساسي وميناء 4 كنسخة إحتياطية.

Q. لدي وحدة تحكم في الشبكة المحلية (4402 WLC) وأستخدم 1240 نقطة وصول في الوضع Lightweight (LAPs). أنا أحاول تمكين تشفير 128-بت على ال WLC. عند تحديد تشفير WEP من فئة 128 بت على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، أستلم خطأ يقول إن 128 بت غير مدعوم على عنصر التحكم في الشبكة المحلية اللاسلكية (1240s): [ERROR] spam_lrad.c 12839: SSID mde Cisco AP xx:xx:xx:xx:xx:xx:xx:xx WEP128 . لماذا أستلم هذا الخطأ؟

أ. إن أطوال المفتاح الموضحة على WLCs هي في الواقع عدد وحدات بت التي هي في السر المشترك ولا تتضمن 24-بت من متجه التهيئة (IV). وكثير من المنتجات التي تتضمن منتجات Aironet تسميه مفتاح WEP 128 بت. في الواقع هو مفتاح 104 بت مع 24 بت IV. حجم المفتاح 104-بت هو ما يجب عليك تمكينه في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتشفير -128 WEPبت.

إذا أخترت حجم مفتاح 128-بت على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإنه في الواقع تشفير مفتاح -152 WEPبت (128+24 IV). فقط AP1030، AP1020، AP1010) cisco 1000 sery LAPs) دعم إستخدام ال 128 WLC بت WEP مفتاح إعداد.

س. لماذا أحصل على `WEP 128 WLAN .13xx 12xx 11xx` . رسالة خطأ عندما أحاول تكوين WEP على WLC؟

أ. على وحدة تحكم شبكة محلية لاسلكية، عندما تختار WEP ساكن إستاتيكي كطريقة تأمين الطبقة 2، فإن لديك هذه الخيارات أو حجم مفتاح WEP.

- غير محدد
- 40 بت
- 104 بت
- 128 بت

لا تتضمن قيم حجم المفتاح هذه متجه تهيئة 24-بت (IV)، والذي يتم ربطه بمفتاح WEP. لذلك، في حالة 64 WEP بت، تحتاج إلى إختيار **40 بت** بحجم مفتاح WEP. تضيف أداة التحكم ال 24-بت IV إلى هذا in order to جعلت 64-بت WEP مفتاح. بالمثل، أختر **104 بت** لمفتاح 128 WEP بت.

كما تدعم وحدات التحكم مفاتيح 152 WEP بت (128 بت + 24 بت IV). لا يتم دعم هذا التكوين على نقاط الوصول من الطراز 11xx و 12xx و 13xx. لذلك عندما تحاول تكوين WEP باستخدام 144 بت، فإن وحدة التحكم تعطي رسالة بأن تكوين WEP هذا لا يتم دفعه إلى نقاط الوصول من الطراز 11xx و 12xx و 13xx.

q. لا يمكن للعملاء المصادقة على شبكة WLAN التي تم تكوينها ل WPA2 ووحدة التحكم تعرض `APF_80211.c:1923 APF-1-proc_RSN_WARP_IE_FAILED :WLAN (RSN (WPA2 WARP IE RSN SSID :RSN.MobileStation:00:0c:0c:51:22` رسالة خطأ. لماذا أستلم هذا الخطأ؟

أ. يحدث هذا غالبا بسبب عدم التوافق في جانب العميل. حاولت هذا steps in order to صححت هذا إصدار:

- تحقق مما إذا كان العميل معتمدا على Wi-Fi ل WPA2 وفحص تكوين العميل ل WPA2.
- تحقق من ورقة البيانات لمعرفة ما إذا كانت الأداة المساعدة للعميل تدعم WPA2. قم بتثبيت أي تصحيح تم إصداره من قبل المورد لدعم WPA2. إذا كنت تستخدم الأداة المساعدة ل Windows، فتأكد من تثبيت حزمة WPA2 من Microsoft لدعم WPA2.
- ترقية برنامج التشغيل والبرامج الثابتة الخاصة بالعميل.
- قم بإيقاف تشغيل امتدادات Aironet على الشبكة المحلية اللاسلكية (WLAN).

Q. ما إن أعدت تشغيل ال WLC، أنا يحصل `mic 3023 - mon Jul 17 15:23:28 2006 MFP anomaly () xx:xx:xx:xx:xx:00 dot11 0 xx xx:xx:xx:xx:xx AP 00:xx:xx:xx:xx:xx 300 Beacon Frame` خطأ رسالة. لماذا يحدث هذا الخطأ وكيف يمكنني التخلص منه؟

أ. تظهر رسالة الخطأ هذه عندما يتم الكشف عن الإطارات ذات قيم MIC غير صحيحة بواسطة نقاط الوصول في الوضع Lightweight التي تم تمكين MFP بها. راجع حماية إطار إدارة البنية الأساسية (MFP) مع WLC ومثال تكوين نقاط الوصول في الوضع Lightweight للحصول على مزيد من المعلومات حول MFP. أكمل واحدة من الخطوات الأربع التالية:

1. تحقق من أي نقاط وصول (AP) أو عملاء غير صحيحين أو مارقين في شبكتك وإزالتهم، مما يؤدي إلى إنشاء

إطارات غير صالحة.
2. تعطيل MFP للبنية الأساسية، إذا لم يتم تمكين MFP على الأعضاء الآخرين في مجموعة التنقل لأن نقاط الوصول في الوضع Lightweight (LAPs) يمكنها سماع إطارات الإدارة من نقاط الوصول في الوضع Lightweight (LAPs) الخاصة بمجموعات التحكم في الشبكة المحلية اللاسلكية (WLCs) الأخرى في المجموعة التي لا تحتوي على تمكين MFP. راجع الأسئلة المتداولة حول مجموعات التنقل لوحدة تحكم الشبكة المحلية (LAN) اللاسلكية للحصول على مزيد من المعلومات حول مجموعة الأجهزة المحمولة.
3. يتوفر إصلاح رسالة الخطأ هذه في إصدار WLC 4.2.112.0 و 5.0.148.2. قم بترقية قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs) إلى أي من هذين الإصدارين.
4. كخيار أخير، حاول إعادة تحميل نقطة الوصول في الوضع Lightweight (LAP) التي تولد رسالة الخطأ هذه.

q. يرتبط العميل AIR-PI21AG-E-K9 بنجاح بنقطة وصول (AP) باستخدام مصادقة مرنة لبروتوكول المصادقة المتوسع عبر الاتصال النفقي الآمن (EAP-FAST). ومع ذلك، عند إيقاف تشغيل نقطة الوصول المقترنة، لا يجوب العميل إلى نقطة وصول أخرى. تظهر هذه الرسالة باستمرار في سجل رسائل وحدة التحكم: ▪ 214:48:49 2 - :security] 1x_auth_pae.c 1922] 2006 2 .ad:75:f4:00:40:96 :Security] apf_ms.c 2557] 2006 لماذا؟

أ. عندما تحتاج بطاقة العميل إلى القيام بالتجوال، فإنها ترسل طلب مصادقة، ولكنها لا تعالج المفاتيح بشكل صحيح (لا تعلم نقطة الوصول/وحدة التحكم، ولا تجيب على عمليات إعادة المصادقة).

وثقت هذا في cisco بق CSCsd02837 id (يسجل زبون فقط). تم إصلاح هذا الخطأ مع معالج تثبيت مهايئات عميل Cisco Aironet 802.11a/b/g 3.5.

