تنفيذ IPv6 في الوصول المعرف بالبرامج

المحتويات

المقدمة

معلومات أساسية

نشر IPv6 باستخدام SD-Access من Cisco

تكوين IPv6 باستخدام مركز بيانات الشبكة القديمة من Cisco

اعتبارات التصميم لـ IPv6 في الوصول إلى Cisco SD

اتصالات العملاء السلكية واللاسلكية وتدفقات المكالمات

تعيين عنوان IPv6 - SLAAC

تعيين عنوان IPv6 - DHCPv6

اتصال IPv6 في Cisco SD-Access

اتصال IPv6 اللاسلكي في وصول SD من Cisco

مضيف نقطة الوصول

مضيف العميل

اتصال العميل-العميل باستخدام IPv6

مصفوفة التبعية

مراقبة مستوى التحكم IPv6

تنفيذ خدمة IPv6 في الوصول إلى Cisco SD

استكشاف أخطاء IPv6 وإصلاحها في Cisco SD-Access

المشكلة المتداولة الرئيسية لتصميم IPv6 مع Cisco SD-Access

المقدمة

يوضح هذا المستند كيفية تنفيذ IPv6 في الوصول المعرف ببرنامج (SD-Access) من ®Cisco.

معلومات أساسية

تم إطلاق IPv4 في عام 1983 وما زال قيد الاستخدام لمعظم حركة مرور الإنترنت. يسمح عنونة IPv4 ذات 32 بت بأكثر من 4 مليارات مجموعة فريدة. ومع ذلك، نظرا لزيادة عدد العملاء المتصلين بالإنترنت، يوجد نقص في عناوين IPv4 الفريدة. وفي تسعينيات القرن العشرين، أصبح استنفاد عنونة الإصدار الرابع من بروتوكول الإنترنت (IPv4) أمرا حتميا. وتحسبا لذلك، قدمت فرقة العمل الهندسية على الإنترنت معيار IPv6. يستخدم IPv6 128 بت ويوفر 340 عنوانا فريدا من عناوين IP غير قابلة للتوسعة، وهو ما يعد أكثر من وحدة تخزين تلبية إحتياجات الأجهزة المتصلة التي تنمو. نظرا لأن الأجهزة الطرفية الأكثر حداثة تدعم المكدس المزدوج و/أو المكدس الأحادي IPv6، فمن المهم للغاية لأي مؤسسة أن تكون جاهزة لتبني IPv6. وهذا يعني أن البنية الأساسية بالكامل يجب أن تكون جاهزة لـ IPv6. يمثل الوصول عبر المحول (SD-Access) من Cisco التطور من تصميمات المجمعات التقليدية إلى الشبكات التي تنفذ بشكل مباشر وجهة نظر المؤسسة. شبكات تعريف برامج Cisco جاهزة الآن للتجميع في مكدس ثنائي (أجهزة IPv6).

ةرادإ IPv6 في أي مؤسسة تواجه التحديات الرئيسية التي تمثل أحد العوائق الرئيسية أمام اعتماد بروتوكول IPv6 على نطاق واسع. تعطي هذه الورقة نظرة عامة على بنية IPv4 القديمة إلى IPv6. تغطي هذه الورقة التغييرات والتعقيدات المرتبطة بترحيل SDN وتقدم ميزة IPv6 على نطاق واسع دعمًا لحلول التركيز الإستراتيجي وتجميع التفاصيل الدقيقة. يجب مراعاة اعتماد بروتوكول IPv6 مع برامج تشغيل Cisco الأساسية من Cisco، والتي تعمل على تشغيل بروتوكول IPv6 في مؤسسة محددة.

في أغسطس 2019، تم إدخال الإصدار 1.3 من مركز بنية الشبكة الرقمية (DNA) من Cisco إلى السوق. في هذا الإصدار، قامت شبكة مجمع Cisco SD-Access بدعم عنوان IP المضيف بدعم من IPv6. يدعم الإصدار 1.3 من مركز DNA بنية الشبكة الفرعية لـ IPv4 وأ IPv6 وأ IPv4v6 من مع العملاء السلكيين واللاسلكيين في المكدس المزدوج. يمكن الحل في التطور المستمر لتوفير ميزات ووظائف جديدة شبكة البنية الفرعية. تعمل بسهولة على دمج بروتوكول IPv6 في أي مؤسسة.

الوصول باستخدام SD-Access من Cisco مع بنية IPv6

توفر تقنية البنية، التي تعد جزءا ال يتجزأ من الوصول إلى البنية الأساسية (SD)، شبكات المجمعات السلكية واللاسلكية مع تغشيات قابلة للبرمجة ومحاكاة افتراضية وأ واحدة شبكة منطقية مما يسمح لشبكة مدام بإضافة شبكة مناطق للشبكة سهلة النشر، أكثر لتلبية هدف التصميم. بالإضافة إلى المحاكاة الافتراضية للشبكات، تعمل تقنية البنية في شبكة مجموعة العمل على تعزيز التحكم في الاتصالات، والتي توفر وضوية المستخدم وتنفيذ السياسات استنادا إلى هوية المجموعة. يعمل حل Cisco SDN بالكامل على DNA الخاص بالنسيج. وبالتالي، من المهم فهم كيفية دعم IPv6 لكل ركيزة من ركائز الحل فيما يتعلق بدعم IPv6.

- Under - تعتمد وظيفة IPv6 لـ Overlay على الأساس حيث تقوم تغشية IPv6 باستخدام عنونة IP المضمنة لـ IPv4 لإنشاء مستوى تحكم بروتوكول لصق المعرف/محدد الموقع (LISP) وإنفاق مستوى بيانات شبكة LAN الموسعة الظاهرية (VXLAN). يمكنك دائما تكوين المكدس المزدوج لبروتوكول التوجيه الأساسي، مجرد LISP الخاص بتغشية التحكم، لاستخدام IPv4.
- التغشية - عندما يتعلق الأمر بالتغشية، يدعم SD-Access الكثير من النطاقات المختلفة لبروتوكول الإنترنت (IP). يتم تضمين حركة مرور IPv6 في الإصدار الرابع من بروتوكول الإنترنت (IPv4) أو شبكة VXLAN داخل بنية SD للوصول إلى نقطة حدود البنية. تعمل نقطة حدود البنية على إزالة كبسلة رأس IPv4 و VXLAN، والتي تتبع عملية توجيه البث الأحادي IPv6 الأصلية من ذلك الحين.
- نقطة مستوى التحكم - يتم تكوين نقطة مستوى التحكم للسماح بتسجيل جميع المضيفين IPv6 و/128 في نطاقات الشبكة الفرعية لمضيف IPv6 داخل قاعدة بيانات التعيين الخاصة بها.
- العقدة الحدودية - على العقدة الحدودية، يتم تمكين تجميع BGP الإصدار IPv6 مع أجهزة الاندماج. تقوم العقدة الحدودية بفصل رأس IPv4 من حركة مرور مخرج البنية بينما يتم تضمين حركة مرور الدخول IPv6 مع رأس IPv4 بواسطة العقدة الحدودية أيضا.
- حافة البنية - يجب أن تكون جميع الواجهات الظاهرية المحولة (SVIs) التي تم تكوينها في Fabric Edge هي IPv6. يتم دفع هذا التكوين بواسطة وحدة التحكم في مركز بنية الشبكة الرقمية (DNA).
- مركز بنية الشبكة الرقمية من Cisco - الدعم الواجهات المادية لمركز بنية الشبكة الرقمية (DNA) من Cisco تقنية المكدس المزدوج اعتبارا من وقت نشر هذا المستند.

والى يمكن نشره إلا في مكدس واحد مع IPv4 وأ IPv6 فقط في الإدارة و/أو واجهات المؤسسات لمركز الحمض النووي.

- العملاء - يدعم Cisco SD-Access المكدس المزدوج (IPv4 و IPv6) أو المكدس الواحد إما IPv4 أو IPv6. ومع ذلك، في حالة نشر مكدس واحد IPv6، ما يزال مركز بنية الشبكة الرقمية (DNA) يتطلب إنشاء تجمع مزدوج المكدس لدعم عميل IPv6 فقط. يدعم IPv4 في تجمع المكدس المزدوج عنوانا وهميا فقط لأن IPv6 من المتوقع أن يقوم العميل بتعطيل عنوان IPv4.

بنية IPv6 المضمنة في الوصول المعرف ببرنامج Cisco.

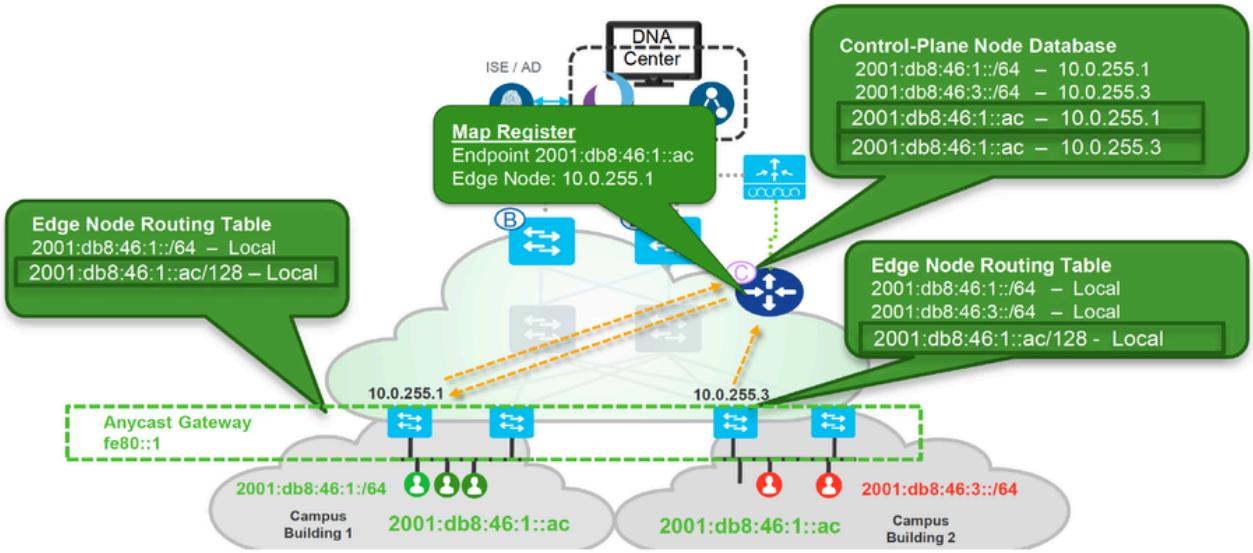


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

بنية تغشية IPv6

تمكين IPv6 باستخدام مركز بنية الشبكة الرقمية من Cisco

هناك طريقتان لتمكين تجمع IPv6 في مركز بنية الشبكة الرقمية من Cisco:
1. إنشاء تجمع IPv4/v6 ثنائي المكدس جديد - Greenfield
2. تحرير IPv6 على تجمع IPv4 الموجود بالفعل - ترحيل Brownfield

ال يدعم الإصدار الحالي (حتى 2.3.x) من مركز بنية الشبكة الرقمية (DNA) الإصدار السادس من بروتوكول الإنترنت (IPv6). مجموعة فقط، إذا كان المستخدم يخطط لدعم عميل عنوان واحد/أصلي IPv6 فقط. يجب إقران عنوان IPv4 البغيض بتجمع IPv6. لاحظ أنه من تجمع IPv4 المنشور الموجود بالفعل مع موقع مقترن به، وقم بتحرير التجمع باستخدام عنوان IPv6. يوفر مركز بنية الشبكة الرقمية (DNA) خيار الترحيل لنسيج SD-Access الذي يتطلب من المستخدم إعادة توفير البنية لذلك الموقع. يتم عرض مؤشر تحذير في البنية التي ينتمي إليها الموقع ويشير إلى أن البنية بحاجة إلى "إعادة تكوين البنية". راجع هذه الصور

للحصول على عينات:

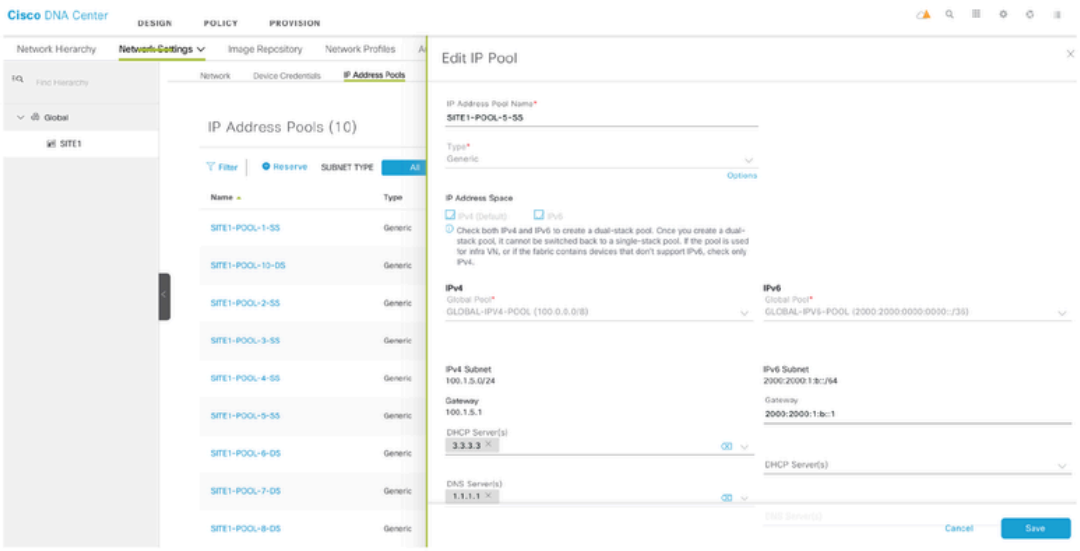


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

ترقية تجمع IPv4 واحد إلى تجمع مزدوج من خلال تحرير خيار تجمع IPv4

Pool upgrade: Warning on fabric page

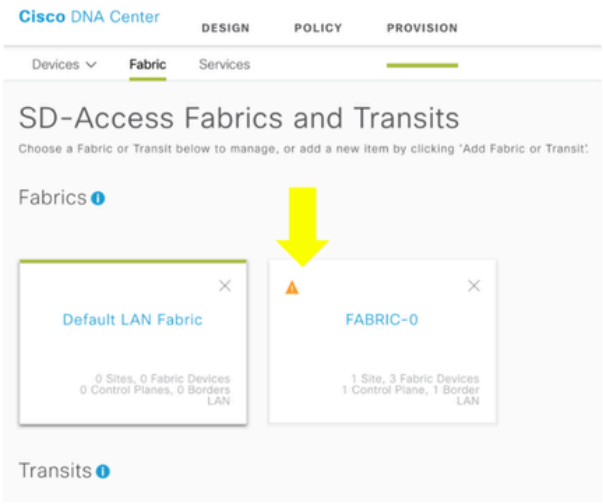


Figure 3.
Fabric has warning indicator which needs to ‘reconfigure the fabric’

تحتوي البنية على مؤشر تحذير يحتاج إلى "إعادة تكوين البنية"

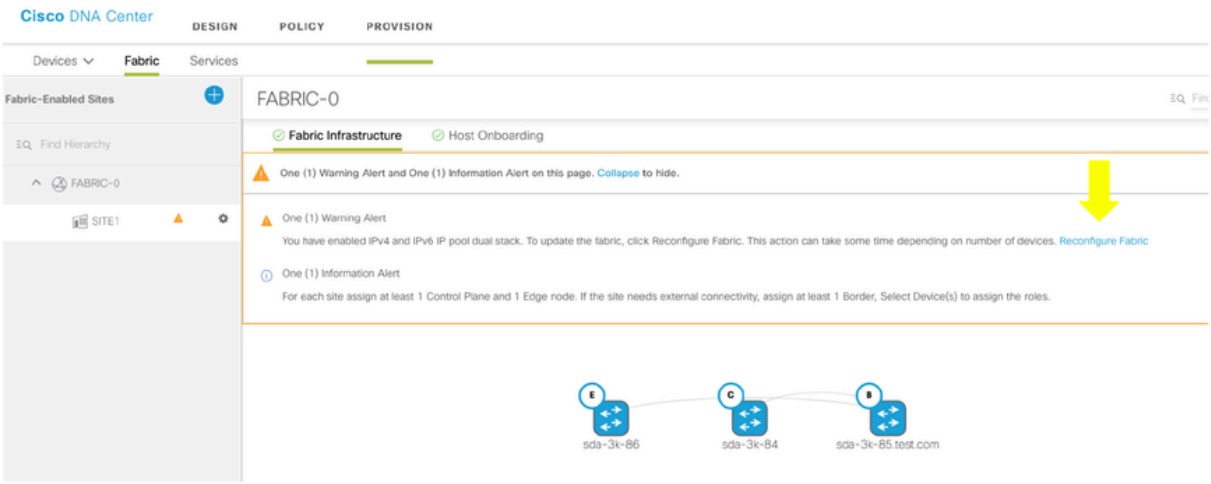


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

يحتاج المستخدم إلى النقر فوق "إعادة تكوين البنية" لإعادة توفير عقد البنية تلقائيا لتفعيل تكوين المكدس المزدوج كجزء من عملية الترحيل

اعتبارات التصميم مع IPv6 في الوصول إلى Cisco SD

على الرغم من أنه لعملاء الوصول إلى SD من Cisco، يمكنهم التشغيل باستخدام إعدادات الشبكة ذات المكدس المزدوج أو IPv6 فقط، فإن تنفيذ بنية الوصول إلى SD الحالي باستخدام إصدار محول مركز بنية الشبكة الرقمية (SW) حتى 2.3.x.x له بعض الاعتبارات حول نشر IPv6.

- دعم وصول SD من Cisco بروتوكولات التوجيه المضمنة الخاصة بالإصدار الرابع من بروتوكول الإنترنت (IP). وبالتالي، يتم نقل حركة مرور عميل IPv6 عندما يتم تضمينها داخل رؤوس IPv4. هذا هو أحد متطلبات نشر برامج LISP الحالية. ولكن هذا لا يعني أن الأساس لا يمكنه تمكين بروتوكول التوجيه IPv6، فقط لا يعمل LISP الخاص بتضمين الوصول إلى SD على تبعيته.
- البث المتعدد الأصلي لـ IPv6 غير مدعوم لأن البنية الأساسية يمكن أن تكون IPv4 فقط في الوقت الحالي.
- لا يمكن تشغيل ميزة Guest Wireless إلا مع المكدس المزدوج. انظر إصدار محرك خدمات الهوية (ISE) الحالي (على سبيل المثال، ما يصل إلى 3.2)، فإن مدخل ضيف IPv6 غير مدعوم، وبالتالي لن يكون عميل ضيف IPv6 فقط قادرا على التصديق.
- لا يتم دعم أتمتة سياسة جودة الخدمة الخاصة بتطبيق IPv6 في إصدار مركز بنية الشبكة الرقمية (DNA) الحالي. يصف هذا المستند الخطوات اللازمة لتنفيذ جودة خدمة IPv6 لعملاء المكدس المزدوج السلكية واللاسلكية في Cisco SD-Access الذي تم نشره لأحد المستخدمين على نطاق واسع.
- يتم دعم ميزة تحديد معدل العميل اللاسلكي لحركة مرور البيانات من الخادم والتدفق من الخادم إما لكل معرف مجموعة الخدمة (SSID) أو لكل عميل استنادا إلى السياسة ل

IPv4 (TCP/UDP) و IPv6 (TCP فقط). تحديد معدل IPv6 UDP غير مدعوم بعد.

- يمكن ترقية تجمع IPv4 إلى تجمع مزدوج المكدس. ولكن ال يمكن تقليل تجمع المكدس المزدوج مرة أخرى إلى تجمع IPv4. إذا كان المستخدم يريد إزالة تجمع المكدس المزدوج إلى تجمع IPv4 الأحادي المكدس، فإنه يحتاج إلى إصدار تجمع المكدس المزدوج بأكمله.
- تم دعم IPv6 المفرد حتى الآن بينما يمكن إنشاء تجمع IPv4 أو ثنائي المكدس في مركز DNA الحالي فقط.
- يدعم النظام الأساسي لبرنامج Cisco IOS® XE تطلب إصدار برنامج أدنى بقيمة 16.9.2 والإصدارات الأحدث.
- تم دعم ميزة الاتصال اللاسلكي لضيف IPv6 حتى الآن في الأنظمة الأساسية لـ AireOS (8.10.105.0+) الحد الأدنى.
- يمكن تعيين تجمع المكدس المزدوج في شبكة INFRA_VN حيث يمكن تعيين نقطة الوصول (AP) وأ طقف تجمع العقدة الموسعة.
- يدعم التشغيل التلقائي لشبكة LAN الإصدار السادس من بروتوكول الإنترنت (IP) بعد.

بالإضافة إلى القيود المذكورة سابقا، عند تصميم بنية وصول إلى SD مع تمكين IPv6، يجب دائما مراعاة قابلية توسع كل مكون من مكونات البنية. إذا كانت نقطة النهاية تتضمن عناوين IPv4 وأ IPv6 متعددة، يتم حساب كل عنوان كإدخال فردي.

تتضمن إدخالات مضيف البنية نقاط الوصول وعقد موسعة الكاسيكية وموسعة وفقا للسياسة.

اعتبارات نطاق العقد الحدودية الإضافية:

يتم إستخدام إدخالات /32 (IPv4) وأ /128 (IPv6) عندما تقوم العقدة الحدودية بإعادة توجيه حركة مرور البيانات من خارج البنية إلى مضيف في البنية.

لجميع المحولات باستثناء المحولات Cisco Catalyst 9500 Series High-Performance Switches والمحولات Cisco Catalyst 9600 Series Switches:

- يستخدم IPv4 إدخال ذاكرة قابلة للتوجيه (TCAM) واحد للمحتوى الثالث (إدخالات مضيف البنية) لكل عنوان IPv4.
- يستخدم IPv6 إدخالين TCAM (إدخالات مضيف البنية) لكل عنوان IPv6.

بالنسبة للمحولات Cisco Catalyst 9500 Series High-Performance Switches والمحولات Cisco Catalyst 9600 Series Switches:

- يستخدم IPv4 إدخال TCAM (إدخالات مضيف البنية) لكل عنوان IPv4.
- يستخدم IPv6 إدخال TCAM (إدخالات مضيف البنية) لكل عنوان IPv6.

