WGB التجوال: التفاصيل الداخلية والتكوين

المحتويات

المقدمة

جسر مجموعة العمل من Cisco (WGB) أداة مفيدة جدا لتصميم شبكة لاسلكية ونشرها لأنه يسمح للأجهزة غير اللاسلكية باكتساب إمكانية التنقل. يوفر WGB العديد من التفاصيل حول التجوال والوصول إلى الأمان وما إلى ذلك، مما يؤثر على سيناريوهات النشر وفقا لاحتياجاتك.

في الإصدارات الشفرة 12.4(JA(25d والإصدارات الأحدث، قدمت Cisco مجموعة من الأوامر والتغييرات من أجل تحسين إستخدام WGB على بيئات التجوال عالية السرعة.

يغطي هذا المستند جوانب مختلفة لكيفية عمل WGB، بما في ذلك نقاط قرارات الخوارزمية المتجولة، وكيفية تكوينه لنموذج الاستخدام المقصود.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- حل Cisco Wireless LAN
- جسر مجموعة العمل من Cisco

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

ما هو جسر مجموعة العمل؟

إن WGB هي في الأساس نقطة وصول (AP) تم تكوينها للعمل كعميل لاسلكي نحو بنية أساسية، ولتوفير اتصال الطبقة 2 للأجهزة المتصلة بواجهة إيثرنت الخاصة بها.

تشتمل عملية نشر WGB النموذجية على هذه المكونات:

- جهاز WGB، عادة مع راديو واحد وواجهة إيثرنت واحدة على الأقل
- بنية تحتية لاسلكية، عادة ما تسمى نقطة الوصول الجذر، ويمكن أن تكون مستقلة أو موحدة.
- جهاز عميل سلكي واحد أو أكثر متصل ب WGB. لا يغطي هذا المستند سيناريوهات أدوار مختلطة (جهاز لاسلكي باسم WGB وجهاز لاسلكي كجذر على نفس نقطة الوصول).

هناك ثلاثة أنواع رئيسية من WGB:

- **Cisco WGB**: Cisco WGB هي أي نقطة وصول مستندة إلى برنامج Cisco IOS® - مكونة على هيئة WGB (1130 و 1240 و 1250، وما إلى ذلك). يستخدم هذا الوضع بروتوكول IAPP لإعلام البنية الأساسية للشبكة بالأجهزة التي تعلمها WGB على واجهة إيثرنت الخاصة به. في هذه الحالة، تتضمن وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) أو نقطة الوصول الجذر إمكانية رؤية الطبقة 2 للأجهزة "المعلقة" من WGB.
- **غير Cisco WGB:** هذا جهاز من إنتاج طرف ثالث يعمل كجهاز WGB، ويربط جهاز أو أكثر من الأجهزة السلكية بالبنية الأساسية اللاسلكية. وهذه البلدان لا تدعم IAPP، ولا تسمح إلا بجهاز سلكي واحد، أو توفر آلية لترجمة عنوان MAC، مما يخفي جميع عملائها السلكيين خلف عنوان MAC واحد 802.11. تحتاج هذه الأنواع من الأجهزة إلى معالجة خاصة على بروتوكول تحليل العنوان (ARP) وإطارات DHCP إذا كانت البنية الأساسية هي عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) نظرا لفحوصات الأمان ومعالجة الإطارات التي تم إجراؤها على وحدات التحكم.

- **cisco ap يشكل ك "WGB عالمي"**: هذا أسلوب أن يقمع آلية IAPP، لذلك ال WGB يستطيع كنت استعملت نحو إما بنية Cisco الأساسية أو طرف ثالث جذر APs. في هذه الحالة، يأخذ WGB عنوان عميل الإيثرنت الخاص به، مما يقلل عدد الأجهزة الموجودة وراءه إلى واحد.

يركز القسم التالي على سيناريو إستخدام Cisco WGB إما نحو بنية أساسية مستقلة أو WLC.

سيناريوهات الاستخدام

تتضمن أمثلة إستخدام WGB النموذجية ما يلي:

- توصيل طابعة سلكية بالشبكة
- عمليات نشر مختلفة للصناعة، حيث يكون من غير الممكن أو العملي تشغيل كابل إلى الجهاز السلكي
- عمليات النشر داخل المركبات، حيث توفر شبكة WGB إمكانية الاتصال من سيارة وقطار مترو، إلخ، إلى شبكة لاسلكية خارجية
- كاميرات سلكية

لكل مثال متطلباته الخاصة من حيث:

- الحزمة العريضة المطلوبة لدعم التطبيق الذي سيتم تشغيله فوق البنية الأساسية اللاسلكية
- تفاوت تأخر التجوال - كم يستغرق انتقال WGB من نقطة الوصول الحالية إلى التالية أثناء تحرك الجهاز؟
- تفاوت وقت إعادة التوجيه - كم عدد الإطارات المفقودة على كل تجوال؟

الطابعة لا تنقل الكثير، لذلك فإن متطلبات التجوال أقل. أما القطار المثبت على WGB من ناحية أخرى، فهو يحتاج إلى ضبط دقيق على المكون المتجول من أجل تأمين السلوك الصحيح أثناء تنقله.

