IPv6 implementeren in Software-Defined Access

Inhoud

Inleiding

In dit document wordt beschreven hoe u IPv6 implementeert in Cisco® Software-Defined Access (SD-Access).

Achtergrondinformatie

IPv4 werd uitgebracht in 1983 en is nog steeds in gebruik voor het grootste deel van het internetverkeer. De 32-bits IPv4-adressering maakte meer dan 4 miljard unieke combinaties mogelijk. Echter, door de toename van het aantal internet-verbonden clients, is er een tekort aan unieke IPv4-adressen. In de jaren negentig werd de uitputting van IPv4-adressering onvermijdelijk. In afwachting hiervan introduceerde Internet Engineering Taskforce de IPv6-standaard. IPv6 maakt gebruik van 128-bits en biedt 340 undecillion unieke IP-adressen, wat meer dan genoeg is om tegemoet te komen aan de behoefte van verbonden apparaten die groeien. Aangezien steeds meer moderne eindpuntapparaten dual-stack en/of single IPv6-stack ondersteunen, is het voor elke organisatie van cruciaal belang om klaar te zijn voor de adoptie van IPv6. Dit betekent dat de gehele infrastructuur klaar moet zijn voor IPv6. Cisco SD-Access is de evolutie van traditionele campusontwerpen naar de netwerken die direct de intentie van een organisatie implementeren. Cisco Software Defined Networks is nu klaar voor dual-stack (IPv6-apparaten).

Een grote uitdaging voor elke organisatie bij de adoptie van IPV6 is het verandermanagement en de complexiteit die gepaard gaat met de migratie van oudere IPv4-systemen naar IPv6. Dit artikel behandelt alle details over de ondersteuning van IPv6-functies op Cisco SDN, strategie en kritieke pitspots, die moeten worden verzorgd wanneer u IPv6 met Cisco Software Defined Networks gebruikt.

In augustus 2019 werd Cisco Digital Network Architecture (DNA) Center versie 1.3 voor het eerst geïntroduceerd met de ondersteuning van IPv6. In deze release ondersteunde het Cisco SD-Access campusnetwerk het host-IP-adres met bekabelde en draadloze clients in IPv4, IPv6 of IPv4v6 Dual-stack van het overlay fabric-netwerk. De oplossing is om voortdurend te evolueren om nieuwe functies en functionaliteiten te brengen die gemakkelijk aan boord van de IPv6 voor elke onderneming.

Cisco SD-Access met IPv6-architectuur

Fabric-technologie, een integraal onderdeel van SD-Access, biedt bekabelde en draadloze campusnetwerken met programmeerbare overlays en eenvoudig te implementeren netwerkvirtualisatie, waarmee een fysiek netwerk een of meer logische netwerken kan hosten om aan de ontwerpintentie te voldoen. Naast netwerkvirtualisatie verbetert de fabric-technologie in het campusnetwerk de controle over communicatie, die software-gedefinieerde segmentatie en beleidshandhaving biedt op basis van gebruikersidentiteit en groepslidmaatschap. De volledige Cisco SDN-oplossing draait op het DNA van de stof. Daarom is het van cruciaal belang om elke pijler van de oplossing te begrijpen met betrekking tot IPv6-ondersteuning.

- Underlay - IPv6-functionaliteit voor Overlay is afhankelijk van de underlay, omdat de IPv6-overlay gebruikmaakt van de IPv4-onderlay IP-adressering om Locator/ID Separation Protocol (LISP)-controlevlak en Virtual Extensible LAN (VXLAN)-dataplantunnels te maken. U kunt altijd de dual-stack inschakelen voor het onderliggende routeringsprotocol, alleen de SD-Access-overlay LISP is alleen afhankelijk van de IPv4-routering.
- Overlay - Als het gaat om de overlay, ondersteunt SD-Access zowel bekabelde als draadloze eindpunten met alleen IPv6. Dat IPv6-verkeer wordt ingekapseld in de IPv4- en VXLAN-header binnen de SD-Access-structuur totdat ze de knooppunten van de fabric-rand bereiken. De fabric border nodes decapsuleren de IPv4- en VXLAN-header, die vanaf dat moment het normale IPv6 unicast-routeringsproces volgt.
- Control Plane Nodes - De Control Plane node is geconfigureerd om alle IPv6-hostsubnetten en de /128-hostroutes binnen de subnetbereiken te registreren in de toewijzingsdatabase.
- Grensknooppunten - Op de grensknooppunten is IPv6 BGP-peering met fusieapparaten ingeschakeld. Het border-knooppunt decapsuleert de IPv4-header van het fabric-egress-verkeer, terwijl het ingress IPv6-verkeer ook door de border-knooppunten wordt ingekapseld met de IPv4-header.
- Fabric Edge – Alle geschakelde virtuele interfaces (SVI's) die in Fabric Edge zijn geconfigureerd, moeten IPv6 zijn. Deze configuratie wordt aangestuurd door de DNA Center Controller.
- Cisco DNA Center – De fysieke interfaces van het Cisco DNA Center ondersteunen geen dual-stack vanaf het moment dat dit document wordt gepubliceerd. Het kan alleen in één

stapel worden geïmplementeerd met IPv4 of IPv6 alleen in de beheer- en of bedrijfsinterfaces van het DNA Center.
- Clients – Cisco SD-Access ondersteunt dual-stack (IPv4 en IPv6) of single-stack IPv4 of IPv6. In het geval dat een enkele IPv6-stack wordt geïmplementeerd, moet DNA Center echter nog steeds een pool met dubbele stack maken om een client met alleen IPv6 te ondersteunen. De IPv4 in de pool met dubbele stapels is alleen een dummy-adres omdat de IPv6-client naar verwachting het IPv4-adres uitschakelt.

IPv6 Overlay Architecture in Cisco Software-Defined Access.

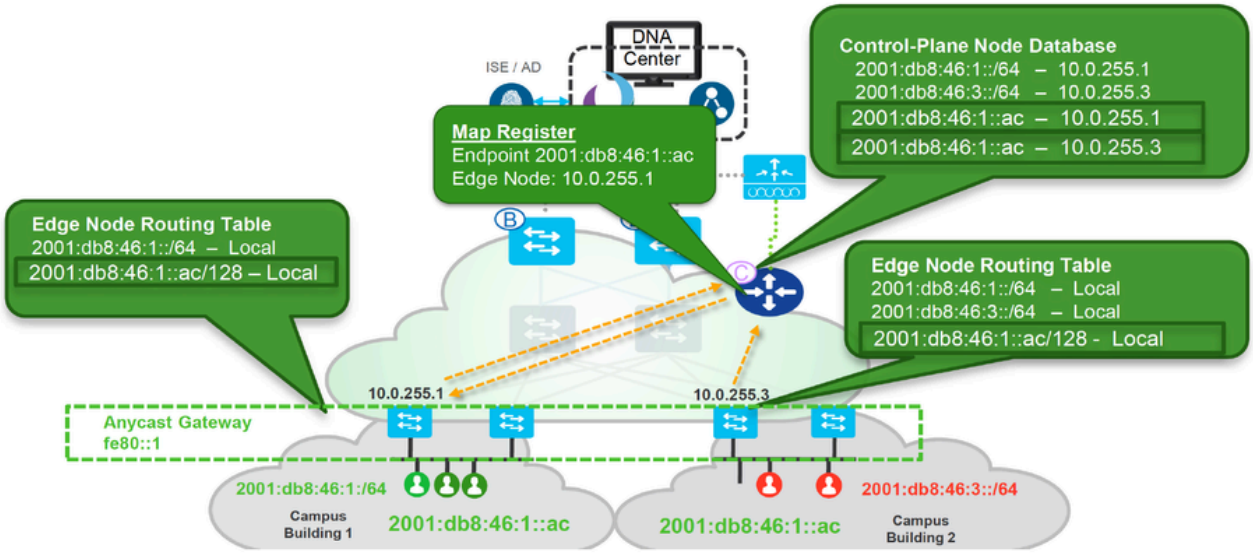


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

IPv6 Overlay Architecture

IPv6 inschakelen met Cisco DNA-Center

Er zijn twee manieren om de IPv6-pool in het Cisco DNA Center in te schakelen:
1. Een nieuwe dual-stack IPv4/v6-pool maken - greenfield
2. Bewerk IPv6 op de IPv4-pool die al bestaat - brownfieldmigratie

De huidige versie (tot 2.3.x) van DNA Center ondersteunt IPv6 niet. Alleen een pool, als de gebruiker van plan is om een enkele/native IPv6-client met alleen adressen te ondersteunen. Een dummy IPv4-adres moet worden gekoppeld aan de IPv6-pool. Merk op dat u de groep met een IPv4-adres bewerkt vanuit de geïmplementeerde IPv4-pool die al bestaat met een site die eraan is gekoppeld. DNA Center biedt de migratieoptie voor de SD-Access Fabric, waarbij de gebruiker de fabric voor die site opnieuw moet inrichten. Er wordt een waarschuwingsindicator weergegeven in de Fabric waar de site thuishoort en deze geeft aan dat Fabric de Fabric opnieuw moet configureren. Zie deze afbeeldingen voor voorbeelden:

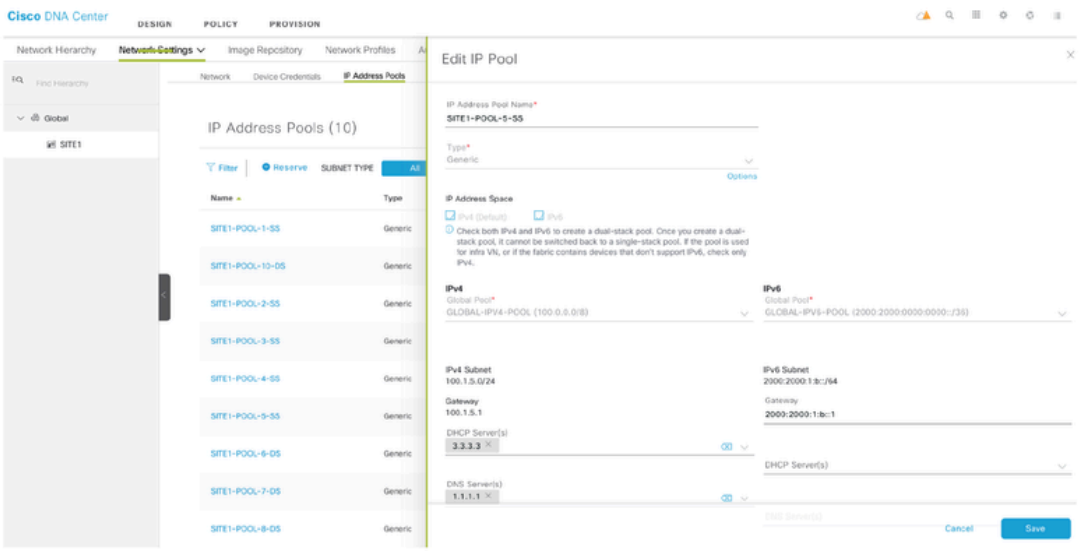


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

Eén IPv4-pool upgraden naar dual-stack-pool door de optie IPv4-pool te bewerken

Pool upgrade: Warning on fabric page

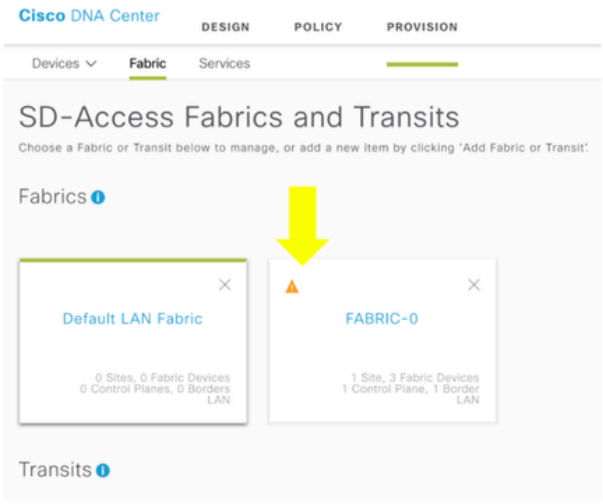


Figure 3.
Fabric has warning indicator which needs to ‘reconfigure the fabric’

Fabric heeft een waarschuwingsindicator die 'de fabric opnieuw moet configureren'

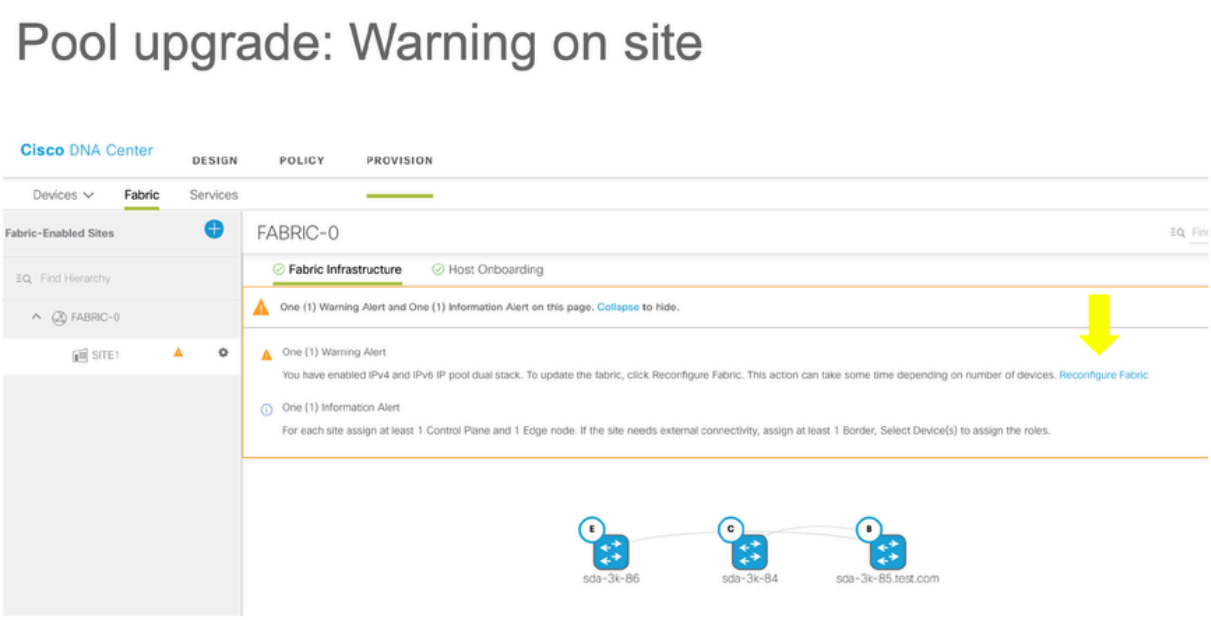


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

De gebruiker moet op 'Fabric opnieuw configureren' klikken om de fabric-nodes automatisch opnieuw in te richten voor de configuratie met dubbele stapels, zodat deze als onderdeel van het migratieproces van kracht wordt

Ontwerpoverwegingen met IPv6 in Cisco SD-Access

Hoewel de Cisco SD-Access-clients kunnen worden uitgevoerd met netwerkinstellingen met twee stapels of alleen IPv6, heeft de huidige implementatie van SD-Access-fabric met de SW-versie (DNA Center Switch) tot 2.3.x.x enkele bedenkingen bij de IPv6-implementatie.

- Cisco SD-Access ondersteunt IPv4-routeringsprotocollen. Het IPv6-clientverkeer wordt dus getransporteerd wanneer het wordt ingekapseld in IPv4-headers. Dit is een vereiste voor de huidige implementatie van LISP-software. Maar het betekent niet dat de onderlaag geen IPv6-routeringsprotocol kan inschakelen, alleen de SD-Access-overlay LISP werkt niet op zijn afhankelijkheid.
- IPv6 native multicast wordt niet ondersteund omdat de onderliggende fabric op dit moment alleen IPv4 kan zijn.
- Gastdraadloos kan alleen worden uitgevoerd met de dubbele stapel. Vanwege de huidige Identity Services Engine (ISE)-release (bijvoorbeeld maximaal 3.2) wordt het IPv6-gastportaal niet ondersteund, waardoor een gastclient die alleen IPv6 gebruikt, niet kan worden geverifieerd.
- Automatisering van het QoS-beleid voor IPv6-toepassingen wordt niet ondersteund in de huidige versie van het DNA Center. Dit document beschrijft de stappen die nodig zijn om IPv6 QoS te implementeren voor bekabelde en draadloze dual-stack clients in Cisco SD-Access die op grote schaal voor een van de gebruikers waren geïmplementeerd.
- De functie voor snelheidsbeperking voor draadloze clients voor downstream- en upstreamverkeer, hetzij per Service Set Identifier (SSID) of per client op basis van beleid,

wordt ondersteund voor IPv4 (TCP/UDP) en IPv6 (alleen TCP). IPv6 UDP-snelheidsbeperking wordt nog niet ondersteund.
- De IPv4-pool kan worden geüpgraded naar een pool met twee stapels. Maar een pool met twee stapels kan niet worden gedowngraded naar een IPv4-pool. Als de gebruiker de pool met twee stapels terug wil verwijderen naar de pool met één stapel IPv4, moet de volledige pool met twee stapels worden vrijgegeven.
- Single IPv6 wordt nog niet ondersteund, terwijl alleen IPv4- of dual-stack-pool kan worden gemaakt in het huidige DNA Center.
- Het platform van Cisco IOS® XE is een minimale softwareversie van 16.9.2 en hoger.
- IPv6 Guest Wireless wordt nog niet ondersteund in Cisco IOS XE-platforms, terwijl AireOS (8.10.105.0+) een oplossing ondersteunt.
- De pool met dubbele stapels kan niet worden toegewezen in de INFRA_VN-pool, waar alleen toegangspunt (AP) of uitgebreide knooppuntenpool kan worden toegewezen.
- LAN-automatisering ondersteunt IPv6 nog niet.

Naast de eerder genoemde beperkingen, moet u bij het ontwerpen van een SD-Access-fabric met IPv6 ingeschakeld altijd rekening houden met de schaalbaarheid van elke fabric-component. Als een eindpunt meerdere IPv4- of IPv6-adressen heeft, wordt elk adres geteld als een afzonderlijke vermelding.

Fabric-hostingvermeldingen bevatten toegangspunten en klassieke en beleidsknooppunten.

Aanvullende overwegingen voor de schaal van de border node:

/32 (IPv4)- of /128 (IPv6)-vermeldingen worden gebruikt wanneer de border node verkeer van buiten de fabric doorstuurt naar een host in de fabric.

Voor alle switches behalve de krachtige Switches uit de Cisco Catalyst 9500-reeks en de Switches uit de Cisco Catalyst 9600-reeks:

- IPv4 maakt gebruik van één TCAM-item (Ternary Content Addressable Memory) (fabric-hostvermeldingen) voor elk IPv4-IP-adres.
- IPv6 gebruikt twee TCAM-vermeldingen (fabric host entries) voor elk IPv6 IP-adres.

Voor de krachtige Switches uit de Cisco Catalyst 9500-reeks en Switches uit de Cisco Catalyst 9600-reeks:

- IPv4 gebruikt één TCAM-vermelding (fabric-hostvermeldingen) voor elk IPv4-IP-adres.
- IPv6 gebruikt één TCAM-vermelding (fabric host entries) voor elk IPv6 IP-adres.