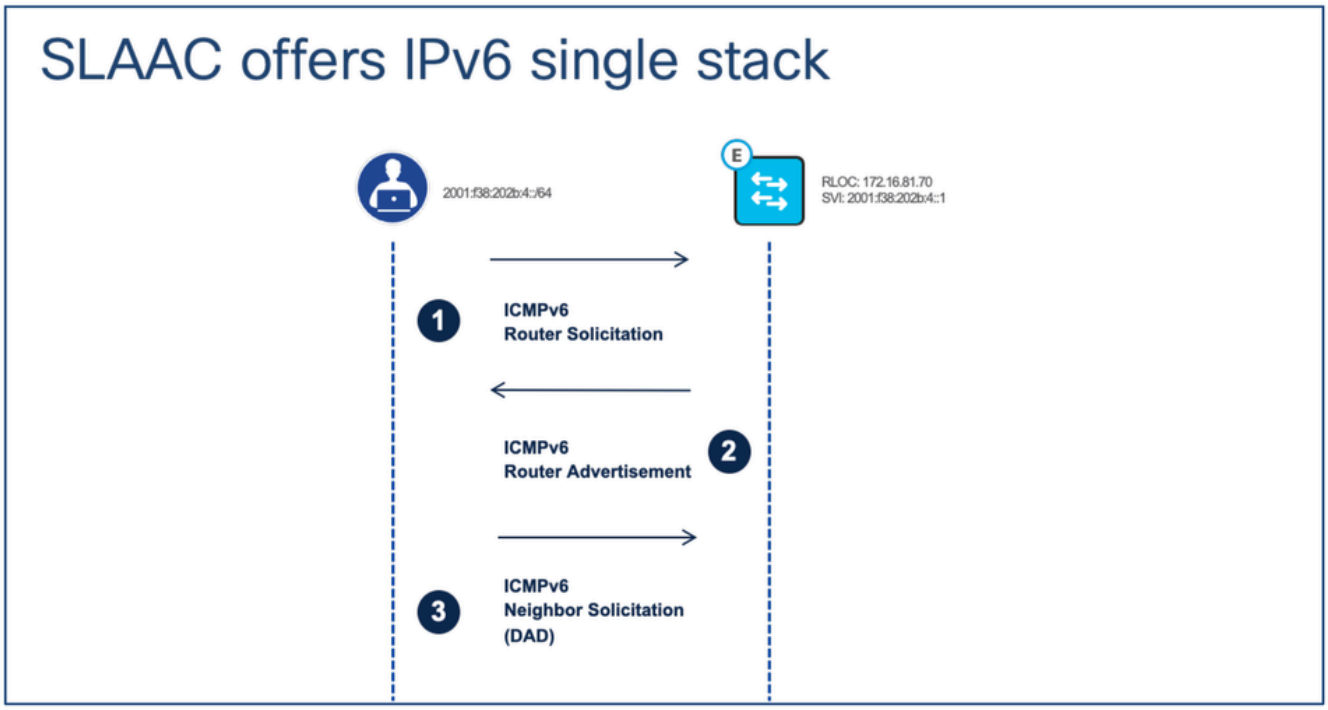
وبعض نقاط النهاية التي تدعم DHCPv6 لمثل الهواتف الذكية المستندة إلى نظام التشغيل Android تدعم أيضا تكوين العنوان التلقائي للعنوان (SLAAC) على الحاجة للحصول على عنوانين IPv6. وبسبب هذا يمكن أن تتهيأ نقطة النهاية واحدة بأكثر من عنوانين IPv6. عنوان IPv6 واحد لكل عقدة من عقد البنية، وخاصة لحد البنية وعقد السلوك المزيد من مواد الأجهزة على كل عقدة من عقد البنية. عند تمرير حركة مرور البيانات الحركة. على سبيل المثال، في كل مرة تدير العقدة الحدودية إرسال حركة مرور البيانات إلى عقد الحافة أي نقطة النهاية، فإنها تقوم بتثبيت مسار مضيف في إدخال TCAM وتحرق إدخال جوار VXLAN في TCAM الخاص بالأجهزة (HW).

إتصالات العملاء السلكية واللاسلكية وتدفقات المكالمات

بمجرد توصيل العميل بحافة البنية، فهناك طرق مختلفة يمكنه من خلالها الحصول على عناوين IPv6. يغطي هذا القسم الطريقة الأكثر شيوعا لعنونة IPv6 العميل، وهي SLAAC و DHCPv6.

تعيين عنوان IPv6 - SLAAC

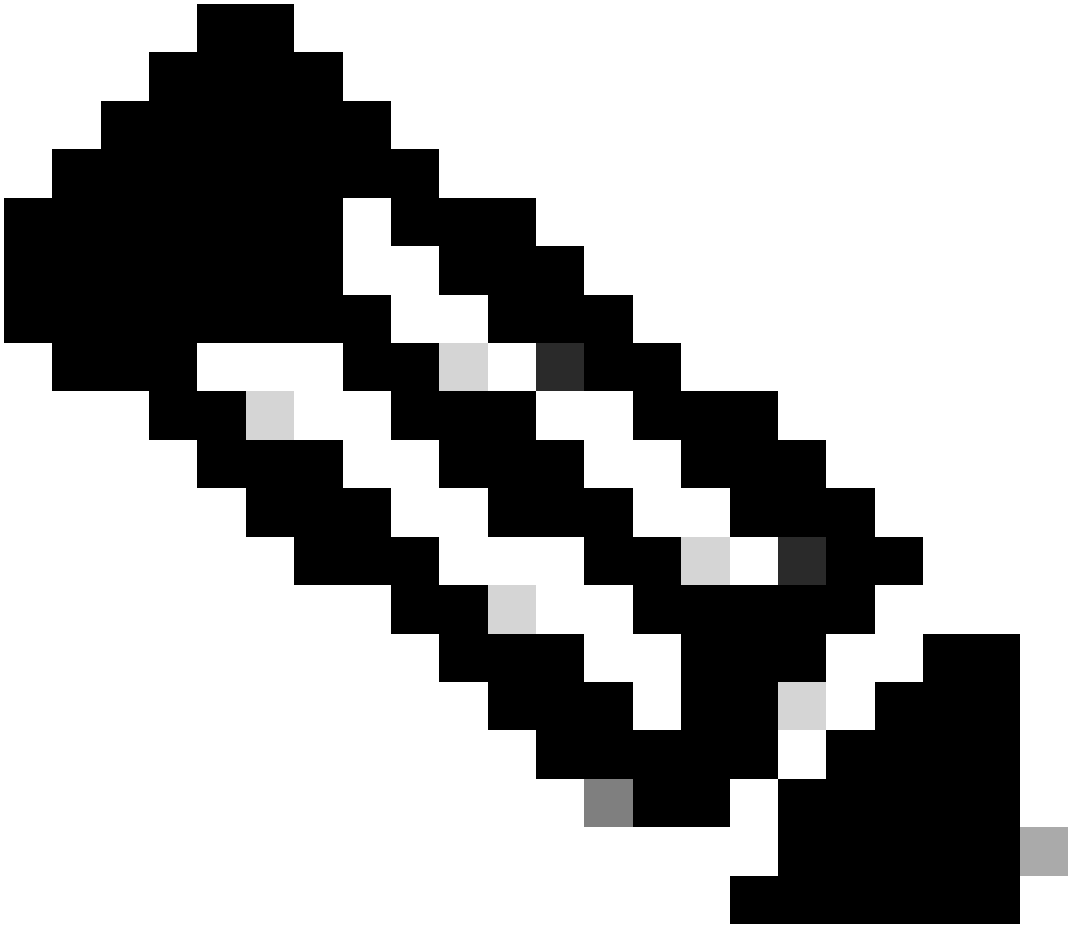
لا يختلف SLAAC في الوصول المعرف بالبرامج (SDA) عن تدفق عملية SLAAC القياسية. لكي يعمل SLAAC بشكل صحيح، يجب تكوين عميل IPv6 باستخدام عنوان محلي للارتباط في الواجهة الخاصة به، وكيفية تكوين العميل نفسه تلقائيا باستخدام العنوان المحلي للارتباط خارج نطاق هذا المستند.



تعيين عنوان IPv6 - SLAAC

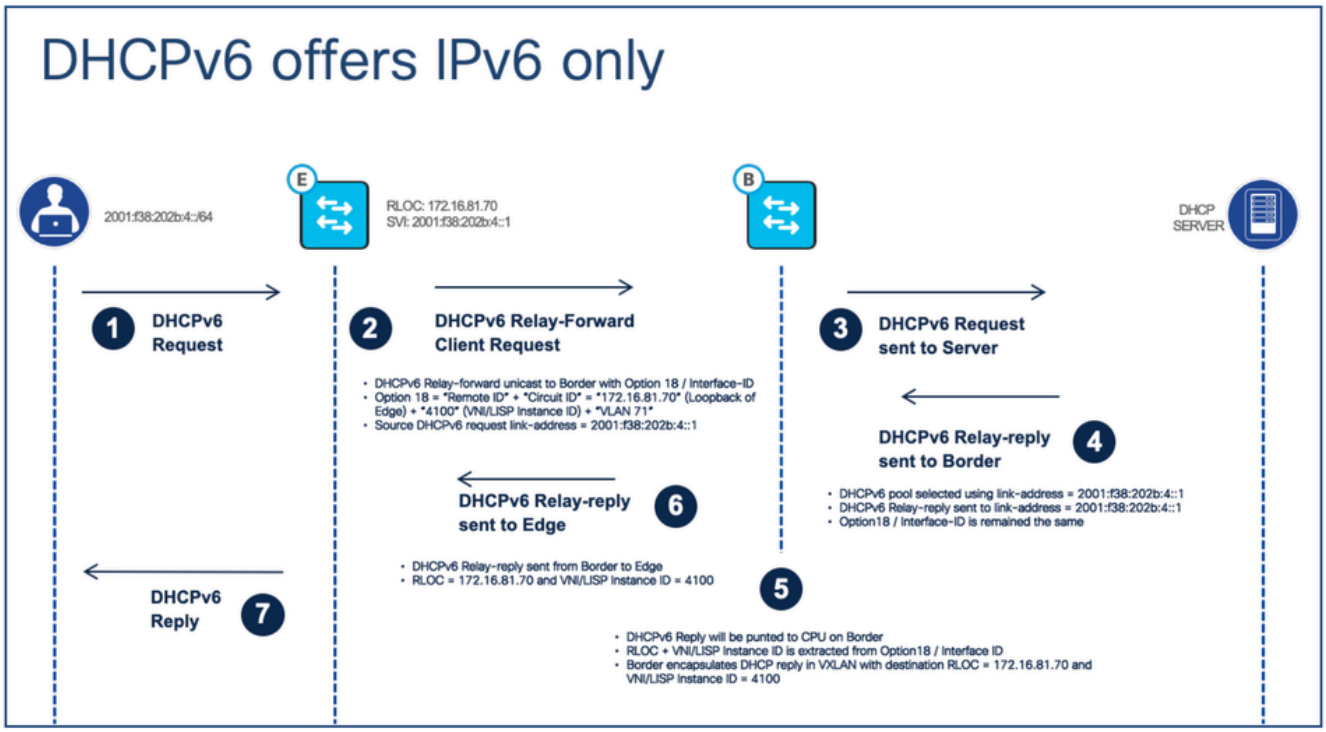
وصف تدفق المكالمات:
الخطوة 1. بعد أن يقوم عميل IPv6 بتكوين نفسه باستخدام عنوان محلي لارتباط IPv6، يرسل العميل رسالة طلب موجه ICMPv6 (RS) إلى Fabric Edge. والغرض من هذه الرسالة هو الحصول على بادئة البث الأحادي العالمية من قطاعها المتصل.
الخطوة 2. بعد أن تتلقى حافة البنية رسالة RS، فإنها تستجيب مرة أخرى باستخدام رسالة إعلان موجه ICMPv6 (RA) التي تحتوي على البادئة العالمية للبث الأحادي IPv6 وطولها داخل.
الخطوة 3. بمجرد أن يحصل العميل على رسالة RA، فإنه يجمع بين البادئة العالمية للبث الأحادي لـ IPv6 ومعرف واجهة EUI-64 الخاص به لإنشاء عنوان البث الأحادي العالمي الفريد لـ IPv6 وتعيين بوابته على العنوان المحلي للارتباط الخاص بـ SVI لحافة البنية المرتبطة بمقطع العميل. بعد ذلك يرسل العميل رسالة طلب طلب مجاورة ICMPv6 لإجراء كشف

العنوان المكرر (DAD) لضمان أن عنوان IPv6 الذي يحصل عليه فريد.



ملاحظة: يتم تضمين جميع الرسائل ذات الصلة SLAAC باستخدام عنوان IPv6 المحلي لارتباط SVI الخاص بالعميل وعقدة البنية.