يمكن أن يتطلب تدفق الفيديو نطاقا ترددیا عريضا كبيرا، لذلك يحتاج إلى معدلات عالية من البيانات اللاسلكية. ومع ذلك، قد يحتاج تطبيق تتبع الاستخدام إلى إطارات قليلة فقط من وقت إلى آخر.

من المهم أن يتم تعريف المتطلبات بشكل صحيح من البداية، حيث أنها لا تؤثر على تكوين WGB فقط، ولكن أيضا على كيفية تصميم البنية الأساسية اللاسلكية. على سبيل المثال، تؤثر نقاط الوصول والمسافة ومستويات الطاقة والأسعار الممكنة وما إلى ذلك على خصائص التجوال. لذلك، تكون كلها نقطة حاسمة إذا كان التجوال العالي السرعة ضروريا.

بشكل عام، يجب أن تعرف التفاصيل التالية:

- ما هو النطاق الترددي المطلوب للتطبيق؟
- ما هو السماح بتأخير التجوال؟
- هل يمكن للتطبيق معالجة حالات انقطاع الاتصال بالشبكة بشكل صحيح؟ هل هناك آلية إضافية للنسخ الاحتياطي؟
- هل يمكن للتطبيق معالجة فقدان الحزمة بشكل صحيح؟ (حتى في أفضل تصميم لاسلكي، يجب أن تتوقع نسبة مئوية من فقدان الحزم.)

لا يتناول هذا المستند تفاصيل حول كيفية تصميم بيئة تردد لاسلكي للتجوال/المناطق الخارجية عالية السرعة. ارجع إلى دليل نشر الشبكة العنكبوتية الخارجية.

تجوال

بالنسبة للجهاز اللاسلكي، يعد التجوال جزءا هاما جدا من وظائفه.

يعني التجوال أساسا إمكانية الانتقال من نقطة وصول إلى أخرى، وكلاهما ينتمي إلى نفس البنية الأساسية اللاسلكية.

بما أن التجوال يحتاج إلى تغيير من نقطة الوصول الحالية إلى التي تليها، هناك انقطاع ناتج أو وقت بدون خدمة. هذا

الانفصال يمكن أن يكون صغيرا. على سبيل المثال، أقل من 200 مللي ثانية في عمليات نشر الصوت أو أكثر من ذلك بكثير، بل بالثواني، إذا كان الأمان المطلوب يفرض المصادقة الكاملة على كل حدث في التجوال.

التجوال مطلوب حتى يتمكن الجهاز من العثور على والد جديد بإشارة أفضل كما نأمل، ويستطيع الاستمرار في الوصول إلى البنية التحتية للشبكة بشكل صحيح. وفي الوقت نفسه، يمكن أن يتسبب عدد كبير جدا من الرومات في انقطاعات متعددة أو في وقت بدون خدمة، مما يؤثر على الوصول. من المهم لجهاز محمول مثل WGB أن يحتوي على خوارزمية تجوال جيدة مزودة بإمكانات تهيئة كافية للتكيف مع بيئات التردد اللاسلكي المختلفة واحتياجات البيانات.

عناصر التجوال

- **المشغلات:** يحتوي كل تطبيق عميل على مشغلات أو أحداث أو أكثر، تتسبب في نقل الجهاز إلى نقطة وصول أصل أخرى عند تلبيته. الأمثلة: فقد المنارة (لم يعد الجهاز يسمع المنارات العادية من نقطة الوصول)، وعمليات إعادة محاولة الحزم، ومستوى الإشارة، وعدم تلقي بيانات، وإطار إلغاء المصادقة الذي تم تلقيه، ومعدل البيانات المنخفض قيد الاستخدام، وما إلى ذلك. يمكن أن تختلف المشغلات المحتملة من تطبيق العميل إلى آخر لأنها ليست موحدة بالكامل. قد يكون للأجهزة الأبسط مجموعة مشغلات ضعيفة، مما يؤدي إلى وجود عملاء غير ملثقين أو جولات غير ضرورية. يدعم WGB كل العناصر السابقة الموصوفة من قبل.
- **وقت المسح:** يقضي الجهاز اللاسلكي (WGB) بعض الوقت في البحث عن الآباء المحتملين. عادة ما يعني ذلك الذهاب على قنوات مختلفة، إجراء تدقيق نشط أو الإنصات سلبيا لنقاط الوصول. بما أن الراديو يجب أن يقوم بالمسح الضوئي، فإن هذا يعني أن الوقت الذي تقضيه WGB في عمل شيء آخر مختلف عن إعادة توجيه البيانات. من وقت الفحص هذا، يمكن ل WGB إنشاء مجموعة صحيحة من الوالدين يمكن الانتقال إليها.
- **تحديد الأصل:** بعد وقت المسح، يمكن أن يقوم WGB بفحص الوالدين المحتملين وتحديد الأفضل وإطلاق عملية الاقتران/المصادقة. في بعض الأحيان، قد تكون نقطة القرار هي البقاء في الأصل الحالي إذا لم يكن هناك فائدة كبيرة من حدث التجوال (تذكر أن التجوال كثيرا قد يكون سيئا).
- **الاقتران/المصادقة:** ينتقل WGB إلى الاقتران بنقطة الوصول الجديدة، والتي تغطي عادة كلا من مرحلتي المصادقة والاقتران 802. 11، بالإضافة إلى إكمال سياسة الأمان التي تم تكوينها على SSID (WPA 2-PSK، None، CCKM، وما إلى ذلك).
- **إستعادة إعادة توجيه حركة المرور:** يقوم WGB بتحديث البنية الأساسية للشبكة لعملائه السلكيين المعروفين من خلال تحديثات IAPP بعد التجوال. بعد هذه النقطة، يتم إستئناف حركة المرور إلى/من العملاء السلكيين إلى الشبكة.