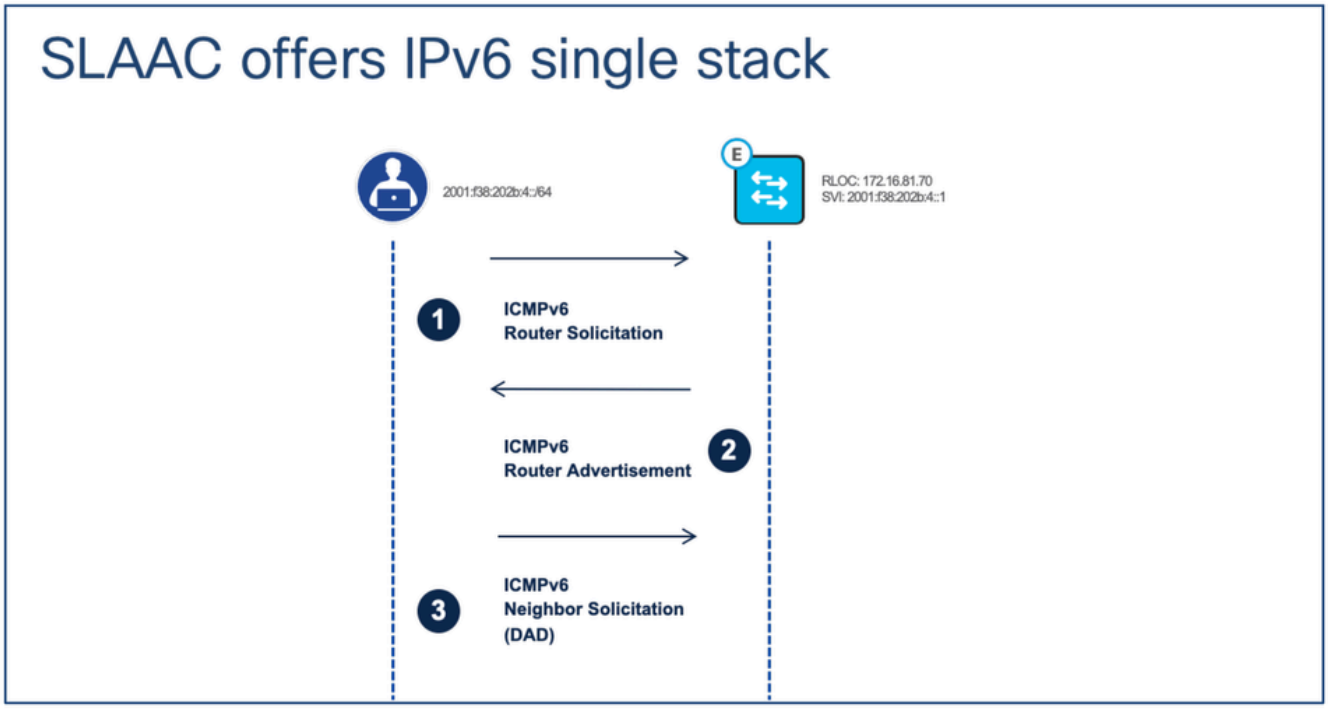
En sommige eindpunten ondersteunen geen DHCPv6, zoals Android OS-smartphones die afhankelijk zijn van Stateless Address Autoconfiguration (SLAAC) om IPv6-adressen te krijgen. Een enkel eindpunt kan eindigen met meer dan twee IPv6-adressen. Dit gedrag verbruikt meer hardwarebronnen op elke knooppunt van de fabric, met name voor de rand- en besturingsknooppunten van de fabric. Elke keer dat het border-knooppunt bijvoorbeeld verkeer naar de edge-knooppunten voor een eindpunt wil verzenden, installeert het een hostroute in de TCAM-vermelding en brandt het een VXLAN-vermelding in de hardware (HW) TCAM.

Bekabelde en draadloze clientverbindingen en gespreksstromen

Zodra de client is verbonden met de Fabric Edge, zijn er verschillende manieren waarop deze de IPv6-adressen krijgt. Deze sectie behandelt de meest voorkomende manier om IPv6-adressen van clients te gebruiken, dat wil zeggen SLAAC en DHCPv6.

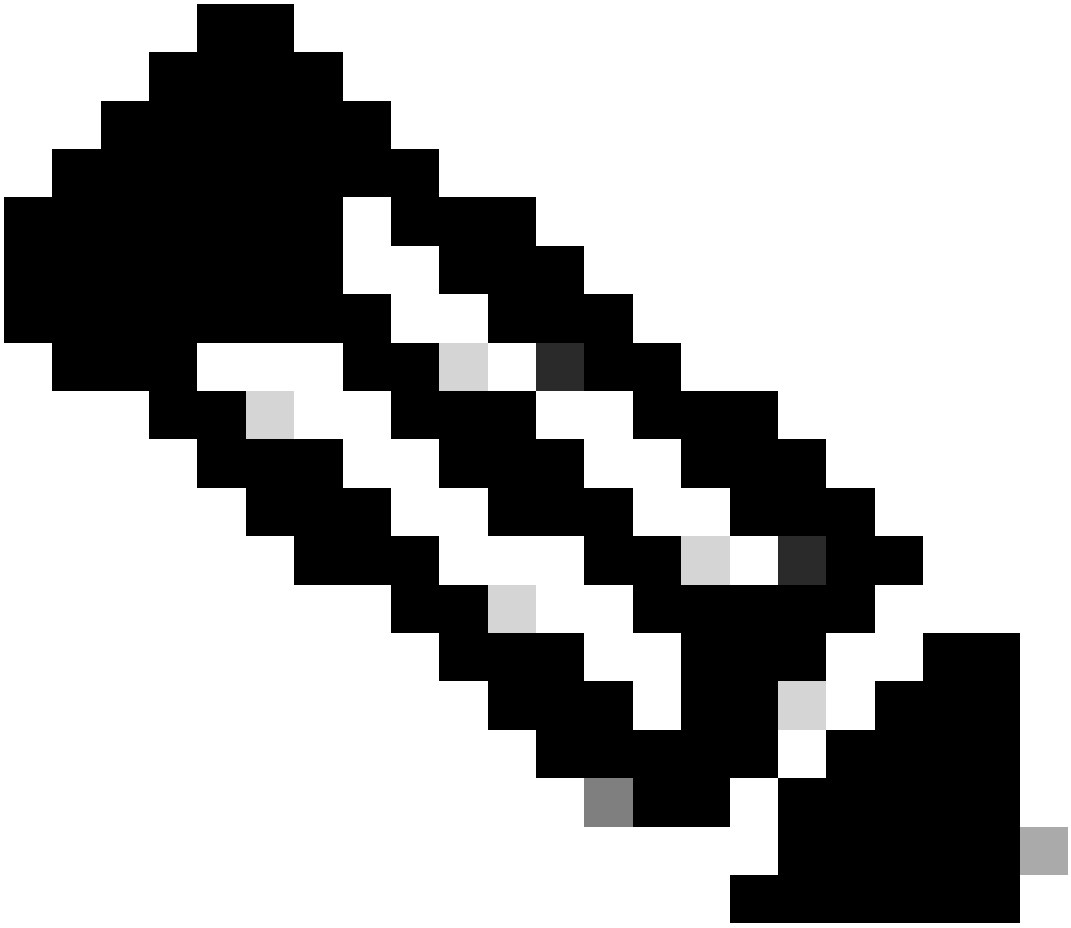
IPv6-adrestoewijzing – SLAAC

De SLAAC in Software-Defined Access (SDA) verschilt niet van de standaard SLAAC-processtroom. Om SLAAC goed te laten werken, moet de IPv6-client worden geconfigureerd met een link-lokaal adres in de interface, maar hoe de client zichzelf automatisch configureert met het link-lokaal adres valt buiten het bereik van dit document.