بشكل عام، يحدث تعذر لرسالة لأي من هذه الأسباب:

- يتم إستخدام اسم المستخدم المحدد على أكثر من جهاز عميل واحد.
- أسلوب المصادقة المستخدم لتلك الشبكة المحلية اللاسلكية (WLAN) له هوية مجهولة خارجية. على سبيل المثال، في PEAP-GTC أو في EAP-FAST، من الممكن تعريف اسم مستخدم عام كهوية خارجية (مرئية)، واسم المستخدم الحقيقي مخفي داخل نفق TLS بين العميل وخادم radius، بحيث لا يمكن لوحدة التحكم رؤيته واستخدامه. في مثل هذه الحالات، يمكن أن تظهر هذه الرسالة. وتتم ملاحظة هذه المشكلة بشكل أكثر شيوعا مع جهة خارجية وبعض عملاء البرامج الثابتة القديمة.

س. عند تثبيت الخادم النصلي الجديد للوحدة النمطية للخدمات اللاسلكية (WiSM) في المحول 6509 وتنفيذ بروتوكول المصادقة المتوسع المحمي (PEAP) مع خادم Microsoft IAS، أستلم هذا الخطأ:* :Discovery *MAR 100:23.700: SYS-5-RELOAD LWAPP :MAR 100:00:23.526: LWAPP-5-CHANGED DOWN *Mar LWAPP :INIT. *Mar 100:00:23.700: LWAPP-5-CHANGED LWAPP client.Reload Mar 100:00:23.557: LWAPP_ERROR_CRYPTO_init_sskeys_TS* LWAPP :100:00:23.528: LWAPP-5-CHANGED Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *Mar 100:00:23.557: lwapp_crypto_init:* SSC .LWAPP :PKI_StartSession failed *Mar 100:00:23.706: SYS-5-Reload . لماذا؟

A. يظهر تصحيح أخطاء RADIUS و dot1x أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يرسل طلب وصول، ولكن لا توجد إستجابة من خادم IAS. أتمت هذا steps in order to تحريت المشكلة:

1. تحقق من تكوين خادم IAS وتحقق منه.
2. تحقق من ملف السجل.
3. تثبيت البرامج، مثل EtherAl، التي يمكن أن تمنحك تفاصيل المصادقة.
4. إيقاف تشغيل خدمة IAS.

س. نقاط الوصول في الوضع Lightweight (LAPs) لا يتم تسجيلها مع وحدة التحكم. ما قد تكون المشكلة؟ أرى رسائل الخطأ هذه على وحدة التحكم: LWAPP :2028 203:20:47 3

```
.00:0b:85:68:F4:F0      :2028 03:20:47 : 3  .AP 00:0b:85:68:f4:f0  CERTIFICATE_PAYLOAD
```

أ. عندما ترسل نقطة الوصول (AP) طلب الانضمام إلى بروتوكول نقطة الوصول في الوضع (Lightweight (LWAPP إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإنها تدمج شهادة X.509 الخاصة بها في رسالة LWAPP. كما يقوم بإنشاء معرف جلسة عمل عشوائي يتم تضمينه في طلب الانضمام إلى LWAPP. عندما يستلم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طلب الانضمام إلى LWAPP، فإنه يتحقق من توقيع شهادة X.509 باستخدام مفتاح APs العام ويتحقق من إصدار الشهادة من قبل مرجع مصدق موثوق به. كما تبحث في تاريخ ووقت بدء الفاصل الزمني لصلاحية شهادة AP، وتقارن ذلك التاريخ والوقت بالتاريخ والوقت الخاصين بها.

يمكن أن تحدث هذه المشكلة بسبب إعداد ساعة غير صحيح على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). أصدرت in order to ثبتت الساعة على ال WLC، **العرض وقت** و**config وقت** أمر.

q. نقطة الوصول لبروتوكول نقطة الوصول في الوضع (Lightweight (LWAPP غير قادرة على الانضمام إلى وحدة التحكم الخاصة بها. يعرض سجل وحدة تحكم الشبكة المحلية اللاسلكية (WLC) رسالة مماثلة لهذا: `.AP 00:0b:85:68:ab:01  CERTIFICATE_PAYLOAD  LWAPP` لماذا؟

a. يمكنك تلقي رسالة الخطأ هذه إذا كان نفق LWAPP بين نقطة الوصول و WLC يجتاز مسار شبكة مع MTU أقل من 1500 بايت. وهذا يتسبب في تجزئة حزم LWAPP. هذا خطأ معروف في وحدة التحكم. أحلت cisco بق id CSCsd39911 (يسجل زبون فقط).

يتمثل الحل في ترقية البرنامج الثابت لوحدة التحكم إلى 4.0(155).

س. أحاول إنشاء قنوات مضيفة بين وحدة التحكم الداخلية الخاصة بي ووحدة تحكم المرساة الافتراضية على المنطقة المنزوعة السلاح. ومع ذلك، عندما يحاول المستخدم الاقتران ب SSID ضيف، يتعذر على المستخدم تلقي عنوان IP من DMZ، كما هو متوقع. لذلك، لا يتم إنشاء قنوات لحركة مرور المستخدم إلى وحدة التحكم على DMZ. يعرض إخراج الأمر debug mobile delivery رسالة مماثلة لهذا: `.WLAN <WLAN ID  .<IP: <controller ip address` ما هي المشكلة؟

ألف - يوفر الاتصال النفقي للزوار أمانا إضافيا لوصول المستعملين الضيوف إلى الشبكة اللاسلكية للشركة. وهذا يساعد على ضمان عدم قدرة المستخدمين الضيوف على الوصول إلى شبكة الشركة دون المرور أولا عبر جدار حماية الشركة. عندما يقترن مستخدم بشبكة WLAN معينة كشبكة WLAN ضيفة، يتم إنشاء قنوات حركة مرور المستخدم إلى وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) الموجودة على المنطقة DMZ خارج جدار حماية الشركة.

الآن، بالنظر إلى هذا السيناريو، يمكن أن يكون هناك عدة أسباب لعدم عمل نفق هذا الضيف كما هو متوقع. كما يشير إخراج أمر **debug**، قد تكون المشكلة في عدم التطابق في أي من سياسات الأمان التي تم تكوينها لشبكة WLAN المحددة في وحدات التحكم في DMZ الداخلية كذلك. تحقق ما إذا كانت سياسات التأمين وكذلك الإعدادات الأخرى، مثل إعدادات مهلة الجلسة، متطابقة.

سبب شائع آخر لهذه المشكلة هو عدم ربط وحدة التحكم في DMZ بنفسها لتلك الشبكة المحلية اللاسلكية (WLAN) المحددة. لكي يعمل نفق الضيف بشكل صحيح ولكي يتمكن DMZ من إدارة عنوان IP الخاص بالمستخدم (المستخدم الذي ينتمي إلى شبكة WLAN الضيف)، فمن الضروري أن يتم إنشاء الترابط المناسب لشبكة WLAN المحددة.