دليل التكوين - سياسات الأمان

أحد الجوانب المهمة للتجوال على الأجهزة المحمولة هو ما هي سياسة الأمان التي سيتم تنفيذها على البنية الأساسية. هناك العديد من الخيارات، كل منها لديه نقاط جيدة/سيئة. هذه هي أهم الأشياء:

- **مفتوح** — من حيث الاساس لا أمن. هذا هو أسرع، وأبسط من كل السياسات. وهذه مشكلة رئيسية تتمثل في عدم تقييد الوصول غير المصرح به إلى البنية التحتية وعدم توفير الحماية ضد الهجمات، مما يحد من إستخدامها على سيناريوهات محددة للغاية. وعلى سبيل المثال، الألغام التي لا يمكن أن تقع فيها هجمات خارجية بسبب الطبيعة المحضة للانتشار.
- **مصادقة عنوان MAC**—وهو أساسا نفس مستوى الأمان كما هو مفتوح، حيث أن انتحال عنوان MAC يعد هجوما بسيطا. غير مستحسن بسبب الوقت الإضافي لإكمال التحقق من صحة MAC، مما يبطئ التجوال.
- **WPA2-PSK**—يقدم مستوى جيد من التشفير (AES-CCMP)، لكن تأمين المصادقة يعتمد على جودة المفتاح المشترك مسبقا. لتدابير الأمان، يوصى بكلمة مرور من 12 حرفا وعشوائية كحد أدنى. مماثل إلى طريقة المفتاح مشترك مسبقا، بما أن المفتاح يكون استعملت على أجهزة متعددة، إن المفتاح يكون كشفت الكلمة يحتاج أن يكون عدلت عبر كل تجهيز. تكون سرعة التجوال مقبولة كما هو الحال في 6 عمليات تبادل الإطارات، ويمكنك حساب الحدود الزمنية العليا/الدنيا لإتمامها لأنها لا تتضمن أي معدات خارجية (بدون خادم RADIUS، وما إلى ذلك). وبوجه عام، فإن هذه الطريقة هي الطريقة المفضلة بعد الموازنة بين المشاكل والفوائد.
- **WPA2 مع 802.1x**—يحسن ذلك من الأسلوب السابق باستخدام بيانات اعتماد لكل جهاز/مستخدم، والتي يمكن

تغييرها بشكل فردي. المشكلة الرئيسية هي أن هذه الطريقة لا تعمل بشكل صحيح أثناء تحرك الجهاز بسرعة، أو عندما تكون هناك حاجة إلى أوقات تجوال قصيرة. وبشكل عام، يستخدم هذا الإطار نفس الإطارات الستة بالإضافة إلى تبادل EAP الذي يمكن أن يتراوح بين أربعة إطارات وما فوق. يعتمد ذلك على نوع EAP المحدد وأحجام الشهادة. وبشكل طبيعي، يستغرق ذلك ما بين 10 إلى 20 إطار، بالإضافة إلى التأخير الإضافي لمعالجة خادم RADIUS.

- **WPA2+CCKM**— توفر هذه الآلية حماية جيدة، وتستخدم 802. 1x لبناء المصادقة الأولية، ثم تقوم بتبادل سريع لإطارين فقط على كل حدث التجوال. يوفر ذلك وقتا للتجوال سريعا جدا. المشكلة الرئيسية هي أنه في حالة فشل التجوال، فإنه يعود إلى 802.1x. ثم تبدأ باستخدام CCKM مرة أخرى بعد أن تصادق. إذا كان التطبيق الموجود أعلى WGB يمكنه تحمل وقت تجوال طويل بشكل عرضي في حالة حدوث مشاكل، يمكن إستخدامه كأفضل خيار مقابل PSK.

لا يغطي هذا المستند التقنيات غير الموصى بها التي لها مشاكل أمان مثل LEAP و WPA-TKIP و WEP، إلخ.

