在软件定义访问中实施IPv6

目录

简介

本文档介绍如何在Cisco®软件定义访问(SD-Access)中实施IPv6。

背景信息

IPv4于1983年发布，目前仍用于大多数互联网流量。32位IPv4编址允许超过40亿种不同的组合。但是，由于连接到Internet的客户端数量增加，因此缺乏唯一的IPv4地址。在20世纪90年代，IPv4编址的耗尽成为必然。
鉴于此，Internet工程任务组引入了IPv6标准。IPv6利用128位，提供340万亿个唯一IP地址，足以满足不断增长的互联设备的需求。随着越来越多的现代终端设备支持双堆栈和/或单个IPv6堆栈，任何组织都必须准备好采用IPv6。这意味着整个基础设施必须准备好采用IPv6。Cisco SD-Access是从传统园区设计向直接实现组织意图的网络的演进。思科软件定义网络现在已准备好加入双堆栈（IPv6设备）。

任何组织在采用IPV6方面都会遇到一个重大挑战，即与传统IPv4系统迁移到IPv6相关的变更管理和复杂性。本文涵盖有关Cisco SDN上IPv6功能支持、策略和关键坑点的所有详细信息，这些在您采用采用Cisco软件定义网络的IPv6时需要加以注意。

2019年8月，Cisco Digital Network Architecture(DNA)Center 1.3版首次引入IPv6支持。在此版本中，Cisco SD-Access园区网络支持来自重叠交换矩阵网络的IPv4、IPv6或IPv4v6双协议栈中的有线和无线客户端的主机IP地址。解决方案是不断改进，以引入新特性和功能，轻松为任何企业引入IPv6。

采用IPv6架构的Cisco SD-Access

交换矩阵技术是SD-Access不可或缺的一部分，它为有线和无线园区网络提供可编程的重叠和易于部署的网络虚拟化，使物理网络能够托管一个或多个逻辑网络，以满足设计意图。除了网络虚拟化之外，园区网络中的交换矩阵技术还增强了通信控制，从而根据用户身份和组成员身份提供软件定义的分段和策略实施。整个思科SDN解决方案在交换矩阵的DNA上运行。因此，了解解决方案中有关IPv6支持的各个支柱至关重要。

- 底层 — 重叠的IPv6功能依赖于底层，因为IPv6重叠利用IPv4底层IP编址来创建定位器/ID分离协议(LISP)控制平面和虚拟可扩展LAN(VXLAN)数据平面隧道。您可以始终为底层路由协议启用双堆栈，只有SD-Access重叠LISP仅取决于IPv4路由。
- 重叠 — 在重叠方面，SD-Access支持仅IPv6有线和无线终端。该IPv6流量封装在SD访问交换矩阵内的IPv4和VXLAN报头中，直到它们到达交换矩阵边界节点。交换矩阵边界节点解封IPv4和VXLAN报头，从那时起开始执行正常的IPv6单播路由过程。
- 控制平面节点 — 控制平面节点配置为允许在其映射数据库中注册子网范围内的所有IPv6主机子网和/128主机路由。
- 边界节点 — 在边界节点上，启用与融合设备的IPv6 BGP对等。边界节点从交换矩阵出口流量解封IPv4报头，同时边界节点也使用IPv4报头封装入口IPv6流量。
- 交换矩阵边缘 — 交换矩阵边缘中配置的所有交换虚拟接口(SVI)都必须是IPv6。此配置由DNA中心控制器推动。
- Cisco DNA Center — 截至本文档发布时，Cisco DNA Center物理接口不支持双堆栈。它只能通过IPv4或IPv6在DNA Center的管理和/或企业界面中部署在一个堆栈中。
- 客户端 — Cisco SD-Access支持双堆栈（IPv4和IPv6）或单堆栈（IPv4或IPv6）。但是，在部署IPv6单堆栈的情况下，DNA Center仍需要创建双堆栈池以支持仅IPv6客户端。双协议栈池中的IPv4只是虚拟地址，因为客户端需要禁用IPv4地址。

