دليل التصميم CX - السلكي للشبكات العامة الكبيرة

المحتويات

المقدمة

دليل تصميم CX

النطاق والتعريف

الشبكات العامة الكبيرة

المراجع الخارجية

الخلاصة والمؤلفون

تصميم الشبكة

اعتبارات التردد اللاسلكي

أنواع المواقع

استراتيجيات التغطية

الجوانب

الشبكات الداخلية

5 جيجاهرتز مقابل 5 جيجاهرتز واحدة 5 جيجاهرتز

الهوائيات

6 جيجاهرتز و كثافة عالية

إدارة الموارد اللاسلكية

تكوين التردد اللاسلكي

القنوات

متطلبات البيانات

أساسيات القوة

قنوات الإطار

RxSOP

تغيير حجم الشبكة

أولوية نطاق التردد

نظام WLC الأساسي

الاتجاهات العالية لـ WLC

الخارجية المنظمة

DNS/DHCP

تشغيل الشبكة

التهيئة الصحيحة

SSIDs

تخطيط SSIDs

WPA2/3 الشخصي

WPA2/3 المؤسسي

الفصل بين SSIDs

عدد SSIDs لكل استنتاجات

سياسة الراديو SSID مقابل مفاهيم SSID القديمة

سمات SSID

المواقع العامة

تعريف ملف التهجين

تعريف ملف تعريف AP

قارم الشبكة
رثكأ قارم كلمات أن تستطيع ،كلمات قارم رثكأ بسبب مشاكل الخاصة
قرم الشبكات الكبيرة بالمشاكل الخاصة
نيمدختسملا ةعاضر قارم :ةيناثلا ميمصتلا قارم
ةيعيبطلا ةيلاتلا تاويحملا
9800 زارطلا يف ةهجاولاو SVIs ذفانم
عمجملا رابسلا ةعاجتسا
IPv6
mDNS
ةكبشلا ةيوقت
نامألا
نقاطلا لوصولا لخدي
WiPS
لدعملا نودحملا للعملاع
تقيدي وصولا للعملاع
روملا عاونأ نم ةياقحلا
رارقلا

المقدمة

يوضح هذا المستند إرشادات التصميم والتكوين لشبكات Wi-Fi العامة الكبيرة.

دليل تصميم CX

تتم كتابة أدلة تصميم CX بواسطة أخصائيين من مركز المساعدة الفنية (TAC) من Cisco والخدمات الاحترافية (PS) من Cisco، كما تتم مراجعتها بواسطة خبراء من Cisco؛ تستند الأدلة إلى ممارسات Cisco الرائدة بالإضافة إلى المعرفة والخبرة المكتسبة من عمليات تنفيذ ال تحصى للعملاء على مدى سنوات عديدة. تساعد الشبكات التي تم تصميمها وتكوينها بما يتماشى مع التوصيات الواردة في هذا المستند على تجنب المزالق الشائعة وتحسين تشغيل الشبكة.

النطاق والتعاريف

يقدم هذا المستند إرشادات التصميم والتكوين للشبكات اللاسلكية العامة الكبيرة.

التعريف: الشبكات العامة الكبيرة - عمليات النشر اللاسلكية، عادة ما تكون عالية

الكثافة، والتي توفر إمكانية الاتصال بالشبكة لآلاف الأجهزة العميلة غير المعروفة و/أو غير المدارة.

يفترض هذا المستند بأن الشبكة الهدف توفر خدمات للأحداث الكبيرة و/أو المؤقتة. كما أنها تلائم الشبكات الدائمة الثابتة للأماكن التي تستقبل العديد من الضيوف. وأي شبكة Wi-Fi في ملعب على سبيل المثال، يتميز مركز تسوق أو مطار بأوجه الشبه مع شبكة يكون للتغطية اللاسلكية للأحداث أو المواقع الكبيرة مجموعة متطلبات خاصة بها، والتي تختلف عن المؤسسات أو الصناعات التحويلية أو حتى شبكات التعليم الكبيرة عادة ما. فالشبكات العامة الضخمة قد تحتوي على الآلاف من الناس، الذين يتركزون في مبنى واحد أو بضعة مبان. فقد تكون لديهم قدرة عالية على التجوال مع العميل بشكل دائم وأثناء عمليات الوصول إلى الذروة، كما يجب أن تكون الشبكة متوافقة قدر الإمكان مع أي شيء من حيث أجهزة العميل اللاسلكية دون أي تحكم في تكوين جهاز العميل وأ تأمينه.

يقدم هذا الدليل مفاهيم عامة للتردد اللاسلكي بالنسبة للكثافة العالية وتفاصيل التنفيذ. ينطبق الكثير من مفاهيم الراديو في هذا الدليل على كل الشبكات عالية الكثافة، بغض النظر عن منصة الأجهزة. ومع ذلك، تركز تفاصيل التنفيذ وتكويناته على Catalyst 9800، حيث إن هذا هو الحل باستخدام وحدة التحكم اللاسلكية Catalyst Wireless الأكثر شيوعا الذي يتم نشره للشبكات العامة الكبيرة اليوم.

يستخدم هذا المستند مصطلحات وحدة التحكم اللاسلكية ووحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) بشكل متبادل.

الشبكات العامة الكبيرة

تكون شبكات الأحداث العامة الكبيرة فريدة في العديد من الجوانب، ويستكشف هذا المستند ويقدم إرشادات حول هذه المجالات الأساسية.

- الشبكات العامة الضخمة مكثفة؛ هناك الآلاف من الأجهزة في مساحة منخفضة قد تكون وقد تتداخل الراديو (RF) والتجوال العام حيث يتجول الناس في بعض المناطق وتتركز بعض الأحداث والأماكن أكثر استاتيكا مع ذروة عرض النطاق الترددي في أوقات محددة للغاية. تحتاج البنية الأساسية إلى التعامل مع كافة تغييرات الحالة هذه بأناقة قدر الإمكان للعملاء الذين يدخلون ويتجولون في المنطقة.
- العميل المقترن هو عميل يعتبر سوء الانضمام إلى فريق العمل إحدى الأولويات. العميل سيء. وهذا يعني أنك تريد إنشاء اقتران العميل بالشبكة بأسرع ما يمكن. العميل غير المتصل بميزة المسح باستخدام تقنية Wi-Fi (Wi-Fi) نقاط الوصول المتوفرة التي تولد طاقة تردد السلكي (RF) غير المرغوب فيها، مما يؤدي إلى حدوث إزدحام إضافي وفقدان للسعة عبر الهواء.
- يجب توفر تصميم عملية نشر الترددات اللاسلكي بعناية قدر الإمكان. يجب تصميم مناسب للترددات اللاسلكي باستخدام هوائيات اتجاهية في حالة الحاجة إلى كثافة

عالية جدا، أو إذا كان الموقع يحتوي على مساحات مفتوحة كبيرة و/أو أسقف عالية.

- في قياسية هي الميزات بعض. التوافق وه المفاتيح لتصميم آخر أقراص ومحرك. ومع ذلك، مواصفات 802.11 بين الميزات الأخرى خاصة، فلا تطرح أي مشكلة للعملاء. ومع ذلك، فإن الواقع مختلف وهناك العديد من برامج تشغيل العملاء غير المبرمجة بشكل جيد التي لا تسيء التصرف عند مواجهة أجهزة الإرشاد المعقدة أو الميزات/الإعدادات التي تفهمها.
- إذا. والوقت باللحجم المتعلقة المشكلات وحلها تحدي نظرا للقيود المتعلقة باللحجم والوقت. إذا كنت تواجه مشكلات في اكتشاف الأجهزة المحمولة، فقد لا تتمكن من العمل مع هذا المستخدم النهائي بشكل فعال. من الممكن أن يكون العثور على المستخدمين أمرا صعبا، غير أنه من الممكن أيضا أن يكونوا غير متعاونين بسبب الطبيعة العابرة لزياراتهم في الموقع.
- الزوار الزائرين من الكبير جدا العدد بسبب السيطرة من أقل قدر وهناك. مهم عامل من الأمن. وطبيعة هجوم أكبر بكثير.

المراجع الخارجية

اسم المستند	المصدر	الموقع
أفضل ممارسات تكوين Cisco Catalyst 9800 Series	Cisco	الارتباط
أستكشاف أخطاء وحدة التحكم في الشبكة المحلية اللاسلكية وإصلاحها	Cisco	الارتباط
التحقق من إنتاجية Wi-Fi: دليل الاختبار والمراقبة	Cisco	الارتباط
دليل نشر نقطة وصول Cisco Catalyst CW9166D1	Cisco	الارتباط
دليل النشر Cisco 9179F	Cisco	الارتباط
دليل نشر الهوائي الاستوائي Catalyst 9104 (C-ANT9104)	Cisco	الارتباط
مراقبة Catalyst 9800 KPIs (مؤشرات الأداء الرئيسية)	Cisco	الارتباط
أستكشاف أخطاء اتصال العملاء لـ Catalyst 9800 وإصلاحها	Cisco	الارتباط
دليل تكوين برنامج وحدة التحكم اللاسلكية من Cisco Catalyst 9800 Series	Cisco	الارتباط
Wi-Fi 6E: الفصل الرائع التالي في تقرير واي فاي	Cisco	الارتباط

إخلاء المسؤولية

تقدم هذه الوثيقة توصيات مبنية على سيناريوهات وافتراضات ومعرفة معينة تم الحصول عليها من عمليات نشر عديدة. ومع ذلك، أنت القارئ مسؤول عن تحديد تصميم الشبكة والأعمال والتوافق مع الإشعارات التنظيمية والأمان والخصوصية ومتطلبات أخرى، بما في ذلك ما إذا كنت ستتبع الإرشادات أو التوصيات الواردة في هذا الدليل.

تصميم الشبكة

اعتبارات التردد اللاسلكي

أنواع الموقع

يركز هذا الدليل على شبكات الزائرين الكبيرة، المفتوحة عادة للجمهور، وبتحكم محدود في المستخدمين النهائيين وأنواع أجهزة العملاء. يمكن نشر هذه الأنواع من الشبكات في مجموعة متنوعة من المواقع ويمكن أن تكون مؤقتة أو دائمة. فغالبا ما تكون حالة الاستخدام الأساسي هي توفير الإتصال بالإنترنت للزوار، على الرغم من أن هذه الحالة نادرا ما تكون هي حالة الاستخدام الوحيدة.

المواقع النموذجية:

- ملاعب وملاعب
- صالات مؤتمرات
- صالات عرض كبيرة

ومن وجهة نظر التردد اللاسلكي، فإن لكل نوع من أنواع المواقع هذه مجموعته الخاصة من الفروق الدقيقة. وعادة ما تكون معظم هذه الأماكن عبارة عن مبانٍ داخلية، بخلاف أماكن عقد المؤتمرات/الحفلات الموسيقية، حيث يمكن أن تكون هذه منشآت دائمة أو مهيأة لعرض معين على أساس مؤقت.

المواقع الأخرى:

- سفينة سياحية
- مطار
- مركز تسوق

وتعد المطارات والسفن السياحية أيضا مثالا لعمليات الانتشار التي تندرج في فئة الشبكات العامة الكبيرة؛ غير أن لهذه الاعتبارات اعتبارات إضافية خاصة بكل حالة وكثيرا

ام تستخدم نقاط وصول داخلية متعددة الاتجاهات.

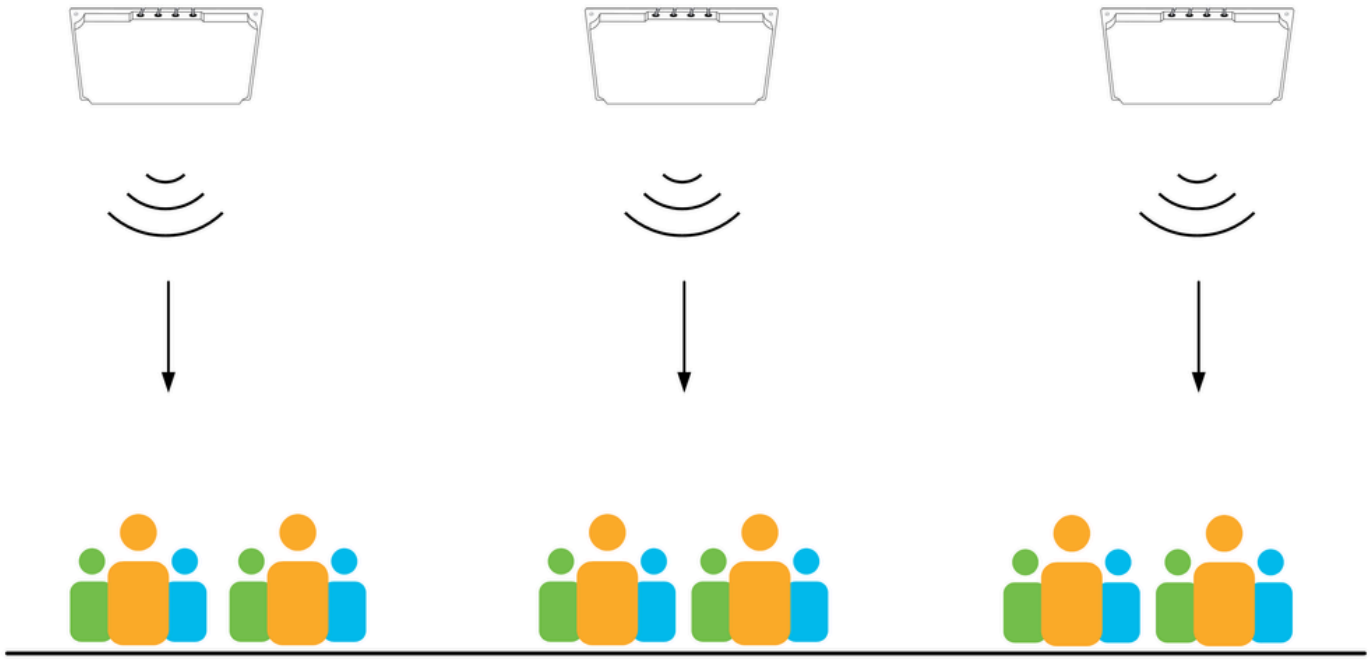
إستراتيجيات التغطية

تعتمد إستراتيجيات التغطية بشكل كبير على نوعية الموقع، الهوائيات المستخدمة، ومواقع تركيب الهوائيات المتوفرة.

فوقي

وتفضل التغطية العامة دائما كلما أمكن ذلك.

تتمتع الحلول العلوية بميزة مميزة وهي أن جميع أجهزة العملاء لديها خط رؤية مباشر للهوائي في جميع الحالات، حتى في السيناريوهات المزدحمة. كما توفر الحلول العلوية التي تستخدم هوائيات اتجاهية مساحة تغطية أكثر تحكما ومعرفة بشكل جيد مما يجعلها أقل تعقيدا من وجهة نظر ضبط الراديو مع توفير موازنة فائقة للأحمال وخصائص التجوال لدى العميل. انظر القسم المتعلق بميزان الطاقة للحصول على مزيد من المعلومات.

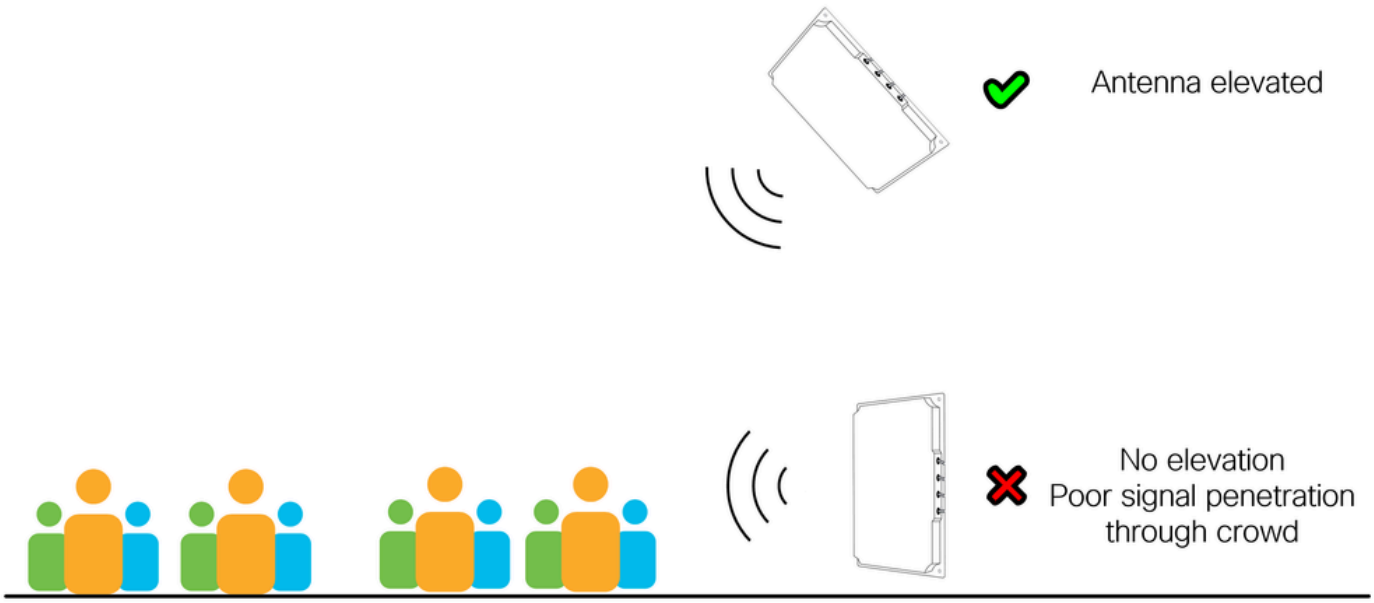


نقاط الوصول أعلى من العملاء

طرف

تعد الهوائيات الجانبية المثبتة في الإتجاه خيارا شائعا وتعمل بشكل جيد في مجموعة متنوعة من السيناريوهات، لا سيما عندما يكون التركيب الزائد غير ممكن بسبب قيود الارتفاع أو التركيب. عند إستخدام التركيب الجانبي، من المهم فهم نوع المساحة التي

يغطيها الهوائي، على سبيل المثال، هل هي منطقة مفتوحة في الهواء الطلق أو منطقة كثيفة داخل المباني؟ إذا كانت منطقة التغطية منطقة ذات كثافة عالية وبها العديد من الأشخاص، فيجب رفع الهوائي قدر الإمكان حيث تكون نسبة انتشار الإشارة عبر الحشود البشرية ضعيفة دائما. تذكر أن معظم الأجهزة المحمولة يتم إستخدامها في أسفل مستوى الخصر، وليس أعلى من رأس المستخدم! ويكون إرتفاع الهوائي أقل أهمية عندما تكون مساحة التغطية منطقة ذات كثافة منخفضة.



دائما ما يكون إرتفاع الهوائي أفضل

متعدد الاتجاهات

يجب تجنب إستخدام الهوائيات متعددة الإتجاه (الداخلية أو الخارجية) بشكل عام في سيناريوهات عالية الكثافة، ويرجع ذلك إلى احتمال وجود مساحة تأثير عالية لتداخل القناة المشتركة. يجب ألا يتم إستخدام الهوائيات متعددة الإتجاه على إرتفاع يزيد عن 6 أمتار (يطبق على الوحدات الخارجية ذات التضخيم العالي).

مقعد تحت المقعد

في بعض الملاعب أو الملاعب قد توجد مواقف لا توجد فيها أماكن مناسبة لتركيب الهوائيات. أما البديل الأخير المتبقي فهو توفير التغطية من الأسفل من خلال وضع نقاط الوصول في المقاعد التي يجلس عليها المستخدمون. يكون هذا النوع من الحلول أكثر صعوبة في النشر بشكل صحيح وهو عادة أكثر تكلفة ويتطلب عدد أكبر من نقاط الوصول وإجراءات تثبيت محددة بشكل كبير.

التحدي الرئيسي مع نشر الجنود تحت المقعد هو الإختلاف الكبير في التغطية بين مكان كامل ومكان فارغ. الجسم البشري عامل جدا في تخفيف إشارة الراديو، مما يعني أنه عندما

لقل أن تكون التغطية الناتجة كافية لتوفير الوصول إلى نقاط الوصول المتداخلة. يكون هناك حشد من الناس يحيطون بالأسوشيتد برس فإن التغطية الناتجة تكون أقل بكثير مما هو مطلوب لمعظم التطبيقات. يتيح هذا العامل بشكل عام مقارنة بالوقت الذي لا يكون فيه هؤلاء الناس هناك. يتيح هذا العامل زيادة التغطية لتخفيف عدد الحشود إمكانية نشر المزيد من نقاط الوصول التي يمكنها تحمل السعة الإجمالية. غير أنه عندما يكون الموقع فارغا فإنه لا يكون هناك أي إطار للجثث البشرية أو أي تداخل ذي شأن، وهذا يؤدي إلى تعقيدات عندما يكون الموقع ممتلئا جزئيا.

ملاحظة: النشر تحت الموقع هو حل صحيح ولكنه غير شائع، ويجب تقييمه على أساس كل حالة على حدة. والتناقش هذه الوثيقة بمزيد من التفصيل تحت الموقع.

الجمالية

في بعض عمليات النشر، تدخل مسألة الجمالية في الاعتبار. وقد تكون هذه المناطق ذات التصميمات المعمارية المحددة، أو ذات القيمة التاريخية، أو مساحات حيث تملي الإعلانات و/أو العلامات التجارية أماكن حيث يمكن (أو لا يمكن) تركيب المعدات. من المحتمل أن تكون هناك حاجة إلى حلول محددة للتغلب على أي قيود تتعلق بالموضع. تتضمن بعض هذه الحلول إخفاء نقطة الوصول (AP)/الهوائي، وتغطية نقطة الوصول (AP)/الهوائي، وتركيب الجهاز في حاوية، أو بسماطة إستخدام موقع مختلف. إلا إن طلاء الهوائي يلغي الضمان. لا تبيع Cisco الهوائيات، ولكن العديد منها متوفر بسهولة من خلال مزودين متعددين الذين يبيعون أيضا أغطية متنوعة وسبل تجعل نقاط الوصول تتطابق مع جمالية متنوعة.

تأثر جميع هذه الحلول على أداء الشبكة. يبدأ المعماريون اللاسلكيون دائما باقتراح وضعيات تركيب مثالية للحصول على أفضل تغطية للراديو، وتوفر هذه المواقع الأولية عادة أفضل أداء. أي تغييرات تطرأ على هذه المواقع تؤدي في الغالب إلى نقل الهوائيات بعيدا عن مواقعها المثالية.