تكوين WPA2-PSK

على WGB، هذا بسيط إلى حد ما للتكوين. تحتاج إلى تعريف SSID وتشفير مناسب على الراديو.

```
dot11 ssid wgbpsk
vlan 32
authentication open
authentication key-management wpa version 2
!wpa-psk ascii YourReallySecurePSK
no ids mfp client

interface Dot11Radio0
ssid wgbpsk
encryption mode ciphers aes-ccm
station-role workgroup-bridge
```

يجب أن يتطابق اسم SSID الخاص بك والمفتاح المشترك مسبقا مع البنية الأساسية للشبكة.

تكوين WPA2 باستخدام 802.1x

يعتمد أساسا على التهيئة السابقة مع إضافة توصيفات EAP وطريقة المصادقة:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management wpa version 2
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
eap profile eapfast
 This covers the EAP method type used on your network. method fast ! ! dot1x credentials wgb ---!
 !--- This is your WGB username/password. username cisco password 7 1511021F0725 interface
Dot11Radio0 encryption mode ciphers aes-ccm ssid wlan1
```

تكوين WPA2 باستخدام CCKM

فقط خطوة واحدة فوق WPA2 مع تغيير بسيط واحد فقط: إستخدام علامة CCKM على تكوين SSID. هذا يفترض أن ال WLAN يكون شكلت ل CCKM فقط على ال WLC جانب:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management cckm
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
```

التحقق من صحة الأسلوب المستخدم

يمكن للتدقيق السريع على WGB الإبلاغ عن التشفير وإدارة المفاتيح المستخدمة، على سبيل المثال، في CCKM:

```
wgb-1260#sh dot11 associations al
Address           : 0024.97f2.75a0     Name             : lap1140-etsi-1
IP Address        : 192.168.40.10      Interface        : Dot11Radio 0
Device            : LWAPP-Parent       Software Version : NONE
CCX Version       : 5                  Client MFP       : Off

- :           State             : EAP-Assoc          Parent
SSID              : wlan1
VLAN              : 0
Hops to Infra     : 0                  Association Id   : 1
Tunnel Address    : 0.0.0.0
Key Mgmt type     : CCKM               Encryption       : AES-CCMP

Current Rate      : m7.-               Capability       : WMM ShortHdr ShortSlot
.Supported Rates  : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7
Voice Rates       : disabled           Bandwidth        : 20 MHz
Signal Strength   : -59  dBm          Connected for    : 72 seconds
Signal to Noise   : 41  dB            Activity Timeout : 8 seconds
Power-save        : Off                Last Activity    : 7 seconds ago
Apsd DE AC(s)    : NONE

Packets Input     : 12064              Packets Output   : 136
Bytes Input       : 2892798            Bytes Output     : 19514
Duplicates Rcvd   : 87                 Data Retries     : 8
Decrypt Failed    : 0                  RTS Retries      : 0
MIC Failed        : 0                  MIC Missing      : 0
Packets Redirected: 0                  Redirect Filtered: 0
```

تهيئة التجوال

على WGB، يمكنك تعديل العديد من المعلمات التي تؤثر على خوارزمية التجوال.

عمليات إعادة محاولة الحزمة

بشكل افتراضي، تعيد شبكة WGB إرسال إطار 64 مرة. إذا لم يتم الاعتراف به (ACK) بشكل صحيح من قبل أحد الوالدين، فإنه يفترض أن الأصل لم يعد صالحا، ويبدأ عملية المسح الضوئي/التجوال. انظر لهذا على أنه مشغل تجوال "غير متزامن" لأنه يمكن القيام به في أي لحظة يفشل فيها الإرسال.

الأمر أن يشكل هذا، يذهب داخل ال dot11 قارن، وهو يأخذ الخيارات التالية:

```
[packet retries NUM [drop
```

num: بين 1 و 128، مع إعداد افتراضي يبلغ 64. عادة ما يكون الرقم الجيد لمصدر التجوال السريع 32. لا ينصح باستخدام رقم أقل في معظم بيئات التردد اللاسلكي.

drop: إذا لم يكن موجودا، يبدأ WGB حدث تجوال عند الوصول إلى الحد الأقصى للمحاولات. في الوقت الحالي، لا يبدأ WGB التجوال الجديد ويستخدم المشغلات الأخرى، مثل فقدان إشارات المنارة.

مراقبة RSSI

يمكن أن يقوم WGB بتنفيذ فحص استباقي للإشارات للأصل الحالي وبدء عملية تجوال جديدة عندما تنخفض الإشارة إلى ما دون المستوى المتوقع.

تتطلب هذه العملية معلمتين:

- مؤقت، يقوم باستيقاظ عملية التحقق كل X ثانية
- مستوى RSSI، والذي يستخدم لبدء عملية تجوال إذا كانت الإشارة الحالية منخفضة.