思科软件定义访问中的IPv6重叠架构。

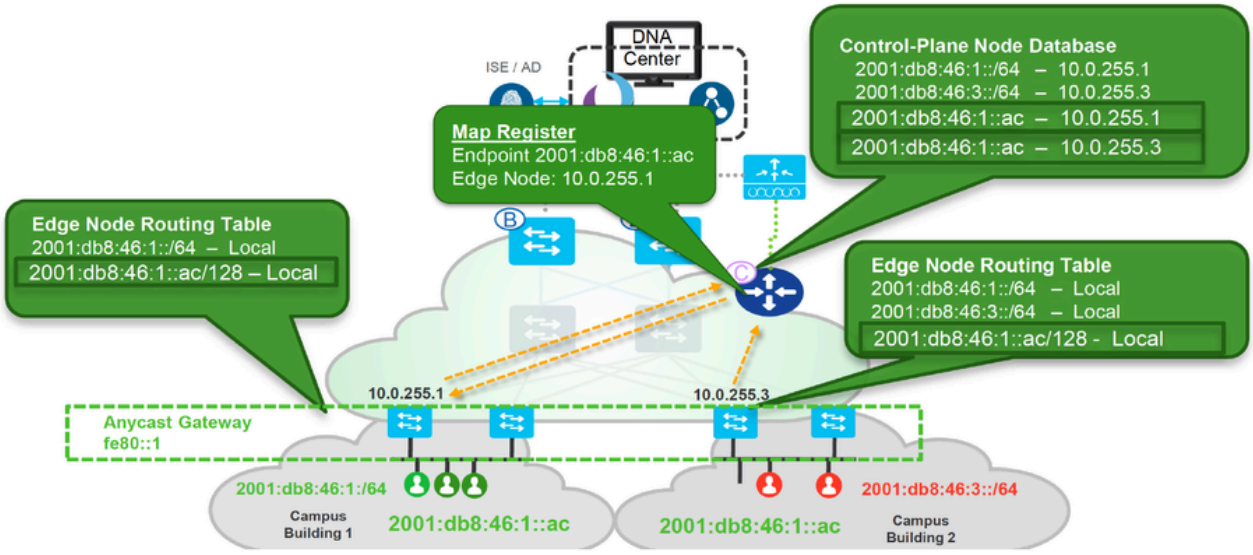


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

IPv6重叠架构

通过Cisco DNA-Center启用IPv6

在Cisco DNA Center中启用IPv6池有两种方法：
1.创建新的双堆栈IPv4/v6池 — 绿地
2.在已经存在的IPv4池上编辑IPv6 - brownfield迁移

当前版本（高达2.3.x）的DNA Center不支持IPv6。如果用户计划支持单一/本地IPv6仅地址客户端，则仅支持池。虚拟IPv4地址需要与IPv6池关联。请注意，从已部署的IPv4池中（该池已存在与其关联的站点），然后使用IPv6地址编辑该池。DNA Center为SD-Access交换矩阵提供迁移选项，需要用户为该站点重新调配交换矩阵。警告指示符显示在站点所属的交换矩阵中，指示交换矩阵需要“重新配置交换矩阵”。有关示例，请参阅以下图像：

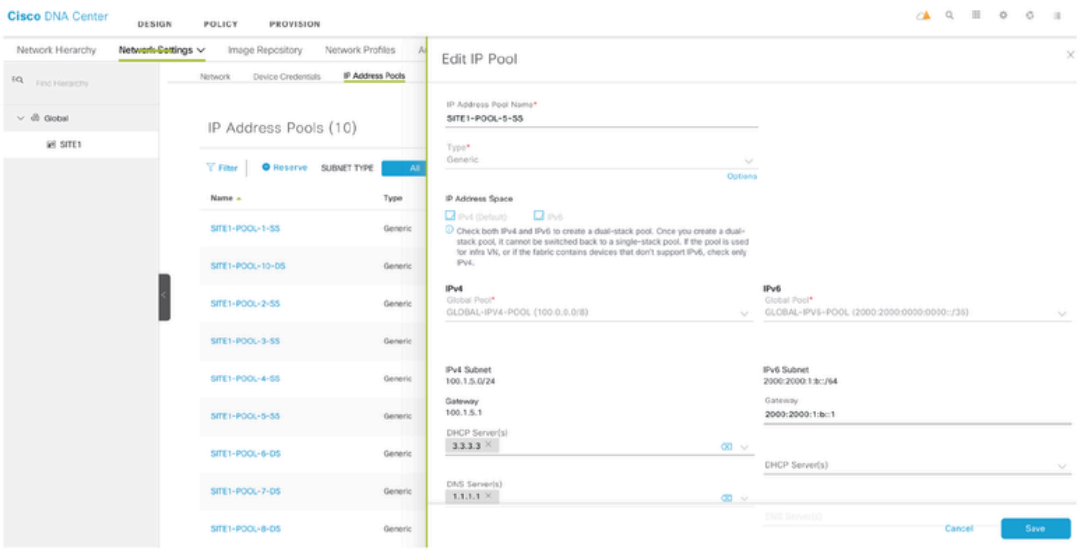


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

通过编辑IPv4池选项将单IPv4池升级到双堆栈池

Pool upgrade: Warning on fabric page

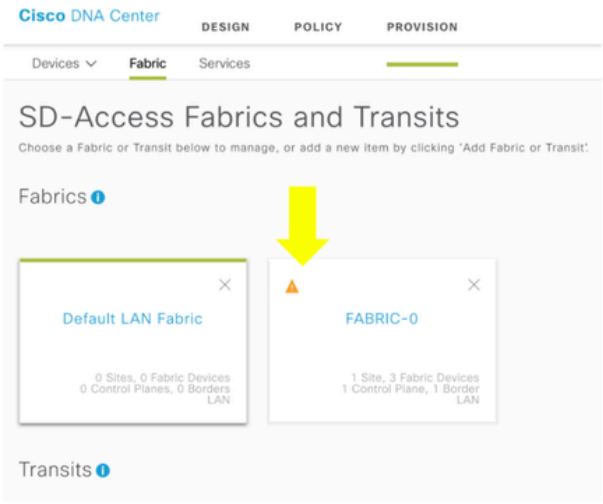


Figure 3.
Fabric has warning indicator which needs to 'reconfigure the fabric'