الأماكن التي تركب فيها الهوائيات تكون عادة مرتفعة حيث يمكن أن تكون سقوف مرتفعة جدا أو أعمدة أو أي موقع يرتفع إلى حد ما فوق منطقة التغطية ومسطحات أو أبنية مرورا وممرات المقصودة. تتم مشاركة هذه المواقع عادة مع التثبيتات الأخرى، مثل: معدات سمعية، وتكييف، وإضاءة، وكاميرات، وأجهزة إستشعار/أجهزة إستشعار مختلفة. على سبيل المثال، لا بد من تركيب معدات الصوت والإضاءة في مواقع محددة للغاية ولكن لماذا؟ بسماطة، لأن معدات الصوت والإضاءة لا تعمل بشكل صحيح عندما تكون مخبأة في صندوق أو خلف حائط.

ينطبق نفس الشيء على الهوائيات اللاسلكية فهي تعمل بأفضل شكل عندما يكون (وغالبا ما يحدث ذلك) أن يكون له تأثير سلبي على أداء الشبكات اللاسلكية، مما يقلل من قيمة الاستثمار في البنية التحتية.

الشبكات الداخلية

شبكات Wi-Fi المخادعة هي شبكات لاسلكية تشترك في مساحة تردد لاسلكي مشتركة وتتضمن ولكنها لا تتم إدارتها بواسطة نفس المشغل. يمكن أن تكون مؤقتة أو دائمة (مثل الهواتف المحمولة التي تشترك في نقطة اتصال Wi-Fi). شبكات Wi-Fi المخادعة هي مصدر تداخل وفي بعض الحالات أيضا خطر أمني. يجب عدم التقليل من تأثير المخربشات على أداء الشبكات اللاسلكية. تقتصر عمليات إرسال Wi-Fi على مجموعة صغيرة نسبيا من طيف الراديو الذي يتم تقاسمه بين جميع أجهزة Wi-Fi، وأي أجهزة لسوء السلوك في حالة مجاورة يمكن أن تعطل أداء الشبكة بالنسبة للعديد من المستخدمين.

وعادة ما يتم تصميم هذه الهوائيات بعناية وضبطها في سياق الشبكات العامة الكبيرة باستخدام هوائيات متخصصة. يغطي التصميم الجيد للتردد اللاسلكي المساحات المطلوبة فقط، وعادة ما يستخدم هوائيات موجهة ذات خصائص إرسال واستقبال مضبوطة لضمان أعلى كفاءة.

وعلى الطرف الآخر من هذا النطاق هناك الأجهزة التي تنتمي إلى فئة المستهلكين، أو الأجهزة التي يوفرها موزود خدمة الإنترنت. إما أن هذه الوحدات لديها خيارات محدودة من أجل ضبط دقيق للتردد اللاسلكي أو تم تكوينها لأقصى نطاق وأداء متوقع، وغالبا ما تكون ذات طاقة المطلوبة فقط، وعادة ما يستخدم هوائيات موجهة ذات خصائص إرسال واستقبال مضبوطة لضمان أعلى كفاءة. إن إدخال مثل هذه الأجهزة في شبكة للحد عالية ومعدلات بيانات منخفضة وقنوات عريضة. إن الكبير يمكن أن يؤدي إلى الفوضى.

فماذا يمكن فعله؟

في حالة النقاط الساخنة الشخصية يكون هناك القليل جدا الذي يمكن القيام به، حيث سيكون من المستحيل تقريبا مراقبة عشرات الآلاف من الناس الذين يدخلون إلى الموقع. في حالة البنية الأساسية، أو الأجهزة شبه الدائمة، هناك بعض الخيارات. وتبدأ عملية القياس الحتملة من التعليم البسيط، والإطاحات الإعلامية للتوعية، ومن خلال وثائق السياسات الإذاعية الموقعة، وتنتهي بالإنفاذ النشط وتحليل الطيف. وفي جميع الحالات، يتعين إتخاذ قرار بشأن حماية طيف الراديو في الموقع المحدد، إلى جانب خطوات ملموسة لتطبيق قرار الشركة.

ويلعب جانب الأمان للشبكات المخادعة عندما تعلن الأجهزة التي يتم التحكم فيها بواسطة SSID الخاص بالشبكة المدارة. وهو ما يعادل هجوم قضاء شهر العسل عن نفس SSID الخارجية المخادعة. ويمكن إستخدامه كوسيلة لسرقة بيانات المستخدم. يوصى دائما بإنشاء قاعدة مخادعة للتنبيه عند اكتشاف SSIDs للبنية الأساسية المعلن عنها بواسطة الأجهزة غير المدارة. يناقش قسم الأمن الفاسدات بمزيد من التفصيل.

سرعة 5 جيجاهرتز مقابل 5 جيجاهرتز واحدة

تشير السرعة المزدوجة 5 جيجاهرتز إلى إستخدام كل الجهازين اللاسلكيين 5 جيجاهرتز على نقاط الوصول المدعومة. هناك فرق أساسي بين السرعة المزدوجة 5 جيجاهرتز التي تستخدم الهوائيات الخارجية والسعة المزدوجة 5 جيجاهرتز والتي تستخدم الهوائيات الداخلية (على سبيل المثال، الخلايا الدقيقة/الكبيرة الموجودة على نقاط الوصول متعددة الإتجاه). وفي

حالة الهوائيات الخارجية المزودة 5 جيجاهرتز غالبا ما تكون آلية مفيدة توفر تغطية وسعة إضافيتين مع تقليل العدد الإجمالي لنقاط الوصول.

وزيم/وركام/قيقد

تحتوي نقاط الوصول (AP) الداخلية على كل من الهوائيين القريبين معا (داخل نقطة الوصول) وهي عرضة لقيود تتعلق بالحد الأقصى من طاقة Tx عند إستخدام 5 جيجاهرتز المزودة بتكوين ذلك وحدة التحكم (Tx) لإرسال منخفضة (تفرض الثاني على طاقة إرسال (Tx) بين أجهزة الراديو. وقد تؤدي إلى إختلال كبير في طاقة إرسال الإرسال (Tx) بين أجهزة الراديو السلكية (مما يؤدي إلى أن يجذب الراديو الأساسي (ذو الطاقة الأعلى) عملاء كثيرين في حين أن الراديو الثانوي (ذو الطاقة الأقل) لا يستخدم على نحو كاف. وفي هذه الحالة، يضيف جهاز الراديو الثاني طاقة إلى البيئة دون تقديم فائدة للزبائن. في حالة ملاحظة هذا السيناريو، قد يكون من الأفضل تعطيل الراديو الثاني ومجرد إضافة نقطة وصول (وحيدة) بسرعة 5 جيجاهرتز) في حالة الحاجة إلى سعة إضافية.

تختلف خيارات التهيئة بين مختلف نماذج نقاط الوصول، ويمكن تشغيل جهاز الإرسال الثاني بسرعة 5 جيجاهرتز عند مستويات طاقة أعلى في نقاط الوصول الأحدث اللاسلكي Wi-Fi للمركز/وزيم نقاط الوصول مثل 9136، كما يمكن تشغيل بعض نقاط الوصول 9130 و 9160 في المركز/المركز. تحقق دائما من إمكانية نموذج نقطة الوصول (AP) الدقيق. كما أن الفتحة الثانية بسرعة 5 جيجاهرتز تكون محدودة في إستخدام القناة الخاصة بها، فعندما يكون أحد الفتحات يعمل في نطاق UNII واحد، يكون الفتحة الأخرى مقيدة بنطاق UNII مختلف، مما يؤثر على تخطيط القنوات وفيما بعد طاقة الإرسال المتوفرة. ضع فرق طاقة إرسال الإرسال (Tx) بين أجهزة الإرسال اللاسلكي المزودة بسرعة 5 جيجاهرتز دائما في الاعتبار، وهذا صحيح في جميع الحالات، بما في ذلك نقاط الوصول (AP) المزودة بهوائيات داخلية.

ارف

تم إدخال تقنية التخصيص اللاسلكي المرن (FRA) كتقنية لتحسين تغطية الـ 5 جيجاهرتز من خلال تحويل أجهزة السلكية إضافية بسرعة 2. 4 جيجاهرتز إلى وضع 5 جيجاهرتز أو أجهزة السلكية 5 جيجاهرتز غير مستخدمة محتملة في وضع الشاشة (لنقاط الوصول التي تدعمها). بما أن هذا المستند يغطي شبكات عامة كبيرة، فقد افترض أن معظم هذه الشبكات تصميم الراديو محددا بشكل جيد باستخدام هوائيات اتجاهية، لذلك التغطية وكذلك تعديل FRA للشبكات العامة الكبيرة. الوصى باستخدام FRA في تكوين ديناميكي. لتكوين محدد على حدة لنقاط الوصول (AP) التي تعمل بسرعة 5 جيجاهرتز، ولكن بمجرد سعادتك في إعداد الشبكة للمساعدة (FRA) عند إستخدام أشعة تحت الحمراء، يمكن إستخدام أشعة تحت الحمراء بشكل إختياري، وبشكل خاص، ينصح بتجميد الأشعة تحت الحمراء.

تنظيمي

يحدد كل مجال تنظيمي القنوات المتاحة للاستخدام والحد الأقصى من مستويات الطاقة، كما توجد قيود على القنوات التي يمكن إستخدامها داخل المباني مقارنة بخارجها. واعتمادا على المجال التنظيمي، قد لا يكون من الممكن في بعض الأحيان إستخدام حل مزدوج بسرعة 5 جيجاهرتز بشكل فعال. ومثال على ذلك هو مجال ETSI حيث يتم السماح باستخدام 30dBm على قنوات UNII-2e، ولكن يتم إستخدام 23 ديسيبل فقط على UNII1/2. في هذا المثال، إذا كان التصميم يتطلب إستخدام 30dBm (عادة بسبب المسافة الأعلى إلى الهوائي)، فإن إستخدام جهاز لاسلكي واحد بسرعة 5 جيجاهرتز يمكن أن يكون الحل الوحيد الممكن.

في بعض الأحيان تتم إضافة قنوات إضافية في إصدار برنامج لاحق إلى مجالات تنظيمية معينة، ولكن من الممكن أن تلك القنوات تحتوي على قوة إرسال قصوى مختلفة أيضا : دقق أن زبائنك يستخدمون هذا قناة وفقط استخدمهم على APs حيث لا transmit power لن يكون مشكلة.
في حالة رغبتك في إستخدام كل القنوات المتاحة، قد يكون من المثير أن تقوم بإنشاء توصيفات تردد لاسلكي حيث تتطلب نقاط الوصول (APs) أعلى طاقة إرسال (مثل نقاط الوصول المثبتة على سقف مرتفع جدا) إستخدام القنوات فقط حيث توجد طاقة أعلى والاحتفاظ بقنوات ذات طاقة أقل لنقاط الوصول الأقرب إلى الأرض في المناطق الأكثر كثافة.

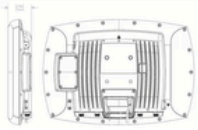
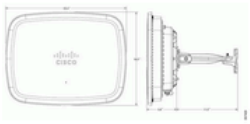
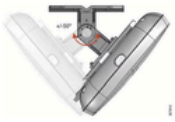
الهوائيات

تستطيع الشبكات العامة الكبيرة إستخدام أي نوع من الهوائيات وتقوم عادة بنشر أكثر الهوائيات ملاءمة لهذه المهمة. إن خلط الهوائيات في نفس منطقة التغطية يجعل عملية تصميم لاسلكي أكثر صعوبة ويجب تجنبها إن أمكن. غير أن الشبكات العامة الكبيرة كثيرا ما تكون لها مناطق تغطية واسعة ذات خيارات تركيب مختلفة حتى داخل نفس المنطقة، مما يجعل من الضروري مزج الهوائيات في بعض الحالات.

يسرد هذا الجدول الهوائيات الخارجية الأكثر إستخداما:

	C-ANT9103 Patch antenna (8x8) 6 dBi	5GHz Beamwidth 70°x70° ~33ft (10m)
	ANT2566P4W-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 110°x55° (120°x60°) ~33ft (10m)
	ANT2566D4M-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 55°x60° (60°x60°) ~33ft (10m)
	ANT2513P4M-N/S HD "Stadium" antenna 13 dBi	5GHz Beamwidth 31°x27° (30°x30°) ~66ft (20m)

يسرد هذا الجدول الهوائيات المتكاملة ذات الإتجاه الأكثر إستخداما:

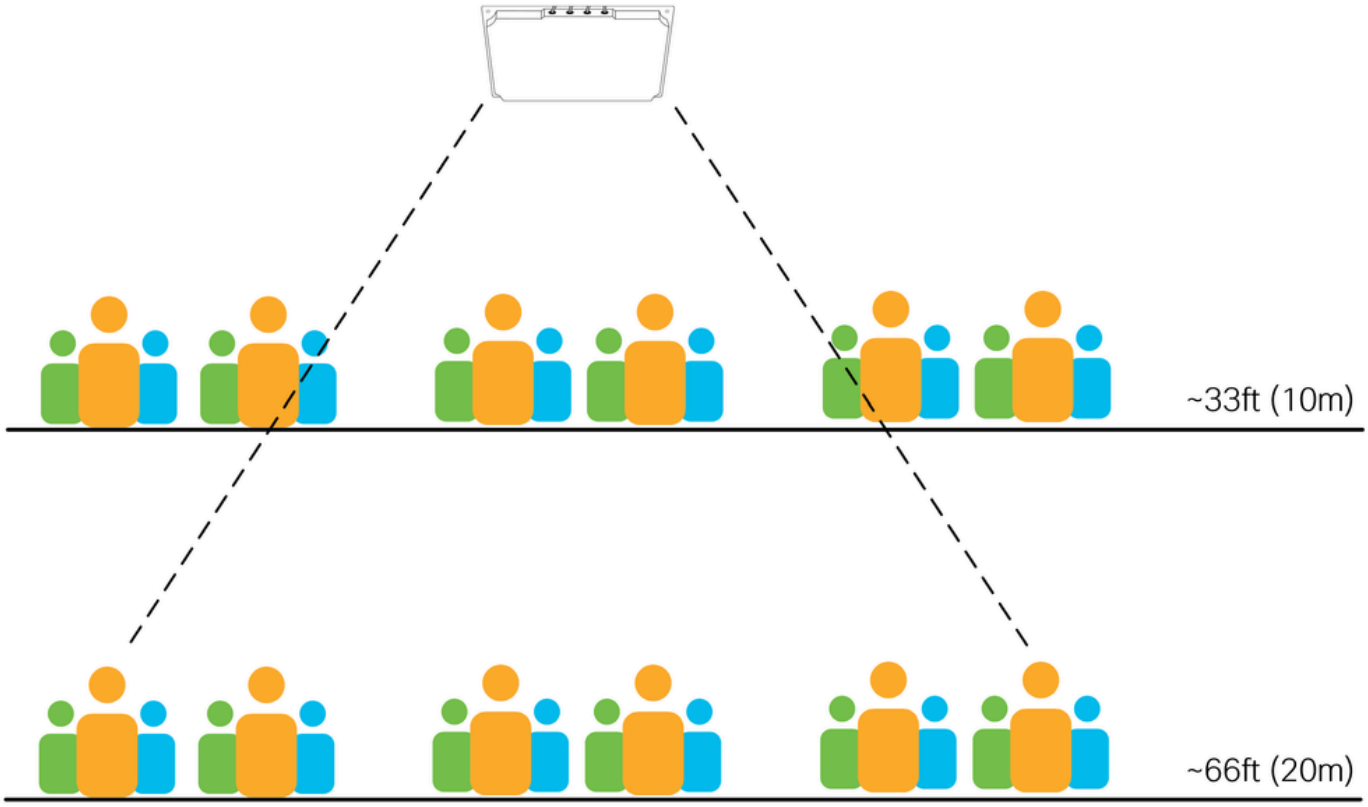
	CW9179F Integrated directional ~100ft (30m) *See data sheet for gain info.*	5GHz Narrow 35° x 35° Wide *See data sheet*	6GHz Narrow 35° x 35° Wide 70° x 35°
	C-ANT9104 Integrated directional ~66ft (20m)	5GHz Narrow 25° x 25° : 10dBi Wide 80° x 25° : 7dBi	
	CW9166D1 Integrated directional ~33ft (10m) *See data sheets for XOR info.*	6GHz 60° x 60° 8 dBi	5GHz 70° x 70° 6 dBi
	CW9176D1 Integrated directional ~33ft (10m) *See data sheets for XOR info.*	6GHz 70° x 70° 8 dBi	5GHz 70° x 70° 8 dBi

من العوامل الأساسية التي يجب مراعاتها عند إختيار الهوائي عرض إطار الهوائي والمسافة/الطول الذي يتم فيه تركيب هذا الهوائي. تظهر الجداول عرض الحزمة للهوائيات المستخدمة بشكل شائع، مع إظهار الأرقام بين قوسين لقيم دائرية (وأسهل تذكرها).

والمسافات المقترحة في الجدول ليست قواعد ثابتة، بل هي مجرد مبادئ توجيهية تستند إلى الخبرة. تسافر الموجات الراديوية بسرعة الضوء ولا تتوقف بمجرد الوصول إلى مسافة اعتباطية. ورغم أن جميع الهوائيات تعمل خارج المسافة المقترحة، يقل الأداء كلما زادت المسافة. يعد إرتفاع التثبيت عامل أساسي أثناء التخطيط.

يوضح الرسم التخطيطي التالي ارتفاعين محتملين لتركيب الهوائي نفسه بمسافة تقارب 33 قدما (10 أمتار) و 66 قدما (20 مترا) في منطقة عالية الكثافة. لاحظ أن عدد العملاء الذين يمكن للهوائي رؤيتهم (وقبول الاتصالات منهم) يتزايد مع المسافة. كما أن الحفاظ على أحجام الخلايا الأصغر حجما يصبح أكثر صعوبة مع مسافات أكبر.

القاعدة العامة هي زيادة كثافة المستخدمين، الأمر الأكثر أهمية هو إستخدام الهوائي الصحيح للمسافة المحددة.



هوائي الاستاد

يعد CW9179F مناسبا تمامًا لتغطية المناطق عالية الكثافة على مسافات عالية، انظر دليل نشر نقطة الوصول Cisco Wireless 9179F للحصول على معلومات.

التغييرات مع مرور الوقت

تعد التغييرات التي تطرأ على البيئة على مر الزمن أمرًا شائعًا في جميع التركيبات اللاسلكية تقريبًا (على سبيل المثال، حركة الجدران الداخلية أو إعادة تخطيط المقاعد في الموقع). وكانت دائمًا الزيارات المنتظمة إلى المواقع وعمليات التفتيش البصري ممارسة موصى بها. بالنسبة لشبكات الأحداث، يكون هناك تعقيد إضافي في التعامل مع أنظمة الصوت والإضاءة، وفي العديد من الحالات أيضًا أنظمة الإتصالات الأخرى (مثل 5G). وغالبًا ما يتم تركيب جميع هذه النظم في مواقع مرتفعة فوق المستخدمين، مما يؤدي أحيانًا إلى التنازع على نفس المساحة. غالبًا ما يكون الموقع الجيد لهوائي الاستاد اللاسلكي مكانًا جيدًا لهوائي الجيل الخامس! علاوة على ذلك، فإنه مع تحديث هذه الأنظمة بمرور الوقت، يمكن نقلها إلى أماكن تعيق و/أو تعيق فيها النظام اللاسلكي بشكل فعال. ومن المهم تتبع التركيبات الأخرى والاتصال بالفرق التي تقوم بتركيبها لضمان تركيب جميع الأنظمة في مواقع مناسبة دون التدخل في بعضها البعض (مادياً أو كهرومغناطيسياً).

كثافة عالية و 6 جيجاهرتز

توفر الحزمة الأنظف والأقل أزدحاما بسرعة 6 غيغاهرتز تجربة أفضل عبر سرعة 5 غيغاهرتز، مع الاستفادة الإضافية من تخفيض وقت البث بسرعة 5 غيغاهرتز، مع اعتماد المزيد من

5 ددرت ةيطغت ةيفوري تانيبلزلا ةزهجأ .زتراهجيغ 6 ةعرس ءاوس حد يلع زتراهجيج 6 و زتراهجيج ةيرلكبلا ةعماجلا تاكبشلا يف كلذ لثم .
تاجتنم نم ديدعلا Cisco ةمدختسإ 6 زتراهجيج ةحاتملا ةيلاعلا ةعرسلا تاهجوم نم ةعومجم نمضتت ؛ةفاكلا ةيلاعلا رشنلا تايلمع مادختسإ نكمي 9179F رطرزلا ىلع ةيطغت ةحاسم ىلع ةيطغت ةعس وأ ةيطغت ىلع لوصحلل 91x6D1 رطرزلا ىلإ ،زاهجلا ىلع لوصحلل ةيطغت ةعس وأ ةحاسم ىلع ةيطغت ةعس ةيلحملا تاكبشلا ربع 6 زتراهجيج ةعرسب ةعس ميمصت تايارخ ريفوت تاجتنملا هذه نيب عمجلا حيتي .
عقاوملا نم ةعونتم ةعومجم .
تاهجوملا ةيجيتارتسالا ةعرسب 6 زتراهجيغ ةيطغت ميمصت قبس نم ةعبتملا ةجهنملا سفن عم لكشب يعيت زتراهجيغ 6 ةعرسب ةيطغت ميمصت

ن Assignment (DCA) و Transmit Power Control (TPC). RRM وه بديل للقناة الثابتة وتكوي
.الطاقة

- .(قائق 10 دتمه افتراضي) نيوكتلل لباق لودج DCA لىع ليغشت متي
- .(قائق 10 دتمه افتراضي) يئاقلتلا لودج TPC لىع ليغشت متي

RRM الذي يعتمد على الأحداث من Cisco (ED-RRM) وه خيار DCA يسمح باتخاذ قرار تغيير
القناة خارج جدول DCA القياسي، عادة إستجابة لظروف التردد اللاسلكي الشديدة. يمكن أن
يقوم ED-RM بتغيير القناة فورا عند اكتشاف مستويات التداخل الزائدة. في البيئات
الصاخبة و/أو غير المستقرة التي تعمل على تمكين ED-RM على فرض مخاطر حدوث
تغييرات مفرطة في القنوات، فإن هذا يعد تأثيرا سلبيا محتملا على أجهزة العميل.