س. أرى الكثير من " برسائل " في وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) لعام 2006، ولكن ليس في وحدات التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 4400. لماذا؟ لقد قمت بتعطيل البث المتعدد على وحدات التحكم. ما هو الفرق في حد قائمة انتظار البث المتعدد بين أنظمة WLC الأساسية 2006 و 4400؟

a. نظرا لتعطيل البث المتعدد على وحدات التحكم، قد تكون الرسائل التي تسبب هذا التنبيه رسائل بروتوكول تحليل العنوان (ARP). لا يوجد فرق في عمق قائمة الانتظار (512 حزمة) بين قوائم التحكم في الشبكة المحلية اللاسلكية

(WLC) لعام 2000 وقوائم التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 4400. الفرق هو أن NPU 4400 تقوم بتصفية حزم ARP بينما يتم عمل كل شيء في برمجية على ال 2006. هذا يفسر لما ال WLC 2006 يرى الرسالة غير ال WLC 4400. يعالج عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 44xx حزم البث المتعدد عبر الأجهزة (من خلال وحدة المعالجة المركزية). يعالج WLC 2000 حزم البث المتعدد عبر البرنامج. تعتبر معالجة وحدة المعالجة المركزية أكثر فعالية من البرامج. وبالتالي، يتم مسح قائمة انتظار ال 4400 بشكل أسرع، في حين أن WLC لعام 2006 يعاني بعض الشيء عندما ترى الكثير من هذه الرسائل.

Q. أرى أن "`[security] apf_foreignNap.c 763: STA [00:0a:E4:36:1f:9b] 1`". رسالة خطأ في إحدى وحدات التحكم الخاصة بي. ما معنى هذا الخطأ وما الخطوات التي يجب إتخاذها لحله؟

أ. يرى هذا رسالة عندما يستلم الجهاز تحكم طلب DHCP لعنوان MAC والذي ليس له جهاز حالة. وغالبا ما يرى ذلك من جسر أو نظام يشغل جهازا افتراضيا مثل VMWare. تستمع وحدة التحكم إلى طلبات DHCP لأنها تقوم بإجراء التطفل على بروتوكول DHCP حتى تعرف العناوين التي يتم ربطها بالعملاء الذين يتم إرفاقهم بنقاط الوصول (APs) الخاصة بها. تمر كل حركات مرور الأجهزة اللاسلكية العميلة عبر وحدة التحكم. عندما تكون وجهة الحزمة عبارة عن عميل لاسلكي، فإنها تنتقل إلى وحدة التحكم ثم تمر عبر نفق بروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) إلى نقطة الوصول وتخرج إلى العميل. واحد شيء أن يستطيع كنت عملت أن يساعد تخفيف هذا رسالة أن يسمح فقط VLANs أن يكون استعملت على الجهاز تحكم إلى الشنطة أن يذهب إلى الجهاز تحكم مع ال **switchport vlan** يسمح أمر على المفتاح.

Q. لماذا أرى رسالة الخطأ هذه على وحدة التحكم: `MSG ' ' = 0x0050b986 = 0xfffffc`؟

أ. قد يرجع ذلك إلى إرتفاع حمل وحدة المعالجة المركزية. عندما يتم تحميل وحدة المعالجة المركزية (CPU) بوحدة التحكم بشكل كبير، كما هو الحال عندما تقوم بنسخ ملفات أو مهام أخرى، فليس لديها الوقت لمعالجة جميع وحدات التحكم في الوصول (ACKs) التي ترسلها وحدة المعالجة المركزية (NPU) إستجابة لرسائل التكوين. وعند حدوث ذلك، تقوم وحدة المعالجة المركزية (CPU) بإنشاء رسائل خطأ. ومع ذلك، لا تؤثر رسائل الخطأ على الخدمة أو الوظيفة.

وثقت هذا في الإثقال جهاز تحكم cpu قسم من الإصدار بطاقة ل cisco لاسلكي lan جهاز تحكم وخفيف وزن منفذ نقطة للإصدار 3.2.116.21.

س. إنني أستلم رسائل الخطأ الأساسية المتعلقة بالخصوصية المكافئة للتوصيل السلكي (WEP) على نظام التحكم اللاسلكي (WCS): `WEP . MAC 'xx:xx:xx:xx:xx:xx' MAC 'xx:xx:xx:xx:xx:xx' '1'`. ومع ذلك، فأنا لا أستخدم WEP كمعلمة أمان في شبكتي. أستخدم فقط Wi-Fi Protected Access (WPA). لماذا أستلم رسائل خطأ WEP هذه؟

أ. إذا كانت جميع التكوينات المتعلقة بالأمان مثالية، فإن الرسائل التي تتلقاها الآن هي بسبب الأخطاء. هناك بعض الأخطاء المعروفة في وحدة التحكم. أحلت cisco بق CSCse17260 id (يسجل زبون فقط) و CSCse11202 (يسجل زبون فقط)، أي بذكر "ال WEP مفتاح بشكل في المحطة يكون خطأ مع WPA و TKIP زبون على التوالي". في الواقع، **CSCse17260** هو تكرار ل **CSCse11202**. يتوفر بالفعل إصلاح **CSCse11202** مع الإصدار 3.2.171.5 من WLC.

ملاحظة: تحتوي أحدث إصدارات عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) على إصلاح لهذه الأخطاء.

س. نستخدم خادم RADIUS الخارجي لمصادقة العملاء اللاسلكيين من خلال وحدة التحكم. ترسل وحدة التحكم رسالة الخطأ هذه بشكل منتظم: `RADIUS .` لماذا نرى رسائل الخطأ هذه؟

أ. عند خروج طلب من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إلى خادم RADIUS، تحتوي كل حزمة على رقم تسلسل تتوقع WLC إستجابة له. إذا لم تكن هناك إستجابة، فهناك رسالة تظهر `radius`.

الوقت الافتراضي ل WLC للاستماع مرة أخرى من خادم RADIUS هو 2 ثانية. يتم تعيين ذلك من واجهة المستخدم

الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) تحت **الأمان > خادم المصادقة**. الحد الأقصى هو 30 ثانية. لذلك، قد يكون من المفيد تعيين قيمة المهلة الزمنية هذه إلى الحد الأقصى لها لحل هذه المشكلة.

في بعض الأحيان، تنفذ خوادم RADIUS **'المرتجعات الصامتة'** لحزمة الطلب التي تأتي من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يمكن أن يرفض خادم RADIUS هذه الحزم بسبب عدم تطابق الشهادة والعديد من الأسباب الأخرى. هذا إجراء صحيح من قبل الخادم. وفي مثل هذه الحالات أيضا، ستعلم وحدة التحكم خادم RADIUS على أنه لا يستجيب.

من أجل التغلب على مشكلة المرتجعات الصامتة، قم بتعطيل ميزة **تجاوز الفشل العدوانية** في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

في حال تمكين ميزة **تجاوز الفشل** القوية في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يكون عدوانيا للغاية لوضع علامة على خادم AAA على أنه لا يستجيب. ومع ذلك، لا ينبغي القيام بذلك لأن خادم AAA قد لا يستجيب فقط لذلك العميل المعين (من خلال تنفيذ تجاهل صامت). يمكن أن يكون إستجابة لعملاء آخرين صحيحين (بشهادات صالحة). ومع ذلك، قد تستمر عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في تمييز خادم AAA على أنه لا يستجيب ولا يعمل.

للتغلب على هذا الأمر، قم بتعطيل ميزة **تجاوز الفشل** القوية. قم بإصدار الأمر **config radius aggressive-failover disable** من واجهة سطر الأوامر (CLI) لوحدة التحكم لتنفيذ هذا الأمر. في حالة تعطيل هذا الخيار، يفشل وحدة التحكم فقط في الوصول إلى خادم AAA التالي إذا كان هناك 3 عملاء متتالين يخفقون في تلقي إستجابة من خادم RADIUS.