交换矩阵具有需要"重新配置交换矩阵"的警告指示器

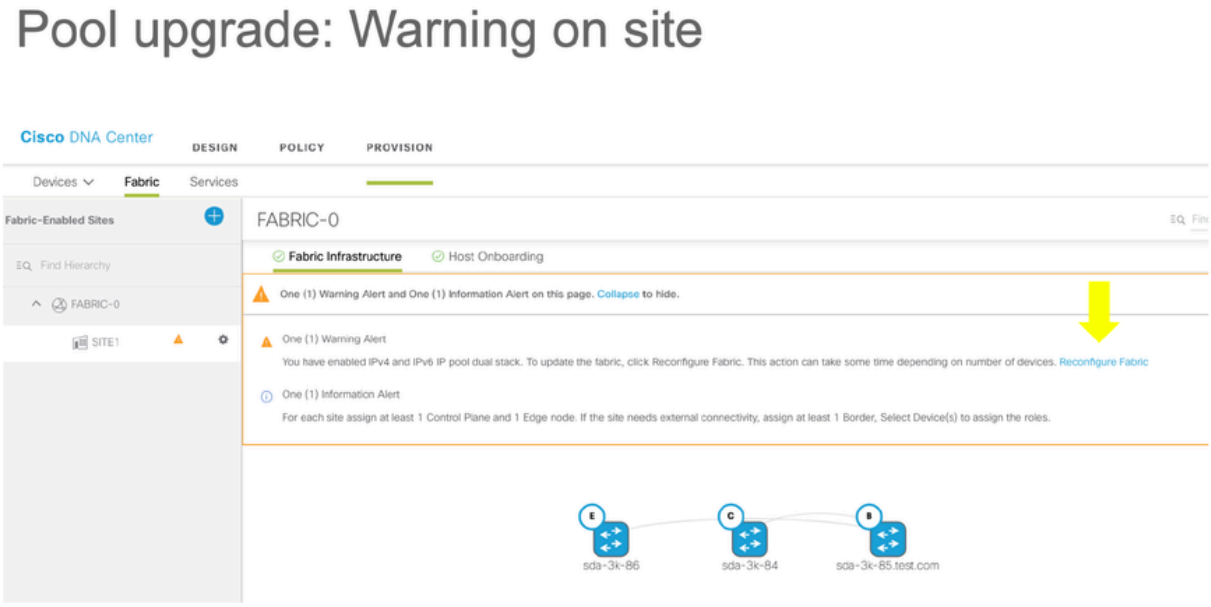


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

用户需要点击"重新配置交换矩阵"以自动重新调配交换矩阵节点，使双堆栈配置在迁移过程中生效

Cisco SD-Access中IPv6的设计注意事项

虽然对于思科SD-Access客户端，它们可以使用双堆栈或仅IPv6网络设置运行，但当前使用DNA中心交换机(SW)版本（最高为2.3.x.x）的SD-Access交换矩阵实施在IPv6部署方面有一些注意事项。

- Cisco SD-Access支持IPv4底层路由协议。因此，将IPv6客户端流量封装在IPv4报头中时会进行传输。这是当前LISP软件部署的要求。但这并不意味着底层无法启用IPv6路由协议，只是SD-Access重叠LISP不会根据其依赖性运行。
- 不支持IPv6本地组播，因为交换矩阵底层目前只能是IPv4。
- 访客无线只能通过双堆栈运行。由于当前身份服务引擎(ISE)版本（例如，高达3.2），不支持IPv6访客门户，因此仅IPv6访客客户端将无法获得身份验证。
- 当前DNA Center版本不支持IPv6应用QoS策略自动化。本文档介绍在思科SD-Access中为某个用户大规模部署有线和无线双栈客户端实施IPv6 QoS所需的步骤。
- IPv4(TCP/UDP)和IPv6（仅TCP）支持基于服务集标识符(SSID)或基于策略的每个客户端的下游和上游流量的无线客户端速率限制功能。尚不支持IPv6 UDP速率限制。
- IPv4池可以升级到双堆栈池。但双堆栈池不能降级为IPv4池。如果用户想要将双堆栈池移回IPv4单堆栈池，则需要释放整个双堆栈池。
- 目前尚不支持单IPv6，但在当前DNA中心中只能创建IPv4或双堆栈池。
- Cisco IOS® XE平台是16.9.2及更高版本的最低软件版本要求。
- Cisco IOS XE平台尚不支持IPv6访客无线，而AireOS(8.10.105.0+)支持解决方法。
- 不能在INFRA_VN中分配双堆栈池，其中只能分配接入点(AP)或扩展节点池。
- LAN自动化尚不支持IPv6。