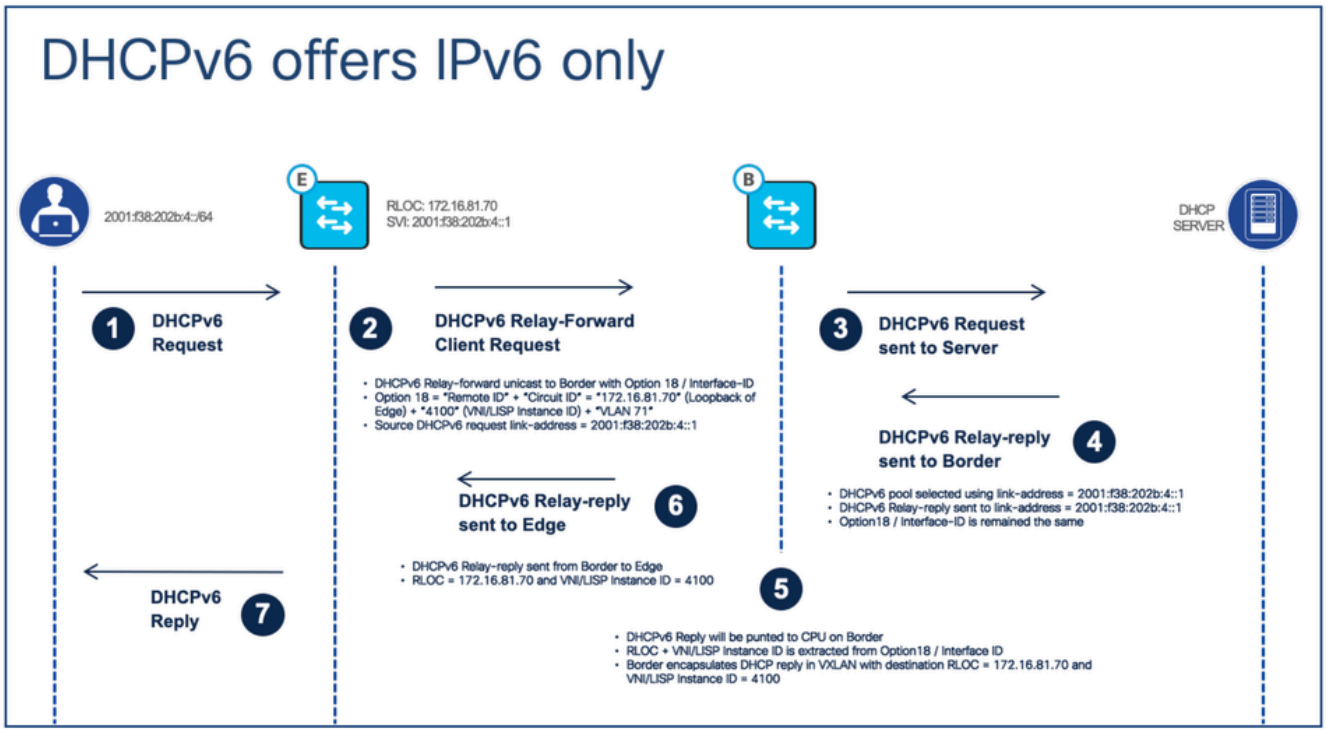
IPv6-adrestoewijzing – SLAAC

Beschrijving van de oproepstroom:
Stap 1. Nadat de IPv6-client zichzelf heeft geconfigureerd met een lokaal IPv6-linkadres, stuurt de client het ICMPv6 Router Solicitation (RS)-bericht naar Fabric Edge. Het doel van dit bericht is om het wereldwijde unicast-voorvoegsel van het gekoppelde segment te verkrijgen.
Stap 2. Nadat de fabric edge het RS-bericht heeft ontvangen, reageert deze terug met een ICMPv6 Router Advertisement (RA)-bericht met het algemene IPv6 unicast-voorvoegsel en de lengte erin.
Stap 3. Zodra de client het RA-bericht heeft ontvangen, combineert deze het algemene IPv6-voorvoegsel unicast met zijn EUI-64-interface-id om zijn unieke IPv6 globale unicast-adres te genereren en zijn gateway in te stellen op het lokale linkadres van de SVI van de fabric edge die gerelateerd is aan het segment van de client. Vervolgens verzendt de client een ICMPv6 Neighbor Solicitation-bericht om dubbele adresdetectie (DAD) uit te voeren om ervoor te zorgen dat het IPv6-adres dat het krijgt uniek is.



Opmerking: Alle SLAAC-gerelateerde berichten zijn ingekapseld met het lokale SVI IPv6-linkadres van de client en de fabric-node.

IPv6-adrestoewijzing – DHCPv6

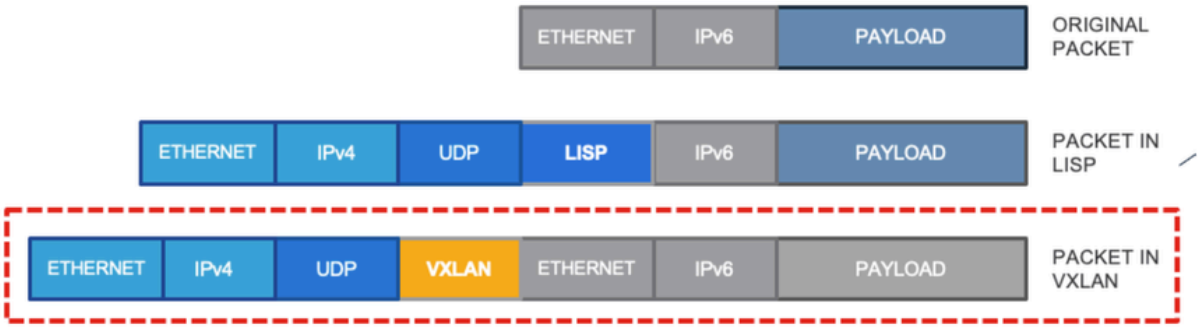


IPv6-adrestoewijzing – DHCPv6

Beschrijving van de oproepstroom:
Stap 1. De client verzendt het DHCPv6-verzoek naar de fabric edge.
Stap 2. Wanneer de fabric edge het DHCPv6-verzoek ontvangt, gebruikt deze het DHCPv6 relay-forward-bericht om het verzoek naar de fabric-rand met DHCPv6 optie 18 te unicasten. In vergelijking met DHCP optie 82 codeert de DHCPv6 optie 18 zowel 'Circuit ID' als 'Remote ID' samen. De LISP Instance ID/VNI, IPv4 Routing Locator (RLOC) en endpoint VLAN worden binnen gecodeerd.
Stap 3. De fabric-rand decapsuleert de VXLAN-header en brengt het DHCPv6-pakket naar de DHCPv6-server.
Stap 4. De DHCPv6-server ontvangt het relay-forward-bericht en gebruikt het adres van de bronkoppeling (DHCPv6 relay agent/client gateway) van het bericht om de IPv6-IP-pool te kiezen om het IPv6-adres toe te wijzen. Stuur dan het DHCPv6 relay-reply bericht terug naar het client gateway adres. Optie 18 blijft ongewijzigd.
Stap 5. Wanneer het verbindingskader het relais-antwoordbericht ontvangt, worden de instantie RLOC en LISP/VNI uit optie 18 geëxtraheerd. De verbindingsrand vat het relaisantwoordbericht in VXLAN samen met een bestemming die het uit optie 18 heeft gehaald.
Stap 6. De fabric-rand verzendt het relay-antwoordbericht van DHCPv6 naar de fabric-rand waarmee de client verbinding maakt.
Stap 7. Wanneer fabric edge het relay-reply-bericht DHCPv6 ontvangt, wordt de VXLAN-header van het bericht gedecapsuleerd en wordt het bericht doorgestuurd naar de client. Dan weet de client het toegewezen IPv6-adres.

IPv6-communicatie in Cisco SD-Access

IPv6-communicatie maakt gebruik van de standaard LISP-gebaseerde besturingsvlak en VXLAN-gebaseerde Data plane communicatiemethoden. Met de huidige implementatie in Cisco SD-Access gebruikt LISP en VXLAN de buitenste IPv4-header om de IPv6-pakketten naar binnen te dragen. Deze afbeelding geeft dit proces weer.



Buitenste IPv4-header met de IPv6-pakketten erin

Dit betekent dat alle LISP-query's het IPv4-native pakket gebruiken, terwijl de control plane-knooppunttabel details bevat over het RLOC met zowel IPv6- als IPv4-IP-adressen van het eindpunt. Dit proces wordt in detail uitgelegd in de volgende sectie vanuit het perspectief van een draadloos eindpunt.

Draadloze IPv6-communicatie in Cisco SD-Access

De draadloze communicatie is gebaseerd op twee specifieke componenten: toegangspunten en draadloze LAN-controllers, naast de typische Cisco SD-Access Fabric-componenten. Draadloze toegangspunten maken een CAPWAP-tunnel (Control and Provisioning of Wireless Access Points) met de Wireless LAN Controller (WLC). Terwijl het clientverkeer zich op de Fabric Edge bevindt, wordt andere communicatie van het besturingsvlak, waaronder radiostatistieken, beheerd door de WLC. Vanuit een IPv6-perspectief moeten zowel de WLC als de AP de IPv4-adressen hebben en alle CAPWAP-communicatie maakt gebruik van deze IPv4-adressen. Terwijl de Non-Fabric WLC en AP IPv6-communicatie ondersteunen, gebruikt Cisco SD-Access de IPv4 voor alle communicatie die IPv6-clientverkeer in IPv4-pakketten vervoert. Dit betekent dat toegewezen AP-pools onder Infra VN niet kunnen worden toegewezen met IP-pools die dual-stack zijn en dat er een fout wordt gegenereerd als er een poging wordt gedaan om deze toewijzing te doen. Draadloze communicatie binnen Cisco SDA kan worden onderverdeeld in deze belangrijke taken:

- Onboarding van toegangspunt
- Client on-boarding

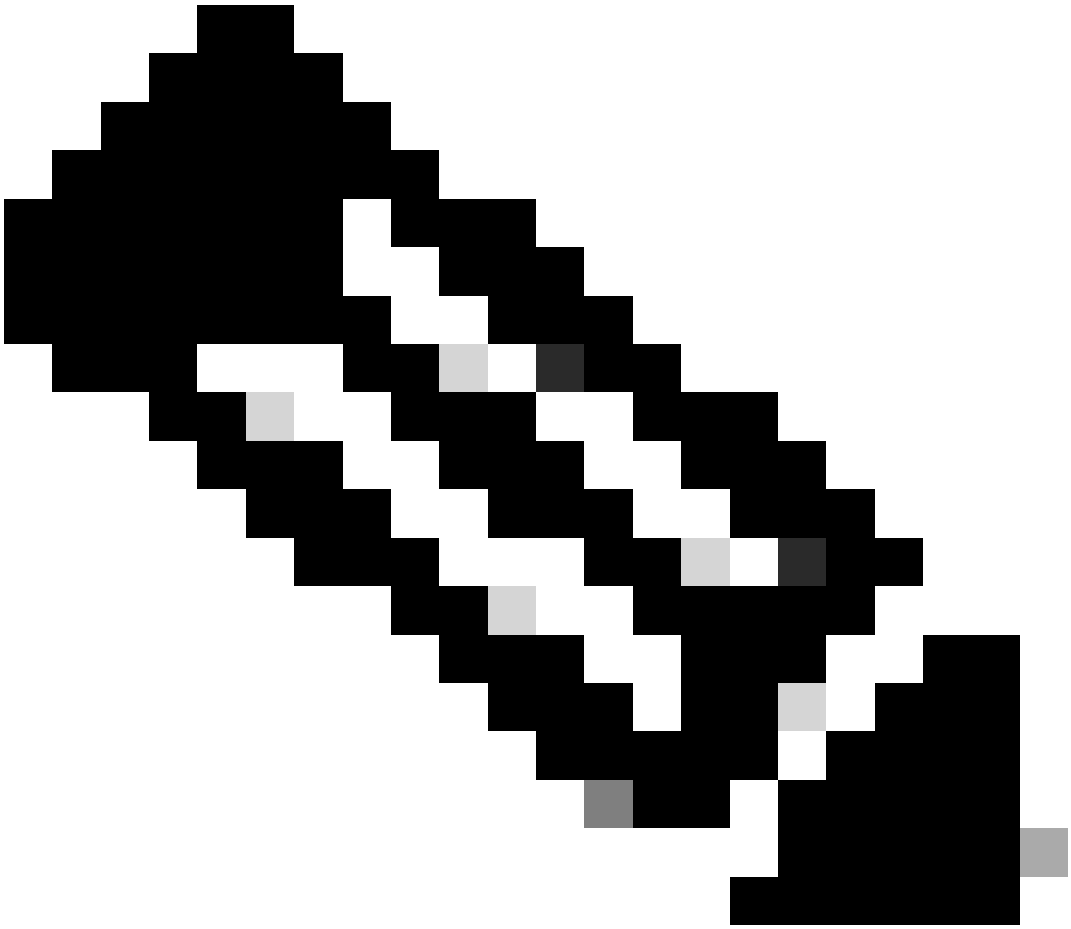
Bekijk deze gebeurtenissen vanuit een IPv6-perspectief.

