소프트웨어 정의 액세스에서 IPv6 구현

목차

소개

이 문서에서는 Cisco® SD-Access(Software-Defined Access)에서 IPv6를 구현하는 방법에 대해 설명합니다.

배경 정보

IPv4는 1983년에 릴리스되었으며 대부분의 인터넷 트래픽에 여전히 사용되고 있습니다. 32비트 IPv4 주소 지정은 40억 개 이상의 고유한 조합을 허용합니다. 그러나 인터넷 연결 클라이언트의 증가로 인해 고유한 IPv4 주소가 부족하게 됩니다. 1990년대 들어 IPv4 주소 지정의 고갈이 불가피하게 되었다.
Internet Engineering Taskforce에서는 이를 예상하여 IPv6 표준을 도입했습니다. IPv6는 128비트를 활용하며 340억 개의 고유 IP 주소를 제공합니다. 이는 증가하는 연결된 장치에 대한 요구 사항을 충족하기에 충분합니다. 점점 더 많은 최신 엔드포인트 장치가 듀얼 스택 및 또는 단일 IPv6 스택을 지원함에 따라 어떤 조직이라도 IPv6를 도입할 준비가 되어 있어야 합니다. 즉, 전체 인프라가 IPv6를 도입할 준비가 되어 있어야 합니다. Cisco SD-Access는 기존의 캠퍼스 설계에서 조직의 목적을 직접 구현하는 네트워크로 발전하는 것입니다. 이제 Cisco Software Defined Networks에서 듀얼 스택(IPv6 디바이스)을 온보딩할 수 있습니다.

IPV6를 채택하는 모든 조직의 주요 과제는 레거시 IPv4 시스템을 IPv6로 마이그레이션하는 것과 관

련된 변경 관리 및 복잡성입니다. 이 문서에서는 Cisco SDN에 대한 IPv6 기능 지원에 대한 모든 세부 사항, 전략 및 Cisco Software Defined Networks를 사용하여 IPv6를 채택할 때 주의해야 하는 중요 포인트 지점을 다룹니다.

2019년 8월에는 IPv6를 지원하는 Cisco DNA(Digital Network Architecture) Center 버전 1.3이 처음 도입되었습니다. 이 릴리스에서는 Cisco SD-Access 캠퍼스 네트워크가 오버레이 패브릭 네트워크의 IPv4, IPv6 또는 IPv4v6 듀얼 스택에서 유선 및 무선 클라이언트와 함께 호스트 IP 주소를 지원했습니다. 이 솔루션은 모든 기업에서 IPv6를 손쉽게 온보딩할 수 있는 새로운 기능을 제공할 수 있도록 지속적으로 발전하는 것입니다.

IPv6 아키텍처를 사용하는 Cisco SD-Access

SD-Access의 필수 구성 요소인 패브릭 기술은 프로그래밍 가능한 오버레이와 구축하기 쉬운 네트워크 가상화를 통해 유선 및 무선 캠퍼스 네트워크를 제공하며, 이 기술은 물리적 네트워크가 하나 이상의 논리적 네트워크를 호스팅할 수 있도록 하여 설계 의도를 충족시킵니다. 네트워크 가상화 외에도, 캠퍼스 네트워크의 패브릭 기술은 사용자 ID 및 그룹 멤버십을 기반으로 소프트웨어 정의 세그멘테이션 및 정책 시행을 제공하는 통신 제어 기능을 향상시킵니다. 전체 Cisco SDN 솔루션은 패브릭의 DNA에서 실행됩니다. 따라서 IPv6 지원과 관련하여 솔루션의 각 요소를 이해하는 것이 중요합니다.

- 언더레이 - IPv6 오버레이가 IPv4 언더레이 IP 주소 지정을 사용하여 LISP(Locator/ID Separation Protocol) 컨트롤 플레인 및 VXLAN(Virtual Extensible LAN) 데이터 플레인 터널을 생성하기 때문에 오버레이에 대한 IPv6 기능은 언더레이에 종속됩니다. SD-Access 오버레이 LISP만 IPv4 라우팅에 따라 달라지므로, 언더레이 라우팅 프로토콜을 위해 항상 듀얼 스택을 활성화할 수 있습니다.
- 오버레이 - 오버레이와 관련하여 SD-Access는 IPv6 전용 유선 및 무선 엔드포인트를 모두 지원합니다. 해당 IPv6 트래픽은 패브릭 보더 노드에 도달할 때까지 SD-Access 패브릭 내의 IPv4 및 VXLAN 헤더에서 캡슐화됩니다. 패브릭 보더 노드는 IPv4 및 VXLAN 헤더의 캡슐화를 해제합니다. 이 헤더는 그때부터 정상적인 IPv6 유니캐스트 라우팅 프로세스를 추구합니다.
- Control Plane Nodes(컨트롤 플레인 노드) - 컨트롤 플레인 노드는 서브넷 범위 내의 모든 IPv6 호스트 서브넷 및 /128 호스트 경로를 매핑 데이터베이스에 등록할 수 있도록 구성됩니다.
- Border nodes(경계 노드) - 경계 노드에서 Fusion 디바이스와의 IPv6 BGP 피어링이 활성화됩니다. 보더 노드는 패브릭 이그레스 트래픽에서 IPv4 헤더를 역캡슐화하는 반면 인그레스 IPv6 트래픽은 보더 노드에 의해 IPv4 헤더로 캡슐화됩니다.
- Fabric Edge - Fabric Edge에 구성된 모든 SVI(Switched Virtual Interface)는 IPv6여야 합니다. 이 구성은 DNA Center Controller에서 푸시됩니다.
- Cisco DNA Center - Cisco DNA Center 물리적 인터페이스는 이 문서를 게시할 당시만 해도 듀얼 스택을 지원하지 않습니다. IPv4 또는 IPv6가 있는 단일 스택에서만 DNA 센터의 관리 및/또는 엔터프라이즈 인터페이스에서만 구축할 수 있습니다.
- 클라이언트 - Cisco SD-Access는 이중 스택(IPv4 및 IPv6) 또는 단일 스택(IPv4 또는 IPv6)을 지원합니다. 그러나 IPv6 단일 스택이 구축된 경우에도 DNA Center는 IPv6 전용 클라이언트를 지원하기 위해 이중 스택 풀을 생성해야 합니다. 클라이언트가 IPv4 주소를 비활성화할 것으로 예상되는 IPv6에서만 듀얼 스택 풀의 IPv4는 더미 주소입니다.

Cisco Software-Defined Access의 IPv6 오버레이 아키텍처

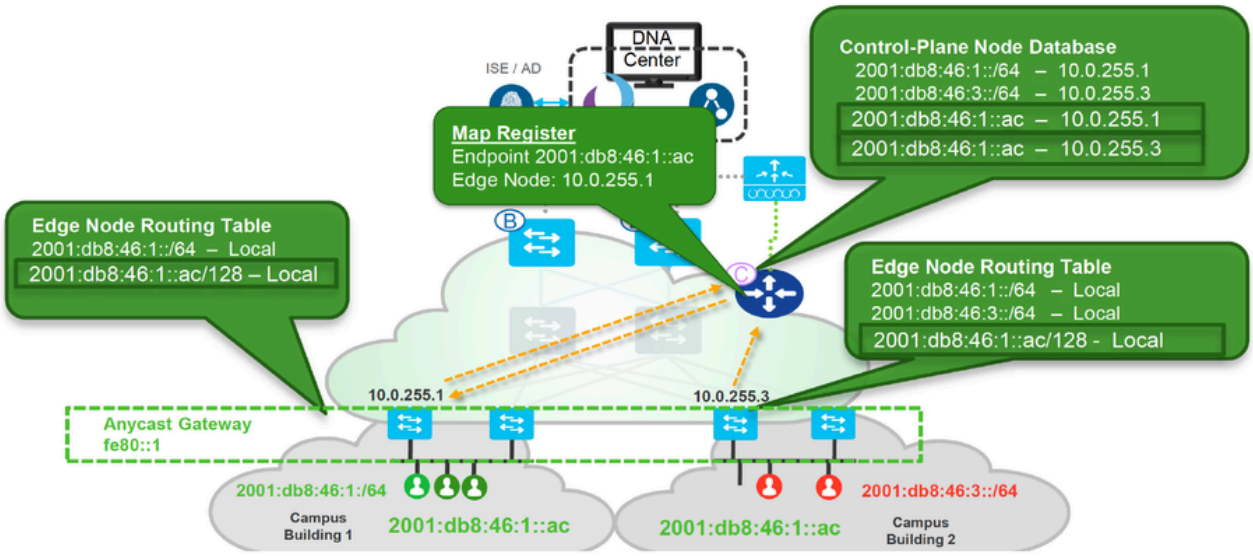


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

IPv6 오버레이 아키텍처

Cisco DNA-Center로 IPv6 활성화

Cisco DNA Center에서 IPv6 풀을 활성화하는 방법에는 두 가지가 있습니다.
1. 새 듀얼 스택 IPv4/v6 풀 생성 - 진출 가능 영역
2. 이미 있는 IPv4 풀에서 IPv6를 편집합니다. 브라운필드 마이그레이션

DNA Center의 현재 릴리스(최대 2.3.x)는 IPv6를 지원하지 않습니다. 단일/네이티브 IPv6 주소 전용 클라이언트를 지원하려는 경우 풀만 지원합니다. 더미 IPv4 주소는 IPv6 풀과 연결해야 합니다. 연결된 사이트와 함께 이미 존재하는 구축된 IPv4 풀에서 IPv6 주소로 풀을 수정합니다. DNA Center는 SD-Access Fabric에 대한 마이그레이션 옵션을 제공하므로 사용자가 해당 사이트에 대한 패브릭을 다시 프로비저닝해야 합니다. 사이트가 속한 Fabric에 경고 표시기가 표시되고 Fabric에 'fabric 재구성'이 필요함을 나타냅니다. 샘플은 다음 이미지를 참조하십시오.

