Implementación de IPv6 en el acceso definido por software

Contenido

Introducción

Este documento describe cómo implementar IPv6 en Cisco® Software-Defined Access (SD-Access).

Antecedentes

IPv4 se lanzó en 1983 y todavía se utiliza para la mayor parte del tráfico de Internet. El direccionamiento IPv4 de 32 bits permitía más de 4000 millones de combinaciones únicas. Sin embargo, debido al aumento en el número de clientes conectados a Internet, existe una escasez de direcciones IPv4 únicas. En la década de 1990, el agotamiento del direccionamiento IPv4 se hizo inevitable.
Anticipándose a esto, Internet Engineering Task Force introdujo el estándar IPv6. IPv6 utiliza 128 bits y ofrece direcciones IP únicas de 340 undecillones, más que suficiente para satisfacer la necesidad de dispositivos conectados que crecen. A medida que los dispositivos de terminales más modernos admiten una pila doble o una pila IPv6 única, es fundamental que cualquier organización esté preparada para la adopción de IPv6. Esto significa que toda la infraestructura

debe estar preparada para IPv6. Cisco SD-Access es la evolución de los diseños de campus tradicionales a las redes que implementan directamente la intención de una organización. Las redes definidas por software de Cisco ya están preparadas para incorporar la pila doble (dispositivos IPv6).

Un reto importante para cualquier organización en la adopción de IPV6 es la gestión de cambios y las complejidades asociadas a la migración de sistemas IPv4 heredados a IPv6. En este informe se tratan todos los detalles sobre la compatibilidad de las funciones de IPv6 en SDN de Cisco, la estrategia y los puntos de conexión críticos, que deben tenerse en cuenta al adoptar IPv6 con Cisco Software Defined Networks.

En agosto de 2019, Cisco Digital Network Architecture (DNA) Center versión 1.3 se presentó por primera vez con compatibilidad con IPv6. En esta versión, la red de campus Cisco SD-Access admitía la dirección IP del host con clientes con cable e inalámbricos en doble pila IPv4, IPv6 o IPv4v6 desde la red de fabric superpuesta. La solución consiste en evolucionar continuamente para ofrecer nuevas funciones y características que incorporen fácilmente IPv6 para cualquier empresa.

Cisco SD-Access con arquitectura IPv6

La tecnología de fabric, una parte integral de SD-Access, proporciona redes de campus por cable e inalámbricas con superposiciones programables y una virtualización de red fácil de implementar, que permiten que una red física aloje una o más redes lógicas para cumplir el propósito del diseño. Además de la virtualización de la red, la tecnología de fabric de la red del campus mejora el control de las comunicaciones, lo que proporciona segmentación definida por software y aplicación de políticas basadas en la identidad del usuario y la pertenencia a grupos. Toda la solución de SDN de Cisco se ejecuta en el ADN del fabric. Por lo tanto, es fundamental comprender cada pilar de la solución con respecto a la compatibilidad con IPv6.

- Subcapa: la funcionalidad IPv6 para la superposición depende de la superposición, ya que la superposición IPv6 utiliza el direccionamiento IP de la superposición IPv4 para crear el plano de control del protocolo de separación Localizador/ID (LISP) y túneles del plano de datos de LAN extensible virtual (VXLAN). Siempre puede habilitar la pila doble para el protocolo de ruteo subyacente, solo que el LISP de superposición de SD-Access sólo depende del ruteo IPv4.
- Superposición: cuando se trata de la superposición, SD-Access admite terminales con cables e inalámbricos solo de IPv6. Ese tráfico IPv6 se encapsula en los encabezados IPv4 y VXLAN dentro del fabric de SD-Access hasta que alcanzan los nodos fronterizos del fabric. Los nodos de borde del fabric desencapsulan el encabezado VXLAN e IPv4, que sigue el proceso normal de ruteo unicast IPv6 desde entonces.
- Nodos del Plano de Control: El nodo del Plano de Control está configurado para permitir que todas las subredes de host IPv6 y las rutas de host /128 dentro de los rangos de subred se registren en su base de datos de asignación.
- Nodos de borde: en los nodos de borde, se habilita el peering BGP IPv6 con dispositivos de fusión. El nodo de borde desencapsula el encabezado IPv4 del tráfico de salida del fabric,

mientras que el tráfico IPv6 de entrada también se encapsula con el encabezado IPv4 por los nodos de borde.
- Perímetro del fabric: todas las interfaces virtuales conmutadas (SVI) que se configuran en el perímetro del fabric deben ser IPv6. Esta configuración la envía el controlador del centro DNA.
- Cisco DNA Center: las interfaces físicas de Cisco DNA Center no admiten la doble pila en el momento de la publicación de este documento. Solo puede implementarse en una sola pila con IPv4 o IPv6 en las interfaces empresariales o de gestión del centro DNA.
- Clientes: Cisco SD-Access admite la pila doble (IPv4 e IPv6) o la pila única, ya sea IPv4 o IPv6. Sin embargo, en el caso de que se implemente una sola pila IPv6, DNA Center todavía necesita crear un grupo de pila doble para admitir un cliente solo de IPv6. El IPv4 en el conjunto de pila dual es una dirección ficticia solo como el IPv6 en el que se espera que el cliente desactive la dirección IPv4.

Arquitectura superpuesta de IPv6 en Cisco Software-Defined Access.

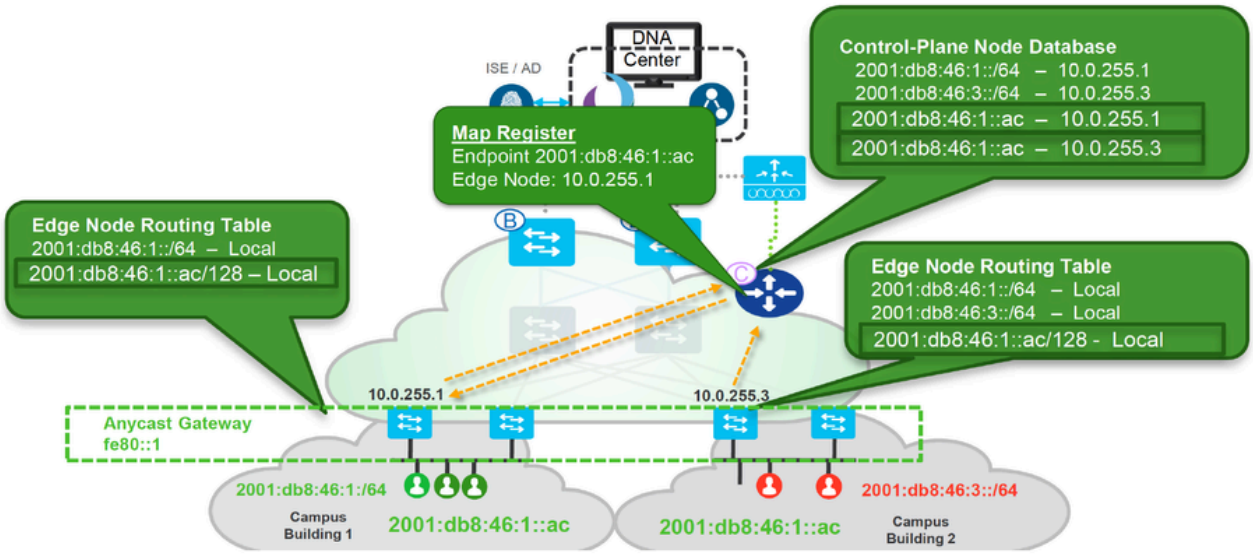


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

Arquitectura superpuesta de IPv6

Habilitación de IPv6 con Cisco DNA-Center

Hay dos formas de habilitar el grupo IPv6 en el Cisco DNA Center:
1. Crear un nuevo conjunto IPv4/v6 de pila doble: totalmente nuevo
2. Edite IPv6 en el conjunto IPv4 que ya existe: migración desde cero

La versión actual (hasta la 2.3.x) de DNA Center no admite IPv6. Sólo un grupo, si el usuario planea admitir un cliente de solo dirección IPv6 único/nativo. Una dirección IPv4 ficticia debe

asociarse al conjunto IPv6. Tenga en cuenta que desde el grupo IPv4 implementado que ya existe con un sitio asociado y edite el grupo con una dirección IPv6. DNA Center proporciona la opción de migración para el fabric de acceso SD, que requiere que el usuario vuelva a aprovisionar el fabric para ese sitio. Se muestra un indicador de advertencia en el fabric al que pertenece el sitio, que indica que el fabric debe "reconfigurarse". Vea estas imágenes para ver ejemplos:

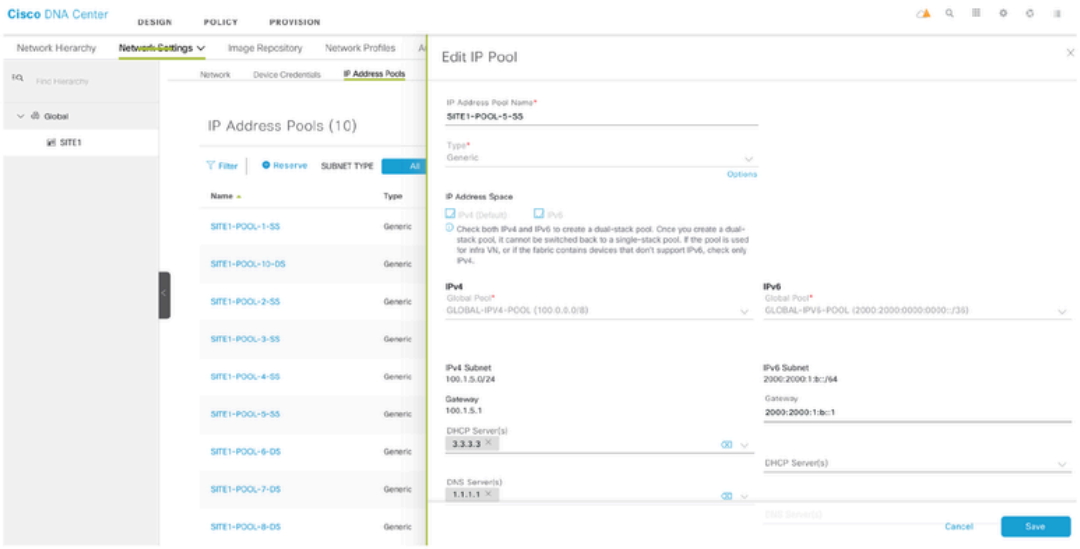


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

Actualización de un único conjunto IPv4 a un conjunto de pila doble mediante la edición de la opción de conjunto IPv4

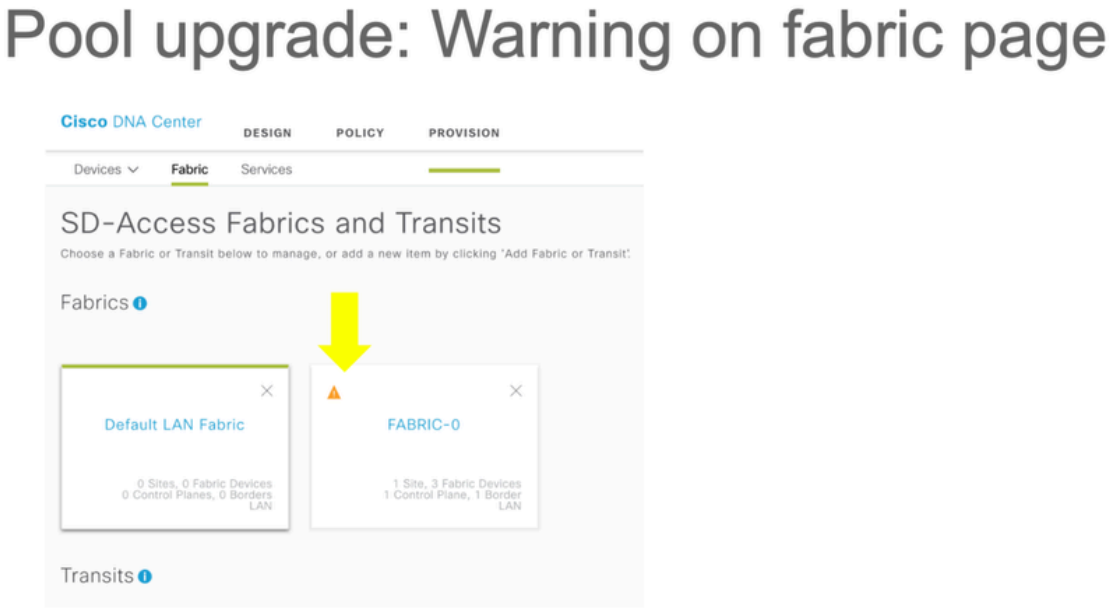


Figure 3.
Fabric has warning indicator which needs to 'reconfigure the fabric'

El fabric tiene un indicador de advertencia que debe "volver a configurar el fabric".

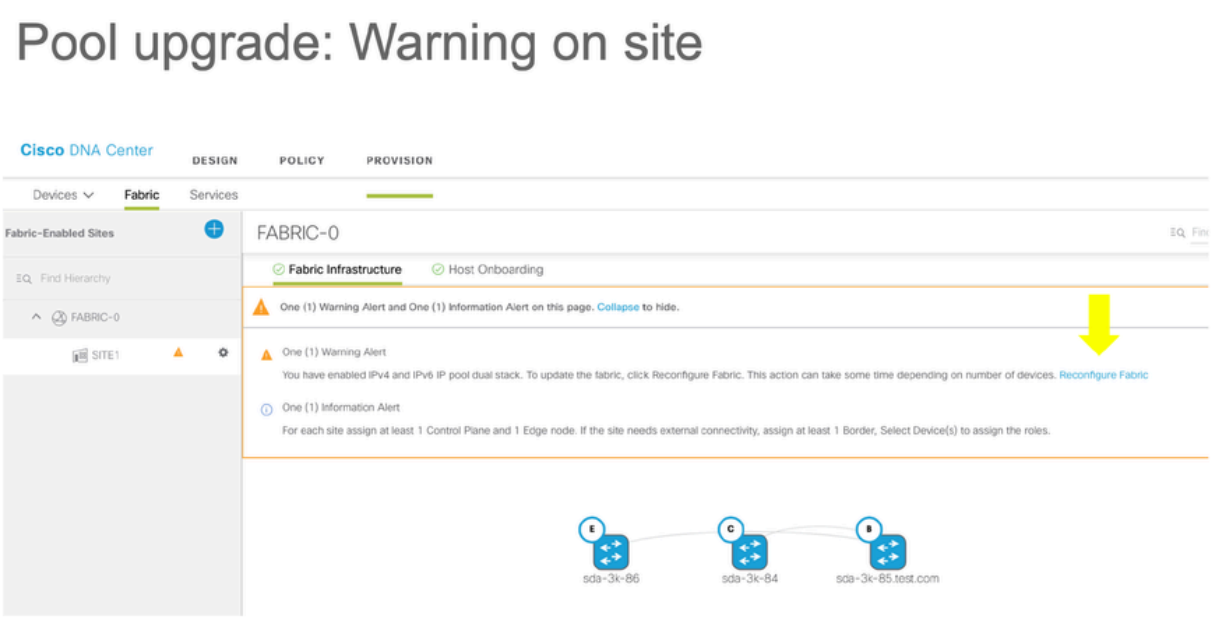


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

El usuario debe hacer clic en "reconfigurar fabric" para volver a aprovisionar automáticamente los nodos de fabric para que la configuración de pila doble surta efecto como parte del proceso de migración

Consideraciones de diseño con IPv6 en Cisco SD-Access

Aunque para los clientes de Cisco SD-Access, pueden ejecutarse con configuraciones de red de pila doble o solo de IPv6, la implementación actual del fabric de SD-Access con la versión 2.3.x.x del switch central DNA (SW) tiene algunas consideraciones sobre la implementación de IPv6.

- Cisco SD-Access es compatible con los protocolos de routing subyacente IPv4. Por lo tanto, el tráfico del cliente IPv6 se transporta cuando se encapsula dentro de los encabezados IPv4. Este es un requisito para la implementación actual del software LISP. Sin embargo, esto no significa que la capa subyacente no pueda habilitar el protocolo de ruteo IPv6, solo que el LISP de superposición de SD-Access no se ejecuta en función de su dependencia.
- No se admite multidifusión nativa IPv6, ya que la estructura subyacente solo puede ser IPv4 en este momento.
- La conexión inalámbrica para invitados solo se puede ejecutar con la pila doble. Debido a la versión actual de Identity Services Engine (ISE) (por ejemplo, hasta 3.2), el portal de invitados IPv6 no es compatible, por lo que un cliente invitado solo de IPv6 no podrá autenticarse.
- La versión actual de DNA Center no admite la automatización de políticas de QoS de aplicaciones IPv6. Este documento describe los pasos necesarios para implementar QoS IPv6 para clientes de doble pila por cable e inalámbricos en Cisco SD-Access que se había implementado para uno de los usuarios a gran escala.
- La función de limitación de velocidad del cliente inalámbrico para el tráfico ascendente y descendente por identificador de conjunto de servicios (SSID) o por cliente en función de la

política es compatible con IPv4 (TCP/UDP) e IPv6 (TCP únicamente). Aún no se admite el límite de velocidad UDP IPv6.
- El grupo IPv4 se puede actualizar a un grupo de pila doble. Sin embargo, un conjunto de pila doble no se puede degradar a un conjunto IPv4. Si el usuario desea volver a quitar el grupo de pila doble al grupo de pila única IPv4, debe liberar todo el grupo de pila doble.
- Aún no se admite IPv6 única, mientras que solo se puede crear IPv4 o conjunto de pila doble en el DNA Center actual.
- La plataforma de Cisco IOS® XE es un requisito de versión de software mínimo de 16.9.2 y versiones posteriores.
- La conexión inalámbrica de invitado IPv6 aún no se admite en las plataformas Cisco IOS XE, mientras que AireOS (8.10.105.0+) admite una solución alternativa.
- No se puede asignar un conjunto de pila doble en INFRA_VN, donde solo se puede asignar un punto de acceso (AP) o un conjunto de nodos extendido.
- La automatización de LAN aún no admite IPv6.

Además de las limitaciones mencionadas anteriormente, al diseñar un fabric de acceso SD con IPv6 habilitado, siempre debe tener en cuenta la escalabilidad de cada componente del fabric. Si un terminal tiene varias direcciones IPv4 o IPv6, cada dirección se cuenta como una entrada individual.

Las entradas de host de fabric incluyen puntos de acceso y nodos clásicos y ampliados por políticas.

Consideraciones adicionales sobre la escala del nodo de borde:

Las entradas /32 (IPv4) o /128 (IPv6) se utilizan cuando el nodo de borde reenvía el tráfico desde fuera del fabric a un host del fabric.

