Implementierung von IPv6 in Software-Defined Access

Inhalt

Einleitung

In diesem Dokument wird die Implementierung von IPv6 in Cisco® Software-Defined Access (SD-Access) beschrieben.

Hintergrundinformationen

IPv4 wurde 1983 veröffentlicht und wird noch immer für den Großteil des Internetdatenverkehrs verwendet. Die 32-Bit-IPv4-Adressierung ermöglichte mehr als 4 Milliarden eindeutige Kombinationen. Aufgrund der zunehmenden Anzahl an Clients mit Internetverbindung mangelt es jedoch an eindeutigen IPv4-Adressen. In den 1990er Jahren wurde die Erschöpfung der IPv4-Adressierung unvermeidlich.
In Erwartung dieser, Internet Engineering Taskforce eingeführt, die IPv6-Standard. IPv6 nutzt 128 Bit und bietet 340 Sextillionen eindeutige IP-Adressen, was mehr als genug ist, um den Bedarf an vernetzten Geräten zu befriedigen, die wachsen. Da immer mehr moderne Endgeräte Dual-Stack- und/oder Single-IPv6-Stack unterstützen, ist es für jedes Unternehmen wichtig, auf die Einführung von IPv6 vorbereitet zu sein. Dies bedeutet, dass die gesamte Infrastruktur für IPv6 gerüstet sein

muss. Cisco SD-Access ist die Weiterentwicklung von traditionellen Campus-Designs zu Netzwerken, die die Ziele eines Unternehmens direkt implementieren. Cisco Software Defined Networks kann jetzt Dual-Stack (IPv6-Geräte) integrieren.

Eine große Herausforderung für jedes Unternehmen bei der Einführung von IPV6 ist das Änderungsmanagement und die Komplexität, die mit der Migration von älteren IPv4-Systemen zu IPv6 verbunden sind. Dieses Whitepaper behandelt alle Details zur Unterstützung von IPv6-Funktionen für Cisco SDN, Strategie und kritische Pit-Spot-Punkte, die bei der Einführung von IPv6 mit Cisco Software Defined Networks berücksichtigt werden müssen.

Im August 2019 wurde das Cisco Digital Network Architecture (DNA) Center Version 1.3 erstmals mit Unterstützung von IPv6 vorgestellt. In dieser Version unterstützte das Cisco SD-Access Campus-Netzwerk die Host-IP-Adresse mit kabelgebundenen und drahtlosen Clients in IPv4, IPv6 oder IPv4v6 Dual-Stack aus dem Overlay Fabric-Netzwerk. Die Lösung muss sich kontinuierlich weiterentwickeln, um neue Funktionen einzuführen, die IPv6 für jedes Unternehmen einfach integrieren können.

Cisco SD-Access mit IPv6-Architektur

Die Fabric-Technologie, ein integraler Bestandteil von SD-Access, stellt kabelgebundene und drahtlose Campus-Netzwerke mit programmierbaren Overlays und einfach bereitzustellender Netzwerkvirtualisierung bereit, die es einem physischen Netzwerk ermöglichen, ein oder mehrere logische Netzwerke zu hosten, um die Designziele zu erfüllen. Neben der Netzwerkvirtualisierung verbessert die Fabric-Technologie im Campus-Netzwerk die Kontrolle der Kommunikation, die eine softwaredefinierte Segmentierung und Richtliniendurchsetzung auf Basis der Benutzeridentität und der Gruppenmitgliedschaft ermöglicht. Die gesamte Cisco SDN-Lösung basiert auf der DNA des Fabric. Daher muss jeder Grundpfeiler der Lösung hinsichtlich der IPv6-Unterstützung verstanden werden.

- Underlay - Die IPv6-Funktionalität für Overlay ist vom Underlay abhängig, da das IPv6-Overlay die IPv4-Underlay-IP-Adressierung nutzt, um Locator/ID Separation Protocol (LISP)-Kontrollebenen- und Virtual Extensible LAN (VXLAN)-Tunnel für die Datenebene zu erstellen. Sie können das Dual-Stack-Protokoll jederzeit für das Underlay-Routing-Protokoll aktivieren, nur der SD-Access-Overlay-LISP hängt vom IPv4-Routing ab.
- Overlay - SD-Access unterstützt beim Overlay sowohl kabelgebundene als auch drahtlose IPv6-Endgeräte. Dieser IPv6-Datenverkehr wird in den IPv4- und VXLAN-Header innerhalb der SD-Access-Fabric eingekapselt, bis er die Fabric-Grenzknoten erreicht. Die Fabric Border Nodes entkapseln den IPv4- und VXLAN-Header, der dem normalen IPv6-Unicast-Routing-Prozess folgt.
- Kontrollebenen-Knoten - Der Kontrollebenen-Knoten ist so konfiguriert, dass alle IPv6-Host-Subnetze und /128-Host-Routen innerhalb der Subnetz-Bereiche in seiner Zuordnungsdatenbank registriert werden können.
- Grenzknoten - An den Grenzknoten ist IPv6-BGP-Peering mit Fusion-Geräten aktiviert. Der Grenzknoten entkapselt den IPv4-Header aus dem Fabric-Ausgangsdatenverkehr, während der eingehende IPv6-Datenverkehr ebenfalls von den Grenzknoten mit dem IPv4-Header

gekapselt wird.

- Fabric Edge - Alle Switched Virtual Interfaces (SVIs), die in Fabric Edge konfiguriert sind, müssen IPv6 sein. Diese Konfiguration wird vom DNA Center Controller weitergeleitet.
- Cisco DNA Center - Die physischen Schnittstellen von Cisco DNA Center unterstützen zum Zeitpunkt der Veröffentlichung dieses Dokuments kein Dual-Stack-System. Die Bereitstellung kann in einem einzelnen Stack mit IPv4 oder IPv6 nur in den Management- und/oder Unternehmensschnittstellen des DNA Centers erfolgen.
- Clients - Cisco SD-Access unterstützt Dual-Stack (IPv4 und IPv6) oder Single-Stack (IPv4 oder IPv6). Im Fall eines einzelnen IPv6-Stacks muss DNA Center jedoch einen Dual-Stack-Pool erstellen, um einen reinen IPv6-Client zu unterstützen. Das IPv4 im Dual-Stack-Pool ist nur eine Dummy-Adresse, da der Client die IPv4-Adresse voraussichtlich deaktivieren wird.

IPv6-Overlay-Architektur in Cisco Software-Defined Access

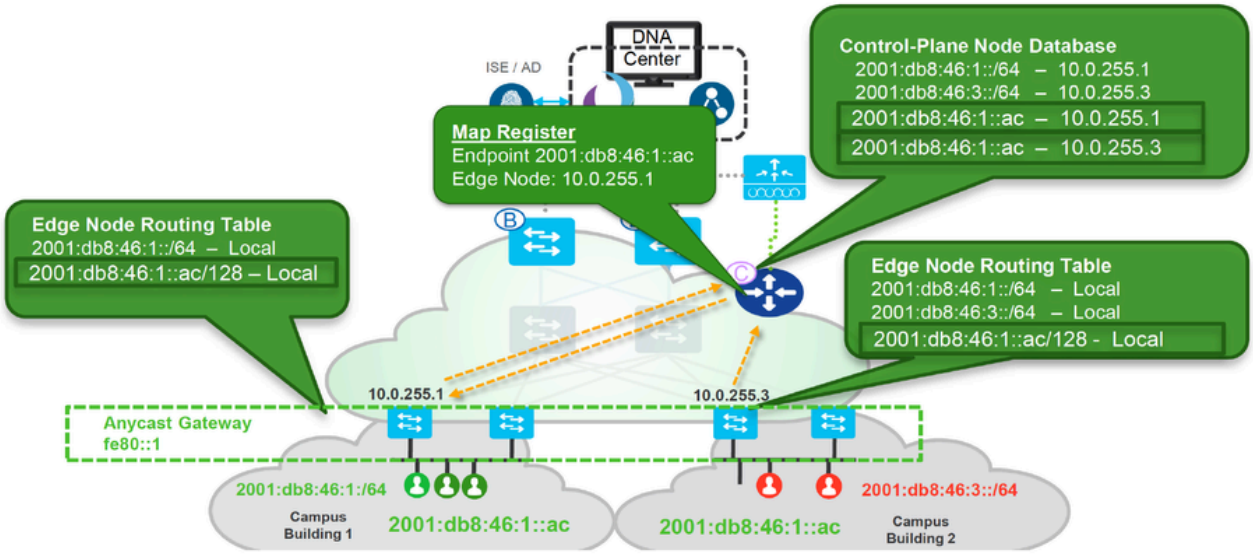


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

IPv6-Overlay-Architektur

IPv6 mit Cisco DNA-Center

Es gibt zwei Möglichkeiten, den IPv6-Pool im Cisco DNA Center zu aktivieren:
1. Erstellen Sie einen neuen Dual-Stack-IPv4/v6-Pool - Greenfield
2. Bearbeiten Sie IPv6 im bereits vorhandenen IPv4-Pool - Brawnfield-Migration.