Q. يتعذر على العديد من العملاء الاقتران ب LWAPP ويسجل جهاز التحكم رسالة `IAPP-3-MSGTAG015: iappSocketTask :iappRecvPkt` رسالة خطأ. لماذا يحدث هذا؟

أ. يحدث هذا غالبا بسبب مشكلة في مهايئات Intel التي تدعم CCX V4، ولكنها تشغل إصدار حزمة عميل أقدم من 10.5.1.0. إذا قمت بترقية البرنامج إلى 10.5.1.0 أو إصدار أحدث، فسيقوم هذا بإصلاح هذه المشكلة. راجع معرف تصحيح الأخطاء من CSCsi91347 Cisco (العملاء المسجلون فقط) للحصول على مزيد من المعلومات حول رسالة الخطأ هذه.

س. أرى رسالة الخطأ هذه على وحدة تحكم الشبكة المحلية اللاسلكية (WLC): `(EAP (21 STA 00:05:4e:42:ad:c5.` لماذا؟

أ. تحدث رسالة الخطأ هذه عندما يحاول المستخدم الاتصال بشبكة WLAN محمية من EAP وفشل في الرقم المكون مسبقا لمحاولات EAP. عند فشل المستخدم في المصادقة، تستثني وحدة التحكم العميل ولا يمكن للعميل الاتصال بالشبكة حتى تنتهي صلاحية مؤقت الاستثناء أو يتم تخطيه يدويا بواسطة المسؤول.

يكتشف الاستثناء محاولات المصادقة التي يقوم بها جهاز واحد. عندما يتجاوز هذا الجهاز الحد الأقصى لعدد مرات الفشل، لا يسمح لعنوان MAC هذا بالاقتران أكثر من ذلك.

يحدث الاستبعاد:

- بعد 5 حالات فشل مصادقة متتالية للمصادقة المشتركة (يتم إستبعاد المحاولة السادسة)
- بعد 5 حالات فشل اقتران متتالية لمصادقة MAC (يتم إستبعاد المحاولة السادسة)
- بعد 3 مرات فشل مصادقة EAP/802.1X متتالية (استبعدت المحاولة الرابعة)
- أي فشل لخادم النهج الخارجي (NAC)
- أي مثيل تكرار لعنوان IP
- بعد ثلاث مرات فشل متتالية لمصادقة الويب (تم إستبعاد المحاولة الرابعة)

يمكن تكوين وحدة التوقيت لمدة إستثناء عميل، ويمكن تمكين الاستبعاد أو تعطيله على مستوى وحدة التحكم أو شبكة WLAN.

س. أرى رسالة الخطأ هذه على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC): 1 WLCSCH01/10.0.16.5 '10.0.16.5' RADIUS () . ما هي المشكلة؟

a. قد يكون هذا بسبب cisco بق CSCsc05495 id. بسبب هذا الخطأ، تقوم وحدة التحكم بشكل دوري بحقن زوج AV غير صحيح (السمة 24، "الحالة") في رسائل طلب المصادقة التي تنتهك RADIUS RFP وتسبب مشاكل لبعض خوادم المصادقة. تم إصلاح هذا الخطأ في 3.2.179.6.

س. إنني أستلم رسالة فشل ملف تعريف الضوضاء تحت جهاز العرض > أجهزة راديو 802. g/11b. أريد أن أفهم لماذا أرى هذه الرسالة الفاشلة؟

أ. يتم تعيين حالة "فشل/تجاوز ملف تعريف التشويش" بعد نتيجة الاختبار التي تم إجراؤها بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وبالمقارنة مع حد المجموعة الحالي. بشكل افتراضي، يتم تعيين قيمة التشويش على -70. تشير حالة FAILED إلى أنه قد تم تجاوز قيمة الحد لتلك المعلمة المحددة أو نقطة الوصول (AP). يمكنك ضبط المعاملات في التوصيف، ولكن يوصى بتغيير الإعدادات بعد أن تفهم تصميم الشبكة بوضوح وكيف سيؤثر ذلك على أداء الشبكة.

يتم تعيين الحدود المعتمدة/الفاشلة لإدارة الموارد اللاسلكية (RRM) بشكل عام لجميع نقاط الوصول (APs) على **المعلمات العالمية Auto RF > 802.11a** و**المعلمات العمومية 802.11b/g >** صفحات **RF التلقائية**. يتم تعيين حدود RRM التي تم تمريرها/فشلها بشكل فردي لنقطة الوصول هذه على **واجهات نقطة الوصول 802.11 >** صفحة **ملف تعريف الأداء**.

Q. أنا يستطيع لا يثبت ميناء 2 كالنسخة إحتياطية ميناء ل ال AP-manager قارن. رسالة الخطأ التي تم إرجاعها. أنا قادر أن يثبت ميناء 2 كالنسخة إحتياطية ميناء لواجهة الإدارة. المنفذ النشط الحالي لكل من الواجهات هو المنفذ 1. لماذا؟

أ. لا يحتوي AP-manager على منفذ نسخ إحتياطي. كان هذا النظام معتمدا في الإصدارات السابقة. لا يتم دعم منفذ النسخ الاحتياطي لواجهة AP-Manager منذ الإصدار 4.0 والإصدارات الأحدث. كقاعدة، يجب تكوين مدير نقطة وصول واحد على كل منفذ (بدون نسخ إحتياطي). إذا كنت تستخدم تجميع الارتباطات (LAG)، فلا يوجد سوى مدير واحد لنقطة الوصول (AP).

يجب تخصيص واجهة AP-Manager الثابتة (أو الدائمة) لمنفذ نظام التوزيع 1 ويجب أن يكون لها عنوان IP فريد. لا يمكن تعيينها إلى منفذ نسخ إحتياطي. عادة ما يتم تكوينها على شبكة VLAN نفسها أو شبكة IP الفرعية كواجهة الإدارة، ولكن هذا ليس متطلبا.

Q. أرى رسالة الخطأ هذه: 60 '00:13:02:8d:f6:41' '1' WPA MIC '00:0b:85:67:6b:0' . لماذا؟

أ. يشمل فحص سلامة الرسائل (MIC) المدمج في Wi-Fi Protected Access (WPA) عداد إطارات يمنع هجوم الدخيل. هذا الخطأ يعني أن شخصا ما في الشبكة يحاول إعادة تشغيل الرسالة التي تم إرسالها بواسطة العميل الأصلي، أو قد يعني ذلك أن العميل معيب.

إذا فشل العميل في التحقق من MIC بشكل متكرر، تقوم وحدة التحكم بتعطيل شبكة WLAN على واجهة نقطة الوصول حيث يتم اكتشاف الأخطاء لمدة 60 ثانية. تم تسجيل فشل الميكروفون الأول، ويتم بدء تشغيل المؤقت لتمكين تنفيذ التدابير المضادة. في حالة حدوث عطل ميكروفون لاحق في غضون 60 ثانية من آخر فشل سابق، فإنه يجب على STA الذي قام كيان IEEE 802.1X الخاص به بالتصرف كمسبب، إجراء مصادقة نفسه أو إلغاء مصادقة كافة STAs باستخدام اقتران أمان إذا كان كيان IEEE 802.1X الخاص به يعمل كمصدق.

علاوة على ذلك، لا يستقبل الجهاز أو يبث أي إطارات بيانات مشفرة TKIP، ولا يستقبل أو يبث أي إطارات بيانات غير مشفرة بخلاف رسائل IEEE 802.1X، إلى أو من أي نظير لمدة 60 ثانية على الأقل بعد أن يكتشف الفشل الثاني. إذا كان الجهاز نقطة وصول، فإنه لا يسمح بالاقترانات الجديدة مع TKIP خلال هذه الفترة التي تبلغ 60 ثانية، وفي نهاية

الفترة التي تبلغ 60 ثانية، تستأنف نقطة الوصول العمليات العادية وتسمح لأنواع STA (إعادة)الاقتران.