تعيين عنوان IPv6 - DHCPv6



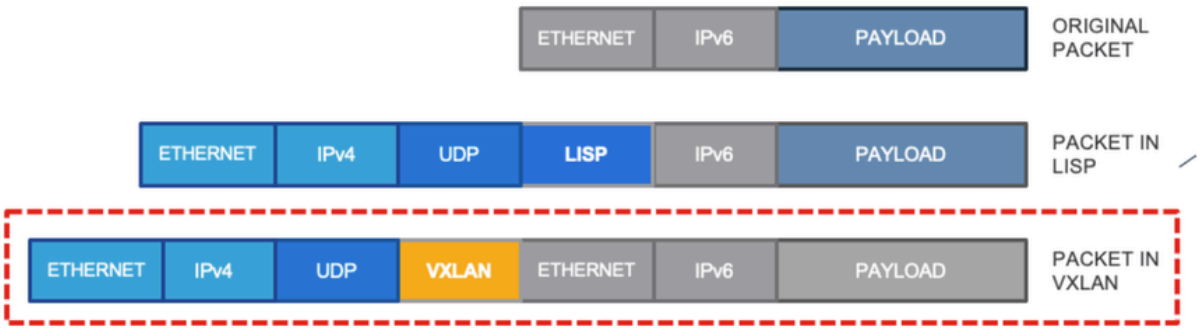
تعيين عنوان IPv6 - DHCPv6

وصف تدفق المكالمات:
الخطوة 1. يرسل العميل طلب DHCPv6 إلى حافة البنية.
الخطوة 2. عندما تتلقى حافة البنية طلب DHCPv6، فإنها سوف تستخدم رسالة إعادة توجيه DHCPv6 للبث الأحادي الطلب إلى حدود البنية مع خيار DHCPv6 18. بالمقارنة مع خيار DHCP رقم 82، يقوم الخيار DHCPv6 بترميز كل من "معرف الدائرة" و"معرف التحكم عن بعد" معا. يتم ترميز معرف مثيل LISP/VNI ومحدد توجيه IPv4 (RLOC) وشبكة VLAN الطرفية بالداخل.
الخطوة 3. تزيل حدود البنية رأس VXLAN ويعقد حزم DHCPv6 إلى خادم DHCPv6.
الخطوة 4. يتلقى خادم DHCPv6 رسالة إعادة التوجيه، وهو يستخدم عنوان إرتباط المصدر (وكيل ترحيل DHCPv6/بوابة العميل) للرسالة لاختيار تجمع IPv6 من أجل تعيين عنوان IPv6. ثم قم بإرسال رسالة الرد على ترحيل DHCPv6 مرة أخرى إلى عنوان بوابة العميل. يبقى الخيار 18 بدون تغيير.
الخطوة 5. عندما يستلم حد النسيج رسالة الرد على الترحيل، فإنه يستخرج ال RLOC و LISP المثيل/VNI من الخيار 18. يغلف حد النسيج رسالة الرد على الترحيل في VXLAN مع غاية والتي استخرجت من الخيار 18.
الخطوة 6. ترسل حدود البنية رسالة الرد على ترحيل DHCPv6 إلى حافة البنية التي يتصل بها العميل.
الخطوة 7. عندما يستقبل حافة البنية رسالة الرد على ترحيل DHCPv6، فإنها تفك صفة رأس VXLAN الخاص بالرسالة وتعيد توجيه الرسالة إلى العميل. ثم يتعرف العميل على عنوان IPv6 المعين له.

اتصال IPv6 في Cisco SD-Access

يستخدم اتصال IPv6 مستوى التحكم القياسي القائم على LISP وأساليب اتصال مستوى

البيانات المستندة إلى VXLAN. مع التنفيذ الحالي في Cisco SD-Access LISP و VXLAN يستخدم رأس IPv4 الخارجي لحمل حزم IPv6 بالداخل. تلتقط هذه الصورة هذه العملية.



رأس IPv4 الخارجي يحمل حزم IPv6 بالداخل

وهذا يعني أن جميع استعلامات LISP تستخدم الحزمة الأصلية IPv4، بينما يحتوي جدول عقدة مستوى التحكم على تفاصيل حول RLOC مع كل من عناوين IPv6 و IPv4 لنقطة النهاية. ويتم شرح هذه العملية بالتفصيل في القسم التالي من منظور نقطة نهاية السلكية.

اتصال IPv6 اللاسلكي في وصول SD من Cisco

يعتمد الاتصال اللاسلكي على تكوين محدد لنقاط الوصول ووحدات التحكم في الشبكة المحلية (LAN) اللاسلكية باستثناء مكونات البنية النمطية SD-Access من Cisco. تقوم نقاط الوصول اللاسلكية بإنشاء نفق نقاط الوصول اللاسلكية (CAPWAP) مع وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وإمدادها. بينما توجد حركة مرور العميل في حافة البنية، تتم إدارة إتصالات مستوى التحكم الأخرى التي تتضمن إحصائيات الراديو بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). من منظور IPv6، يجب أن يكون لكل من WLC و AP عناوين IPv4 وأن تستخدم جميع إتصالات CAPWAP عناوين IPv4 هذه. بينما تدعم أداة التحكم في الشبكة المحلية اللاسلكية (WLC) غير الليفية واتصال نقطة الوصول (AP) الإصدار السادس من بروتوكول الإنترنت (IP)، يستخدم وصول Cisco SD الإصدار الرابع من بروتوكول الإنترنت (IPv4) لجميع الاتصالات التي تنقل أي حركة مرور بيانات لبروتوكول IPv6 العميل داخل حزم IPv4. وهذا يعني أنه لا يمكن تعيين تجمعات AP المخصصة تحت الشبكة الخاصة الظاهرية (VN) باستخدام تجمعات IP التي تكون مكدس مزدوج ويتم إلقاء خطأ في حالة إجراء أي محاولة لهذا التعيين. يمكن تقسيم الاتصال اللاسلكي في إطار SDA من Cisco إلى المهام الرئيسية التالية:

- ضم نقطة الوصول
- تسجيل العميل على متن الطائرة

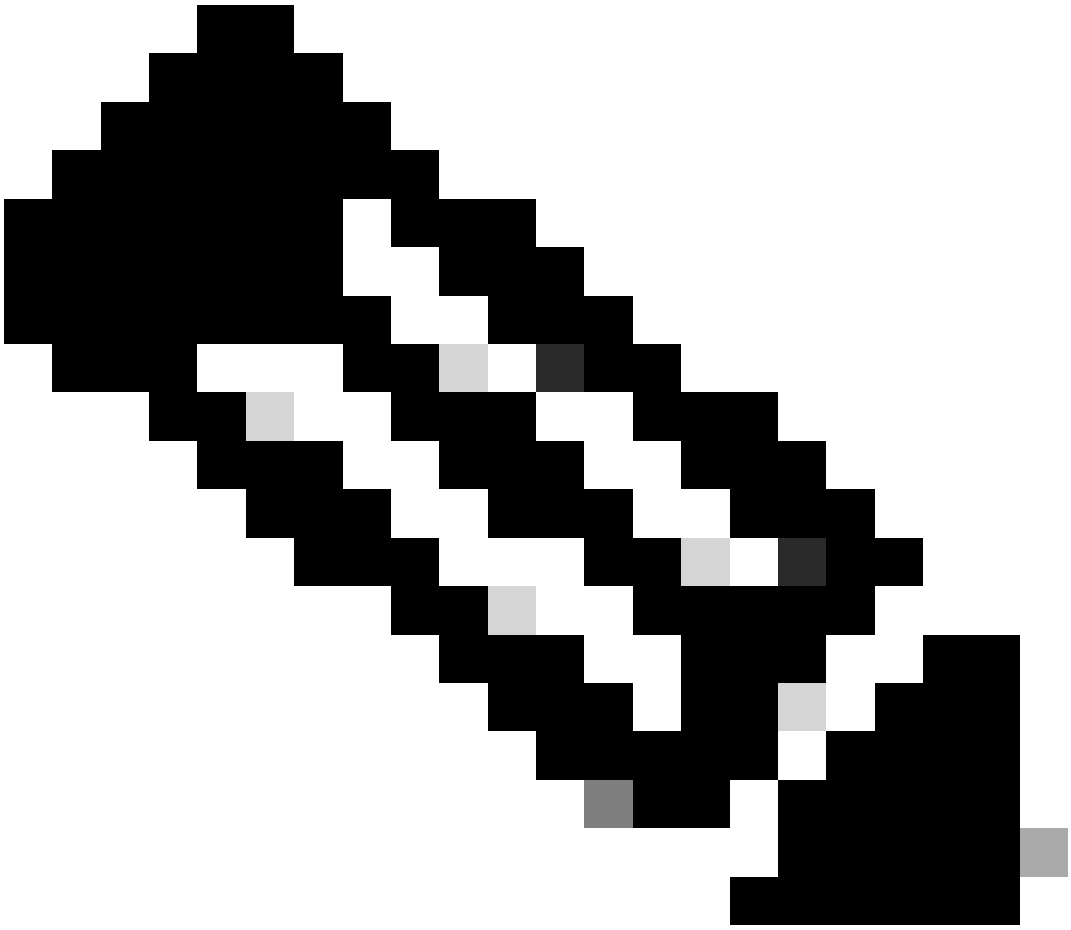
انظر إلى هذه الأحداث من منظور IPv6.

ضم نقطة الوصول

تظل هذه العملية هي نفسها بالنسبة للإصدارين 6 و 4 من بروتوكول IPv4، نظرا لأن لكل من WLC و AP عناوين IPv4 والخطوات المضمنة هنا:

1. تم تكوين منفذ Fabric Edge (FE) لنقطة الوصول (AP) المدمجة.
2. تتصل نقطة الوصول بمنفذ FE، ومن خلال نقطة الوصول (CDP AP) تقوم بإعلام FE حول وجوده (وهذا يسمح لـ FE بتعيين شبكة VLAN الصحيحة).
3. تحصل نقطة الوصول على عنوان IPv4 من نقطة الوصول الخاصة بخادم DHCP وسجلات FE وتحديثات عقدة مستوى التحكم (CP) مع تفاصيل نقطة الوصول.
4. تنضم نقطة الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عبر الطرق التقليدية (مثل خيار DHCP رقم 43).
5. يتحقق WLC مما إذا كانت نقطة الوصول قادرة على عمل البنية ويستعلم عن مستوى التحكم لمعلومات AP RLOC (على سبيل المثال، RLOC المطلوب/الاستجابة المستلمة).
6. يرد CP مع RLOC IP من AP إلى WLC.
7. يسجل WLC التحكم في الوصول إلى وسائط AP (العنوان) (MAC) في CP.
8. يقوم CP بتحديث FE مع تفاصيل من WLC حول نقطة الوصول (وهذا يخبر FE ببدء نفق VXLAN مع نقطة الوصول).

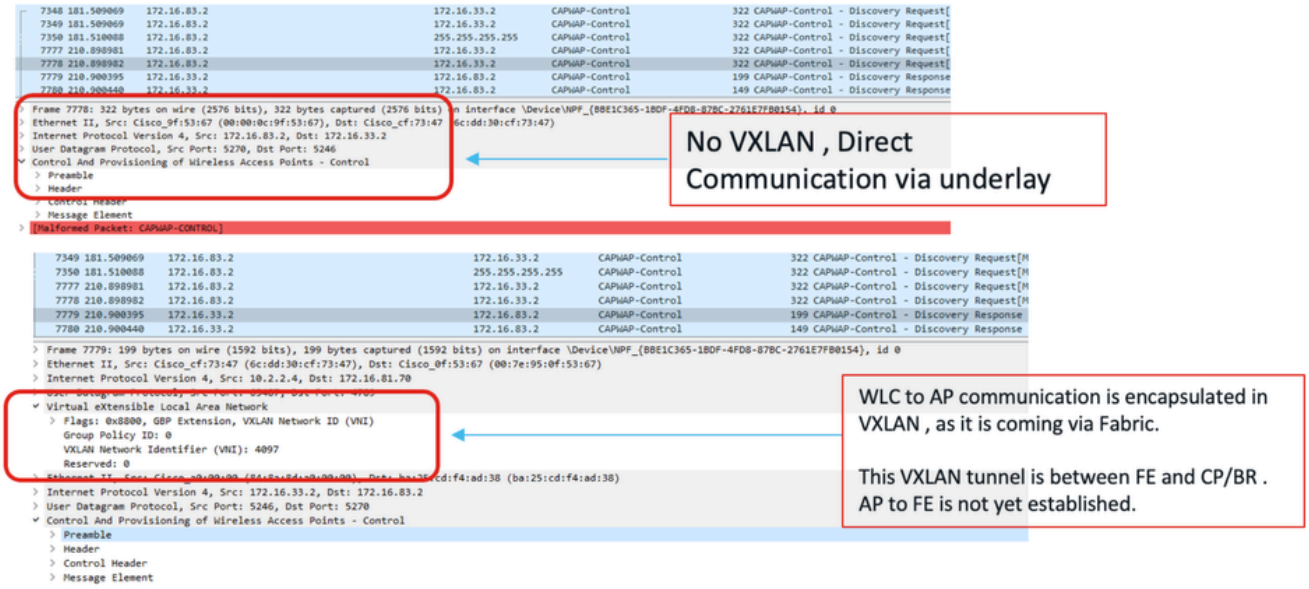
يعالج FE المعلومات وينشئ نفق VXLAN مع AP. عند هذه النقطة، يعلن AP عن SSID ممكن للتسجيل.



