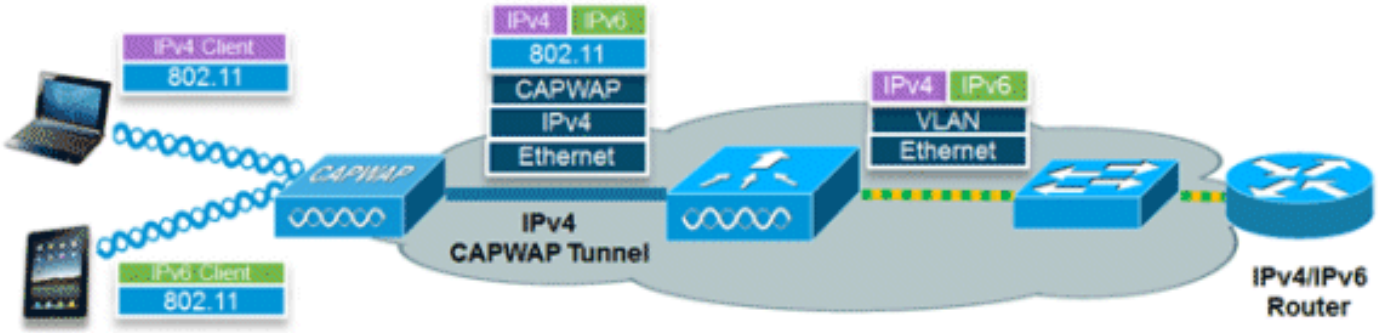
دليل نشر عميل IPv6 لشبكة LAN اللاسلكية

المحتويات

المقدمة

يقدم هذا المستند معلومات حول نظرية التشغيل والتكوين لحل شبكة LAN اللاسلكية الموحدة من Cisco فيما يتعلق بدعم عملاء IPv6.

اتصال العميل اللاسلكي ل IPv6



تتيح مجموعة ميزات IPv6 داخل الإصدار 7.2 من برنامج الشبكة اللاسلكية الموحدة من Cisco للشبكة اللاسلكية دعم العملاء الذين يستخدمون IPv4 و Dual-Stack و IPv6 فقط على الشبكة اللاسلكية نفسها. كان الهدف الإجمالي لإضافة دعم عميل IPv6 إلى شبكة LAN اللاسلكية الموحدة من Cisco هو الحفاظ على تماثل الميزات بين عملاء IPv4 و IPv6 بما في ذلك إمكانية التنقل والأمان والوصول إلى الضيوف وجودة الخدمة وإمكانية رؤية نقطة النهاية.

يمكن تعقب ما يصل إلى ثمانية عناوين عميل IPv6 لكل جهاز. ويتيح هذا لعملاء IPv6 الحصول على عنوان التكوين التلقائي للعنوان (SLAAC) المحلي عديم الحالة وبروتوكول التكوين الديناميكي للمضيف لعنوان (DHCPv6 IPv6)، وحتى العناوين في البادئات البديلة لتكون على واجهة واحدة. كما يمكن لعملاء جسر مجموعة العمل (WGB) المتصلين بوصلة نقطة وصول (AP) مستقلة في وضع WGB دعم IPv6.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية Series 2500 أو Series 5500 أو WiSM2
- نقاط الوصول من السلسلة 1130 و 1240 و 1250 و 1040 و 1140 و 1260 و 3500 و 3600 Series APs و

1520 أو 1550 Series
- الموجه القادر على بروتوكول IPv6

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

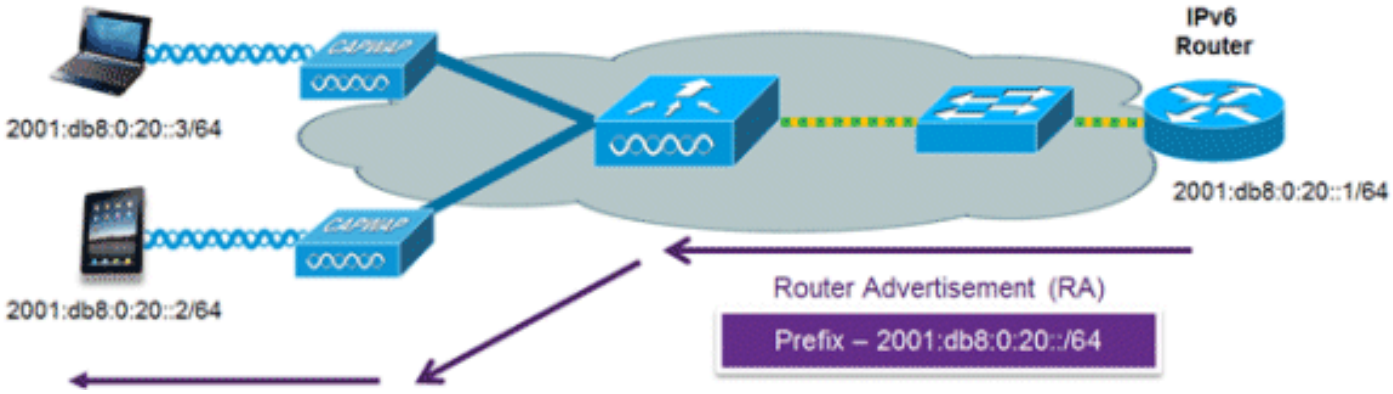
الاصطلاحات

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

المتطلبات الأساسية لاتصال عميل IPv6 اللاسلكي

لتمكين اتصال عميل IPv6 اللاسلكي، يجب أن تدعم الشبكة السلكية الأساسية توجيه IPv6 وآلية تعيين العناوين مثل SLAAC أو DHCPv6. يجب أن يكون لوحدة التحكم في الشبكة المحلية اللاسلكية تجاور L2 مع موجه IPv6، ويجب وضع علامة على شبكة VLAN عندما تدخل الحزم وحدة التحكم. لا تتطلب نقاط الوصول الاتصال على شبكة IPv6، حيث يتم تضمين جميع حركة مرور البيانات داخل نفق IPv4 CAPWAP بين نقطة الوصول ووحدة التحكم.

تعيين عنوان SLAAC

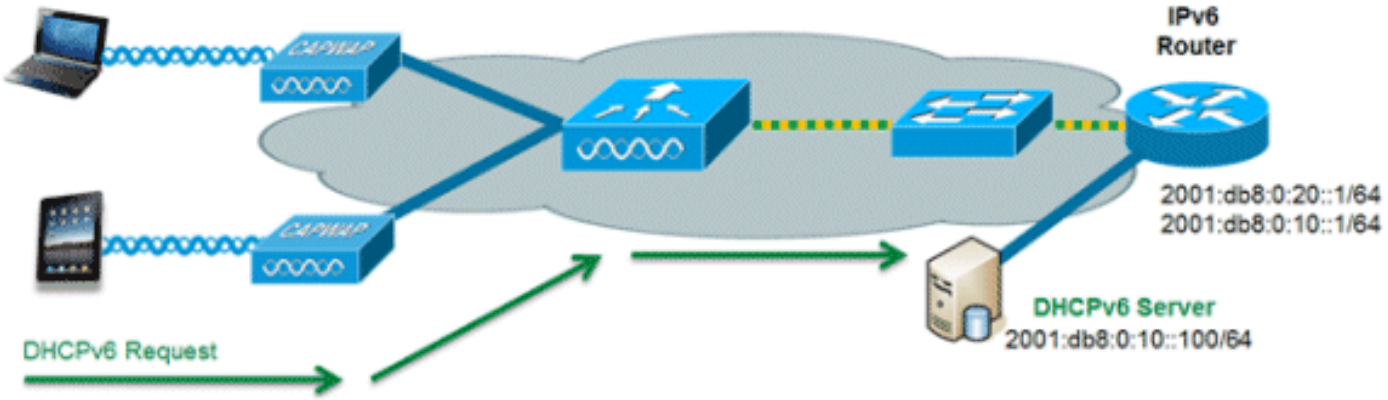


الطريقة الأكثر شيوعا لتعيين عنوان عميل IPv6 هي SLAAC. توفر SLAAC إمكانية اتصال سهلة التوصيل والتشغيل حيث يقوم العملاء بتعيين عنوان ذاتيا استنادا إلى بادئة IPv6. يتم تحقيق هذه العملية عندما يرسل موجه IPv6 رسائل إعلان دورية للموجه تقوم بإعلام العميل ببادئة IPv6 المستخدمة (أول 64 وحدة بت) وبالعبارة الافتراضية IPv6. ومن هذه النقطة، يمكن للعملاء إنشاء وحدات 64 بت المتبقية من عنوان IPv6 الخاص بهم استنادا إلى خوارزميين إثنين هما: EUI-64 الذي يستند إلى عنوان MAC الخاص بواجهة التوصيل، أو العناوين الخاصة التي يتم إنشاؤها بشكل عشوائي. ويرجع إختيار الخوارزمية إلى العميل وغالبا ما يكون قابلا للتكوين. يتم إجراء اكتشاف العناوين المكررة بواسطة عملاء IPv6 لضمان عدم اصطدام العناوين العشوائية التي يتم انتقاؤها مع عملاء آخرين. يتم إستخدام عنوان الموجه الذي يرسل الإعلانات كبوابة افتراضية للعميل.

يتم إستخدام أوامر تكوين Cisco IOS® هذه من موجه IPv6 قادر على Cisco لتمكين عنونة SLAAC وإعلانات الموجه:

```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

تعيين عنوان DHCPv6



لا يلزم إستخدام DHCPv6 لاتصال عميل IPv6 إذا كان SLAAC قيد النشر بالفعل. هناك وضعان للعملية ل DHCPv6 يدعيان **عديم الحالة** و**ذو حالة**.

يتم إستخدام وضع DHCPv6 **عديم الحالة** لتزويد العملاء بمعلومات شبكة إضافية غير متوفرة في إعلان الموجه، ولكن ليس عنوان IPv6 حيث إن هذا يتم توفيره بالفعل من قبل SLAAC. يمكن أن تتضمن هذه المعلومات اسم مجال DNS وخادم (خوادم) DNS وخيارات مورد DHCP الأخرى المحددة. تكوين الواجهة هذا لموجه Cisco IOS IPv6 الذي ينفذ DHCPv6 عديم الحالة مع تمكين SLAAC:

```
ipv6 unicast-routing
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 enable
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