Die aktuelle Version (bis zu 2.3.x) von DNA Center unterstützt kein IPv6. Nur ein Pool, wenn der Benutzer plant, einen einzigen/nativen Nur-IPv6-Adressclient zu unterstützen. Eine Dummy-IPv4-Adresse muss mit dem IPv6-Pool verknüpft werden. Beachten Sie, dass aus dem bereitgestellten IPv4-Pool, der bereits mit einem zugewiesenen Standort vorhanden ist, eine IPv6-Adresse für den

Pool erstellt wurde. Das DNA Center bietet eine Migrationsoption für die SD-Access-Fabric, bei der der Benutzer die Fabric für diesen Standort neu bereitstellen muss. In der Fabric, zu der der Standort gehört, wird eine Warnmeldung angezeigt, die besagt, dass die Fabric neu konfiguriert werden muss. Beispiele finden Sie in den folgenden Bildern:

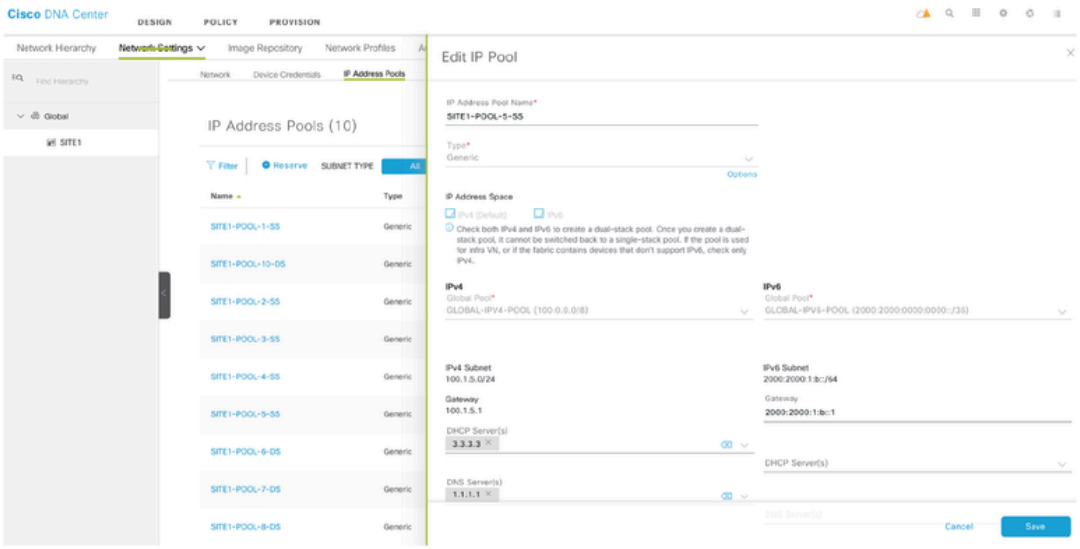


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

Upgrade eines einzelnen IPv4-Pools auf einen Dual-Stack-Pool durch Bearbeiten der IPv4-Pooloption

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

Fabric hat eine Warnmeldung, die eine "Neukonfiguration der Fabric" erfordert.

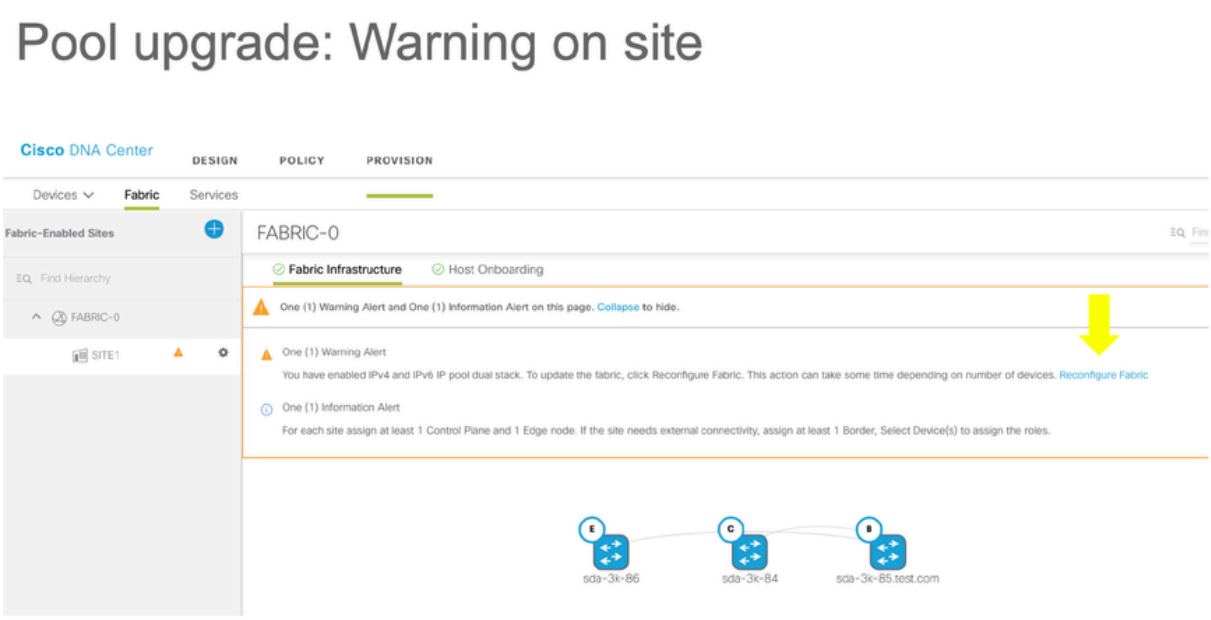


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

Der Benutzer muss auf "Reconfigure Fabric" klicken, um die Fabric-Knoten automatisch neu bereitzustellen, damit die Dual-Stack-Konfiguration im Rahmen des Migrationsprozesses wirksam wird.

Überlegungen zum IPv6-Design bei Cisco SD-Access

Obwohl die Cisco SD-Access-Clients mit Dual-Stack- oder IPv6-basierten Netzwerkeinstellungen ausgeführt werden können, enthält die aktuelle SD-Access Fabric-Implementierung mit der DNA Center Switch (SW)-Version bis 2.3.x.x einige Überlegungen zur IPv6-Bereitstellung.

- Cisco SD-Access unterstützt IPv4-grundlegende Routing-Protokolle. Der IPv6-Client-Datenverkehr wird also transportiert, wenn er in IPv4-Header gekapselt wird. Dies ist eine Voraussetzung für die aktuelle LISP-Softwarebereitstellung. Dies bedeutet jedoch nicht, dass das Underlay das IPv6-Routing-Protokoll nicht aktivieren kann, sondern nur, dass der SD-Access-Overlay-LISP aufgrund seiner Abhängigkeit nicht ausgeführt wird.
- Natives IPv6-Multicast wird nicht unterstützt, da das Fabric-Underlay derzeit nur IPv4 sein kann.
- Wireless für Gäste kann nur mit dem Dual Stack ausgeführt werden. Aufgrund der aktuellen Identity Services Engine (ISE)-Version (z. B. bis 3.2) wird das IPv6-Gastportal nicht unterstützt. Daher kann ein reiner IPv6-Gastclient nicht authentifiziert werden.
- Die Automatisierung von IPv6-Anwendungs-QoS-Richtlinien wird in der aktuellen DNA Center-Version nicht unterstützt. In diesem Dokument werden die erforderlichen Schritte zur Implementierung von IPv6 QoS für kabelgebundene und drahtlose Dual-Stack-Clients in Cisco SD-Access beschrieben, die für einen der Benutzer in großem Umfang bereitgestellt wurden.
- Für IPv4 (TCP/UDP) und IPv6 (nur TCP) wird eine Wireless-Client-Ratenbegrenzungsfunktion für Downstream- und Upstream-Datenverkehr unterstützt,

entweder pro Service Set Identifier (SSID) oder pro Client auf Basis einer Richtlinie. Eine IPv6-UDP-Ratenbegrenzung wird noch nicht unterstützt.
- Ein Upgrade des IPv4-Pools auf einen Dual-Stack-Pool ist möglich. Ein Dual-Stack-Pool kann jedoch nicht auf einen IPv4-Pool herabgestuft werden. Wenn der Benutzer den Dual-Stack-Pool wieder aus dem Single-Stack-IPv4-Pool entfernen möchte, muss er den gesamten Dual-Stack-Pool freigeben.
- Ein einzelnes IPv6 wird noch nicht unterstützt, während im aktuellen DNA Center nur ein IPv4- oder Dual-Stack-Pool erstellt werden kann.
- Die Plattform von Cisco IOS® XE umfasst die Mindestanforderung der Softwareversion 16.9.2 und höher.
- IPv6 Guest Wireless wird auf Cisco IOS XE-Plattformen noch nicht unterstützt, während AireOS (8.10.105.0+) eine Problemumgehung unterstützt.
- Ein Dual-Stack-Pool kann nicht in INFRA_VN zugewiesen werden, wenn nur ein Access Point (AP) oder ein erweiterter Node-Pool zugewiesen werden kann.
- Die LAN-Automatisierung unterstützt IPv6 noch nicht.

Wenn Sie eine SD-Access-Fabric mit aktiviertem IPv6 entwerfen, müssen Sie neben den oben genannten Einschränkungen stets die Skalierbarkeit jeder Fabric-Komponente berücksichtigen. Wenn ein Endpunkt mehrere IPv4- oder IPv6-Adressen hat, wird jede Adresse als individueller Eintrag gezählt.

Fabric-Hosteinträge umfassen Access Points sowie klassische und richtlinienerweiterte Knoten.

Weitere Überlegungen zur Skalierung von Randknoten:

/32 (IPv4)- oder /128 (IPv6)-Einträge werden verwendet, wenn der Grenzknoten Datenverkehr von außerhalb der Fabric an einen Host in der Fabric weiterleitet.

Für alle Switches mit Ausnahme der Cisco Catalyst High-Performance Switches der Serie 9500 und der Cisco Catalyst Switches der Serie 9600:

- IPv4 verwendet einen Ternary Content Addressable Memory (TCAM)-Eintrag (Fabric-Host-Einträge) für jede IPv4-IP-Adresse.
- IPv6 verwendet zwei TCAM-Einträge (Fabric-Host-Einträge) für jede IPv6-IP-Adresse.

Vorteile der Cisco Catalyst High-Performance Switches der Serie 9500 und der Cisco Catalyst Switches der Serie 9600:

- IPv4 verwendet einen TCAM-Eintrag (Fabric-Host-Einträge) für jede IPv4-IP-Adresse.
- IPv6 verwendet einen TCAM-Eintrag (Fabric-Host-Einträge) für jede IPv6-IP-Adresse.