除了前面提到的限制之外，当您设计启用了IPv6的SD-Access交换矩阵时，必须始终牢记每个交换矩阵组件的可扩展性。如果某个终端有多个IPv4或IPv6地址，则每个地址都将视为一个单独的条目。

交换矩阵主机条目包括接入点以及经典和策略扩展节点。

其他边界节点扩展注意事项：

当边界节点将流量从交换矩阵外部转发到交换矩阵中的主机时，使用/32(IPv4)或/128(IPv6)条目。

对于除Cisco Catalyst 9500系列高性能交换机和Cisco Catalyst 9600系列交换机之外的所有交换机：

- IPv4对每个IPv4 IP地址使用一个三重内容可寻址存储器(TCAM)条目（交换矩阵主机条目）。
- IPv6对每个IPv6 IP地址使用两个TCAM条目（交换矩阵主机条目）。

对于Cisco Catalyst 9500系列高性能交换机和Cisco Catalyst 9600系列交换机：

- IPv4对每个IPv4 IP地址使用一个TCAM条目（交换矩阵主机条目）。
- IPv6对每个IPv6 IP地址使用一个TCAM条目（交换矩阵主机条目）。

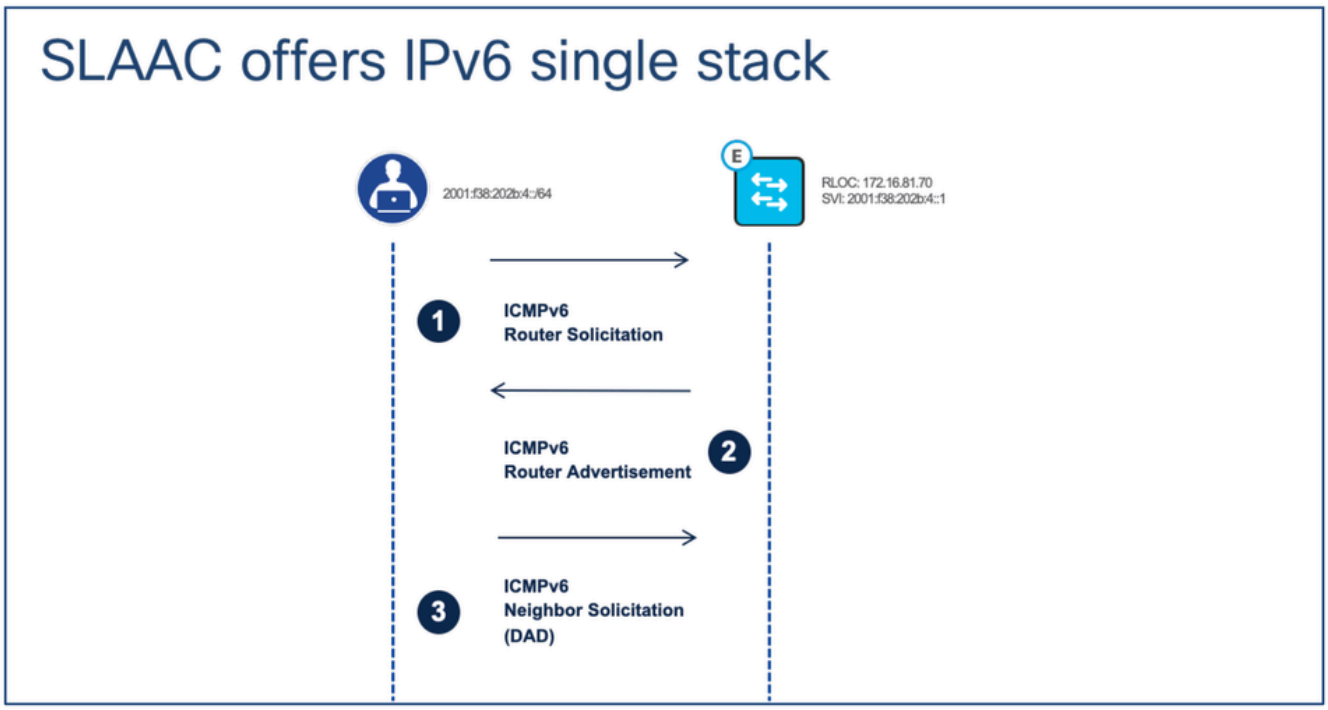
某些终端不支持DHCPv6，例如基于Android操作系统的智能手机，它们依靠无状态地址自动配置(SLAAC)获取IPv6地址。单个终端可能拥有两个以上的IPv6地址。此行为在每个交换矩阵节点上消耗更多硬件资源，尤其是对于交换矩阵边界和控制节点。例如，每当边界节点要向任何终端的边缘节点发送流量时，它都会在TCAM条目中安装主机路由并在硬件(HW)TCAM中烧写VXLAN邻接条目。