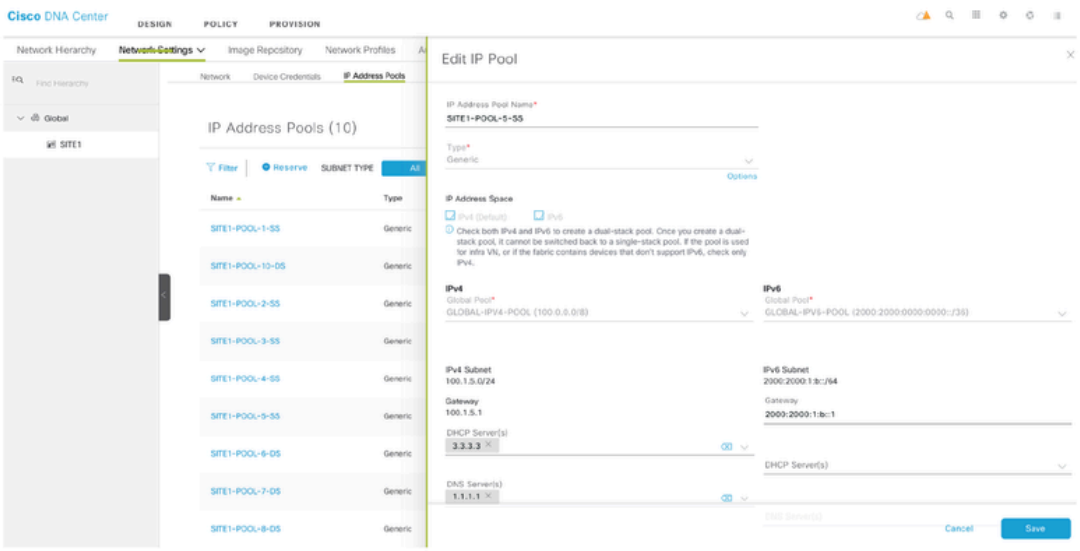


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

IPv4 풀 옵션을 편집하여 단일 IPv4 풀을 듀얼 스택 풀로 업그레이드

Pool upgrade: Warning on fabric page

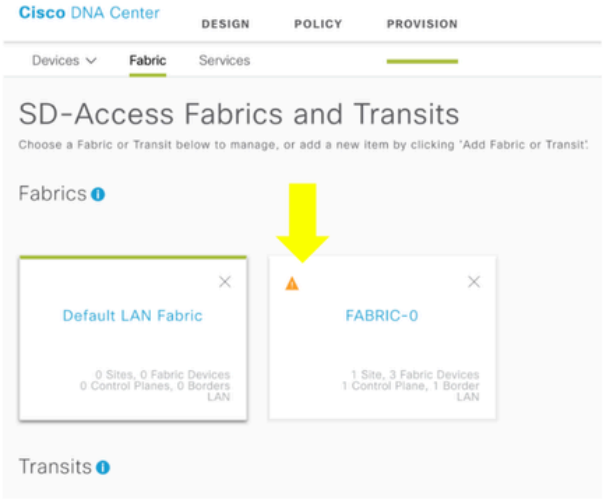


Figure 3.
Fabric has warning indicator which needs to 'reconfigure the fabric'

패브릭에 '패브릭을 다시 구성'해야 하는 경고 표시기가 있습니다.

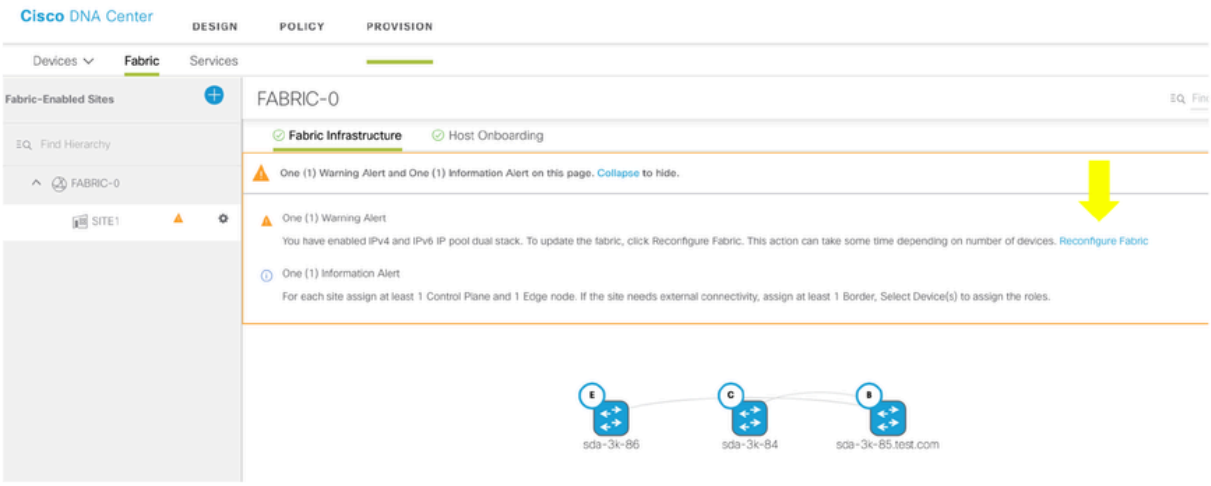


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

마이그레이션 프로세스의 일부로 듀얼 스택 컨피그레이션을 적용하려면 패브릭 노드를 자동으로 다시 프로비저닝하려면 '패브릭 재구성'을 클릭해야 합니다

Cisco SD-Access의 IPv6 설계 고려 사항

Cisco SD-Access 클라이언트의 경우 이중 스택 또는 IPv6 전용 네트워크 설정으로 실행할 수 있지만, 최대 2.3.x.x 버전의 DNA Center Switch(SW)를 사용하는 현재 SD-Access 패브릭 구현에서는 IPv6 구축에 대해 몇 가지 고려해야 할 사항이 있습니다.

- Cisco SD-Access는 IPv4 언더레이 라우팅 프로토콜을 지원합니다. 따라서 IPv6 클라이언트 트래픽은 IPv4 헤더 내에서 캡슐화될 때 전송됩니다. 이는 현재 LISP 소프트웨어 구축을 위한 요구 사항입니다. 그러나 언더레이가 IPv6 라우팅 프로토콜을 활성화할 수 없다는 의미는 아닙니다. SD-Access 오버레이 LISP만 그 종속에 따라 실행되지 않습니다.
- 현재 패브릭 언더레이는 IPv4만 될 수 있으므로 IPv6 네이티브 멀티캐스트는 지원되지 않습니다.
- 게스트 무선은 이중 스택에서만 실행할 수 있습니다. 현재 ISE(Identity Services Engine) 릴리스(예: 최대 3.2)로 인해 IPv6 게스트 포털이 지원되지 않으므로 IPv6 전용 게스트 클라이언트는 인증할 수 없습니다.
- IPv6 애플리케이션 QoS 정책 자동화는 현재 DNA Center 릴리스에서 지원되지 않습니다. 이 문서에서는 대규모 사용자 중 한 명을 위해 구축된 Cisco SD-Access에서 유선 및 무선 듀얼 스택 클라이언트에 IPv6 QoS를 구현하는 데 필요한 단계를 설명합니다.
- SSID(Service Set Identifier)별 또는 정책을 기반으로 하는 클라이언트별 다운스트림 및 업스트림 트래픽에 대한 무선 클라이언트 속도 제한 기능이 IPv4(TCP/UDP) 및 IPv6(TCP에만 해당)에 대해 지원됩니다. IPv6 UDP 속도 제한은 아직 지원되지 않습니다.
- IPv4 풀은 듀얼 스택 풀로 업그레이드할 수 있습니다. 그러나 듀얼 스택 풀은 IPv4 풀로 다운그레이드할 수 없습니다. 사용자가 듀얼 스택 풀을 IPv4 싱글 스택 풀로 다시 제거하려면 전체

듀얼 스택 풀을 해제해야 합니다.
- 현재 DNA Center에서는 IPv4 또는 듀얼 스택 풀만 생성할 수 있지만 단일 IPv6는 아직 지원되지 않습니다.
- Cisco IOS® XE의 플랫폼은 최소 소프트웨어 버전 요구 사항인 16.9.2 이상입니다.
- IPv6 게스트 무선은 Cisco IOS XE 플랫폼에서 아직 지원되지 않으며 AireOS(8.10.105.0+)는 해결 방법을 지원합니다.
- AP(Access Point) 또는 확장 노드 풀만 할당할 수 있는 INFRA_VN에서는 듀얼 스택 풀을 할당할 수 없습니다.
- LAN 자동화는 아직 IPv6를 지원하지 않습니다.

앞에서 언급한 제한 사항 외에 IPv6이 활성화된 SD-Access 패브릭을 설계할 때는 항상 각 패브릭 구성 요소의 확장성을 염두에 두어야 합니다. 엔드포인트에 여러 IPv4 또는 IPv6 주소가 있는 경우 각 주소는 개별 항목으로 계산됩니다.

패브릭 호스트 항목에는 액세스 포인트와 클래식 및 정책 확장 노드가 포함됩니다.

추가 보더 노드 크기 조정 고려 사항:

/32(IPv4) 또는 /128(IPv6) 항목은 보더 노드가 트래픽을 패브릭 외부에서 패브릭의 호스트로 전달할 때 사용됩니다.

Cisco Catalyst 9500 Series 고성능 스위치 및 Cisco Catalyst 9600 Series 스위치를 제외한 모든 스위치의 경우:

- IPv4는 모든 IPv4 IP 주소에 대해 하나의 TCAM(Ternary Content Addressable Memory) 항목(패브릭 호스트 항목)을 사용합니다.
- IPv6에서는 각 IPv6 IP 주소에 대해 두 개의 TCAM 항목(패브릭 호스트 항목)을 사용합니다.