ملاحظة: في حالة ما إذا كانت نقطة الوصول تذيع معرفات فئات (SSID) غير بينوية في

والا تبث معرف فئة (SSID) الخاص بالبنية، فتحقق من نفق شبكة VXLAN بين نقطة الوصول وعقدة حافة البنية.

لاحظ أيضا أن نقطة الوصول إلى اتصال WLC تحدث دائما عبر UnderLay CAPWAP وأن كل WLC إلى اتصال AP يستخدم VXLAN CAPWAP عبر تاكب. هذا يعني، إن على قبض أنت ربط أن ذهب من ap إلى WLC، أنت فقط ترى CAPWAP بينما الحركة مرور عكسي يتلقى VXLAN نفق. رأيت هذا مثال للاتصال بين AP و WLC.



التقاط الحزمة من AP إلى WLC (نفق CAPWAP) مقابل WLC إلى AP (نفق VxLAN في البنية)

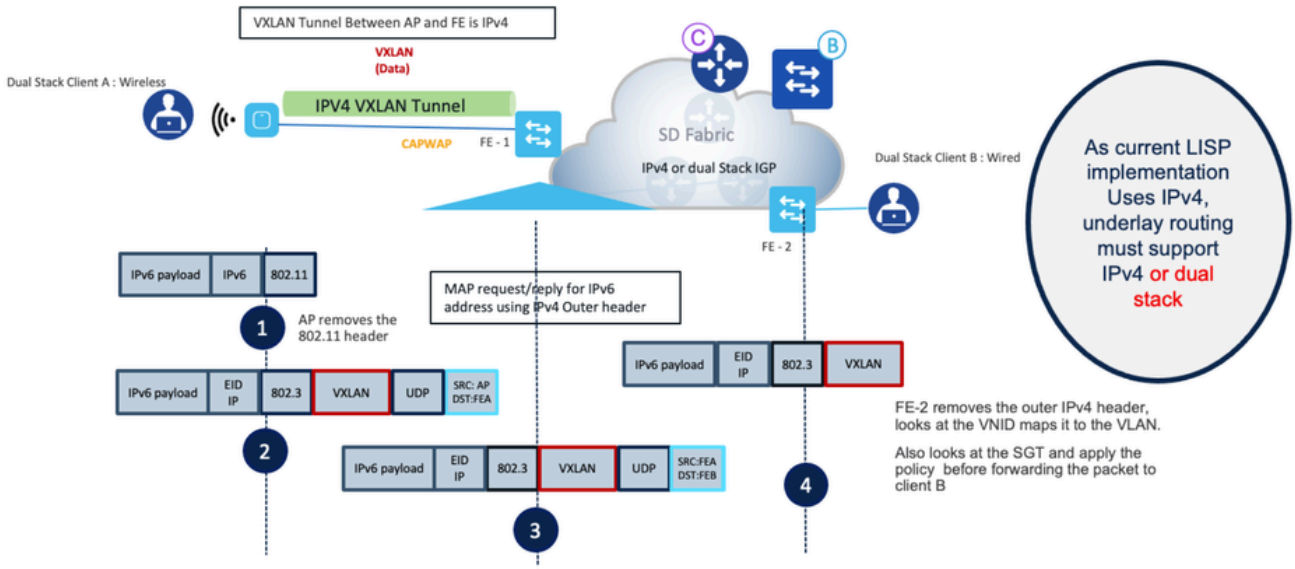
ضم العميل

لا تزال عملية إدراج عميل بروتوكول IPv6/Dual-Stack هي نفسها ولكن العميل يستخدم طرق تعيين عناوين بروتوكول IPv6 مثل SLAAC/DHCPv6 للحصول على عناوين IPv6.
1. يتالقى العميل مع "البنية" ويمكن SSID على نقطة الوصول.
2. يعرف WLC نقطة الوصول عن بعد.
3. يصادق العميل ويسجل WLC تفاصيل العميل L2 مع CP ويحدث نقطة الوصول.
4. يقوم العميل ببدء عنونة IPv6 من الأساليب المكونة - SLAAC/DHCPv6.
5. يقوم FE بتشغيل تسجيل عميل IPv6 إلى قاعدة بيانات تتبع مضيف CP (HTDB).
تستخدم نقاط الوصول إلى FE و FE إلى الوجهات الأخرى تضمين IPv6 و LISP داخل إطارات IPv4.

اتصال العميل-العميل باستخدام IPv6

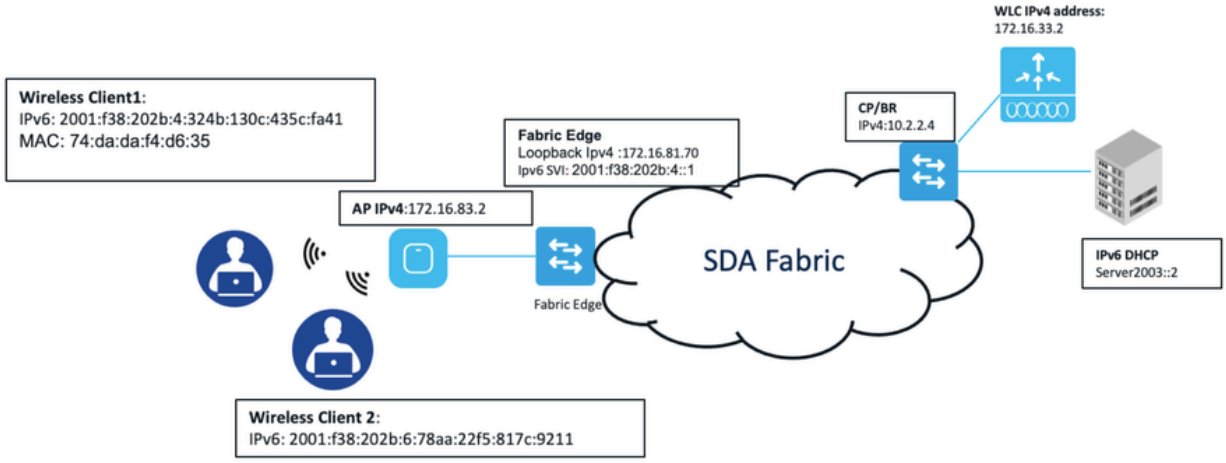
تلخص الصورة هنا عملية اتصال العميل اللاسلكي ل IPv6 مع عميل آخر متصل ب IPv6. (وهذا يفترض أن العميل قد تمت مصادقته وأنه قد حصل على عنوان IPv6 عبر طرق تم تكوينها.)
1. يرسل العميل الإطارات 802.11 إلى نقطة الوصول مع حمولة IPv6.
2. تقوم نقطة الوصول بإزالة رؤوس 802.11 وترسل الحمولة الأصلية ل IPv6 في نفق IPv4

VXAN إلى Fabric Edge.
3. يستخدم Fabric Edge طلب بروتوكول الوصول إلى الرسائل (MAP) لتحديد الوجهة وإرسال الإطار إلى RLOC الوجهة مع IPv4 VXLAN.
4. في المحول الوجهة، تتم إزالة رأس IPv4 VXLAN ويتم إرسال حزمة IPv6 إلى العميل.

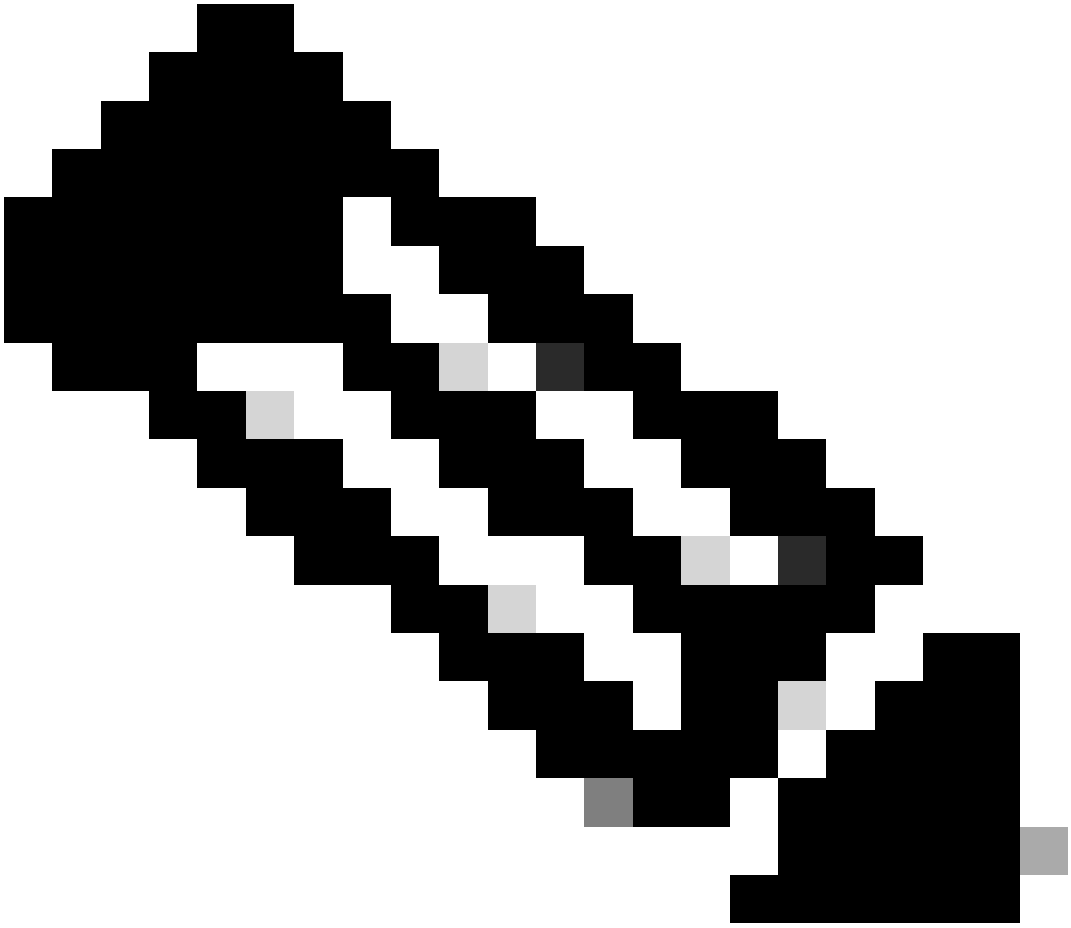


عميل لاسلكي ثنائي المكدس إلى تدفقات حزم العميل السلكية ثنائية المكدس

ابحث في هذه العملية بشكل متعمق باستخدام حزم الالتقاط وأرجع إلى الصورة الخاصة بعناوين IP وتفاصيل عنوان MAC. لاحظ أن هذا الإعداد يستخدم كل من عملاء المكدس المزدوج المتصلين بنفس نقاط الوصول ولكن المعينة باستخدام شبكات IPv6 فرعية (SSIDs) مختلفة.