Einige der Endgeräte unterstützen DHCPv6 nicht, z. B. Android OS-basierte Smartphones, die IPv6-Adressen über die Stateless Address Autoconfiguration (SLAAC) beziehen. Ein einzelner Endpunkt kann dann mehr als zwei IPv6-Adressen erhalten. Dieses Verhalten beansprucht mehr Hardwareressourcen auf jedem Fabric-Knoten, insbesondere für die Fabric Border und die Kontrollknoten. Beispielsweise installiert er jedes Mal, wenn der Grenzknoten Datenverkehr an die Edge-Knoten für einen beliebigen Endpunkt senden möchte, eine Host-Route im TCAM-Eintrag

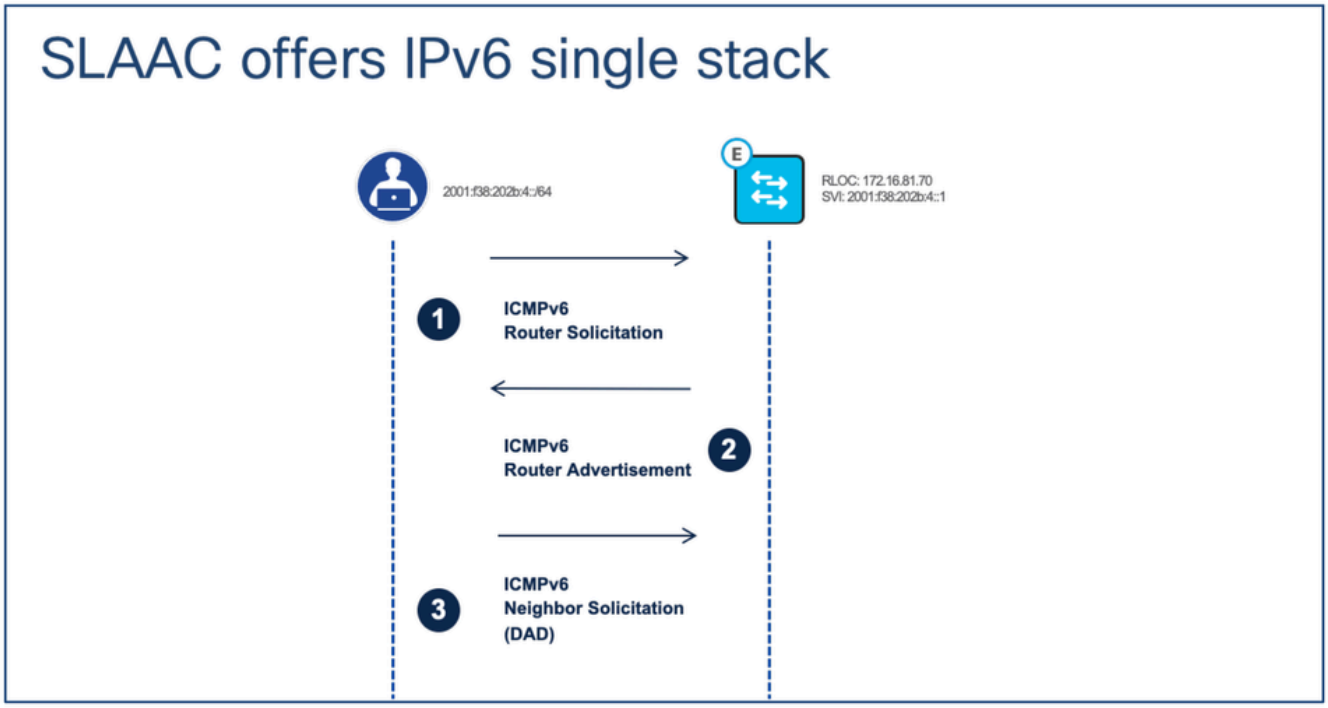
und brennt einen VXLAN-Adjacency-Eintrag im Hardware (HW)-TCAM.

Kabelgebundene und Wireless-Client-Verbindungen und Anrufverläufe

Sobald der Client mit dem Fabric Edge verbunden ist, gibt es verschiedene Möglichkeiten, wie er die IPv6-Adressen erhält. In diesem Abschnitt wird die gängigste Methode zur Client-IPv6-Adressierung beschrieben, nämlich SLAAC und DHCPv6.

IPv6-Adresszuweisung - SLAAC

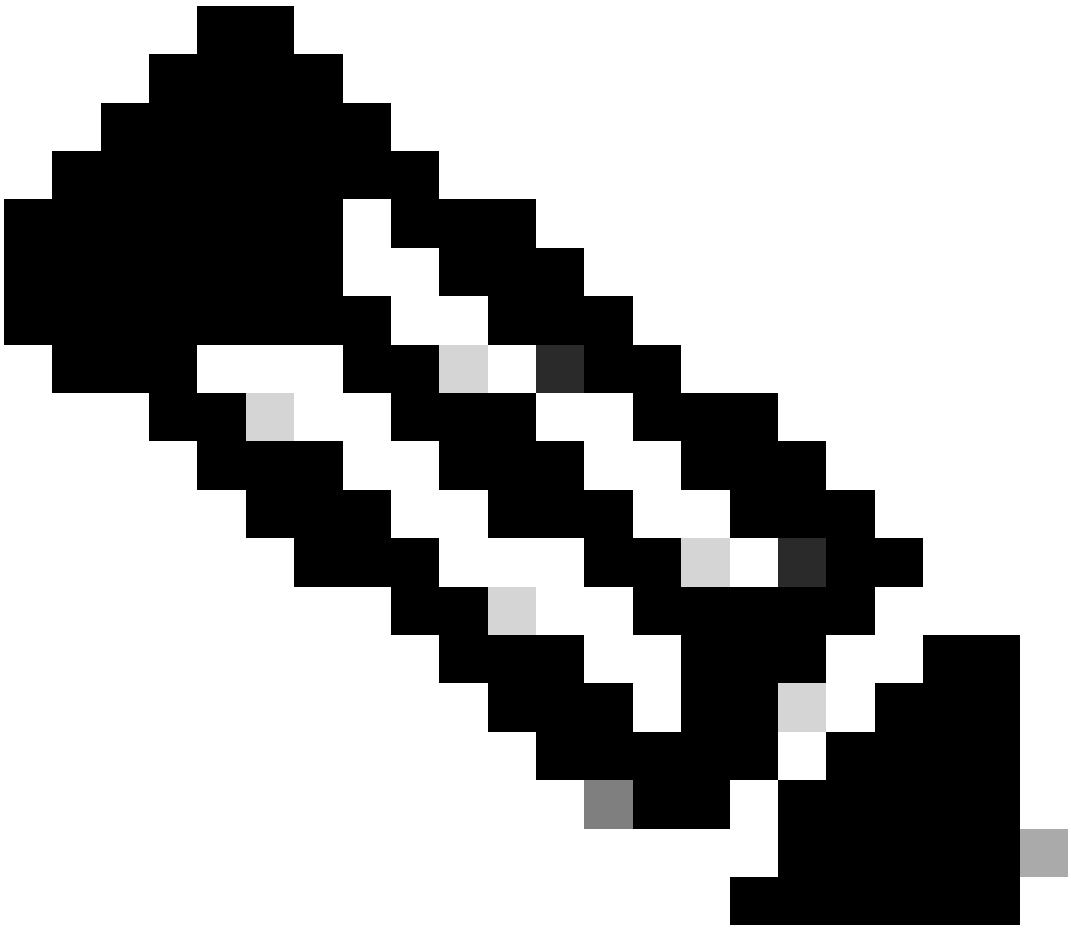
Die SLAAC in Software-Defined Access (SDA) unterscheidet sich nicht vom standardmäßigen SLAAC-Prozessablauf. Damit SLAAC ordnungsgemäß funktioniert, muss der IPv6-Client mit einer Link-Local-Adresse in seiner Schnittstelle konfiguriert werden. Die Art und Weise, wie der Client sich automatisch mit der Link-Local-Adresse konfiguriert, wird in diesem Dokument nicht behandelt.



IPv6-Adresszuweisung - SLAAC

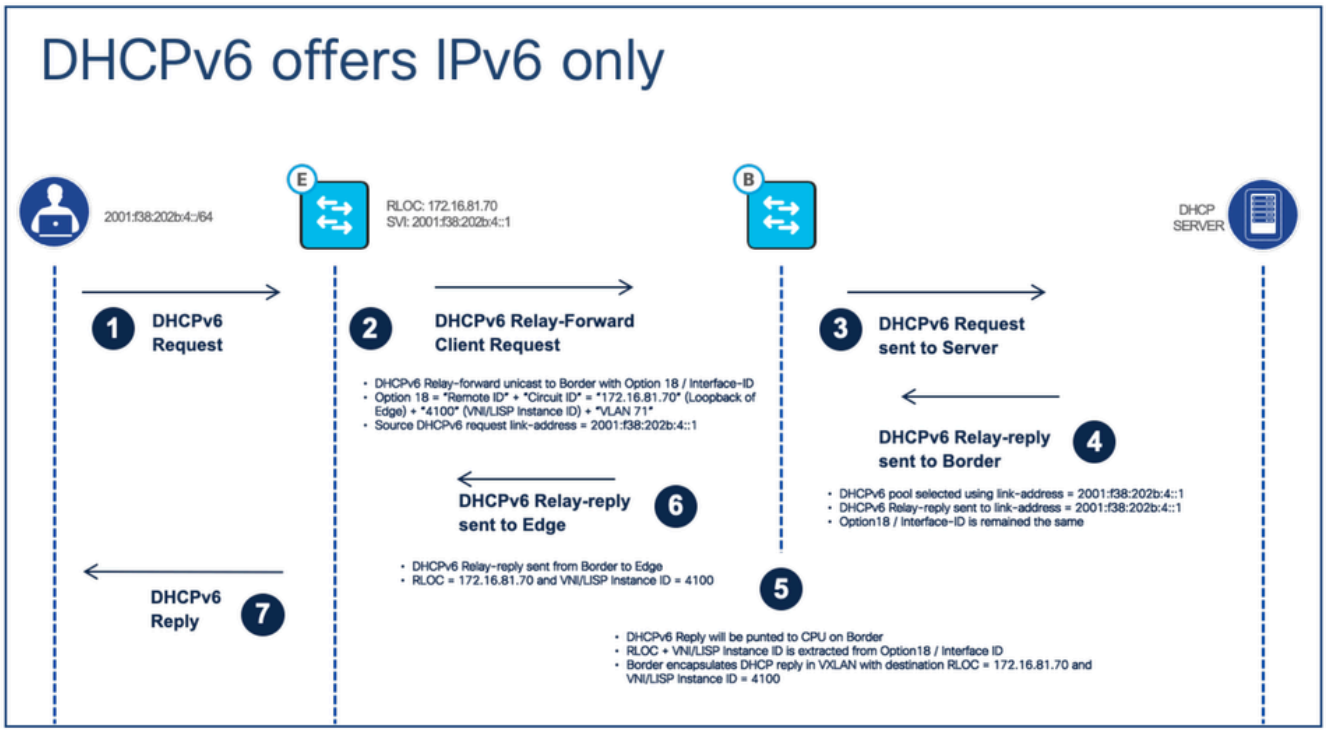
Anrufflussbeschreibung:
Schritt 1: Nachdem der IPv6-Client sich selbst mit einer IPv6-Link-Local-Adresse konfiguriert hat, sendet der Client eine ICMPv6 Router Solicitation (RS)-Nachricht an Fabric Edge. Der Zweck dieser Nachricht besteht darin, das globale Unicast-Präfix des verbundenen Segments zu erhalten.
Schritt 2: Nachdem der Fabric Edge die RS-Nachricht empfangen hat, antwortet er mit einer ICMPv6 Router Advertisement (RA)-Nachricht, die das globale IPv6-Unicast-Präfix und dessen Länge enthält.