Cisco Catalyst 9500 Series 고성능 스위치 및 Cisco Catalyst 9600 Series 스위치의 경우:

- IPv4는 각 IPv4 IP 주소에 대해 하나의 TCAM 항목(패브릭 호스트 항목)을 사용합니다.
- IPv6에서는 모든 IPv6 IP 주소에 대해 하나의 TCAM 항목(패브릭 호스트 항목)을 사용합니다.

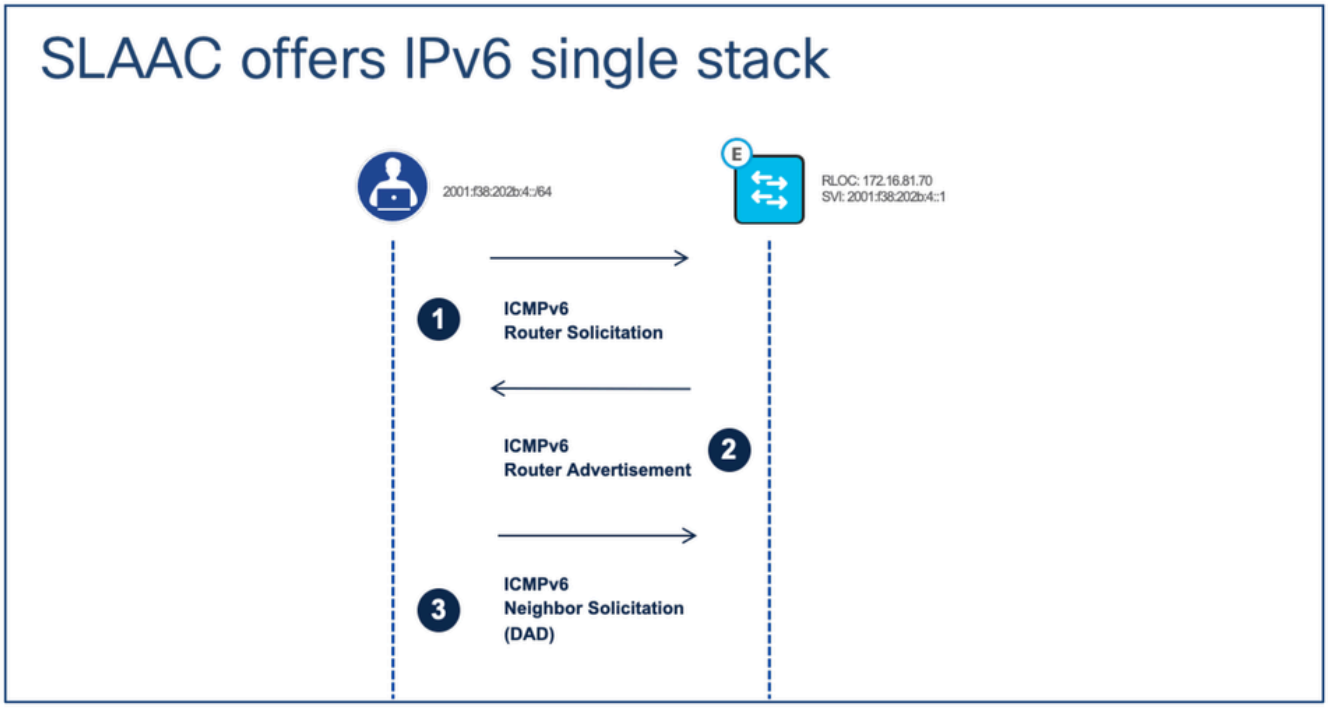
그리고 일부 엔드포인트는 IPv6 주소를 얻기 위해 SLAAC(Stateless Address Autoconfiguration)에 의존하는 Android OS 기반 스마트폰과 같은 DHCPv6를 지원하지 않습니다. 단일 엔드포인트는 2개 이상의 IPv6 주소로 끝날 수 있습니다. 이 동작은 각 패브릭 노드에서, 특히 패브릭 보더 및 제어 노드에서 더 많은 하드웨어 리소스를 소비합니다. 예를 들어, 경계 노드가 엔드포인트의 에지 노드로 트래픽을 전송하고자 할 때마다 TCAM 항목에 호스트 경로를 설치하고 하드웨어(HW) TCAM에서 VXLAN 인접성 항목을 구웁니다.

유무선 클라이언트 연결 및 통화 흐름

클라이언트가 패브릭 에지에 연결되면 IPv6 주소를 가져오는 다양한 방법이 있습니다. 이 섹션에서는 클라이언트 IPv6 주소 지정, 즉 SLAAC 및 DHCPv6에 대한 가장 일반적인 방법을 다룹니다.

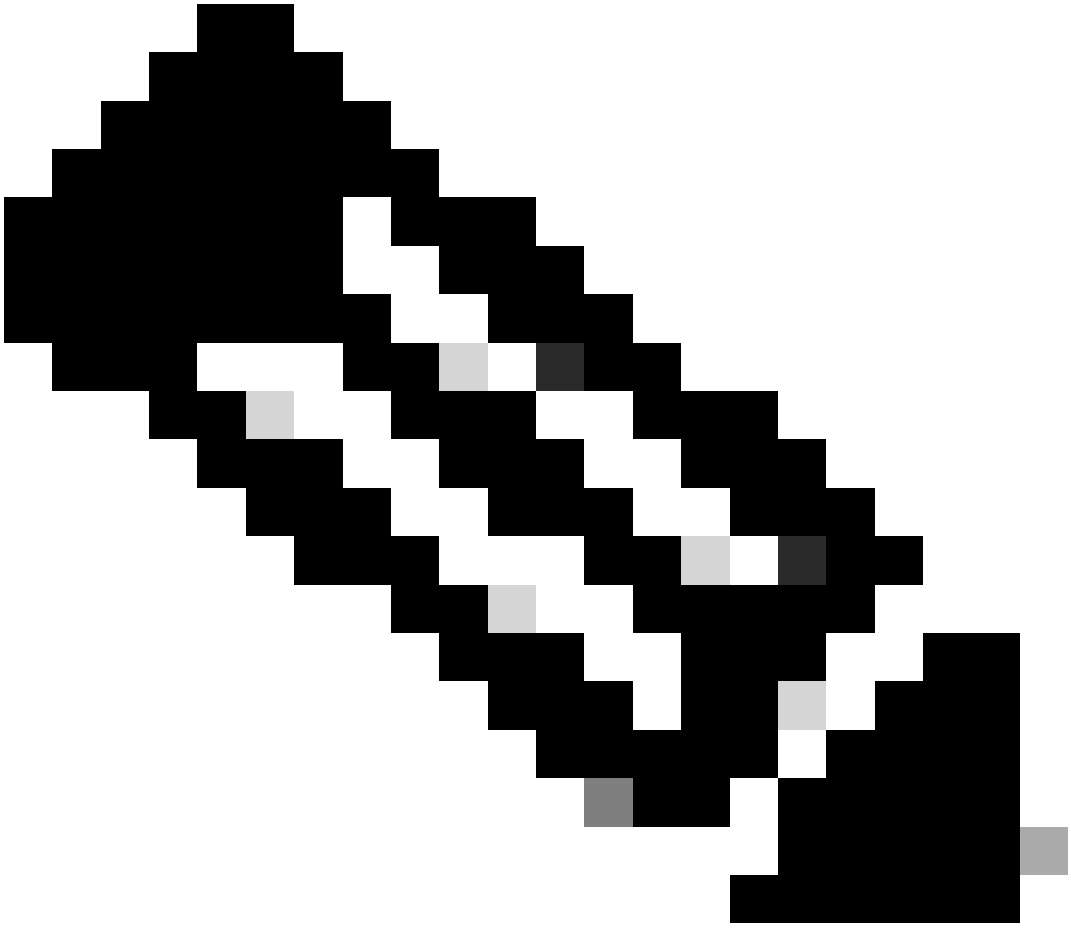
IPv6 주소 할당 - SLAC

SDA(Software-Defined Access)의 SLAAC는 표준 SLAAC 프로세스 흐름과 다르지 않습니다. SLAAC가 제대로 작동하려면 IPv6 클라이언트가 해당 인터페이스에서 링크-로컬 주소로 구성되어야 합니다. 클라이언트가 링크-로컬 주소로 자동으로 구성되는 방식은 이 문서의 범위를 벗어납니다.