وهذا يمنع الهجوم المحتمل على نظام التشفير. لا يمكن إيقاف تشغيل أخطاء الميكروفون هذه في إصدارات WLC قبل 4.1. باستخدام الإصدار 4.1 من وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية والإصدارات الأحدث، هناك أمر لتغيير وقت المسح بحثا عن أخطاء الميكروفون. الأمر هو **config wlan security tkip hold-down <0-60> ثاني <wlan id>**. أستخدم القيمة 0 لتعطيل اكتشاف فشل MIC للتدابير المضادة.

Q. رأيت هذا خطأ رسالة في جهاز تحكم سجل: **[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed.** لماذا؟

أ. تشاهد رسائل الخطأ هذه غالبا عندما يكون منفذ الخدمة لوحدة التحكم قد تم تمكين DHCP، ولكنه لا يتلقى عنوان IP من خادم DHCP.

بشكل افتراضي، تحتوي واجهة منفذ الخدمة المادية على عميل DHCP مثبت وتبحث عن عنوان عبر DHCP. يحاول عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طلب عنوان DHCP لمنفذ الخدمة. إن ما من DHCP نادل يكون يتوفر، بعد ذلك DHCP طلب ل الخدمة ميناء يفشل. لذلك، يلد هذا الخطأ رسالة.

ال workaround أن يشكل عنوان ساكن إستاتيكي إلى الخدمة ميناء (even if الخدمة ميناء يكون مفصول) أو يتلقى DHCP نادل يتوفر أن يعين عنوان إلى الخدمة ميناء. ثم، قم بإعادة تحميل وحدة التحكم، إذا لزم الأمر.

تم بالفعل حجز منفذ الخدمة للإدارة خارج النطاق لوحدة التحكم واستعادة النظام والصيانة في حالة فشل الشبكة. هو أيضا الميناء وحيد أن يكون نشط عندما الجهاز تحكم يكون في جزمة أسلوب. لا يمكن لمنفذ الخدمة حمل علامات 802.1Q. لذلك، هو ينبغي كنت ربطت إلى منفذ منفذ منفذ على المفتاح مجاور. إستخدام منفذ الخدمة إختياري.

تتحكم واجهة منفذ الخدمة في الاتصالات من خلال النظام وتعيينه بشكل ثابت على منفذ الخدمة. يجب أن يكون له عنوان IP على شبكة فرعية مختلفة من الإدارة و AP-Manager وأي واجهات ديناميكية. أيضا، لا يمكن تعيينها إلى منفذ نسخ إحتياطي. يمكن أن يستخدم منفذ الخدمة DHCP للحصول على عنوان IP، أو يمكن تعيين عنوان IP ثابت له، ولكن لا يمكن تعيين عبارة افتراضية لواجهة منفذ الخدمة. يمكن تحديد المسارات الثابتة من خلال وحدة التحكم للوصول إلى الشبكة البعيدة إلى منفذ الخدمة.

س. لا يستطيع زبائني اللاسلكي الاتصال بشبكة LAN اللاسلكية (WLAN). يبلغ WiSM الذي تتصل نقطة الوصول (AP) به هذه الرسالة: **00:0g:23:05:7d:d0} AP DoS 0 00:00:00:00:00:00 MAC.** ماذا يعني هذا؟

أ. كشرط للوصول إلى الوسط، يتحقق طبقة MAC من قيمة متجه تخصيص الشبكة (NAV) الخاص بها. يمثل NAV قيمة العداد في كل محطة تمثل مقدار الوقت الذي يحتاج الإطار السابق إلى إرسال إطاره. يجب أن تكون قيمة NAV صفر قبل أن تتمكن المحطة من محاولة إرسال إطار. قبل إرسال إطار، تقوم المحطة بحساب مقدار الوقت اللازم لإرسال الإطار بناء على طول الإطار ومعدل البيانات. تضع المحطة قيمة تمثل هذا الوقت في حقل المدة في رأس الإطار. عندما تتلقى المحطات الإطار، فإنها تفحص قيمة حقل المدة هذه وتستخدمها كأساس لتعيين NAVs المقابلة لها. تحتفظ هذه العملية بالمتوسط للمحطة المرسلة.

يشير NAV العالي إلى وجود قيمة NAV متضخمة (آلية إستشعار شركة النقل الظاهرية ل 802.11). إذا كان عنوان MAC الذي تم الإعلام عنه هو 00:00:00:00:00، فمن المحتمل أن يكون قد تم انتحال (من المحتمل أن يكون هجوما حقيقيا) وتحتاج إلى تأكيد ذلك باستخدام التقاط الحزمة.

Q. بعد تكوين وحدة التحكم وإعادة تشغيلها، لن نتمكن من الوصول إلى وحدة التحكم في وضع ويب الآمن (https). يتم تلقي رسالة الخطأ هذه أثناء محاولة الوصول إلى وضع ويب الآمن لوحدة التحكم: (). ما هو سبب هذه المشكلة؟

ألف - يمكن أن تكون هناك عدة أسباب مرتبطة بهذه المسألة. قد يكون هناك سبب مشترك واحد متعلق بتكوين الواجهة الظاهرية لوحدة التحكم. لحل هذه المشكلة، قم بإزالة الواجهة الظاهرية ثم أعد إنشاؤها باستخدام هذا

الأمر:

```
WLC>config interface address virtual 1.1.1.1
```

ثم قم بإعادة تشغيل وحدة التحكم. بعد إعادة تمهيد وحدة التحكم، قم بإعادة إنشاء شهادة مصادقة الويب محليا على وحدة التحكم باستخدام هذا الأمر:

```
WLC>config certificate generate webauth
```

في مخرجات هذا الأمر، يجب أن ترى هذه الرسالة: .

الآن، يجب أن تكون قادرا على الوصول إلى وضع ويب الآمن لوحدة التحكم عند إعادة التشغيل.

Q. تقوم وحدات التحكم أحيانا بالإبلاغ عن رسالة التنبيه هذه الخاصة ب "إلغاء اقتران توقيع طوفان IDS" ضد عملاء صحيحين يكون عنوان MAC للمهاجم هو عنوان نقطة وصول (AP) منضم إلى وحدة التحكم هذه: '.'x.x.x.x' '802.11b/g' '<AP '<AP name "Disassoc flood' 'Disassociation flood' MAC .'x' "hh:hh:hh:hh:hh:hh" "x" "x". ولماذا يحدث ذلك؟

a. هذا بسبب cisco بق CSCsg81953 id (يسجل زبون فقط).

أحيانا ما يتم الإبلاغ عن هجمات تدفق IDS على العملاء الصحيحين حيث يكون عنوان MAC للمهاجم هو عنوان AP الذي تم انضمامه إلى جهاز التحكم.

عندما يكون العميل مقترنا بنقطة الوصول ولكنه يتوقف عن الاتصال بسبب إزالة البطاقة والتجوال خارج النطاق، إلخ، إلى نقطة الوصول، فإن نقطة الوصول ستنتظر حتى انتهاء مهلة الخمول. بمجرد الوصول إلى مهلة الخمول، ترسل نقطة الوصول إلى ذلك العميل إطارا غير مرتبط. عندما لا يعترف العميل بالإطار المفكك، تعيد نقطة الوصول إرسال الإطار عدة مرات (حوالي 60 إطارا). يقوم النظام الفرعي لمعرف الهوية الخاص بوحدة التحكم بسماع رسائل الإرسال والتنبيهات هذه باستخدام هذه الرسالة.