Schritt 3: Sobald der Client die RA-Nachricht erhält, kombiniert er das globale IPv6-Unicast-Präfix mit seiner EUI-64-Schnittstellenkennung, um seine eindeutige globale IPv6-Unicast-Adresse zu generieren und sein Gateway auf die Link-lokale Adresse der SVI des Fabric-Edge festzulegen, die mit dem Segment des Clients verknüpft ist. Anschließend sendet der Client eine ICMPv6 Neighbor Solicitation-Nachricht, um eine Duplicate Address Detection (DAD) durchzuführen und sicherzustellen, dass die erhaltene IPv6-Adresse eindeutig ist.



Anmerkung: Alle SLAAC-bezogenen Nachrichten werden mit der SVI IPv6 Link-Local-Adresse des Clients und des Fabric-Knotens gekapselt.

IPv6-Adresszuweisung - DHCPv6

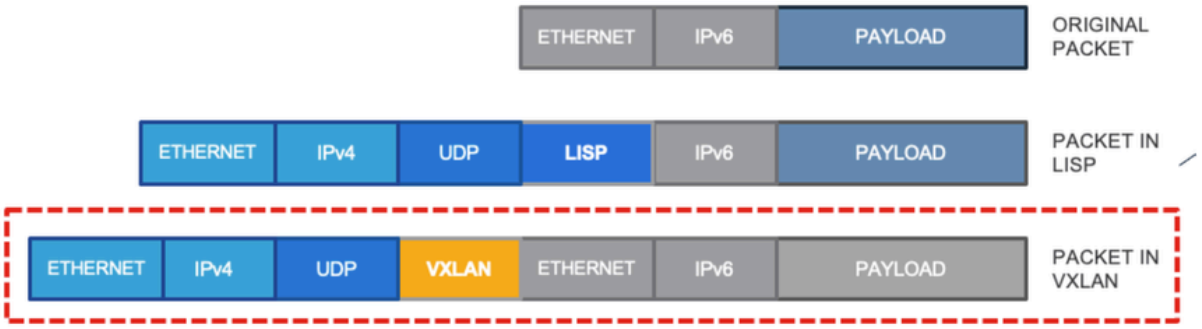


IPv6-Adresszuweisung - DHCPv6

Anrufflussbeschreibung:
Schritt 1: Der Client sendet die DHCPv6-Anforderung an den Fabric-Edge.
Schritt 2: Wenn der Fabric-Edge die DHCPv6-Anforderung empfängt, wird die DHCPv6-Weiterleitungsnachricht verwendet, um die Anforderung mit DHCPv6-Option 18 an den Fabric-Rand weiterzuleiten. Im Vergleich zur DHCP-Option 82 kodiert die DHCPv6-Option 18 sowohl 'Circuit ID' als auch 'Remote ID'. Die LISP-Instanz-ID/VNI, der IPv4 Routing Locator (RLOC) und das Endpunkt-VLAN sind innen codiert.
Schritt 3: Der Fabric Border entkapselt den VXLAN-Header und sendet das DHCPv6-Paket per Unicast an den DHCPv6-Server.
Schritt 4: Der DHCPv6-Server empfängt die Relay-Forward-Nachricht und verwendet die Quell-Link-Adresse (DHCPv6 Relay Agent/Client Gateway) der Nachricht, um den IPv6-IP-Pool auszuwählen und die IPv6-Adresse zuzuweisen. Senden Sie dann die DHCPv6-Relay-Response-Nachricht an die Client-Gateway-Adresse zurück. Option 18 bleibt unverändert.
Schritt 5: Wenn die Fabric Border die Relay-Response-Nachricht empfängt, extrahiert sie die RLOC- und LISP-Instanz/VNI aus Option 18. Fabric Border kapselt die Relay-Response-Nachricht in VXLAN mit einem Ziel, das sie aus Option 18 extrahiert.
Schritt 6: Die Fabric-Grenze sendet die DHCPv6-Relay-Antwort-Nachricht an den Fabric-Edge, mit dem der Client verbunden ist.
Schritt 7: Wenn Fabric Edge die DHCPv6-Relay-Antwort-Nachricht empfängt, entkapselt es den VXLAN-Header der Nachricht und leitet die Nachricht an den Client weiter. Anschließend kennt der Client die ihm zugewiesene IPv6-Adresse.

IPv6-Kommunikation in Cisco SD-Access

Für die IPv6-Kommunikation werden die standardmäßigen Kommunikationsmethoden auf LISP-Basis und auf VXLAN-Basis genutzt. Bei der aktuellen Implementierung in Cisco SD-Access verwendet LISP und VXLAN den äußeren IPv4-Header, um die internen IPv6-Pakete zu übertragen. Dieses Bild zeichnet diesen Prozess auf.



Äußerer IPv4-Header mit den IPv6-Paketen im Inneren

Das bedeutet, dass alle LISP-Abfragen das native IPv4-Paket verwenden, während die Kontrollebenen-Knotentabelle Details zum RLOC mit IPv6- und IPv4-IP-Adressen des Endpunkts enthält. Dieser Prozess wird im nächsten Abschnitt unter dem Aspekt der Wireless-Endgeräte ausführlich erläutert.

Wireless IPv6-Kommunikation in Cisco SD-Access

Die Wireless-Kommunikation erfolgt über zwei spezifische Komponenten: Access Points und Wireless LAN-Controller, mit Ausnahme der typischen Cisco SD-Access Fabric-Komponenten. Wireless Access Points erstellen einen CAPWAP-Tunnel (Control and Provisioning of Wireless Access Points) mit dem Wireless LAN Controller (WLC). Während der Client-Datenverkehr am Fabric Edge vorhanden ist, wird die Kommunikation auf anderer Steuerungsebene, einschließlich der Funkstatistiken, vom WLC verwaltet. Aus IPv6-Sicht müssen sowohl der WLC als auch der WAP über die IPv4-Adressen verfügen, und bei der CAPWAP-Kommunikation werden diese IPv4-Adressen verwendet. Während der Non-Fabric-WLC und der Access Point die IPv6-Kommunikation unterstützen, verwendet Cisco SD-Access IPv4 für die gesamte Kommunikation, die IPv6-Datenverkehr von Clients innerhalb von IPv4-Paketen überträgt. Das bedeutet, dass zugewiesene AP-Pools unter Infra VN nicht mit IP-Pools verknüpft werden können, die Dual-Stack-Pools sind, und dass ein Fehler ausgelöst wird, wenn versucht wird, diese Zuordnung vorzunehmen. Die drahtlose Kommunikation innerhalb von Cisco SDA kann in die folgenden Hauptaufgaben unterteilt werden:

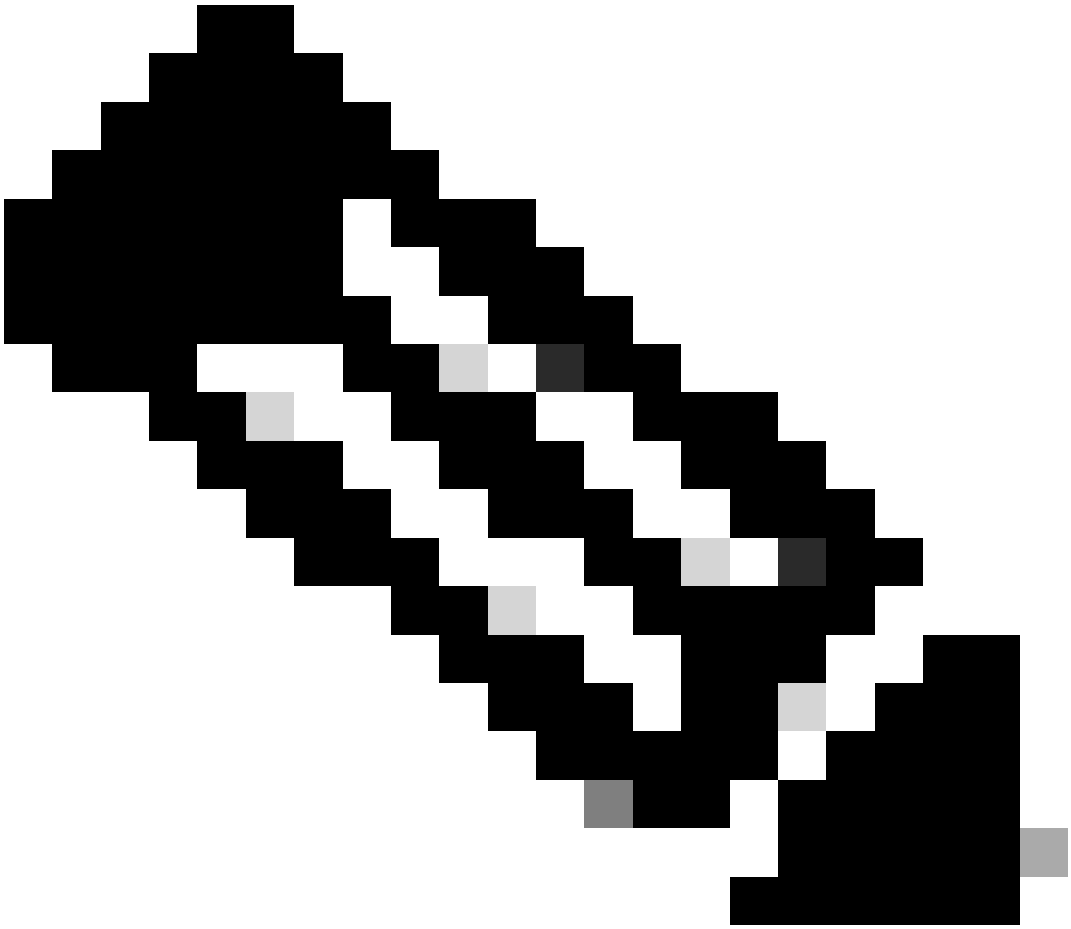
- Access Point-Onboarding
- Client-On-Boarding