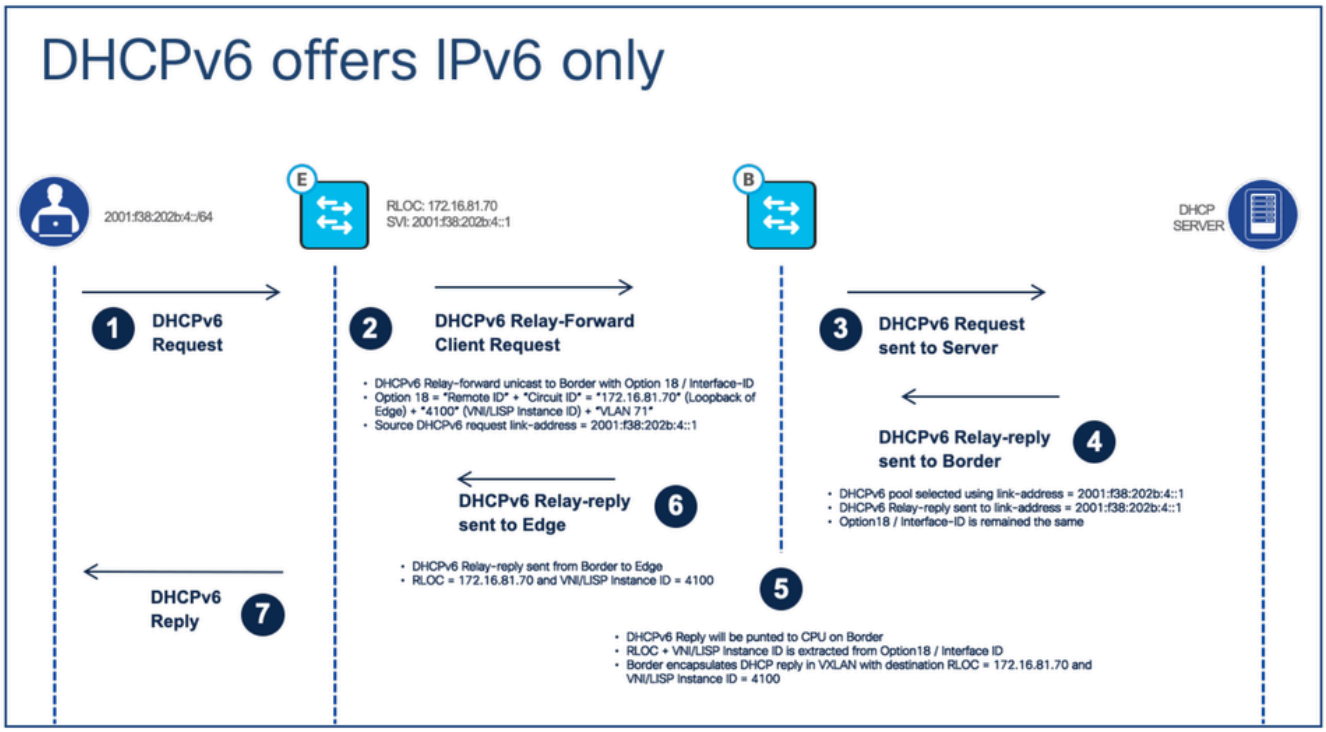
IPv6 주소 할당 - SLAC

통화 흐름 설명:
1단계. IPv6 클라이언트가 IPv6 링크-로컬 주소로 자신을 구성한 후 클라이언트는 ICMPv6 RS(Router Solicitation) 메시지를 Fabric Edge로 전송합니다. 이 메시지의 목적은 연결된 세그먼트의 전역 유니캐스트 접두사를 얻기 위한 것입니다.
2단계. 패브릭 에지가 RS 메시지를 수신하면 전역 IPv6 유니캐스트 접두사 및 그 길이를 포함하는 ICMPv6 RA(라우터 알림) 메시지로 응답합니다.
3단계. 클라이언트가 RA 메시지를 수신하면 고유한 IPv6 글로벌 유니캐스트 주소를 생성하고 클라이언트의 세그먼트와 관련된 패브릭 에지의 SVI의 링크-로컬 주소에 게이트웨이를 설정하기 위해 IPv6 글로벌 유니캐스트 접두사와 EUI-64 인터페이스 식별자를 결합합니다. 그런 다음 클라이언트는 IPv6 주소가 고유한지 확인하기 위해 DAD(Duplicate Address Detection)를 수행하기 위해 ICMPv6 Neighbor Solicitation 메시지를 전송합니다.



참고: 모든 SLAAC 관련 메시지는 클라이언트 및 패브릭 노드의 SVI IPv6 링크-로컬 주소로 캡슐화됩니다.

IPv6 주소 할당 - DHCPv6



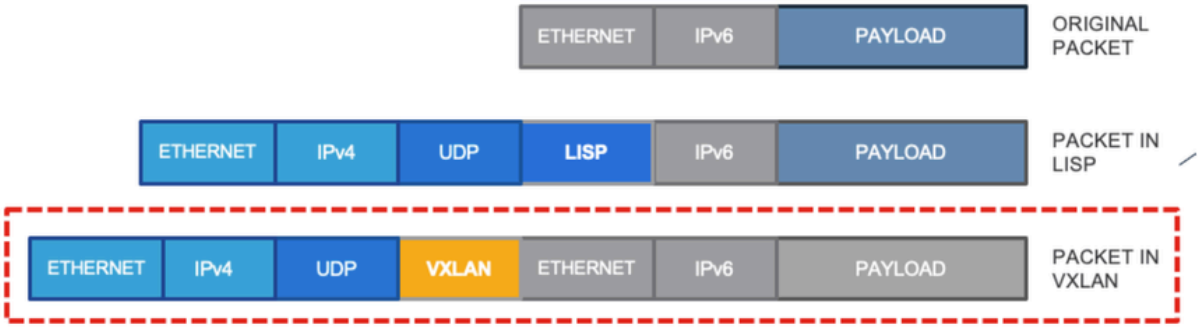
IPv6 주소 할당 - DHCPv6

통화 흐름 설명:
1단계. 클라이언트가 패브릭 에지에 DHCPv6 요청을 보냅니다.
2단계. 패브릭 에지가 DHCPv6 요청을 수신하면 DHCPv6 릴레이 포워드 메시지를 사용하여 요청을 패브릭 경계에 DHCPv6 옵션 18로 유니캐스트합니다. DHCP 옵션 82와 비교하여 DHCPv6 옵션 18은 'Circuit ID'와 'Remote ID'를 모두 인코딩합니다. LISP 인스턴스 ID/VNI, IPv4 RLOC(Routing Locator) 및 엔드포인트 VLAN이 내부에서 인코딩됩니다.
3단계. 패브릭 경계는 VXLAN 헤더를 역캡슐화하고 DHCPv6 패킷을 DHCPv6 서버로 유니캐스트합니다.
4단계. DHCPv6 서버가 릴레이 전달 메시지를 수신하면 메시지의 소스 링크 주소(DHCPv6 릴레이 에이전트/클라이언트 게이트웨이)를 사용하여 IPv6 주소를 할당하기 위해 IPv6 IP 풀을 선택합니다. 그런 다음 DHCPv6 릴레이 응답 메시지를 클라이언트 게이트웨이 주소로 다시 보냅니다. 옵션 18은 변경되지 않습니다.
5단계. 패브릭 경계가 릴레이 응답 메시지를 수신하면 옵션 18에서 RLOC 및 LISP 인스턴스/VNI를 추출합니다. 패브릭 경계는 옵션 18에서 추출한 대상을 사용하여 VXLAN에서 릴레이 응답 메시지를 캡슐화합니다.
6단계. 패브릭 경계는 클라이언트가 연결하는 패브릭 에지에 DHCPv6 릴레이 응답 메시지를 전송합니다.
7단계. 패브릭 에지가 DHCPv6 릴레이 응답 메시지를 수신하면 메시지의 VXLAN 헤더를 역캡슐화하고 메시지를 클라이언트에 전달합니다. 그러면 클라이언트는 할당된 IPv6 주소를 알고 있습니다.

Cisco SD-Access의 IPv6 통신

IPv6 통신에서는 표준 LISP 기반 컨트롤 플레인 및 VXLAN 기반 데이터 플레인 통신 방법을 사용합니다. Cisco SD-Access LISP 및 VXLAN의 현재 구현에서는 외부 IPv4 헤더를 사용하여 IPv6 패킷

을 내부로 전달합니다. 이 이미지는 이 프로세스를 캡처합니다.



내부에 IPv6 패킷을 전달하는 외부 IPv4 헤더

즉, 모든 LISP 쿼리는 IPv4 네이티브 패킷을 사용하는 반면, 컨트롤 플레인 노드 테이블에는 엔드포인트의 IPv6 및 IPv4 IP 주소가 모두 있는 RLOC에 대한 세부 정보가 포함됩니다. 이 프로세스는 무선 엔드포인트 관점에서 다음 섹션에서 자세히 설명합니다.

Cisco SD-Access의 무선 IPv6 통신

무선 통신은 일반적인 Cisco SD-Access Fabric 구성 요소와 별도로 두 개의 특정 구성 요소 액세스 포인트 및 무선 LAN 컨트롤러를 사용합니다. 무선 액세스 포인트는 WLC(Wireless LAN Controller)를 사용하여 CAPWAP(Control and Provisioning of Wireless Access Points) 터널을 생성합니다. 클라이언트 트래픽이 패브릭 에지에 있는 동안 무선 통계를 포함하는 다른 컨트롤 플레인 통신은 WLC에서 관리합니다. IPv6 관점에서 WLC와 AP에 모두 IPv4 주소가 있어야 하며 모든 CAPWAP 통신에서 이러한 IPv4 주소를 사용합니다. Non-Fabric WLC 및 AP는 IPv6 통신을 지원하지만, Cisco SD-Access는 IPv4 패킷 내에서 클라이언트 IPv6 트래픽을 전달하는 모든 통신에 IPv4를 사용합니다. 즉, Infra VN에서 할당된 AP 풀을 듀얼 스택인 IP 풀로 매핑할 수 없으며, 이 매핑을 시도하면 오류가 발생합니다. Cisco SDA 내의 무선 통신은 다음과 같은 주요 작업으로 나눌 수 있습니다.