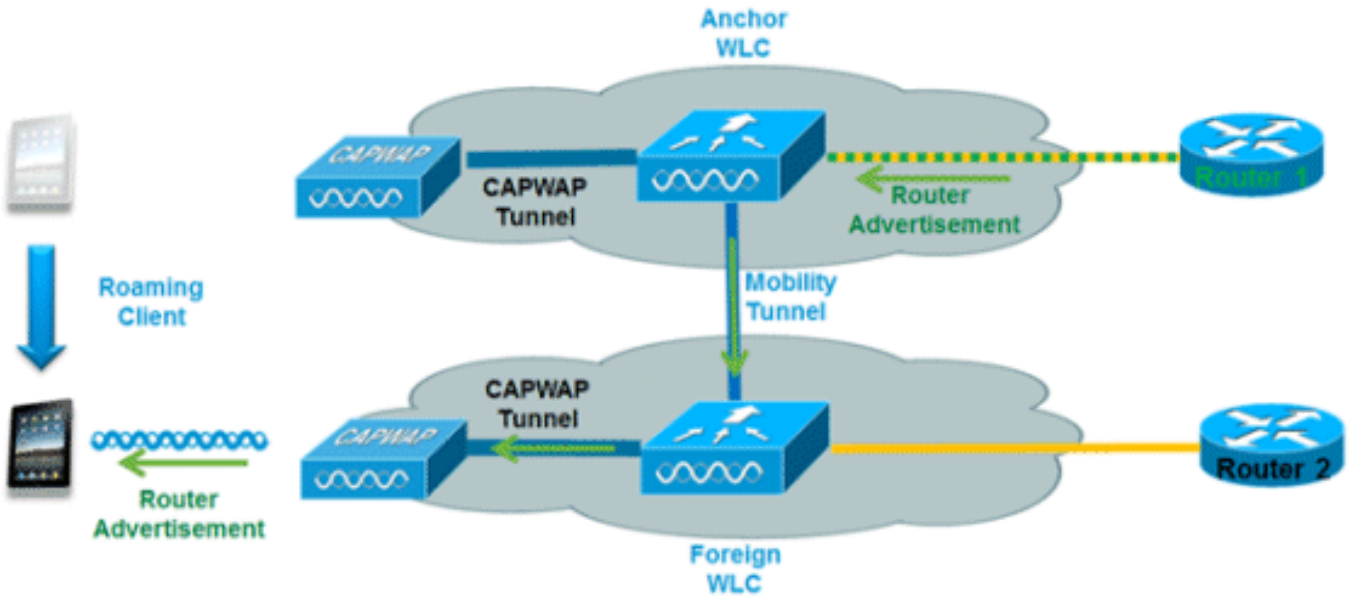
يعمل خيار DHCPv6 **ذو الحالة**، المعروف أيضا باسم الوضع المدار، بشكل مماثل ل DHCPv4 من حيث أنه يعين عناوين فريدة لكل عميل بدلا من العميل الذي ينتج آخر 64 وحدة بت من العنوان كما هو الحال في SLAAC. تكوين الواجهة هذا خاص بموجه Cisco IOS IPv6 الذي ينفذ DHCPv6 ذو الحالة مع تعطيل SLAAC:

```
ipv6 unicast-routing
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 enable
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

معلومات إضافية

خارج نطاق هذا المستند عن تكوين الشبكة السلكية لاتصال IPv6 بالكامل على مستوى المجمع باستخدام طرق اتصال المكدس المزدوج أو الاتصال النفقي. لمزيد من المعلومات، ارجع إلى دليل النشر الذي تم التحقق من صحته من Cisco نشر IPv6 في شبكات المجمعات.

إمكانية تنقل عميل IPv6



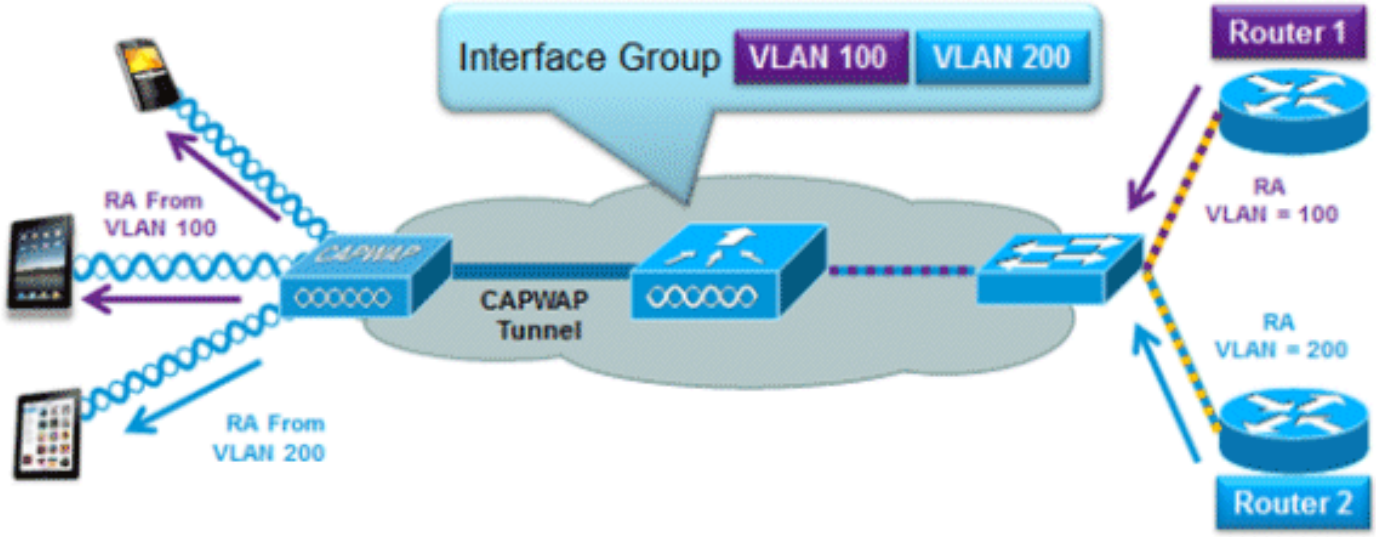
للتعامل مع عملاء IPv6 المتجولين عبر وحدات التحكم، يجب التعامل مع رسائل ICMPv6 مثل طلب الجوار (NS) والإعلان المجاور (NA) والإعلان عن الموجه (RA) وطلب الموجه (RS) بشكل خاص لضمان بقاء العميل على شبكة الطبقة 3 نفسها. يعد التكوين الخاص بقابلية تنقل بروتوكول IPv6 هو نفسه الخاص بقابلية تنقل بروتوكول IPv4 ولا يتطلب وجود برامج منفصلة على جانب العميل لتحقيق التجوال بسلاسة. والتكوين الوحيد المطلوب هو أن وحدات التحكم يجب أن تكون جزءا من نفس مجموعة/مجال التنقل.

فيما يلي عملية نقل عميل IPv6 عبر وحدات التحكم:

1. إن يتلقى كلا جهاز تحكم منفذ إلى ال نفسه VLAN الزبون كان اصلا على، ال roam يكون ببساطة طبقة 2 يطوف حدث حيث الزبون سجل يكون نسخت إلى الجهاز تحكم جديد ولا حركة مرور يكون أنثقت إلى الخلف إلى المرسى جهاز تحكم.
2. إذا لم يكن لدى وحدة التحكم الثانية حق الوصول إلى شبكة VLAN الأصلية التي كان العميل يعمل عليها، سيحدث حدث تجوال من الطبقة 3، مما يعني أنه يجب إنشاء قنوات لجميع حركة المرور من العميل عبر نفق التنقل (IP عبر Ethernet) إلى وحدة التحكم في الإرساء.لضمان احتفاظ العميل بعنوان IPv6 الأصلي، يتم إرسال نقاط الوصول من شبكة VLAN الأصلية بواسطة وحدة التحكم في الإرساء إلى وحدة التحكم الخارجية حيث يتم تسليمها إلى العميل باستخدام البث الأحادي من L2 من نقطة الوصول.عندما يذهب العميل المتنقل إلى تجديد عنوانه عبر DHCPv6 أو إنشاء عنوان جديد عبر SLAAC، يستمر إنشاء حزم RS و NA و NS عبر الشبكة المحلية الظاهرية (VLAN) الأصلية حتى يستلم العميل عنوان IPv6 قابل للتطبيق على شبكة VLAN هذه.

ملاحظة: يرتكز التنقل لعملاء IPv6 فقط على معلومات شبكة VLAN. هذا يعني أن IPv6-only زبون حركية لا يساند على VLANs untagged.

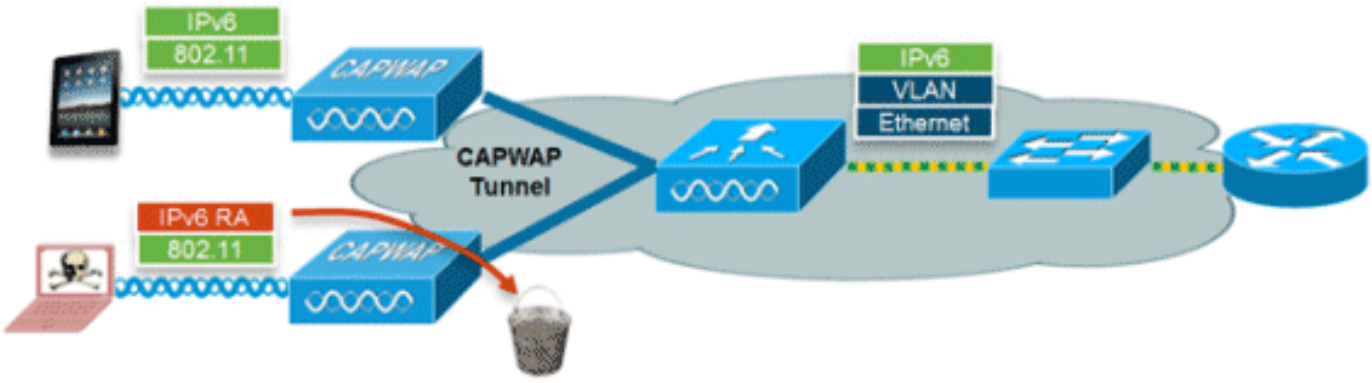
دعم تحديد شبكة VLAN (مجموعات الواجهة)



تتيح ميزة مجموعات الواجهة للمؤسسة إمكانية الحصول على شبكة WLAN واحدة مع شبكات VLAN متعددة تم تكوينها على وحدة التحكم للسماح بموازنة حمل العملاء اللاسلكيين عبر شبكات VLAN هذه. يتم إستخدام هذه الميزة بشكل شائع للحفاظ على أحجام الشبكات الفرعية ل IPv4 صغيرة مع تمكين شبكة WLAN في الوقت نفسه من التطوير إلى آلاف المستخدمين عبر شبكات VLAN متعددة في المجموعة. من أجل دعم عملاء IPv6 باستخدام مجموعات الواجهة، لا يتطلب الأمر أي تكوين إضافي لأن النظام يرسل تلقائيا RA الصحيح إلى العملاء الصحيحين عبر البث الأحادي اللاسلكي من المستوى الثاني. بمحاكاة RA الأحادية، لا يستلم العملاء على ال نفسه WLAN، غير أن VLAN مختلف، ال RA غير صحيح.

أمان الخطوة الأولى لعملاء IPv6

حماية إعلان الموجه



تزيد ميزة "حماية RA" من أمان شبكة IPv6 من خلال إسقاط نقاط الوصول عن بعد (RAs) الواردة من عملاء اللاسلكي. وبدون هذه الميزة، يمكن لعملاء IPv6 الذين تم تكوينهم بشكل غير صحيح أو ضار الإعلان عن أنفسهم كموجه للشبكة، وغالبا ما يكون ذلك بأولوية عالية يمكن أن تكون لها الأولوية على موجهات IPv6 المشروعة.

بشكل افتراضي، يتم تمكين واقي RA في نقطة الوصول (ولكن يمكن تعطيله في نقطة الوصول) ويتم تمكينه دائما على وحدة التحكم. يفضل إسقاط نقاط الوصول (RA) في نقطة الوصول لأنه حل أكثر قابلية للتطوير ويوفر عدادات إسقاط RA محسنة لكل عميل. في جميع الحالات، سيتم إسقاط IPv6 RA عند نقطة ما، مما يحمي العملاء اللاسلكيين الآخرين والشبكة السلكية عند الخادم من عملاء IPv6 الضارين أو الذين تم تكوينهم بشكل غير صحيح.

حماية خادم DHCPv6

تمنع ميزة "حماية خادم DHCPv6" العملاء اللاسلكيين من توزيع عناوين IPv6 إلى عملاء لاسلكيين آخرين أو عملاء سلكية من الخادم. لمنع تسليم عناوين DHCPv6، يتم إسقاط أي حزم إعلان DHCPv6 من عملاء اللاسلكي. تعمل

هذه الميزة على وحدة التحكم، ولا تتطلب أي تكوين ويتم تمكينها تلقائيا.

واقي مصدر بروتوكول IPv6

تمنع ميزة "واقي مصدر IPv6" عميل لاسلكي من انتحال عنوان IPv6 لعميل آخر. هذه الميزة مماثلة لواقي مصدر بروتوكول IPv4. يتم تمكين واقي مصدر IPv6 بشكل افتراضي ولكن يمكن تعطيله عبر واجهة سطر الأوامر.

محاسبة عنوان IPv6

بالنسبة لمصادقة RADIUS ومحاسبته، تعيد وحدة التحكم عنوان IP واحد باستخدام السمة "framed-ip-address". يتم إستخدام عنوان IPv4 في هذه الحالة.

تستخدم السمة "call-station-id" هذه الخوارزمية لإرسال عنوان IP مرة أخرى عند تكوين "نوع معرف محطة الاتصال" على وحدة التحكم على "عنوان IP":

1. عنوان IPv4
2. عنوان IPv6 العالمي أحادي البث
3. ربط عنوان IPv6 المحلي

نظرا لأن عناوين IPv6 للعميل يمكن أن تتغير بشكل متكرر (عناوين مؤقتة أو خاصة)، فمن المهم تتبعها عبر الوقت. تقوم Cisco NCS بتسجيل جميع عناوين IPv6 المستخدمة بواسطة كل عميل وتسجيلها تاريخيا في كل مرة يجول فيها العميل أو ينشئ جلسة جديدة. يمكن تكوين هذه السجلات في NCS للاحتجاز لمدة تصل إلى عام.

ملاحظة: تم تغيير القيمة الافتراضية ل "نوع معرف محطة الاتصال" على وحدة التحكم إلى "عنوان MAC للنظام" في الإصدار 7.2. عند الترقية، يجب تغيير هذا للسماح بالتتبع الفريد للعملاء بواسطة عنوان MAC حيث قد تتغير عناوين IPv6 في منتصف الجلسة وتسبب مشاكل في المحاسبة إذا تم تعيين معرف Call-Station-ID على عنوان IP.