Diese Ereignisse aus der IPv6-Perspektive betrachten

Access Point-Onboarding

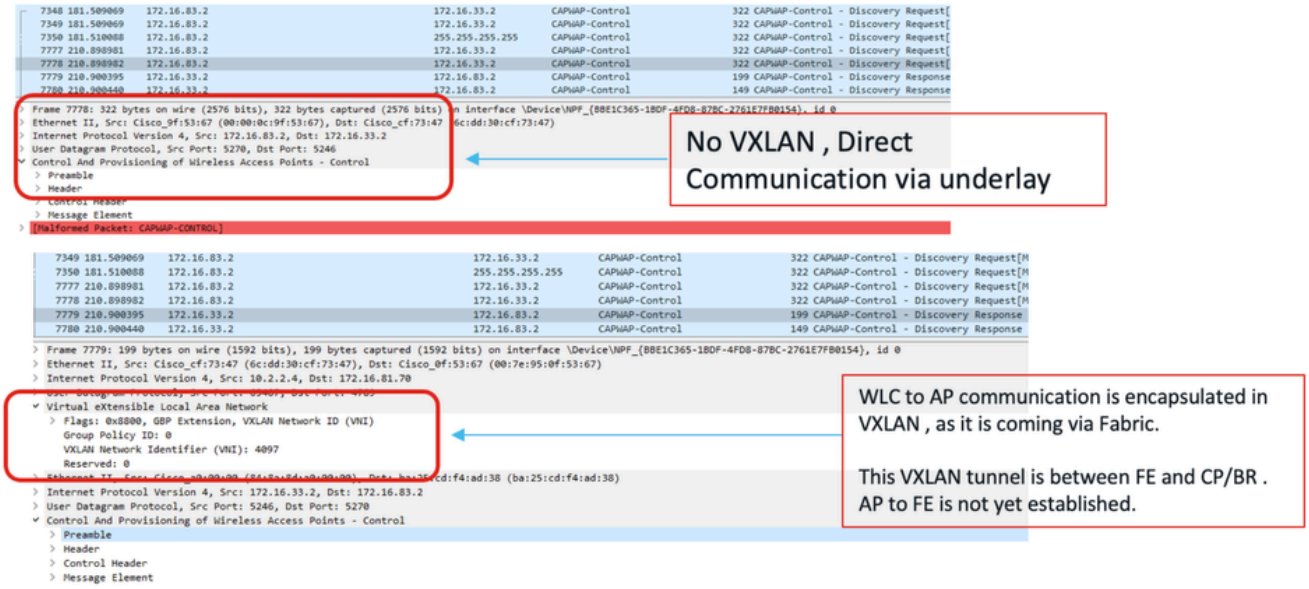
Dieser Prozess bleibt für IPv6 und IPv4 derselbe, da sowohl WLC als auch AP über IPv4-Adressen und -Schritte verfügen:
1. Der Fabric Edge (FE)-Port ist für die Integration des AP konfiguriert.
2. Der WAP ist mit dem FE-Port verbunden und benachrichtigt FE über den CDP-WAP über sein Vorhandensein (auf diese Weise kann FE das richtige VLAN zuweisen).
3. AP ruft die IPv4-Adresse vom DHCP-Server ab und FE registriert AP und aktualisiert Control Plane (Control Plane (CP) Node) mit AP-Details.
4. Der AP wird über traditionelle Methoden (wie DHCP-Option 43) dem WLC hinzugefügt.
5. Der WLC prüft, ob der Access Point Fabric-fähig ist, und fragt die Kontrollebene nach AP-RLOC-Informationen ab (z. B. RLOC Requested/Response Received).
6. CP antwortet mit der RLOC IP des AP auf den WLC.
7. WLC registriert die AP Media Access Control (Address) (MAC) in CP.
8. Der CP aktualisiert den FE mit den Details des WLC über den AP (dadurch wird der FE angewiesen, den VXLAN-Tunnel mit dem AP zu initiieren).

FE verarbeitet die Informationen und erstellt einen VXLAN-Tunnel mit AP. Zu diesem Zeitpunkt kündigt der Access Point die Fabric-fähige SSID an.



> Anmerkung: Falls der Access Point die Nicht-Fabric-SSIDs sendet und keine Fabric-SSID sendet, prüfen Sie, ob der VXLAN-Tunnel zwischen dem Access Point und dem Fabric Edge-Knoten vorhanden ist.

Beachten Sie auch, dass die AP-zu-WLC-Kommunikation immer über Underlay-CAPWAP erfolgt und dass die gesamte Kommunikation zwischen WLC und AP VXLAN-CAPWAP über Overlay verwendet. Wenn Sie also Pakete erfassen, die vom AP zum WLC übertragen werden, wird nur CAPWAP angezeigt, während der umgekehrte Datenverkehr über einen VXLAN-Tunnel läuft. In diesem Beispiel wird die Kommunikation zwischen dem Access Point und dem WLC erläutert.



Paketerfassung vom AP zum WLC (CAPWAP-Tunnel) im Vergleich zu WLC zum AP (VxLAN-Tunnel im Fabric)

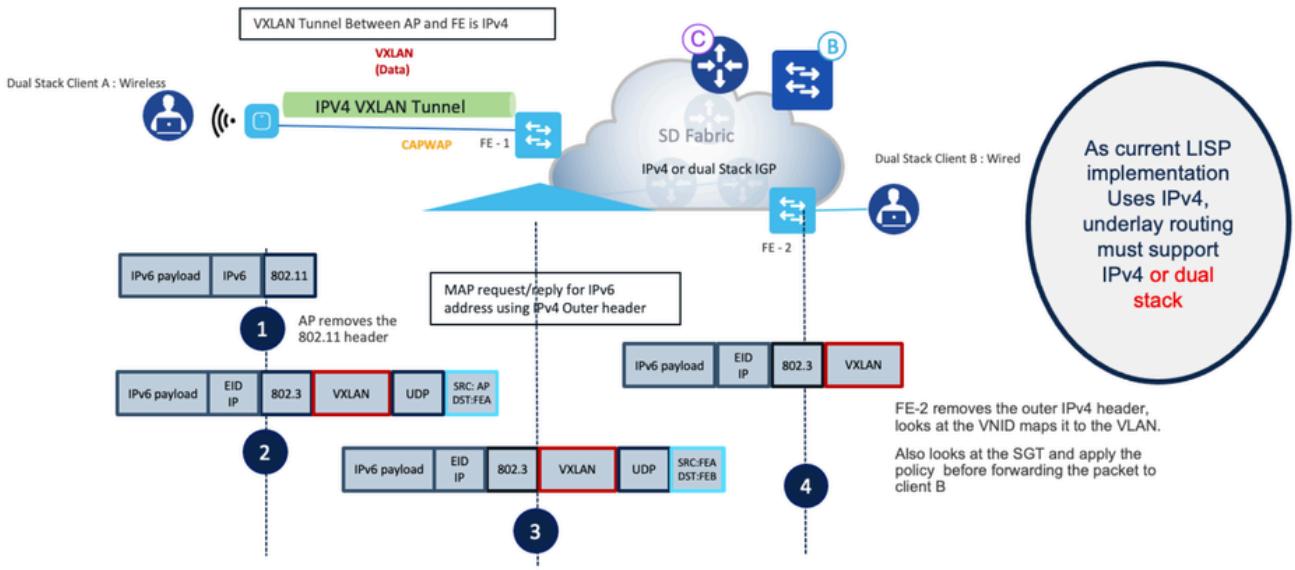
Client-Integration

Der On-Boarding-Prozess für Dual-Stack/IPv6-Clients bleibt derselbe, aber der Client verwendet die IPv6-Adresszuweisungsmethoden wie SLAAC/DHCPv6, um die IPv6-Adressen abzurufen.
1. Der Client wird der Fabric hinzugefügt und aktiviert SSID auf dem AP.
2. WLC kennt den AP RLOC.
3. Client authentifiziert und WLC registriert die Client L2 Details mit CP und aktualisiert AP.
4. Der Client initiiert die IPv6-Adressierung über konfigurierte Methoden - SLAAC/DHCPv6.
5. FE löst die IPv6-Client-Registrierung bei der CP Host Tracking Database (HTDB) aus. AP zu FE und FE zu anderen Zielen verwenden die VXLAN- und LISP IPv6-Kapselung innerhalb von IPv4-Frames.