على سبيل المثال:

```
in d0
mobile station period 4 threshold 75
```

لا يجب أن يكون الوقت أقل مما تستغرقه WGB لإكمال عملية المصادقة من أجل منع "تكرار تكرار تكرار التجوال" في بعض الحالات أو لتجنب سلوك تجوال عدواني للغاية. وعموما، ينبغي إختباره لمعرفة ما يستوفي إحتياجات الطلب.

بالنسبة لمستخدم التوصيل الملاحي (PSK)، يمكن أن يكون أقل من الطرق المستندة إلى EAP (نموذجي 2 و 4 للتطبيقات المتراصة جدا).

يتم التعبير عن مستوى RSSI كعدد صحيح موجب، على الرغم من أنه من حيث الأساس مستوى عادي - dBm مقدرا. يجب إستخدام رقم أعلى قليلا من الحد الأدنى المطلوب للحفاظ على معدل البيانات يعمل بشكل صحيح. على سبيل المثال، إذا كان الحد الأدنى لمعدل السرعة الذي تريده هو 6 ميجابت في الثانية، فيجب أن يكون الحد المسموح به ل RSSI وهو -87 كافيا. عند سرعة 48 ميجابت في الثانية، تحتاج إلى -70 ديسيبل لكل ميللي وات، إلخ.

ملاحظة: يمكن أن يؤدي هذا الأمر أيضا إلى تشغيل "التجوال حسب تغيير معدل البيانات"، والذي يكون كثيفا جدا. يجب إستخدامه مع الحد الأدنى من المعدل للحصول على نتائج جيدة.

الحد الأدنى لمعدل البيانات

ابتداء من 12.4(25d)JA، أضافت Cisco معلمة قابلة للتكوين للتحكم في الوقت الذي يجب أن تقوم فيه WGB بتشغيل حدث تجوال جديد، إذا كان معدل البيانات الحالي للأصل منخفض قيمة معينة.

وهذا مفيد لضمان الحفاظ على الحد الأدنى المطلوب للسرعة من أجل دعم تطبيقات الفيديو أو الصوت.

قبل توفر هذا الأمر، قام WGB بتشغيل التجوال بشكل متكرر عندما وجد أن المعدل أقل من المرة السابقة. في الوقت X+1 بشكل أساسي، إذا كان المعدل أقل من وقت X السابق، فإن WGB يبدأ عملية تجوال. سترى هذه الرسائل على السجلات:

```
Mar  1 00:36:43.490: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio1, parent lost: Had to lower*
data rate
```

هذا متداخل جدا، وفي العادة، كان الحل الوحيد هو تكوين معدل بيانات واحد في كل من WGB و APs الأصل.

الآن، الطريقة الموصى بها هي تكوين هذا الأمر دائما، كلما تم إستخدام أمر فترة محطة متنقلة:

```
in d0
mobile station  minimum-rate 2.0
```

بهذا، يتم تشغيل عملية التجوال الجديدة فقط إذا كان المعدل الحالي أقل من القيمة التي تم تكوينها. يقلل ذلك من عمليات التنقل غير الضرورية ويسمح بالحفاظ على قيمة السعر المتوقعة.

ملاحظة: يتوقع حدوث **الرسالة** " " حتى مع هذا التكوين، ولكن الآن يجب ملاحظة ما إذا كان WGB هو TX بسرعة أقل من السرعة التي تم تكوينها، عندما تم تشغيل وقت التحقق من فترة محطة التنقل.

مسح القنوات

يقوم WGB بمسح كل "قنوات البلد" أثناء القيام بحدث تجوال. هذا يعني أنه اعتمادا على مجال الراديو، يمكنك مسح القنوات من 1 إلى 11 على مدى موجات 2. 4 جيجاهيرتز أو من 1 إلى 13.

كل قناة ممسوحة ضوئيا تستغرق بعض الوقت. في 802. 11bg هذه حوالي 10 إلى 13 ميللي ثانية. على 802.11a، يمكن أن يصل إلى 150 ملي ثانية إذا كانت القناة ممكنة DFS (وبالتالي لا سبر، فقط قم بالمسح الضوئي السلبي هناك).

التحسين الجيد هو تقييد القنوات الممسوحة ضوئيا لاستخدام القنوات الموجودة في الخدمة فقط بواسطة البنية الأساسية. وهذا مهم بشكل خاص في 802.11a، لأن قائمة القنوات كبيرة، ويمكن أن يكون الوقت لكل قناة طويلا إذا كان DFS قيد الاستخدام.