قوائم التحكم في الوصول إلى IPv6

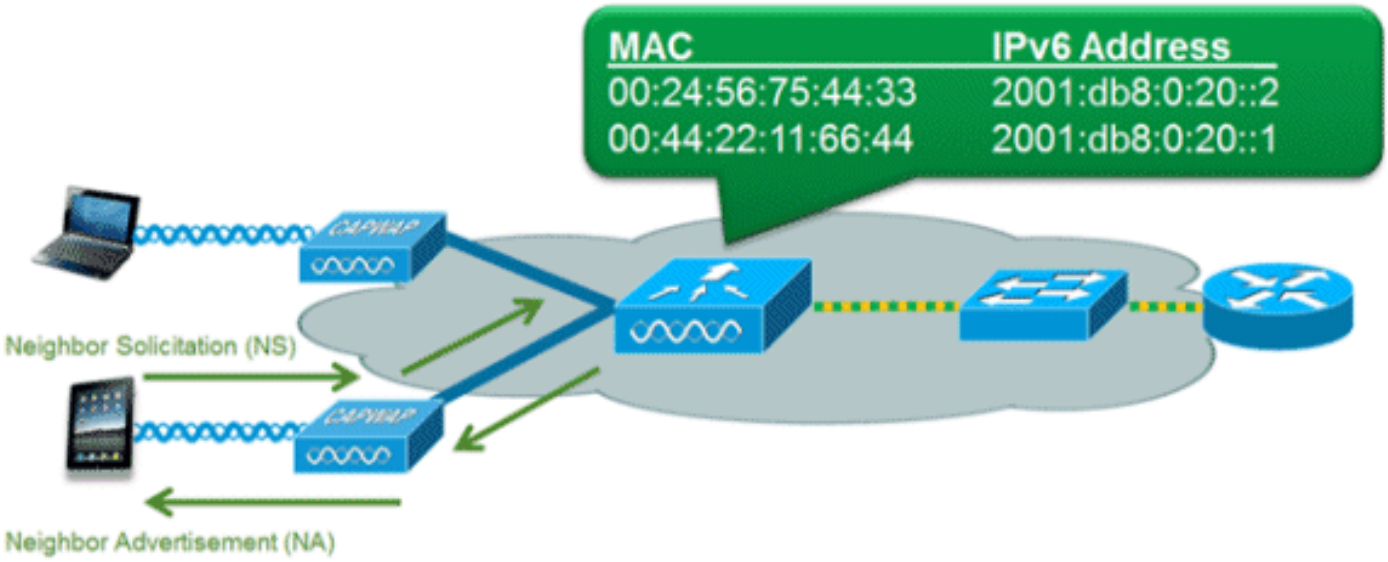
من أجل تقييد الوصول إلى موارد سلكية معينة للتدفق أو حظر تطبيقات معينة، يمكن إستخدام قوائم التحكم في الوصول (ACL) إلى IPv6 لتحديد حركة المرور والسماح بها أو رفضها. تدعم قوائم التحكم في الوصول (ACL) إلى IPv6 نفس الخيارات الخاصة بقوائم التحكم في الوصول (ACL) إلى IPv4 بما في ذلك منفذ المصدر والوجهة ومنفذ المصدر والوجهة (يتم دعم نطاقات المنافذ أيضا). كما يتم دعم قوائم التحكم في الوصول (ACL) السابقة للمصادقة لدعم مصادقة ضيف IPv6 باستخدام خادم ويب خارجي. تدعم وحدة التحكم اللاسلكية ما يصل إلى 64 قائمة تحكم في الوصول (ACL) فريدة لبروتوكول IPv6 مع 64 قاعدة فريدة في كل منها. تستمر وحدة التحكم اللاسلكية في دعم 64 قائمة تحكم في الوصول (ACL) إضافية فريدة إلى IPv4 مع 64 قاعدة فريدة في كل منها لإجمالي 128 قائمة تحكم في الوصول (ACL) لعميل مزدوج المكدس.

تجاوز AAA لقوائم التحكم في الوصول (ACL) إلى IPv6

من أجل دعم التحكم في الوصول المركزي من خلال خادم AAA مركزي مثل محرك خدمات الهوية من Cisco (ISE) أو ACS، يمكن توفير قائمة التحكم في الوصول ل IPv6 على أساس كل عميل باستخدام سمات تجاوز AAA. لاستخدام هذه الميزة، يجب تكوين قائمة التحكم في الوصول إلى IPv6 على وحدة التحكم ويجب تكوين شبكة WLAN باستخدام ميزة تجاوز AAA التي تم تمكينها. السمة الفعلية المسماة AAA لقائمة التحكم في الوصول (ACL) إلى IPv6 هي ***Airespace-IPv6-ACL-Name*** مماثلة للسمة *Airespace-ACL-Name* المستخدمة لتوفير قائمة التحكم في الوصول (ACL) المستندة إلى IPv4. يجب أن تكون سمة AAA التي تم إرجاعها سلسلة مساوية لاسم قائمة التحكم في الوصول (ACL) الخاصة ب IPv6 كما تم تكوينها على وحدة التحكم.

تحسين الحزم لعملاء IPv6

التخزين المؤقت لاكتشاف الجوار



يستخدم بروتوكول اكتشاف الجوار ل IPv6 (NDP) حزم NA و NS بدلا من بروتوكول تحليل العنوان (ARP) للسماح لعملاء IPv6 بحل عنوان MAC للعملاء الآخرين على الشبكة. يمكن أن تكون عملية NDP مخاطبة جدا لأنها تستخدم عناوين البث المتعدد في البداية لتنفيذ تحليل العنوان، وهذا يمكن أن يستهلك وقت بث لاسلكي قيم حيث يتم إرسال حزم البث المتعدد إلى جميع العملاء على مقطع الشبكة.

لزيادة كفاءة عملية NDP، يسمح التخزين المؤقت لاكتشاف الجوار لوحدة التحكم بالعمل كوكيل والرد على استعلامات NS التي يمكن حلها. تم تمكين التخزين المؤقت لاكتشاف الجوار بواسطة جدول الربط المجاور الأساسي الموجود في وحدة التحكم. يتعقب جدول الربط المجاور كل عنوان IPv6 وعنوان MAC المقترن به. عندما يحاول عميل IPv6 حل عنوان طبقة إرتباط عميل آخر، يتم اعتراض حزمة NS بواسطة وحدة التحكم التي تستجيب مرة أخرى باستخدام حزمة NA.

تقييد إعلان الموجه

تتيح ميزة تقييد إعلانات الموجهات لوحدة التحكم فرض تحديد معدل نقل البيانات الذي يتم توجيهه نحو الشبكة اللاسلكية. من خلال تمكين التحكم في RA، يمكن قص الموجهات التي تم تكوينها لإرسال RA بشكل متكرر (على سبيل المثال، كل ثلاث ثوان) مرة أخرى إلى الحد الأدنى من التردد الذي سيظل يحافظ على اتصال عميل IPv6. وهذا يسمح بتحسين وقت البث من خلال تقليل عدد حزم البث المتعدد التي يجب إرسالها. وفي جميع الحالات، إذا أرسل أحد العملاء RS، فسيتم السماح ل RA من خلال وحدة التحكم والبث الأحادي إلى العميل الطالب. ويهدف ذلك إلى ضمان عدم تأثر العملاء الجدد أو العملاء المتجولين سلبا بعمليات تقييد الوصول عن بعد (RA).

وصول ضيف IPv6

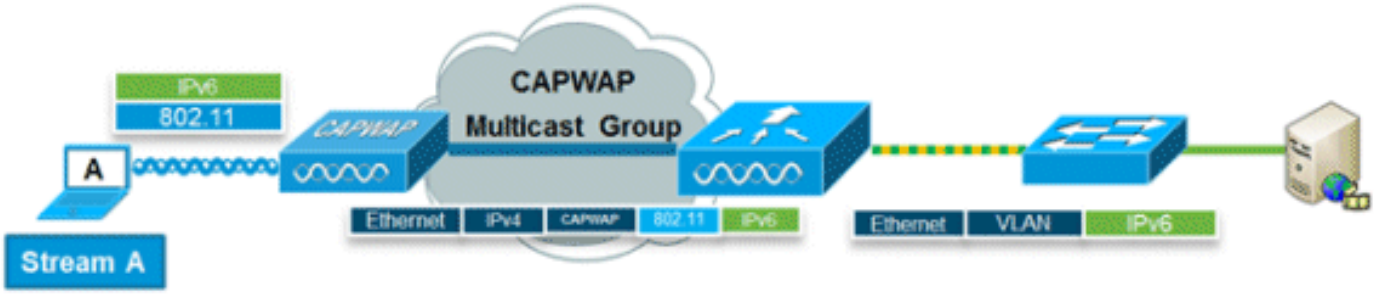
تعمل ميزات الضيف اللاسلكي والسلكي الموجودة لعملاء IPv4 بنفس الطريقة لعملاء المكدس المزدوج وعملاء IPv6 فقط. بمجرد قيام المستخدم الضيف بالترابط، يتم وضعه في حالة تشغيل "WEB_AUTH_REQ" حتى تتم مصادقة العميل عبر البوابة المقيدة ل IPv4 أو IPv6. ستقوم وحدة التحكم باعتراض حركة مرور كل من IPv4 و IPv6 HTTP/HTTPS في هذه الحالة وإعادة توجيهها إلى عنوان IP الظاهري لوحدة التحكم. بمجرد مصادقة المستخدم عبر البوابة المقيدة، يتم نقل عنوان MAC الخاص به إلى حالة التشغيل ويسمح لكل من حركة مرور IPv4 و IPv6 بالمرور. بالنسبة لمصادقة الويب الخارجية، تسمح قائمة التحكم في الوصول (ACL) للمصادقة المسبقة باستخدام خادم ويب خارجي.

لدعم إعادة توجيه عملاء IPv6 فقط، تقوم وحدة التحكم تلقائيا بإنشاء عنوان ظاهري IPv6 استنادا إلى العنوان الظاهري IPv4 الذي تم تكوينه على وحدة التحكم. يتبع عنوان IPv6 الظاهري قاعدة `[< IPv4 >:ffff::]`. على سبيل المثال، سيترجم عنوان IP ظاهري 1.1.1.1 إلى `[ffff:1.1.1.1::]`.

عند إستخدام شهادة SSL موثوق بها لمصادقة الوصول الضيف، تأكد من تحديد كل من العنوان الظاهري لوحدة التحكم IPv4 و IPv6 في DNS لمطابقة اسم مضيف شهادات SSL. وهذا يضمن أن العملاء لا يتلقون تحذيرا أمنيا يشير إلى أن الشهادة لا تطابق اسم المضيف للجهاز.

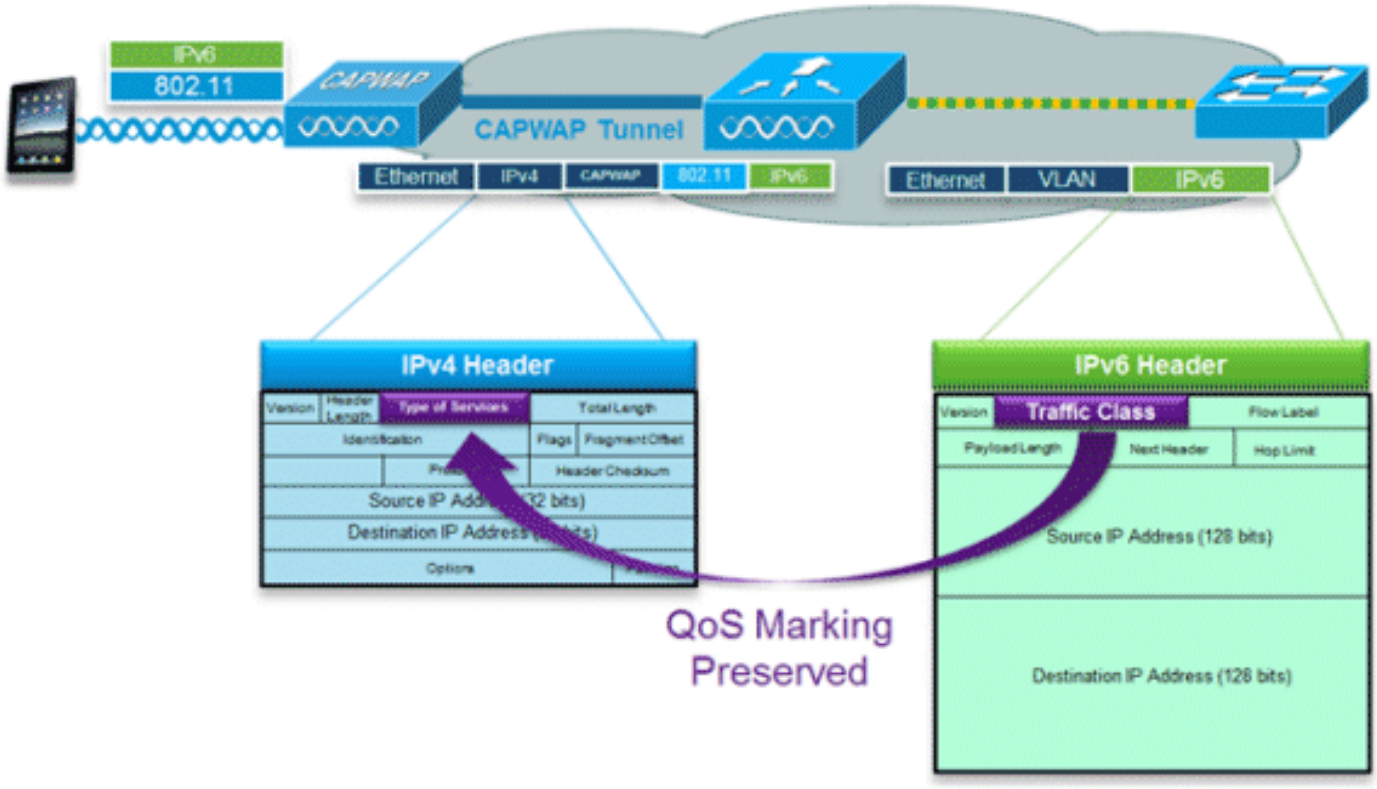
ملاحظة: لا تحتوي شهادة SSL التي تم إنشاؤها تلقائيا لوحدة التحكم على العنوان الظاهري IPv6. قد يتسبب ذلك في قيام بعض مستعرضات ويب بتقديم تحذير أمان. يوصى باستخدام شهادة SSL موثوق بها للوصول إلى الضيوف.

تدفق فيديو IPv6



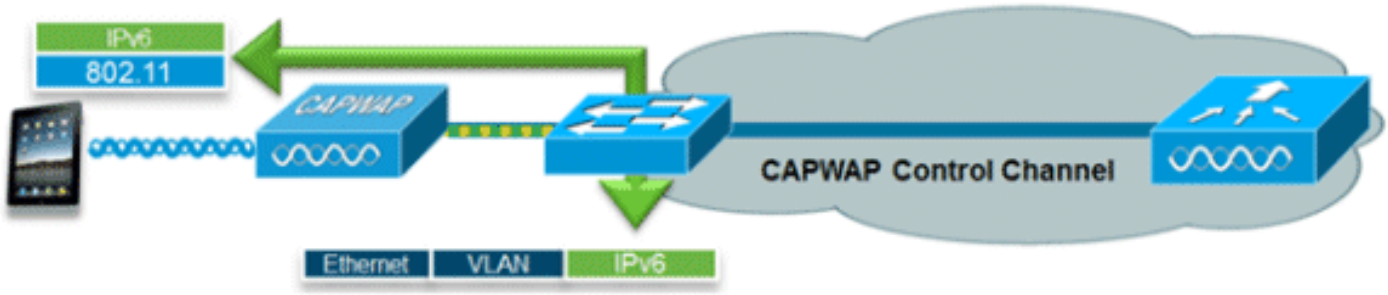
يتيح VideoStream إمكانية توصيل فيديو للبث المتعدد اللاسلكي بشكل يمكن الاعتماد عليه وقابل للتطوير، مما يعمل على إرسال البث بتنسيق أحادي لكل عميل. يقع البث المتعدد الفعلي إلى تحويل البث الأحادي (من L2) عند نقطة الوصول موفرا حلا قابلا للتطوير. ترسل وحدة التحكم حركة مرور فيديو IPv6 داخل نفق البث المتعدد IPv4 CAPWAP الذي يسمح بتوزيع الشبكة بكفاءة إلى نقطة الوصول.

جودة خدمة IPv6