ومع - الثابت التكوين على عام بشكل ويفضل (RM) الراديو موارد إدارة إستخدام تشجيع يتم
ذلك، مع بعض التنبيهات والاستثناءات.

- يجب أن يقتصر TPC على مجموعة مناسبة من القيم باستخدام إعداد الحد الأدنى/الحد
الأقصى ل TPC، حسب الحاجة، ومحاذاته دائما مع تصميم التردد اللاسلكي.
- تمكين TPC Channel Aware في البيئات عالية الكثافة.

- يجب تغيير دورة DCA من الإعداد الافتراضي الذي يبلغ 10 دقائق.
- تستخدم ED-RM في البيئات المشغولة والضبابية ذات الكثافة العالية.
- تعطيل تجنب تحميل Cisco AP.
- إن خيارات تجنب نقاط الوصول (AP) المخادعة مثل تجنب تداخل نقاط الوصول (AP)
الأجنبية يمكن أن تؤدي إلى بيئة غير مستقرة إذا كان هناك العديد من
المخادعين. إن إزالة المرافق أفضل دوما من محاولة الرد عليه.
- يمكن أن تتأثر قرارات RRM بنقاط الوصول/الهوائيات التي لا تسمع بعضها البعض
بشكل صحيح، كما في حالة الهوائيات الموجهة التي تشير بعيدا عن بعضها البعض.
- تتطلب دائما RRM وتقنية (C9104 على سبيل المثال) الهوائيات بعض تدعم لا
تهيئة ثابتة.
- يصلح RRM التصميم الضعيف للتردد اللاسلكي.

وفي جميع الحالات، يجب نشر إدارة الموارد مع فهم النتائج المتوقعة، ومواءمتها للعمل ضمن
حدود مناسبة لبيئة التردد اللاسلكي المحددة. وتستكشف الأقسام التالية من هذا
المستند هذه النقاط بمزيد من التفاصيل.

تكوين التردد اللاسلكي

القنوات

بشكل عام كلما زادت القنوات كان ذلك أفضل. في عمليات النشر عالية الكثافة، يمكن أن
يكون هناك عدد أكبر من نقاط الوصول (AP) أو أجهزة الراديو المنشورة مقارنة بالقنوات

نم المتاحة، مما يعني نسبة إعادة استخدام قناة كبيرة، بالإضافة إلى ذلك، مستويات أعلى من تداخل القناة المشتركة. يجب استخدام جميع القنوات المتاحة، كما أن تحديد قائمة القنوات المتاحة غير مرغوب فيه بشكل عام.

قد تكون هناك حالات يلزم فيها وجود نظام السلكي محدد (منفصل) في نفس المساحة المادية، كما يجب تخصيص قناة (قنوات) مخصصة له، وفي الوقت نفسه إزالة القناة (القنوات) المخصصة من قائمة DCA للنظام الأساسي. يجب تقييم هذه الأنواع من استبعادات القنوات بعناية كبيرة ويجب استخدامها فقط عند الضرورة. ومثال على ذلك هو المكان الذي يمكن أن يكون وصلة من نقطة إلى نقطة تعمل في منطقة مفتوحة مجاورة للشبكة الرئيسية أو في منطقة صحفية داخل المدرج. إذا تم إستبعاد أكثر من قناة أو قناتين من قائمة DCA، فإن ذلك يعد سببا لإعادة تقييم الحل المقترح. في بعض الحالات، مثل المطارات، باستثناء حتى قناة واحدة قد لا يكون في بعض الأحيان خيارا ممكنا.

يمكن إستخدام تعيين القناة الديناميكية (DCA) مع RRM المستندة إلى WLC أو RRM المحسنة AI.

الفاصل الزمني الافتراضي لـ DCA هو 10 دقائق مما يمكن أن يؤدي إلى تغييرات متكررة للقنوات في بيئات RF غير المستقرة. يجب زيادة مؤقت DCA الافتراضي من الدقائق العشر الافتراضية في جميع الحالات، ويجب محاذاة الفاصل الزمني DCA المحدد مع متطلبات التشغيل للشبكة المعنية. مثال على التكوين يمكن أن يكون: الفاصل 4 لكل مرة واحدة إلى 8. يحد هذا من تغير القناة إلى 4 ساعات، وقت الإرساء لمدة 4 ساعات، بدءا من الساعة 8 صباحا.

بما أن التدخلات من المحتمل أن تحدث، فإن التكيف معها لكل دورة DCA الجلب بالضرورة أن الآلي DCA إستخدام المزايا الكثير من تلك التفاعلات مؤقتة. من التقنيات الجديدة إستخدام DCA قيمة حيث أن القناة عندما يكون لديك شيء في الساعات القليلة الأولى وتجميد الخوارزمية وخطة القناة مستقر تكون سعيدا به.

في DCA، يعمل (WLC)، عند إعادة تمهيد عنصر التحكم في الشبكة المحلية اللاسلكية، يتم إعادة تشغيل الوضع المتميز لمدة 100 دقيقة للعثور على خطة قناة مناسبة. من الأفضل إعادة تشغيل المثال التالي) على سبيل المثال عند إجراء تغييرات مهمة على تصميم التردد اللاسلكي (على سبيل المثال، أستخدم هذه العملية، لبدء هذه العملية. (القناة عرض تغيير أو متعددة وصول نقاط وإزالة أو إضافة الأمر يدويا.

```
ap dot11 [24ghz | 5ghz | 6ghz] rrm dca restart
```

ملاحظة: قد تؤدي تغييرات القنوات إلى تعطيل أجهزة العميل.

زتراهجيج 2.4

ضعف يذكر أن هذه الحزمة التي تبلغ سرعتها 2.4 غيغاهرتز قد تعرضت للانتقاد في بعض الأحيان. وهو يحتوي فقط على ثلاث قنوات غير متداخلة والعديد من التقنيات الأخرى بخلاف Wi-Fi التي يستخدمها، مما يؤدي إلى إنشاء استدلالات غير مرغوب فيها. تصر بعض المنظمات على تقديم الخدمة لها، ولذلك ما هو الاستنتاج المعقول؟ ومن المعلوم أن الحزمة 2.4 غيغاهرتز لا تقدم للمستخدمين النهائيين تجربة مرضية. والأسوأ من ذلك، عندما تحاول توفير الخدمة على تردد 2.4 جيجاهرتز، فإنك تؤثر على تقنيات أخرى بسرعة 2.4 جيجاهرتز. في المواقع وأجهزة الكمبيوتر، ما زال العديد من الأشخاص يتوقعون مثل تقنية Bluetooth. أن تعمل سماعات الرأس اللاسلكية لديهم عندما يقومون بإجراء مكالمة أو عندما تقوم بالمسهم الذكية بتشغيلها كالمعتاد. إذا كانت شبكة Wi-Fi الكثيفة تعمل على تردد 2.4 جيجاهرتز فأنت تؤثر على تلك الأجهزة التي لا تستخدم حتى شبكة Wi-Fi بسرعة 2.4 جيجاهرتز.

والأمر المؤكد هو أنه إذا كان يتعين عليك بالفعل توفير خدمة Wi-Fi بسرعة 2.4 جيجاهرتز، فمن الأفضل أن تقوم بذلك على معرف SSID منفصل (يمكنك تفريغه لأجهزة الإنترنت القديمة التي تصل تلقائيا لكل الأشياء أو تسميته "legacy"). وهذا يعني أن الأجهزة المزودة النطاق لا تتصل بتردد 2.4 جيجاهرتز، بل تتصل بها فقط الأجهزة أحادية النطاق بسرعة 2.4 جيجاهرتز.

توصي Cisco وتدعم إستخدام قنوات 40 ميجاهرتز في 2.4 جيجاهرتز.

زتره اغيغ 5

عملية نشر نموذجية للشبكة اللاسلكية عالية الكثافة. أستخدم كل القنوات المتوفرة حيثما كان ذلك ممكنا.

يختلف عدد القنوات باختلاف المجال التنظيمي. خذ بعين الإعتبار تأثير الرادار على الموقع المحدد، إستخدم قنوات DFS (بما فيها قنوات TDWR) حيثما أمكن.

يوصى بعرض قناة بسرعة 20 ميجاهرتز بشدة لجميع عمليات النشر عالية الكثافة.

يمكن إستخدام 40 ميجاهيرتز على نفس الأساس المستخدم في 2. 4 جيجاهيرتز، أي عندما تكون هناك حاجة ماسة إليه (وأين) فقط.

قم بتقييم الحاجة بالإضافة إلى الفوائد الحقيقية للقنوات بسرعة 40 ميغاهيرتز في بيئة معينة. تتطلب القنوات التي تبلغ سرعتها 40 ميجاهرتز نسبة أعلى من الإشارة إلى التشويش (SNR) لتحقيق أي تحسن ممكن في الخرج، وإذا لم يكن من الممكن زيادة النطاق الترددي العريض (SNR)، فإن القنوات التي تبلغ سرعتها 40 ميجاهرتز لا تخدم أي غرض مفيد. تعطي الشبكات عالية الكثافة الأولوية لسعة المعالجة المتوسطة لجميع المستخدمين على حساب سعة المعالجة الأعلى لأي مستخدم واحد. من الأفضل وضع المزيد من نقاط الوصول على قنوات بسرعة 20 ميجاهرتز بدلا من إستخدام نقاط وصول (AP) بسرعة 40 ميجاهرتز حيث يتم إستخدام القناة الثانوية فقط لإطارات البيانات وبالتالي

فإنها تستخدم بكفاءة أقل بكثير من وجود خليتين رايو مختلفتين، تعمل كل منهما بسرعة 20 ميجاهرتز (من حيث السعة الإجمالية، وليس من حيث سعة معالجة العميل الواحد).

أكثر التفاصيل أهمية هو أن تبقى نفس عرض القناة داخل مساحة معينة. وبالفعل إذا قمت بتكوين عرض قناة مختلف فسيميل العملاء إلى التشبث بنقاط الوصول (AP) ذات أكبر عرض قناة حتى وإن كانت هناك نقطة وصول أخرى أقرب عند أقوى قوة الإشارة.

6 جيجاهرتز

تدعم بعض المودمات 6 غيغاهرتز حتى الآن في كل دولة. علاوة على ذلك، تحتوي BIOS حتى الأجهزة على محول Wi-Fi قادر على العمل بتردد 6 جيجاهرتز ولكنها تتطلب تحديث البرامج الثابتة في الدولة المعنية. أكثر الطرق شيوعا التي يكتشف بها العملاء أجهزة الراديو بسرعة 6 جيجاهرتز الآن هي من خلال إعلان تقرير الجوار المنخفض (RNR)، وهذا يعلن عن وجود شبكات بسرعة 6 جيجاهرتز للعملاء باستخدام أحد أجهزة الراديو الأخرى AP. وهذا يعني أنه يجب ألا تعمل تردد 6 جيجاهيرتز لوحدها دون السلكي آخر على نقطة الوصول نفسها.

عند تكوين SSID ثنائي النطاق (بسرعة 5 جيجاهرتز و 6 جيجاهرتز)، سيتضمن الإعلان RNR الخاص ب SSID بسرعة 6 جيجاهرتز، مما يسمح للعميل بالعثور بسرعة 5 جيجاهرتز دون الاضطرار إلى مسح النطاق ضوئيا. SSID بسرعة 6 جيجاهرتز على

بينما تتمثل الطريقة الأخرى في تكوين SSID وهمي (و/أو مخفي) على تردد 2.4 جيجاهرتز، تتمثل النية هنا في الإعلان عن محول RNR بسرعة 6 جيجاهرتز باستخدام جهاز الراديو بسرعة 2.4 جيجاهرتز. ويعد هذا النهج مفيدا في الحالات التي يلزم فيها إضافة سعة تبلغ 6 جيجاهرتز دون إضافة أجهزة السلكية إلى البيئة بتردد 5 جيجاهرتز.

6 غيغاهيرتز يسمح باستخدام مساحات أكبر من عرض القناة، لكن ذلك يعتمد بشكل كبير على عدد القنوات المتاح في المجال التنظيمي. مع توفر 24 قناة تعمل بتردد 6 جيجاهرتز في أوروبا، فمن غير المعقول التفكير في قنوات 40 ميجاهرتز لتوفير الحد الأقصى للإنتاجية بشكل أفضل مقارنة مع 20 ميجاهرتز التي ربما تستخدمها على الأرجح في 5 جيجاهرتز. أما في الولايات المتحدة، والتي لديها ما يقرب من ضعف عدد القنوات، فإن استخدام 40 ميغاهرتز أمر بديهي، وحتى استخدام 80 ميغاهرتز أمر لا عقل فيه. يجب عدم استخدام الترددات الواسعة النطاق في الأحداث أو المواقع عالية الكثافة.

إن التنبيه مع عرض القناة الأكبر حجما بسرعة 6 جيجاهرتز هو أنه من غير الممكن دائما استخدام نفس عرض القناة في 5 جيجاهرتز، وهذا سيؤثر على سلوك التجوال على بعض أجهزة العميل. أكثر التفاصيل أهمية هو أن تبقى نفس عرض القناة داخل مساحة معينة. في الواقع، إذا قمت بتكوين عرض قناة مختلف، فسيميل العملاء إلى الالتصاق بنقاط الوصول (AP) ذات عرض القناة الأكبر حتى وإن كانت هناك نقطة وصول أخرى أقرب عند قوة إشارة أقوى، وينطبق هذا أيضا على التجوال بين مدى موجات 5 جيجاهيرتز و 6 جيجاهيرتز.

معدلات البيانات

إن معدل البيانات الذي يتفاوض عليه العميل مع نقطة وصول (AP) هو إلى حد كبير دالة على نسبة الإشارة إلى التشويش (SNR) لذلك الاتصال، والعكس صحيح أيضا، حيث تتطلب معدلات البيانات الأعلى معدل اتصال SNR أعلى. في الواقع، إن SNR وهو الذي يحدد أقصى سرعة ممكنة للارتباط - ولكن لماذا يكون هذا مهما عند تكوين معدلات البيانات؟ بل لأن بعض معدلات البيانات لها معنى خاص.

يمكن تكوين معدلات بيانات OFDM الكلاسيكية (802.11a) في واحد من ثلاثة إعدادات: معطل، ويجب أن يدعم كل من العميل و AP معدل قبل أن يمكن إستخدامه. معدلات OFDM هي (بالملليثانية): 6 و 9 و 12 و 18 و 24 و 36 و 48 و 54، وأ مدعوم وأ إلزامي.

معدل مدعوم - نقطة الوصول تستخدم المعدل

معدل إلزامي - تستخدم نقطة الوصول المعدل، وترسل حركة مرور الإدارة باستخدام هذا المعدل

معطل - ال ap لا يستعمل السعر، يجبر الزبون أن يستعمل معدل آخر

ملاحظة: ويشار إلى المعدلات الإلزامية أيضا بالمعدلات الأساسية

تكمن أهمية المعدل الإلزامي في أن جميع إطارات الإدارة يتم إرسالها باستخدام هذا المعدل، تم بالإضافة إلى إطارات البث والبث المتعدد. في حالة وجود معدلات إلزامية متعددة تم تكوينها، تستخدم إطارات الإدارة أقل معدل إلزامي تم تكوينه، وتستخدم محطات البث والبث المتعدد أحد المعدلات الإلزامية (تكون هذه النقطة قابلة للتكوين في ملف تعريف التردد اللاسلكي).

تتضمن إطارات الإدارة إشارات يجب أن يسمعها العميل لكي يتمكن من الاقتران بنقطة الوصول. وتذكر، تؤدي زيادة المعدل الإلزامي أيضا إلى زيادة متطلبات SNR لنقل البيانات، وهذا يعني عادة أن العميل الذي يحتاج إلى أن يكون أقرب إلى نقطة الوصول ليتمكن من فك ترميز المنارة وربطها. ومن ثم، فإننا نتلاعب أيضا بنطاق الاقتران الفعال لنقطة الوصول عن طريق التلاعب بمعدل البيانات الإلزامي، مما يرغم العملاء على الاقتراب من نقطة الوصول، أو نحو إتخاذ قرار توجيه محتمل. فالعملاء القريبون من نقطة الوصول يستخدمون معدلات بيانات أعلى، ومعدلات البيانات الأعلى تستخدم وقتا أقل للتهوية - والتأثير المقصود هو خلية أكثر فعالية. من المهم تذكر أن زيادة معدل البيانات لا تؤثر إلا على معدل نقل إطارات معينة، ولا تؤثر على انتشار التردد اللاسلكي للهوائي أو نطاق التداخل. لا تزال هناك حاجة لممارسات تصميم الترددات اللاسلكية الجيدة لتقليل تداخل وضوضاء القنوات المشتركة.

وعلى العكس من ذلك، فإن ترك معدلات أقل على أنها إلزامية يعني عادة إمكانية اقتران العملاء من مسافة أبعد بكثير، مما يفيد في سيناريوهات كثافة نقاط الوصول (AP) المنخفضة، ولكن مع إمكانية التسبب في الفوضى أثناء التجوال في سيناريوهات عالية الكثافة. إن كل من يحاول تحديد موقع نقطة وصول مخادعة تبث برامجها بسرعة 6 ميجابت

في الثانية يعلم أنه بإمكانك الكشف عن نقطة الوصول هذه بعيدا جدا عن موقعها الفعلي!

فيما يتعلق بموضوع البث والبث المتعدد، يتم في بعض الحالات تكوين معدل إلزامي ثنائي (أعلى) لزيادة معدل تسليم حركة مرور البث المتعدد. إذا كان هذا الإجراء حيث لا يتم التعرف على البث المتعدد أبدا أو إذا تم إعادة إرساله مطلقا في حالة فقد الإطارات. بما أن بعض العملاء قد يكون متأصلا في جميع الأنظمة اللاسلكية، فمن المحتم فقدان بعض إطارات البث المتعدد بغض النظر عن المعدل الذي تم تكوينه. الطريقة الأفضل للتسليم الموثوق به للبث المتعدد هي تقنيات التحويل من البث المتعدد إلى البث الأحادي التي تنقل البث المتعدد كتدفق للبث الأحادي، وهذا له فائدة من كل من معدلات البيانات الأعلى والتسليم الموثوق (المعروف).

يفضل إستخدام معدل إلزامي واحد فقط، وتعطيل جميع المعدلات التي تقل عن المعدل الإلزامي، وترك جميع المعدلات أعلى من المعدل الإلزامي كما هو مدعوم. يعتمد معدل الاستخدام المحدد على حالة الاستخدام، حيث أن المعدلات المنخفضة المذكورة آنفا تكون مفيدة في السيناريوهات الأقل كثافة والخارجية حيث تكون المسافات بين نقاط الوصول أكبر. بالنسبة لشبكات الأحداث والكثافة العالية، يجب تعطيل المعدلات المنخفضة.

إذا كنت غير متأكد من أين تبدأ؛ إستخدام معدل إلزامي بسرعة 12 ميجابت في الثانية لعمليات النشر منخفضة الكثافة و 24 ميجابت في الثانية لعمليات النشر عالية الكثافة. لقد أثبت العديد من الأحداث الكبيرة والمعالم وحتى عمليات نشر المكاتب عالية الكثافة في المؤسسات بأنها تعمل بشكل جيد بالثقة مع إعداد معدل إلزامي يبلغ 24 ميجابت في الثانية. يوصى بإجراء إختبار مناسب لحالات إستخدام معينة تتطلب معدلات أقل من 12 ميجابت في الثانية أو أعلى من 24 ميجابت في الثانية.

ملاحظة: من الأفضل ترك جميع معدلات 802.11n/ac/ax/be ممكنة (جميع المعدلات في قسم الإنتاجية العالية في واجهة المستخدم الرسومية (GUI) في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، إذا لم تكن هناك حاجة لتعطيل أي من هذه.

قوة الإرسال

تختلف توصيات طاقة الإرسال بناء على نوع النشر. هنا نميز بين الإنتشار الداخلي باستخدام هوائيات متعددة الإتجاهات، وتلك التي تستخدم هوائيات موجهة. يمكن أن يوجد العديد من الهوائيات في شبكة عامة كبيرة، على الرغم من أن هذين النوعين يغطيان عادة أنواعا مختلفة من المناطق.

بالنسبة لعمليات النشر متعددة الإتجاه، من الشائع إستخدام التحكم التلقائي في طاقة الإرسال (TPC) بحد أدنى تم تكوينه بشكل ثابت، وفي بعض الحالات أيضا حد أقصى تم تكوينه بشكل ثابت.

ملاحظة: تشير حدود TPC إلى طاقة إرسال الراديو وتستبعد اكتساب الهوائي. أحرص دائما على التأكد من أن مواصفات هوائي الربح مكونة بشكل صحيح لطراز الهوائي المستخدم، وهذا يتم تلقائيا في حالة الهوائيات الداخلية والهوائيات ذاتية التعريف.

مثال 1

الحد الأدنى لـ TPC: 5 ديسيبل لكل ميلي واط، الحد الأقصى لـ TPC: الحد الأقصى (30 ديسيبل لكل ميلي واط)

وهذا قد ينتج عنه خوارزمية TPC التي تحدد قوة الإرسال تلقائيا، ولكن لا يتم ذلك مطلقا بأقل من الحد الأدنى المكون وهو 5 ديسيبل لكل ميلي واط.

مثال 2

الحد الأدنى لـ TPC: 2dBm و الحد الأقصى لـ TPC: 11 ديسيبل لكل متر

وهذا من شأنه أن يؤدي إلى خوارزمية TPC التي تحدد قوة الإرسال تلقائيا، ولكنها تظل دائما بين 2dBm و 11dBm.

المنهج الجيد هو إنشاء عدة توصيفات للتردد اللاسلكي ذات حدود مختلفة، على سبيل المثال، الطاقة المنخفضة (2-5 ديسيبل لكل ميلي واط) والطاقة المتوسطة (5-11 ديسيبل لكل ميلي واط) والقوة العالية (11-17 ديسيبل لكل ميلي واط)، ثم تعيين نقاط وصول متعددة الاتجاهات لكل توصيف للتردد اللاسلكي حسب الحاجة. يمكن ضبط قيم كل ملف تعريف RF على حالة الاستخدام المخصصة ومنطقة التغطية. ويتيح ذلك لخوارزميات إدارة العلاقات مع الراديو العمل بشكل ديناميكي مع البقاء ضمن حدود محددة مسبقا.