Client-Client-Kommunikation mit IPv6

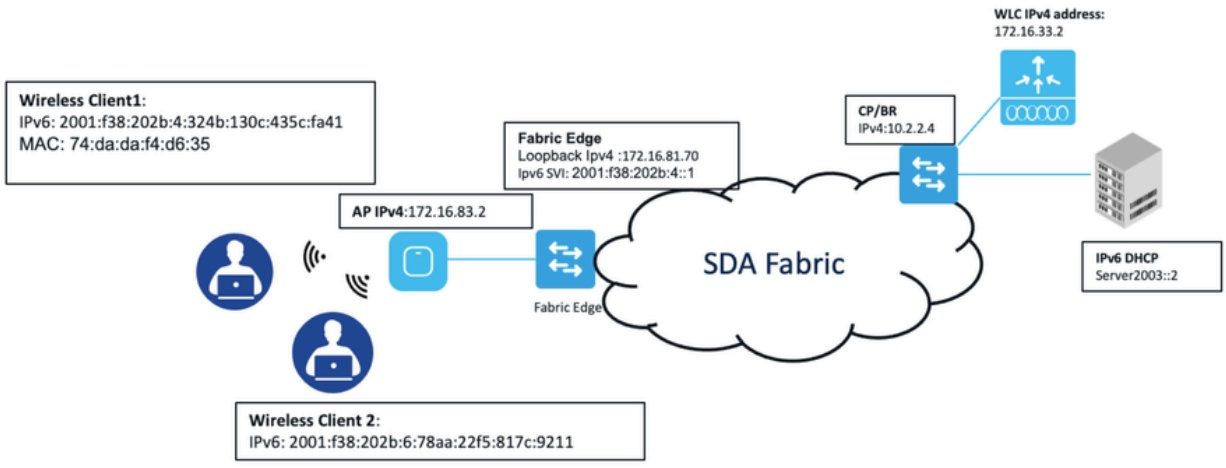
Das Bild fasst den IPv6 Wireless Client-Kommunikationsprozess mit einem anderen

kabelgebundenen IPv6 Client zusammen. (Dies setzt voraus, dass der Client authentifiziert ist und die IPv6-Adresse über konfigurierte Methoden erhalten hat.)
1. Der Client sendet die 802.11-Frames mit IPv6-Payload an den AP.
2. AP entfernt die 802.11-Header und sendet die ursprüngliche IPv6-Nutzlast im IPv4-VXAN-Tunnel an Fabric Edge.
3. Fabric Edge verwendet die Message Access Protocol (MAP)-Anforderung zur Identifizierung des Ziels und sendet den Frame mit IPv4 VXLAN an das Ziel-RLOC.
4. Am Ziel-Switch wird der IPv4-VXLAN-Header entfernt und das IPv6-Paket an den Client gesendet.

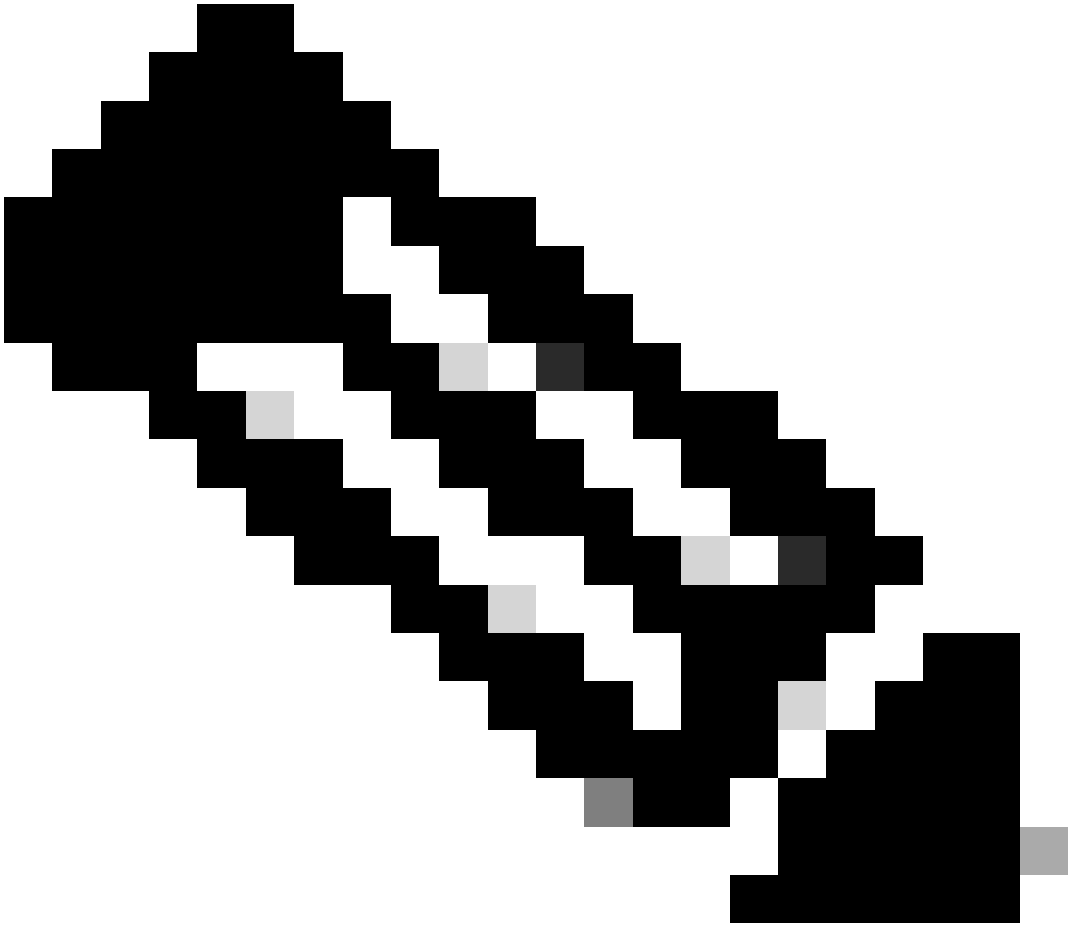


Dual-Stack Wireless Client-zu-Dual-Stack kabelgebundene Client-Paketflüsse

Sehen Sie sich diesen Prozess mit den Paketerfassungen im Detail an, und beziehen Sie sich auf das Image für IP-Adressen und MAC-Adressdetails. Hinweis: Bei dieser Konfiguration werden beide Dual-Stack-Clients verwendet, die mit denselben Access Points verbunden sind, jedoch unterschiedlichen IPv6-Subnetzen (SSIDs) zugeordnet sind.

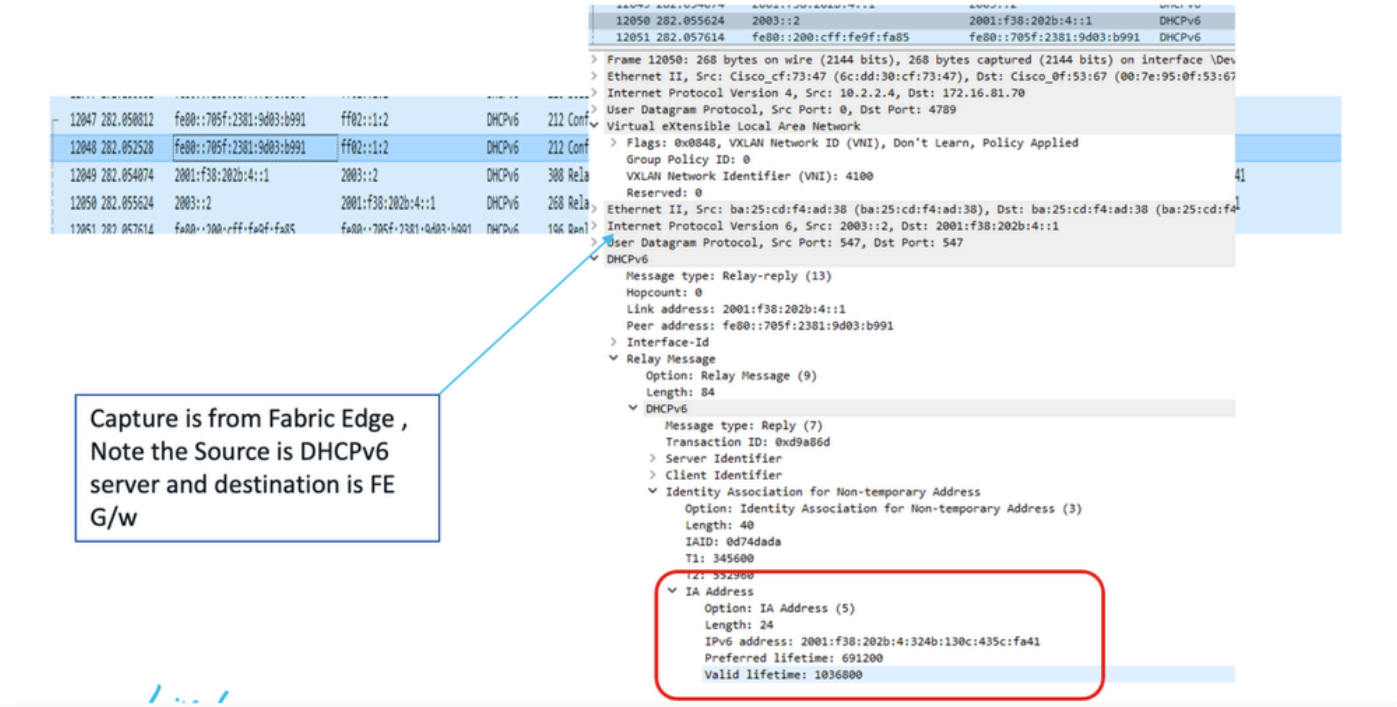


Details zu IP-Adressen und MAC-Adressen für das SD-Access Fabric-Netzwerk



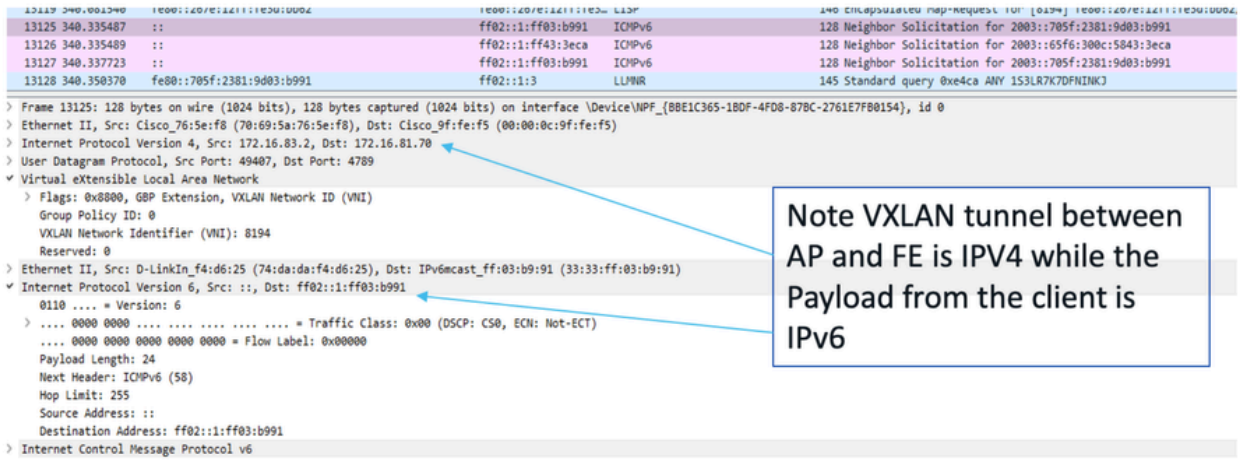
Anmerkung: Bei jeder IPv6-Kommunikation außerhalb der Fabric, z. B. DHCP/DNS, muss IPv6-Routing zwischen der Grenze und der Nicht-Fabric-Infrastruktur aktiviert sein.