تستخدم حزم IPv6 علامة مماثلة لاستخدام IPv4 لقيم DSCP التي تدعم ما يصل إلى 64 فئة مختلفة من فئات حركة مرور البيانات (0-63). بالنسبة للحزم المتدفقة من الشبكة السلكية، يتم نسخ قيمة فئة حركة مرور بيانات IPv6 إلى رأس نفق CAPWAP لضمان الحفاظ على جودة الخدمة من نهاية إلى نهاية. وفي إتجاه البث، يحدث نفس الشيء مع تمييز حركة مرور العميل التي تم وضع علامة عليها في الطبقة 3 مع فئة حركة مرور IPv6 عن طريق تمييز حزم CAPWAP الموجهة لوحدة التحكم.

FlexConnect و IPv6



FlexConnect - شبكات WLAN للتحويل المحلي

يدعم FlexConnect في وضع التحويل المحلي عملاء IPv6 من خلال ربط حركة مرور البيانات بشبكة VLAN المحلية، المماثلة لعملية IPv4. يتم دعم إمكانية تنقل العميل للطبقة 2 أثناء التجوال عبر مجموعة FlexConnect.

يتم دعم هذه الميزات الخاصة بالإصدار السادس من بروتوكول الإنترنت (IPv6) في وضع التحويل المحلي من خلال تقنية FlexConnect:

- حماية IPv6 RA
- ربط IPv6
- مصادقة ضيف IPv6 (مستضافة بواسطة وحدة التحكم)

هذه الميزات الخاصة ب IPv6 غير مدعومة في وضع التحويل المحلي ل FlexConnect:

- إمكانية التنقل من المستوى 3
- تدفق فيديو IPv6
- قوائم التحكم في الوصول إلى IPv6
- واقي مصدر بروتوكول IPv6
- حماية خادم DHCPv6
- التخزين المؤقت لاكتشاف الجوار
- تقييد إعلان الموجه

FlexConnect - شبكات WLAN للتحويل المركزي

بالنسبة لنقاط الوصول في وضع FlexConnect باستخدام التحويل المركزي (إعادة توجيه حركة مرور البيانات إلى وحدة التحكم)، يجب تعيين وحدة التحكم على "البث المتعدد - وضع البث الأحادي" ل "وضع البث المتعدد لنقطة الوصول". بما أن نقاط الوصول FlexConnect لا تنضم إلى مجموعة CAPWAP للبث المتعدد من وحدة التحكم، فيجب نسخ حزم البث المتعدد في وحدة التحكم والبث الأحادي إلى كل نقطة وصول على حدة. هذه الطريقة أقل فعالية من "وضع البث المتعدد - وضع البث المتعدد" وتضع حمل إضافي على وحدة التحكم.

هذه الميزة الخاصة ب IPv6 غير مدعومة في وضع التحويل المركزي ل FlexConnect:

- تدفق فيديو IPv6

ملاحظة: شبكات WLAN المحولة مركزيا التي تشغل IPv6 غير مدعومة على وحدة التحكم Flex 7500 Series Controller.

إمكانية رؤية عملاء IPv6 باستخدام NCS

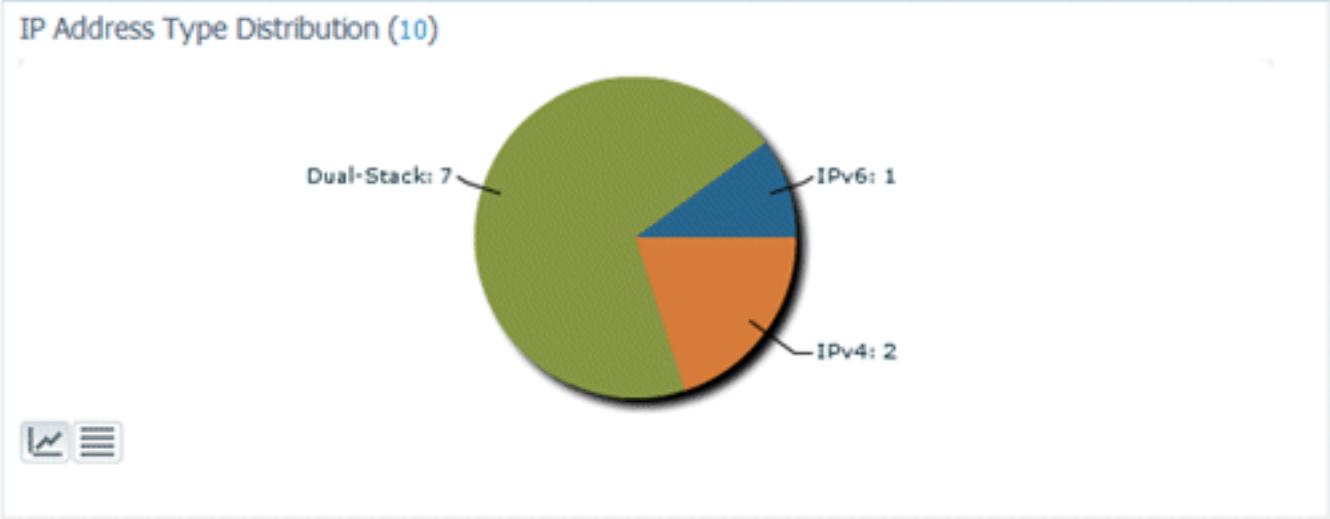
مع إصدار NCS v1.1، تتم إضافة العديد من الإمكانات الإضافية الخاصة بالإصدار السادس من بروتوكول الإنترنت

(IPv6) لمراقبة شبكة من عملاء IPv6 على كل من الشبكات السلكية واللاسلكية وإدارتها.

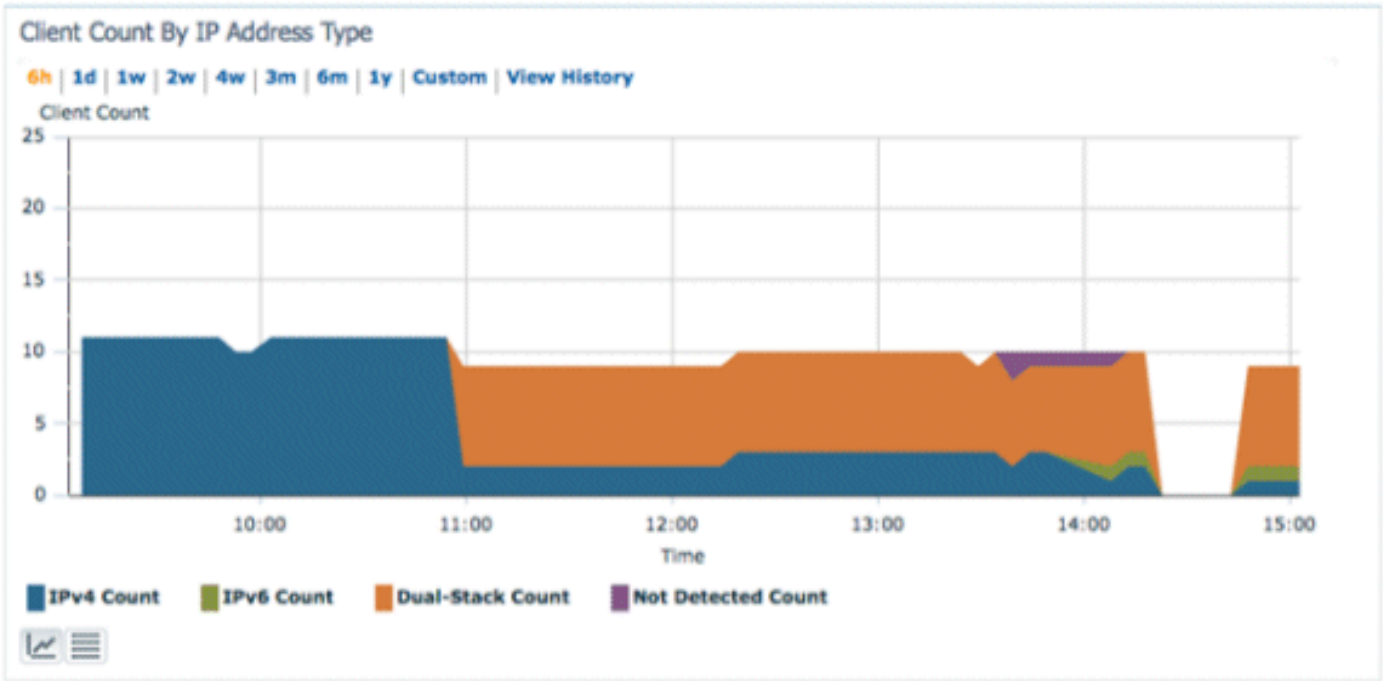
عناصر لوحة معلومات IPv6

لعرض أنواع العملاء الموجودة على الشبكة، تتوفر "dashlet" في بطاقات الشبكة (NCS) لتوفير نظرة متعمقة على إحصائيات IPv6 المحددة وتوفير إمكانية التنقل التفصيلي إلى عملاء IPv6.

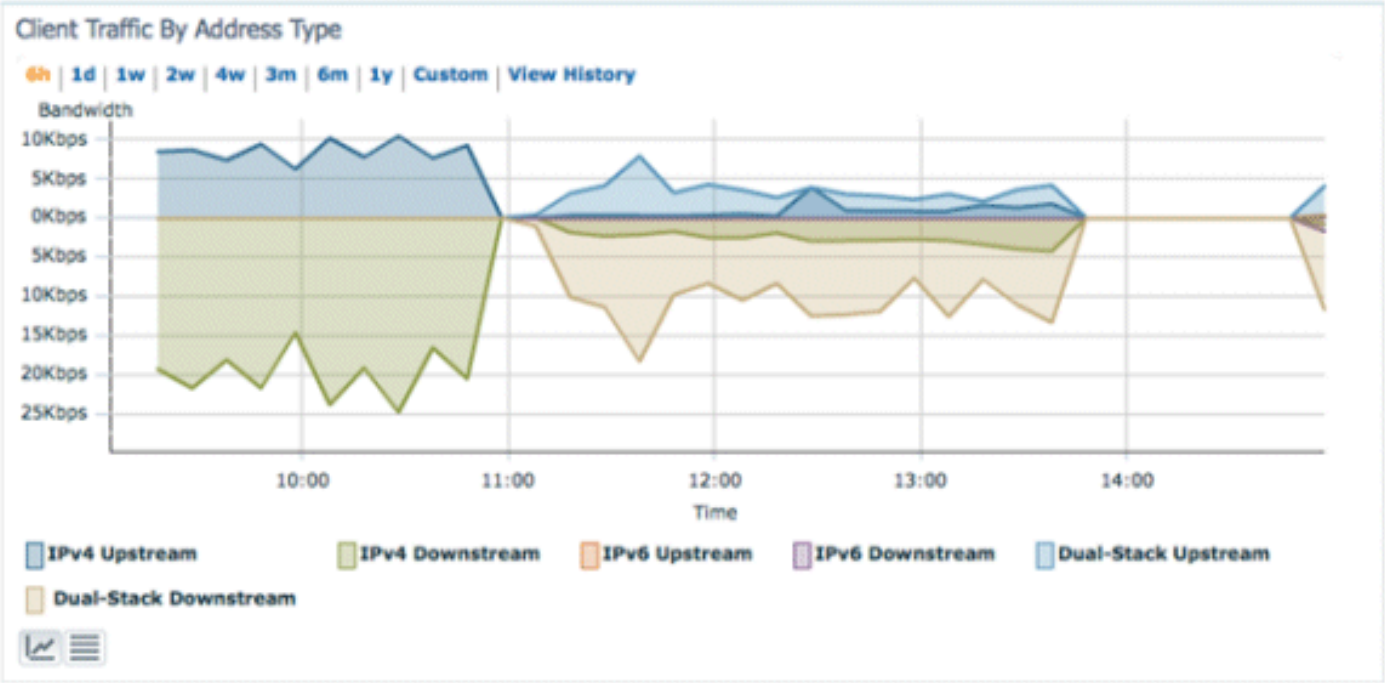
dashlet نوع عنوان IP - يعرض أنواع عملاء IP على الشبكة:



عدد العملاء حسب نوع عنوان IP - يعرض نوع عميل IP عبر الوقت:



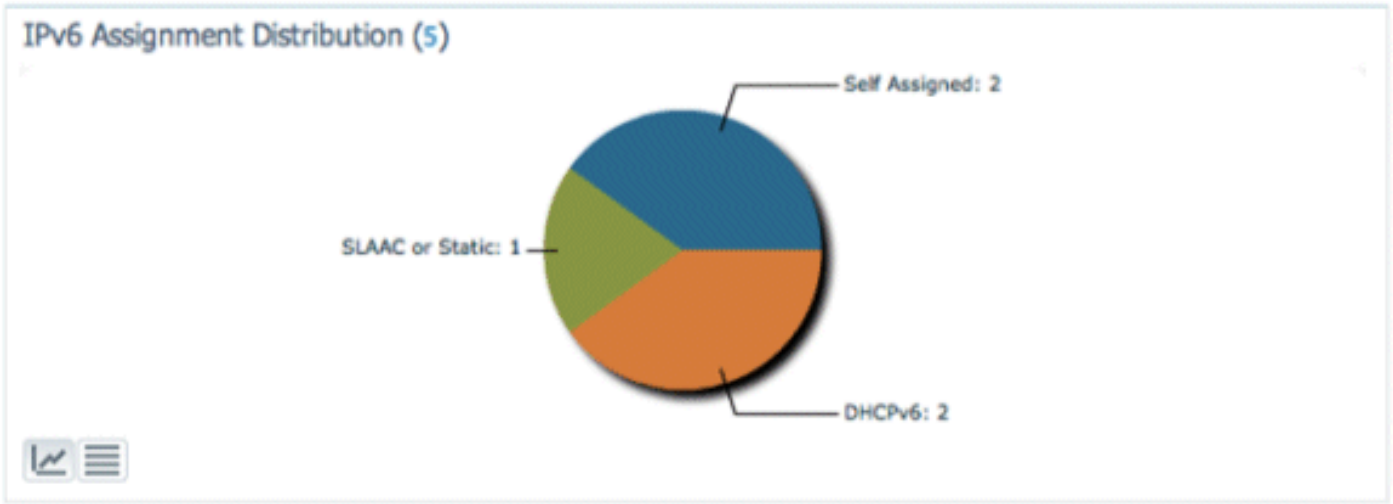
حركة مرور العميل حسب نوع عنوان IP - يعرض حركة مرور البيانات من كل نوع من أنواع العملاء. يتضمن العملاء في فئة المكدس المزدوج حركة مرور بيانات IPv4 و IPv6 على حد سواء:



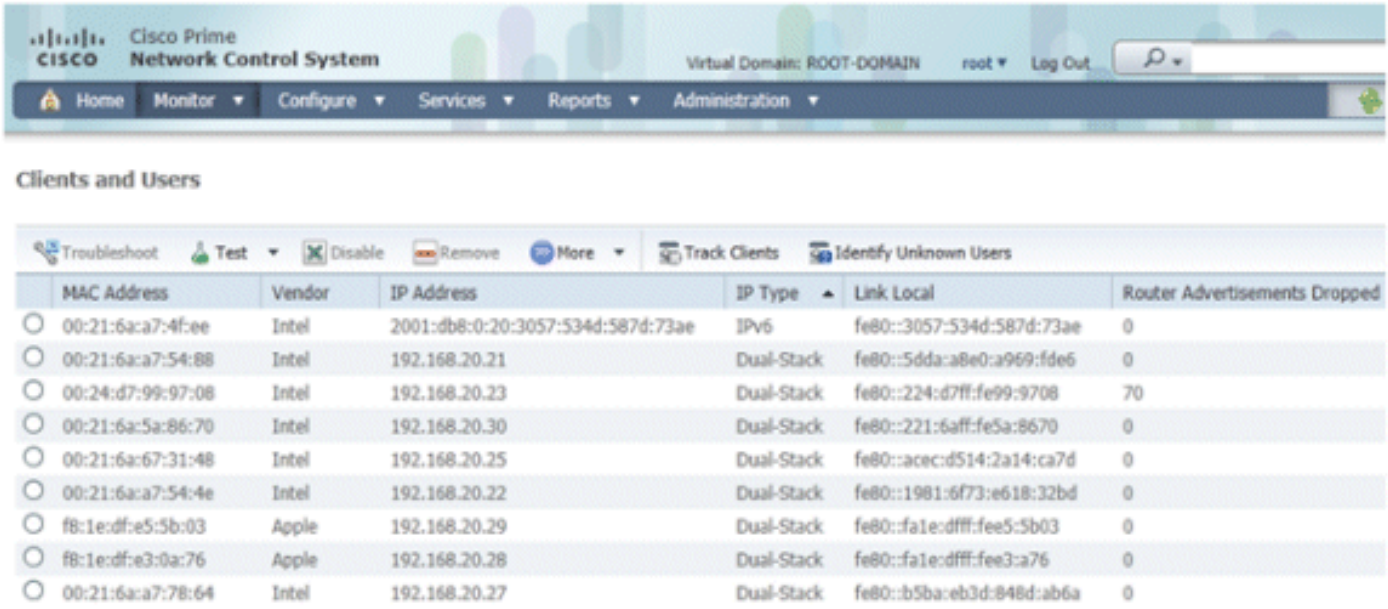
تعيين عنوان IPv6 - يعرض طريقة تعيين العنوان لكل عميل كواحدة من الفئات الأربع التالية:

- DHCPv6 - للعملاء الذين لديهم عناوين تم تعيينها بواسطة خادم مركزي. قد يكون لدى العميل أيضا عنوان SLAAC.
- SLAAC أو STATIC - للعملاء الذين يستخدمون التعيين التلقائي للعنوان عديم الحالة أو باستخدام عناوين تم تكوينها بشكل ثابت.
- غير معروف - في بعض الحالات، لا يمكن اكتشاف تعيين عنوان IPv6.يقع هذا شرط فقط على العملاء السلكيين في NCS بما أن بعض مفتاح لا يتطفل على معلومات تعيين عنوان IPv6.
- مخصص ذاتيا - للعملاء الذين لديهم عنوان إرتباط محلي فقط والذي يكون مكلفا ذاتيا بالكامل.يمكن أن يواجه العملاء في هذه الفئة مشاكل في اتصال IPv6 نظرا لأنهم يفتقرون إلى عنوان فريد عالمي أو محلي.

يمكن النقر فوق كل قسم من أقسام المخطط الدائري، مما يسمح للمسؤول بالتوصيل لأسفل إلى قائمة العملاء.



مراقبة عملاء IPv6



لمراقبة معلومات عميل IPv6 وإدارتها، تمت إضافة هذه الأعمدة إلى صفحة العملاء والمستخدمين:

- نوع IP - نوع العميل استنادا إلى عناوين IP التي تم رؤيتها من العميل. الخيارات المحتملة هي IPv4 أو IPv6 أو ثنائي المكدس الذي يحدد عميلا بكل من عناوين IPv4 و IPv6.
- نوع تعيين IPv6 - يتم الكشف عن طريقة تعيين العنوان بواسطة NCS على أنها إما SLAAC أو Static أو DHCPv6 أو Self-Assign أو غير معروف.
- فريد عمومي - أحدث عنوان عمومي ل IPv6 يتم إستخدامه بواسطة العميل. يكشف تمرير الماوس فوق محتويات العمود عن أي عناوين IPv6 عالمية فريدة إضافية يستخدمها العميل.
- فريد محلي - أحدث عنوان فريد محلي ل IPv6 يتم إستخدامه بواسطة العميل. يكشف الماوس فوق محتويات العمود عن أي عناوين IPv6 عالمية فريدة إضافية يستخدمها العميل.
- الارتباط المحلي - عنوان IPv6 الخاص بالعميل الذي تم تعيينه ذاتيا ويتم إستخدامه للاتصال قبل تعيين أي عنوان IPv6 آخر.
- سقطت إعلانات الموجه - عدد إعلانات الموجه التي تم إرسالها بواسطة العميل وتم إسقاطها في نقطة الوصول. يمكن إستخدام هذا العمود لتعقب العملاء الذين قد يكون تكوينهم غير صحيح أو تم تكوينهم بشكل خبيث ليتصرفوا كموجه IPv6. هذا العمود قابل للفرز، مما يسمح بتعريف العملاء المخالفين بسهولة.

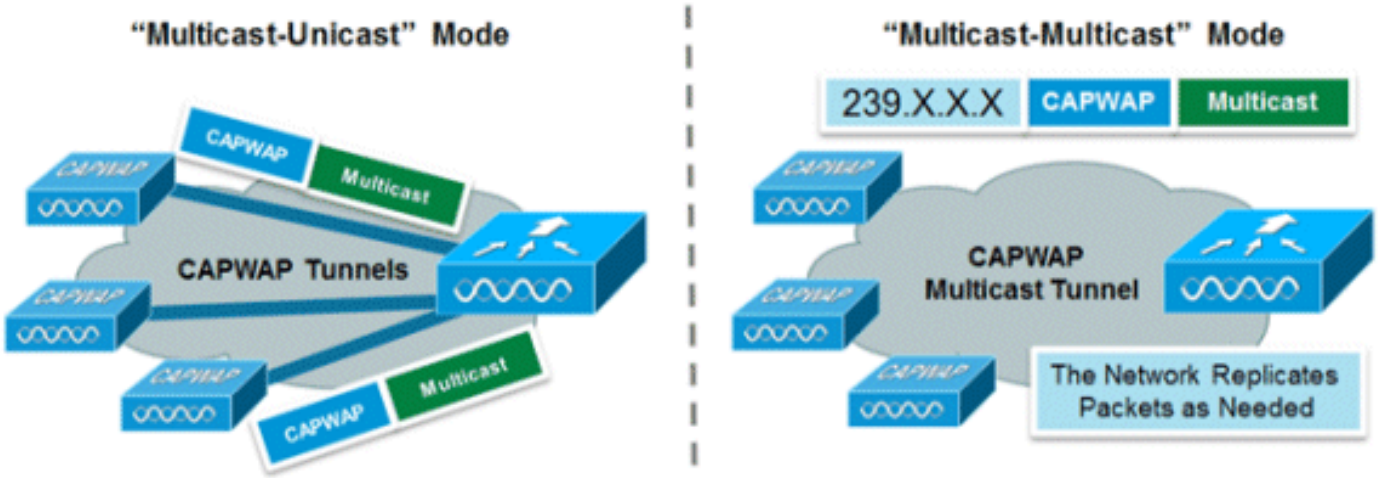
بالإضافة إلى عرض أعمدة IPv6 المحددة، سيظهر عمود عنوان IP عنوان IP الحالي للعميل مع أولوية عرض عنوان IPv4 أولا (في حالة عميل مكدس مزدوج) أو عنوان IPv6 العالمي الفريد في حالة عميل IPv6 فقط.

تكوين دعم عميل IPv6 اللاسلكي

وضع توزيع البث المتعدد إلى APs

تدعم الشبكة اللاسلكية الموحدة من Cisco طريقتين لتوزيع البث المتعدد على نقاط الوصول (APs) المرتبطة بوحدة التحكم. في كلا الوضعين، يتم تضمين حزمة البث المتعدد الأصلية من الشبكة السلكية داخل حزمة CAPWAP من الطبقة 3 يتم إرسالها عبر إما Capwap Unicast أو Multicast إلى نقطة الوصول. بما أن الحركة مرور يكون