- 액세스 포인트 온보딩
- 클라이언트 온보딩

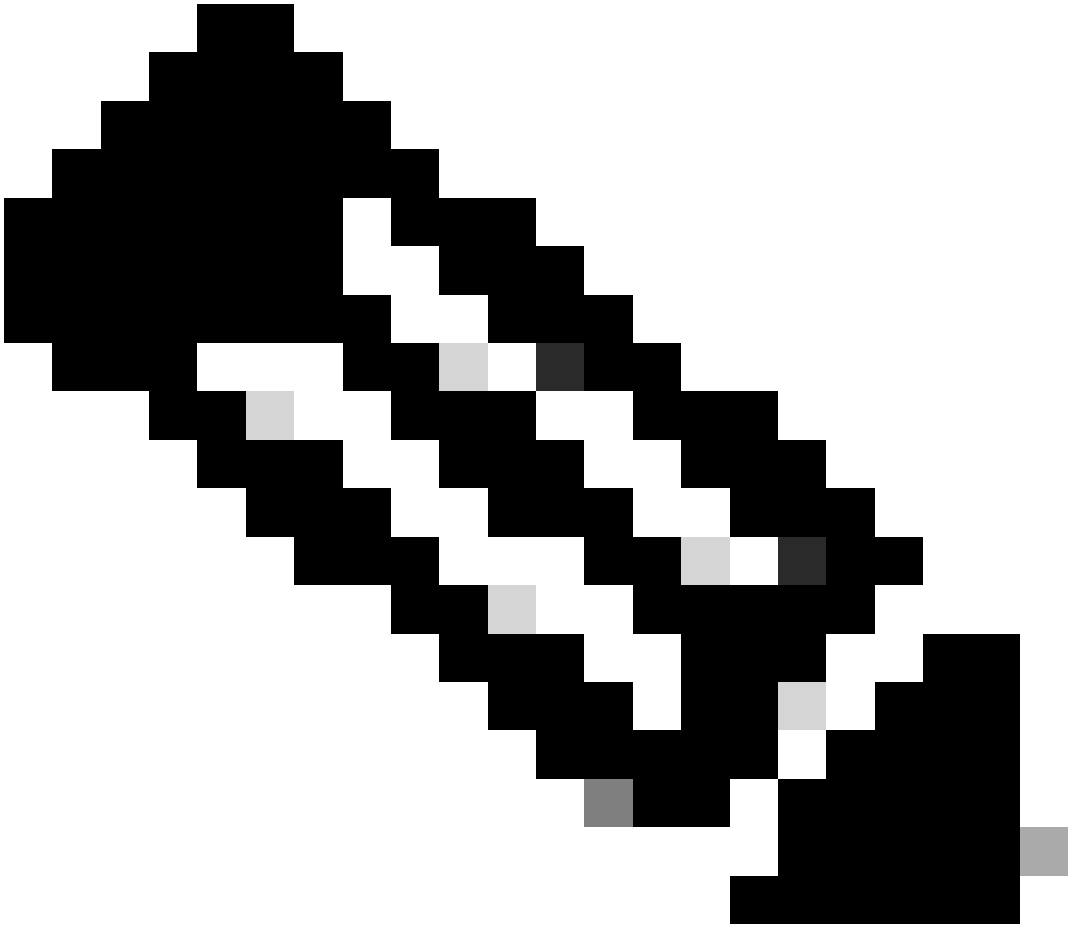
IPv6 관점에서 이러한 이벤트를 살펴보십시오.

액세스 포인트 온보딩

이 프로세스는 WLC와 AP가 모두 IPv4 주소와 여기에 포함된 단계를 포함하므로 IPv6 및 IPv4에 대해서도 동일하게 유지됩니다.
1. FE(Fabric Edge) 포트가 AP를 온보딩하도록 구성되었습니다.
2. AP가 FE 포트에 연결하고 CDP AP를 통해 FE에 해당 프레즌스에 대해 알립니다(이를 통해 FE가 올바른 VLAN을 할당할 수 있음).
3. AP가 DHCP 서버에서 IPv4 주소를 가져오고 FE가 AP를 등록하고 AP 세부사항과 함께 Control Plane(CP) 노드를 업데이트합니다.

4. AP가 기존 방법(예: DHCP 옵션 43)을 통해 WLC에 조인합니다.
5. WLC는 AP가 패브릭을 사용할 수 있는지 확인하고 컨트롤 플레인에 AP RLOC 정보(예: RLOC 요청/응답 수신)를 쿼리합니다.
6. CP가 AP의 RLOC IP로 WLC에 회신합니다.
7. WLC는 CP에 AP MAC(Media Access Control)을 등록합니다.
8. CP는 WLC에서 AP에 대한 세부 정보로 FE를 업데이트합니다(FE가 AP와 함께 VXLAN 터널을 시작하도록 함).

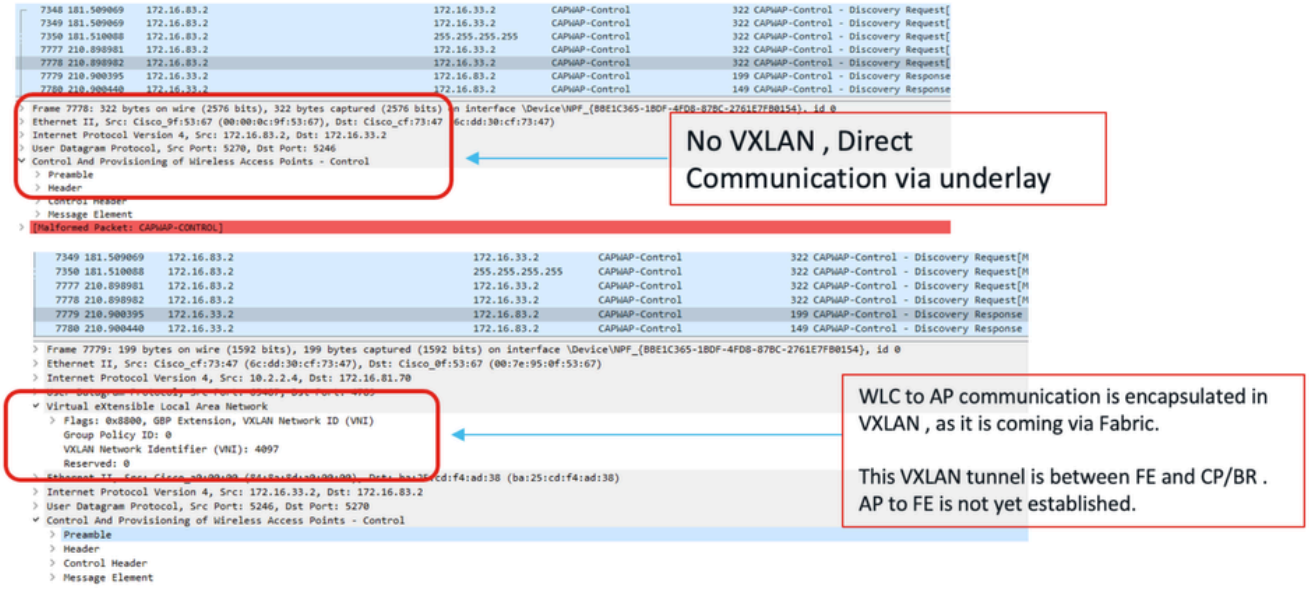
FE는 정보를 처리하고 AP를 사용하여 VXLAN 터널을 생성합니다. 이때 AP는 패브릭 지원 SSID를 광고합니다.



참고: AP가 비 패브릭 SSID를 브로드캐스트하고 패브릭 SSID를 브로드캐스트하지 않는 경우, 액세스 포인트와 패브릭 에지 노드 간의 VXLAN 터널을 확인합니다.

또한 AP-WLC 통신은 항상 언더레이 CAPWAP를 통해 발생하며 모든 WLC-AP 통신은 오버레이를 통해 VXLAN CAPWAP를 사용합니다. 즉, AP에서 WLC로 이동하는 패킷을 캡처할 경우 역방향 트래픽에 VXLAN 터널이 있는 동안에만 CAPWAP가 표시됩니다. AP와 WLC 간의 통신에 대해서는

이 예를 참조하십시오.



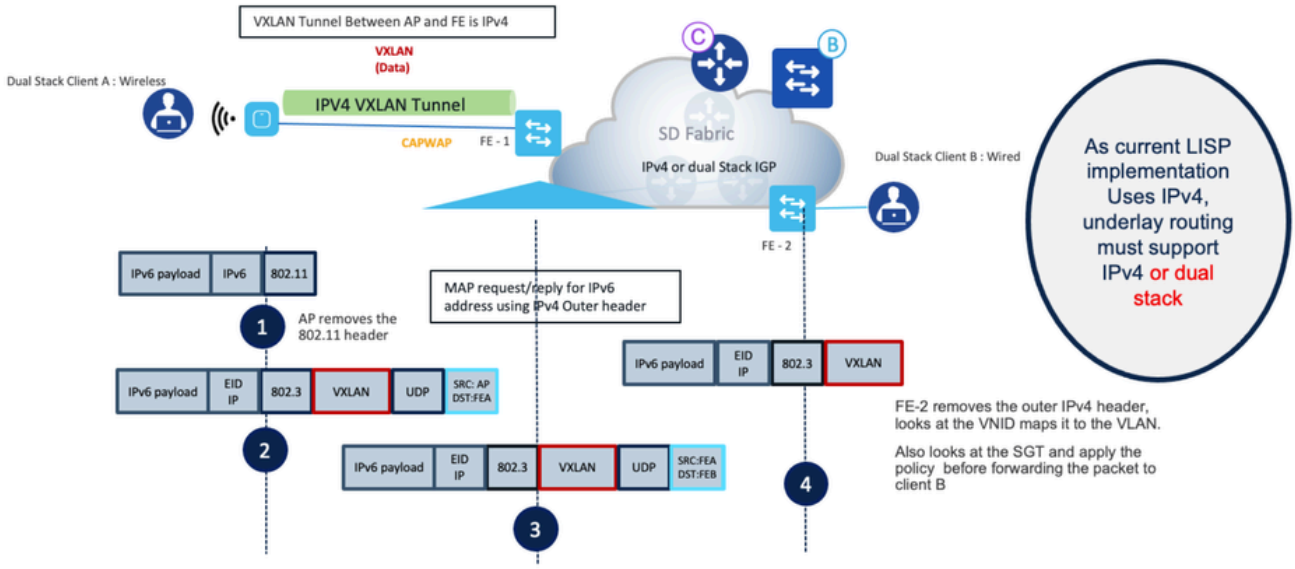
AP에서 WLC로 패킷 캡처(CAPWAP 터널) 대 WLC에서 AP로 패킷 캡처(패브릭의 VxLAN 터널)

클라이언트 등록

듀얼 스택/IPv6 클라이언트 온보딩 프로세스는 동일하게 유지되지만 클라이언트는 IPv6 주소를 가져오기 위해 SLAAC/DHCPv6와 같은 IPv6 주소 할당 방법을 사용합니다.
1. 클라이언트가 패브릭에 가입하고 AP에서 SSID를 활성화합니다.
2. WLC는 AP RLOC를 알고 있습니다.
3. 클라이언트가 인증하고 WLC가 클라이언트 L2 세부 정보를 CP에 등록하고 AP를 업데이트합니다.
4. 클라이언트는 구성된 메서드(SLAAC/DHCPv6)에서 IPv6 주소 지정을 시작합니다.
5. FE는 CP HTDB(호스트 추적 데이터베이스)에 대한 IPv6 클라이언트 등록을 트리거합니다. AP에서 FE로, 다른 대상으로 FE에서 IPv4 프레임 내에서 VXLAN 및 LISP IPv6 캡슐화를 사용합니다.