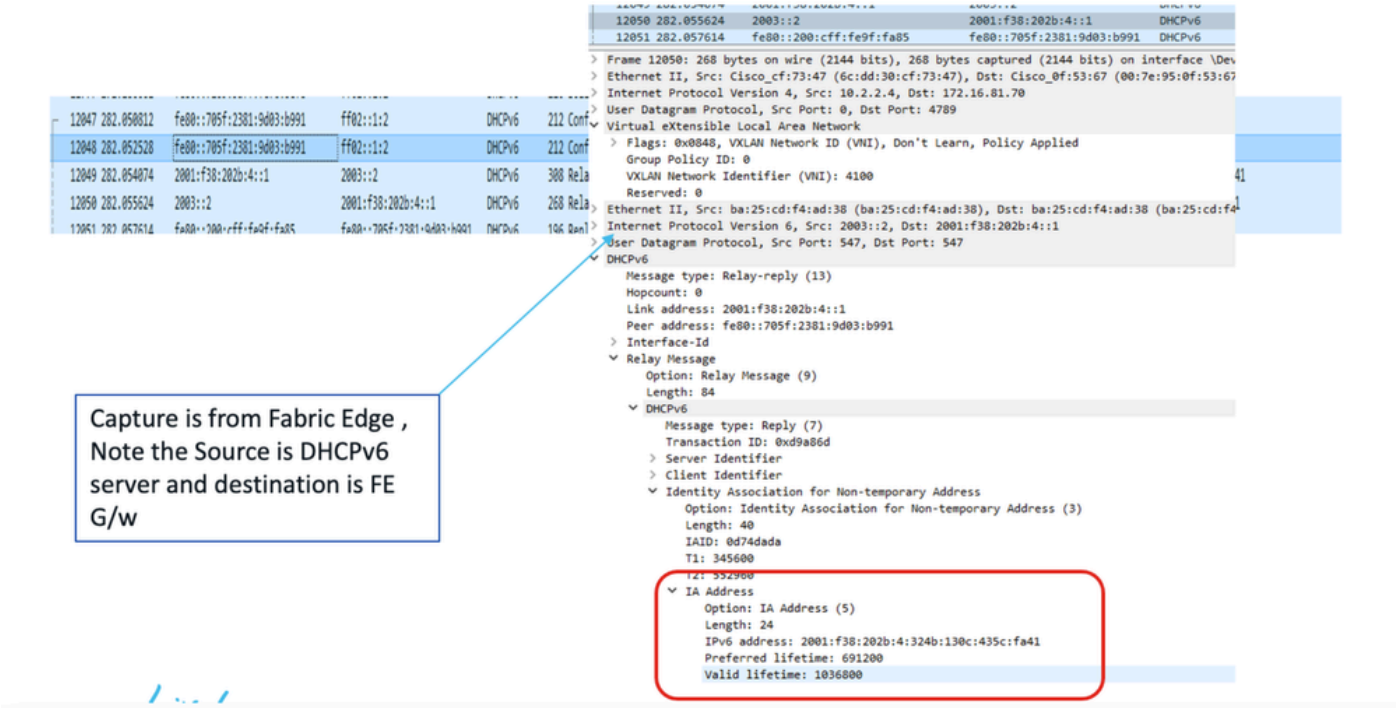


تفاصيل عناوين IP وعناوين MAC لشبكة بنية وصول إلى SD



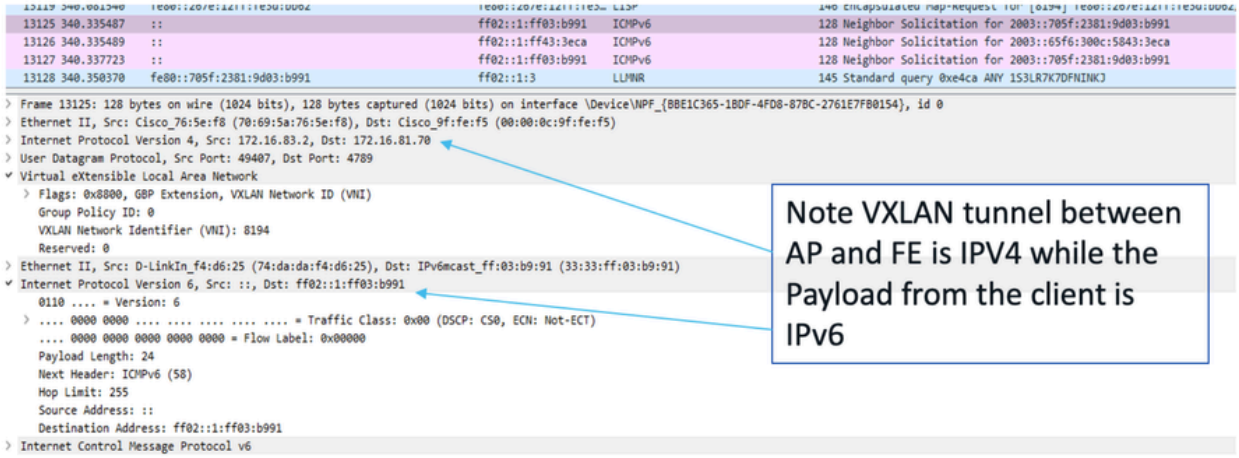
ملاحظة: بالنسبة لأي اتصال IPv6 خارج البنية الأساسية، على سبيل المثال، يجب تمكين التوجيه عبر بروتوكول DHCP/DNS و IPv6 بين البنية الأساسية الحدودية وغير الليفية.

الخطوة 1. يقوم العميل بمصادقة عنوان IPv6 والحصول عليه من الأساليب التي تم تكوينها.



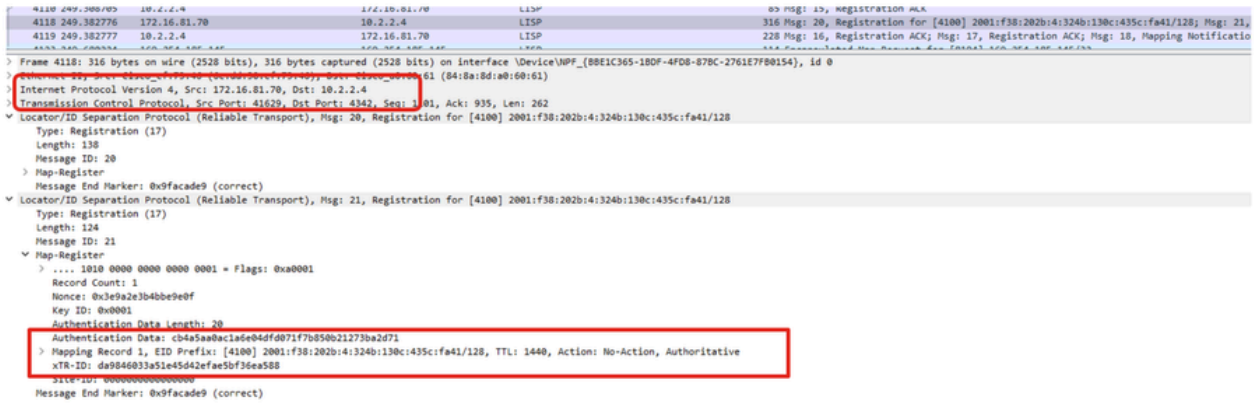
التقاط الحزمة من خادم DHCPv6 إلى عقدة حافة البنية

الخطوة 2. يرسل العميل اللاسلكي إطارات 802.11 إلى نقطة الوصول مع حمولة IPv6.
الخطوة 3. تزيل نقطة الوصول الرأس اللاسلكي وترسل الحزمة إلى حافة البنية. وهذا يستخدم رأس نفق VXLAN الذي يستند إلى IPv4 لأن نقطة الوصول تحتوي على عنوان IPv4.



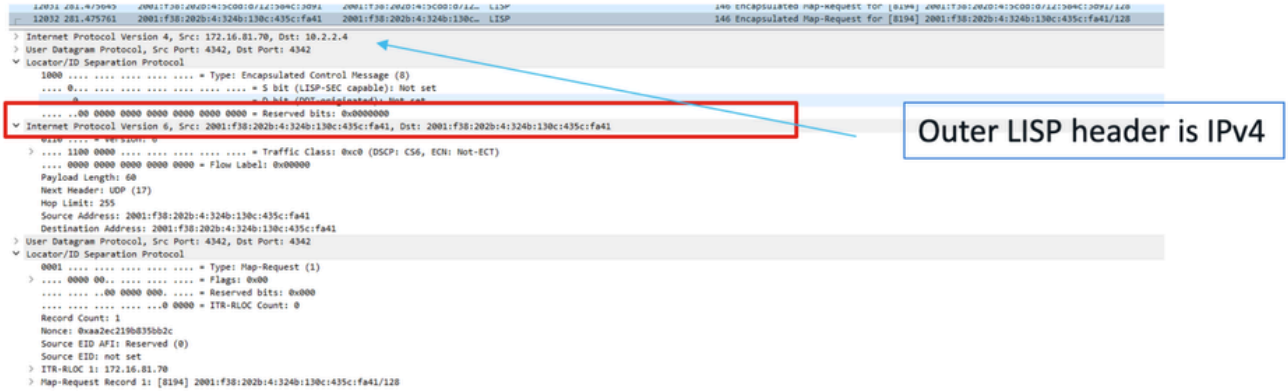
التقاط الحزمة لنفق VxLAN بين FE و AP

الخطوة 3.1. يقوم Fabric Edge بتسجيل عميل IPv6 باستخدام مستوى التحكم. يستخدم هذا الأسلوب تسجيل IPv4 مع تفاصيل عميل IPv6 الموجود بداخله.



التقاط الحزم لسجلات FE باستخدام مستوى التحكم لعميل IPv6

الخطوة 3.2. يرسل FE طلب الخريطة إلى مستوى التحكم لتحديد RLOC الوجهة.



التقاط الحزمة من FE إلى CP مع رسائل تسجيل الخريطة

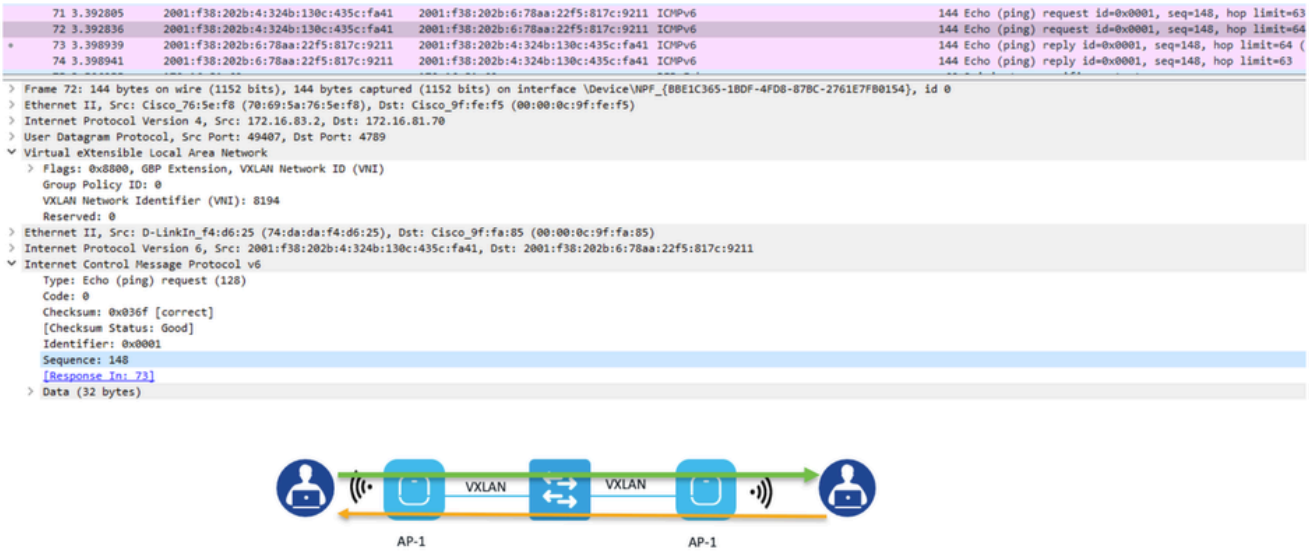
كما يحافظ Fabric Edge على ذاكرة التخزين المؤقت للخريطة لعملاء IPv6 المعروفين، كما هو موضح في هذه الصورة.

```
Pod2-Edge-2#sh lisp eid-table vrf Campus_VN ipv6 map-cache
LISP IPv6 Mapping Cache for EID-table vrf Campus_VN (IID 4100), 6 entries

::/0, uptime: 6w4d, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
2001:F38:202B:3::/64, uptime: 3w1d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2001:F38:202B:4::/64, uptime: 3w1d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2001:F38:202B:4:324B:130C:435C:FA41/128, uptime: 00:00:05, expires: 23:59:54, via map-reply, self, complete
  Locator       Uptime    State     Pri/Wgt     Encap-IID
  172.16.81.70  00:00:05  up, self   10/10        -
2001:F38:202B:6::/64, uptime: 1w2d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2002::/15, uptime: 05:57:20, expires: 00:14:34, via map-reply, forward-native
  Encapsulating to proxy ETR
Pod2-Edge-2#
```