CAPWAP يغلف، APs لا ينبغي أن يكون على ال نفسه VLAN بما أن الزبون حركة مرور. تتم مقارنة الطريقتين لتوزيع البث المتعدد هنا:



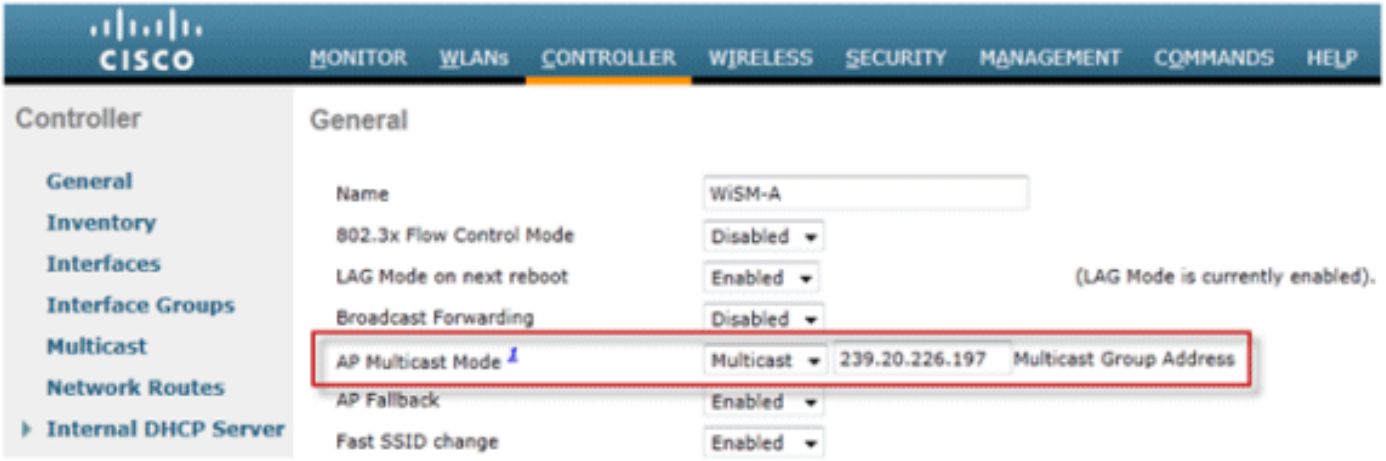
	وضع البث الأحادي المتعدد	وضع البث المتعدد
آلية التسليم	تقوم وحدة التحكم بنسخ حزمة البث المتعدد وإرسالها إلى كل نقطة وصول في نفق Unicast CAPWAP	ترسل وحدة التحكم نسخة واحدة من حزمة البث المتعدد
أوضاع AP المدعومة	تقنية FlexConnect والمحلي	الوضع المحلي فقط
يتطلب توجيه البث المتعدد من المستوى الثالث على الشبكة السلكية	لا	نعم
تحميل وحدة التحكم	عالي	منخفض
تحميل الشبكة السلكية	عالي	منخفض

تكوين وضع توزيع البث المتعدد

وضع البث المتعدد هو الخيار الموصى به لأسباب تتعلق بقابلية التطوير وكفاءة النطاق الترددي السلكي.

ملاحظة: هذه الخطوة مطلوبة بشكل مطلق لوحدة التحكم اللاسلكية من السلسلة 2500 فقط، ولكنها تتيح إمكانية إرسال متعدد البث بشكل أكثر كفاءة، كما يوصى بها لجميع الأنظمة الأساسية لوحدة التحكم.

انتقل إلى علامة التبويب "وحدة التحكم" ضمن الصفحة "عام" وتأكد من تكوين وضع بث AP المتعدد لاستخدام وضع **البث المتعدد** ومن تكوين عنوان مجموعة صالح. عنوان المجموعة عبارة عن مجموعة بث متعدد IPv4 ويوصى بأن يكون في نطاق X.X.X-239.255.255.255.239، وهو نطاق مخصص لتطبيقات البث المتعدد الخاصة.

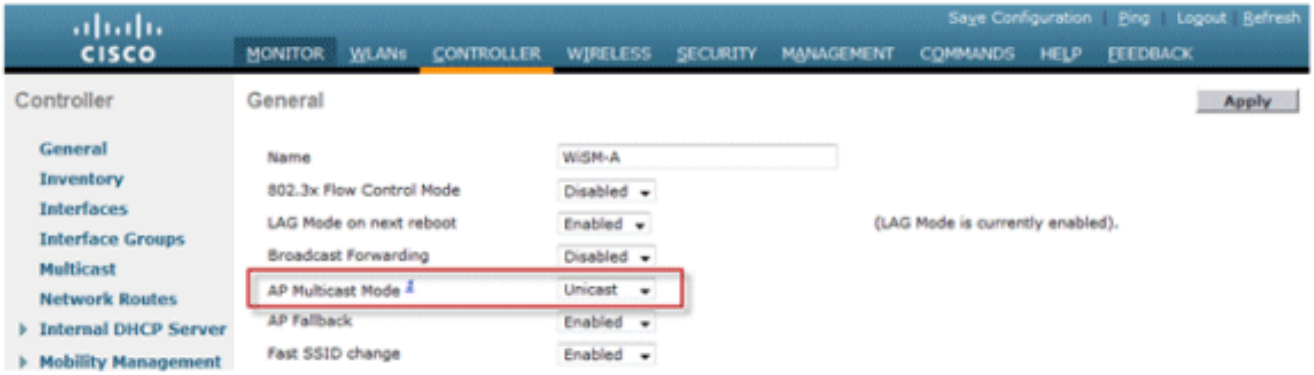


ملاحظة: لا تستخدم نطاقات عنوان x.x.x.224 أو x.239.0.0 أو x.239.128.0 لعنوان مجموعة البث المتعدد. تتداخل العناوين الموجودة في هذه النطاقات مع عناوين MAC المحلية للارتباط وتفيض جميع منافذ المحولات، حتى مع تمكين التطفل على بروتوكول IGMP.

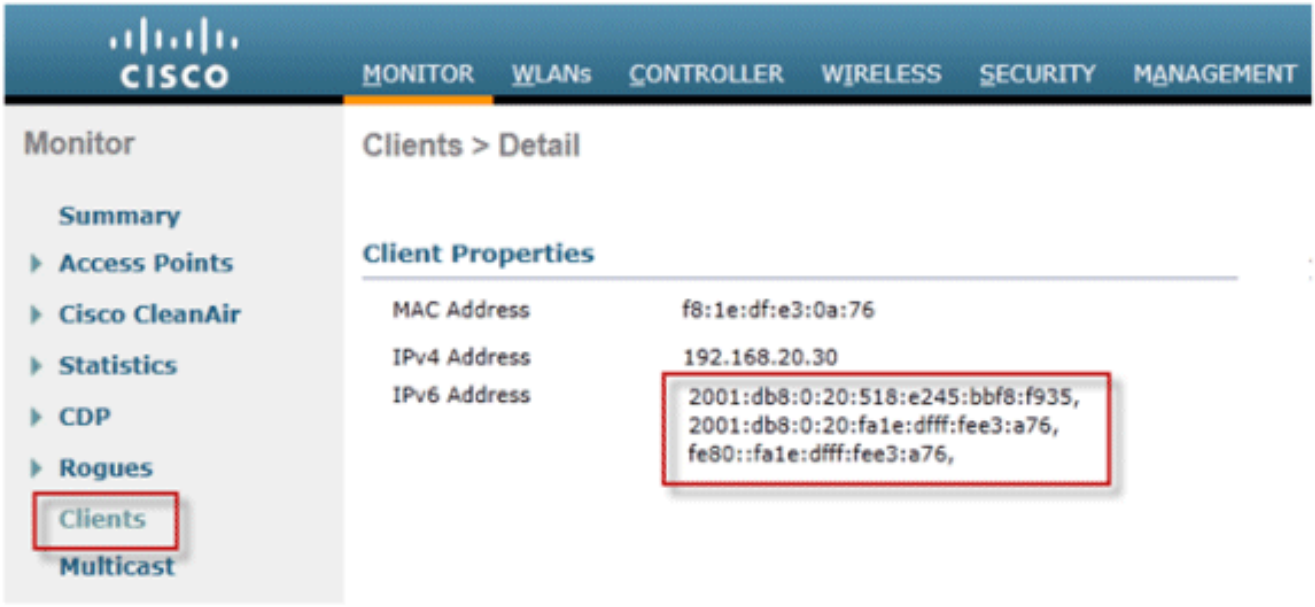
تكوين وضع توزيع البث الأحادي للبث المتعدد

إذا لم يتم تكوين الشبكة السلكية بشكل صحيح لتقديم البث المتعدد CAPWAP بين وحدة التحكم ووضع AP أو وضع FlexConnect، وسيتم إستخدام نقاط الوصول لشبكات WLAN المحولة مركزيا التي تدعم IPv6، حينئذ يلزم وضع البث الأحادي.

1. انتقل إلى علامة التبويب **وحدة التحكم** أسفل الصفحة العامة، وتأكد من تكوين وضع البث المتعدد لنقطة الوصول لاستخدام وضع **البث الأحادي**.



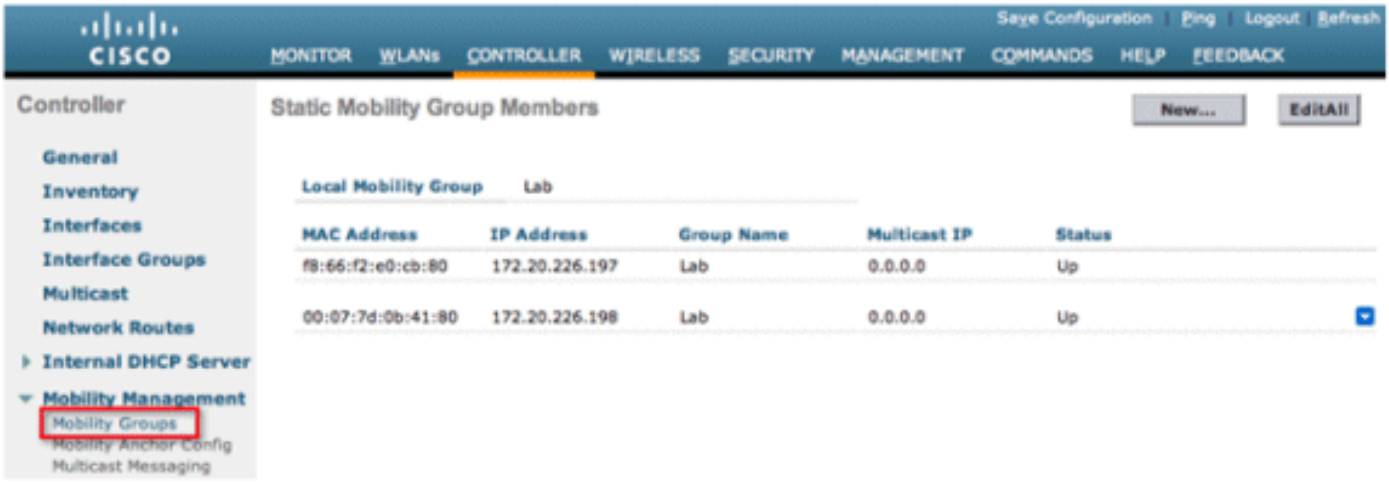
2. توصيل عميل قادر على بروتوكول IPv6 بالشبكة المحلية اللاسلكية. تحقق من أن العميل يتلقى عنوان IPv6 بالانتقال إلى علامة التبويب **مراقبة** ثم إلى القائمة **العملاء**.



تكوين قابلية تنقل IPv6

لا يوجد تكوين محدد لحركة IPv6 باستثناء وضع وحدات التحكم في نفس مجموعة التنقل أو داخل نفس مجال التنقل. وهذا يسمح لما يصل إلى إجمالي 72 وحدة تحكم بالمشاركة في مجال قابلية التنقل الذي يوفر إمكانية تنقل تتسم بالسلاسة حتى لأكبر المجمعات.

انتقل إلى علامة التبويب **وحدة التحكم > مجموعات التنقل**، وأضف كل وحدة تحكم بواسطة عنوان MAC وعنوان IP في المجموعة. يجب القيام بذلك على جميع وحدات التحكم في مجموعة التنقل.

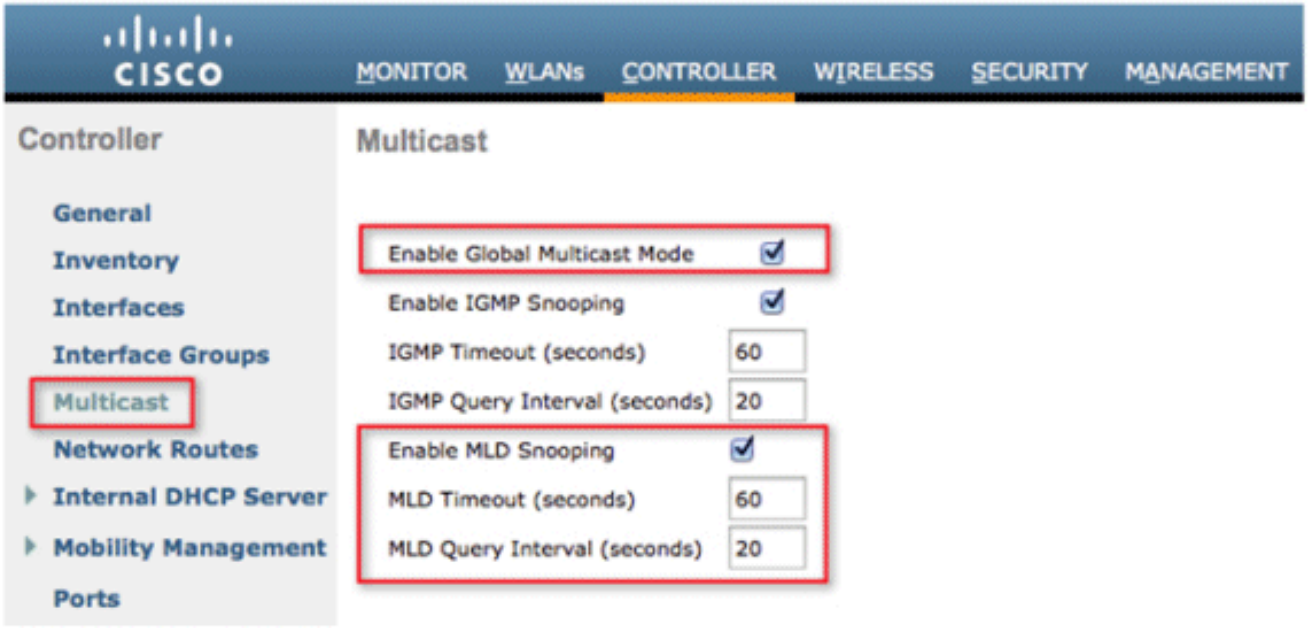


تكوين البث المتعدد ل IPv6

تدعم وحدة التحكم التطفل على بروتوكول MLDv1 للبث المتعدد ل IPv6 الذي يسمح لها بتعقب تدفقات البث المتعدد وتوفيرها بذكاء للعملاء الذين يطلبون هذه التدفقات.

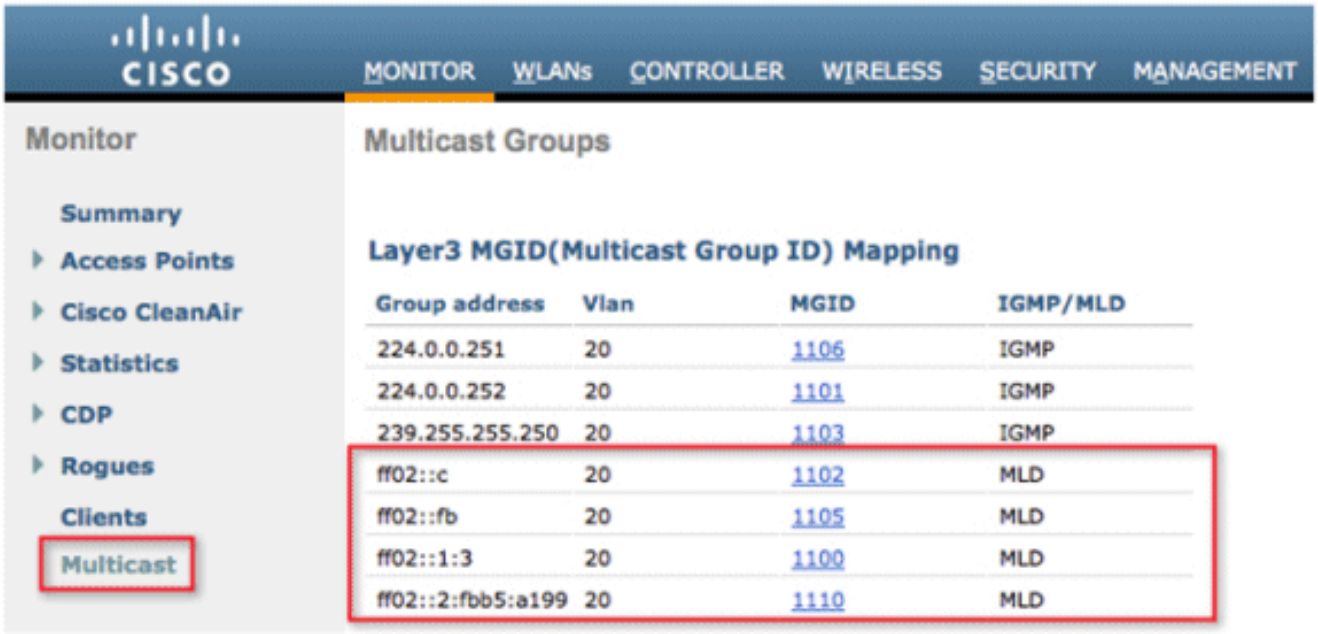
ملاحظة: على عكس الإصدارات السابقة من الإصدارات، لا يصرح دعم حركة مرور البث الأحادي ل IPv6 بتمكين "وضع البث المتعدد العام" على وحدة التحكم. يتم تمكين دعم حركة مرور البث الأحادي IPv6 تلقائيا.

1. انتقل إلى صفحة **وحدة التحكم > البث المتعدد** و**تمكين التطفل على بروتوكول MLD** لدعم حركة مرور IPv6 للبث المتعدد. من أجل تمكين البث المتعدد ل IPv6، يجب تمكين **وضع البث المتعدد العام** لوحدة التحكم أيضا.



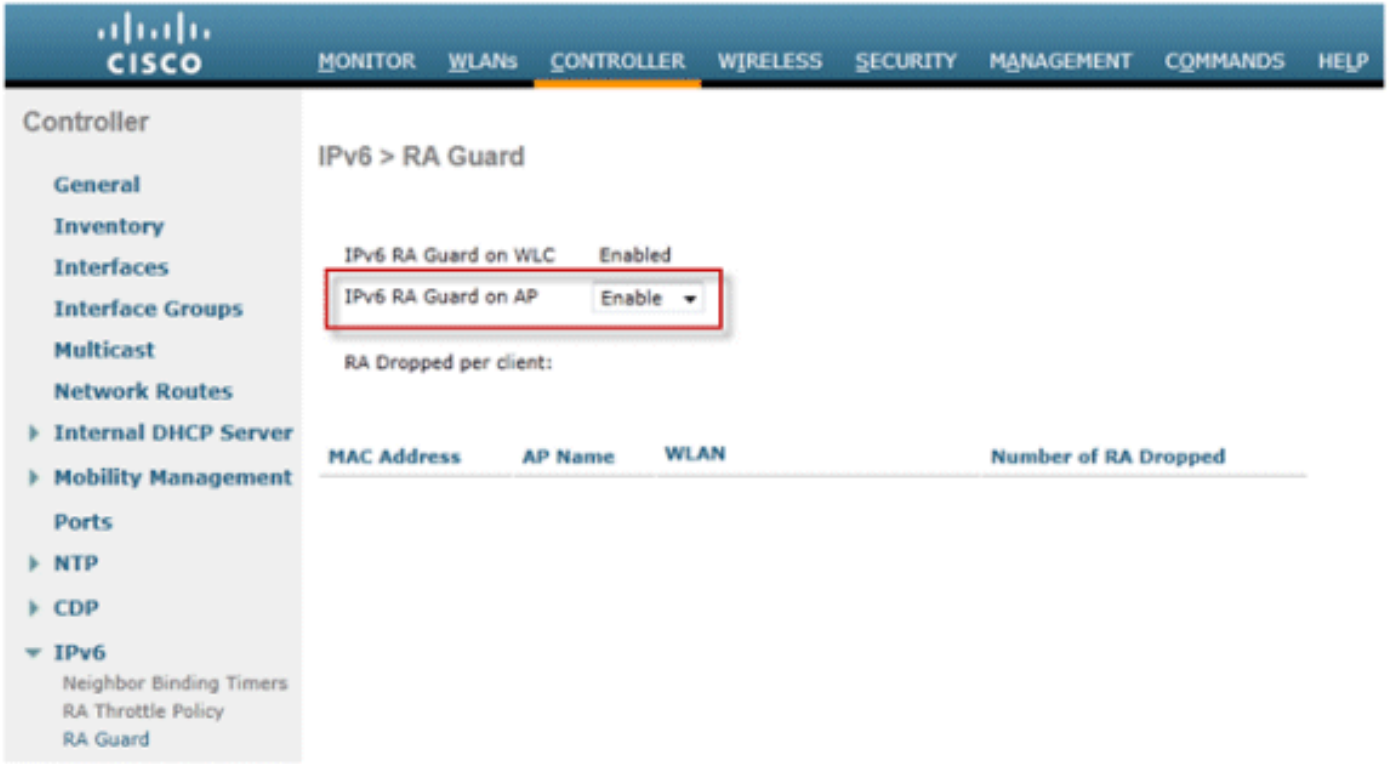
ملاحظة: يجب تمكين التطفل على وضع البث المتعدد العام و IGMP و MLD إذا كانت تطبيقات اكتشاف النظير إلى النظير مثل Apple's Bonjour مطلوبة.

2. للتحقق من أنه يتم حاليا التطفل على حركة مرور البث المتعدد ل IPv6، انتقل إلى صفحة **المراقبة** و صفحة **البث المتعدد**. لاحظ أنه يتم سرد كل من مجموعات البث المتعدد ل IGMP) IPv4) و MLD) IPv6). انقر فوق MGID لعرض العملاء اللاسلكيين المنضمين إلى عنوان هذه المجموعة.



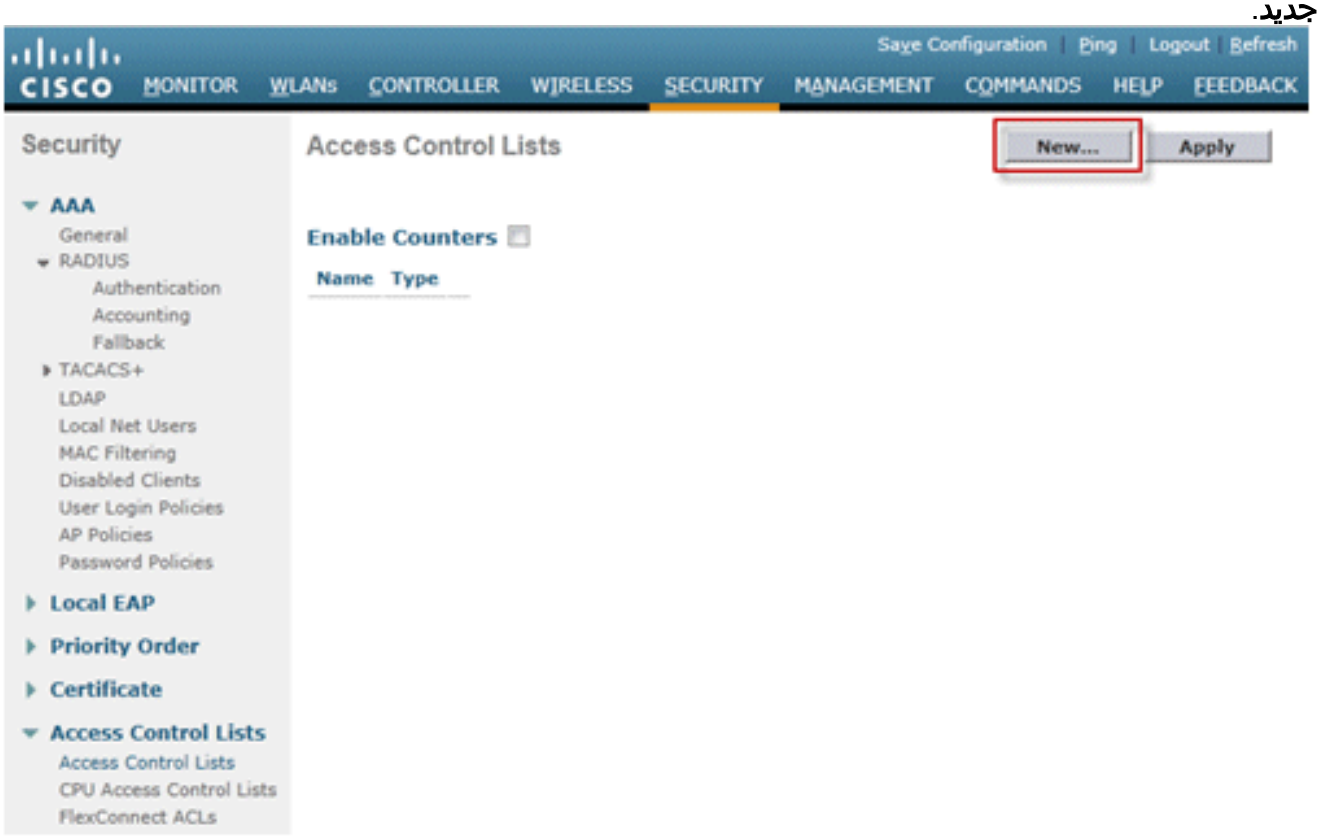
تكوين واقي IPv6 RA

انتقل إلى علامة التبويب **وحدة التحكم** ثم **IPv6 > واقي RA** في القائمة اليسرى. **تمكين** حماية IPv6 RA على AP. لا يمكن تعطيل واقي RA على وحدة التحكم. بالإضافة إلى تكوين حارس RA، تعرض هذه الصفحة أيضا أي عملاء تم تعريفهم على أنهم يرسلون RAs.



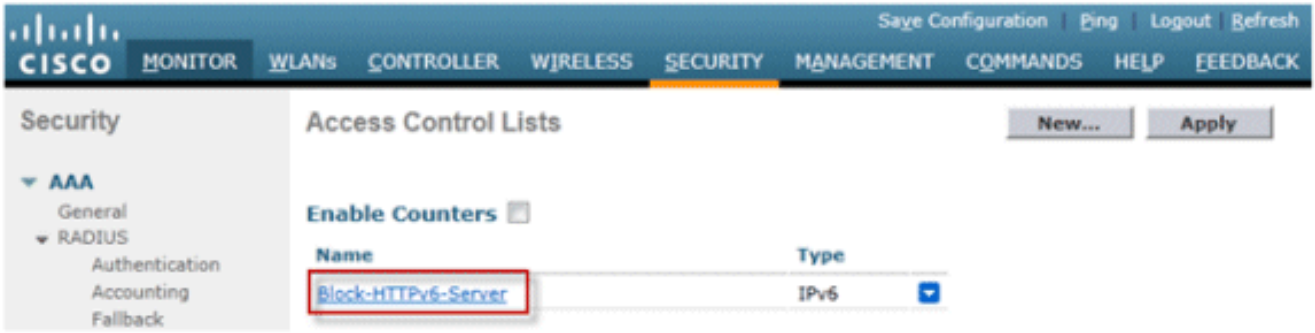
تكوين قوائم التحكم في الوصول إلى IPv6

1. انتقل إلى علامة التبويب **الأمان**، وافتح **قوائم التحكم في الوصول**، وانقر فوق **جديد**.

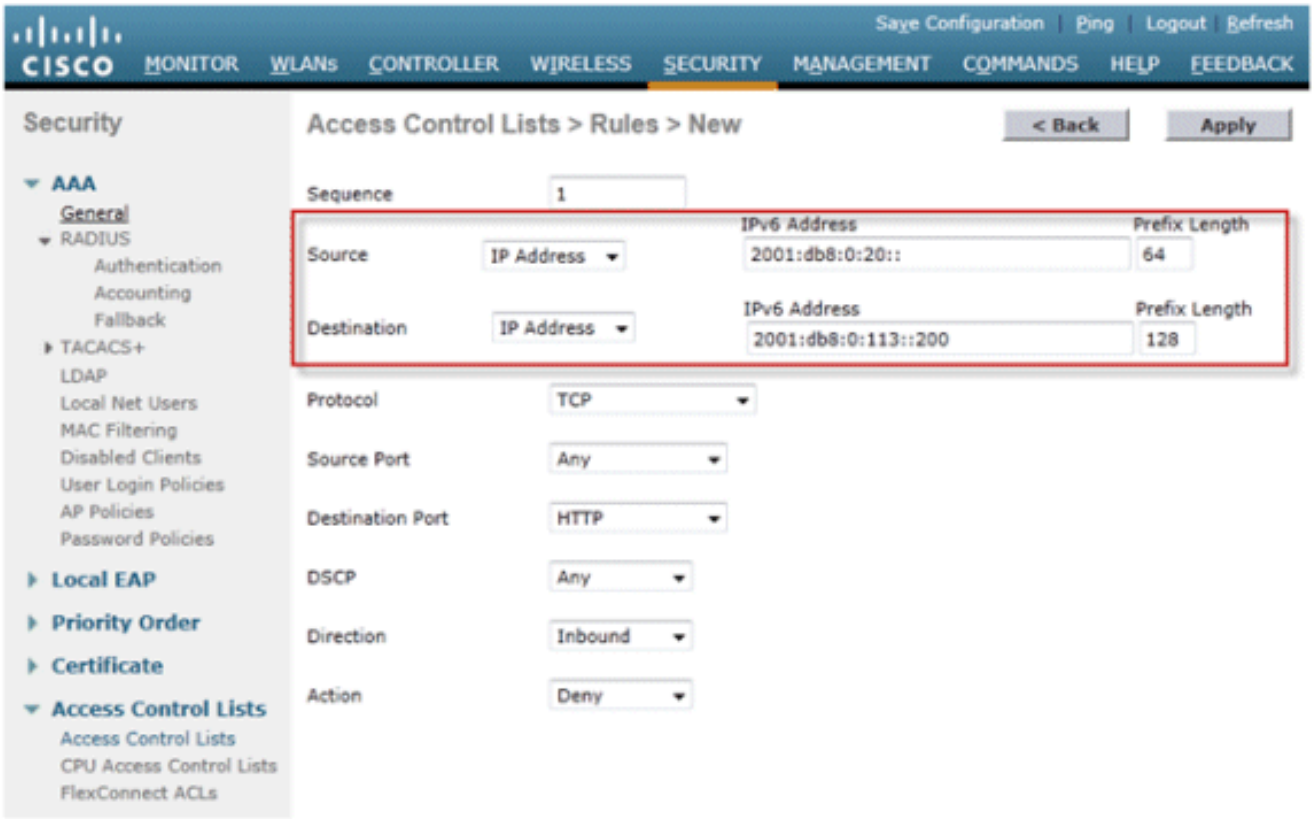


2. أدخل اسما فريدا لقائمة التحكم في الوصول (ACL)، وقم بتغيير نوع قائمة التحكم في الوصول إلى **IPv6**، وانقر فوق **تطبيق**.

3. انقر فوق قائمة التحكم في الوصول (ACL) الجديدة التي تم إنشاؤها في الخطوات أعلاه.

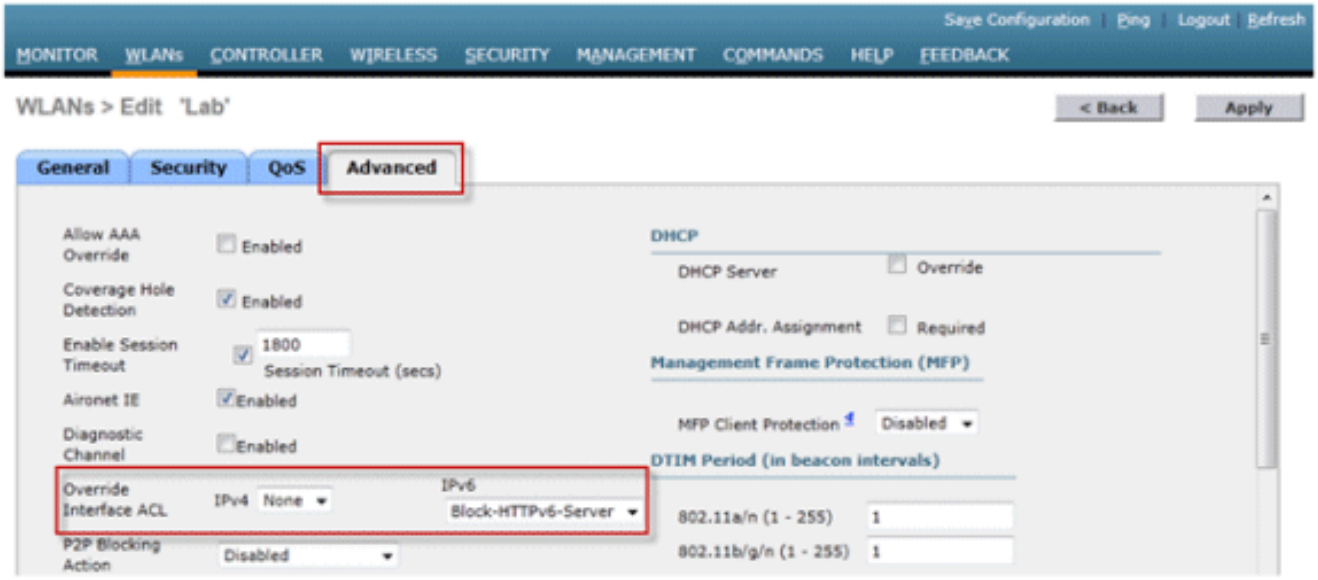


4. انقر فوق **إضافة قاعدة جديدة**، وأدخل المعلمات المطلوبة للقاعدة، ثم انقر فوق **تطبيق**. أترك رقم التسلسل فارغا لوضع القاعدة في نهاية القائمة. يتم إستخدام الخيار "الإتجاه" الخاص ب "الوارد" لحركة المرور الواردة من الشبكة اللاسلكية و"الصادر" لحركة المرور الموجهة للعملاء اللاسلكيين. تذكر، القاعدة الأخيرة في قائمة التحكم في الوصول (ACL) هي رفض كلي ضمني. أستخدم طول البادئة 64 لمطابقة شبكة IPv6 الفرعية بأكملها، وطول البادئة 128 لتقييد الوصول إلى عنوان فردي بشكل فريد.



5. يتم تطبيق قوائم التحكم في الوصول (ACL) إلى IPv6 على أساس كل شبكة محلية لاسلكية (WLAN)/SSID ويمكن إستخدامها على شبكات محلية لاسلكية (WLAN) متعددة في نفس الوقت. انتقل إلى علامة التبويب **شبكات WLAN** وانقر فوق معرف شبكة WLAN الخاص بمعرف SSID المعني لتطبيق قائمة التحكم في الوصول (ACL) الخاصة ب IPv6. انقر فوق علامة التبويب **خيارات متقدمة** وقم بتغيير قائمة التحكم في الوصول