Schritt 1: Der Client authentifiziert sich und ruft die IPv6-Adresse von den konfigurierten Methoden ab.



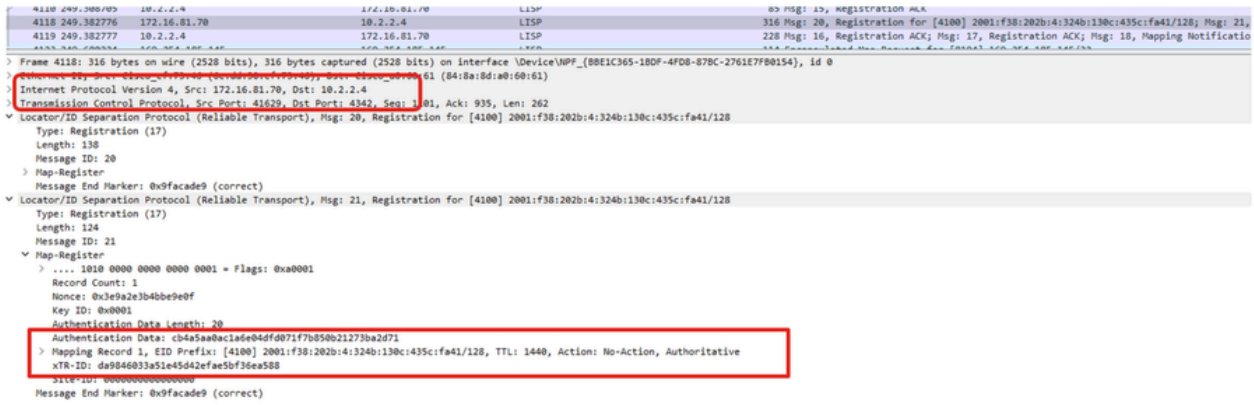
Paketerfassung vom DHCPv6-Server zum Fabric Edge-Knoten

Schritt 2: Der Wireless-Client sendet die 802.11-Frames mit der IPv6-Nutzlast an den Access Point.
Schritt 3: Der Access Point entfernt den Wireless-Header und sendet das Paket an den Fabric-Edge. Dabei wird der IPv4-basierte VXLAN-Tunnel-Header verwendet, da der Access Point über die IPv4-Adresse verfügt.



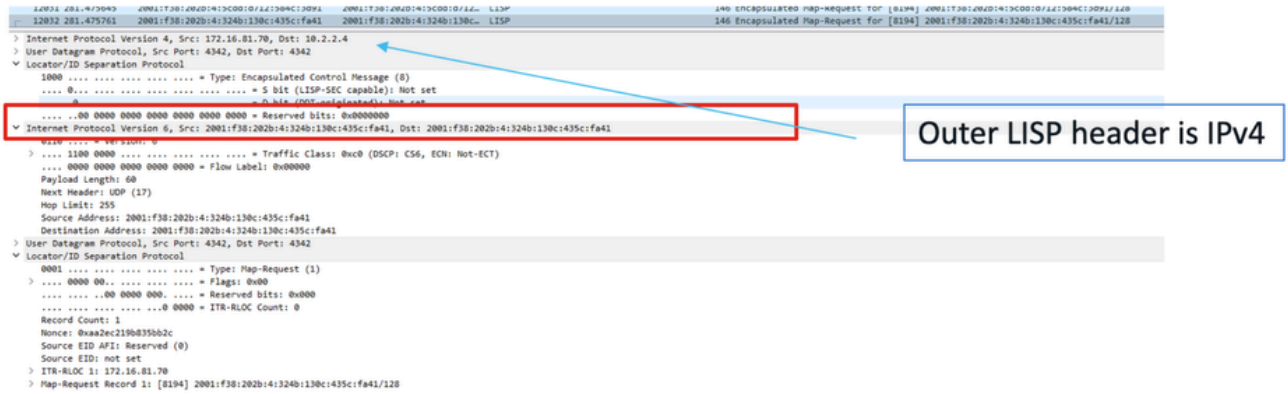
Paketerfassung für den VxLAN-Tunnel zwischen FE und AP

Schritt 3.1: Fabric Edge registriert den IPv6-Client auf der Kontrollebene. Dabei wird die IPv4-Registrierungsmethode mit Details zum IPv6-Client verwendet.



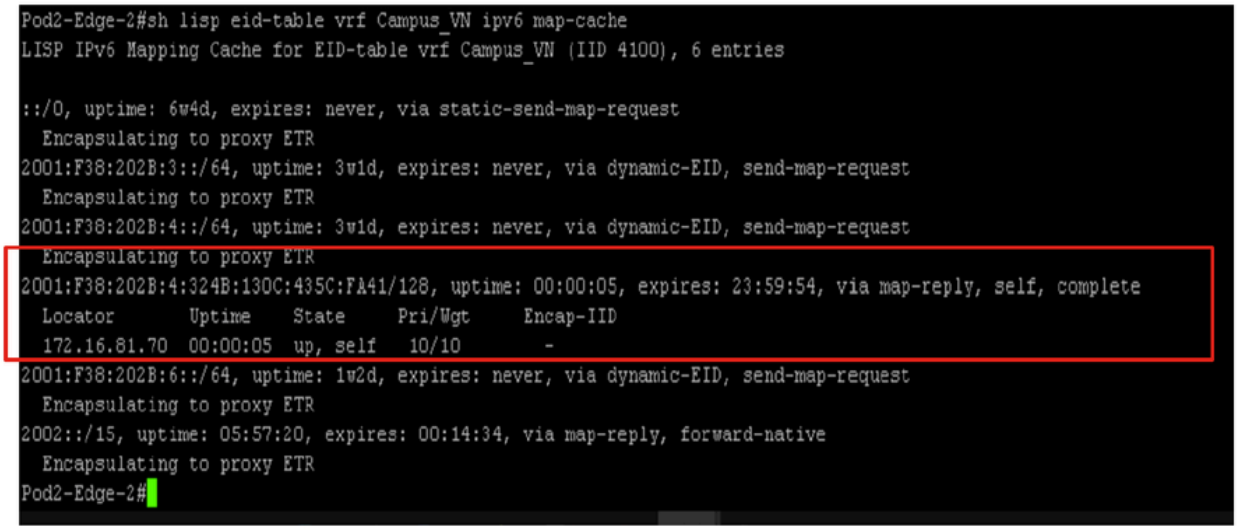
Paketerfassung für FE-Register mit Kontrollebene für IPv6-Client

Schritt 3.2: FE sendet die MAP-Anforderung an die Steuerungsebene, um das Ziel-RLOC zu identifizieren.



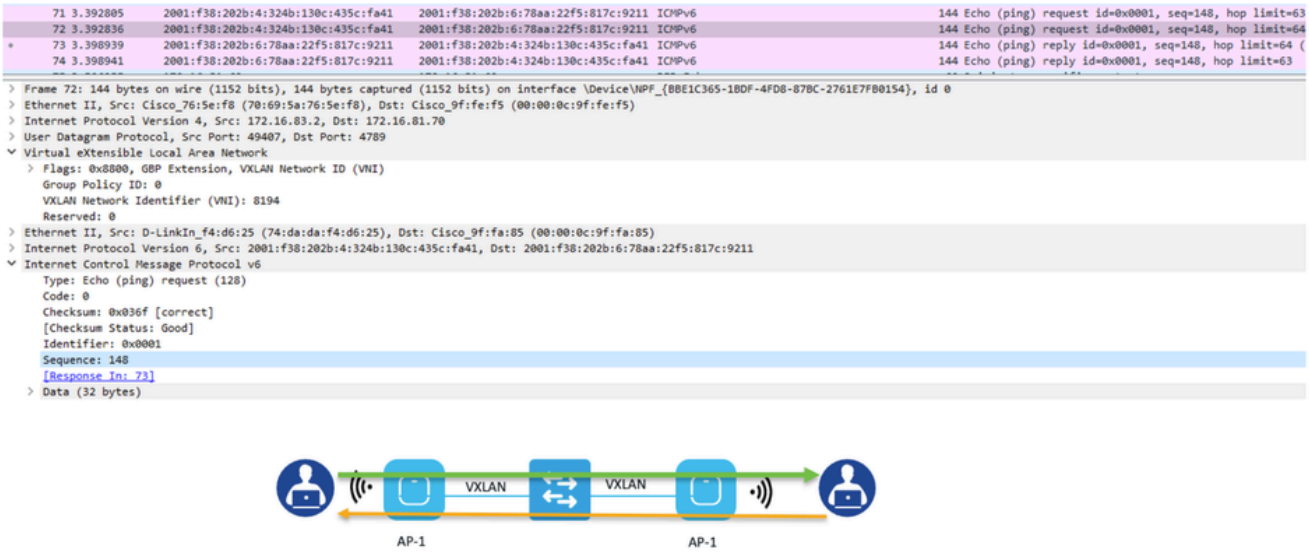
Paketerfassung von FE an CP mit MAP-Registrierungsnachrichten

Fabric Edge unterhält auch den MAP-Cache für bekannte IPv6-Clients, wie in diesem Bild dargestellt.