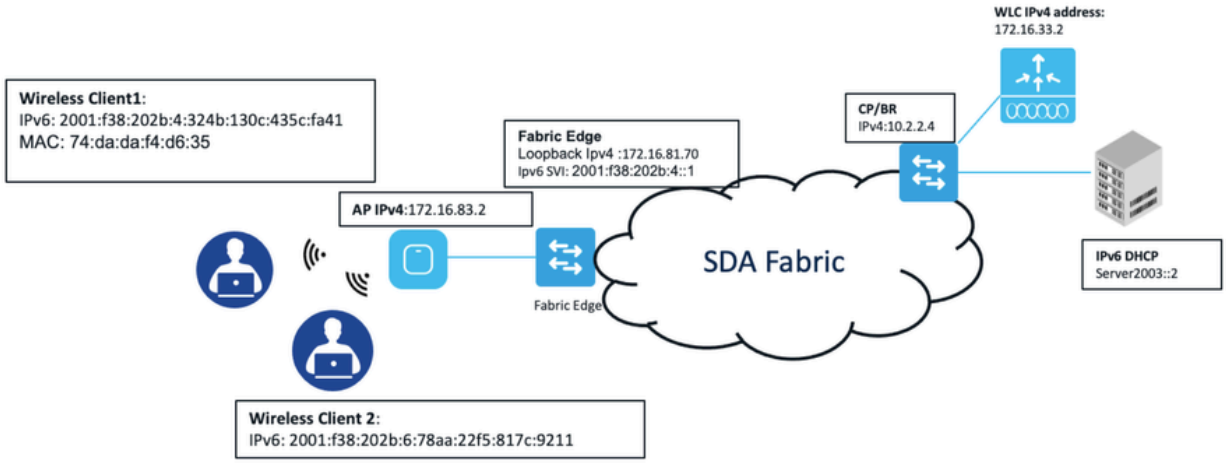
IPv6와의 클라이언트-클라이언트 통신

이 그림에는 다른 IPv6 유선 클라이언트와의 IPv6 무선 클라이언트 통신 프로세스가 요약되어 있습니다. (이는 클라이언트가 인증되었고 구성된 방법을 통해 IPv6 주소를 얻었다고 가정합니다.)
1. 클라이언트가 IPv6 페이로드와 함께 802.11 프레임을 AP에 전송합니다.
2. AP가 802.11 헤더를 제거하고 IPv4 VXAN 터널의 원래 IPv6 페이로드를 패브릭 엣지로 전송합니다.
3. 패브릭 에지는 MAP(Message Access Protocol) 요청을 사용하여 대상을 식별하고 프레임을 IPv4 VXLAN을 통해 대상 RLOC에 전송합니다.
4. 대상 스위치에서 IPv4 VXLAN 헤더가 제거되고 IPv6 패킷이 클라이언트로 전송됩니다.

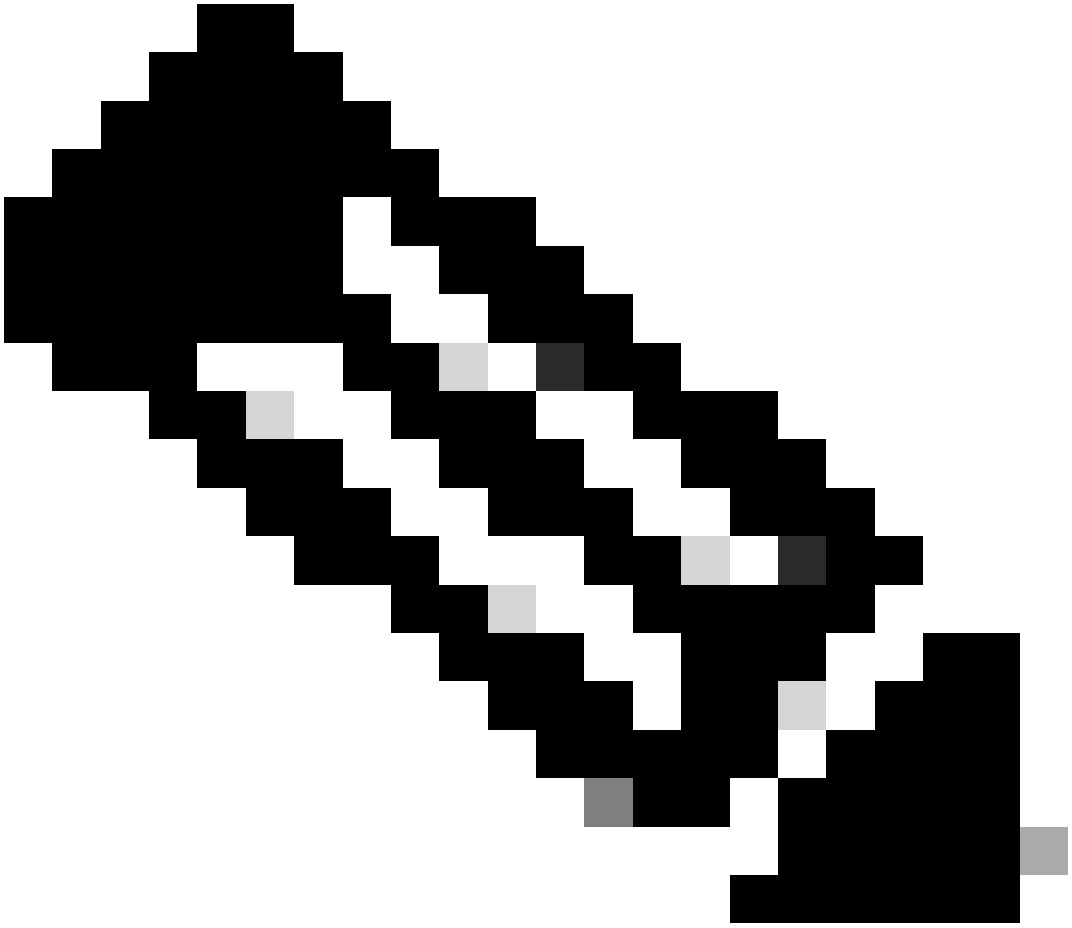


듀얼 스택 무선 클라이언트에서 듀얼 스택 유선 클라이언트 패킷 흐름

패킷 캡처를 통해 이 프로세스를 자세히 살펴보고 IP 주소 및 MAC 주소 세부 정보를 보려면 이미지를 참조하십시오. 이 설정에서는 동일한 액세스 포인트에 연결되었지만 서로 다른 IPv6 서브넷(SSID)으로 매핑된 듀얼 스택 클라이언트를 모두 사용합니다.