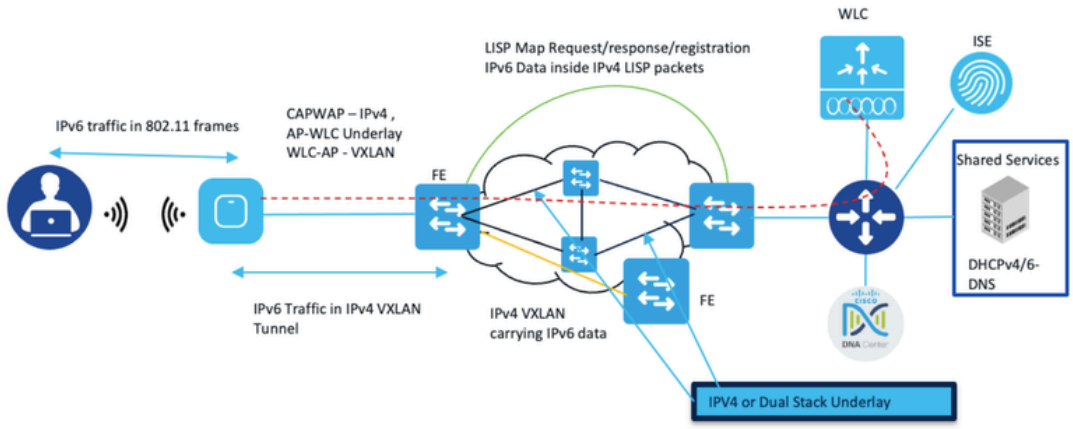
خرج شاشة Fabric Edge من معلومات ذاكرة التخزين المؤقت للمخزن المؤقت للخريطة المتغشية مع الإصدار السادس من بروتوكول الإنترنت (IP)

الخطوة 4. تتم إعادة توجيه الحزمة إلى RLOC الوجهة مع شبكة VXLAN الخاصة ب IPv4 التي تحمل حمولة IPv6 الأصلية داخلها. بما أن كلا الزبونين ربطا إلى نفس ap، لا IPv6 يأخذ عملية أوزي هذا ممر.

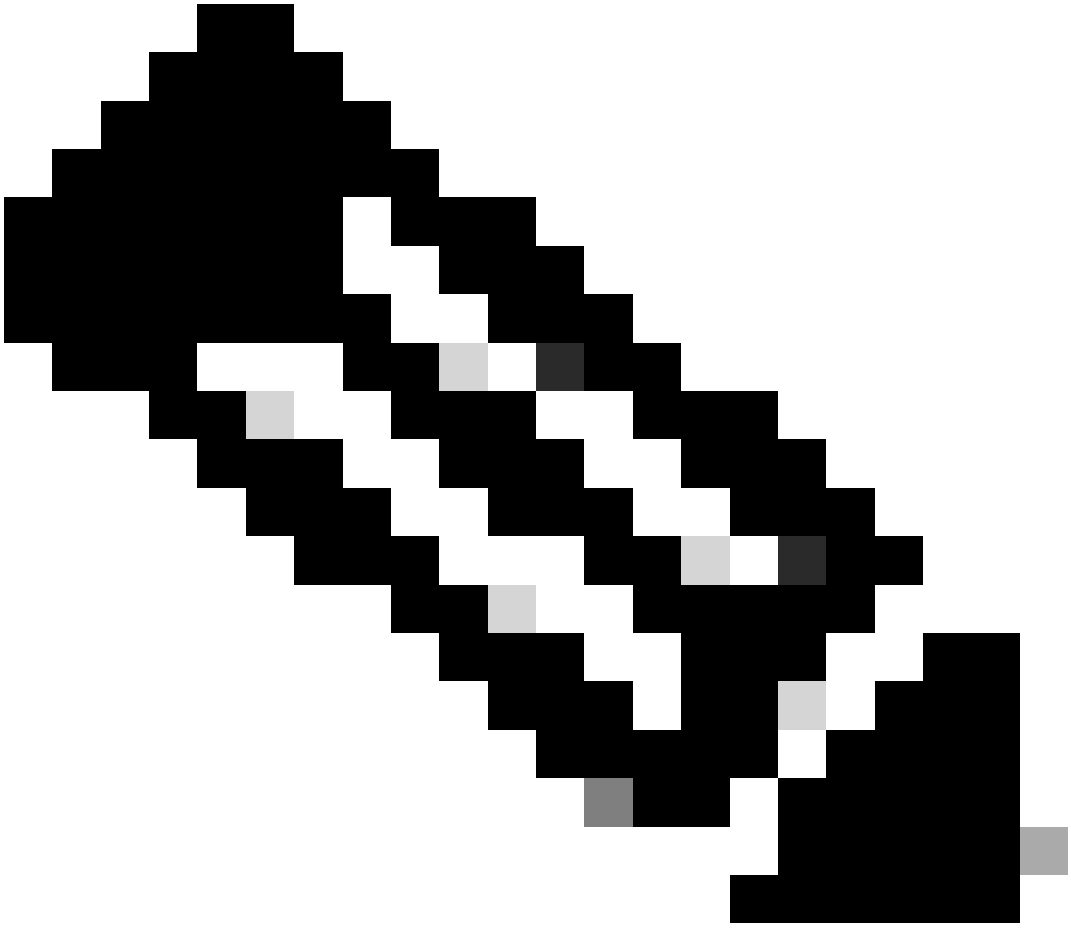


التقاط الحزمة لعملية اختبار اتصال IPv6 بين عميلين لاسلكيين مسجلين في نقطة الوصول نفسها

تلخص هذه الصورة اتصال IPv6 من منظور العميل اللاسلكي.



يلخص الشكل اتصال IPv6 من منظور العميل اللاسلكي



ملاحظة: وصول ضيف IPv6 (مدخل ويب) عبر خدمات تعريف Cisco غير مدعوم بسبب القيود المفروضة على ISE.

مصفوفة التبعية

من المهم ملاحظة التبعيات ودعم IPv6 من المكونات اللاسلكية المختلفة التي تعد جزءا من الوصول عبر برتوكول SD من Cisco. يلخص الجدول في هذه الصورة مصفوفة الميزات هذه.

C9800 IPv6 Features by Release

Feature		AireOS	16.12	17.1
Infra IPv6 (CAPWAP over IPv6)				
	Local	YES	YES	YES
	Flex	YES	YES	YES
	Fabric	NO	YES	YES
Infra IPv6 (WLC Platforms)				
	Hardware Wireless Controller	YES	YES	YES
	Wireless Controller in the switches	NO	YES	YES
	Public Cloud: AWS	NO	NO	NO
	Public Cloud: GCP	NO	NO	NO
	Private Cloud: ESXi	YES	YES	YES
	Private Cloud: KVM	YES	YES	YES
	Private Cloud: NFVIs	NO	YES	YES
Interop IPv6 support				
	C9800 <-> DNA-C (Infra IPv6)	NO	TBD	NO
	C9800 <-> CMX (Infra IPv6)	NO	TBD	YES
	C9800 <-> ISE (Infra IPv6)	NO	TBD	YES
	WLC<->PI(Infra IPv6)	YES(Over SNMP)	YES	YES
	OpenDNS(Infra iPv6)	NO	YES	YES
	Netflow over IPv6	NO	YES	YES
	ETA for IPv6	NO	NO	YES

ميزات CAT9800 WLC IPv6 حسب الإصدار

مراقبة مستوى التحكم لـ IPv6

بمجرد تمكين IPv6، تبدأ في رؤية إدخالات إضافية حول IPv6 المضيف في خوادم خادم الخريطة (MS)/محلل الخريطة (MR). بما أن المضيف يمكن أن يكون له عناوين IPv6 متعددة، يحتوي جدول البحث MS/MR الخاص بك على إدخالات لجميع عناوين IP. يتم دمج هذا مع جدول IPv4 الموجود بالفعل.
يجب عليك تسجيل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة بالجهاز وإصدار هذه الأوامر للتحقق من جميع الإدخالات.

```
Pod2-Border#sh lisp site

LISP Site Registration Information

* = Some locators are down or unreachable

# = Some registrations are sourced by reliable transport


Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   4097     172.16.83.0/24
               2w1d      yes#   172.16.81.70:41629   4097     172.16.83.2/32
```

```
              never     no     --                  4099     172.16.79.0/24

              never     no     --                  4100     172.16.71.0/24

              never     no     --                  4100     172.16.72.0/24

              never     no     --                  4100     172.16.78.0/24

              never     no     --                  4100     2001:F38:202B:3::/64

              1w0d      yes#   172.16.81.65:16775  4100     2001:F38:202B:3:5B84:C9B0:1271:D4B/128

              1w0d      yes#   172.16.81.70:41629  4100     2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128

              never     no     --                  4100     2001:F38:202B:4::/64

              6d14h     yes#   172.16.81.70:41629  4100     2001:F38:202B:4:324B:130C:435C:FA41/128

              6d15h     yes#   172.16.81.70:41629  4100     2001:F38:202B:4:705F:2381:9D03:B991/128

              14:10:42  yes#   172.16.81.70:41629  4100     2001:F38:202B:4:B8AE:8711:5852:BE6A/128

              never     no     --                  4100     2001:F38:202B:6::/64
```

```
Pod2-Border#sh lisp site summary

                    ----------- IPv4 ----------- ----------- IPv6 ----------- ----------- MAC -----------

Site name           Configured Registered Incons Configured Registered Incons Configured Registered Incons

site_uci                     5          1      0          3          5      0          5          5      0


Site-registration limit for router lisp 0:              0

Site-registration count for router lisp 0:             11

Number of address-resolution entries:                  14

Number of configured sites:                             1

Number of registered sites:                             1

Sites with inconsistent registrations:                  0

IPv4

  Number of configured EID prefixes:                    5

  Number of registered EID prefixes:                    1

  Maximum MS entries allowed:                       81920

IPv6

  Number of configured EID prefixes:                    3
```

```
  Number of registered EID prefixes:                5

  Maximum MS entries allowed:                   81920

MAC

  Number of configured EID prefixes:                5

  Number of registered EID prefixes:                5

  Maximum MS entries allowed:                   81920
```

يمكنك أيضا التحقق من تفاصيل حول المضيف IPv6 من خلال الضمان.