有线和无线客户端连接和呼叫流程

客户端连接到交换矩阵边缘后，可通过多种不同方式获取IPv6地址。本节介绍客户端IPv6编址的最常用方法，即SLAAC和DHCPv6。

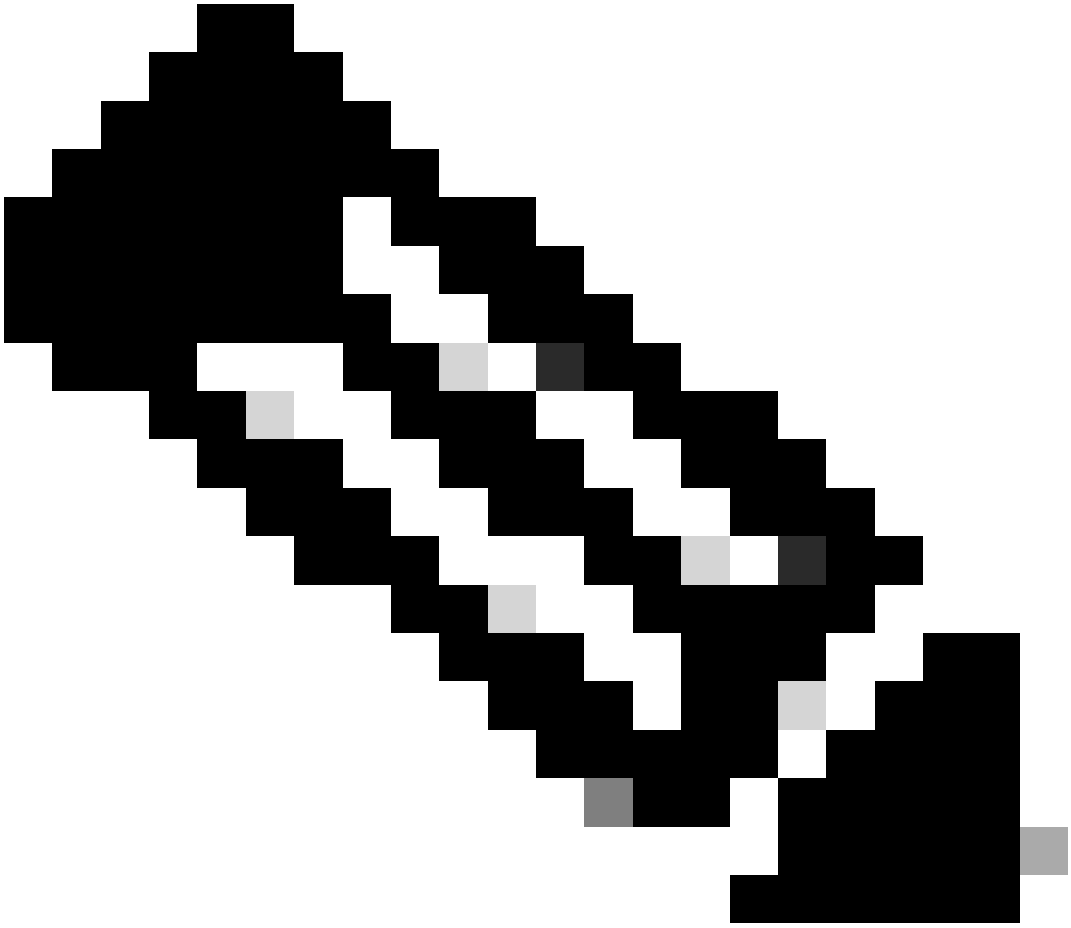
IPv6地址分配 — SLAAC

软件定义访问(SDA)中的SLAAC与标准SLAAC流程没有区别。为了使SLAAC正常工作，必须在IPv6客户端的接口上配置本地链路地址，而客户端如何使用本地链路地址自动配置自己则不在本文档的讨论范围之内。