يعتبر أسلوب إستخدام الهوائيات الاتجاهية متماثل للغاية والفارق الوحيد هو مستوى الدقة المطلوب. يجب تصميم موضع الهوائي الاتجاهي والتحقق منه خلال إستطلاع للتردد اللاسلكي قبل النشر، وتكون قيم تكوين الراديو المحددة هي عادة نتيجة لهذه العملية.

على سبيل المثال، إذا كان يلزم توفر هوائي تصحيح قابل للتركيب على السقف لتغطية مساحة معينة من إرتفاع يبلغ 26 قدما تقريبا (8 أمتار)، فيجب أن يحدد إستقصاء التردد اللاسلكي الحد الأدنى لقوة إرسال الإرسال (Tx) اللازمة لتحقيق هذه التغطية المقصودة (TPC) لملف تعريف الكمبيوتر المكتبية (وهذا يحدد الحد الأدنى لقيمة أجهزة التردد اللاسلكي). وبالمثل، من خلال إستطلاع التردد اللاسلكي نفسه، سنتفهم التداخل المحتمل المطلوب بين هذا الهوائي والهوائي التالي، أو حتى النقطة التي نريد عندها أن تنتهي التغطية - وهذا من شأنه أن يوفر أقصى قيمة من خلال كمبيوتر شخصي لملف تعريف التردد اللاسلكي.

TPC قيم بنفس إما الإتجاه للهوائيات اللاسلكي التردد تعريف ملفات تكوين يتم عادة
(عادة <= 3dBm) المحتملة القيم من ضيق نطاق وأ ،الأقصى والدنيا.

يفضل أن تضمن توصيفات التردد اللاسلكي اتساق التكوين، والا يوصى بالتكوين
الثابت لنقاط الوصول الفردية. من الممارسات الجيدة تسمية ملفات تخصيص التردد
اللاسلكي وفقا لمساحة التغطية ونوع الهوائي وحقيبة الاستخدام، على سبيل المثال
RF-Portal-Patch-Ceiling.

والكمية الصحيحة لقوة Tx هي عندما يتم تحقيق قيمة SNR المطلوبة بواسطة أضعف
عميل في منطقة التغطية المقصودة، وليس أكثر من ذلك. 30dBm هي قيمة مستهدفة
(أي في مكان مليء بالناس). في ظل ظروف العالم الحقيقي SNR لعميل رائعة.

CHD

اكتشاف ثقوب التغطية (CHD) عبارة عن خوارزمية منفصلة لتحديد ثقوب التغطية
(WLAN). ومن الصالحة. يتم تكوين CHD بشكل عام وكذلك لكل شبكة محلية السلكية
(المناطق التأثيرات المحتملة التي تنجم عن CHD زيادة طاقة Tx لتعويض ثقوب التغطية
التي يوجد بها عملاء يتم اكتشافهم باستمرار باستخدام إشارة ضعيفة، وهذا التأثير
يكون على مستوى الراديو ويؤثر على جميع شبكات WLAN، حتى عند إطلاقه بواسطة
شبكة محلية السلكية واحدة تم تكوينها لـ CHD.

عادة ما يتم تكوين الشبكات العامة الكبيرة على مستويات طاقة معينة باستخدام ملفات
تعريف التردد اللاسلكي، ويمكن أن يكون بعضها في مناطق مفتوحة مع وجود عملاء
(AP) يتنقلون إلى المناطق ومنها، ولا توجد حاجة إلى خوارزمية لضبط طاقة نقطة الوصول
إلى Tx بشكل ديناميكي كاستجابة لأحداث العميل هذه.

يجب تعطيل CHD بشكل عام للشبكات العامة الكبيرة.

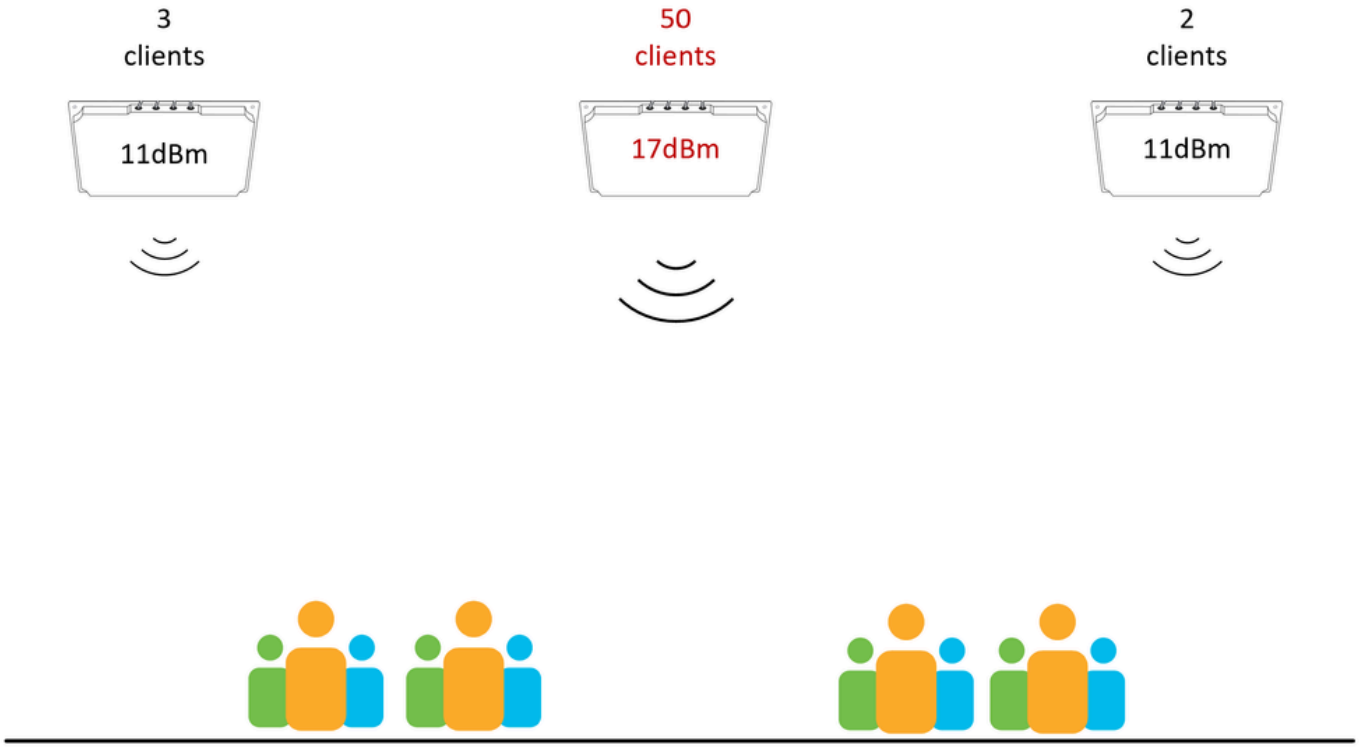
ميزان الطاقة

تفضل معظم أجهزة العميل إشارة مستلمة أعلى عند إختيار نقطة الوصول التي ترى
القارتان بها. يجب تجنب الحالات التي يتم فيها تكوين نقطة وصول بقوة إرسال Tx أعلى
بشكل ملحوظ مقارنة بنقاط الوصول الأخرى المحيطة. تجتذب نقاط الوصول التي تعمل
بطاقة إرسال (TX) أعلى عدد أكبر من العملاء، مما يؤدي إلى توزيع غير متساوٍ للأجهزة
العميلة بين نقاط الوصول (على سبيل المثال، يتم تحميل نقطة وصول (AP)/جهاز إرسال
السلكي واحد مع العملاء بينما يتم إستخدام نقاط الوصول المحيطة بشكل غير كامل). هذا
المتوقف شائع في عمليات النشر التي تتميز بتداخل تغطية كبير من هوائيات متعددة،
وفي الحالات التي تحتوي فيها نقطة وصول واحدة على هوائيات متعددة متصلة.

تتطلب هوائيات الاستاد مثل C9104 عناية خاصة عند إختيار طاقة Tx حيث تتداخل حزمة
الهوائي بحسب التصميم، رجاء الاطلاع على أدلة نشر الهوائي ذات الصلة للحصول على

مزيد من المعلومات حول ذلك.

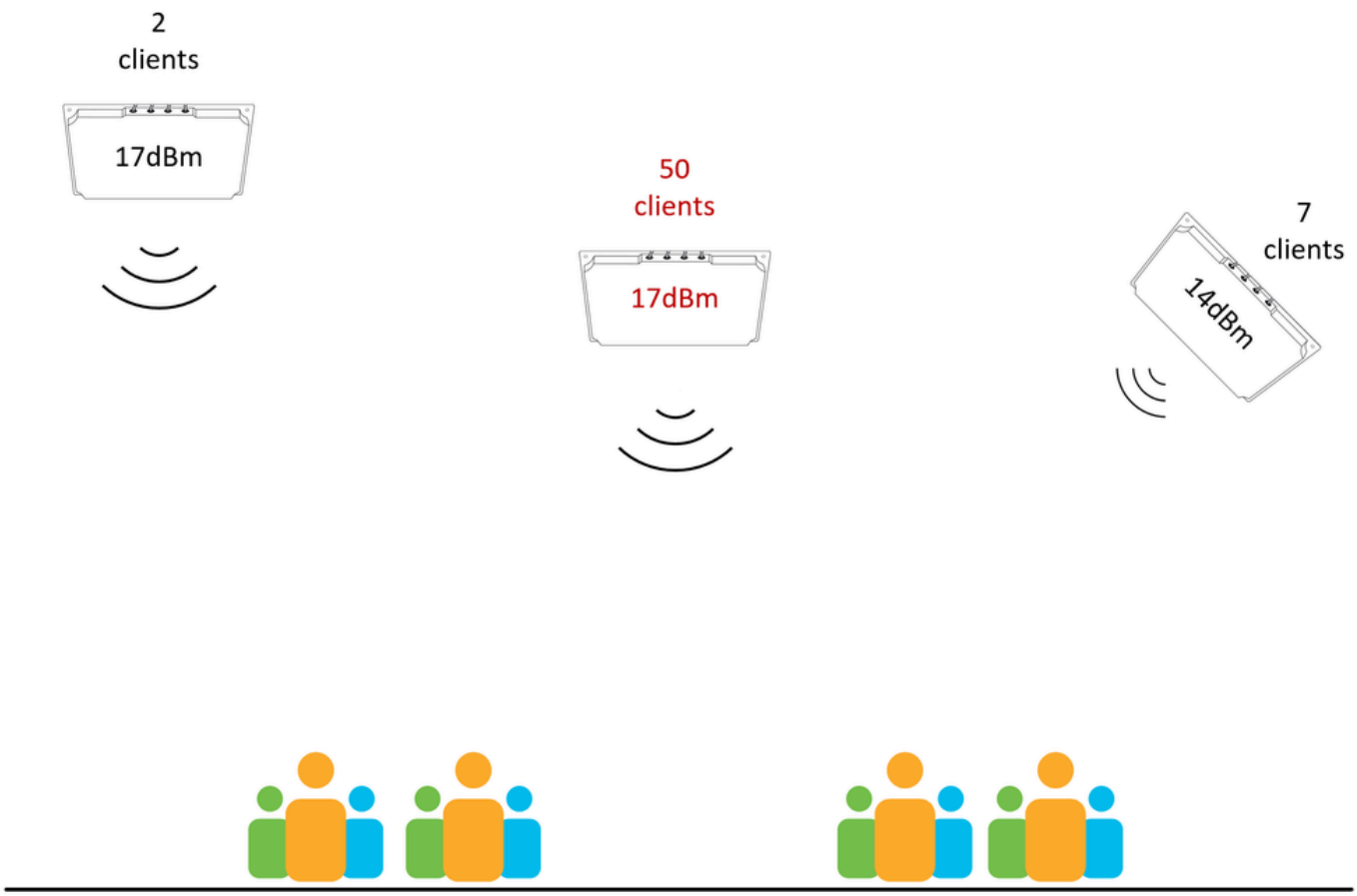
في الرسم بياني أسفله، يتم تكوين الهوائي الأوسط بطاقة إرسال (tx) أعلى من الهوائيات المحيطة. من المحتمل أن يؤدي هذا التكوين إلى أن يصبح العملاء "عالقين" في الهوائي الأوسط.



نقطة وصول ذات طاقة أكبر من نقاط الوصول (AP) المجاورة تجذب جميع العملاء حولها

يظهر الرسم البياني التالي وضعا أكثر تعقيدا، لا توجد كل الهوائيات بنفس الارتفاع، ولا تستخدم كل الهوائيات نفس الميل/الإتجاه. إن تحقيق توازن في إستهلاك الطاقة أكثر تعقيدا من مجرد تهيئة جميع أجهزة الراديو بنفس طاقة الإرسال (tx). وفي سيناريوهات من هذا القبيل، قد يلزم إجراء إستطلاع لموقع ما بعد النشر، وهذا يوفر نظرة على التغطية من وجهة نظر جهاز العميل (على الأرض). ويمكن بعد ذلك إستخدام بيانات الاستطلاع لموازنة التكوين للحصول على أفضل تغطية وتوزيع العميل.

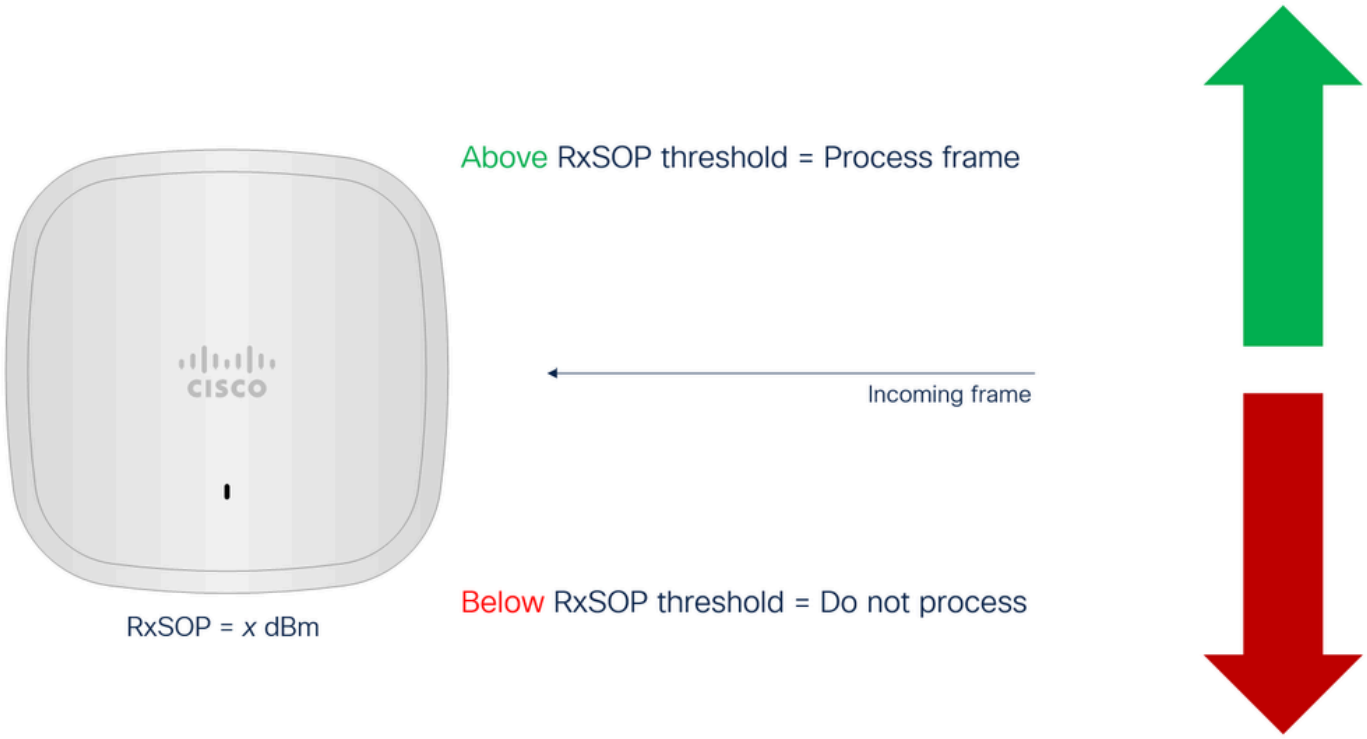
إن تصميم مواقع موحدة لنقاط الوصول (AP) لتجنب المواقف المعقدة كهذه هو أفضل طريقة لمنع سيناريوهات توليف التردد اللاسلكي (على الرغم من أنه لا يوجد خيار آخر في بعض الأحيان!).



نقطة وصول واحدة تجذب جميع العملاء على الرغم من تماثل طاقة Tx، ولكن الارتفاع والزوايا تلعب دورا

RxSOP

على النقيض من الآليات مثل معدلات طاقة أو بيانات Tx التي تؤثر على خصائص خلية الإرسال، يهدف RxSOP (بداية المتلقي لاكتشاف الحزمة) إلى التأثير على حجم خلية الاستقبال. يمكن إعتبار RxSOP في جوهره عتبة للضوضاء، من حيث إنه يحدد مستوى الإشارة المستلمة الذي لا تحاول نقطة الوصول تحته فك تشفير عمليات الإرسال. لا تقوم نقطة الوصول بمعالجة أي عمليات إرسال تصل بمستوى إشارة أقل من حد RxSOP الذي تم تكوينه ويتم التعامل معها بفعالية على أنها تشويش.



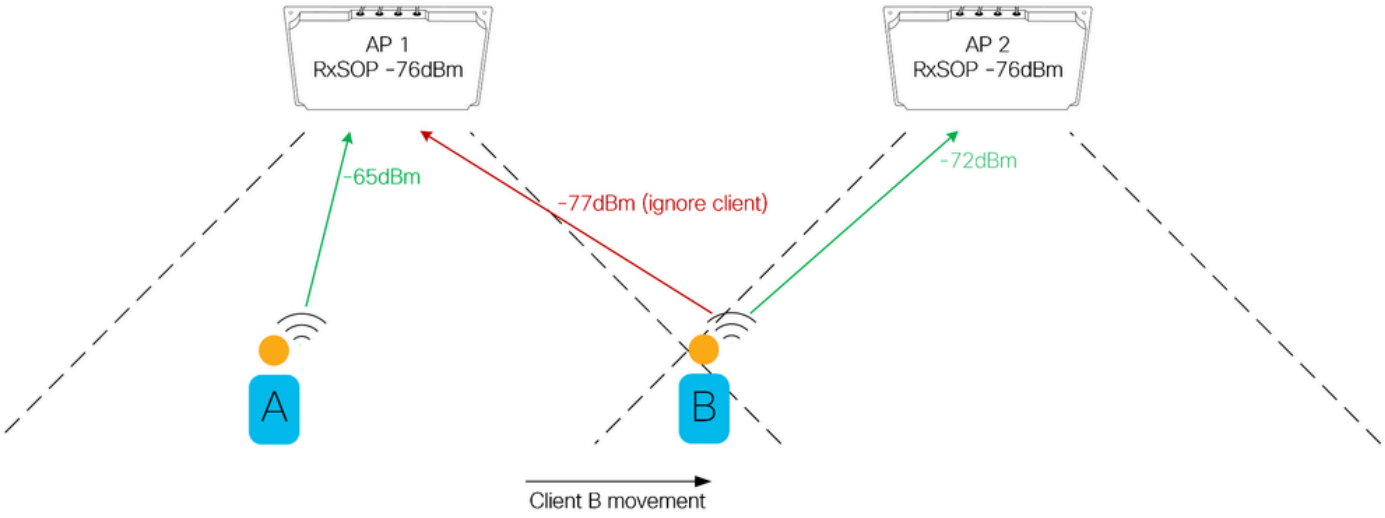
شرح مفهوم RxSOP

أهمية RxSop

يستخدم RxSOP إستخدامات متعددة. يمكن إستخدامه لتحسين قدرة نقاط الوصول (AP) على الإرسال في البيئات المزعجة والتحكم في توزيع الأجهزة العميلة بين الهوائيات وكذلك تحسين الأجهزة العميلة الأضعف واللاصقة.

في حالة البيئات المزعجة، تذكر أنه قبل إرسال إطار 802. 11 لمحطة الإرسال (نقطة الوصول في هذه الحالة) تحتاج أولا إلى تقييم مدى توفر الوسيط، فإن جزءا من هذه العملية هو الاستماع أولا إلى الإرسال الذي يحدث بالفعل. من الشائع في بيئات Wi-Fi الكثيفة أن يتعايش العديد من نقاط الوصول في مساحة محدودة نسبيا، وغالبا ما يتم ذلك باستخدام نفس القنوات. في مثل هذه البيئات المشغولة، يمكن لنقطة الوصول الإبلاغ عن إستخدام القناة من تلك التي تحيط APs (بما في ذلك الانعكاسات) وتأخير إرسالها الخاصة. من خلال تعيين العتبة المناسبة ل RxSOP، يمكن لنقطة الوصول تجاهل عمليات الإرسال الأضعف هذه (تقليل إستخدام القنوات المتصور) مما يؤدي إلى فرص إرسال أكثر تكرارا وتحسين الأداء. تعتبر البيئات التي تبلغ فيها نقاط الوصول عن إستخدام القنوات بشكل كبير (على سبيل المثال، > 10٪) دون أي تحميل عميل (على سبيل المثال، مكان فارغ) مرشحة جيدة لضبط RxSOP.

لتحسين العميل باستخدام RxSOP، ضع في الاعتبار هذا الرسم التخطيطي.



تجوال العميل المتأثر بالتrxsop

في هذا المثال، هناك نقطتان مختلفتان للتغطية موزعتان بمناطق تغطية محددة جيدا. ينتقل العميل B من منطقة التغطية ل AP1 إلى منطقة التغطية ل AP2. هناك نقطة وصيل عكسي تقوم AP2 عندها بسماع العميل بشكل أفضل من AP1، ولكن العميل لم ينتقل بعد إلى AP2. هذا مثال جيد على كيفية تمكين حد RxSOP من فرض حدود منطقة التغطية. إن ضمان اتصال العملاء دائما بأقرب نقطة وصول (AP) يحسن الأداء من خلال التخلص من إتصالات العملاء البعيدة و/أو الضعيفة التي تتم خدمتها بمعدلات بيانات أقل. يتطلب تكوين حدود RxSOP بهذه الطريقة فهما شاملا للمكان الذي تبدأ منه منطقة التغطية المتوقعة لكل نقطة وصول وتنتهي به.