هناك ثلاث نقاط يجب أخذها عند تصميم خطة قناة ل WGB/التجوال:

- بالنسبة لنطاق ترددي يبلغ 2.4 جيجاهرتز، حاول الالتزام ب 11/6/1 لتقليل تداخل القناة الجانبية إلى الحد الأدنى. أي خطة لقناة أخرى تحتوي على 4، غير ذلك، تميل لأن يكون من الصعب هندستها بشكل صحيح من وجهة نظر التردد اللاسلكي، دون زيادة التداخل.
- إن إستخدام إعداد قناة واحدة لجميع نقاط الوصول هي فكرة جيدة من وجهة نظر المسح الضوئي. ويكون هذا منطقيا فقط إذا كان العدد الإجمالي للعملاء المطلوب دعمهم منخفضا للغاية، ولم تكن هناك متطلبات نطاق ترددي عال. يؤدي ذلك إلى إستبعاد وقت تغيير الراديو من وقت المسح. كن على دراية بأن عددا قليلا من البيئات يمكن أن يستفيد من هذا الخيار، لذا استعن بعناية.
- بالنسبة لنطاق ترددي يبلغ 5.0 جيجاهرتز، إذا كان ذلك ممكنا بموجب الأنظمة المحلية، فإن إستخدام قنوات غير DFS داخلية (من 36 إلى 48) يتيح وقتا أسرع للمسح، حيث يمكن ل WGB الاستكشاف بشكل فعال لكل واحد، بدلا من عمل الإصغاء السلبي لوقت أطول.

قد تحتاج خطة القناة المستخدمة لنشرك إلى إستيعاب المتطلبات الأخرى. أستخدم توصيات تصميم التردد اللاسلكي العامة.

لتكوين قائمة قناة المسح الضوئي:

```
in d0
mobile station scan 1 6 11
```

ملاحظة: تظهر محطات المحمول فقط عند إستخدام دور WGB على الراديو.

ملاحظة: تأكد من تطابق قائمة المسح الضوئي ل WGB مع قائمة قنوات البنية الأساسية. إذا لم تكن هناك مساحة، فلن يجد WGB نقاط الوصول المتوفرة.

تكوين المؤقتات

بدءا من 12.4(JA(25a، هناك العديد من الأوامر الجديدة لتحسين مؤقت الاسترداد عند العثور على مشكلة، والتي تتوفر فقط عندما تكون نقطة الوصول في وضع WGB.

```
? wgb-1260(config)#workgroup-bridge timeouts
```

```
  assoc-response  Association Response time-out value
 auth-response   Authentication Response time-out value
    client-add      client-add time-out value
      eap-timeout     EAP Timeout value
  iapp-refresh    IAPP Refresh time-out value
```

في حالة client-add، auth-response، ASSOC-response، هذه تشير إلى الوقت الذي سينتظر فيه WGB نقطة الوصول الأصل للرد، قبل إعتبار نقطة الوصول خالية من المرشح التالي ومحاولة تعيينه. القيم الافتراضية هي 5 ثوان، وهو طويل جدا بالنسبة لبعض التطبيقات. الحد الأدنى للموقت هو 800 مللي ثانية ويوصى به لمعظم تطبيقات الأجهزة المحمولة.

أثناء مهلة EAP، تقوم WGB بتعيين الحد الأقصى للوقت للانتظار، حتى تكتمل عملية مصادقة EAP بالكامل. يعمل هذا من وجهة نظر ملتمس EAP لإعادة تشغيل العملية إذا كان مصدق EAP لا يستجيب. القيمة الافتراضية هي 60 ثانية. احذر من عدم تكوين قيمة يمكن أن تكون أقل من الوقت الفعلي المطلوب لإكمال مصادقة 802.1x كاملة. عادة، يكون تعيين هذا إلى 2 إلى 4 ثوان صحيحا لمعظم عمليات النشر.

بالنسبة ل iapp-refresh، يقوم WGB بشكل افتراضي بإنشاء تحديث مجمع IAPP إلى نقطة الوصول الأصلية بعد التجوال لإعلام العملاء السلكيين المعروفين. توجد عملية إعادة إرسال ثانية بعد الاقتران بعد حوالي 10 ثوان. يسمح هذا المؤقت بإجراء "إعادة محاولة سريعة" لكتلة IAPP بعد الاقتران من أجل التغلب على احتمال فقدان التحديث الأول ل IAPP بسبب RF أو مفاتيح التشفير التي لم يتم تثبيتها بعد على نقطة الوصول الأصل. بالنسبة لسيناريوهات التجوال السريع، يمكن إستخدام 100 مللي ثانية. ومع ذلك، تأكد من وجود عدد كبير من WGB قيد الاستخدام. وهذا يزيد بشكل ملحوظ العدد الإجمالي ل IAPP الذي تم إرساله إلى البنية الأساسية بعد كل تجوال.