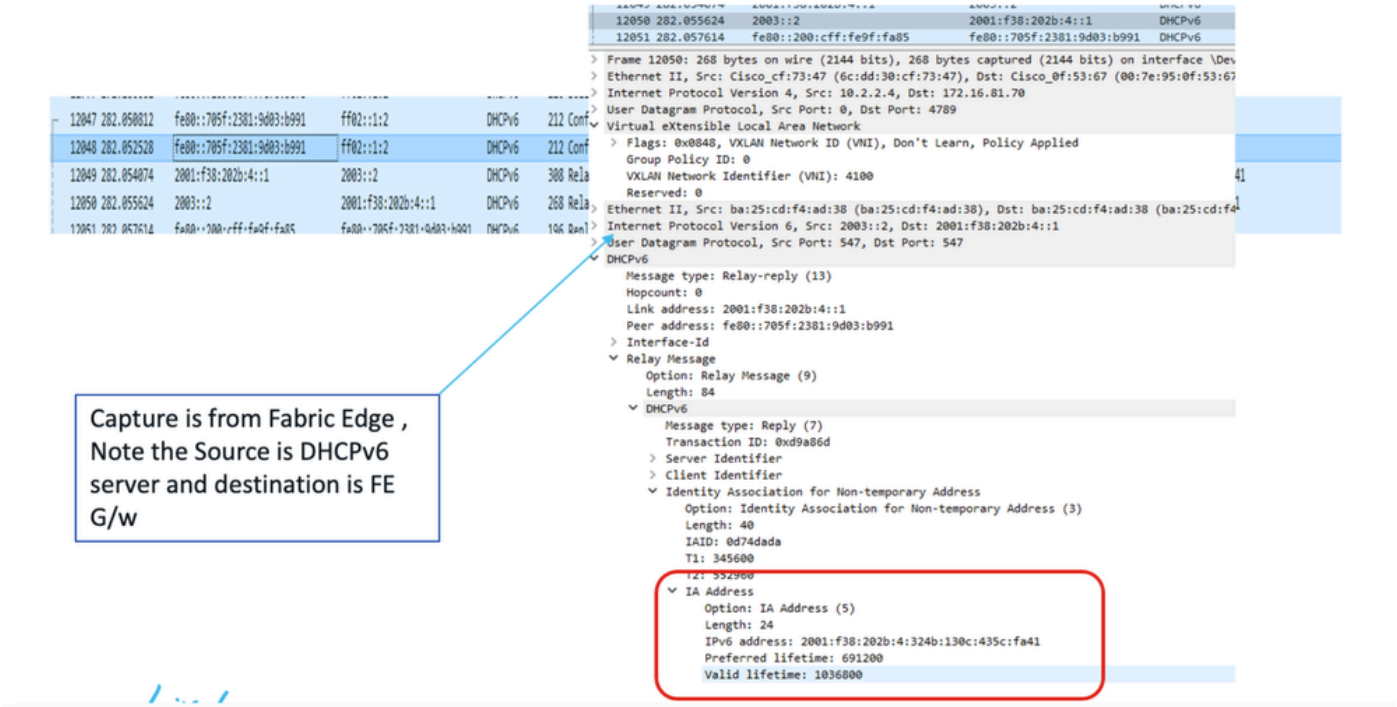


샘플 SD 액세스 패브릭 네트워크 IP 주소 및 MAC 주소 세부사항



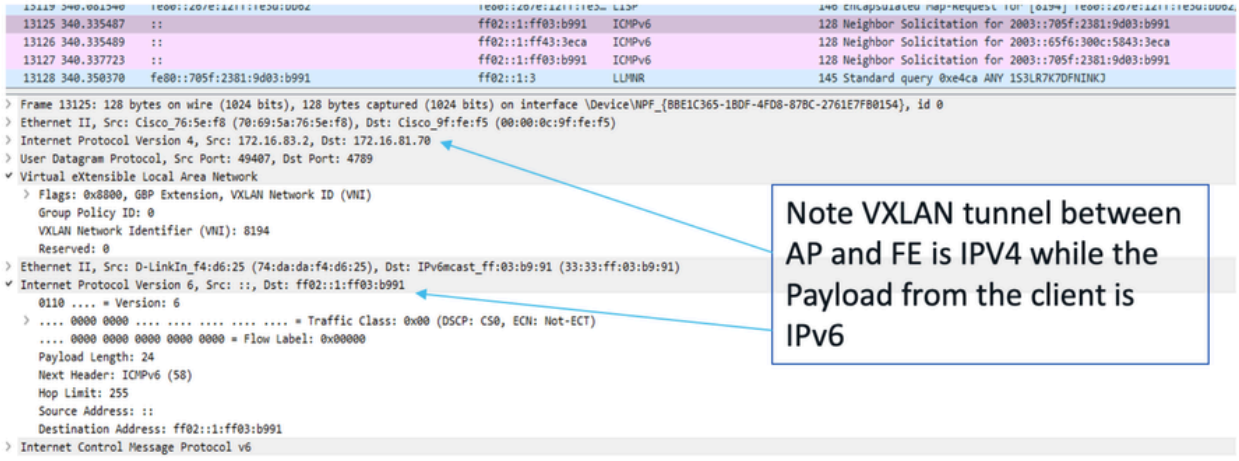
참고: DHCP/DNS와 같이 패브릭 외부의 모든 IPv6 통신의 경우, IPv6 라우팅은 보더리와 패브릭이 아닌 인프라 사이에서 활성화되어야 합니다.

1단계. 클라이언트는 구성된 메서드에서 IPv6 주소를 인증하고 가져옵니다.



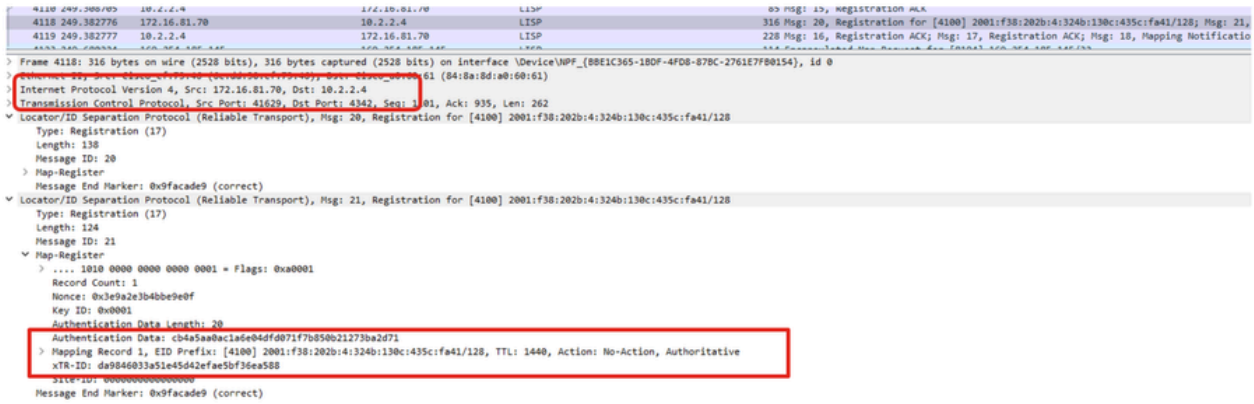
DHCPv6 서버에서 패브릭 에지 노드로의 패킷 캡처

2단계. 무선 클라이언트가 IPv6 페이로드와 함께 802.11 프레임을 액세스 포인트에 전송합니다.
3단계. 액세스 포인트가 무선 헤더를 제거하고 패킷을 패브릭 엣지로 전송합니다. 액세스 포인트에 IPv4 주소가 있으므로 IPv4 기반의 VXLAN 터널 헤더가 사용됩니다.



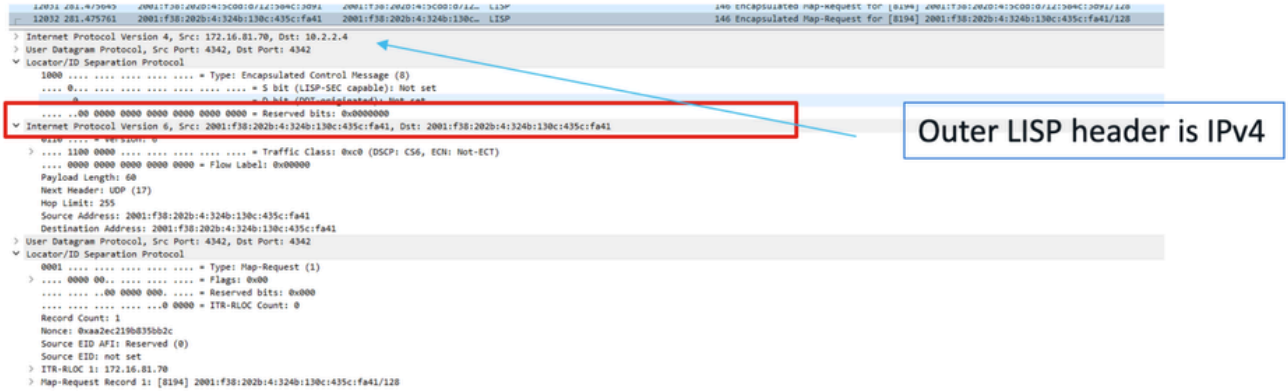
FE와 AP 간 VxLAN 터널의 패킷 캡처

3.1단계. Fabric Edge는 IPv6 클라이언트를 컨트롤 플레인에 등록합니다. IPv6 클라이언트 세부사항이 포함된 IPv4 등록 방법을 사용합니다.



IPv6 클라이언트용 컨트롤 플레인에 FE용 패킷 캡처 등록

3.2단계. FE는 대상 RLOC를 식별하기 위해 MAP 요청을 제어 플레인으로 전송합니다.



MAP 등록 메시지를 사용하여 FE에서 CP로 패킷 캡처

또한 패브릭 에지는 이 이미지에 표시된 대로 알려진 IPv6 클라이언트에 대한 MAP 캐시를 유지 관리합니다.

```
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#
```

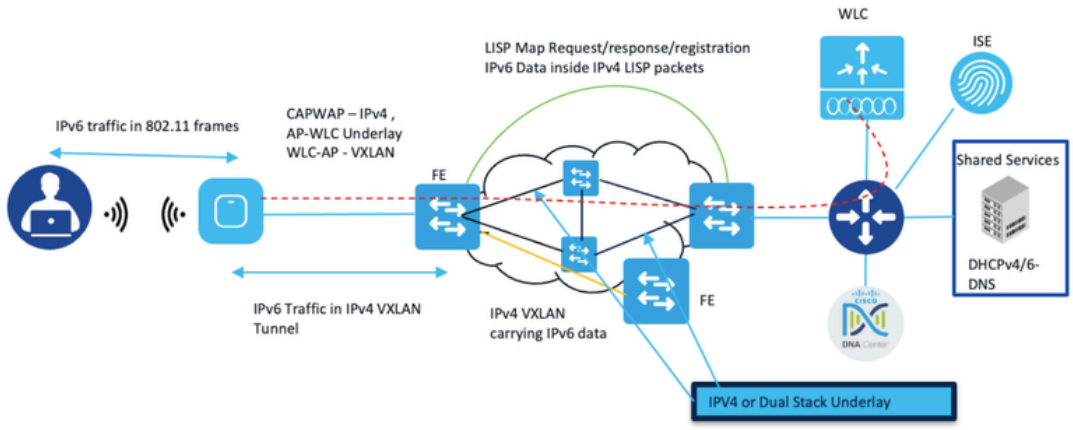
IPv6 오버레이 맵 캐시 정보의 패브릭 에지 화면 출력

4단계. 패킷은 원래 IPv6 페이로드를 내부에 전달하는 IPv4 VXLAN을 사용하여 대상 RLOC로 전달됩니다. 두 클라이언트가 동일한 AP에 연결되어 있으므로 IPv6 ping이 이 경로를 사용합니다.