مخاطر ال RxSOP.

يؤدي تعيين عتبة RxSOP بشكل مفرط إلى حدوث ثقوب في التغطية، حيث أن نقطة الوصول ال تقوم بفك ترميز عمليات الإرسال الصحيحة من أجهزة العميل الصالحة. وقد يؤدي هذا إلى عواقب سلبية على العميل لعدم إستجابة نقطة الوصول؛ وفي نهاية المطاف، إذا لم يسمع إرسال العميل فلا سبب للاستجابة. يجب ضبط حدود RxSOP بعناية، مع التأكد دائما من أن القيم التي تم تكوينها لا تستثني العملاء الصالحين داخل منطقة التغطية. لاحظ أنه من المحتمل ألا يستجيب بعض العملاء بشكل جيد للتجاهل بهذه الطريقة، كما أن إعدادات RxSOP العدوانية للغاية لا تمنح العميل فرصة التجوال بشكل طبيعي، مما يجبر العميل بشكل فعال على العثور على نقطة وصول أخرى. يفترض العميل الذي يمكنه فك ترميز منارة من نقطة وصول أنه قادر على الإرسال إلى نقطة الوصول تلك، وبالتالي، فإن نية توليف RxSOP هي مطابقة حجم خلية الاستقبال مع نطاق المنارة من نقطة الوصول. تذكر دائما أن جهاز العميل (الصحيح) لا يتمتع دائما بخط نظر مباشر إلى نقطة الوصول، وغالبا ما يتم تخفيف الإشارة من قبل المستخدمين الذين يواجهون بعيدا عن الهوائي أو يحملون أجهزتهم في أكياس أو جيوب.

تكوين RxSOP

يتم تكوين RxSOP لكل ملف تعريف التردد اللاسلكي.

لكل نطاق توجد حدود سابقة الإعداد (منخفضة/متوسطة/عالية) بقيم dBM معرفة مسبقا. تلك الإعدادات المسبقة مختلفة لكل نطاق (على سبيل المثال، "منخفض" له قيمة مختلفة في dBm بين 2.4 جيجاهيرتز و 5 جيجاهيرتز) التوصية هنا هي إستخدام قيم مخصصة دائما، حتى إذا كانت القيمة المقصودة هي أحد الإعدادات المسبقة المتوفرة، فإن ذلك يجعل التكوين أكثر قابلية للقراءة. يعجز الإعداد "تلقائي" RxSOP بشكل فعال، بمعنى أن نقطة الوصول تحاول فك ترميز أي حزمة يمكنها كالمعتاد.

Setting	Value
Auto	Not configured
Low	-80dBm
Medium	-78dBm
High	-76dBm
Custom	-60dBm to -85dBm

جدول إعدادات RxSop

ملاحظة: لا تتطلب تغييرات RxSOP إعادة ضبط الراديو ويمكن القيام بها أثناء التنقل.

تغيير حجم الشبكة

بشكل عام، فإن إستخدام الجهاز إلى أقصى حد من قدراته الموثقة هو فكرة سيئة. وتنقل صحائف البيانات الحقيقية، ولكن الأرقام المذكورة يمكن أن تكون في ظروف محددة من النشاط. يتم إختبار وحدات التحكم اللاسلكية واعتمادها لدعم عدد معين من العملاء ونقاط الوصول (AP) وسعة معالجة معينة، ولكن هذا لا يفترض أن العملاء يتجولون في كل ثانية، وأن يمكنك تكوين قوائم تحكم في الوصول (ACL) فريدة وطويلة للغاية لكل عميل أو تمكين جميع ميزات التطفل المتاحة. لذلك من المهم النظر في جميع الجوانب بعناية للتأكد من تطوير الشبكة خالل ساعات الذروة والحفاظ أيضا على هامش أمان للنمو المستقبلي.

عدد نقاط الوصول

إن إحدى المهام الأولى لنشر أي شبكة هي إعداد الميزانية وطلب الكمية المناسبة من المعدات، وأكبر عامل متغير هو عدد ونوعية نقاط الوصول والهوائيات. يجب أن تعتمد الحلول اللاسلكية دائما على تصميم ترددات الراديو، إلا أن ذلك (ولسوء الحظ) غالبا ما يكون هو الخطوة الثانية في دورة حياة المشروع. وفي حالة عمليات النشر البسيطة داخل المؤسسات، هناك العديد من تقنيات التقدير التي يمكنها، إلى مستوى معقول من

اليقين، التنبؤ بعدد نقاط الوصول التي يمكن أن تكون مطلوبة حتى قبل أن يظر المهندس المعماري اللاسلكي في مخططات الأرصفة. النماذج التنبؤية يمكن أيضا أن تكون مفيدة جدا في هذه الحالة.

أما بالنسبة للتركيبات الأكثر صعوبة مثل الشبكات العامة الصناعية أو الخارجية أو الشبكات العامة الكبيرة أو في أي مكان حيث تكون هناك حاجة إلى هوائيات خارجية، فإن تقنيات التقدير البسيطة تكون غير كافية في كثير من الأحيان. يلزم توفر مستوى معين من الخبرة مع المنشآت المماثلة السابقة لتقدير نوع وكمية المعدات اللازمة بشكل كاف. إن زيارة الموقع من قبل مهندس لاسلكي هي الحد الأدنى للتعرف على تصميم موقع أو منشأة معقدة.

يقدم هذا القسم إرشادات حول كيفية تحديد الحد الأدنى لعدد نقاط الوصول والهوائيات للعملية النشر المحددة. والكميات النهائية وموقع تركيب معينة ستحدد دائما من خلال عملية تحليل المتطلبات وتصميم الراديو.

يجب أن تستند قائمة مكونات الصنف الأولية إلى عاملين: نوعية الهوائيات وكمية الهوائيات.

نوع الهوائيات

لا توجد إختصارات هنا. يتم تحديد نوع الهوائي حسب المساحة التي يجب تغطيتها. بالإضافة إلى خيارات التركيب المتوفرة في تلك المنطقة. لا يمكن تحديد ذلك من دون فهم المساحة الفعلية، وهذا يعني أن زيارة الموقع مطلوبة من قبل شخص يعرف الهوائيات وأنماط تغطيتها.

كمية الهوائيات

يمكن اشتقاق كمية المعدات اللازمة من فهم المبلغ المتوقع للاتصالات بالعملاء.

الأجهزة لكل شخص

يمكن تحديد عدد المستخدمين من البشر من خلال عدد المقاعد في الموقع، أو عدد التذاكر المباعة، أو العدد المتوقع للزوار استنادا إلى إحصائيات تاريخية. يمكن لكل مستخدم بشري حمل أجهزة متعددة، ومن الشائع افتراض وجود أكثر من جهاز واحد لكل مستخدم، رغم أن قدرة المستخدم البشري على إستخدام أجهزة متعددة بنشاط في نفس الوقت أمر مشكوك فيه. يعتمد عدد الزوار الذين يتصلون بشكل نشط بالشبكة أيضا على نوع الحدث و/أو النشر.

مثال 1: ومن الطبيعي ان لا يحتوي المدرج المؤلف من 80،000 مقعد على 80،000 جهاز متصل، وهذه النسبة تكون عادة اقل بكثير. نسب المستخدمين المتصلين البالغة 20٪ ليست غير شائعة خلال الأحداث الرياضية، اذا يعني أنه بالنسبة للمثال الخاص بالمدرج الذي يضم 80000 مقعد، فإن العدد المتوقع للأجهزة المتصلة يمكن أن يكون 16000 (80000 × 20٪)

ابلطا مدختسملا ناك اذإ ،ةمدختسملا ةيآلا ىلع آلإلحاق ارقملا اذه دمتعي .(16000 = بتنفيذ بعض الإجراءات (مثل النقر فوق مدخل ويب) فإن الأقراص تكون أقل من عندما يكون PSK مثل البسيطة المصادقة الثنائية على الأجهزة. يمكن أن تكون عملية الانضمام الثنائية باستخدام OpenRoaming الذي يدمج التي تم تذكرها من حدث سابق، أو شيء أكثر تقدما مثل إستخدام OpenRoaming لتحديد نسب اتصال الأجهزة دون تفاعل مع المستخدم. يمكن للشبكات المستخدم بما يزيد عن 50٪، الأمر الذي يمكن أن يكون له تأثير كبير على تخطيط السعة.

مثال 2: من المنطقي أن نتوقع أن مؤتمر التقنية يتمتع بنسبة اتصال عالية بين المستخدمين. يقضي الحاضرون في المؤتمر وقتا أطول في الاتصال بالشبكة ويتوقعون أن يكونوا قادرين على الوصول إلى برنامج الإلكتروني وأداء المهام اليومية على مدار اليوم. ومن المرجح أيضا أن يتصل هذا النوع من المستخدمين بأكثر من جهاز واحد بالشبكة - على سبيل المثال، الكمبيوتر المحمول والهاتف الذكي. بالنسبة لمؤتمرات التكنولوجيا، يفترض أن 100٪ من الزوار يتصلون بالشبكة، وأن هذا الرقم يمكن أن يكون أقل اعتمادا على نوع المؤتمر.

في كل المثالين، يتمثل المفتاح في فهم العدد المتوقع للأجهزة المتصلة والوجود في أي وقت. وفي كلتا الحالتين يتم توصيل هذا الجهاز إلى شبكة عامة كبيرة. واحد لكل جهاز السلكي، ذلك، تعد الأجهزة العميلة (وليس المستخدمين البشر) هي التي تتصل بهذا الرادي. والأجهزة العميلة هي أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية التي يستخدمها الأشخاص.

الأجهزة لكل جهاز السلكي

تحتوي نقاط الوصول من Cisco على الحد الأقصى لعدد الأجهزة العميلة بمقدار 200 جهاز. نقاط الوصول Wi-Fi 6 و 400 جهاز لكل جهاز السلكي نقاط الوصول Wi-Fi 6E APs. ومع ذلك، فإن الحد الأقصى من عدد العملاء المتصلين لكل جهاز السلكي أقل من 50٪ من الحد الأقصى لعدد العملاء المدعوم بواسطة نقطة الوصول. كما يعتمد عدد الأجهزة اللاسلكية على نوع نقطة الوصول والأغراض التخطيطية، ويصى بإبقاء عدد العملاء لكل جهاز السلكي أقل من 50٪ من الحد الأقصى لسعة نقطة الوصول. تدرس أحدث المعايير 5 جيجاهرتز، وتستكشف القسم الموجود على الهواتف المحمولة، والهواتف الذكية بمزيد من التفاصيل.

في هذه المرحلة، من الأفضل تقسيم الشبكة إلى مناطق مميزة مع عدد الأجهزة المتوقع لكل منطقة. تذكر بأن هذا القسم يهدف إلى تقديم عدد أدنى من نقاط الوصول والهوائيات.

لكل عميل متوقع، قدم عدد العملاء المتوقع في منطقة تغطية منفصلة، مثال ثالث على سبيل المثال، خذ بالاعتبار عدد أجهزة الراديو التي تقدم لكل جهاز سلكي 75 ميغابت في الثانية (صحيح) وتستخدم في منطقة، المطبوعة.

Area	Expected Devices	Devices / Radio	Radios
Area 1	1000	75	14
Area 2	2000	75	27
Area 3	2500	75	34
Total			75

عدد أجهزة الراديو/العملاء المتوقع لكل منطقة

ويجب الآن دمج هذه الأرقام الأولية مع فهم أنواع نقاط الوصول والهوائيات المنتشرة في كل منطقة، وفي حالة إستخدام تردد أحادي أو مزدوج يبلغ 5 جيجاهرتز. تعتمد العمليات الحسابية بسرعة 6 جيجاهرتز نفس المنطق الذي يتبع سرعة 5 جيجاهرتز. 2. 4 غيغاهرتز لا تؤخذ بعين الإعتبار في هذا المثال.

لنفترض أن كل منطقة من المناطق الثلاثة تستخدم تركيب هوائي تصحيح 2566P وهوائي 5 جيجاهرتز - يستخدم هذا الاستاد 9104، بمزيج من السرعة الفردية والثنائية بسرعة السيناريو لأغراض التوضيح.

Area	Total Radios	2566P (Dual 5GHz)	2566P (Single 5GHz)	9104 (Dual 5GHz)
Area 1	14	0	6	4
Area 2	27	6	3	6
Area 3	34	7	0	10
Total Antennas		26	9	20
Total APs		13	9	0 (integrated)

الهوائيات لكل مساحة

تسرد كل منطقة نوع الهوائيات ونقاط الوصول (AP) المطلوبة. لاحظ أنه في حالة إستخدام هوائيين بسرعة 5 جيجاهرتز، تكون النسبة 2 هوائيات لنقطة وصول واحدة.

يوضح هذا القسم طريقة لتقدير عدد أولي من الهوائيات ونقاط الوصول (AP) اللازمة لعملية النشر. ويتطلب التقدير فهم المساحات الفعلية، وخيارات التركيب المحتملة في كل منطقة، ونوع الهوائيات التي ستستخدم في كل منطقة، وعدد الأجهزة العميلة المتوقعة.

وكل عملية نشر مختلفة وكثيرا ما تكون هناك حاجة إلى معدات إضافية لتغطية مجالات معينة أو تنطوي على تحديات، وهذا النوع من التقديرات لا يأخذ في الاعتبار سوى قدرة

العملاء (وليس التغطية) ويعمل على تحديد نطاق الاستثمار المطلوب. تخضع المواقع النهائية لوضع نقطة الوصول/الهوائي وإجمالي المعدات دائما لفهم شامل للتحقق من حالة الاستخدام وفي الموقع من قبل محترف السلكي متمرس.

سعة المعالجة المتوقعة

يمكن لكل قناة السلكية توفير سعة متاحة وتترجم عادة إلى الخرج. تتم مشاركة هذه السعة بين جميع الأجهزة المتصلة بالمذياع، مما يعني أن الأداء لكل مستخدم ينخفض مع إضافة المزيد من إتصالات المستخدم إلى الراديو. هذا التراجع في الأداء ليس خطيا ويعتمد أيضا على المزيج الدقيق من العملاء المتصلين.

تختلف إمكانات العميل بين الأجهزة حسب مجموعة شرائح العميل وعدد التدفقات المكانية التي يدعمها العميل. يرد في الجدول أدناه الحد الأقصى لمعدلات بيانات العملاء لكل عدد من التدفقات المكانية المدعومة. لاحظ أن معظم أجهزة العملاء تدعم مسارين مكانيين كحد أقصى.

Client Capability	20MHz channel Wi-Fi 5 (802.11ac)	20MHz channel Wi-Fi 6 (802.11ax)
1 Spatial Stream(s)	86.7Mbps	121.9Mbps
2 Spatial Stream(s)	173.3Mbps	243.8Mbps
3 Spatial Stream(s)	288.9Mbps	365.6Mbps
4 Spatial Stream(s)	346.7Mbps	487.5Mbps

الحد الأقصى المتوقع من سعة المعالجة الحقيقية لكل نوع عميل

المعدلات المدرجة هي المعدلات القصوى النظرية لمعدل نقل البيانات متعدد الطبقات (MCS) (نظام التعديل والترميز) المستمدة من معيار 802.11 وتفترض نسبة الإشارة إلى التشويش (SNR) >30 ديسيبل لكل ميلليواط. يتمثل الهدف الرئيسي للتصميم الخاص بالشبكات اللاسلكية التي تتسم بأداء فائق في تحقيق هذا المستوى من الاتصال المتبادل بين الشبكات اللاسلكية (SNR) لجميع العملاء في جميع المواقع، ولكن نادرا ما يحدث ذلك. تتسم الشبكات اللاسلكية بطبيعتها الديناميكية وتستخدم ترددات غير مرخصة، كما أن للعديد من التدخلات غير الخاضعة للتحكم تأثير على بروتوكول SNR الخاص بالعميل، بالإضافة إلى قدرات العميل.

وحتى في الحالات التي يتم فيها تحقيق المستوى المطلوب من البروتوكول الآمن (SNR)، فإن المعدلات المدرجة سابقا لا تراعي النفقات العامة للبروتوكول، وبالتالي، لا ترسم خطوطا مباشرة إلى الإنتاج العالمي الحقيقي (مقاس بأدوات إختبار السرعة المختلفة). دائما ما يكون العالم الحقيقي أقل من معدل MCS.

بالنسبة لجميع الشبكات اللاسلكية (بما في ذلك الشبكات العامة الكبيرة)، يعتمد

إخراج بيانات العميل دائما على:

- إمكانات العميل.
- نسبة الإشارة إلى الضوضاء للعميل في تلك النقطة الزمنية المحددة.
- عدد العملاء الآخرين المتصلين في تلك النقطة المحددة في الوقت المناسب.
- قدرات عملاء آخرين في تلك النقطة المحددة من الوقت.
- نشاط زبائن آخرين في تلك اللحظة باذات.
- تداخل عند تلك النقطة الزمنية المحددة.

وبناء على أختلاف هذه العوامل، لا يمكن ضمان حد أدنى لكل عميل في جميع أنحاء الشبكات اللاسلكية، بغض النظر عن مورد المعدات.

دليل الاختبار Wi-Fi: للحصول على مزيد من المعلومات، يرجى الرجوع إلى التحقق من خرج والمرافقة.

النظام الأساسي WLC

إختيار منصة WLC الخاصة بك يمكن أن يبدو سهلا. إن أول ما تفكر فيه هو النظر إلى العدد المقدر لنقاط الوصول وعدد العملاء الذين تسعى إلى إدارتهم. تحتوي ورقة البيانات الخاصة بكل نظام WLC على الحد الأقصى للكائنات المدعومة على النظام الأساسي: قوائم التحكم في الوصول وعدد العملاء والمواقع وما إلى ذلك. وهذه هي الاعداد القصوى الرحفية في 9800-80 التي تدعم 6000 APs فقط، على سبيل المثال. ولكن هل من الحكمة ان تصبوا إلى القصى حد في كل مكان؟

تم إختبار وحدات التحكم اللاسلكية من Cisco لتكون قادرة على الوصول إلى هذه المستويات القصوى، ولكن لا يمكنها بالضرورة الوصول إلى جميع المستويات القصوى المدعومة في جميع الظروف في نفس الوقت. عند أخذ مثال الخرج، حيث يمكن أن يصل عدد نقل البيانات من 9800 إلى 80 جيجابت في الثانية من إعادة توجيه بيانات العميل، ولكن هذا في الحالة التي تبلغ فيها كل حزمة عميل الحد الأقصى والحجم الأمثل من 1500 بايت. إذا قمت بفضل المزيج المثالي من أحجام الحزم، يكون الحد الأقصى للإنتاجية الفعلي أقل. وبالمثل، سيتم تقليل الخرج أكثر، ونفس الشيء بالنسبة لإمكانية تمكين تشفير DTLS، لأن هذا يتطلب 40 جيجابت في الثانية من أصل 80 جيجابت في الثانية التي تتوقع توفر أكثر من نوع من التطبيق. إنه لمن المألوف أن تتوقع أن تتمكن من الحصول على شبكة كبيرة مع تمكين العديد من المميزات. وانظر أن هذه الميزات المستخدمة ونوع نشاط الشبكة، فإن الطريقة التي تختلف بشكل كبير باختلاف المميزات المستخدمة باستخدام datapath هي قياس إستخدام وحدة المعالجة التي تسعة على فكرة فعلية عن السعة الوحيدة للحصول على الأمر. التركيز على قياس الحمل، وهي نسبة مئوية من الحد الأقصى لسعة المعالجة التي يمكن لوحدة التحكم توجيهها.

```
WLC#show platform hardware chassis active qfp datapath utilization summary

  CPP 0:                5 secs         1 min         5 min        60 min
```

Input:	Total (pps)	9	5	5	8
	(bps)	17776	7632	9024	10568
Output:	Total (pps)	5	3	3	6
	(bps)	11136	11640	11440	41448
Processing: Load (pct)		0	0	0	0

WLC#

يال بشكل مثالي (APs) لوصول قطة و6000 إستيعاب 80-9800 زارطلا نكمي ،ةلثامم ةقيرطبو ال راطم وأ بعلم لثم ةعاد ةيلعلا ةطشنألا نم لالخ نم .غير أن 6000 قطة و لوصول في مكان عام مثل ملعب أو بطاملا ،طيحملا لاتصالا ةيقيبطتلا ةعارم ةقدار تجاوز العميل او .مظنم نم اطاشن تعتبر ةيزكرملا ةجلاعملا ةدحو إستخدام في زيادة إستجابة ةرياكلا ةماعلا تاكبشلا ىلعأب مستوى في ةيزكرملا (CPU) ةيكلسلالا ةيلحملا ةكبشلا في دحاو مكحت رصنع ىلع .(WLC) اذإ تمق إضافة تازيم ةيتحرك ةرم لك في لاسرإ متي (طيسبلا تاكبشلا ةرادإ لوكوتورب) SNMP و ةبقارملا ءالمعلا ،فيكمي نأ يصبح لحملا بسرعة كبيرا جدا. أحد لاوصافتا ةيسيئرلا لأي ءاهيف ،ءالمعلا مضب ةقلعتملا ثادحألا نم ريثك ربكأ ددع كانه نأ وه حدث كبير وأ ريبك عام مكان ةدايز في ببستي ،مما ىلإ فيرق لمعلا أثناء تنقل ألاشخاص وإشراكهم/عزلهم بشكل دئام. ةيزكرملا (CPU) ةجلاعملا ةدحو ىلع طغضلا ومستوى مكحتلا.

لقد أظهرت عمليات النشر المتعددة أن زوج (HA) واحد من وحدات التحكم اللاسلكية التي تستخدم باستات الرئيسية في عمليات النشر الكبيرة مع عمليات التعامل مع 9800 إلى 80 يمكنها التواجد من أكثر وأ 1000 عن يزيد ما .ولصو ةطقن 1000 عن يزيد ما .ومن الشائع أيضا توزيع نقاط الوصول على زوجين أو أكثر من المتاحة لأجهزة التحكم للأحداث الحرجة حيث يكون وقت التشغيل والتوفر هما أولوياتهما الرئيسية. عندما يتم توزيع الشبكات الكبيرة عبر شبكات WLC متعددة، يكون هناك حاجة إلى تنسيق إضافي للتجوال بين وحدات التحكم، يجب مراعاة التجوال العملاء بعناية في الأماكن ذات الكثافة العالية مثل حوض الاستاد.