Para todos los switches excepto los switches de alto rendimiento Catalyst de Cisco serie 9500 y los switches Catalyst de Cisco serie 9600:

- IPv4 utiliza una entrada de memoria de contenido ternario direccionable (TCAM) (entradas de host de fabric) para cada dirección IP de IPv4.
- IPv6 utiliza dos entradas TCAM (entradas de host de fabric) para cada dirección IP IPv6.

Para los switches de alto rendimiento Catalyst de Cisco serie 9500 y los switches Catalyst de Cisco serie 9600:

- IPv4 utiliza una entrada TCAM (entradas de host de fabric) para cada dirección IP IPv4.
- IPv6 utiliza una entrada TCAM (entradas de host de fabric) para cada dirección IP IPv6.

Además, algunos de los terminales no son compatibles con DHCPv6, como los smartphones con sistema operativo Android que se basan en la configuración automática de direcciones sin estado (SLAAC) para obtener direcciones IPv6. Un único terminal puede acabar con más de dos direcciones IPv6. Este comportamiento consume más recursos de hardware en cada nodo de fabric, especialmente en los nodos de control y de borde de fabric. Por ejemplo, cada vez que el nodo de borde desea enviar tráfico a los nodos de borde para cualquier terminal, instala una ruta

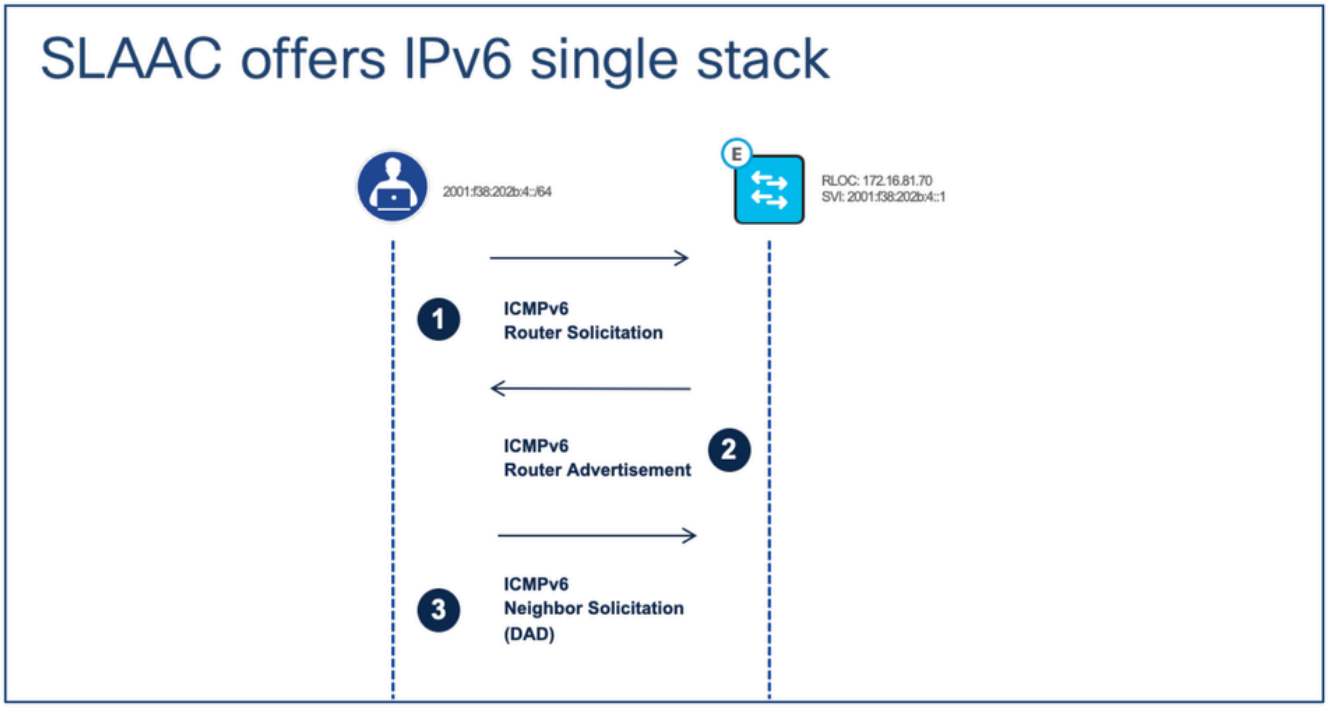
de host en la entrada TCAM y graba una entrada de adyacencia VXLAN en el TCAM de hardware (HW).

Conexiones de clientes por cable e inalámbricas y flujos de llamadas

Una vez que el cliente está conectado al Fabric Edge, hay diferentes maneras en las que obtiene las direcciones IPv6. Esta sección trata sobre la forma más común de direccionamiento IPv6 del cliente, es decir, SLAAC y DHCPv6.

Asignación de dirección IPv6 - SLAAC

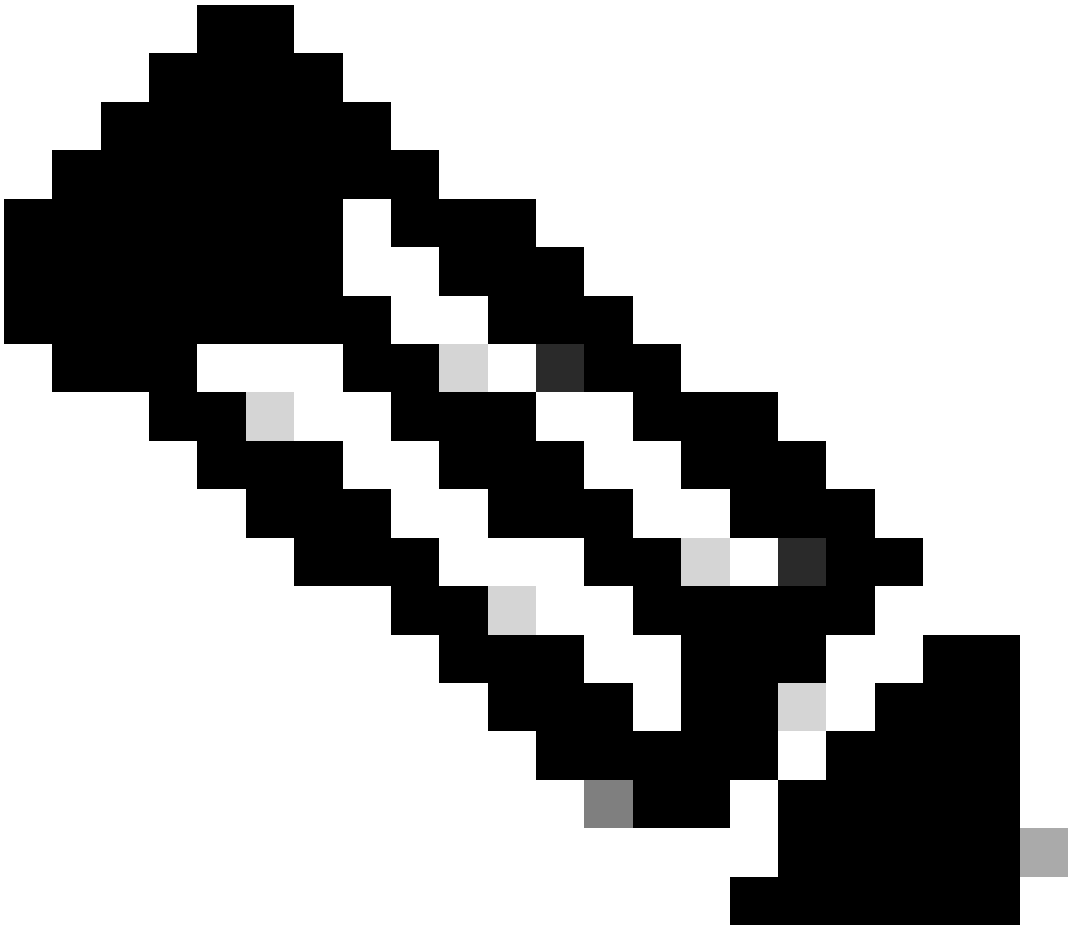
El SLAAC en el acceso definido por software (SDA) no es diferente del flujo de proceso SLAAC estándar. Para que SLAAC funcione correctamente, el cliente IPv6 debe configurarse con una dirección local de link en su interfaz; la forma en que el cliente se configura automáticamente con la dirección local de link está fuera del alcance de este documento.