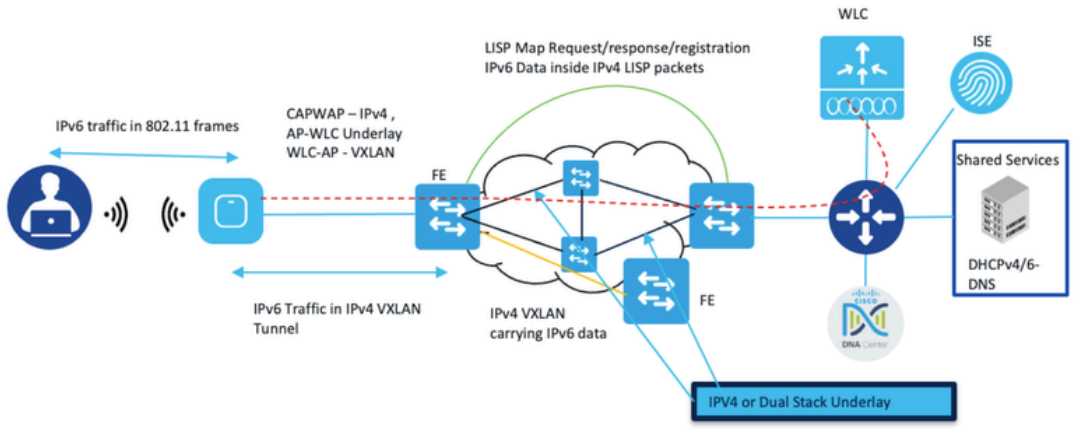
Fabric Edge-Bildschirmausgabe von IPv6-Overlay-Map-Cache-Informationen

Schritt 4: Das Paket wird mit dem IPv4-VXLAN, das die ursprüngliche IPv6-Nutzlast enthält, an das Ziel-RLOC weitergeleitet. Da beide Clients mit demselben WAP verbunden sind, nimmt der IPv6-Ping-Befehl diesen Pfad an.

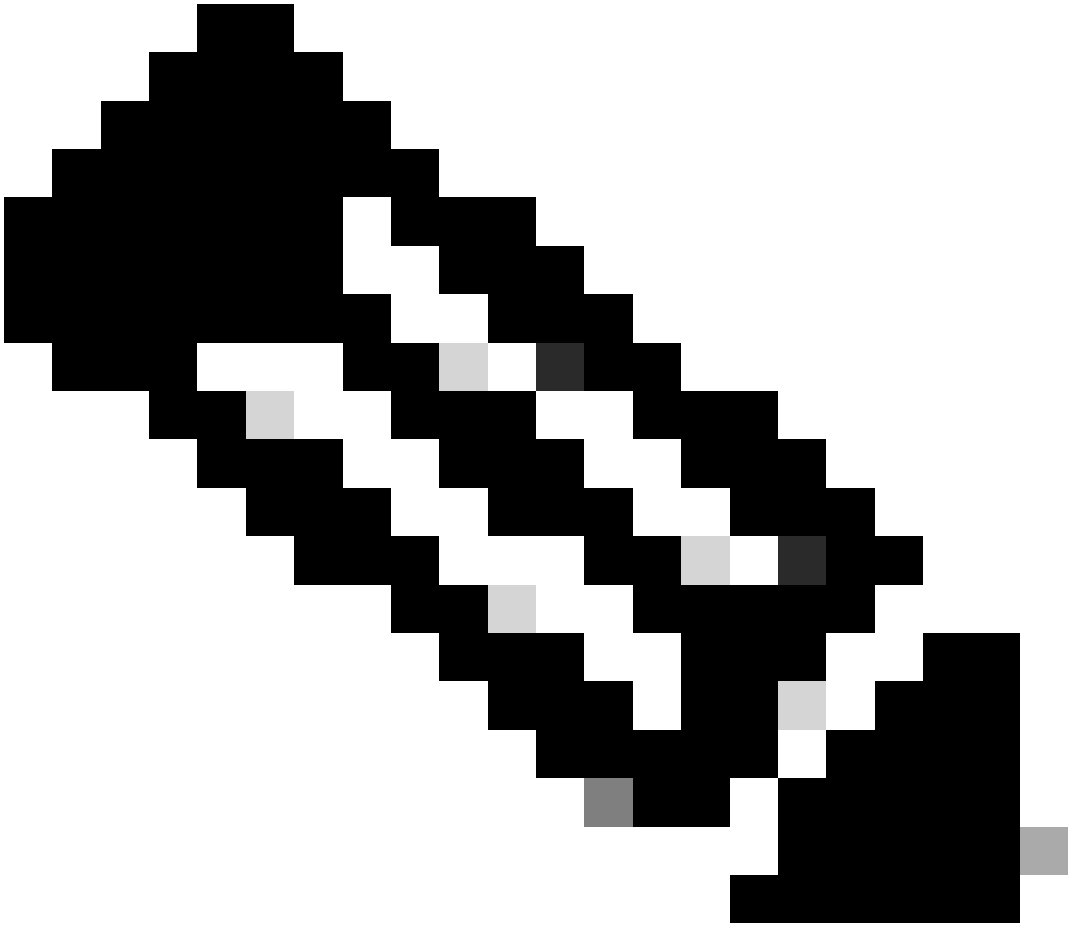


Paketerfassung für IPv6-Ping zwischen zwei Wireless-Clients, die am selben AP registriert sind

Dieses Bild fasst die IPv6-Kommunikation aus Sicht eines Wireless-Clients zusammen.



Die Abbildung fasst die IPv6-Kommunikation aus der Sicht eines Wireless-Clients zusammen.



Anmerkung: IPv6 Guest Access (Webportal) über Cisco Identity Services wird aufgrund von ISE-Beschränkungen nicht unterstützt.

Abhängigkeitsmatrix

Beachten Sie die Abhängigkeiten und die Unterstützung von IPv6 von verschiedenen Wireless-Komponenten, die Teil von Cisco SD-Access sind. Die Tabelle in diesem Bild fasst diese Funktionsmatrix zusammen.

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

Cat 9800 WLC IPv6 - Funktionen nach Version

Überwachen der Kontrollebene für IPv6

Sobald Sie IPv6 aktivieren, werden zusätzliche Einträge zu Host-IPv6 auf den Map Server (MS)/Map Resolver Servern (MR) angezeigt. Da ein Host über mehrere IPv6-IP-Adressen verfügen kann, enthält die MS/MR-Lookup-Tabelle Einträge für alle IP-Adressen. Diese wird mit der bereits vorhandenen IPv4-Tabelle kombiniert.
Sie müssen sich in der Geräte-CLI anmelden und diese Befehle eingeben, um alle Einträge zu überprüfen.

```
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
```

Sie können auch die Details zum Host-IPv6 mithilfe der Absicherung überprüfen.

IPv6 QoS-Implementierung in Cisco SD-Access

Die aktuelle Cisco DNA Center-Version (bis zu Version 2.3.x) unterstützt keine Automatisierung der IPv6-QoS-Anwendungsrichtlinien. Benutzer können jedoch manuell IPv6-Vorlagen für kabelgebundene und Wireless-Netzwerke erstellen und die QoS-Vorlage in Fabric Edge-Knoten verschieben. Da DNA Center die IPv4-QoS-Richtlinie nach der Anwendung auf allen physischen Schnittstellen automatisiert, können Sie über eine Vorlage manuell eine Klassenzuordnung (die mit der IPv6-Zugriffskontrollliste (ACL) übereinstimmt) vor "class-default" einfügen.

Nachfolgend finden Sie ein Beispiel für eine kabelgebundene IPv6-QoS-Vorlage, die mit einer vom DNA Center generierten Richtlinienkonfiguration integriert wurde:

```
!
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
```

Fehlerbehebung bei IPv6 in Cisco SD-Access

Fehlerbehebung SD-Access IPv6 ist ganz wie IPv4, können Sie immer den gleichen Befehl mit verschiedenen Schlüsselwortoptionen verwenden, um das gleiche Ziel zu erreichen. Hier sehen Sie einige Befehle, die häufig zur Fehlerbehebung bei SD-Access verwendet werden.

```
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
```

Von Border Node zum Überprüfen des Overlay-DHCPv6-Server-Pings:

```
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
```

Schnelle FAQs zum IPv6-Design mit Cisco SD-Access

Frage: Unterstützt das Cisco Software Defined Network IPv6 für Underlay- und Overlay-Netzwerke?
A. Mit der aktuellen Version (2.3.x) wird zum Zeitpunkt der Erstellung dieses Dokuments nur Overlay unterstützt.

Frage: Unterstützt Cisco SDN natives IPv6 für kabelgebundene und Wireless-Clients?
A: Ja. Dies erfordert Dual-Stack-Pools, die im DNA-Center erstellt werden, während IPv4 der Dummy-Pool ist, da die Clients IPv4-DHCP-Anfragen deaktivieren und nur IPv6-DHCP- oder SLAAC-Adressen angeboten werden.

Frage: Kann ich ein natives Campus-Netzwerk, das nur IPv6 unterstützt, in meiner Cisco SD-Access Fabric verwenden?
Antwort: Nicht mit der aktuellen Version (bis zu 2.3.x). Sie ist Teil der Roadmap.

Frage: Unterstützt Cisco SD-Access L2 IPv6-Übergabe?
A. Derzeit nicht. Es werden nur L2-IPv4-Handoff und/oder L3-Dual-Stack-Handoff unterstützt.

Frage: Unterstützt Cisco SD-Access Multicast für IPv6?
A. Ja, nur Overlay-IPv6 mit Headend-Replikation und Multicast wird unterstützt. Natives IPv6-Multicast wird noch nicht unterstützt.

Frage: Unterstützt Cisco SD-Access Fabric Enabled Wireless Gäste in Dual-Stack-Umgebungen?
A. Noch nicht unterstützt von Cisco IOS XE (Cat9800) WLC. AireOS WLC wird über einen Workaround unterstützt. Nähere Informationen zur Umsetzung des Workaround erhalten Sie beim Cisco Customer Experience Team.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.