الخاصة بواجهة التجاوز ل IPv6 إلى اسم قائمة التحكم في الوصول (ACL).

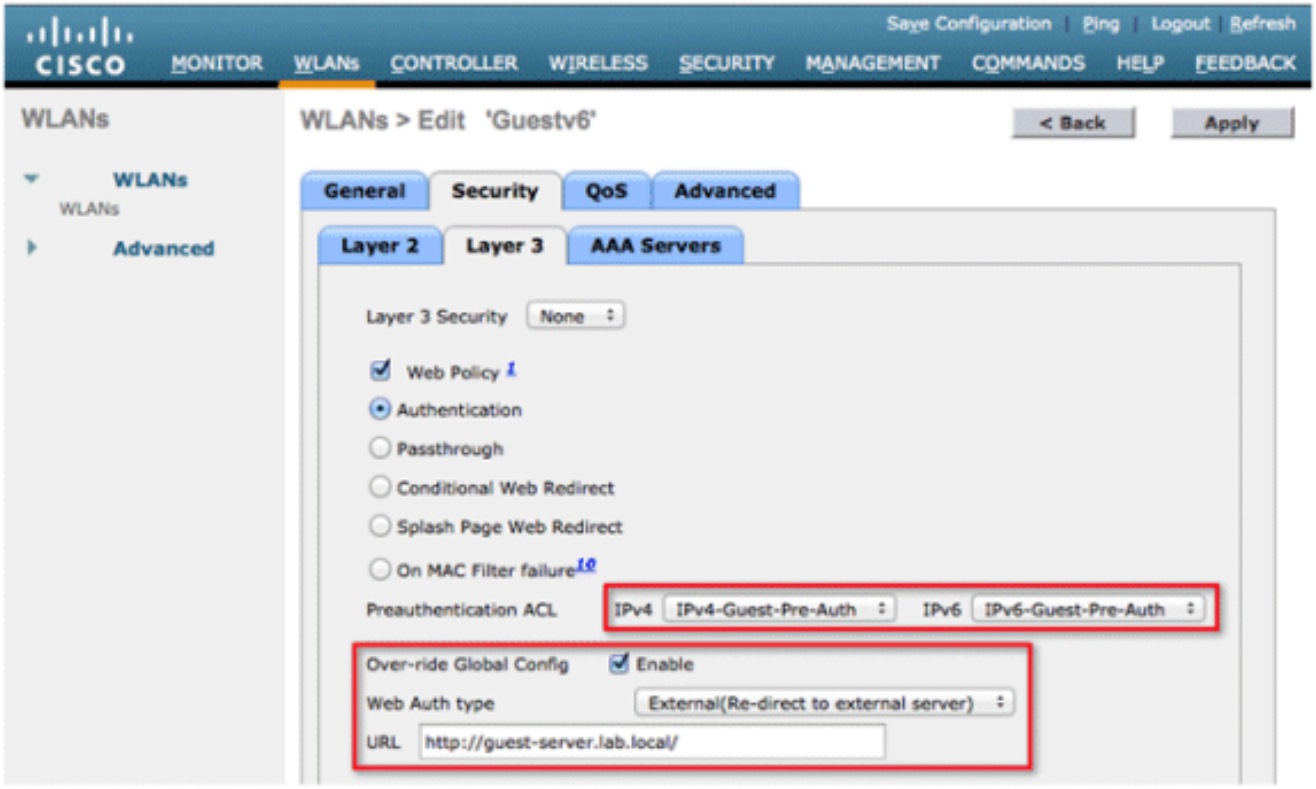


تكوين وصول ضيف IPv6 لمصادقة الويب الخارجية

1. تكوين قائمة التحكم في الوصول للمصادقة المسبقة ل IPv4 و IPv6 لخادم الويب. وهذا يسمح بحركة المرور من وإلى الخادم الخارجي قبل مصادقة العميل بالكامل.

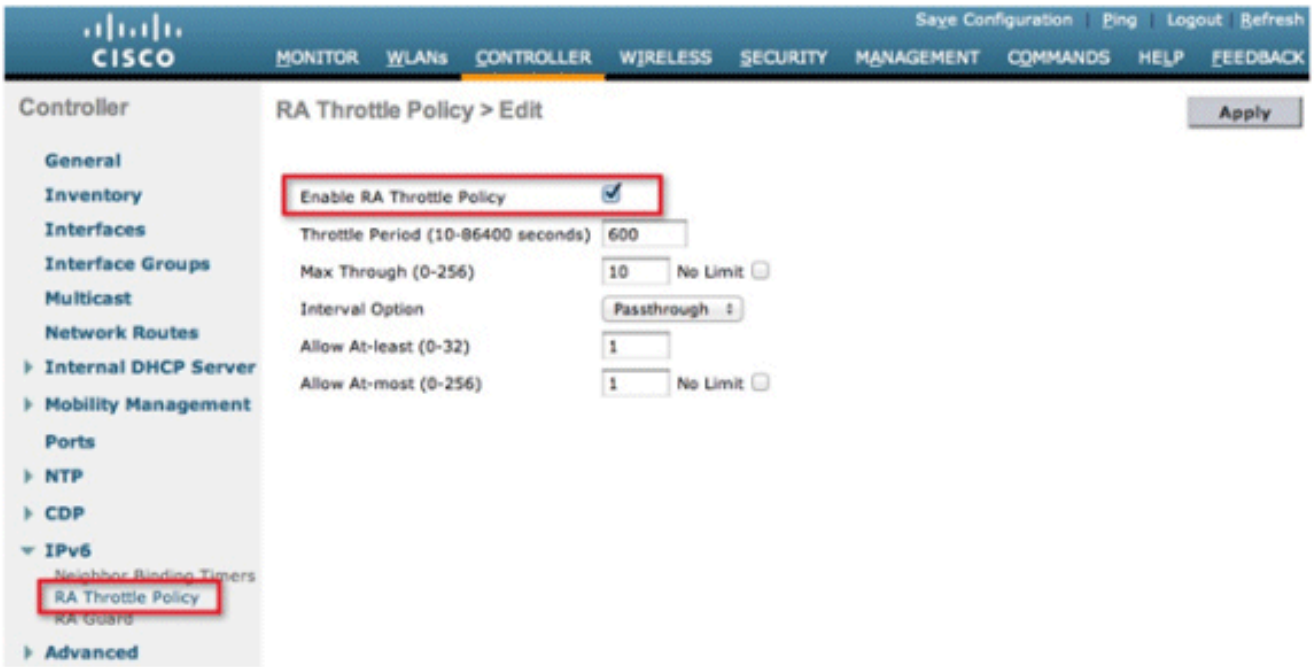
لمزيد من المعلومات حول عملية الوصول إلى الويب الخارجي، ارجع إلى مصادقة الويب الخارجية باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية.

2. قم بتكوين شبكة WLAN الضيف بالتصفح إلى علامة التبويب WLANs في الأعلى. قم بإنشاء SSID للضيف واستخدم نهج ويب للطبقة 3. يتم تحديد قوائم التحكم في الوصول (ACL) السابقة للمصادقة المحددة في الخطوة 1 ل IPv4 و IPv6. حدد قسم التكوين العام الذي تم تجاوزه وحدد **خارجي** من المربع المنسدل نوع مصادقة الويب. أدخل عنوان URL الخاص بخادم ويب. يجب أن يكون اسم المضيف للخادم الخارجي قابلا للحل في IPv4 و IPv6 DNS.



تكوين التحكم في IPv6 RA

1. انتقل إلى قائمة المستوى الأعلى **لوحدة التحكم** وانقر فوق **IPv6 > خيار سياسة تقييد حركة المرور (RA)** على الجانب الأيسر. تمكين تقييد RA بالنقر فوق خانة الاختيار.



ملاحظة: عند حدوث تقييد RA، يتم السماح بالموجه الأول القادر على بروتوكول IPv6 فقط من خلال. بالنسبة للشبكات ذات بادئات IPv6 المتعددة التي يتم تقديمها بواسطة موجهات مختلفة، يجب تعطيل تقييد RA.

2. قم بضبط فترة الكبح والخيارات الأخرى فقط بموجب نصيحة من TAC. ومع ذلك، يوصى بإجراء الافتراضي لمعظم عمليات النشر. يجب تعديل خيارات التكوين المختلفة لسياسة تقييد الوصول عن بعد (RA) مع مراعاة هذا الأمر:يجب أن تكون القيم العددية ل "السماح على الأقل" أقل من "السماح على الأكثر" والتي يجب أن تكون أقل من "الحد الأقصى من خلال".يجب ألا تستخدم سياسة تقييد الوصول (RA) فترة كبح تزيد عن 1800 ثانية لأن هذه هي مدة الحياة الافتراضية لمعظم RAs.

ويرد أدناه وصف لكل خيار من خيارات تقييد القدرة على التحمل:

- فترة الكبح - الفترة الزمنية التي يحدث فيها الاختناق. يسري تقييد RA فقط بعد الوصول إلى حد "Max Through" لشبكة VLAN.
- الحد الأقصى للخلال - هذا هو الحد الأقصى لعدد نقاط الوصول عن بعد (RAs) لكل شبكة محلية ظاهرية (VLAN) قبل تحريك الارتباطات التشعيبية. يتيح خيار "لا حدود" الحصول على كمية غير محدودة من RAs من دون تقييد.
- خيار الفاصل الزمني - يسمح خيار الفاصل الزمني لوحدة التحكم بالعمل بشكل مختلف استنادا إلى قيمة RFC 3775 المحددة في IPv6 RA.المرور - تسمح هذه القيمة لأي نقاط وصول (RAs) باستخدام خيار الفاصل الزمني RFC3775 بالمرور بدون التحكم.تجاهل - ستتسبب هذه القيمة في قيام جهاز تحكم RA بمعالجة الحزم باستخدام خيار الفاصل الزمني كقيمة RA عادية وخاضعا للتقييد إذا كان ساري المفعول.كبح - ستتسبب هذه القيمة في أن تخضع دائما RAs التي تحتوي على خيار الفاصل الزمني لتحديد المعدل.
- السماح على الأقل - الحد الأدنى لعدد RAs لكل موجه الذي سيتم إرساله كبث متعدد.
- Allow At (السماح على الأكثر) - الحد الأقصى لعدد RAs لكل موجه الذي سيتم إرساله كبث متعدد قبل أن يصبح التقييد نافذ المفعول. سيتيح خيار "لا حد" عدد غير محدود من نقاط الوصول عن بعد (RA) من خلال هذا الموجه.

تكوين جدول ربط IPv6 المجاور

1. انتقل إلى قائمة المستوى الأعلى لوحدة التحكم وانقر فوق **IPv6 > مؤقتات الربط المجاورة** في القائمة اليسرى.

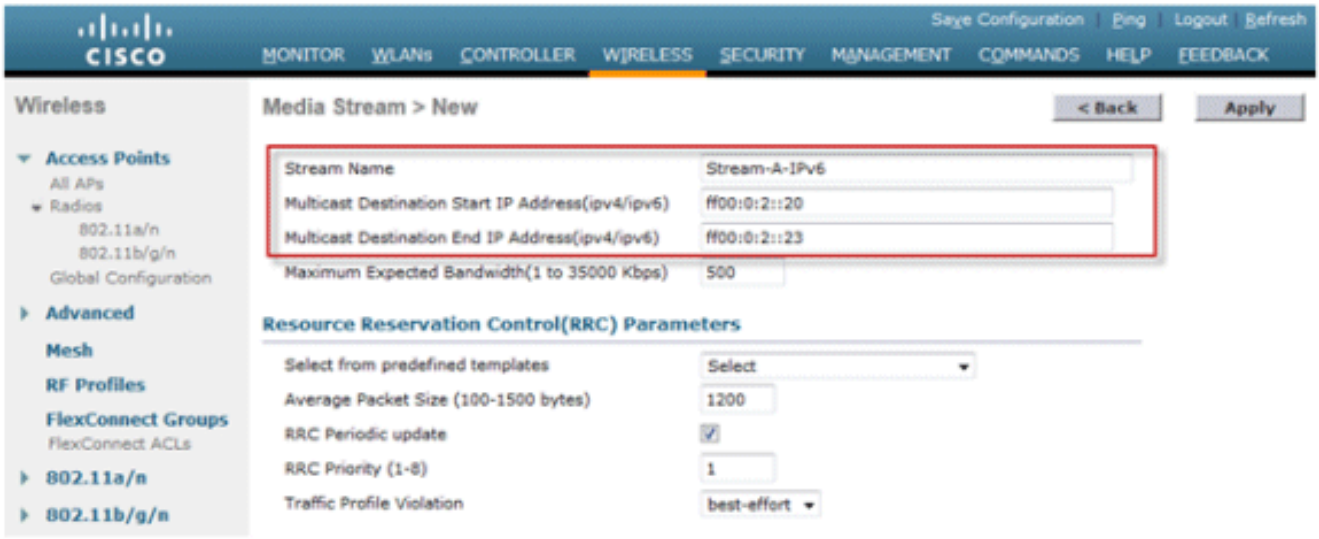
2. تعديل العمر الافتراضي، العمر الذي يمكن الوصول إليه، والعمر المتدني حسب الحاجة. بالنسبة لعمليات النشر مع العملاء كثيري التنقل، يجب تغيير وحدات التوقيت الخاصة بمؤقت العنوان غير المتزامن. القيم الموصى بها هي:عمر افتراضي أقل - 30 ثانيةالعمر الافتراضي القابل للوصول - 300 ثانيةعمر الولاية - 86400 ثانيةيشير كل مؤقت مدى الحياة إلى الحالة التي يمكن أن يكون فيها عنوان IPv6:**مدة البقاء** - يحدد المؤقت المؤقت للأسفل المدة التي يجب خلالها الاحتفاظ بإدخالات ذاكرة التخزين المؤقت ل IPv6 في حالة تعطل واجهة وصلة وحدة التحكم.**العمر الافتراضي القابل للوصول** - يحدد هذا المؤقت المدة التي سيتم خلالها وضع علامة نشط على عنوان IPv6 مما يعني أنه قد تم تلقي حركة مرور البيانات من هذا العنوان مؤخرا. بمجرد انتهاء صلاحية المؤقت هذا، يتم نقل العنوان إلى حالة "Stale".**العمر الافتراضي** - يحدد هذا المؤقت المدة اللازمة للاحتفاظ بعناوين IPv6 في ذاكرة التخزين المؤقت التي لم يتم رؤيتها خلال "العمر الافتراضي القابل للوصول". بعد مدة البقاء هذه، تتم إزالة العنوان من جدول الربط.

تكوين دفق فيديو IPv6

1. تأكد من تمكين ميزات VideoStream العامة على وحدة التحكم. ارجع إلى حل الشبكة اللاسلكية الموحدة من Cisco: دليل نشر VideoStream للحصول على معلومات حول تمكين VideoStream على شبكة 802.11a/g/n بالإضافة إلى WLAN SSID.
2. انتقل إلى علامة التبويب **لاسلكي** في وحدة التحكم، وفي القائمة اليسرى، أختر **تدفق الوسائط** > **التدفقات**. انقر

فوق **إضافة جديد** لإنشاء دفق جديد.

3. قم بتسمية الدفق وأدخل عنواني البدء والنهاية IPv6. عند إستخدام تدفق واحد فقط، تكون عناوين البداية والنهاية متساوية. بعد إضافة العناوين، انقر فوق **تطبيق** لإنشاء الدفق.



أستكشاف أخطاء اتصال عميل IPv6 وإصلاحها

يتعذر على بعض العملاء تمرير حركة مرور IPv6

لا تقوم بعض عمليات تنفيذ مكدس شبكات IPv6 العميل بالإعلان عن نفسها بشكل صحيح عند الدخول إلى الشبكة، وبالتالي لا يقوم جهاز التحكم بتطفل عنوانها بشكل مناسب لوضعها في جدول الربط المجاور. يتم حظر أي عناوين غير موجودة في جدول الربط المجاور وفقا لميزة واقي مصدر IPv6. للسماح لهؤلاء العملاء بتمرير حركة المرور، يلزم تكوين هذه الخيارات:

1. تعطيل ميزة واقي مصدر IPv6 من خلال CLI (واجهة سطر الأوامر):