Asignación de dirección IPv6 - SLAAC

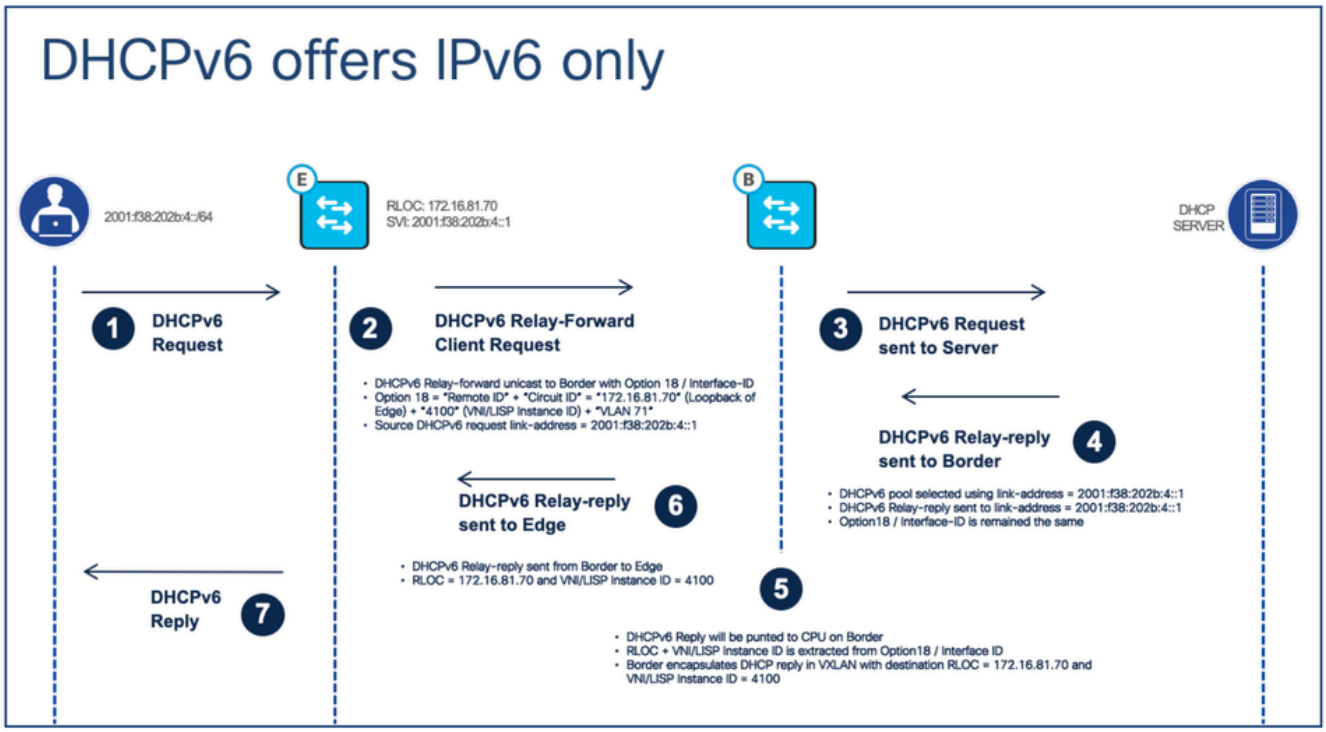
Descripción del flujo de llamadas:
Paso 1. Una vez que el cliente IPv6 se configura a sí mismo con una dirección local de vínculo IPv6, el cliente envía un mensaje de solicitud de enrutador (RS) ICMPv6 al extremo del fabric. El propósito de este mensaje es obtener el prefijo unicast global de su segmento conectado.
Paso 2. Después de que el borde del fabric reciba el mensaje RS, responde con un mensaje de anuncio de router ICMPv6 (RA) que contiene el prefijo unicast IPv6 global y su longitud interna.
Paso 3. Una vez que el cliente recibe el mensaje RA, combina el prefijo unicast global IPv6 con su identificador de interfaz EUI-64 para generar su dirección unicast global IPv6 única y establecer

su gateway a la dirección local de link de la SVI de la frontera de la estructura que está relacionada con el segmento del cliente. A continuación, el cliente envía un mensaje de solicitud de vecino ICMPv6 para realizar la detección de direcciones duplicadas (DAD) y asegurarse de que la dirección IPv6 que obtiene es única.



Nota: Todos los mensajes relacionados con SLAAC se encapsulan con la dirección local de enlace IPv6 SVI del cliente y el nodo de fabric.

Asignación de direcciones IPv6 - DHCPv6

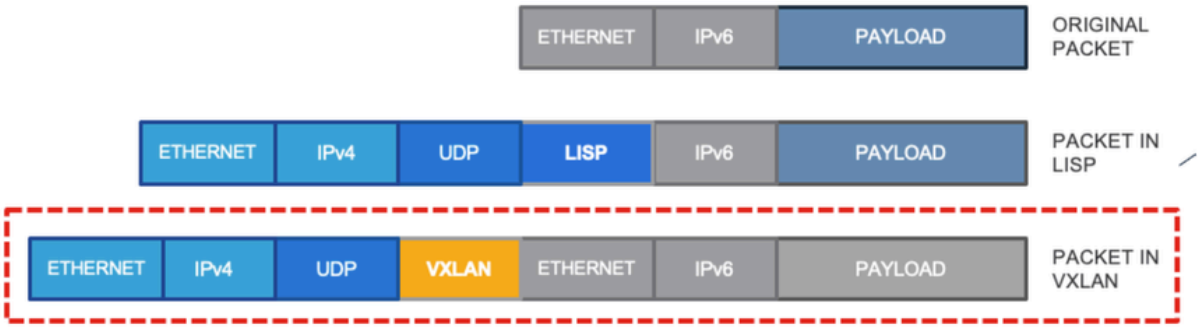


Asignación de direcciones IPv6 - DHCPv6

Descripción del flujo de llamadas:
Paso 1. El cliente envía la solicitud DHCPv6 al borde del fabric.
Paso 2. Cuando el borde del fabric recibe la solicitud DHCPv6, utilizará el mensaje de retransmisión DHCPv6 para unidifusión de la solicitud al borde del fabric con la opción 18 de DHCPv6. En comparación con la opción 82 de DHCP, la opción 18 de DHCPv6 codifica conjuntamente 'ID de circuito' e 'ID remoto'. El ID/VNI de instancia de LISP, el localizador de routing IPv4 (RLOC) y la VLAN de terminal están codificando en su interior.
Paso 3. El borde del fabric desencapsula el encabezado VXLAN y unidifusión el paquete DHCPv6 al servidor DHCPv6.
Paso 4. El servidor DHCPv6 recibe el mensaje de retransmisión, utiliza la dirección de enlace de origen (agente de retransmisión DHCPv6/gateway del cliente) del mensaje para elegir el conjunto IPv6 para asignar la dirección IPv6. A continuación, envíe el mensaje de respuesta de retransmisión DHCPv6 a la dirección del gateway del cliente. La opción 18 se mantiene sin cambios.
Paso 5. Cuando el borde del entramado recibe el mensaje relay-reply, extrae la instancia/VNI RLOC y LISP de la opción 18. El borde del entramado encapsula el mensaje relay-reply en VXLAN con un destino que extrajo de la opción 18.
Paso 6. El borde del fabric envía el mensaje de respuesta de retransmisión DHCPv6 al borde del fabric al que se conecta el cliente.
Paso 7. Cuando el borde del entramado recibe el mensaje de respuesta de retransmisión DHCPv6, desencapsula el encabezado VXLAN del mensaje y reenvía el mensaje al cliente. A continuación, el cliente conoce su dirección IPv6 asignada.

Comunicación IPv6 en Cisco SD-Access

La comunicación IPv6 utiliza el plano de control basado en LISP estándar y los métodos de comunicación del plano de datos basados en VXLAN. Con la implementación actual en Cisco SD-Access LISP y VXLAN utiliza el encabezado IPv4 exterior para transportar los paquetes IPv6 dentro. Esta imagen captura este proceso.



Encabezado IPv4 exterior que lleva los paquetes IPv6 dentro

Esto significa que todas las consultas LISP utilizan el paquete nativo IPv4, mientras que la tabla de nodos del plano de control tiene detalles sobre el RLOC con las direcciones IP IPv6 e IPv4 del terminal. Este proceso se explica con detalle en la siguiente sección desde la perspectiva de los terminales inalámbricos.

Comunicación IPv6 inalámbrica en Cisco SD-Access

La comunicación inalámbrica se basa en dos componentes específicos: puntos de acceso y controladores de LAN inalámbrica, aparte de los componentes típicos de Cisco SD-Access Fabric. Los puntos de acceso inalámbricos crean un túnel de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP) con el controlador de LAN inalámbrica (WLC). Mientras que el tráfico del cliente existe en el borde del entramado, otra comunicación del plano de control que incluye las estadísticas de radio es administrada por el WLC. Desde una perspectiva IPv6, tanto el WLC como el AP deben tener las direcciones IPv4 y todas las comunicaciones CAPWAP utilizan estas direcciones IPv4. Mientras que el WLC y el AP no-Fabric soportan la comunicación IPv6, Cisco SD-Access utiliza el IPv4 para todas las comunicaciones que llevan cualquier tráfico IPv6 del cliente dentro de los paquetes IPv4. Esto significa que los agrupamientos AP asignados bajo Infra VN no se pueden asignar con agrupamientos IP que son de doble pila y se arroja un error si se hace cualquier intento de esta asignación. La comunicación inalámbrica dentro de Cisco SDA se puede dividir en las siguientes tareas principales:

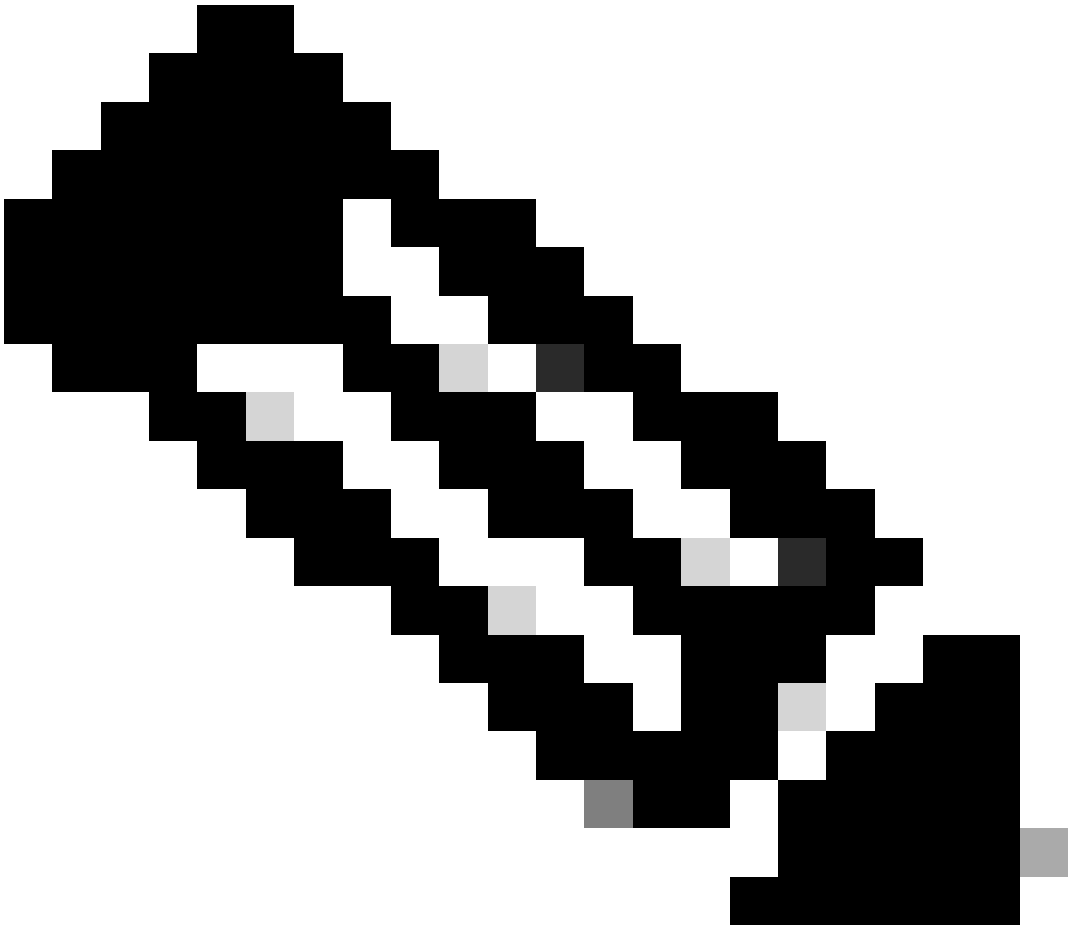
- Incorporación de puntos de acceso
- Incorporación de clientes

Observe estos eventos desde una perspectiva IPv6.

Incorporación de puntos de acceso

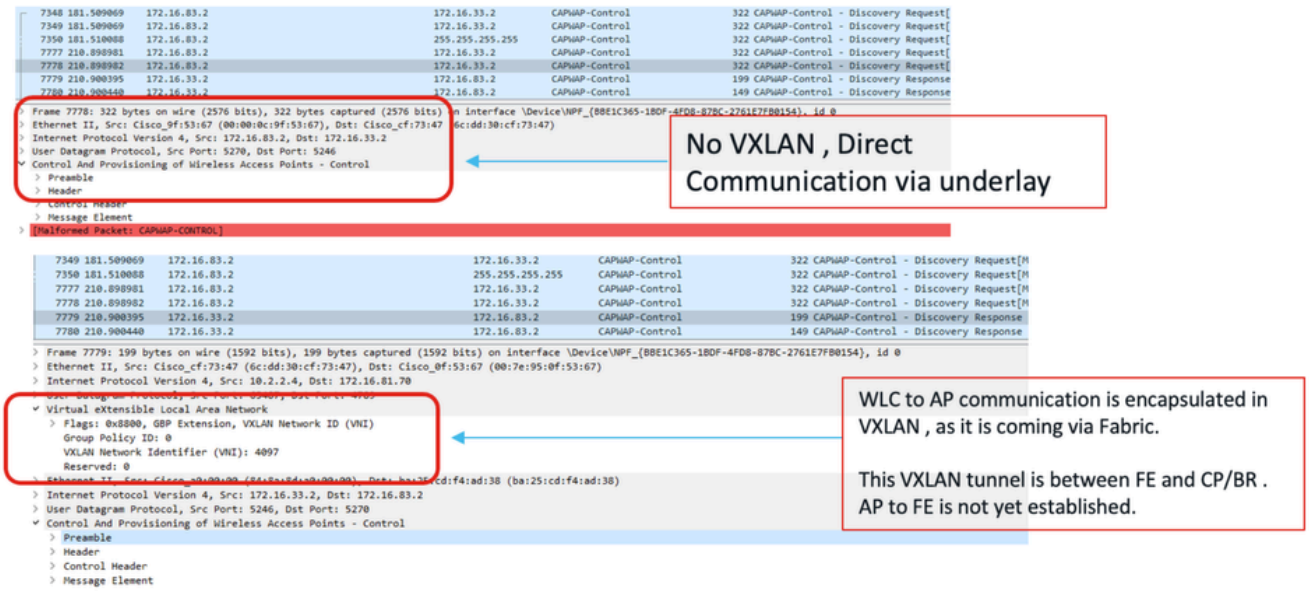
Este proceso sigue siendo el mismo para IPv6 e IPv4, ya que tanto el WLC como el AP tienen direcciones IPv4 y pasos incluidos aquí:
1. El puerto Fabric Edge (FE) se configura para el AP incorporado.
2. El AP se conecta al puerto FE, y a través del AP CDP notifica al FE sobre su presencia (esto permite que el FE asigne la VLAN correcta).
3. El AP obtiene la dirección IPv4 del servidor DHCP y el FE registra el AP y actualiza el plano de control (nodo del plano de control (CP)) con los detalles del AP.
4. AP se une al WLC a través de métodos tradicionales (como la opción 43 de DHCP).
5. El WLC verifica si el AP es apto para el entramado y consulta el plano de control para la información de RLOC del AP (por ejemplo, RLOC solicitada/respuesta recibida).
6. CP responde con la IP RLOC del AP al WLC.
7. El WLC registra el control de acceso a los medios (dirección) (MAC) del AP en el CP.
8. CP actualiza el FE con los detalles del WLC sobre el AP (esto indica al FE que inicie el túnel VXLAN con el AP).

FE procesa la información y crea un túnel VXLAN con AP. En este punto, el AP anuncia el SSID habilitado para el entramado.



Nota: En caso de que el AP difunda los SSID que no son de fabric y no difunda el SSID de fabric, verifique el túnel VXLAN entre el punto de acceso y el nodo de borde del fabric.

Además, tenga en cuenta que la comunicación de AP a WLC siempre sucede a través de CAPWAP subyacente y toda la comunicación de WLC a AP utiliza VXLAN CAPWAP a través de la superposición. Esto significa que, si usted captura los paquetes que van del AP al WLC, usted ve solamente CAPWAP mientras que el tráfico inverso tiene un túnel VXLAN. Vea este ejemplo para la comunicación entre el AP y el WLC.



Capturas de paquetes del punto de acceso al WLC (túnel CAPWAP) frente al WLC al punto de acceso (túnel VxLAN en el fabric)

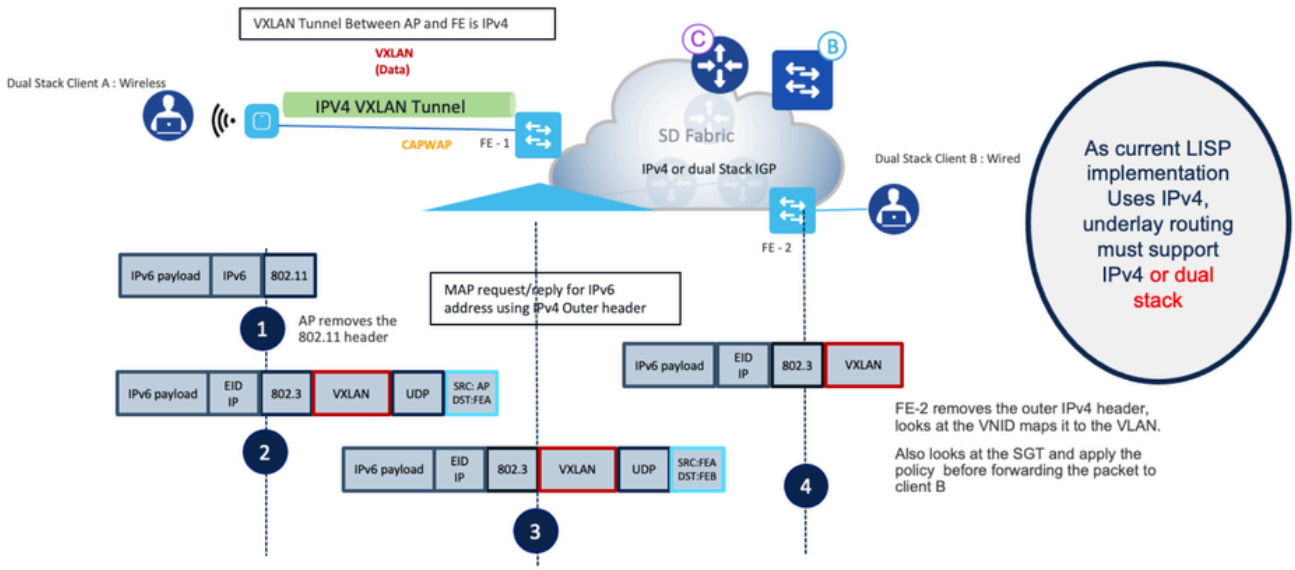
Incorporación de clientes

El proceso de incorporación de cliente IPv6/pila dual sigue siendo el mismo, pero el cliente utiliza los métodos de asignación de direcciones IPv6 como SLAAC/DHCPv6 para obtener las direcciones IPv6.
1. El cliente se une al entramado y habilita el SSID en el AP.
2. El WLC conoce el RLOC AP.
3. El cliente autentica y el WLC registra los detalles del cliente L2 con el CP y actualiza el AP.
4. El cliente inicia el direccionamiento IPv6 desde los métodos configurados: SLAAC/DHCPv6.
5. FE activa el registro del cliente IPv6 en la base de datos de seguimiento de host (HTDB) de CP. AP a FE y FE a otros destinos utilizan la encapsulación VXLAN y LISP IPv6 dentro de las tramas IPv4.