تم حل هذا الخطأ في الإصدار 4.0.217.0. قم بترقية إصدار وحدة التحكم إلى هذا الإصدار للتغلب على رسالة التنبيه هذه مقابل العملاء والنقاط الوصول الصالحة.

Q. أنا أستلم هذا خطأ رسالة في ال syslog من الجهاز تحكم: :WARNING] apf_80211.c 2408] :apf_utils.c 198 [] <xx:xx:xx:xx:xx:xx> . لماذا؟

أ. في الواقع، تشير رسائل إلى أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه لمعدلات بيانات مطلوبة معينة ضمن الإعدادات اللاسلكية، ولكن بطاقة واجهة الشبكة (NIC) تفتقد المعدل المطلوب.

إذا كانت لديك معدلات بيانات، مثل 1 و 2 م، معينة على جهاز التحكم المطلوب، ولكن لا تتصل بطاقة واجهة الشبكة (NIC) بمعدلات البيانات هذه، فيمكنك تلقي هذا النوع من الرسائل. هذا سوء سلوك بطاقة NIC. ومن ناحية أخرى، إذا كانت وحدة التحكم الخاصة بك هي 802.11g ممكنة والعميل هو بطاقة 802.11b(فقط)، فهذه رسالة مشروعة. إذا لم تتسبب هذه الرسائل في أي مشاكل وكان من الممكن أن تظل البطاقات متصلة، يمكن تجاهل هذه الرسائل . إذا كانت الرسائل خاصة بالبطاقة، فتأكد من أن برنامج تشغيل هذه البطاقة محدث.

q. هذه syslog :001f.ca26.bfb4: LWAPP-3-CLIENTERRORLOG: Decode msg:يتم بث رسالة <WLAN <id الخطأ على شبكتنا. لماذا يحدث هذا وكيف أوقفه؟

أ. يتم بث هذه الرسالة بواسطة نقاط الوصول في الوضع Lightweight. ويتضح ذلك عندما تقوم بتكوين ميزة تجاوز WLAN لشبكة WLAN وتلك الشبكة المحلية اللاسلكية الخاصة لا يتم الإعلان عنها.

قم بتكوين `config ap syslog host global 0.0.0.0` لإيقاف ذلك أو يمكنك وضع عنوان IP محدد إذا كان لديك خادم syslog حتى يتم بث الرسالة إلى الخادم وحده.

Q. أنا أستلم هذا خطأ رسالة على لاسلكي lan جهاز تحكم (WLC): `[] : apf_mm.c : :581` `00:90:7a:05:56:8a` . لماذا؟

أ. بشكل عام، تشير رسالة الخطأ هذه إلى أن جهاز التحكم قد أعلن عن تصادمات لعميل لاسلكي (أي نقاط وصول منفصلة تعلن أن لديهم العميل)، ولم يتلق جهاز التحكم أي تحويل من نقطة وصول إلى أخرى. لا توجد حالة شبكة لصيانتها. قم بحذف العميل اللاسلكي واجعل العميل يحاول مرة أخرى. إذا حدثت هذه المشكلة بشكل متكرر، فقد تكون هناك مشكلة في تكوين التنقل. وإلا، فقد يكون شذوذا متعلقا بعميل أو شرط معين.

س. يوجه جهاز التحكم رسالة الإنذار هذه: `'12'. ما هو هذا الخطأ وكيف يمكن حله؟`

أ. يتم رفع رسالة التنبيه هذه عندما تنخفض نسبة إشارة إلى ضوضاء العميل (SNR) إلى أقل من قيمة حد SNR للراديو المعين. 12 هي قيمة حد SNR الافتراضية لاكتشاف فتحة التغطية.

تحدد خوارزمية اكتشاف فتحة التغطية وتصحيحها ما إذا كانت هناك فتحة تغطية عند مرور مستويات SNR الخاصة بالعملاء أسفل حد SNR معين. يختلف حد SNR هذا بناء على قيمتين: طاقة إرسال AP وقيمة ملف تعريف تغطية وحدة التحكم.

بالتفصيل، يتم تحديد حد SNR للعميل بواسطة كل قوة إرسال لنقطة الوصول (ممثلة في dBm)، ناقص القيمة الثابتة 17dBm، ناقص قيمة ملف تعريف تغطية قابل للتكوين الخاص بالمستخدم (يتم تعيين هذه القيمة افتراضيا إلى 12 ديسيبل).

- **قيمة قطع SNR للعميل (|dB|) = [طاقة إرسال AP (dBm) - ثابت (17 dBm) - ملف تعريف التغطية (dB)]**

يمكن الوصول إلى قيمة ملف تعريف التغطية القابلة للتكوين هذه من قبل المستخدم بهذه الطريقة:

1. في واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى العنوان الرئيسي للشبكة اللاسلكية وحدد خيار **الشبكة** الخاص بمعيار الاختيار للشبكة المحلية اللاسلكية (WLAN) على الجانب الأيسر (802.11a أو 802.11b/g). بعد ذلك، حدد **التردد اللاسلكي التلقائي** في أعلى يمين النافذة.
2. في صفحة معلمات RF العمومية التلقائية، ابحث عن قسم حدود التوصيفات. في هذا القسم، يمكنك العثور على قيمة التغطية (من 3 إلى 50 ديسيبل لكل متر). هذه القيمة هي قيمة ملف تعريف التغطية القابلة للتكوين الخاصة بالمستخدم.
3. يمكن تحرير هذه القيمة للتأثير على قيمة حد SNR للعميل. الطريقة الأخرى للتأثير على عتبة SNR هذه هي زيادة طاقة الإرسال وتعويض اكتشاف فتحة التغطية.

س. أنا أستخدم ACS v 4.1 ووحدة تحكم شبكة محلية لاسلكية 4402 (WLC). عندما يحاول عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مصادقة عميل لاسلكي إلى ACS 4.1، يفشل ACS في الاستجابة مع ACS ويبلغ عن رسالة الخطأ هذه: *حدث خطأ داخلي* ". لدي جميع التكوينات الخاصة بي صحيحة. لماذا يحدث هذا الخطأ الداخلي؟

أ. هناك مصادقة متعلقة بمعرف تصحيح الأخطاء من CSCsh62641 Cisco (يسجل زبون فقط) في ال ACS 4.1، حيث يعطي ال acs الخطأ الداخلي أن وقع رسالة خطأ.

قد يكون هذا الخطأ هو المشكلة. هناك تصحيح يتوفر لهذا الخطأ على صفحة ACS 4.1 Downloads (العملاء المسجلون فقط) التي يجب أن تقوم بإصلاح المشكلة.

q. ال cisco 4400 sery لاسلكي lan جهاز تحكم (WLC) لن يمهد. تم إستلام رسالة الخطأ هذه على وحدة التحكم: ** IDE 0:4 ** (IRQ) dev 0 blk 0: status 0x51 ** reg: 10 0. لماذا؟

أ. قد يكون سبب هذا الخطأ مشكلة في الأجهزة. افتح حالة مركز المساعدة الفنية لاستكشاف هذه المشكلة وإصلاحها بشكل إضافي. in order to فتحت حالة TAC، أنت تحتاج أن يتلقى عقد صالح مع cisco. أحلت دعم فني in order to اتصل ال cisco TAC.