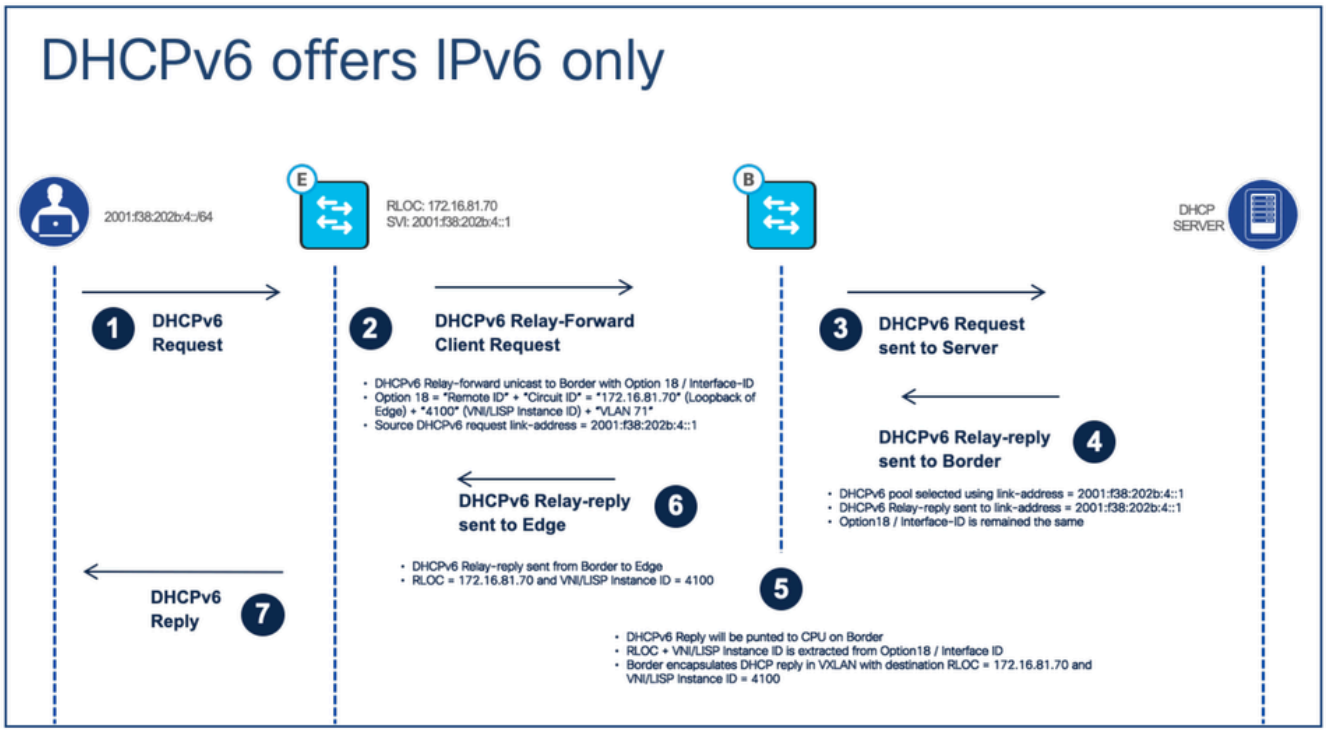
IPv6地址分配 — SLAAC

呼叫流程说明：
步骤1.在IPv6客户端使用IPv6本地链路地址进行自我配置后，客户端将ICMPv6路由器请求(RS)消息发送到交换矩阵边缘。此消息的目的是获取其连接网段的全局单播前缀。
步骤2.交换矩阵边缘收到RS消息后，用ICMPv6路由器通告(RA)消息进行响应，该消息包含全局IPv6单播前缀及其内部长度。
步骤3.客户端收到RA消息后，会将IPv6全局单播前缀与其EUI-64接口标识符结合以生成其唯一的IPv6全局单播地址，并将其网关设置为与客户端网段相关的交换矩阵边缘SVI的本地链路地址。然后，客户端发出ICMPv6邻居请求消息，以便执行重复地址检测(DAD)以确保其获得的IPv6地址是唯一的。