Onboarding van toegangspunt

Dit proces blijft hetzelfde voor IPv6 en IPv4, omdat zowel WLC als AP IPv4-adressen en stappen

bevatten:
1. De Fabric Edge (FE)-poort is geconfigureerd voor het geïntegreerde toegangspunt.
2. AP maakt verbinding met de FE-poort en via CDP meldt AP FE over zijn aanwezigheid (hierdoor kan FE het juiste VLAN toewijzen).
3. AP krijgt het IPv4-adres van de DHCP-server en FE registreert AP en werkt het Control Plane (CP-knooppunt) bij met AP-gegevens.
4. AP sluit zich aan bij WLC via traditionele methoden (zoals DHCP-optie 43).
5. WLC controleert of AP Fabric geschikt is en vraagt het besturingsvlak om AP RLOC-informatie (bijvoorbeeld RLOC requested/response received).
6. CP antwoordt met het RLOC IP van het toegangspunt op het WLC.
7. WLC registreert de AP Media Access Control (Address) (MAC) in CP.
8. CP werkt de FE bij met de gegevens van WLC over het toegangspunt (dit vertelt FE om de VXLAN-tunnel met het toegangspunt te starten).

FE verwerkt de informatie en maakt een VXLAN-tunnel met AP. Op dit punt adverteert AP met Fabric Enabled SSID.

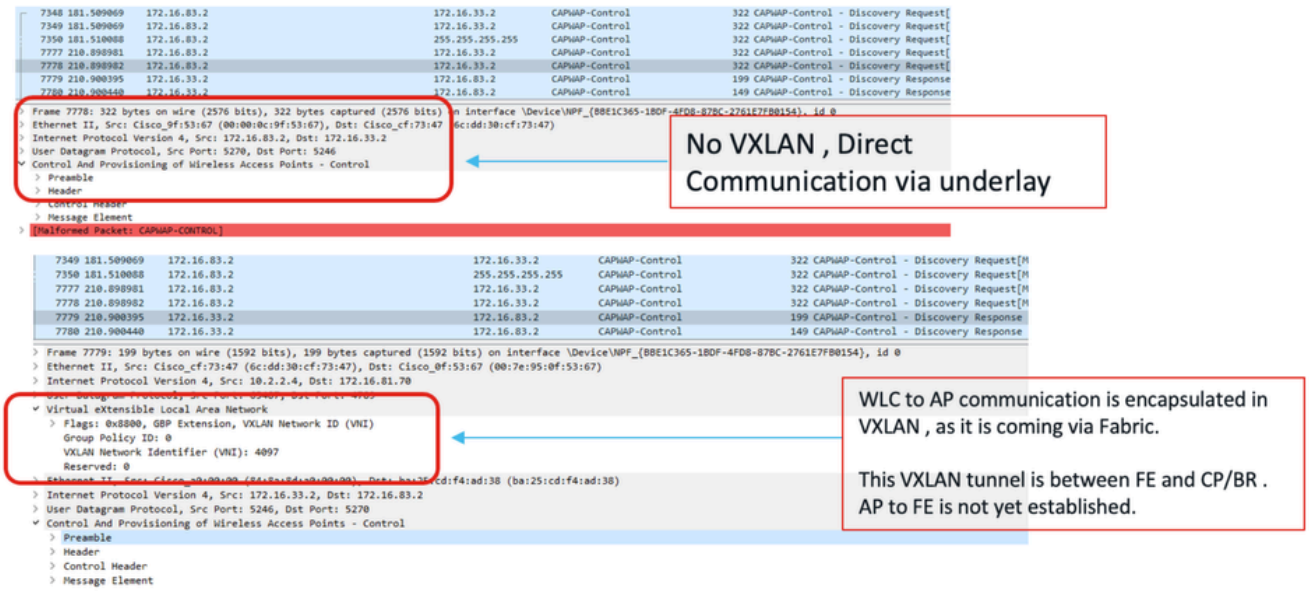


Opmerking: Als het toegangspunt de niet-verbindings-SSID's uitzendt en de verbindings-

---

SSID niet uitzendt, controleert u of de VXLAN-tunnel tussen het toegangspunt en de knooppunt Fabric Edge is geopend.

Houd er ook rekening mee dat de communicatie van AP naar WLC altijd via Underlay CAPWAP verloopt en dat alle communicatie van WLC naar AP via VXLAN CAPWAP via overlay verloopt. Dit betekent dat als u pakketten vastlegt die van AP naar WLC gaan, u alleen CAPWAP ziet terwijl het omgekeerde verkeer een VXLAN-tunnel heeft. Zie dit voorbeeld voor de communicatie tussen AP en WLC.



Pakketopnamen van AP naar WLC (CAPWAP Tunnel) versus WLC naar AP (VxLAN Tunnel in de Fabric)

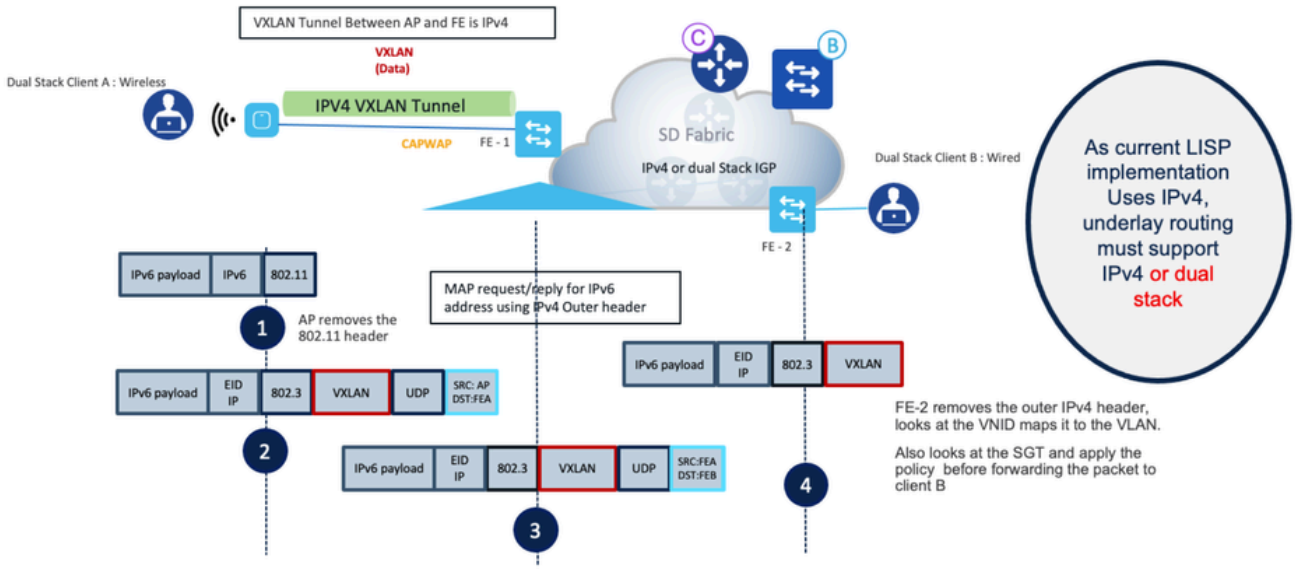
Client Onboarding

Dual-Stack/IPv6 Client on-boarding proces blijft hetzelfde, maar de client maakt gebruik van de IPv6-adres toewijzingsmethoden zoals SLAAC/DHCPv6 om de IPv6-adressen te krijgen.
1. De client wordt lid van de verbinding en maakt SSID op het toegangspunt mogelijk.
2. WLC kent het AP RLOC.
3. De client verifieert en WLC registreert de gegevens van client L2 met CP en werkt AP bij.
4. De client start de IPv6-adressering vanaf geconfigureerde methoden – SLAAC/DHCPv6.
5. FE activeert IPv6-clientregistratie naar CP Host Tracking Database (HTDB). AP naar FE en FE naar andere bestemmingen gebruiken de VXLAN- en LISP IPv6-inkapseling binnen IPv4-frames.