س. تمر وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) في مشاكل المخزن المؤقت للذاكرة. بمجرد امتلاء المخازن المؤقتة للذاكرة، تتعطل وحدة التحكم وتحتاج إلى إعادة تمهيد لإعادتها إلى الإنترنت. تظهر رسائل الخطأ التالية في سجل الرسائل: Mon APR 9 10:41:03 2007 [ERROR] dtl_net.c :506 MON APR 9 10:41:03 2007 . MBUF :Mon APR 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537 . MBUFS :[ERROR] sysapi_if_net.c 219: MbufGet لماذا؟

a. يرجع هذا إلى معرف تصحيح الأخطاء من CSCsh93980 Cisco (العملاء المسجلون فقط). تم حل هذا الخطأ في WLC، الإصدار 4.1.185.0. قم بترقية وحدة التحكم إلى إصدار البرنامج هذا أو إصدار أحدث للتغلب على هذه الرسالة.

TPA Q/168.1.233. أجرينا ترقية وحدة التحكم في الشبكة المحلية اللاسلكية (4400s WLC) إلى 4.1 رمز، وقصفت رسائل Syslog الخاصة بنا بالقنابل، مثل هذا: May 03:03:55:49.591 dtl_net.c:1191 (DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93 0.0.0.0] ARP (1 SPA9.2 192.168.1.233. إلى ماذا تشير هذه الرسائل؟

أ. يمكن أن يحدث ذلك عندما يتم تمييز WLAN على أنها DHCP مطلوبة . في مثل هذه الحالات، يسمح فقط لمحطات أن يستلم عنوان من خلال DHCP أن يقترن. غير مسموح بالعملاء الثابتين بالاقتران بشبكة WLAN هذه. يعمل WLC كعميل ترحيل DHCP ويسجل عنوان IP لجميع المحطات. يتم إنشاء رسالة الخطأ هذه عندما يستقبل WLC طلب ARP من محطة قبل أن يستلم WLC حزم DHCP من المحطة ويسجل عنوان IP الخاص بها.

q. عند إستخدام تقنية التزويد بالطاقة عبر شبكة إيثرنت (PoE) على وحدة التحكم في الشبكة المحلية اللاسلكية Cisco 2106، لا يتم تمكين أجهزة الراديو AP. يتعذر على . . تظهر رسالة خطأ. كيف يمكنني إصلاح هذا؟

أ. تحدث رسالة الخطأ هذه عندما يكون المحول، الذي يشغل نقطة الوصول، محولا قياسيا ولكن نقطة الوصول لا تدعم الوضع القياسي المسبق لطاقة الإدخال.

محول قياسي مسبقا من Cisco هو محول لا يدعم الإدارة الذكية للطاقة (IPM) ولكنه يحتوي على طاقة كافية لنقطة وصول قياسية.

أنت ينبغي مكنت **ال pre-standard** أسلوب الطاقة على ال ap أن يكون عرضة إلى هذا خطأ رسالة. يمكن القيام بذلك من واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم باستخدام **الأمر | enable} config ap power standard {all | cisco_ap {disable}**.

يجب تكوين هذا الأمر بالفعل، إذا كان مطلوبا، إذا قمت بالترقية إلى الإصدار 4.1 من البرنامج من إصدار سابق. ولكن، من المحتمل أن تحتاج إلى إدخال هذا الأمر للتثبيتات الجديدة، أو إذا قمت بإعادة ضبط نقطة الوصول على إعدادات المصنع الافتراضية.

تتوفر محولات 15 وات القياسية هذه من Cisco:

- AIR-WLC2106-K9
- WS-C3550 و WS-C3560 و WS-C3750

- الطراز C1880
- 2600 و 2610 و 2611 و 2621 و 2650 و 2651
- الطراز 2610xm، الطراز 2611xm، الطراز 2621xm، الطراز 2650xm، الطراز 2651xm، الطراز 2691
- 2811، 2821 م 2851 م
- 3631-Telco، 3620، 3640، 3660
- 3725، 3745 ه
- 3825، 3845 ه

q. تقوم وحدة التحكم بإنشاء `:dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED ARP xx:xx.-xxx.x .` رسالة syslog مماثلة لهذا. ماذا تعني رسالة syslog هذه؟

أ. بينما يرسل بعض العملاء اللاسلكيين ردا على ARP، تحتاج وحدة معالج الشبكة (NPU) إلى معرفة هذا الرد . لذلك تتم إعادة توجيه رد ARP إلى NPU ولكن يجب ألا يحاول برنامج WLC إضافة هذا الإدخال إلى معالج الشبكة. وإذا قام بذلك، يتم إنشاء هذه الرسائل. لا يوجد تأثير وظيفي على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بسبب هذا الأمر ولكن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يقوم بإنشاء رسالة syslog هذه.

Q. لقد قمت بتثبيت محول Cisco 2106 WLC جديد وتكوينه. تشير وحدة التحكم في الشبكة المحلية اللاسلكية إلى فشل مستشعر درجة الحرارة. عندما تقوم بتسجيل الدخول إلى واجهة الويب تحت ملخص وحدة التحكم"، فإنها تقول " بجوار درجة الحرارة الداخلية. كل شيء آخر يبدو أنه يعمل بشكل طبيعي.

ألف - إن فشل مستشعر درجة الحرارة الداخلي هو فشل تجميلي ويمكن حله بترقية WLC إلى الإصدار 4-2-61.0.

يمكن أن يستخدم كل من WLC 2106 و WLC 526 **المبنية على أو بعد 2007/01/07** شريحة مستشعر درجة الحرارة من مورد آخر. يعمل هذا المستشعر الجديد بشكل جيد، ولكنه لا يتوافق مع البرنامج بعد إصدار 4.2. وبالتالي البرامج الأقدم غير قادرة على قراءة درجة الحرارة وتظهر هذا الخطأ. ولا تتأثر جميع وظائف وحدات التحكم الأخرى بهذا الخلل.

هناك يعرف cisco بق CSCsk97299 id (يسجل زبون فقط) يربط إلى هذا إصدار. يذكر هذا الخطأ في ملاحظة الإصدار من WLC، الإصدار 4.2.

س. أحصل على `:RADIUS_db.c:1823 AAA-5-RADSERVER_NOT_FOUND RADIUS <WLAN ID> -` رسالة لجميع SSID. تظهر هذه الرسالة حتى بالنسبة إلى SSIDs التي لا تستخدم خوادم AAA.

أ. تعني رسالة الخطأ هذه أن وحدة التحكم لم تتمكن من الاتصال بخادم RADIUS الافتراضي أو أنه لم يتم تعريف واحد.

أحد الأسباب المحتملة لهذا السلوك هو معرف تصحيح الأخطاء من CSCsk08181 Cisco (العملاء المسجلون فقط)، والذي تم حله في الإصدار 4.2. قم بترقية وحدة التحكم إلى الإصدار 4.2.

q. `: 10 :sim.c:1061 sim-3-macaddr_get_fail 17:55:00.725 1 upper}mac address}` . تظهر رسالة خطأ على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC). إلى ماذا يدل ذلك؟

a. هذا يعني أن وحدة التحكم تعرضت لخطأ أثناء إرسالها حزمة مصدر وحدة المعالجة المركزية.