注意：所有与SLAAC相关的消息都使用客户端和交换矩阵节点的SVI IPv6本地链路地址进行封装。

IPv6地址分配 — DHCPv6

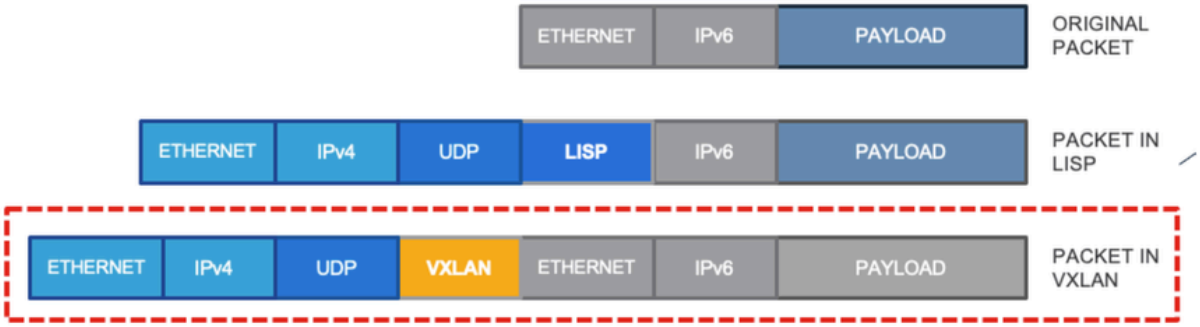


IPv6地址分配 — DHCPv6

呼叫流程说明：
步骤1.客户端向交换矩阵边缘发出DHCPv6请求。
步骤2.交换矩阵边缘收到DHCPv6请求时，它将使用DHCPv6中继转发消息将请求通过DHCPv6选项18单播到交换矩阵边界。与DHCP选项82相比，DHCPv6选项18将“电路ID”和“远程ID”编码在一起。LISP实例ID/VNI、IPv4路由定位器(RLOC)和终端VLAN都在内部编码。
步骤3.交换矩阵边界解封VXLAN报头并将DHCPv6数据包单播到DHCPv6服务器。
步骤4. DHCPv6服务器收到中继转发消息，使用消息的源链路地址（DHCPv6中继代理/客户端网关）选择IPv6 IP池来分配IPv6地址。然后将DHCPv6中继应答消息发送回客户端网关地址。第18项保持不变。
步骤5.交换矩阵边界收到中继应答消息后，从选项18提取RLOC和LISP实例/VNI。交换矩阵边界将中继应答消息封装到VXLAN中，并将其从选项18提取的目标。
步骤6.交换矩阵边界向客户端连接的交换矩阵边缘发送DHCPv6中继应答消息。
步骤7.当交换矩阵边缘收到DHCPv6中继应答消息时，它将解封该消息的VXLAN报头并将该消息转发给客户端。然后，客户端知道其分配的IPv6地址。

Cisco SD-Access中的IPv6通信

IPv6通信使用基于LISP的标准控制平面和基于VXLAN的数据平面通信方法。在思科SD-Access LISP和VXLAN中的当前实施中，使用外部IPv4报头在内部传输IPv6数据包。此映像捕获此过程。



内部传输IPv6数据包的外部IPv4报头

这意味着所有LISP查询都使用IPv4本地数据包，而控制平面节点表包含有关终端的IPv6和IPv4 IP地址的RLOC的详细信息。下一节从无线端点的角度详细介绍此过程。

Cisco SD-Access中的无线IPv6通信

除了典型的思科SD-Access交换矩阵组件外，无线通信依赖于两个特定组件接入点和无线局域网控制器。无线接入点通过无线局域网控制器(WLC)创建无线接入点的控制和调配(CAPWAP)隧道。 当客户端流量存在于交换矩阵边缘时，包括无线电统计信息在内的其他控制平面通信由WLC管理。从IPv6的角度来看，WLC和AP都必须具有IPv4地址，并且所有CAPWAP通信都使用这些IPv4地址。虽然非交换矩阵WLC和AP支持IPv6通信，但思科SD-Access使用IPv4进行所有在IPv4数据包中传输任何客户端IPv6流量的通信。这意味着在Infra VN下分配的AP池无法与双堆栈的IP池进行映射，如果对此映射进行任何尝试，则会引发错误。Cisco SDA内的无线通信可分为以下主要任务：