Client-clientcommunicatie met IPv6

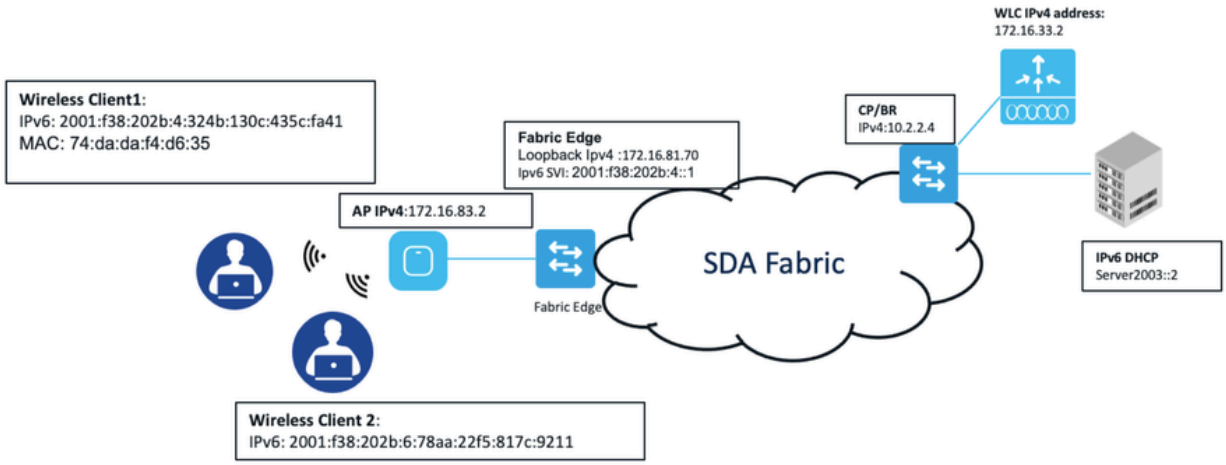
De afbeelding hier vat het IPv6 draadloze client communicatie proces met een andere IPv6 bekabelde client. (Hierbij wordt ervan uitgegaan dat de client is geverifieerd en het IPv6-adres via geconfigureerde methoden heeft ontvangen.)

1. De client verzendt de 802.11-frames naar het toegangspunt met IPv6-payload.
2. AP verwijdert de 802.11-headers en verzendt de oorspronkelijke IPv6-payload in de IPv4 VXAN-tunnel naar Fabric Edge.
3. Fabric Edge gebruikt het Message Access Protocol (MAP)-verzoek om de bestemming te identificeren en verzendt het frame naar de bestemming RLOC met IPv4 VXLAN.
4. Bij de destination Switch wordt de IPv4 VXLAN-header verwijderd en het IPv6-pakket naar de client verzonden.

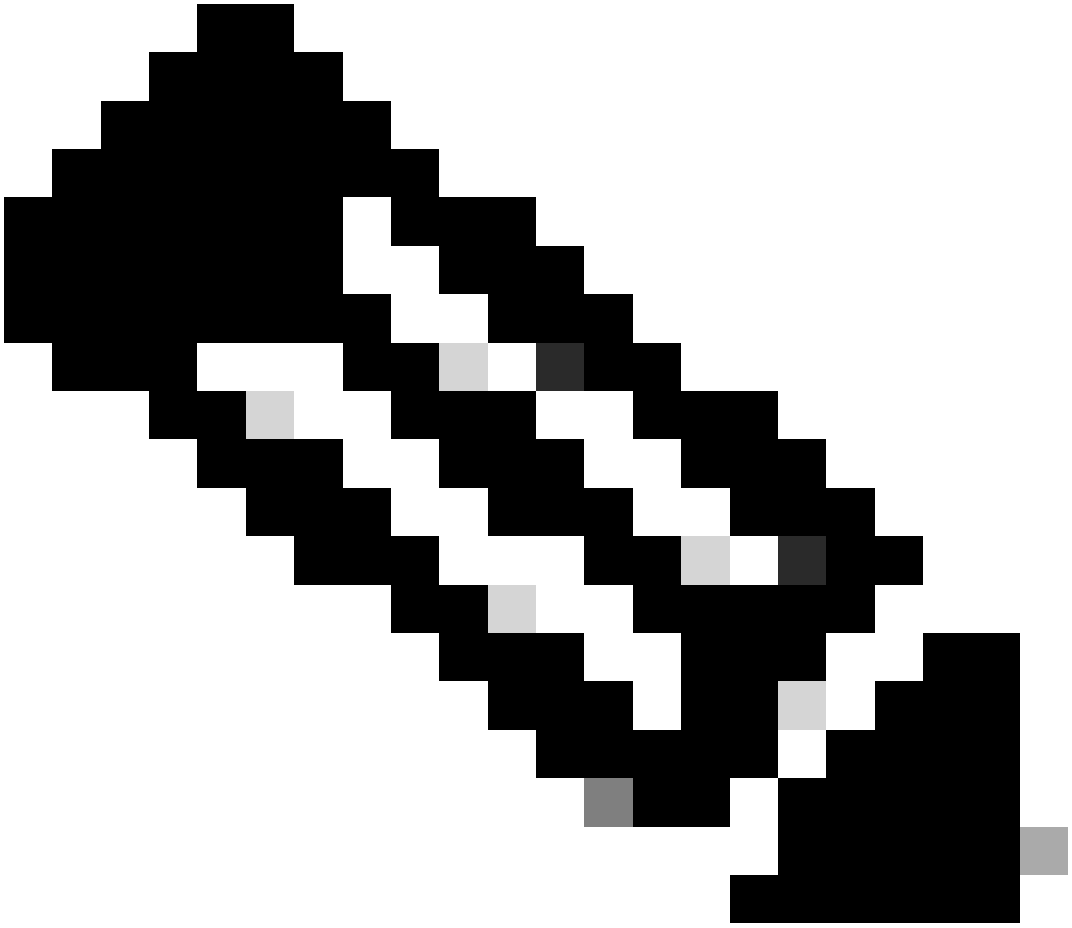


Draadloze client-naar-bekabelde clientpakketstromen met dubbele stapel

Bekijk dit proces grondig met de pakketopnames en raadpleeg de afbeelding voor IP-adressen en MAC-adresgegevens. Opmerking: bij deze installatie worden beide Dual Stack-clients gebruikt die zijn verbonden met dezelfde toegangspunten, maar zijn toegewezen met verschillende IPv6-subnetten (SSID's).

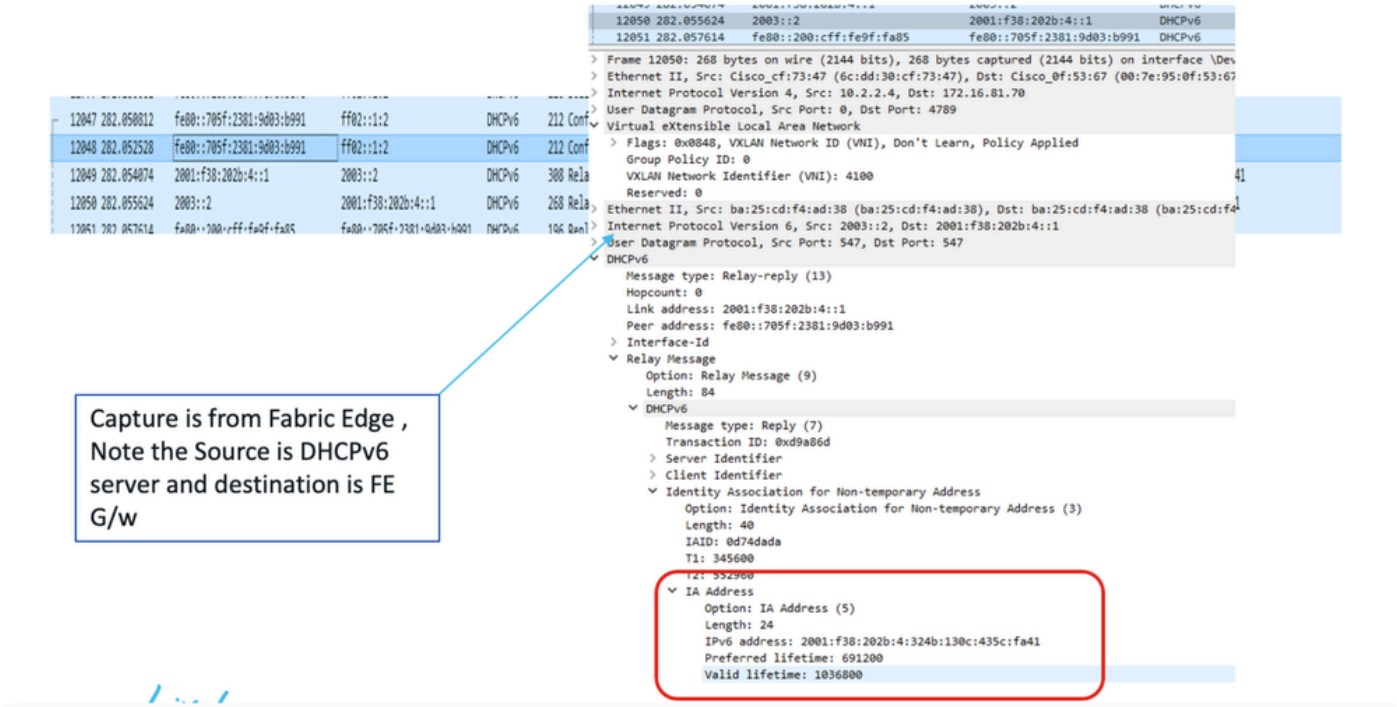


Voorbeelden van IP-adressen en MAC-adressen van SD-Access Fabric-netwerken



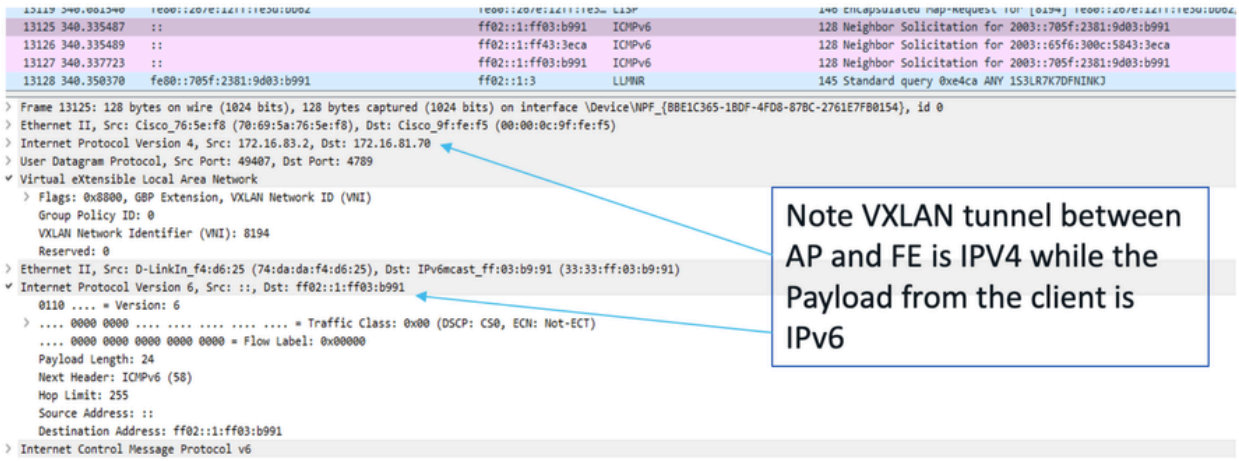
Opmerking: voor elke IPv6-communicatie buiten de fabric, bijvoorbeeld DHCP/DNS, moet IPv6-routering zijn ingeschakeld tussen de randinfrastructuur en de niet-structuurinfrastructuur.