.هذه المستند في الموقع علامة قسم أيضا راجع

الإتاحة العالية ل WLC

وهذا يوفر تكرار الأجهزة، (HA SSO) عبر التوفر عالي الحالة مع توزيع الحمولات باستخدام زوج يوصى .جمالبر ضد فشل الحماية أيضا يوفر ولكنه .HA SSO، يكون عطل البرنامج على مستخدمين النهائيين بين تتولى عنصر التحكم في الشبكة جهاز واحد شفاف للمستخدم .ومن المزايا الأخرى لزوج الخدمة الثانوي المهمة بسلاسة تمامًا. الخدمة لأثناء (ISSU) HA SSO الترقيات المستمرة التي توفرها ميزة ترقية البرامج.

إذا كانت الشبكة كبيرة بالقدر الكافي، فينصح أيضا باستخدام وحدة تحكم إضافية (N+1). ويمكن أن تخدم عدة أغراض لا يمكن أن يحققها مكتب تنسيق الشؤون الإنسانية.

يمكنك إختبار إصدار برنامج جديد على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) هيإ طقف إختبار قبل ترقية وجوز الإنتاج) تحريل بعض نقاط الوصول للاختبار و(ةدرانلا تاحالا ضعب .(ةكبشلا مجح نم نيعم مسق رابتخالا في WLCs الك ىلع رثؤت نأ نكمي ةكبشلا نم ءزجلا ىلإ لوصولا طاقن نيوكت ةداعإ وهنا يسمح N+1 وجز HA (دنعما يتم نسخ المشكلة نسخا متمائلا إلى وضع الاستعداد) ىلإ لوصولا طاقن نم ديزملا ةفاضإ كنكمي ثيح نشط-نشط ويراني سيف WLC نمآ دوجو .بشكل تدريجي. كما يمكن أن يخدم أيضا كجهاز تحكم في الإمداد لتكوين نقاط وصول جديدة (APs).

تتسم وحدات التحكم في الوصول إلى النقل (9800-CL) بقابليتها للتوسع والقوة (من 2 إلى 4 أجهزة في الثانية لصورة SR-IOV) والتي تميل إلى تقييدها بعدد صغير من نقاط الوصول في بيئات FlexConnect المحلية (وربما عدد أكبر بكثير في بيئات التحويل المركزي). ومع ذلك، يمكن أن تكون مفيدة كأجهزة N+1 عندما تحتاج إلى وحدات تحكم إضافية وأن تستكشف مشكلة وإصلاحها.

الأنظمة الخارجية

تركز هذه المستندات بشكل رئيسي على المكونات اللاسلكية لشبكات الأحداث في حين أن هناك العديد من الأنظمة الداعمة التي تتطلب الإهتمام بها خلال مرحلة الكبيرة، إلا أنه توجد أيضا بعض هذه الأنظمة التي، ستتم مناقشة التطوير والتصميم.

شبكة أساسية

تم نشر الشبكات اللاسلكية الكبيرة في وضع التحويل المركزي مع الشبكات العادية ARP و MAC عناوين إدخالات من جدا كبير عدد دعم هذا يعني ما .الفرعية الكبيرة. ومن المهم للغاية أن توفر الأنظمة المتواجدة البنية الأساسية اللاسلكية المتواجدة. ومن المهم أن تتوفر الأنظمة المتواجدة البنية الأساسية اللاسلكية المتواجدة. ومن المهم للغاية أن تو

حد DHCP على و DNS تامدخ بلطتت ال .ةديجلا ءالمعلا ةبرجت نامضل نايسايأ نامظنلا اذه
قلعتي فيما إلى راتبعإ يف ،لب تحاتجأ اضيأ إلى إراتبعإ فيما يتعلق
سواء القياس المناسب لمعالجة الحمل فحسب، لب تحتاج أيضا إلى إعتبار فيما يتعلق
بالتنسيب داخل الشبكة. تضمن الأنظمة سريعة الاستجابة، الموضوعة في نفس موقع
عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، أفضل تجربة وتتجنب الأوقات
.الطويلة لضم العملاء

المصادقة والتفويض والمحاسبة (AAA)/بوابة الويب

ديجل لكشب ومحكم بشكل جيد، إذا فإن إختيار نظام مناس

التوصية على نقاط الوصول إلى الوضع المحلي وحركة المرور المحولة مركزيا. في حالة إستخدام FlexConnect مع التحويل المحلي، التي تم دعم وضع أكثر من 100 (وأ بعد 300 نقطة وصول (AP) في الشبكة الفرعية نفسها حيث أنها تعاني من الكثير من 17.9) VLAN عمليات الإرسال عبر البث. يتطلب FlexConnect نقاط وصول (APs) لخدمة شبكة الشبكات الفرعية الكبيرة نفسها لدعم التجوال السلس وبالتالي التي ينصح بدعم الشبكات الفرعية الكبيرة في هذا السيناريو.

- احتفظ بـ DHCP في وضع التوصيل على وحدة التحكم اللاسلكية باستخدام وظيفة DHCP لترحيل DHCP التي تتم معالجتها بواسطة بوابة الطبقة 3 للشبكة الفرعية. وهذا يسمح بأقصى قدر من الكفاءة والبساطة. الفكرة هي عدم مشاركة وحدة التحكم اللاسلكية في عملية DHCP على الإطلاق.
- .أستخدم DHCP المطلوب على أي شبكة WLAN عامة، بغض النظر عن طريقة المصادقة. على الرغم من أن هذا قد يؤدي إلى تشغيل نسبة مئوية صغيرة من اقترانات العملاء الفاشلة، إلا أنه قد يمنع حدوث مشاكل أمان كبيرة إما من قبل العملاء الذين يحاولون تعيين عناوين IP الثابتة لأنفسهم أو من قبل العملاء الذين يسيئون التصرف ويحاولون إعادة إستخدام عنوان IP سابق دون إذن.

تشغيل الشبكة

التهيئة الصحيحة

من المغري تمكين الكثير من الخيارات للاستفادة من أحدث ميزات شبكة Wi-Fi الحديثة. على الرغم من ذلك، تعمل بعض الميزات بشكل رائع في البيئات الصغيرة ولكن لها تأثير كبير في البيئات الكبيرة والكثيفة. بالمثل، يمكن أن تواجه بعض الخصائص مشاكل في التوافق. على الرغم من أن أجهزة Cisco تحترم جميع المعايير وتوفر التوافق مع مجموعة كبيرة متنوعة من العملاء الذين تم إختبارهم، فإن العالم مليء بأجهزة عميلة فريدة تحتوي أحيانا على إصدارات برامج تشغيل تحتوي على أخطاء أو عدم توافق مع ميزات معينة.

بناء على مستوى التحكم الذي تمارسه على العملاء، يجب أن تكون محافظا. على سبيل المثال، إذا قمت بنشر شبكة Wi-Fi للتجميع السنوي الكبير لشركتك، فأنت تعلم أن معظم العملاء هم أجهزة خاصة بالشركة ويمكنك تخطيط مجموعة الميزات للتمكين وفقا لذلك. ومن ناحية أخرى، إذا كنت تشغل شبكة Wi-Fi بالمطار، فإن مستوى رضاء ضيوفك يرتبط مباشرة بقدرتهم على الاتصال بشبكتك، ولا تملك أي تحكم على الإطلاق في الأجهزة العميلة التي يمكن للناس إستخدامها.

SSIDs

كم معرف SSID؟

وكانت التوصية دائما هي إستخدام أقل عدد ممكن من عناوين SSID. ويتفاقم هذه في الشبكات عالية الكثافة حيث يكون احتمال وجود نقاط وصول متعددة على نفس القناة

نأب رقي امم ،SSIDs نم ريثكلا رشنلا تايلمع نم ديعلا مدختسا ام ةداعو .اتقرينوم ضم
ءاجرإ كيلع بجي .لقأ لكشب امهادختسإ نكمي ال نأ هنم عيلن ،نكلو SSIDs نم ديعلا امهيد
SSIDs مي قسو SSID نيب ةهباشتلا هجوأو هفلم SSID لكل ةيجاتو ةيفنت ةسارد
.دحاو ىلإ ةددعتملا.

.امهادختساو SSID/ةيامحلا عاونأ ضعب ىلع فرعتن دعنا

WPA2/3 يصخش

SSID حاتفملا كرتشملا قبسم ةئيهبعش ةئاهلا ببسب ةطاسبلا .هيمنكي إما طاعة
.راوزلل ةقيرطب هلصوي تاراشلا ىلع وأ روقلا ىلع وأ تامالعلا ىلع وأ تاحفلا يف ناكم ام ىلع
SSID فرعم ىلع ةبسنلاب ىتح كرتشم SSID حاتفم لضفي نايحألا ضعبو يف
.(ةطيرشلا نوكي نأ هنكمي يذلا) فيضلا
DHCP تجمع كالهتسإ نم هنكمي ال .لاصتلل ةيطبعتلا ةدوصقملا ببسب DHCP
.تجمع IP نوانع كالهتسإ ىلع ةردق ريغ اهنإف ،كلذل ،ةكبشلاب لصتت ال ةزهجألا ةرامل

ارظنلا رورم ةكرح ريفشت ةلوهسب نكمي هنأ ةيصوصخلا WPA2 PSK الو رفوي
ىلع سكعلا نم كلذ ،فإ WPA3 SAE رفوي .بلط ىلع لدعي ال نأ صخش لكل حاتفملا سفن
،ةيصوصخلا ىتحو ،كاذإ صخش لكل حاتفملا يسيئرلا ،فإهنم رييغ نكمملا شاقتسا
.نيرخآلا ءالمعلا لبق نم مدختسملا ريفشتلا حاتفم

ةزهجأو ةيكذلا فاوهلا نم ديعلا نأ امك ،نامألل لضفألا رايخلا SAE WPA3 ربتعي
ةزهجألا أو "ءاشيألا لك" ةيكذلا ةزهجألا هذه ،ءاظحإ يف ةلكشم ببسب ،نكل .قافولا
.ةنمآلا ريغ ةكرتشملا ةكبشلا ىلع ةيلمعلا ريفشت حاتفم ىلع لوصحلا وأ ةكبشلا
.ةيلمعلا ريفشت ةيمزراوخ ىلع ءاضقلا وأ ةيلمعلا ةرادإ ةمظنأ

SSID WPA2 PSK-WPA3 SAE لقنتا عضو يف ريفكتلا يف بعصتلا نم ريثكلا دجوي
.ةيفاضإ ةيامحو ةرفشم ةقيرط ىلإ ةجاحلا ىلإ ريشي يذلا GCMP256 ريفشت ىلإ
.ةيكلسلا ةكبشلا ىلع ةيلمعلا ريفشت ةيمزراوخ ىلع ءاضقلا وأ ةيلمعلا ةرادإ ةمظنأ
.ةيكلسلا ةكبشلا ىلع ةيلمعلا ريفشت ةيمزراوخ ىلع ءاضقلا وأ ةيلمعلا ةرادإ ةمظنأ

WPA3 SSID ىلع (SAE-EXT-FT و SAE-EXT) نيصن نيكوت Wi-Fi 7 بلطتي

توفر الحد الأقصى من التوافق.

بالنسبة لمعيار 802.1X، يوصى بـ SSID ولضع الانتقال نظرًا لعدم ملاحظة مشكلة مع إصدارات Android 8 وأ Apple IOS التوافق مع الأجهزة الحديثة) تم الإبلاغ عن المشكلة مع أجهزة قديمة). تتيح الإصدارات IOS XE 17.12 والإصدارات الأحدث الحصول على SSID مؤسسة الأمن، بين جيجاهرتز 6 وواحدة حيث يتم استخدام WPA3 فقط والإعلان عنه على سرعة الاتصال. ننصح بتمكين WPA3 على SSIDs التي توفر WPA2 كخيار على مدى موجات 5 جيجاهرتز. يتم تمكين للمؤسسة في أقرب وقت ممكن.

يمكن إستخدام WPA Enterprise SSIDs للمستخدمين الرئيسيين الذين توجد لهم قاعدة بيانات لموفر الهوية تسمح بإرجاع معلمات AAA (مثل شبكات VLAN أو مواقع التحكم في الوصول) وأو SSID التعليم. يمكن أن تتضمن هذه الأنواع من SSID الضيف (من خلال السماح للزوار بالاتصال لفترة قصيرة بسهولة دون إدخال أي بيانات اعتماد) مع أمان SSID الخاص بالشركة. فهي تعمل على تقليل عبء الدعم على مسؤول الشبكة إلى الحد الأدنى من خلال السماح للزوار بالاتصال بشبكة الإنترنت بشكل نموذجي مع معيار 802. 1X، OpenRoaming SSID، شركاء الخدمة الذين يقدمون الوصول إلى الشبكة بأي شيء للانضمام إلى القيام بأي شيء للانضمام إلى Edroam أو OpenRoaming SSID، يضطر العملاء إلى تعريف عدم وجود اتصال بالإنترنت (يمكن توفيره بسهولة من خلال تطبيق الجدران النارية أو أن يكون لديهم ملف تعريف على هواتفهم).

Wi-Fi 7 (مع أكثر العملاء صرامة) تقدم تشفير GCMP256 لتقديم نقطة الوصول دعم قد يتطلب برامج تشغيل حديثة. IOS-XE 17.18.3 الذي يتطلب أيضا

SSIDs للضيف

يكون SSID للضيف مفتوحًا. يمكنك إضافة بوابة ويب (أو الوصول إلى الشبكة) بما في ذلك البوابات المخصصة المدارة للمصادقة المفتوحة: المصادقة الخارجية (وقوفًا للسهولة المطلوبة أو المتطلبات المحلية) بأشكالها المختلفة: عند استخدام بوابة ويب، ولكن ليس المفهوم كما هو. المركزية للويب، والمحلية أو الخارجية أو المحلية. يمكن أن تصبح قابلية التوسع مشكلة في البيئات الكبيرة بسرعة. راجع قسم الضيف، يمكن أن تصبح قابلية التوسع مشكلة في البيئات الكبيرة بسرعة. راجع قسم تكوين قابلية التوسعة للحصول على مزيد من المعلومات حول هذا الأمر.

تتطلب العمليات التي تتم بسرعة 6 جيجاهرتز إستخدام معرف SSID المحسن الخاص بالاتصال بالضيف Enhanced Open بدلاً من الفتح المفتوح. وما زال هذا يسمح لأي شخص بالاتصال بالضيف Enhanced Open دون ذلك، بتشفير الخصوصية (خصوصية أفضل من WPA2-PSK even!) ولكنه يوفر الخصوصية الذكية وتوفير أي مفتاح أو بيانات اعتماد عند الاتصال في SSID. ويدعم الآن بائعو الهواتف وأنظمة التشغيل الرئيسية تقنية Enhanced Open ولكن الدعم ال ينتشر على نطاق واسع حتى الآن في قاعدة العملاء الالسلكيين. يمنع وضع الانتقال المفتوح المحسن عمليات SSID التشغيل الرئيسية طريقة المناسبة هي على الأرجح تشغيل SSID مفتوح محسن على مدى موجات 6 جيجاهرتز فقط، مع الإبقاء على SSID المفتوح القديم للتوافق. يجب عليك إعطاء SSIDs اسما مختلفا لأنها تبث على مدى موجات 5 جيجاهرتز بالكامل على SSID الضيف ولكنه يضيف SSID في قائمة فحص العميل وهذا يضيف طرق تأمين مختلفة.

في الأحداث والأماكن الكبيرة، يوصى عادة بتكوين PSK على SSID الضيف بدلاً من تركه

عاش إنإلى يؤدي ذلك ولكن أفضل سيكون المفتوح الاتصال عن تحسين وضع مفتوحا تمامًا) لجعل هذا ممكنًا. وعلى الرغم من أن SSIDs وبجب إثبات توافق العميل بشكل مكثف) إثنين من SSIDs على PSK قاعدة بطاقة عملية الانضمام إلى شبكة الإنترنت أكثر تعقيدًا) يجب عليك تجنب العملاء غير الأشارات الأخاص وأ الإعلان عنها بطريقة ما، إلا أنها تذكرهم أي الرسميين الذين يتصلون بالشبكة لاقائيا دون أن يكون لدى المستخدم النهائي القدرة على استخدام الشبكة. كما يقوم المزيد والمزيد من باعة أنظمة التشغيل المتنقلة بإلغاء تحديد أولويات الشبكات المفتوحة، وتقديم تحذير أمني. في الحالات الأخرى، يمكنك طلب اتصال عدد أقصى من المرات، وبالتالي فإن الفتح هو الاختيار الأفضل.

إستنتاج حول عدد SSIDs

ال يمكن أن تكون هناك إجابة مرضية على السؤال الخاص بعدد SSIDs التي يتعين عليك طاقم SSIDs وعدد SSIDs، وعدد المآذن التي يمكن لمعدل البيانات المتأثر على الحد الأدنى الالتزام بها. يعتمد التأثير على الوصول التي تبث على نفس القناة. في أحد أحداث Cisco الكبيرة، أستخدمت البنية الأساسية اللاسلكية 5 SSIDs: WPA2 PSK و WPA 3 SAE SSID للأمان 6 و 802.1X و Wi-Fi من تطبيق الحدث للترحيب بأمان بأي شخص يشكل Edroam SSID للمؤسسة التسهيل الوصول للحاضرين المثقفين و OpenRoaming SSID للتغطية الجيجاهيرتز. وقد كان ذلك أكثر مما ينبغي SSID منفصلة للموظفين ووصول إلى شبكة الإدارة. بالفعل، ولكن التأثير ظل معقولا بفضل العدد الكبير من القنوات المتاحة، واستخدام الهوائيات الإتجاه للحد من تداخل القنوات بقدر الإمكان.

مفاهيم SSID القديمة مقابل SSID الرئيسية

تم الإعلان عن "قديم" لمنصف SSID بمعرفة جيجاهرتز 2.4 خدمة تقييد بحت، نصف ولفترة معينة، وفير 2.4 جيجاهرتز. أصبح هذا الأمر أقل شيوعا حيث يتوقف الناس عن طقم بتردد عنه الخدمة بسرعة 2.4 جيجاهرتز بشكل كامل. بيد أن الفكرة يمكن ويجب أن تستمر ولكن مع تحرك WPA3 SAE، ولكن الوضع الانتقالي يمنحك مشاكل في التوافق مع مفاهيم أخرى. ترى مم "القديم" تسمية WPA3 SAE SSID الرئيسي. ومن خلال WPA2 SSID "قديم" و "القديم" لعملائك؟ لديه العملاء، كما يمكنك بسهولة ملاحظة عدد العملاء الذين لا يزالون يواجهون مشكلات التوافق مع SSID الرئيسي الخاص بك ويتطلب هذا الطراز القديم.

العملاء ضعف بعض مشاكل مع بسبب 802. 11v لم سمعت شائعات بأن 802. 11v لكن لماذا نتوقف هنا؟ SSID؟ الأقدم وأ أن بعض برامج تشغيل العملاء لا تحب رؤية تحليلات الأجهزة المتكنة على SSID الرئيسي المتقدم وتتركها في طقم بتمكين كافة هذه المميزات المفيدة الموجودة في SSID القديم/التوافق. يتيح لك هذا إختبار بدء إستخدام المميزات الجديدة في SSID الرئيسي مع توفير الحد الأقصى من توافق SSID للعملاء للرجوع إليها. هذا النظام يعمل طقم بهذه الطريقة. إذا قمت بتسمية SSID المستندة إلى التوافق باسم رئيسي خاص بك بشيء مثل "<name>-WPA3"، فإنك تلاحظ الأشخاص وتسمي SSID المتقدم الخاص بك. وتسمي SSID القديم الذي اعتادوا عليه، والتبني يبقون صغارا لسنوات عديدة الذين يتمسكون ب SSID "الجديد" الخاص بك. يؤدي طرح الإعدادات أو المميزات الجديدة بعد ذلك إلى تناقص غير حاسم بسبب انخفاض عدد العملاء الذين يتصلون بها.

- ةنسبلاب ةصاخ ةفيضم ةدايزلا هذهو .Aironet تاذادتمإ ليطعتل تقو يأ نم لضفألا ،ةيملاعلا تاموعملا ةكبش لمعيو عقاوملا ةعاطتسا ببستي نأ نكلو ،ةيلمعلا ءاطخأ فشاكم دحأ ىلع ةيلاعف رثكأ ةقطنم ريفوتل ةجومولا ةيلمعلا يف ةلوهسب ةحاتم ةيكلسلا ةكبشلا ةيامحلا ريفشتلا ةقيرطو ةيلمعلا هذه ءانثأ ةيلاعف رثكأ ةيامح

- ريي كبير تأثير له لن أالسلكي لالزاجه لكل WLAN تاكبش عرأ نم رثكأ مادختسإ لواحم عدم إ. ةيلحم تاكبش مخم سراختسإ، فإ. نإ .صعبا حدا سيل هنإ .كلسلالا مادختسإ الترددع ىلع ةرايد ىلع نكل ولمعي نأ نكمي (WLAN) ةيكلسلا ءائضلا ثبلا تقو ةمات .WLAN تاكبش نم ديزملاو ديزملا مادختساب
- .ةعئاشلا ءالعملا لاوانأ نم قبل نم ةزايتم لكشب ةموعدم ميياعم يه k11. 802 و v11. 802 ةيعرفلا ةكبشلا ىلإ لوصولا ةطقن ليصوت ةداعإ ىلإ جاتحت يتلا ةيكلسلا ةكبشلا ةيعرف ىلإ ةجاحلا هذه ءالعملا ةدحو مادختسإ ةدايز ىلإ ةجاحلا هذه ققحتت .

بالنسبة لعمليات النشر الواسعة جغرافيا التي تتضمن العديد من المواقع والعديد من عالمات الموقع، يوصى بأن يكون عدد عالمات الموقع مضاعفا لعدد عمليات WNCD على النظام الأساسي الذي تستخدمه.

غير أنه بالنسبة لشبكات الحدث التي تكون عادة تحت سقف واحد، أو بنايات متعددة في نفس الموقع، فإن التوصية تنص على مطابقة عدد عالمات الموقع مع عدد الأقراص غير المضغوطة بدقة على المنصة المحددة. والهدف النهائي هو أن تتعامل كل عملية WNCD (وبالتالي كل مركز من مراكز وحدة المعالجة المركزية (CPU) المخصصة للمهام اللاسلكية) مع عدد مماثل تقريبا من أحداث تجول العملاء حتى يتم موازنة الحمل عبر جميع مراكز وحدة المعالجة المركزية (CPU).