Comunicación cliente-cliente con IPv6

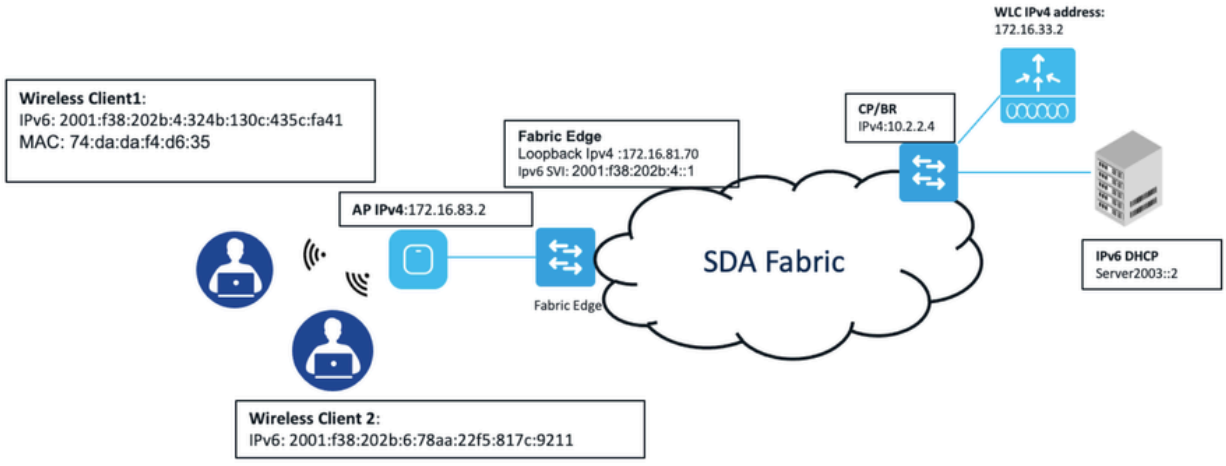
En la imagen siguiente se resume el proceso de comunicación del cliente inalámbrico IPv6 con

otro cliente con cables IPv6. (Esto supone que el cliente está autenticado y obtuvo la dirección IPv6 a través de métodos configurados).
1. El cliente envía las tramas 802.11 al AP con carga útil IPv6.
2. El AP elimina los encabezados 802.11 y envía la carga útil IPv6 original en el túnel VXAN IPv4 al borde del fabric.
3. Fabric Edge utiliza la solicitud de protocolo de acceso a mensajes (MAP) para identificar el destino y envía la trama al RLOC de destino con VXLAN IPv4.
4. En el switch de destino, se elimina el encabezado VXLAN IPv4 y el paquete IPv6 se envía al cliente.

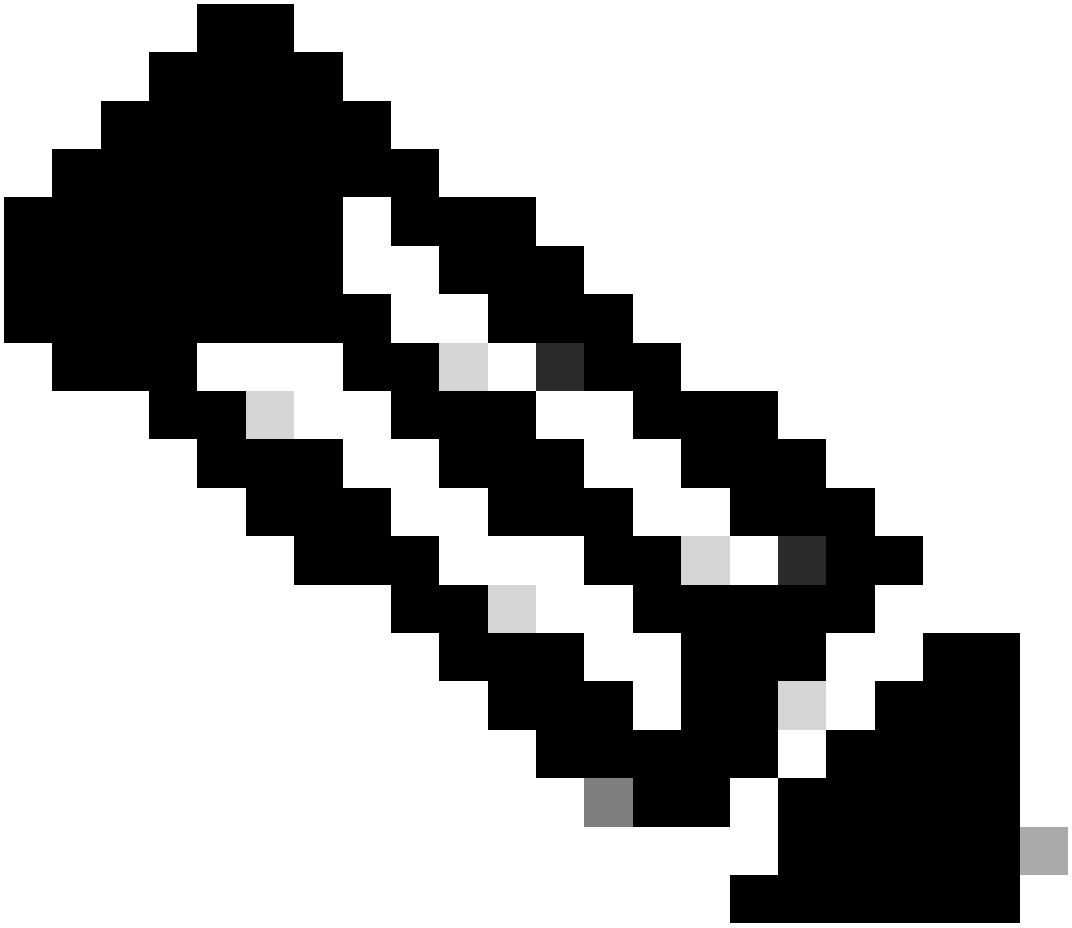


Flujo de paquetes de cliente por cable de doble pila a cliente inalámbrico de doble pila

Examine en profundidad este proceso con las capturas de paquetes y consulte la imagen para obtener detalles de las direcciones IP y MAC. Tenga en cuenta que esta configuración utiliza clientes de doble pila conectados con los mismos puntos de acceso pero asignados a diferentes subredes IPv6 (SSID).