Stap 1. De client verifieert en haalt het IPv6-adres op van de geconfigureerde methoden.



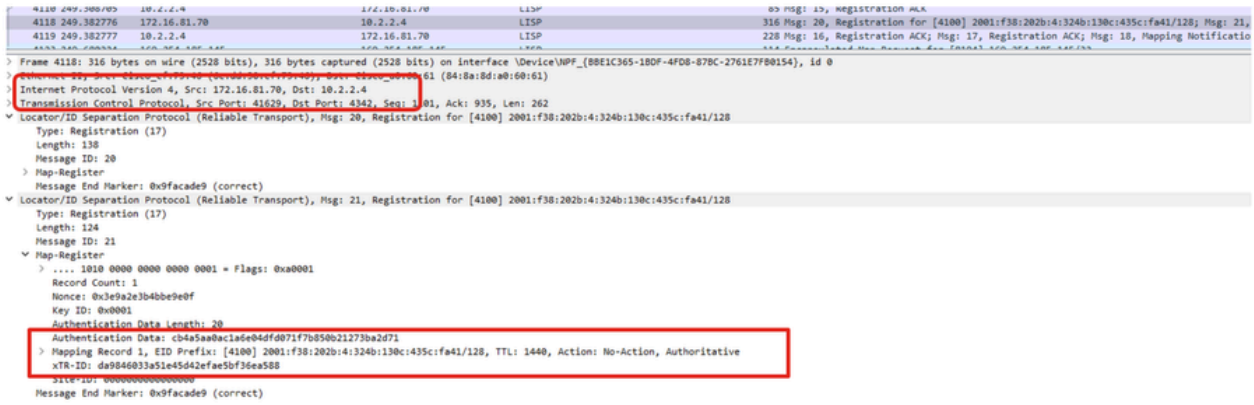
Pakketvastlegging van DHCPv6-server naar Fabric Edge-node

Stap 2. De draadloze client verzendt de 802.11-frames naar het toegangspunt met de IPv6-payload.
Stap 3. Het toegangspunt verwijdert de draadloze header en stuurt het pakket naar de Fabric-rand. Dit maakt gebruik van de VXLAN-tunnelheader die op IPv4 is gebaseerd, omdat Access Point het IPv4-adres heeft.



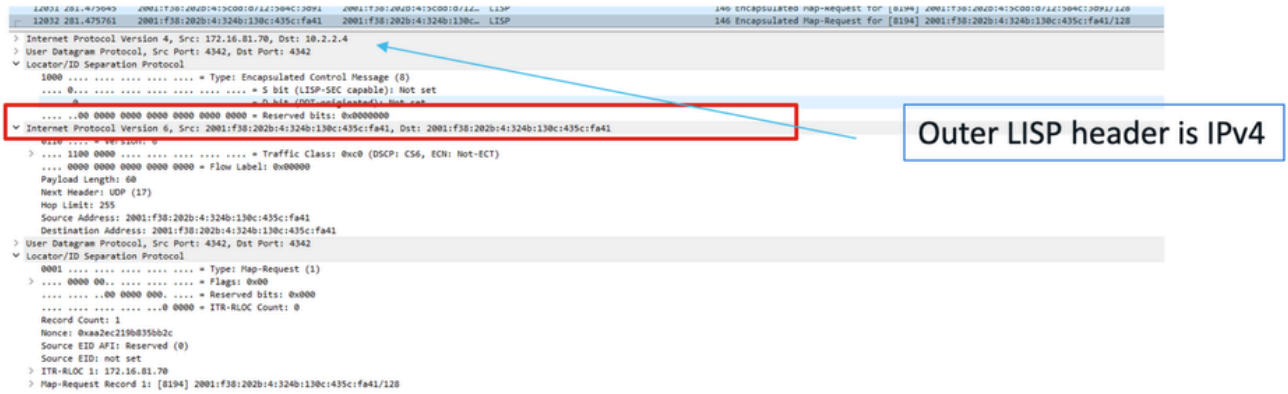
Packet Capture voor de VxLAN-tunnel tussen FE en AP

Stap 3.1. Fabric Edge registreert de IPv6-client met het besturingsvlak. Hierbij wordt de IPv4-registratiemethode gebruikt met details van de IPv6-client erin.



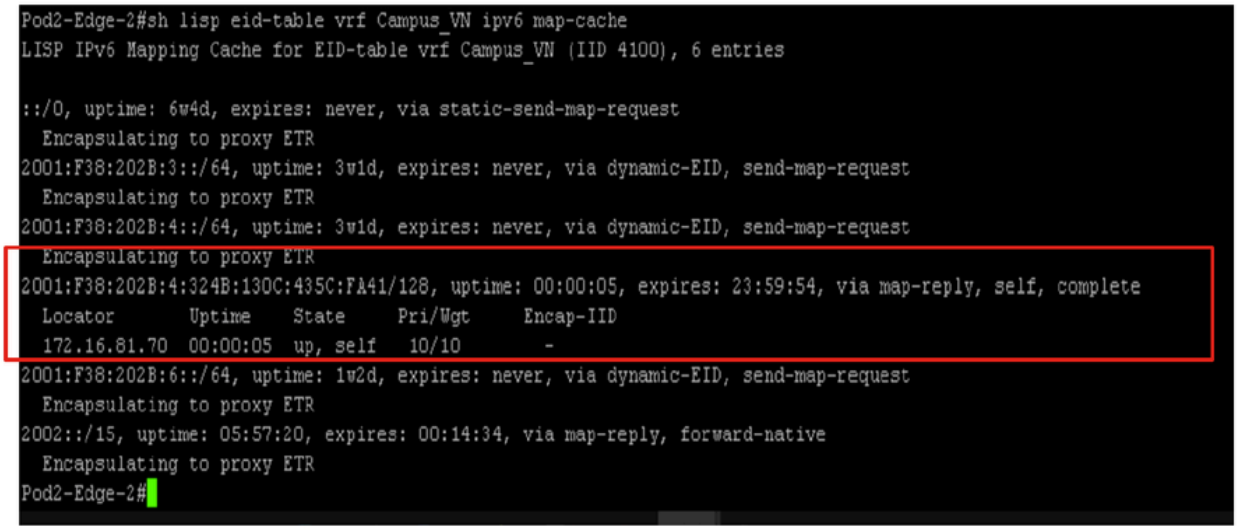
Packet Capture voor FE-registers met Control Plane voor IPv6-client

Stap 3.2. FE stuurt het MAP-verzoek naar het controlevliegtuig om de bestemming RLOC te identificeren.



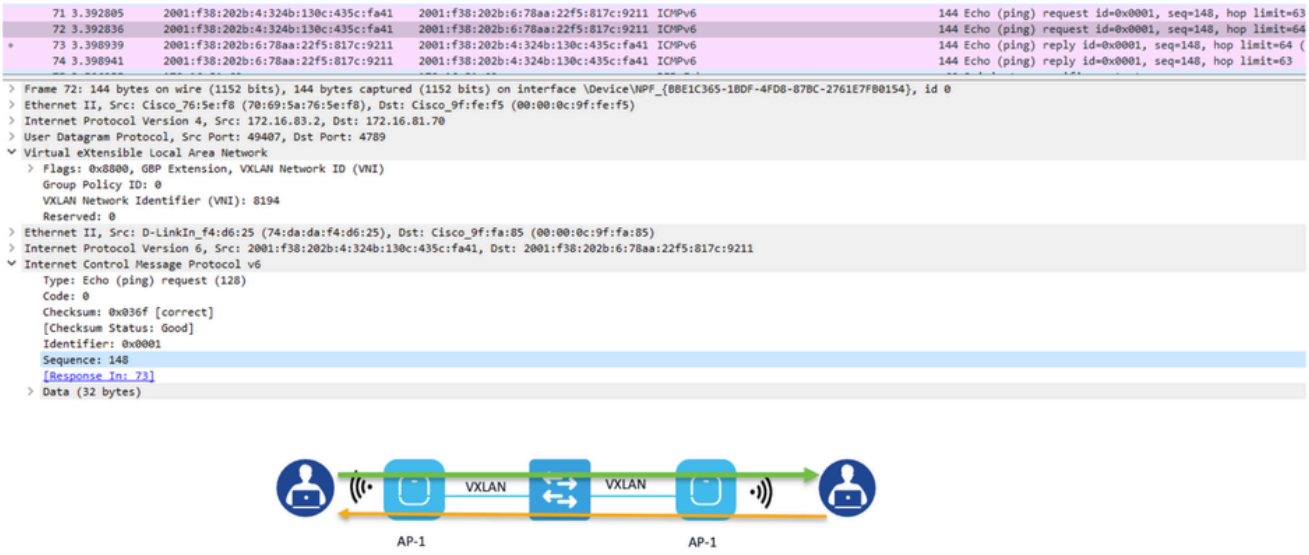
Packet Capture van FE naar CP met MAP-registratieberichten

Fabric Edge onderhoudt ook de MAP-cache voor bekende IPv6-clients, zoals weergegeven in deze afbeelding.