Platform type	Number of WNCD processes
9800-CL small OVA	1
9800-CL medium OVA	3
9800-CL large OVA	7
9800-L	1
9800-40/CW9800-M	5
9800-80/CW9800-H	8

عدد عمليات WNCD لكل نوع من أنواع الأنظمة الأساسية

في الصميم، ما يهم حقا هو تجميع نقاط الوصول (APs) الموجودة في نفس الحي المادي في نفس طابق الموقع، بحيث تبقى أحداث التجوال المتكررة للعملاء بين نقاط الوصول هذه في نفس عملية وحدة المعالجة المركزية. هذا يعني أنه حتى إذا كان لديك مكان واحد كبير، فإنه من المستحسن أن تقوم بتقسيم الموقع إلى عدة عالمات تمييز للموقع (عدد أكبر من عدد ممكن من العمليات التي تتم في الموقع باستخدام تقنية WNCD)، ونقاط الوصول الجماعية في هذه المناطق، بشكل منطقي قدر الإمكان، لتكوين مجموعات حي الترددات اللاسلكي المنطقية والتي توزع أيضا بالتساوي بين عالمات الموقع.

بدءا من IOS XE 17.12، يمكن تمكين خوارزمية موازنة الأحمال حتى تقوم وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بتجميع نقاط الوصول (APs) استنادا إلى قرب الترددات اللاسلكي (RF) الخاص بها. ويؤدي ذلك إلى رفع العبء عن أيديكم وإيجاد توزيع متوازن لنقاط الوصول عبر عملية WNCD. قد يكون هذا مفيدا إذا لم تتمكن من رسم مجموعات من نقاط الوصول المجاورة بسهولة وضعها في المقدار الصحيح لعالمات الموقع. إحدى خصائص هذه الخوارزمية أنها تعيين نقاط الوصول إلى عملية WNCD بغض النظر عن تعييني عالمة الموقع الخاص بهم، وهذا يعني أنها لا تغير تعييني عالمة الموقع الخاص بـ AP. يمكنك بعد ذلك تعييني عالمات المواقع الأساسية بشكل خالص على منطق التكويني وترك الخوارزمية توازن نقاط الوصول عبر وحدات المعالجة المركزية (CPU) بالطريقة المثلى.

يتم توثيق ميزة موازنة حمل نقطة الوصول التلقائية المستندة إلى الترددات اللاسلكي

في دليل تكوين برنامج وحدة التحكم اللاسلكية من السلسلة Cisco Catalyst 9800 Series، الإصدار 17.12.x من Cisco IOS XE Dublin.

اذا .يجب مراقبة إستخدام وحدة المعالجة المركزية لعمليات WNCD أثناء الأحداث الكبيرة. نظهرت عملية أو أكثر من عمليات شاشات WNCD درجة عالية من الاستخدام، فقد يكون السبب هو أن شاشة WNCD تتعامل مع عدد كبير جدا من نقاط الوصول أو العملاء، أو أن نقاط الوصول أو العملاء الذين تتعامل معهم أكثر انشغالا من المتوسط (إذا كانت كلها تجوب بشكل مستمر كما في المطار على سبيل المثال).

ملف تعريف النهج

- قم بتمكين ARP ووكيل "اكتشاف العناوين المكررة" (DAD)، وهذا يسمح للجنة التحكم في الشبكة المحلية اللاسلكية (WLC) بالرد بالنيابة عن العملاء اللاسلكيين. يؤدي هذا أيضا إلى توفير عندما يحاول جهاز ما التعرف على عنوان MAC لجهاز لاسلكي. بطاريات أجهزة عميلة لاسلكية.
- قم بتمكين ميزات WGB إلا عند الحاجة.
- قم بتمكين DHCP المطلوب لتجنب العملاء الذين لديهم عناوين IP ثابتة.
- بعض المسؤولين يجعلون هذا-المهلة قصيرا (300 ثانية). لتجنب الطويلة-المهلة الخمول، ولكن ينتج عن مهلة الخمول الطويلة العملاء الذين يتعين عليهم إعادة المصادقة، حيث تؤثر على التقارير (التي تتم تأخير دعد العملاء من إدخالات العميل الشبح) الوقت الحقيقي. من الأفضل الاحتفاظ بمهلة الخمول أقل من مؤقت تدوير مفتاح المجموعة لتجنب فيضانات المحاسبة عند حذف العملاء. يمكن تكوين الفاصل الزمني لتناوب مفتاح المجموعة في واجهة مستخدم الويب تحت التكوين > الأمان > EAP المتقدم ك "EAP-Broadcast Key Interval"
- أجعل مهلة الجلسة 86400 ثانية لتجنب حالات عدم الاتصال وإعادة المصادقة غير الضرورية.

ملف تعريف ربط AP

- تأكد من تمكين MSS الخاص بضبط TCP.
- تمكين التشغيل المسبق ل DSCP الموثوق به. العديد من العملاء الذين يوضع علامات على بروتوكول 802.11e WMM، مما يعني أن الثقة اللاسلكيين في علامات DSCP هي طريقة مضمونة لتوفير الأولوية المناسبة للتطبيقات الصوتية.
- قم بتمكين Syslog لكل IP الخاص بنقاط الوصول الخاصة بك. يشكل Syslog وحدة طرفية للتحكم إلى حد كبير، ولكن ليس فقط مفيدا أن تحرى APs، وهو أيضا أفضل للشبكة من التقصير عملية إعداد أن يجعل APs يبث هم syslog في ال VLAN المحلي. يمكن أن ينتج عن تسجيل نقطة الوصول تحميل رسالة كبير، حتى في حالات التي ال يتم فيها مراقبة AP syslog، فإنها ما تزال فكرة جيدة للحد من عدد الرسائل المنع ب (على سبيل المثال 0.0.0.0) Syslog ل وهمي IP وتكوين عنوان /أو، المناسبة الرسالة خطورة تعيين خلال من الأحداث.
- فشل عمليات إعادة محاولة CAPWAP والمهلة إلى الحد الأقصى. يتم زيادة المؤقتات لإطلاق الحزم المفقودة، ولكن الشبكة أكثر مقاومة لعمليات إسقاط الحزم المفقودة، ولكن الشبكات بسرعة أقل،

البسيطة.

- قم بتمكين SSH وتكوين بيانات الاعتماد. تعطيل وحدة تحكم نقطة الوصول.
- قم بتمكين شاشة AP إذا لزم الأمر ولكن ليس جهاز مراقبة الراديو.
- قم بتمكين الكشف عن المخادع وتكوين حد RSSI من -70 ديسيبل.

مراقبة الشبكة

بمجرد تشغيل الشبكة، يجب عليك مراقبتها عن كثب بحثا عن المشاكل. في بيئة مكتبية قياسية، يستطيع المستخدمون التعرف على الشبكة ويمكنهم إما مساعدة بعضهم البعض في حالة حدوث مشكلات أو فتح تذكرة مكتب دعم داخلية. في مكان أكبر ومع العديد من الزوار يأتون لتركزوا على أكبر المشاكل بدلا من أفراد معينين والذين يمكن أن يكون لديهم سوء ترتيب، لذلك تحتاج إلى إستراتيجية المراقبة الصحيحة.

أن الأداة الأفضل هي GUI أو CLI 9800 حافزة من المدة، غير أنه ليس monitore الشبكة من أو/و بيانات حول كوك شكل بالفعل مباشرة عندما يكون لديك أقرب طريق إنه. أكثر بيانات حول يومي. خيارات المراقبة الرئيسية هي تشغيل أو تريد التي المشكلة. في الوقت الفعلي مع عينة في أوامر تشغيل أو تريد المشكلة. من الممكن إستخدام Cisco Catalyst Center أو برنامج لوحة معلومات مخصصة للقياس عن بعد. هذه الأدوات بروتوكول SNMP من المراقبة أدوات، ولكن عندما تستخدم خارجية جهات قبل من المعدات من الشبكات بائعي جميع مع يكفي بما مخصصة بيانات توفر لا أو الفعلي الوقت عن بعيدة بيانات تكون فإن البروتوكول، كبروتوكول المراقبة أدوات تكوين أو تحديث أو إستكشاف المشكلات وحلها على أقرب وقت ممكن. وهو يتيح أيضا، علاوة على المراقبة، الإستجابة للحالات الطارئة ومعالجة العديد من الحالات.

إذا كنت تريد عرض لوحة معلومات تتبع الاستخدام المخصصة يمكن أن تكون مفيدة

بالنسبة للمراقبة المخصصة يعد كل من NETconf RPC (السحب) و NETCONF Streaming الأفضل (الدفع) Telemetry. على الرغم من أنه تتبع الدفق المخصص بالاقتران مع Catalyst Center يتطلب بعض العناية، حيث يوجد حد لعدد الاشتراكات القياس عن بعد التي يمكن تكوينها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ويوفر مركز (استخدام) العديد من هذه الاشتراكات مسبقا.

عند استخدام NETconf RPC يلزم إجراء بعض الاختبارات لضمان عدم تحميل عنصر التحكم بشكل مفرط، ومن المهم بشكل خاص مراعاة معدلات التحديث لبعض نقاط البيانات والوقت المستغرق لإرجاع البيانات. على سبيل المثال، يتم تحديث استخدام قناة AP (من AP إلى WLC) كل 60 ثانية، ويمكن أن تستغرق مجموعة مقاييس RF ل 1000 APs (من WLC) عدة ثوان، في هذا المثال لن يكون إستقصاء WLC كل 5 ثوان مفيدا، وسيكون هناك أسلوب أفضل لجمع مقاييس RF على مستوى النظام كل 3 دقائق.

دائما ما يكون NetConf هو المفضل على SNMP.

عند استخدام تجميع البيانات، بما في ذلك إستخدام المعالج، يمكن تجاهل عملية مراقبة مكونات الشبكة الأساسية. ففشل أي من هذه المكونات الأساسية وما إلى ذلك. يمكن أن يتسبب فقدان الاتصال اللاسلكي في انقطاع الاتصال اللاسلكي.

أكثر الأخطاء شيوعا التي تسبب مشاكل في الذاكرة، أكثر مراقبة تمت بمراقبة الذاكرة، كلما إستطعت أن

أن أضي أيمكن ،رمستم لكشب عاخدام زاجم أي ةارشإ في ريي غت أي نع غالبإلا
ك بةصاخلا "النشر" ةيملعم ةبقارم نم دكأت .ةمات ةلوسوم بكحم زاجم أي عبشي
ةدحول يلاعلا مادختسالا ديق تسيل امأن دكأتو دعب نع سايقلا نع ةلوؤسملاو
.ةيزكرملا ةجلاعملا ف ،كلذ رمألا ناك اذإ .ةلظنلا يف كيلإ عادإلا عبتاتو دكأتم
.9800 ماع تارامسم لضفأ عابتإ

ةريبكلا تاكبشلا باصلخا لكاشملا

إذا كان لديك SSID باستخدام مصادقة الويب، فقد تكون هناك مشكلة في العملاء الذين يستخدمون أجهزة iOS 14 أو iPadOS 14 الجديدة. يتصلون بـ SSID ويحصلون على عنوان IP ولكنهم لا يصادقون أبدًا لأن المستخدم النهائي لن يتمكن من الوصول إلى بوابة الويب. (يجب أن تعترض وحدة التحكم اللاسلكي طلب الاتصال الخاص بالعميل الذي هو في حالة التي تسمى مصادقة الويب HTTP من قبل العميل الذي هو في حالة انتظار تشغيل الشبكة، بمجرد .WLC وإذا كان يستخدم وكيل المستخدم لتحديد عدد العملاء الذين هم في حالة تعليق مصادقة الويب في وقت معين لمعرفة كيفية مقارنتها بالأرقام المتوقعة. نفس الشيء للعملاء في حالة تعلم IP. لديك دائمًا عملاء في تلك الحالة عندما يكتشف العميل أن DHCP الخاص به، ولكن معرفة ما وهو رقم العميل المناسب للشبكة يمكن أن يساعد على تعيين خط أساس وتحديد اللحظات التي يمكن أن تكون فيها هذه الأرقام مرتفعة جدًا ويشير إلى مشكلة أكبر.

بالنسبة للأماكن الكبيرة، من غير الشائع رؤية ما يقارب 10٪ من العملاء في حالة تعليق بسبب مصادقة الويب.

مراقبة اليوم الثاني: مراقبة رضا المستخدمين

ال :ةكبشلا لغشتل جذومن نم نيتاهن مدختسم ةكاوش ،نوكي هنأك نوعان نم ةبقارم وبمجرد تشغيل الشبكة، يمكنهم التوصيل بشبكة Wi-Fi لعملاء (قطع الاتصال) التوصيل، أو أن شبكة Wi-Fi لا تعمل بشكل صحيح أو أن المستخدمين لا يتمتعون بالوصول إلى الإنترنت أو الموارد التي يحتاجون إليها. هذه هي المشكلات التي يواجهها معظم مسؤولي الشبكات يوميًا. تكون هذه المشكلات مزعجة للمستخدمين النهائيين ولكنها ليست بالضرورة كبيرة بما يكفي لتبرير فتح حالة TAC. ومع ذلك، فإن تراكم هذه المشكلات يمكن أن يؤثر على رضا المستخدمين العام عن الشبكة.

كيفية التحقق من إنتاجية Wi-Fi: دليل الاختبار والمراقبة. يعطي هذا المستند cisco.com نظرة عامة على الأدوات والميزات المتاحة في Catalyst Center والتي يمكن استخدامها لمراقبة تجربة العميل وتحديد المشكلات التي تؤثر على رضا المستخدم النهائي. سنناقش أيضًا كيفية استكشاف الأخطاء وإصلاحها باستخدام واجهة المستخدم الرسومية (GUI) وواجهة سطر الأوامر (CLI) لوحدة تحكم Catalyst 9800.

ةيكلسلال الاتصال للجنة العامة الأساسية المقاييس راقب ،ةديج ةعامة ممارسة ،كأو أخيرا
.(ةيسيئرلا ءادألا رشؤم ةدعاسمب Monitor Catalyst 9800 KPIs (ءادألا رشؤمو

تيئيئة قابلية التطوير

9800 زارطلا يف تاهاوجلاو SVIs ذفانم

تجنب إنشاء SVIs لشبكات VLAN الخاصة بالعميل على عنصر التحكم في الشبكة
WLC المحلية اللاسلكية (WLC). عادة ما يكون لدى المسؤولين الذين يستخدمون شبكات
القديمة الخاصة بنظام التشغيل AireOS لإنشاء واجهة الطبقة 3 لكل شبكة محلية ظاهرية (VLAN) عميلة، ولكن اذه مطلوب ما يكون اردان. تزيد الواجهات من متجه هجوم
رثكأ تالاخدإ عم لوصولا في مكحتلا تاقوافم نم ديزملا بلطتت نأ نكمي ويه مكحتلا ىوتسم
تعقيدا. يمكن الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)،
بشكل افتراضي، على أي من الواجهات الخاصة به، يلزم مزيد من العمل لحماية عنصر
التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام مزيد من الواجهات. كما تزيد من
.هيفاضلا تافلتخملا نم لذ ،هيجوتلا قيدعتو

ابتداء من IOS XE 17.9، لم تعد واجهات SVI مطلوبة لتطفل DNS أو سيناريوهات ترحيل
DHCP. لذلك هناك عدد قليل جدا من الأسباب لتكوين واجهة SVI في شبكة VLAN للعميل.

إستجابة المسبار المجمع

بالنسبة للشبكات العامة الكبيرة، من المستحسن تعديل الفاصل الزمني الافتراضي
لمسبار التجميع الذي يتم إرساله بواسطة نقاط الوصول. بشكل افتراضي، تقوم نقاط
الوصول بتحديث عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كل 500 مللي
ثانية حول المستكشفات التي يرسلها العملاء. يتم إستخدام هذه المعلومات من خلال
موازنة الأحمال وتحديد النطاق والموقع ومميزات 802.11k. إذا كان هناك العديد من العملاء ونقاط
الوصول، فمن المستحسن تعديل الفاصل الزمني للتحديث لمنع مشاكل أداء مستوى
التحكم في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). الإعداد الموصى به هو
50 استجابات مجمعة بالمسبار كل 64 ثانية. تأكد أيضا من أن نقاط الوصول لا تقوم
بالإبلاغ عن التحقيقات من عناوين MAC المدارة محليا حيث لا توجد نقطة تعقب لأولئك
الذين يعتبرون أن زبون واحد يمكن أن يستخدم العديد من أجهزة MAC المدارة
محليا أثناء المسح لتجنب التعقب بغرض معين.

```
wireless probe limit 50 64000

no wireless probe locally-administered-mac
```

IPv6

لوكوتورب من السادس للإصدار الضرورية في حالة الشبكة التي لا يزال العديد من مزودي الإنترنت (IP) لا يدعمون بروتوكول الإنترنت من الإصدار السادس مع خيارين مقبولين: إما أن تكون الشبكة مدعومة بالكامل، أو أن تكون غير مدعومة على الإطلاق: (IPv6) يجب عليك حظر بروتوكول الإنترنت من الإصدار السادس باستثناء بروتوكول الإنترنت (IP) و تمكينه في بعض الأماكن دون تهيئة مناسبة. وهذا من شأنه أن يجعل عالم IP بأكمله غير قابل للاستخدام بالنسبة لشبكة الخاص بك.

إذا قمت بتمكين IPv6، فمن الإلزامي تكوين عنوان IPv6 ظاهري في النطاق 2001:DB8:/32 (تكون هذه الخطوة غالبا ما يتم نسيانها).

على الرغم من أن IPv6 يعتمد كثيرا على البث المتعدد لعمليات الاكتشاف الأساسية، إلا أنه لا يزال بإمكان العميل إعادة توجيه البث المتعدد إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تشير إعادة توجيه البث المتعدد إلى إعادة توجيه بيانات البث المتعدد للعميل وليس إلى الاكتشاف المواجه واستدعاء البروتوكولات الأخرى المطلوبة لتشغيل IPv6.

إذا كان اتصال الإنترنت أو موفر خدمة الإنترنت يوفر عناوين IPv6، فيمكنك إتخاذ قرار بالسماح ب IPv6 على مستوى الشبكة الأساسية لديك. وهذا يختلف عن تمكين IPv6 في البنية التحتية للعميل. لا تزال حركة مرور بيانات IPv4 في العمل وقطع الاتصال بالكامل، ولكن يمكن لنقاط الوصول المحلية (APs) والشبكة المحلية اللاسلكية (WLC) تشغيل IPv6 داخل حزم CAPWAP الخاصة بهم. يتطلب تمكين IPv6 على البنية الأساسية لديك أيضا التفكير في حماية وصول العميل إلى نقاط الوصول المحلية (APs) والشبكة الفرعية للإدارة.

تحقق من تكرار RA لبوابات العميل. تقدم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) سياسة تقييد حركة مرور البيانات (RA) التي تحد من عدد عمليات إعادة توجيه البيانات إلى العميل حيث يمكن أن تحدث هذه العمليات أحيانا.

mDNS

بشكل عام، من الأفضل إبقاء نظام أسماء المواقع الطبوغرافية في وضع التشغيل الافتراضي.

يشير ربط DNS إلى مفهوم السماح بإرسال حزم DNS كبث متعدد من الطبقة 2 (وبالتالي إلى سياق mDNS خدمة شائعة في شبكة الفرعية للعميل بالكامل). أصبحت المنازل والمكاتب الصغيرة حيث يكون من العملي للغاية اكتشاف الخدمات في الشبكة في جميع العملاء في نفس الشبكة الفرعية لديك. ومع ذلك، في شبكة كبيرة، يعني ذلك إرسال الحزمة إلى كل شيء في الشبكة الفرعية وهو ما يمثل مشكلة من منظور حركة المرور في شبكة عامة كبيرة. ومن الناحية الأخرى، يتسبب الربط في أي نقاط عامة على الوصول أو وحدة المعالجة المركزية (WLC) حيث أنها تعترض الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وأ عبارة DNS إلى مفهوم إستخدام عنصر حركة مرور بيانات منظمة. يشير وكيل DNS إلى جميع الخدمات في الشبكة. وهذا يسمح بتوفير خدمات نظام أسماء النطاقات عبر حدود الطبقة 2 بطريقة فعالة وكذلك

لتقليل حركة المرور الإجمالية. باستخدام وكلاء DNS، ترسل العملاء، على سبيل المثال، استعلامات DNS إلى وكلاء DNS المحليين بدلاً من الخادم الفعلي. في شبكة متعددة البث (mDNS)، يتم إعلان الخدمة الدوري الخاص بها عبر نظام أسماء النطاقات (DNS) بواسطة وحدة التحكم في الشبكة المحلية الفرعية نفسها من الطبقة 2 ولكن لا تتوقع وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بتوجيهه إلى جميع العملاء اللاسلكيين الآخرين. وبدلاً من ذلك، تحيط علماً بالخدمة المعروضة وتسجيلها في دليل الخدمات الخاص بها. عندما يطلب أي عميل خدمات الوسائط المتعددة هذه عن طريق الإعلان، فإن WLC ترد نيابة عن العملاء اللاسلكيين الآخرين حول الطلبات وعروض الخدمات غير الضرورية هذه على تجنب حركة مرور الشبكة اللاسلكية المحلية (WLC) (أو نقطة الوصول (AP)، إذا كنت تعتمد على طاقم الوصول في سيناريوهات FlexConnect). إذا كنت تستخدم وكلاء DNS، فمن المهم أن تراقب استخدام وحدة المعالجة المركزية (CPU) بسبب التطفل على حركة مرور بيانات شبكات DNS. إذا كنت تستخدم وكلاء DNS، فمن المهم أن تراقب استخدام وحدة المعالجة المركزية (CPU) باستمرار.

لدى تطفل وتصيلها إلى عاصفة من البث المتعدد في الشبكة الفرعية الكبيرة يؤدي تلقائيًا إلى استخدام وحدة المعالجة المركزية (CPU) بشكل عالٍ (باستخدام ميزة وكلاء DNS) على شبكة WLAN بأكملها. قم بتعطيلها بشكل عام وذلك على كل شبكة WLAN على حدة.