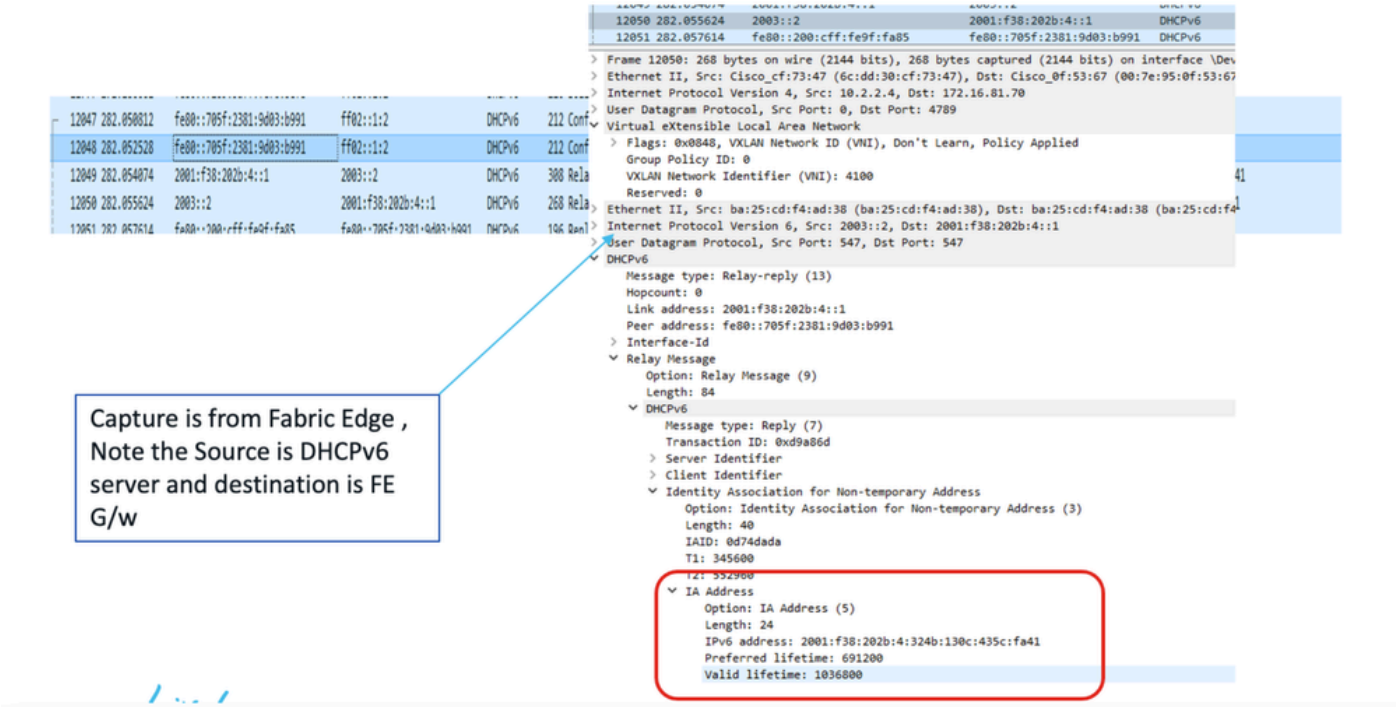


Detalle de direcciones IP y direcciones MAC de red de acceso SD de ejemplo



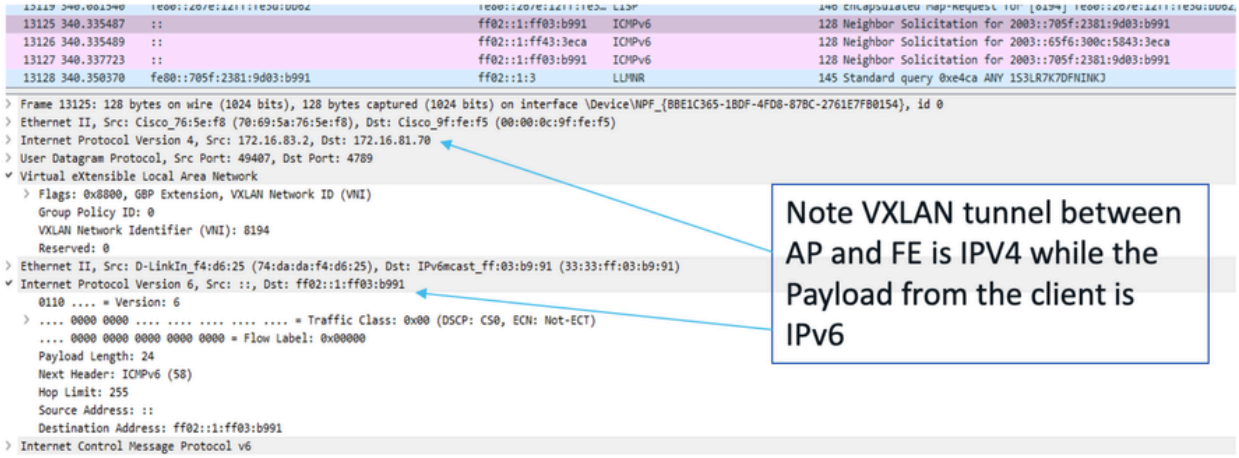
Nota: Para cualquier comunicación IPv6 fuera del fabric, por ejemplo, DHCP/DNS, debe habilitarse el routing IPv6 entre la infraestructura de frontera y la que no es de fabric.

Paso 1. El cliente autentica y obtiene la dirección IPv6 de los métodos configurados.



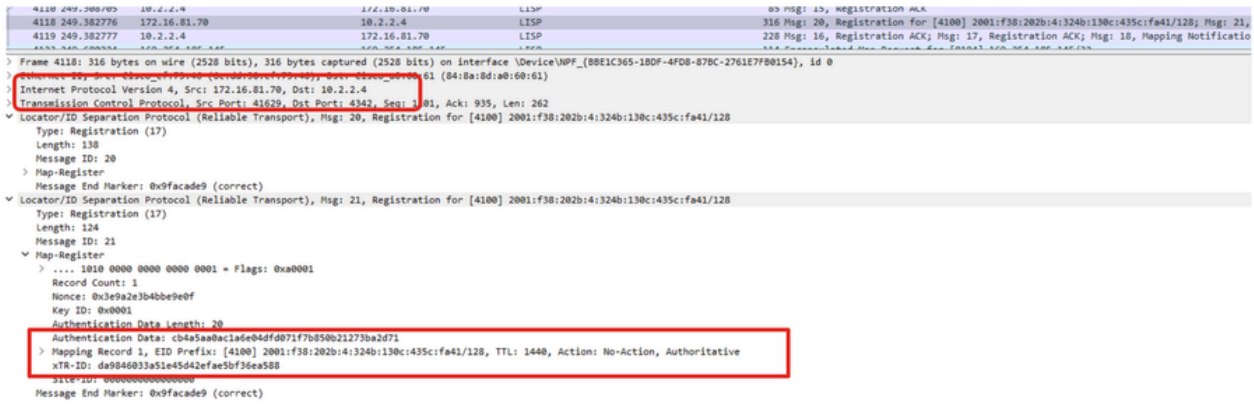
Captura de paquetes del servidor DHCPv6 al nodo de fabric perimetral

Paso 2. El cliente inalámbrico envía las tramas 802.11 al punto de acceso con la carga útil IPv6.
Paso 3. El punto de acceso elimina el encabezado inalámbrico y envía el paquete al extremo del fabric. Utiliza el encabezado de túnel VXLAN, que se basa en IPv4, ya que el punto de acceso tiene la dirección IPv4.



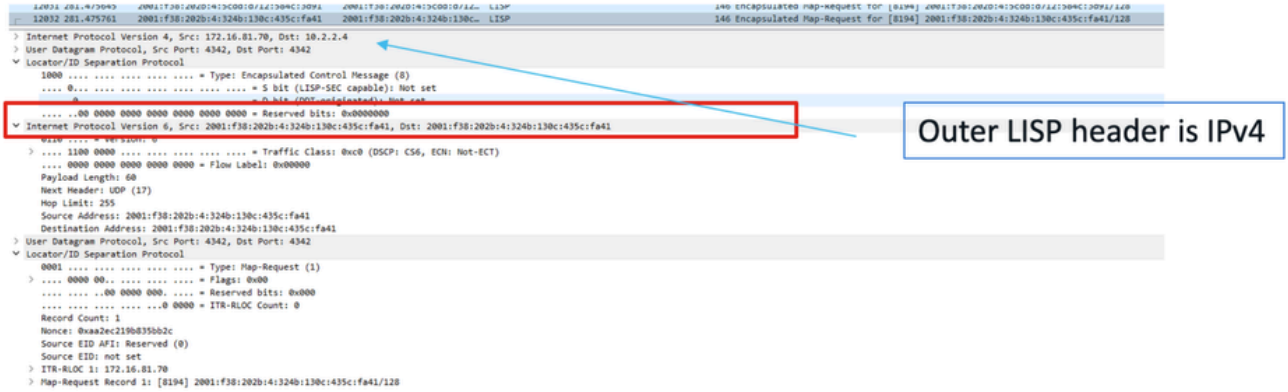
Captura de paquetes para el túnel VxLAN entre FE y AP

Paso 3.1. Fabric Edge registra el cliente IPv6 con el plano de control. Utiliza el método de registro IPv4 con los detalles del cliente IPv6 en el interior.



Captura de paquetes para registros FE con plano de control para cliente IPv6

Paso 3.2. FE envía la solicitud MAP al plano de control para identificar el RLOC de destino.



Captura de paquetes de FE a CP con mensajes de registro MAP

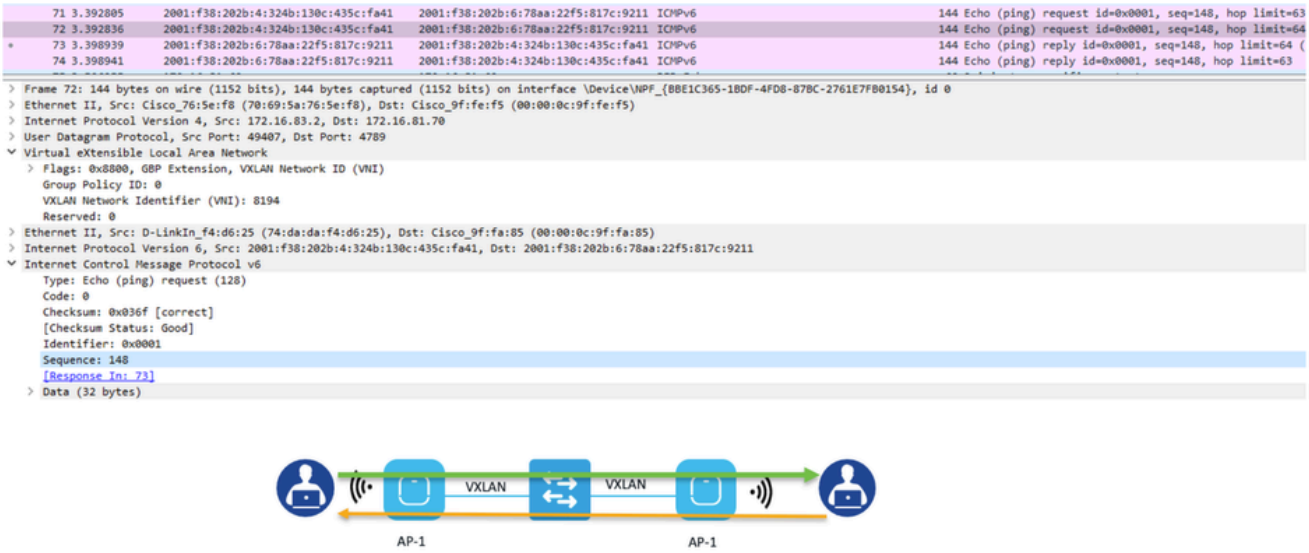
Fabric Edge también mantiene la memoria caché de MAP para clientes IPv6 conocidos, como se muestra en esta imagen.

```
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#
```