```
config network ip-mac-binding disable
```

2. تمكين إعادة توجيه طلب الإرسال المجاور للبث المتعدد من خلال CLI (واجهة سطر الأوامر):

config ipv6 ns-mcast-fwd enable

التحقق من نجاح تجوال الطبقة 3 لعميل IPv6:

أصدرت هذا **يضبط** أمر على على حد سواء المرسى وجهاز تحكم خارجي:

debug client

debug mobility handoff enable

debug mobility packet enable

نتائج تصحيح الأخطاء على وحدة التحكم في الإرساء:

```
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Complete to
                                                        Mobility-Incomplete
                00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Setting handles to 0x00000000
= 00:21:6a:a7:4f:ee pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE
                                                                          .0
             00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Deleted mobile LWAPP rule on AP
                                                        [fe:7f:49:03:30:04]
  00:21:6a:a7:4f:ee Updated location for station old AP 04:fe:7f:49:03:30-1, new
                                                     AP 00:00:00:00:00:00-0
          (00:21:6a:a7:4f:ee Stopping deletion of Mobile Station: (callerId: 42
    00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
 Mobility-Complete, mobility role=Anchor, client state=APF_MS_STATE_ASSOCIATED
 (00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20
       00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
   00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Adding Fast Path rule type = Airespace AP
             Client on AP 00:00:00:00:00:00, slot 0, interface = 13, QOS = 0
                                        ,IPv4 ACL ID = 255, IPv6 ACL ID = 255
 = 00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP
     TokenID = 7006  Local Bridging Vlan = 20, Local Bridging intf id = 13 ,0
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
                                                     (IPv6 ACL ID 255 ,255
                                  .00:21:6a:a7:4f:ee 0.0.0.0 Removed NPU entry
    00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
                                                              Anchor role
             00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1
  00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
                    !! MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS
  00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
                    !! MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS
             00:21:6a:a7:4f:ee 0.0.0.0, VLAN Id 20 Not sending gratuitous ARP
       00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:0, apMac 0x0:0:0:0:0:0
            00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:0 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
                                        w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x5
                                    statuscode 0, reasoncode 99, status 3
                                         00:21:6a:a7:4f:ee Copy CCX LOCP 4
```