مثال للقيم التراكمية:

```
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

تم إختبار هذه بنجاح على سيناريوهات نشر WGB أثناء التنقل.

عمليات تحسين WGB الأخرى

هناك تغييرات طفيفة أخرى يجب أخذها في الاعتبار لسيناريوهات نشر WGB:

ذي صلة بالراديو

- تقليل **عمليات إعادة محاولة RTS** - **عمليات إعادة محاولة RTS 32**. يمكن أن يوفر ذلك بعض الوقت من تردد الراديو (RF) في السيناريوهات الملتهبة. وعادة لا يكون ذلك ضروريا.
- نوع الهوائي: في حالة إستخدام هوائي واحد (دون أي تنوع) يجب تهيئة الراديو لتحسين الأداء العام:

```
antenna transmit right-a
antenna receive right-a
```

إن تنوع الهوائي مرغوب، لكنه غير ممكن دائما عندما يتم تركيب الهوائيات فيزيائيا على المركبة. يعتبر تحديد الهوائي بشكل سليم أمرا حيويا للتجوال. يمكن أن يكون 2 ديسيبل فقط فرقا كبيرا في معدل مرات التجوال العام.

السجل ذو الصلة

- لتوفير بعض المللي ثانية، قم بتقليل مستوى تسجيل وحدة التحكم إلى الأخطاء فقط: **أخطاء وحدة التحكم**

للتسجيل. لا تعطله تماما لأنه قد يؤثر سلبا على أداء التجوال في بعض الحالات.
- وبشكل مثالي، أستخدم برنامج Telnet أو SSH من جانب الإيثرنت لجمع تصحيح الأخطاء أو السجلات. ولهذا تأثير أقل على الأداء مقارنة بتصحيح أخطاء التسجيل عبر وحدة التحكم: **تصحيح أخطاء مراقبة التسجيل**.
- الأمر لفهم ما يحدث لنقطة عرض WGB المتجولة هو **وصلة طباعة تتبع نقطة dot11 0 11**. وهذا يؤثر بشكل منخفض على وحدة المعالجة المركزية، ولكنه لا يمكن خيارات تصحيح الأخطاء الأخرى ما لم يتم توجيهها لأن كل خيار قد يزيد من إجمالي وقت التجوال.
- حاول إستخدام SNTP عند الإمكان. يؤدي ذلك إلى إستمرار مزامنة وقت WGB، مما يساعد في أستكشاف الأخطاء وإصلاحها.

إستخدام MFP

- يمكن أن يكون MFP مفيدا من وجهة نظر أمنية. ومع ذلك، فإن المأخذ هو أنه في سيناريوهات فشل التجوال، لا يقبل WGB إطارات إلغاء المصادقة من أصل نقطة الوصول لتشغيل تجوال جديد إذا كان مفتاح التشفير بينهما قد حدث خطأ لأي سبب من الأسباب.
- في سيناريوهات الفشل النادرة هذه، يمكن أن يستغرق WGB حتى 5 ثوان لتشغيل فحص جديد، إذا كان يمكن سماع الأصل الحالي باستخدام إشارة تردد لاسلكي جيدة. هناك آلية كشف "شاملة" يمكن أن يتم تشغيلها بواسطة WGB في حالة عدم تلقي إطارات بيانات صالحة خلال ذلك الوقت.
- بشكل افتراضي، تحاول WGB إستخدام MFP العميل إذا كان SSID به WPA2 AES قيد الاستخدام.
- يوصى بتعطيل MFP العميل إذا كانت هناك حاجة إلى أوقات إسترداد سريعة (WGB للاستجابة لإطارات الطلب غير المحمية). إنها تسوية بين إحتياجات الأمان وأوقات الاسترداد السريعة. ويعتمد القرار على ما هو أكثر أهمية لسيناريو الانتشار.

```
dot11 ssid wgbpsk
no ids mfp client
```

EAP-TLS على WGB و"الفاصل الزمني لحفظ الساعة"

ارجع إلى قسم مزامنة ساعات طالب IOS وتوفير الوقت إلى ذاكرة NVRAM في ملاحظات الإصدار لنقاط الوصول والجسور Cisco Aironet ل Cisco IOS الإصدار 12.4(21a)JY.

تذكر أنه إذا كنت تستخدم uWGB، فإن uWGB قد لا تحصل أبدا على فرصة لإجراء مزامنة SNTP لأنها ترتبط عادة بعنوان MAC المرفق ولا يكون BVI uWGB لديه وصول إلى الشبكة. لذلك، في حالة uWGB، يوصى بالحصول على مزامنة ساعة جيدة في ذاكرة NVRAM عند النشر كحد أدنى. إذا كان لجهاز التشغيل المرفق القدرة على أن يكون مصدر بروتوكول وقت الشبكة (NTP) (بالإضافة إلى عميل محدث عبر اتصال uWGB)، فمن الممكن عندئذ النظر في الحصول على مزامنة SNTP ل uWGB منه كنقطة انعكاس NTP فعالة.

مثال التكوين الكامل

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wgb-1260
!
logging rate-limit console 9
logging console errors
!
clock timezone CET 1
no ip domain lookup
!
```

```
!
dot11 syslog
!
!
dot11 ssid wgbpsk
vlan 32
authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 060506324F41584B56
no ids mfp client
!
!
!
!
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid wgbpsk
!
antenna transmit right-a
antenna receive right-a
packet retries 32
station-role workgroup-bridge
rts retries 32
mobile station scan 2412 2437 2462
mobile station minimum-rate 6.0
mobile station period 3 threshold 70
bridge-group 1
!

interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
!
interface BVI1
ip address 192.168.32.67 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.32.1
no ip http server
no ip http secure-server

bridge 1 route ip

sntp server 192.168.32.1
clock save interval 1
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
```

```
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

تحليل تصحيح الأخطاء

في أي مشاكل تحدث، من المهم التقاط مخرجات أمر وصلات **الطباعة** ذات **التتبع** 0 dot11 dot11 كخطوة أولى. يوفر ذلك رؤية جيدة لما يحدث في عملية التجوال.

هذا مثال للأصل الحالي كمرشح:

```
Sep 27 11:42:38.797: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Signal strength
                                                                                    too low
Sep 27 11:42:38.797: CDD051F1-0 Uplink: Lost AP, Signal strength too low
```

هذا هو المشغل لالتقاء الإشارة المنخفضة. يعتمد على أمر نقطة المحطة المتنقلة X Threshold Y. يتم إرسال الرسالة الأولى دائما إلى وحدة التحكم، الثانية هي جزء من تتبع أخطاء الوصلة. وهي ليست مشكلة، بل إنها جزء من عملية WGB العادية.

```
Sep 27 11:42:38.798: CDD052C7-0 Uplink: Wait for driver to stop
```

تفرض عملية الوصلة إزالة قائمة انتظار الراديو قبل بدء مسح القناة. يمكن أن تستغرق هذه الخطوة من بضع ثوان إلى عدة ثوان وفقا لاستخدام القناة وعمق قائمة الانتظار. لم يتم انقضاء مهلة إطارات البيانات. فلدى الاطارات الصوتية مقارنة زمنية، لذلك يجب ان تسقط بسرعة. ويمكن ملاحظة بعض التأخير في بيئات صاخبة.

```
Sep 27 11:42:38.798: CDD05371-0 Uplink: Enabling active scan
Sep 27 11:42:38.799: CDD05386-0 Uplink: Scanning
```

هذا هو الفحص الفعلي للقناة الذي يجري. إنه يضع جهاز الراديو لحوالي 10 إلى 13 ميللي ثانية لكل قناة مهيأة.

```
Sep 27 11:42:38.802: CDD064CD-0 Uplink: Rcvd response from 0021.d835.ade0 channel 1 3695
```

هذه هي قائمة استجابات الاستكشافات التي تم تلقيها. الاول القناة، والثاني ميكروثانية مأخوذة لاستقبالها.

```
Sep 27 11:42:38.808: CDD078F1-0 Uplink: Compare1 0021.d835.ade0 - Rssi 58dBm, Hops 0, Count 0,
                                                                                    load 0
Sep 27 11:42:38.809: CDD07929-0 Uplink: Compare2 0021.d835.cce0 - Rssi 46dBm, Hops 0, Count 0,
                                                                                    load 0
```

تم إجراء مقارنة فعلية في هذه التفاصيل:

```
Sep 27 11:42:38.809: CDD07BDB-0 Uplink: Same as previous, send null data packet
```

التحديد الأصلي

```
Sep 27 11:42:38.809: CDD07BF7-0 Uplink: Done
,Sep 27 11:42:38.808: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0
.Associated To AP AP1 0021.d835.ade0 [None WPAv2 PSK]Roaming completed
```

هذه هي النقطة التي "انتهى" فيها التجوال. تستأنف حركة المرور بمجرد أن تتم معالجة إطارات IAPP بواسطة الأصل.

معلومات المقارنة الأصلية

```
Sep 27 14:16:47.590: F515B1FF-0 Uplink: Compare1 0021.d835.7620 - Rssi 60dBm, Hops 0, Count 0,
```

```
                                                                    load 3
Sep 27 14:16:47.591: F515B238-0 Uplink: Compare2 0021.d835.e8b0 - Rssi 58dBm, Hops 0, Count -1,
                                                                    load 0
```

تطبع المقارنة 1 عدد الاقترانات الفعلي -1 (وبالتالي لا يتم أخذ WGB نفسه في الرقم) إذا كانت نقطة الوصول "الحالية" لا تزال هي واحدة من نقاط الوصول WGB المقترنة، ثم القفزات والحمولة الفعلية.

المقارنة 2 تطبع الاختلافات. لهذا السبب من الممكن رؤية عدد سالب. إذا كان للاختبار رقم أعلى من الحالي، سترى سالب.

بناء على عدد الاقترانات الحالي، التحميل، فرق الإشارات، قيمة حد الهاتف المحمول، قد يحدد WGB أو لا يحدد أصلا جديدا.

دائما ما تكون المقارنة بين نقطتين AP، مع إستبدال نقطة الوصول المحددة للتكرار التالي. وبالتالي، قد يكون سبب بعض القرارات هو RSSI في حلقة واحدة، أو نتيجة عوامل أخرى في الاختبار التالي.

معلومات ذات صلة

- كيفية استخدام AIOS WGB مع مصادقة EAP-TLS في شبكة Cisco اللاسلكية الموحدة
- 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).