في بعض المستخدمين بتمكين نظام أسماء النطاقات (mDNS) لأن بعض الخدمات تحتاج إليه في أماكن معينة، ولكن من المهم فهم حجم حركة المرور غير المرغوب فيها التي تضيفها هذه الخدمات. وكثيرًا ما تعلن أجهزة Apple عن نفسها كما تسعى باستمرار إلى الحصول على عناوين IP حتى عندما تكون في حالة سكون. الأمر الذي يؤدي إلى تشويش خلفي على استفسارات شركة Microsoft DNS، مما يؤدي إلى انقطاع الخدمات. إذا كنت بحاجة إلى السماح بخدمة معينة من أي شخص يستفيد بشكل عام من أي شيء، فقم بتمكينها بشكل عام ثم قم بتعطيلها بشكل عام وقم بتمكينها فقط لأعمال معينة، حيث تكون مطولة وحوالي تقييد النطاق حيث يتم السماح بـ mDNS عبر شبكة WLAN.

تقوية الشبكة

الأمان

في الشبكات العامة الكبيرة، يمكن أن تحدث الكثير من الأشياء دون أن يعلم المسؤول عنها. يطلب الأشخاص عمليات إسقاط الكبلات في أماكن عشوائية، أو قم بتوصيل محولات الطاقة المنزلية في موقع للحصول على مزيد من المحولات لأغراض المخادعة، ... إلخ. إذا كنت تعتقد أن هذه الأشياء تعادل دون طلب الإذن أو اذا كنت تعتقد أن هذه الأشياء لا يجب أن تحدث في شبكتك، فإن الأمر يتطلب منك عرض الخطر بالفعل من قبل عملاء المستخدم النهائيين و/أو المهاجمين الذين يحصلون على وصول مادي إلى شبكتك. يمكن أن تكون المصادقة 802.1X هي الحل الأمثل للتحكم في الوصول للشبكة التي يمكن للمستخدمين الوصول إليها. يمكن أن تكون المصادقة 802.1X مؤلمة للإعداد والتكوين، ولكن بمجرد تكوينها بشكل صحيح، فإنها تمنع أي شخص من توصيل كمبيوتر محمول بمنفذ switchport على أي من المحولات الموجودة في شبكتك. يمكنك أيضًا استخدام ميزة الأمان المحلية Catalyst على المحولات التي تدعم هذه الميزة، ولكن هذا يتطلب منك إدارة قوائم MAC يدويًا على كل محول وصلة. يمكن أن تكون المصادقة 802.1X أكثر أمانًا بكثير من المصادقة المستندة إلى MAC، ولكن هذا يتطلب منك إدارة قوائم MAC يدويًا على كل محول وصلة. يمكن أن تكون المصادقة 802.1X أكثر أمانًا بكثير من المصادقة المستندة إلى MAC، ولكن هذا يتطلب منك إدارة قوائم MAC يدويًا على كل محول وصلة.

نقاط الوصول الدخيلة

تعتمد إستراتيجيتكم لمحاربة الفاسقين على عوامل قليلة. يلجأ العديد من الإداريين إلى قواعد صارمة جدا، لكن الأسئلة الرئيسية هي:

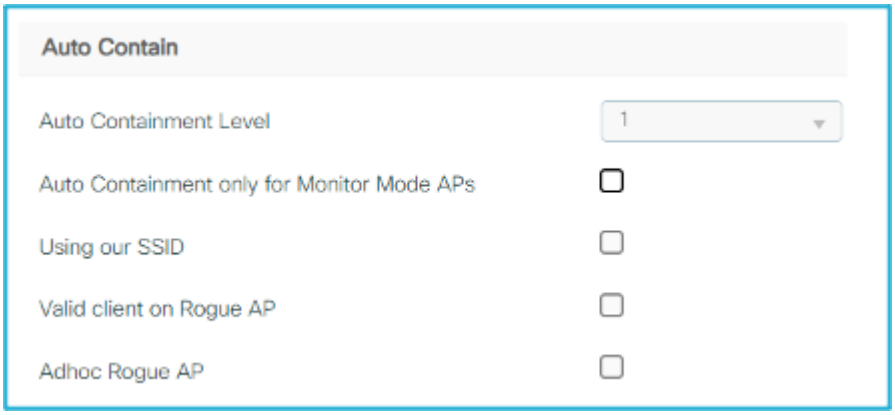
- عندما تحصل على المئات (إن لم يكن الآلاف) من التنبيهات المخادعة، فهل تمتلك الموارد البشرية اللازمة للنظر إليها جميعها واتخاذ الإجراءات اللازمة لتنفيذها جميعها؟
- هل هدفكم هو إزالة المخادعين جسديا للمحافظة على طيف نظيف من الترددات اللاسلكية؟ إذا كان الأمر كذلك، فأنتم بحاجة إلى أشخاص كثيرين للقيام بهذه العملية. وأي ربما هدفك هو مراقبة عامل الأمن فقط والتأكد من أن المحتالين لا يمثلون أي خطر؟ إذا كان هذا أكثر بكثير من تكلفة العمل البشري.
- قد يؤثر تمكين الكشف عن المخادع على وقت البث لديك، كما أن إحتواء المخادعين عادة ما يكون له تأثير أكبر، هل قمت بتحليل هذا التأثير وأخذته بعين الاعتبار؟

وفيما يتعلق بتأثير الكشف عن المخادع، فإن رقاقة مخصصة تعمل بتقنية 9130 و 9120 (والتالي الكشف عن المخادع)، مما يجعل CleanAir وتتكفل بالمسح الضوئي خارج القناة لتأثير على جهاز الراديو الذي يخدم العملاء خلايا تقريبا. كما أن نقاط الوصول من السلسلة 9160 مزودة بشريحة CleanAir Pro تتمتع بإمكانية مسح مماثلة دون تأثير، ولكن نقاط الوصول الأخرى التي لا يتوفر لديها شريحة CleanAir بحاجة إلى قطع القناة وتنفيذ عمليات المسح بحثا عن المخادع وأ عمليات الإجراء التي تخدم العملاء اللاسلكية التي تخدمه دورا في القرار باستخدام نقاط الوصول الذي تستخدمه نموذج نقطة الوصول المخصصة في وضع المراقبة للكشف عن المخادع واحتوائها من عدمه.

ملاحظة: تعمل الهواتف المحمولة التي تشترك في نقطة اتصال Wi-Fi في وضع "الأقران" إلى "البنية الأساسية" حيث يشير وضع الوصول التقليدية مثل نقاط الوصول "البنية الأساسية" وهو أقل شيوعا. وجود اتصال مباشر بين الأجهزة المحمولة.

تأكد من أن تعمل القواعد التنظيمية إحتواء المخادعين، لذا فمن الضروري أن تتأكد من وعادة ما تمنع السلطات المحلية قبل تمكينها. إن إحتواء هذه المشكلة لا يعني إغلاق هذه المشكلة عن بعد، بل غمر العملاء الذين يحاولون الاتصال بنقطة الوصول الدخيلة بإطارات تجريد من المصادقة حتى لا يتواصلوا. لا يمكن أن يعمل هذا إلا على SSID للأمان القديم (لا يعمل في WPA2) لأن نقاط الوصول الخاصة بك غير قادرة على إدارة PMF متاحة في WPA2 وأ WPA3 عندما يكون توقيع إطارات إلغاء المصادقة بشكل صحيح. يؤثر الاحتواء تأثيرا سلبيا على أداء الترددات اللاسلكي على القناة المستهدفة حيث تقوم نقاط الوصول بملء وقت البث بإطارات إلغاء المصادقة. لذلك يجب إعتبار ذلك أحد الإجراءات الأمنية لمنع زبائنك الشرعيين من الاحتكاك بنقطة وصول دخيلة عن طريق الخطأ. ولجميع الأسباب المذكورة، يوصى بعدم القيام بأي عملية إحتواء لأن ذلك لا يحل المشكلة المراقة تماما ويسبب المزيد من مشاكل الترددات اللاسلكي. إذا كنت بحاجة إلى الاحتواء، فيكون من المنطقي تمكينها للواردات التي تفسد أحد عناوين SSID المدارة لأنها تمثل هجوما واضحا لقضاء عسل النحل.

يمكنك إما تكوين الاحتواء التلقائي باستخدام خيار "إستخدام SSIDs":



إعدادات الاحتواء التلقائي

يمكنك أيضا تكوين قواعد مخادعة لتصنيف نقاط الوصول الضالة الخبيثة وفقا للمعايير الخاصة بك. ال تنس إدخال اسم SSIDs المجاورة والموافق عليها كمرواغات مألوفة لإزالة تلك من قائمة التنبيه الخاصة بك.

تمكين مصادقة نقطة الوصول أو PMF لحماية نقاط الوصول من الانتحال.

المخادع السلكية هي نقطة وصول مخادعة متصلة بشبكتك السلكية، مما يشكل تهديدا أمنيا متزايدا بشكل واضح. الكشف عن المخادعين السلكيين أكثر تعقيدا لأن عنوان MAC الخاص به. يتوفر مركز Cisco Catalyst على Ethernet MAC لخادع يختلف قادة عن عنوان MAC خوارزميات ال تزال تحاول اكتشاف ما إذا كان أحد المخادعين يتم توصيله بالإنترنت ويبحث عن أجهزة MacS العميلة المخادعة التي يتم الاستماع إليها عبر الهواء ويتم رؤيتها في البنية الأساسية السلكية. أفضل حل لمنع المخادعين السلكيين بشكل كامل هو تأمين جميع منافذ المحول لديك باستخدام مصادقة 802.1X.

إذا كنت ستقوم بالتصرف مداي على نقطة وصول دخيلة، فإن الاستفادة من Cisco Spaces وه المفتاح للحصول على موقع دقيق للمارقين. ال يزال من المرجح جدا أن تقوم بالبحث مرة واحدة في الموقع لأن الناس يميلون إلى إخفاء نقاط الوصول المخادعة في بعض الأحيان ولكن تقليل مساحة البحث إلى بضعة أمتار يجعل ذلك مسعى عمليا جدا. وبدون "مسافات"، ظهور المخادع على الخريطة بجوار نقطة الوصول، كاشفا أنها الأعلى صوتا، مما يجعل منطقة بحث كبيرة جدا. توجد العديد من الأدوات والأجهزة اللاسلكية التي تظهر لك إشارة نقطة الوصول المخادعة في الوقت الفعلي لمساعدتك في تحديد مكان المخادع فعليا.

مهم، فقط، كان معظى CleanAir أن حيث ولكن، بالضبط بالفاسدين بالضبط، العالقة لها بالفاسدين بالضبط، ولكن حيث أن CleanAir ال تؤثر سلبيا على العروض باستثناء اكتشاف ملاحظة أن تمكين CleanAir يؤثر على أداء 2.4 جيجاهيرتز. يمكنك تكوين الشبكة اللاسلكية حيث أن هذا يؤثر على منارة BLE الخاصة بك لتجاهل متدخلي Bluetooth بالكامل بما أنهم موجودون في كل مكان في عالم اليوم، والا يمكنك منع عملائك من تمكين Bluetooth الخاص بهم.

ضع بعض .يستطيع المخادعين ال تظهر في قائمة الكشف عن المخادعين هناك فئة أخرى من
العملاء إستخدام Wi-Fi المباشر بين بعضهم البعض، وبالتالي ال يستخدمون أي نقطة
الدردشة. وهذا ال يمثل في الواقع مصدر قلق أمني ولكنه يستخدم وقت طيران
.اللاسلكي
ومن الأمثلة على ذلك نظام Apple AirDrop حيث يكتشف جهازان بعضهما البعض عبر تقنية
Wi-Fi لنقل الملفات. يرغب Bluetooth ثم يمكنهما الموافقة على إستخدام قناة
المستخدمون في نقل هذا الملف على أية حال، لذلك من الأفضل السماح لهم بنقله بأسرع
وقت ممكن حتى يتوقف التداخل في أقرب وقت ممكن. ومع ذلك، كن على دراية بأن اكتشاف
الإسقاط الجوي يمكن في بعض الأحيان أن يجعل رفرفة نفق VPN إذا لم يعالج تطبيق
Wi-Fi، وبدون أن يدرك المستخدمين النهائيين، وبالنسبة للمستخدمين AWDL بشكل صحيح، حالة واجهة VPN
الخاص بالبنية الأساسية لديك وهو الذي يتسم بوجود سيئة عندما يكون في الواقع وهو
مزيج من تطبيق VPN الخاص به مع بروتوكول الإسقاط الجوي الذي يتسبب في الرفرفة.
Wi-Fi. إذا حل تعطيل المعيل المشكلة، فلن يكون ذلك مشكلة على جانب Bluetooth
مثال آخر معروف هو Apple SideCar حيث يمكنك إستخدام iPad لتوسيع شاشة الكمبيوتر إلى
شاشة أخرى. يمكن أن يؤدي ذلك إلى إستخدام تردد الراديو بشكل كبير لأن الدفق مستمر
ويمكن أن يستخدم عرض قناة كبيرة.

WiPS

يغطي نظام WiPS وموجات الهجمات الأكثر تقدما من مجرد اكتشاف وجود جهاز مخادع غير مصرح
به. وعلاوة على هذه الهجمات، توفر أيضا في بعض الأحيان نسخة من الحدث لتحليل الطب
الشرعي.

وفي حين أن هذه ميزة أمان مفيدة جدا للمؤسسة، إلا أن الشبكة ذات الواجهة العامة يجب أن
تواجه السؤال الأبدي: ما الذي يجب فعله ضدها؟

وهو صعوبة إدارة العديد من العملاء الذين لا يمكنك التحكم فيهم، يمكن تقسيم أجهزة
الإنذار إلى فئتين. التنبيه الذي يمكنك تجاهله من مركز Cisco Catalyst إذا رأيت الكثير
منهم:

- 10001: رفض الخدمة: تنبيه طوفان المصادقة
- 10002: رفض الخدمة: تنبيه طلب القارتان
- 10003: رفض الخدمة: جهاز إنذار الفيضان لمجس البث
- 10004: رفض الخدمة: الإنذار بالفيضان
- 10005: رفض الخدمة: تنبيه الإرسال الخاص ب DIS-Association
- 10006: رفض الخدمة: تنبيه طوفان إلغاء المصادقة
- 10007: DOS: تنبيه إلغاء مصادقة البث
- 10008: DOS: تحذير هجوم EAPOL-Logoff
- 10009: جهاز الإنذار بالفيضان
- 10010: تنبيه طلب القارتان RTS
- 10011: فيض إلغاء المصادقة حسب الزوج
- 10021: جلسة الإسقاط الجوي (عادة ما يحدث هذا كثيرا في أي شبكة ويصور بسطاء
نشاط النظير إلى النظير بين أجهزة Apple)

- 10022: طلب اقتران غير صحيح
- 10023: تسرب فشل المصادقة حسب التوقيع
- 10024: MAC OUI غير صالح من خلال التوقيع
- 10025: المصادقة التي تم تكوينها بشكل سيئ

ضع في اعتبارك أن سبب هذه الإنذارات هو سوء سلوك العميل. لا يمكن منع هجوم من المحتمل أن يكون سببه

حركة طاقة إعادة توجيه إذا لم يتم تطبيق أي من هذه الشروط على العميل. ومع ذلك، قد يكون لهذا تأثير مختلف على أداء العميل. يمكن أن تتسبب التطبيقات التي تستخدم اتصالات متعددة، مثل تطبيقات البث المباشر، في حدوث مشكلات في الأداء عند تحديد معدل حركة المرور. يوصي خبراء Cisco CX بإستخدام تطبيقات تابعة لجهات خارجية لتحديد معدل حركة المرور الخاصة بالتطبيقات التي تعتمد على الإنترنت بشكل كبير. راجع وثائق Cisco Wireless Controller وMeraki :
https://documentation.meraki.com/Wireless/Operate_and_Maintain/How_Tos/Firewall_and_Traffic_Shapin

راجع وثائق Cisco Wireless Catalyst، وكذلك في
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html

تقييد وصول العملاء

يوصى بتمكين حظر النظير إلى النظير على جميع شبكات WLAN لديك (ما لم يكن لديك متطلبات تطبيقات تتصل من عميل إلى عميل - ولكن يجب مراعاة ذلك بعناية) لتجنب الاتصال بين العملاء على شبكة WLAN نفسها من الاتصال ببعضهم البعض. تمنع هذه الميزة العملاء من الاستمرار في الاتصال ببعضهم البعض، كما يمكن للعملاء الذين يتنقلون إلى شبكات WLC مختلفة الاتصال بالأجهزة القريبة. ولكن يجب على العملاء الأفراد أو مجموعة التنقل تجاوز هذه الميزة لحظر النظير إلى النظير. ومن المزايا الأخرى لهذه الميزة أنها تمنع أيضا برامج الفيروسات والتجسس. تمنع هذه الميزة أجهزة أخرى تحاول التنصت على حركة المرور الخاصة بالعملاء الآخرين المتصلين في الشبكة الفرعية بسيطة عن طريق إرسال جميع حركة المرور إلى بوابة التوجيه الافتراضية.

يجب تطبيق ACL على شبكات WLAN الخاصة بك لمنع الاتصال من عميل إلى عميل. يتحكم ACL في الوصول (ACL) التي تمنع العميل من الاتصال بالعميل على مستوى العميل أو SVIs للعميل إذا كان لديك شبكة محلية لاسلكية (WLAN) تغطي النظر عن ما إذا كنت تستخدم IPv6 في شبكتك، فقم بتطبيق ACL لكل من IPv4 و IPv6 (إذا كان ذلك ممكنا).

تتمثل الخطوة الإلزامية الأخيرة في منع الوصول اللاسلكي إلى أي شكل من أشكال حركة المرور الخاصة بك.

مثال:

```
ip access-list extended ACL_DENY_CLIENT_VLANS

10 deny ip any 10.131.0.0 0.0.255.255

20 deny ip 10.131.0.0 0.0.255.255 any

30 deny ip any 10.132.0.0 0.0.255.255
```

```
40 deny ip 10.132.0.0 0.0.255.255 any

50 deny ip any 10.133.0.0 0.0.255.255

60 deny ip 10.133.0.0 0.0.255.255 any

70 deny ip any 10.134.0.0 0.0.255.255

80 deny ip 10.134.0.0 0.0.255.255 any

90 deny ip any 10.135.0.0 0.0.255.255

100 deny ip 10.135.0.0 0.0.255.255 any

110 deny ip any 10.136.0.0 0.0.255.255

120 deny ip 10.136.0.0 0.0.255.255 any

130 deny ip any 10.137.0.0 0.0.255.255

140 deny ip 10.137.0.0 0.0.255.255 any

150 permit ip any any
```

يمكن تطبيق قائمة التحكم في الوصول (ACL) هذه على واجهة الإدارة SVI:

```
interface Vlan130

ip access-group ACL_DENY_CLIENT_VLANS in
```

يتم هذا على WLC مع عميل VLANs 131 إلى 137 في الطبقة 2 VLAN قاعدة معطيات غير تمنع قائمة التحكم في الوصول (ACL) هذه جميع العملاء اللاسلكي من إرسال أي حركة مرور إلى واجهات التحكم في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مستويات إدارة والتحكم في الشبكة الوحيد الذي تحتاج إلى السماح به، حيث أنه يلزم أيضا السماح باتصال CAPWAP لجميع نقاط الوصول. ولهذا السبب تحتوي قائمة التحكم في الوصول (ACL) هذه على تصريح افتراضي، ولكنها تمنع جميع الإجراءات الأخرى. بدلا من الاعتماد على إجراء الرفض الافتراضي لجميع نطاقات العملاء اللاسلكي، يجب تحديد نطاقات شبكات AP الفرعية ونطاقات الإدارة المسموح بها.

وبالمثل، يمكنك إنشاء قائمة تحكم في الوصول (ACL) أخرى تحدد جميع الشبكات الفرعية الممكنة للإدارة:

```
ip access-list standard ACL_MGMT

10 permit 10.128.0.0 0.0.255.255

20 permit 10.127.0.0 0.0.255.255
```

```
30 permit 10.100.0.0 0.0.255.255

40 permit 10.121.0.0 0.0.255.255

50 permit 10.141.0.0 0.0.255.255
```

رطس ةهجاو ىلإ لوصولل هذه (ACL) لوصولا يف مكحتلا ةمئاق قيبطت كلذ دعب كنمي مكحتلا رماوألا:

```
line vty 0 50

access-class ACL_MGMT in

exec-timeout 180 0

ipv6 access-class ACL_IPV6_MGMT in

logging synchronous

length 0

transport preferred none

transport input ssh

transport output ssh
```

.بيو لوؤسم ىلإ لوصولل (ACL) لوصولا يف مكحتلا ةمئاق سفن قيبطت اضيأ نكمي

رورملا ةمدخ عاونأ نم ةيامحلا

.ىرخألا تاقيبطتلا نم ربكأ ةفاثكب او لبقتلا ددعتملا لاسرإلا تاقيبطت ضعب مدختست ةكبش يف مكحتلا دنع ،ةفاضملا لبقتلا ةيامحلا نإف ،قفطو ةيكلسلا ةكبشلا ءاوهلا ربع لاسرإ متي امدنع لبقتلا ةيامحلا نإف ،كلذ عمو .حيرصلا تنرتنإلا ىلإ لوصولا ةيناكمإ ىلع ةيلمعلا هذه رثؤت نأ نكمي .ةددعتم ةيجراخ ةهجاو ربع ةهجولا ىلإ ةمزح لاسرإ لواحي مهنأ مهفت نأ انهه .ببسلا اذه ىلإ ةجاحلا نود ةيلمعلا هذه ءارجإ ىلع ةردقلا ةكبشلا ةرادإ ةزهجأ ىلع ةيلحمل

نيكمتلا بلطتم عم دعتملا بلسلتملا ليغشتلا ةداعإ هيجوت بلس دعتملا بلسلا .ىرخألا لئاسرلا ةيفاضإ ةزهجأ ىلع دوجوملا هجوملا ةداعإ هيجوت بلس معطلا ةمامإ .تسدخم ،IPv6 وه امك ،حضوم مسبقا .يفضلا فاشكتسالا تاودأ عيمج ىلع رثؤت دق ةيفرعلا ةكبشلا .ةريبك ةكبش يف ينمأ قلق درصم حوضوم لكشي ام ،امهنم

إذا قمت بتمكين إعادة توجيه البث المتعدد العام، فتأكد من إستخدام إعداد AP CAPWAP المتعدد. عم هذا يمكن، عندما ال WLC يستلم multicast رطب من السلكي بنية للبث

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).