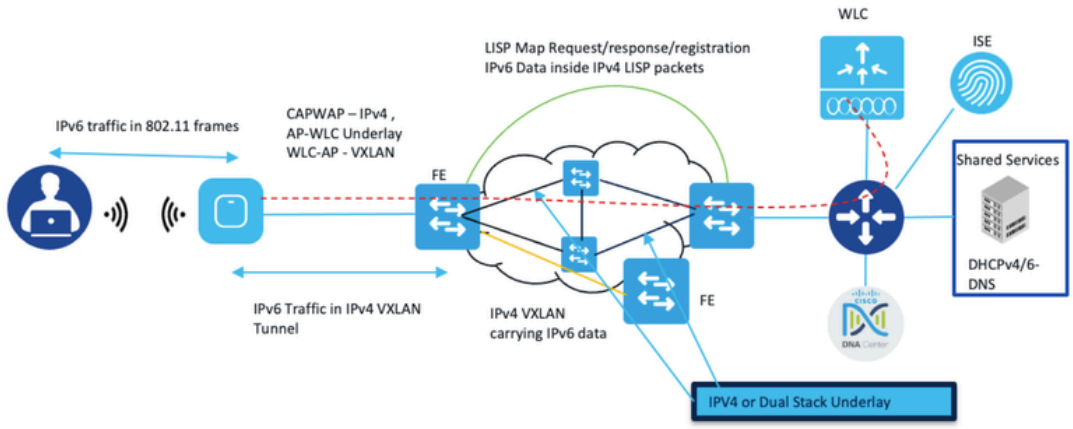
Salida de pantalla de Fabric Edge de información de caché de mapas superpuestos de IPv6

Paso 4. El paquete se reenvía al RLOC de destino con el VXLAN IPv4 que transporta la carga útil IPv6 original en su interior. Como ambos clientes están conectados al mismo AP, el ping IPv6 toma esta trayectoria.

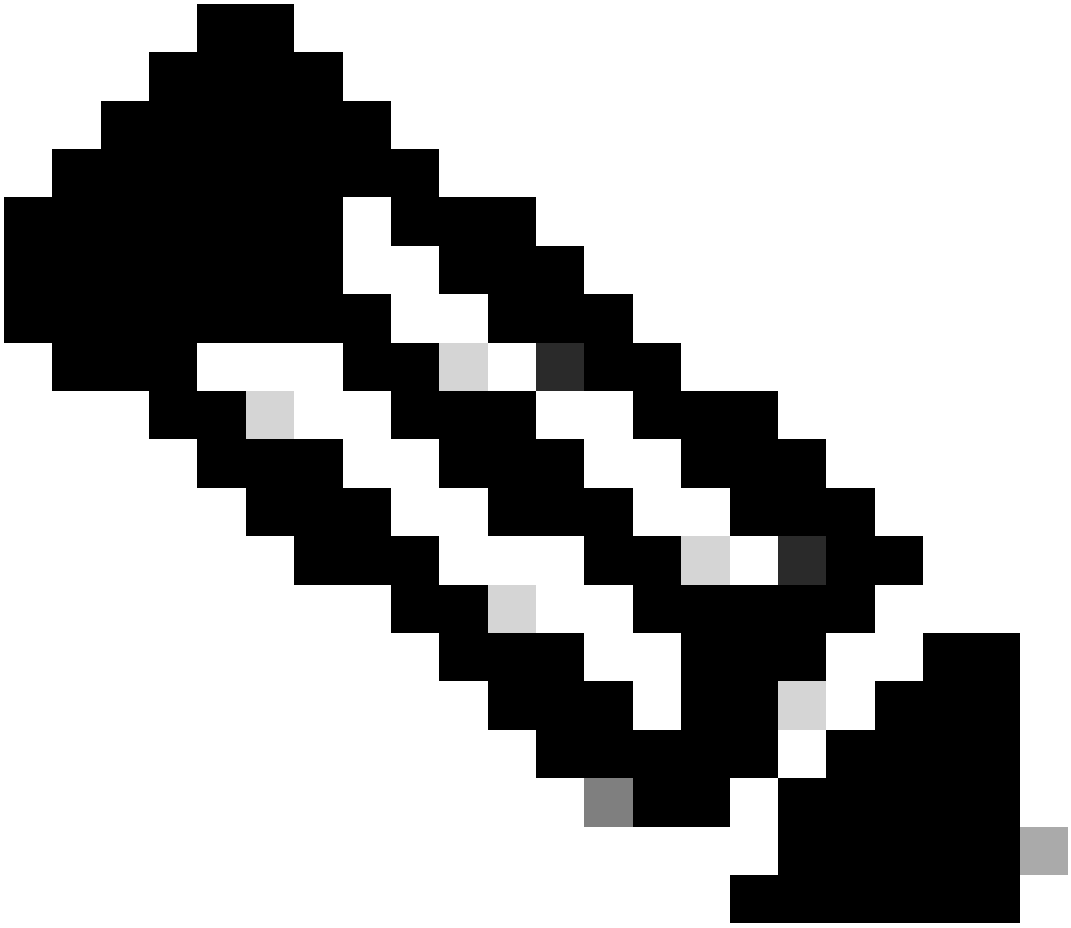


Captura de paquetes para ping IPv6 entre dos clientes inalámbricos registrados en el mismo AP

Esta imagen resume la comunicación IPv6 desde la perspectiva del cliente inalámbrico.



En la figura se resume la comunicación IPv6 desde la perspectiva del cliente inalámbrico



Nota: No se admite el acceso de invitado IPv6 (portal web) a través de Cisco Identity Services debido a las limitaciones de ISE.

Matriz de dependencia

Es importante tener en cuenta las dependencias y la compatibilidad con IPv6 de los diferentes componentes inalámbricos que forman parte de Cisco SD-Access. La tabla de esta imagen resume esta matriz de funciones.

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

Características de Cat9800 WLC IPv6 por versión

Supervisión del plano de control para IPv6

Una vez que habilite IPv6, comenzará a ver entradas adicionales sobre el host IPv6 en los servidores del servidor de mapas (MS)/resolución de mapas (MR). Como un host puede tener varias direcciones IP IPv6, la tabla de búsqueda de MS/MR tiene entradas para todas las direcciones IP. Esto se combina con la tabla IPv4 que ya existe.
Debe iniciar sesión en la CLI del dispositivo y ejecutar estos comandos para verificar todas las entradas.

```
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
```

También puede comprobar los detalles sobre el host IPv6 a través de la garantía.

Implementación de QoS IPv6 en Cisco SD-Access

La versión actual de Cisco DNA Center (hasta la 2.3.x) no admite la automatización de la política de aplicaciones de QoS de IPv6. Sin embargo, los usuarios pueden crear manualmente plantillas inalámbricas y por cable IPv6, así como insertar la plantilla de QoS en los nodos periféricos del fabric. Dado que DNA Center automatiza la política de QoS de IPv4 en todas las interfaces físicas una vez aplicadas, puede insertar manualmente un mapa de clase (que coincida con la lista de control de acceso (ACL) de IPv6) antes de 'class-default' a través de una plantilla.

Este es el ejemplo de plantilla con QoS de IPv6 por cable integrada con la configuración de políticas generada por DNA Center:

```
!
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
```


```
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
```

Troubleshooting de IPv6 en Cisco SD-Access

Solucionar problemas de SD-Access IPv6 es muy similar a IPv4, siempre puede utilizar el mismo comando con diferentes opciones de palabras clave para lograr el mismo objetivo. Esto muestra algunos comandos que se utilizan con frecuencia para resolver problemas de SD-Access.

```
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
```

Desde el nodo de borde para verificar el ping del servidor DHCPv6 de superposición:

```
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
```

Preguntas frecuentes rápidas sobre el diseño de IPv6 con Cisco SD-Access

P. ¿La red definida por software de Cisco admite IPv6 para redes subyacentes y superpuestas?
R. La versión actual (2.3.x) sólo admite la superposición en el momento de escribir este documento.

P. ¿Es Cisco SDN compatible con IPv6 nativo tanto para clientes por cable como inalámbricos?
R. Sí. Esto requiere grupos de pila dual que se crean en el centro de DNA, mientras que IPv4 es el grupo ficticio, ya que los clientes desactivan las solicitudes DHCP de IPv4 y solo se ofrecen direcciones DHCP o SLAAC de IPv6.

P. ¿Puedo tener una red de campus nativa solo de IPv6 en mi Cisco SD-Access Fabric?
A. No con la versión actual (hasta 2.3.x). Está en la hoja de ruta.

P. ¿Es Cisco SD-Access compatible con la transferencia de IPv6 de nivel 2?
R: No en este momento. Solo se admite transferencia de L2 IPv4 o L3 Dual-Stack.

P. ¿Cisco SD-Access admite multidifusión para IPv6?
R. Sí, solo se admite IPv6 superpuesta con multidifusión de replicación de cabecera. La multidifusión IPv6 nativa todavía no es compatible.

P. ¿Admite Cisco SD-Access Fabric Enabled Wireless invitados en doble pila?
R. Aún no compatible con el WLC Cisco IOS XE (Cat9800). El WLC de AireOS se soporta a través de una solución alternativa. Para obtener más información sobre la implementación de la solución alternativa, póngase en contacto con el equipo de experiencia del cliente de Cisco.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).