س. تظهر رسائل الخطأ التالية على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC):

- `'cliWebInitParms.cfg' :Jul 10 14:52:21.902 nvstore.c:304 System-3-FILE_READ_FAILED`
- `'rfidInitParms.cfg' :Jul 10 14:52:21.624 nvstore.c:304 System-3-FILE_READ_FAILED`
- `'dhcpParms.cfg' :Jul 10 14:52:21.610 nvstore.c:304 System-3-FILE_READ_FAILED`

- `'bcastInitParms.cfg' :Jul 10 14:52:21.287 nvstore.c:304 System-3-FILE_READ_FAILED`
- `:- .osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: sshpmInitParms.cfg 18:16:05:56.753 11ca7618: fp_main_task:`
- `:- .Mar 18:16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: bcastInitParms.cfg 11ca7618: fp_main_task:`

إلى ماذا تشير رسالة الخطأ هذه؟

أ. هذه الرسائل هي رسائل إعلامية وهي جزء من إجراء التمهيد العادي. تظهر هذه الرسائل بسبب فشل في قراءة أو حذف عدة ملفات تكوين مختلفة. عندما لا يتم العثور على ملفات تكوين معينة أو إذا تعذر قراءة ملف التكوين، يرسل تسلسل التكوين لكل عملية هذه الرسالة، على سبيل المثال، لا يوجد تكوين خادم DHCP، ولا علامات (معرف التردد اللاسلكي)، وما إلى ذلك. هذه رسائل منخفضة الخطورة يمكن تجاهلها بأمان. لا تؤدي هذه الرسائل إلى مقاطعة تشغيل وحدة التحكم.

q. ال `:HE6-WLC01local0alert2008-07-2512:48:18apf_rogue.c:740 APF-1-unable_to_KEEP_ROUGE_CONTAINS xx:02:xx:xx:xx:00:14 - ap` . تظهر رسالة خطأ. إلى ماذا يدل ذلك؟

أ. هذا يعني أن نقطة الوصول التي قامت بوظيفة الاحتواء المخادعة لم تعد متوفرة، ولا يمكن لوحدة التحكم العثور على أي نقطة وصول مناسبة لتنفيذ الاحتواء المخادع.

q. تظهر رسالة النظام `SPA (DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4 0.0.0] ARP (op 1 192.168.1.152/TPA 192.168.0.206` على وحدة التحكم في الشبكة المحلية اللاسلكية. ماذا تعني هذه الرسالة؟

أ. من الممكن أن يكشف النظام عن انتحال ARP أو تسميمه. ولكن، لا تعني هذه الرسالة بالضرورة حدوث أي انتحال ضار ل ARP. تظهر الرسالة عندما تكون هذه الشروط صحيحة:

- يتم تكوين شبكة WLAN باستخدام DHCP المطلوب، ويقوم جهاز عميل، بعد الاقتران على شبكة WLAN تلك، بإرسال رسالة ARP دون إكمال DHCP أولا. قد يكون هذا سلوكا عاديا؛ وقد يحدث ذلك، على سبيل المثال، عندما يتم توجيه العميل بشكل ثابت، أو عندما يحمل العميل إيجار DHCP صالح من اقتران سابق. قد تبدو رسالة الخطأ بهذا المثال:

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid
SPA 192.168.1.152/TPA 192.168.0.206
```

التأثير من هذا شرط أن الزبون يعجز أن يرسل أو يستلم أي حركة مرور بيانات، إلى أن هو DHCPs من خلال ال WLC.أحلت ال DTL رسالة قسم من cisco لاسلكي lan جهاز تحكم نظام رسالة مرشد ل كثير معلومة.

q. لا تستخدم نقاط الوصول في الوضع Lightweight (LAPs) تقنية التزويد بالطاقة عبر شبكة إيثرنت (POE) لتشغيل الجهاز. أرى السجلات الموجودة على وحدة التحكم في الشبكة المحلية اللاسلكية:

```
AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-
line power
```

ما هي المشكلة؟

أ. قد يحدث ذلك إذا لم يتم تكوين إعدادات التزويد بالطاقة عبر شبكة إيثرنت (POE) بشكل صحيح. عندما يتم تشغيل نقطة وصول تم تحويلها إلى وضع Lightweight، على سبيل المثال، من النوع AP1131 أو AP1242 أو نقطة وصول من السلسلة 1250 بواسطة حاقن طاقة متصل بمحول IPM (Cisco Pre-Intelligent Power Management)، فأنت بحاجة إلى تكوين تقنية التزويد بالطاقة عبر شبكة إيثرنت (PoE)، المعروفة أيضا باسم الطاقة المضمنة.

ارجع إلى تكوين الطاقة عبر الإيثرنت للحصول على مزيد من المعلومات حول كيفية تكوين التزويد بالطاقة عبر الإيثرنت (POE) .

Q. ترى هذه الرسالة على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC):

```
Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery*
request from AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6
```

إلى ماذا يدل ذلك؟

أ. تتبع نقاط الوصول في الوضع Lightweight خوارزمية معينة للعثور على وحدة تحكم. يتم شرح عملية الاكتشاف والانضمام بالتفصيل في تسجيل نقطة الوصول في الوضع Lightweight (LAP) إلى وحدة تحكم شبكة محلية لاسلكية (WLC)

تظهر رسالة الخطأ هذه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، عندما تستلم طلب اكتشاف بعد أن تصل إلى الحد الأقصى لسعة نقطة الوصول (AP) الخاصة بها.

إذا لم يتم تكوين وحدة التحكم الأساسية لنقطة الوصول في الوضع Lightweight أو إذا كانت هي وحدة تحكم جديدة خارج نقطة الوصول في الوضع Lightweight (LAP)، فإنها ترسل طلبات اكتشاف LWAPP إلى جميع وحدات التحكم القابلة للوصول. إذا وصلت طلبات الاكتشاف إلى وحدة تحكم تعمل بقدرة نقطة الوصول الكاملة الخاصة بها، فإن WLC تحصل على الطلبات وتدرك أنها في أقصى سعة لنقطة الوصول الخاصة بها، ولا تستجيب للطلب وتعطي هذا الخطأ.

س. أين يمكنني العثور على مزيد من المعلومات حول رسائل نظام LWAPP؟

أ. راجع دليل رسائل نظام وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 4.2 للحصول على مزيد من المعلومات حول رسائل نظام LWAPP.

س. تظهر رسالة خطأ على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC). إلى ماذا يدل ذلك؟

أ. يفشل WLC في تحميل حزمة مصادقة ويب مخصصة/مرور إذا كان لأي من الملفات المضمنة أكثر من 30 حرف في اسم الملف، والذي يتضمن امتداد الملف. تحتوي حزمة مصادقة الويب المخصصة على حد يصل إلى 30 حرف لأسماء الملفات. تأكد من أنه لا يوجد أسماء ملفات ضمن الحزمة أكبر من 30 حرف.

q. قد لا تعرض وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs)، التي تشغل الرمز 5.2 أو 6.0 بعدد كبير من مجموعات نقاط الوصول، واجهة المستخدم الرسومية (GUI) عبر الويب جميع مجموعات نقاط الوصول التي تم تكوينها. ما هي المشكلة؟

a. يمكن رؤية مجموعات نقاط الوصول المفقودة إذا كنت تستخدم الأمر **show wlan ap-groups** J CLI.

حاول إضافة مجموعة نقاط وصول إضافية واحدة إلى القائمة. على سبيل المثال، تم نشر 51 مجموعة نقطة وصول، بينما تم فقد المجموعة 51 (الصفحة 3). قم بإضافة المجموعة 52، وستظهر الصفحة 3 في واجهة المستخدم الرسومية (GUI) للويب.

لحل هذه المشكلة، قم بالترقية إلى WLC، الإصدار 7.0.220.0.

معلومات ذات صلة

- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 4.0 من Cisco
- الأسئلة المتداولة حول استكشاف أخطاء WiSM وإصلاحها
- أستكشاف أخطاء وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية وإصلاحها

- صفحة الدعم اللاسلكي
- 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).