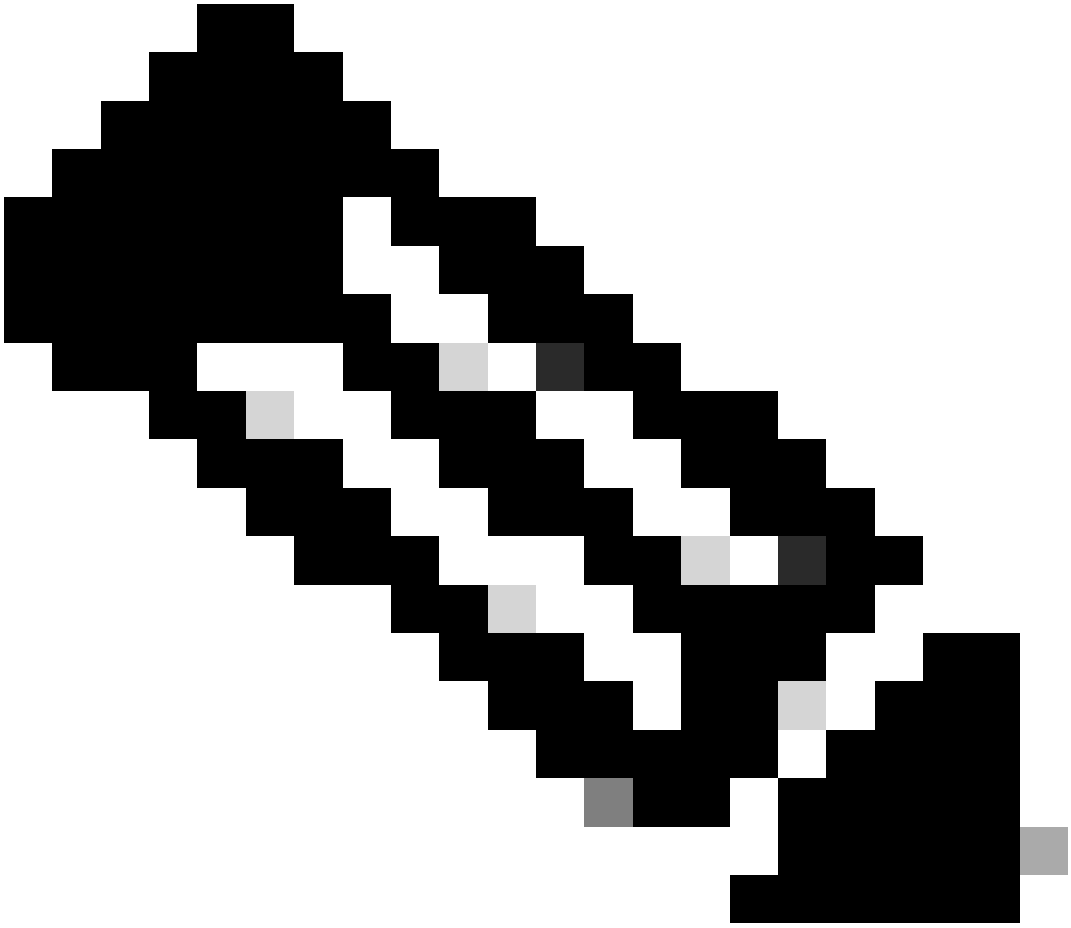
```
    71 3.392805     2001:f38:202b:4:324b:130c:435c:fa41   2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001, seq=148, hop limit=63
    72 3.392836     2001:f38:202b:4:324b:130c:435c:fa41   2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001, seq=148, hop limit=64
    73 3.398939     2001:f38:202b:6:78aa:22f5:817c:9211   2001:f38:202b:4:324b:130c:435c:fa41 ICMPv6      144 Echo (ping) reply id=0x0001, seq=148, hop limit=64 (
    74 3.398941     2001:f38:202b:6:78aa:22f5:817c:9211   2001:f38:202b:4:324b:130c:435c:fa41 ICMPv6      144 Echo (ping) reply id=0x0001, seq=148, hop limit=63
> Frame 72: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface \Device\NPF_{BBE1C365-1BDF-4FD8-87BC-2761E7FB0154}, id 0
> Ethernet II, Src: Cisco_76:5e:f8 (70:69:5a:76:5e:f8), Dst: Cisco_9f:fe:f5 (00:00:0c:9f:fe:f5)
> Internet Protocol Version 4, Src: 172.16.83.2, Dst: 172.16.81.70
> User Datagram Protocol, Src Port: 49407, Dst Port: 4789
v Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 8194
    Reserved: 0
> Ethernet II, Src: D-LinkIn_f4:d6:25 (74:da:da:f4:d6:25), Dst: Cisco_9f:fa:85 (00:00:0c:9f:fa:85)
> Internet Protocol Version 6, Src: 2001:f38:202b:4:324b:130c:435c:fa41, Dst: 2001:f38:202b:6:78aa:22f5:817c:9211
v Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x036f [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 148
    [Response In: 73]
  > Data (32 bytes)
```

동일한 AP에 등록된 두 무선 클라이언트 간의 IPv6 ping을 위한 패킷 캡처

이 그림에는 무선 클라이언트 관점에서 IPv6 통신이 요약되어 있습니다.



이 그림에는 무선 클라이언트 관점에서 IPv6 통신이 요약되어 있습니다



참고: ISE의 제한으로 인해 Cisco Identity Services를 통한 IPv6 게스트 액세스(웹 포털)가 지원되지 않습니다.

종속성 매트릭스

Cisco SD-Access의 일부인 서로 다른 무선 구성 요소에서 IPv6를 지원한다는 점과 종속성을 확인하는 것이 중요합니다. 이 그림의 표에는 이 기능 매트릭스가 요약되어 있습니다.

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

릴리스별 Cat9800 WLC IPv6 기능

IPv6에 대한 컨트롤 플레인 모니터링

IPv6을 활성화하면 맵 서버(MS)/맵 확인자(MR) 서버에서 호스트 IPv6에 대한 추가 항목이 표시됩니다. 호스트에 여러 IPv6 IP 주소가 있을 수 있으므로 MS/MR 조회 테이블에는 모든 IP 주소에 대한 항목이 있습니다. 이는 이미 존재하는 IPv4 테이블과 결합됩니다.
모든 항목을 확인하려면 디바이스 CLI에 로그인하고 이 명령을 실행해야 합니다.

```
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
```

보증을 통해 호스트 IPv6 세부사항에 대한 세부사항을 확인할 수도 있습니다.

Cisco SD-Access에서 IPv6 QoS 구현

현재 Cisco DNA Center 릴리스(최대 2.3.x)는 IPv6 QoS 애플리케이션 정책 자동화를 지원하지 않습니다. 그러나 사용자는 수동으로 IPv6 유선 및 무선 템플릿을 생성하고 QoS 템플릿을 패브릭 에지 노드에 푸시할 수 있습니다. DNA Center는 적용된 모든 물리적 인터페이스에서 IPv4 QoS 정책을 자동화하므로 템플릿을 통해 'class-default' 앞에 클래스 맵(IPv6 ACL(Access Control List)과 일치)을 수동으로 삽입할 수 있습니다.

다음은 DNA Center 생성 정책 컨피그레이션과 통합된 유선 IPv6 QoS 지원 템플릿 샘플입니다.

```
!
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
```

Cisco SD-Access에서 IPv6 문제 해결

SD-Access IPv6의 문제 해결은 IPv4와 매우 유사합니다. 동일한 목표를 달성하기 위해 항상 동일한 명령을 다른 키워드 옵션과 함께 사용할 수 있습니다. 다음은 SD-Access 트러블슈팅에 자주 사용되는 몇 가지 명령을 보여줍니다.

```
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
```

오버레이 DHCPv6 서버 ping을 확인하려면 Border Node에서 다음을 수행합니다.

```
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
```

Cisco SD-Access를 통한 IPv6 설계에 대한 빠른 FAQ

Q. Cisco Software Defined Network는 언더레이 및 오버레이 네트워크에 IPv6를 지원합니까?
A. 이 문서를 작성할 때 현재 릴리스(2.3.x)에서는 오버레이만 지원됩니다.

Q. Cisco SDN은 유선 및 무선 클라이언트 모두에 대해 네이티브 IPv6를 지원합니까?
A. 예. 이를 위해서는 DNA 센터에서 생성되는 듀얼 스택 풀이 필요하지만, 클라이언트가 IPv4 DHCP 요청을 비활성화하고 IPv6 DHCP 또는 SLAAC 주소만 제공되므로 IPv4는 더미 풀입니다.

Q. Cisco SD-Access Fabric에 네이티브 IPv6 전용 캠퍼스 네트워크를 보유할 수 있습니까?
A. 현재 릴리스에서는 지원되지 않습니다(최대 2.3.x). 로드맵에 나와 있습니다.

Q. Cisco SD-Access는 L2 IPv6 핸드오프를 지원합니까?
A. 현재는 없습니다. L2 IPv4 핸드오프 및 L3 듀얼 스택 핸드오프만 지원됩니다.

Q. Cisco SD-Access는 IPv6용 멀티캐스트를 지원합니까?
A. 예, 헤드엔드 복제 멀티캐스트가 포함된 오버레이 IPv6만 지원됩니다. 네이티브 IPv6 멀티캐스트는 아직 지원되지 않습니다.

Q. Cisco SD-Access Fabric Enabled Wireless는 듀얼 스택에서 게스트를 지원합니까?
A. Cisco IOS XE(Cat9800) WLC에서는 아직 지원되지 않습니다. AireOS WLC는 해결 방법을 통해 지원됩니다. 해결 방법에 대한 자세한 구현은 Cisco 고객 경험 팀에 문의하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.