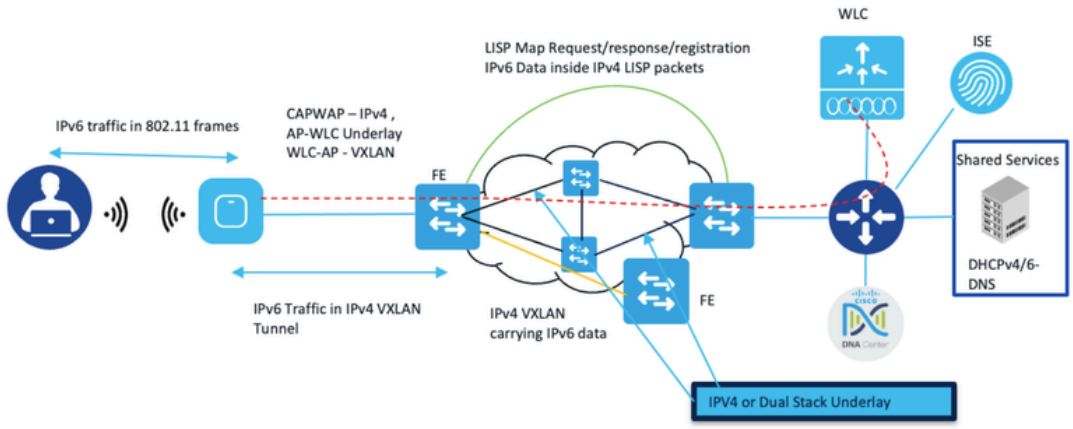
Fabric Edge-schermuitvoer van IPv6-overlay-kaartcache-informatie

Stap 4. Het pakket wordt doorgestuurd naar de bestemming RLOC met de IPv4 VXLAN die de oorspronkelijke IPv6-payload binnenin draagt. Aangezien beide clients zijn verbonden met hetzelfde toegangspunt, volgt de IPv6-ping dit pad.

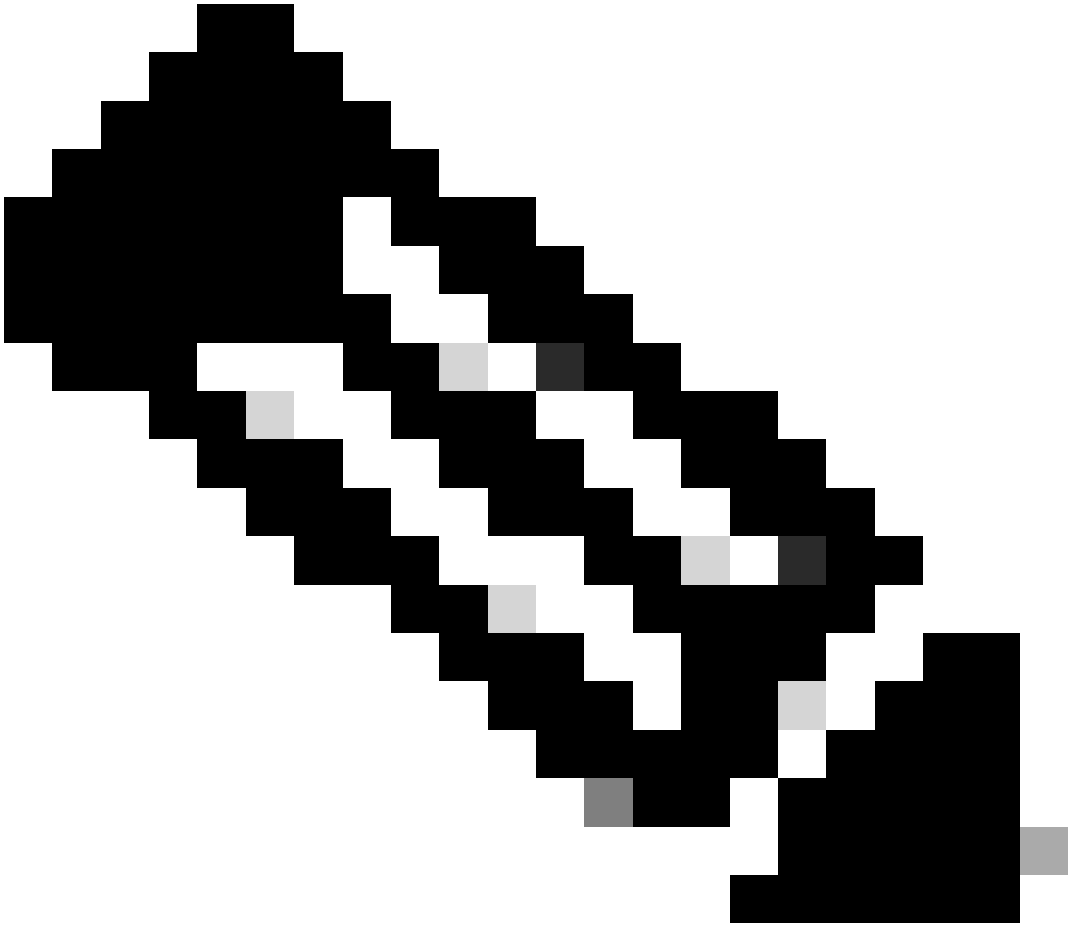


Packet Capture voor IPv6-ping tussen twee draadloze clients die op hetzelfde toegangspunt zijn geregistreerd

Deze afbeelding vat de IPv6-communicatie samen vanuit het perspectief van de draadloze client.



De figuur vat de IPv6-communicatie samen vanuit het perspectief van de draadloze client



Opmerking: IPv6-gasttoegang (webportaal) via Cisco Identity Services wordt niet ondersteund vanwege beperkingen op ISE.

afhankelijkheidsmatrix

Het is belangrijk om de afhankelijkheden en ondersteuning voor IPv6 op te merken van verschillende draadloze componenten die deel uitmaken van Cisco SD-Access. De tabel in deze afbeelding vat deze functiematrix samen.

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

Cat9800 WLC IPv6-functies van release

Controleer het controlevlak voor IPv6

Zodra u IPv6 hebt ingeschakeld, ziet u aanvullende vermeldingen over host IPv6 op de Map-server (MS)/Map Resolver (MR)-servers. Aangezien een host meerdere IPv6-adressen kan hebben, bevat de opzoektabel MS/MR vermeldingen voor alle IP-adressen. Dit wordt gecombineerd met de reeds bestaande IPv4-tabel.
U moet zich aanmelden bij de CLI van het apparaat en deze opdrachten geven om alle vermeldingen te controleren.

```
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
```

U kunt ook de details over de IPv6-host controleren via assurance.

IPv6 QoS-implementatie in Cisco SD-Access

De huidige versie van het Cisco DNA Center (maximaal 2.3.x) biedt geen ondersteuning voor automatisering van het IPv6 QoS-toepassingsbeleid. Gebruikers kunnen echter handmatig bekabelde en draadloze IPv6-sjablonen maken en de QoS-sjabloon in Fabric Edge-knooppunten duwen. Aangezien DNA Center het IPv4 QoS-beleid automatiseert op alle fysieke interfaces die eenmaal zijn toegepast, kunt u handmatig een klassentoewijzing invoegen (die overeenkomt met IPv6 Access Control List (ACL)) vóór 'class-default' via een sjabloon.

Hier is het voorbeeld bekabelde IPv6 QoS-enabled sjabloon geïntegreerd met DNA Center-gegenereerde beleidsconfiguratie:

```
!
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
```

Problemen met IPv6 oplossen in Cisco SD-Access

Problemen oplossen met SD-Access IPv6 lijkt veel op IPv4, u kunt altijd dezelfde opdracht gebruiken met verschillende zoekwoordopties om hetzelfde doel te bereiken. Dit toont een aantal opdrachten die vaak worden gebruikt om problemen met SD-Access op te lossen.

```
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
```

Van Border Node naar overlay DHCPv6 server ping controleren:

```
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
```

Veelgestelde vragen over IPv6-ontwerp met Cisco SD-Access

V. Biedt Cisco Software Defined Network ondersteuning voor IPv6 voor onderliggende en overlay-netwerken?
A. Alleen overlay wordt ondersteund met de huidige versie (2.3.x) op het moment dat dit document wordt geschreven.

V. Ondersteunt Cisco SDN native IPv6 voor zowel bekabelde als draadloze clients?
A. Ja. Hiervoor zijn dual-stack pools nodig die in het DNA Center worden gemaakt, terwijl IPv4 de dummy pool is, omdat de clients IPv4 DHCP-verzoeken uitschakelen en alleen IPv6 DHCP- of SLAAC-adressen worden aangeboden.

V. Kan ik een eigen campusnetwerk met alleen IPv6 in mijn Cisco SD-Access Fabric hebben?
A. Niet met de huidige versie (maximaal 2.3.x). Het staat op de roadmap.

V. Biedt Cisco SD-Access ondersteuning voor L2 IPv6-overdracht?
A. Op dit moment niet. Alleen L2 IPv4-overdracht en L3 Dual-Stack-overdracht worden ondersteund.

V. Ondersteunt Cisco SD-Access multicast voor IPv6?
A. Ja, alleen overlay IPv6 met kopreplicatie multicast wordt ondersteund. Native IPv6 multicast wordt nog niet ondersteund.

V. Ondersteunt Cisco SD-Access Fabric Enabled Wireless gasten in dual-stack?
A. Nog niet ondersteund in Cisco IOS XE (Cat9800) WLC. AireOS WLC wordt ondersteund via een tijdelijke oplossing. Neem voor meer informatie over de implementatie van de oplossing contact op met het Cisco Customer Experience-team.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.