تنفيذ جودة خدمة IPv6 في الوصول إلى Cisco SD

ال يدعم إصدار مركز بنية الشبكة الرقمية (DNA) الحالي من Cisco (حتى 2.3.x) التشغيل التلقائي لسياسة تطبيق جودة خدمة IPv6. وهو ذلك، يمكن للمستخدمين إنشاء قوالب سلكية و السلكية خاصة بالإصدار السادس من بروتوكول الإنترنت (IPv6) ودعم ودي اي (IPv6) يقوم (DNA) الرقمية الشبكة بنية مركز أن ارظن .Fabric Edge عقد إلى الخدمة جودة قالب بأتمتة سياسة جودة خدمة IPv4 على جميع الواجهات المادية بمجرد تطبيقها، فيمكنك إدراج خريطة فئة (تطابق قائمة التحكم في الوصول (ACL) إلى IPv6 ودي اي) قبل "إعدادات الفئة الافتراضية" عبر قالب.

وفيما يلي نموذج القالب الذي يدعم جودة خدمة IPv6 السلكية والمدمج مع تكوين النهج الذي تم إنشاؤه بواسطة مركز بنية الشبكة الرقمية:

```
!
interface GigabitEthernetx/y/z
service-policy input DNA-APIC_QOS_IN
class-map match-any DNA-APIC_QOS_IN#SCAVENGER <<< Provisioned by DNAC
match access-group name DNA-APIC_QOS_IN#SCAVENGER__acl
match access-group name IPV6_QOS_IN#SCAVENGER__acl <<< Manually add
!
ipv6 access-list IPV6_QOS_IN#SCAVENGER__acl <<< Manually add
sequence 10 permit icmp any any
!
Policy-map DNA-APIC_QOS_IN
class IPV6_QOS_IN#SCAVENGER__acl <<< manually add
set dscp cs1
For wireless QoS policy, Cisco DNA Center with current release (up to 2.3.x) will provision IPv4 QoS on
and apply IPv4 QoS into the WLC (Wireless LAN Controller). It doesn't automate IPv6 QoS.
© 2021 Cisco and/or its affiliates. All rights reserved. Page 20 of 24
Below is the sample wireless IPv6 QoS template. Please make sure to apply the QoS policy into the wirel
interface from the wireless VLAN:
ipv6 access-list extended IPV6_QOS_IN#TRANS_DATA__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#REALTIME
```

```
remark ### a placeholder ###
!
ipv6 access-list extended IPV6-QOS_IN#TUNNELED__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#VOICE
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#SCAVENGER__acl
permit icmp any any
!
ipv6 access-list extended IPV6_QOS_IN#SIGNALING__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#BROADCAST__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#BULK_DATA__acl
permit tcp any any eq ftp
permit tcp any any eq ftp-data
permit tcp any any eq 21000
permit udp any any eq 20
!
ipv6 access-list extended IPV6_QOS_IN#MM_CONF__acl
remark ms-lync
permit tcp any any eq 3478
permit udp any any eq 3478
permit tcp range 5350 5509
permit udp range 5350 5509
!
ipv6 access-list extended IPV6_QOS_IN#MM_STREAM__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#OAM__acl
remark ### a placeholder ###
!
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
!
class-map match-any IPV6_QOS_IN#TRANS_DATA
match access-group name IPV6_QOS_IN#TRANS_DATA__acl
!
class-map match-any IPV6_QOS_IN#REALTIME
match access-group name IPV6_QOS_IN#TUNNELED__acl
!
class-map match-any IPV6_QOS_IN#TUNNELED
match access-group name IPV6_QOS_IN#TUNNELED__acl
!
class-map match-any IPV6_QOS_IN#VOICE
match access-group name IPV6_QOS_IN#VOICE
!
class-map match-any IPV6_QOS_IN#SCAVENGER
match access-group name IPV6_QOS_IN#SCAVENGER__acl
!
class-map match-any IPV6_QOS_IN#SIGNALING
match access-group name IPV6_QOS_IN#SIGNALING__acl
class-map match-any IPV6_QOS_IN#BROADCAST
match access-group name IPV6_QOS_IN#BROADCAST__acl
!
class-map match-any IPV6_QOS_IN#BULK_DATA
match access-group name IPV6_QOS_IN#BULK_DATA__acl
!
class-map match-any IPV6_QOS_IN#MM_CONF
```

© 2021 Cisco and/or its affiliates. All rights reserved. Page 21 of 24

```
match access-group name IPV6_QOS_IN#MM_CONF__acl
!
class-map match-any IPV6_QOS_IN#MM_STREAM
match access-group name IPV6_QOS_IN#MM_STREAM__acl
!
class-map match-any IPV6_QOS_IN#OAM
match access-group name IPV6_QOS_IN#OAM__acl
!
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
policy-map IPV6_QOS_IN
class IPV6_QOS_IN#VOICE
set dscp ef
class IPV6_QOS_IN#BROADCAST
set dscp cs5
class IPV6_QOS_IN#REALTIME
set dscp cs4
class IPV6_QOS_IN#MM_CONF
set dscp af41
class IPV6_QOS_IN#MM_STREAM
set dscp af31
class IPV6_QOS_IN#SIGNALING
set dscp cs3
class IPV6_QOS_IN#OAM
set dscp cs2
class IPV6_QOS_IN#TRANS_DATA
set dscp af21
class IPV6_QOS_IN#BULK_DATA
set dscp af11
class IPV6_QOS_IN#SCAVENGER
set dscp cs1
class IPV6_QOS_IN#TUNNELED
class class-default
set dscp default
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
interface Vlan1xxx < = = (wireless VLAN)
service-policy input IPV6_QOS_IN
end
```

أستكشاف أخطاء IPv6 وإصلاحها في Cisco SD-Access

أستكشاف أخطاء SD-Access IPv6 وإصلاحها يشبه IPv4 تماما، يمكنك دائما إستخدام الأمر نفسه مع خيارات كلمات أساسية مختلفة لتحقيق الهدف نفسه. يوضح هذا الأمر بعض الأوامر التي يتم إستخدامها بشكل متكرر لاستكشاف أخطاء SD-Access وإصلاحها.

```
Pod2-Edge-2#sh device-tracking database
Binding Table has 24 entries, 12 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match 0002:Orig trunk 0004:Orig access
0008:Orig trusted trunk 0010:Orig trusted access 0020:DHCP assigned

0040:Cga authenticated 0080:Cert authenticated 0100:Statically assigned
Network Layer Address Link Layer Address Interface vlan prlvl age state Time left
```

```
DH4 172.16.83.2 7069.5a76.5ef8 Gi1/0/1 2045 0025 5s REACHABLE 235 s(653998 s)
L 172.16.83.1 0000.0c9f.fef5 Vl2045 2045 0100 22564mn REACHABLE
ARP 172.16.79.10 74da.daf4.d625 Ac0 71 0005 49s REACHABLE 201 s try 0
L 172.16.79.1 0000.0c9f.f886 Vl79 79 0100 22562mn REACHABLE
L 172.16.78.1 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
DH4 172.16.72.101 000c.29c3.16f0 Gi1/0/3 72 0025 9803mn STALE 101187 s
L 172.16.72.1 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
L 172.16.71.1 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
ND FE80::7269:5AFF:FE76:5EF8 7069.5a76.5ef8 Gi1/0/1 2045 0005 12s REACHABLE 230 s
ND FE80::705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 107s REACHABLE 145 s try 0
L FE80::200:CFF:FE9F:FA85 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
L FE80::200:CFF:FE9F:FA09 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
L FE80::200:CFF:FE9F:F886 0000.0c9f.f886 Vl79 79 0100 87217mn DOWN
L FE80::200:CFF:FE9F:F1AE 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
ND 2003::B900:53C0:9656:4363 74da.daf4.d625 Ac0 71 0005 26mn STALE 451 s
ND 2003::705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 3mn REACHABLE 49 s try 0
ND 2003::5925:F521:C6A7:927B 74da.daf4.d625 Ac0 71 0005 3mn REACHABLE 47 s try 0
L 2001:F38:202B:6::1 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
ND 2001:F38:202B:4:B8AE:8711:5852:BE6A 74da.daf4.d625 Ac0 71 0005 83s REACHABLE 164 s try 0
ND 2001:F38:202B:4:705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 112s REACHABLE 133 s try 0
DH6 2001:F38:202B:4:324B:130C:435C:FA41 74da.daf4.d625 Ac0 71 0024 107s REACHABLE 135 s try 0(985881 s)
L 2001:F38:202B:4::1 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
DH6 2001:F38:202B:3:E6F4:68B3:D2A6:59E6 000c.29c3.16f0 Gi1/0/3 72 0024 9804mn STALE 367005 s
L 2001:F38:202B:3::1 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
Pod2-Edge-2#sh lisp eid-table Campus_VN ipv6 database
LISP ETR IPv6 Mapping Database for EID-table vrf Campus_VN (IID 4100), LSBs: 0x1
Entries total 5, no-route 0, inactive 1
© 2021 Cisco and/or its affiliates. All rights reserved. Page 23 of 24
2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128, dynamic-eid InfraVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:324B:130C:435C:FA41/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:705F:2381:9D03:B991/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:ACAF:7DDD:7CC2:F1B6/128, Inactive, expires: 10:14:48
2001:F38:202B:4:B8AE:8711:5852:BE6A/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
Pod2-Edge-2#show lisp eid-table Campus_VN ipv6 map-cache
LISP IPv6 Mapping Cache for EID-table vrf Campus_VN (IID 4100), 6 entries
::/0, uptime: 1w3d, expires: never, via static-send-map-request
Encapsulating to proxy ETR
2001:F38:202B:3::/64, uptime: 5w1d, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128, uptime: 00:00:04, expires: 23:59:55, via map-reply, self, comp
Locator Uptime State Pri/Wgt Encap-IID
172.16.81.70 00:00:04 up, self 10/10 -
2001:F38:202B:4::/64, uptime: 5w1d, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2001:F38:202B:6::/64, uptime: 6d15h, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2002::/15, uptime: 00:05:04, expires: 00:09:56, via map-reply, forward-native
© 2021 Cisco and/or its affiliates. All rights reserved. Page 24 of 24
Encapsulating to proxy ETR
```

من العقدة الحدودية لفحص خادم DHCPv6 الذي تم تغليفه:

```
Pod2-Border#ping vrf Campus_VN 2003::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2003::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

الأسئلة المتداولة السريعة لتصميم IPv6 مع Cisco SD-Access

س. هل تدعم شبكة Cisco المعرفة IPv6 للشبكات الأساسية والمترابطة؟
أ. يتم دعم التغشية فقط مع الإصدار الحالي (2.3.x) في وقت كتابة هذا المستند.

q. هل تدعم شبكة SDN من Cisco بروتوكول IPv6 الأصلي لكل من العملاء السلكيين واللاسلكيين؟
ج. نعم. وهذا يتطلب تجمعات مزدوجة المكدس التي يتم إنشاؤها في مركز بيانات الشبكة الرقمية (DNA) بينما يكون IPv4 هو التجمع البكم حيث يقوم العملاء بتعطيل طلبات IPv4 DHCP ويتم عرض عناوين IPv6 DHCP أو SLAAC فقط.

س. هل يمكنني الحصول على شبكة مجمع IPv6 أصلية في بنية Cisco SD-Access؟
أ. ليس مع الإصدار الحالي (حتى 2.3.x). إنه على خارطة الطريق.

س. هل يدعم الوصول إلى المحول (SD) من Cisco تسليم الإصدار السادس من بروتوكول الإنترنت (IP) من المستوى الثاني؟
ألف - ليس في الوقت الحاضر. يتم دعم نقل L2 IPv4 فقط وأ توصيل L3 ثنائي المكدس.

س. هل يدعم الوصول إلى SD من Cisco البث المتعدد ل IPv6؟
أ. نعم، يتم دعم تغشية IPv6 فقط مع البث المتعدد لنسخ وحدة الاستقبال والبث. البث المتعدد ل IPv6 الأصلي غير مدعوم بعد.

س. هل يقوم Cisco SD-Access Fabric بتمكين ضوف الدعم اللاسلكي في المكدس المزدوج؟
a. ال يسان بعد في cisco ios XE (Cat9800) WLC. يتم دعم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من AireOS من خالل حل بديل. للحصول على تفاصيل تنفيذ الحل البديل، اتصل بفريق تجربة العملاء من Cisco.

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).