```
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:2, anchorip:0xac14e2c6
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
```

نتائج تصحيح الأخطاء على وحدة التحكم الخارجية:

```
(00:21:6a:a7:4f:ee Adding mobile on LWAPP AP f0:25:72:3c:0f:20(1
00:21:6a:a7:4f:ee Reassociation received from mobile on AP f0:25:72:3c:0f:20
<=== (00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255
(none' (ACL ID 255) --- (caller apf_policy.c:1697'
<=== (00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255
(none' (ACL ID 255) --- (caller apf_policy.c:1864'
00:21:6a:a7:4f:ee Applying site-specific Local Bridging override for station
'00:21:6a:a7:4f:ee - vapId 3, site 'default-group', interface 'client-b1
00:21:6a:a7:4f:ee Applying Local Bridging Interface Policy for station
'00:21:6a:a7:4f:ee - vlan 25, interface id 12, interface 'client-b1
00:21:6a:a7:4f:ee processSsidIE  statusCode is 0 and status is 0
00:21:6a:a7:4f:ee processSsidIE  ssid_done_flag is 0 finish_flag is 0
00:21:6a:a7:4f:ee STA - rates (8): 140 18 152 36 176 72 96 108 0 0 0 0 0 0 0 0
apfMsConnTask_4: Jan 22 20:37:45.370: 00:21:6a:a7:4f:ee suppRates  statusCode*
is 0 and gotSuppRatesElement is 1
00:21:6a:a7:4f:ee Processing RSN IE type 48, length 22 for mobile
00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Initializing policy
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state
(AUTHCHECK (2
00:21:6a:a7:4f:ee 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last
(state 8021X_REQD (3
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) DHCP Not required on AP
f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP
f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee apfMsAssoStateInc
00:21:6a:a7:4f:ee apfPemAddUser2 (apf_policy.c:268) Changing state for mobile
00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Idle to Associated
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 49) in 1800
seconds
00:21:6a:a7:4f:ee Sending Assoc Response to station on BSSID f0:25:72:3c:0f:20
status 0) ApVapId 3 Slot 1)
00:21:6a:a7:4f:ee apfProcessAssocReq (apf_80211.c:6290) Changing state for
mobile 00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Associated to Associated
<…SNIP…>
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last
(state L2AUTHCOMPLETE (4
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not required on AP
f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP
f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last
(state DHCP_REQD (7
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 5253, Adding TMP rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
type = Airespace AP - Learn IP address
on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
IPv4 ACL ID = 255, IP
,00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0
= DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id
12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
(ACL ID 255, IPv6 ACL ID 255
```

00:21:6a:a7:4f:ee Stopping retransmission timer for mobile 00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Sent an XID frame
00:21:6a:a7:4f:ee Username entry () already exists in name table, length = 253
00:21:6a:a7:4f:ee Username entry () created in mscb for mobile, length = 253
- 00:21:6a:a7:4f:ee Applying post-handoff policy for station 00:21:6a:a7:4f:ee valid mask 0x1000
00:21:6a:a7:4f:ee QOS Level: -1, DSCP: -1, dot1p: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
:00:21:6a:a7:4f:ee Session: -1, User session: -1, User elapsed -1 Interface :N/A, IPv4 ACL: N/A, IPv6 ACL
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to DHCP_REQD (7) last state (DHCP_REQD (7
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemCreateMobilityState 6370, Adding TMP rule
= 00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule type
= Airespace AP - Learn IP address on AP f0:25:72:3c:0f:20, slot 1, interface ,QOS = 0 IPv4 ACL ID = 255 ,13
,00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0
= DSCP = 0, TokenID = 7006 Local Bridging Vlan = 25, Local Bridging intf id 12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4 (ACL ID 255, IPv6 ACL ID 255
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station: (callerId: 55) in 1800 seconds
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and !! MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS
00:21:6a:a7:4f:ee apfMsRunStateInc
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 5776
(00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and !! MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to Mobility-Complete, mobility role=Foreign, client state=APF_MS_STATE_ASSOCIATED
(00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Replacing Fast Path rule type = Airespace AP Client
on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0 IPv4 ACL ID = 255, IPv6 ACL ID = 25
= 00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP
TokenID = 7006 Local Bridging Vlan = 25, Local Bridging intf id = 12 ,0
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID (IPv6 ACL ID 255 ,255
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in Foreign role
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and !! MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and !! MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS
00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:1, apMac 0xf0:25:72:3c:f:20
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:1 ssid: Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6 w:0x1 aalg:0x0, PMState: RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x7 statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:3, anchorip:0xac14e2c5
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae

00:21:6a:a7:4f:ee Copy IPv6 LOCP: 2001:db8:0:20:3057:534d:587d:73ae

أوامر CLI المفيدة ل IPv6:

Show ipv6 neighbor-binding summary

Debug ipv6 neighbor-binding filter client enable

Debug ipv6 neighbor-binding filter errors enable

الأسئلة المتكررة

س: ما هو الحجم الأمثل لبادئة IPv6 للحد من مجال البث؟

a: على الرغم من إمكانية تقسيم شبكة IPv6 الفرعية إلى شبكات فرعية أسفل /64، إلا أن هذا التكوين سوف يكسر SLAAC ويسبب مشاكل في اتصال العميل. إذا كانت هناك حاجة إلى التجزئة لتقليل عدد البيئات المضيفة، يمكن إستخدام ميزة مجموعات الواجهة لتوازن التحميل بين العملاء بين شبكات VLAN الخلفية الطرفية المختلفة، والتي يستخدم كل منها بادئة IPv6 مختلفة.

س: هل توجد أي قيود على قابلية التوسعة عندما يتعلق الأمر بدعم عملاء IPv6؟

ألف: يتمثل الحد الرئيسي من قابلية التطوير لدعم عميل IPv6 في جدول الربط المجاور الذي يتتبع جميع عناوين IPv6 الخاصة بالعميل اللاسلكي. يتم قياس هذا الجدول لكل نظام أساسي لوحدة التحكم لدعم الحد الأقصى لعدد العملاء مضروبا في ثمانية (الحد الأقصى لعدد العناوين لكل عميل). إن إضافة جدول ربط IPv6 يمكن أن ترفع إستخدام ذاكرة وحدة التحكم بنسبة تتراوح من 10 إلى 15٪ تقريبا تحت الحمل الكامل، وذلك حسب النظام الأساسي.

وحدة التحكم اللاسلكية	الحد الأقصى لعدد العملاء	حجم جدول ربط IPv6 المجاور
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

س: ما هو تأثير ميزات IPv6 على وحدة المعالجة المركزية (CPU) ووحدة الذاكرة الخاصة بوحدة التحكم؟

a: يكون التأثير أقل من ذلك لأن وحدة المعالجة المركزية (CPU) تحتوي على مراكز متعددة لمعالجة مستوى التحكم. عند الاختبار باستخدام الحد الأقصى من الأجهزة العميلة المدعومة، والتي يحتوي كل منها على 8 عناوين IPv6، كان إستخدام وحدة المعالجة المركزية (CPU) أقل من 30٪، وكان إستخدام الذاكرة أقل من 75٪.

س: هل يمكن تعطيل دعم عميل IPv6؟

أ: بالنسبة للعملاء الذين يرغبون في تمكين IPv4 فقط في شبكتهم وحجب IPv6، يمكن إستخدام قائمة تحكم في الوصول (ACL) لبروتوكول IPv6 لحركة مرور رفض كل شيء وتطبيقها على أساس كل شبكة محلية لاسلكية (WLAN).

س: هل من الممكن وجود شبكة محلية لاسلكية (WLAN) واحدة للإصدار الرابع من بروتوكول الإنترنت (IPv4)

وأخرى للإصدار السادس من بروتوكول الإنترنت (IPv6)؟

A: لا يمكن أن يكون لديك نفس اسم SSID ونوع الأمان لشبكتي WLAN مختلفتين تعملان على نقطة الوصول نفسها. لتجزئة عملاء IPv4 من عملاء IPv6، يجب إنشاء شبكتي WLAN. يجب تكوين كل شبكة محلية لاسلكية (WLAN) باستخدام قائمة تحكم في الوصول (ACL) التي تمنع حركة مرور بيانات IPv4 أو IPv6 على التوالي.

س: لماذا يكون من المهم دعم عناوين IPv6 متعددة لكل عميل؟

a: يمكن أن يكون للعملاء عناوين IPv6 متعددة لكل واجهة يمكن أن تكون ثابتة أو SLAAC أو DHCPv6 معينة بالإضافة إلى أن لديهم دائما عنوان محلي-إرتباط معين ذاتيا. يمكن أن يكون للعملاء أيضا عناوين إضافية باستخدام بادئات IPv6 مختلفة.

س: ما هي العناوين الخاصة بالإصدار السادس من بروتوكول الإنترنت (IP) ولماذا تعتبر مهمة لتعقبها؟

أ: يتم إنشاء العناوين الخاصة (المعروفة أيضا بالمؤقتة) عشوائيا بواسطة العميل عندما يكون تعيين عنوان SLAAC قيد الاستخدام. وغالبا ما يتم تدوير هذه العناوين بوتيرة يوم أو نحو ذلك، لمنع إمكانية تعقب المضيف التي قد تأتي من إستخدام نفس البادئة للمضيف (آخر 64 وحدة بت) في جميع الأوقات. من المهم تتبع هذه العناوين الخاصة لأغراض التدقيق مثل تعقب انتهاك حقوق النشر. تقوم Cisco NCS بتسجيل جميع عناوين IPv6 المستخدمة بواسطة كل عميل وتسجيلها تاريخيا في كل مرة يجول فيها العميل أو ينشئ جلسة جديدة. يمكن تكوين هذه السجلات في NCS للاحتجاز لمدة تصل إلى عام.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).