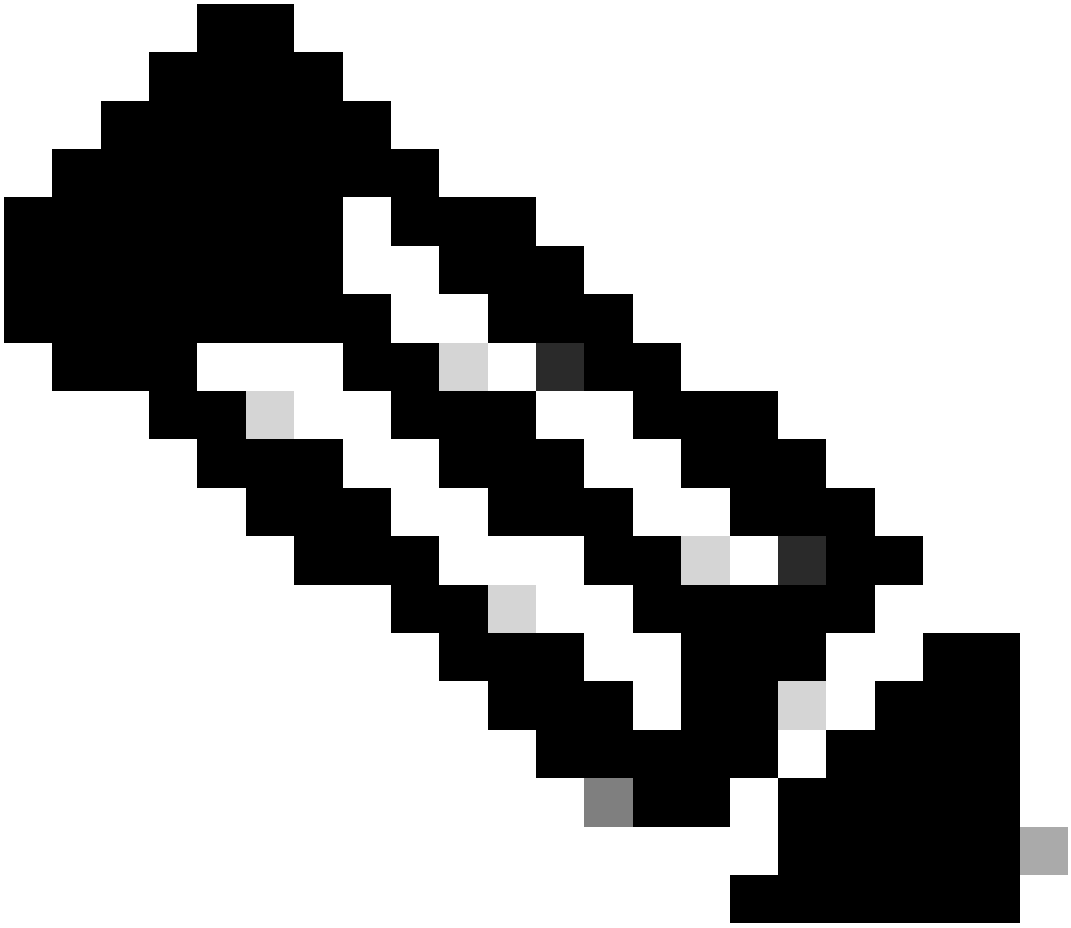
- 接入点自注册
- 客户端入网

从IPv6角度查看这些事件。

接入点自注册

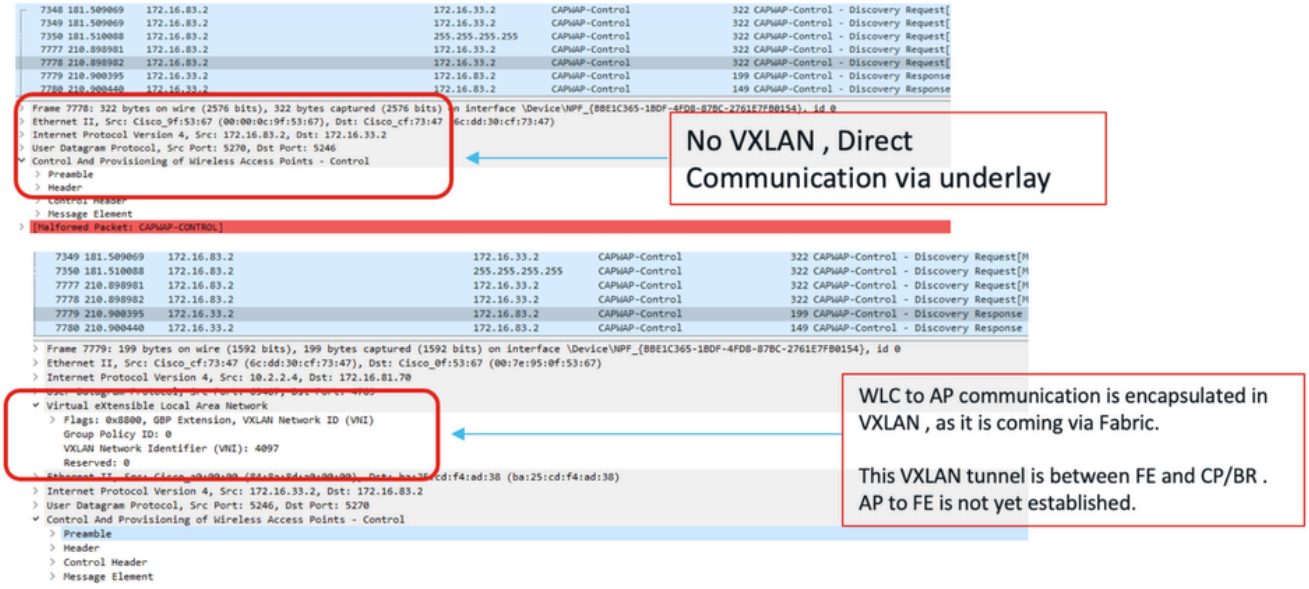
对于IPv6和IPv4，此过程保持不变，因为WLC和AP都包含此处的IPv4地址和步骤：
1.交换矩阵边缘(FE)端口配置为板载AP。
2. AP连接到FE端口，并通过CDP AP通知FE其存在（这允许FE分配正确的VLAN）。
3. AP从DHCP服务器获取IPv4地址，FE注册AP并更新控制平面(控制平面(CP)节点)的AP详细信息。
4. AP通过传统方法（如DHCP选项43）加入WLC。
5. WLC检查AP是否支持交换矩阵，并在控制平面中查询AP RLOC信息（例如，请求的RLOC/接收的响应）。
6. CP向WLC回复AP的RLOC IP。
7. WLC在CP中注册AP媒体访问控制（地址）(MAC)。
8. CP使用来自WLC的有关AP的详细信息更新FE（这会通知FE通过AP启动VXLAN隧道）。

FE处理信息并创建带AP的VXLAN隧道。此时，AP会通告启用交换矩阵的SSID。



注意：如果AP广播非交换矩阵SSID而不广播交换矩阵SSID，请检查接入点和交换矩阵边缘节点之间的VXLAN隧道。

另请注意，AP到WLC的通信始终通过Underlay CAPWAP进行，而所有WLC到AP的通信都通过重叠使用VXLAN CAPWAP。这意味着，如果捕获从AP到WLC的数据包，则只有在反向流量具有VXLAN隧道时才能看到CAPWAP。有关AP和WLC之间的通信，请参阅此示例。



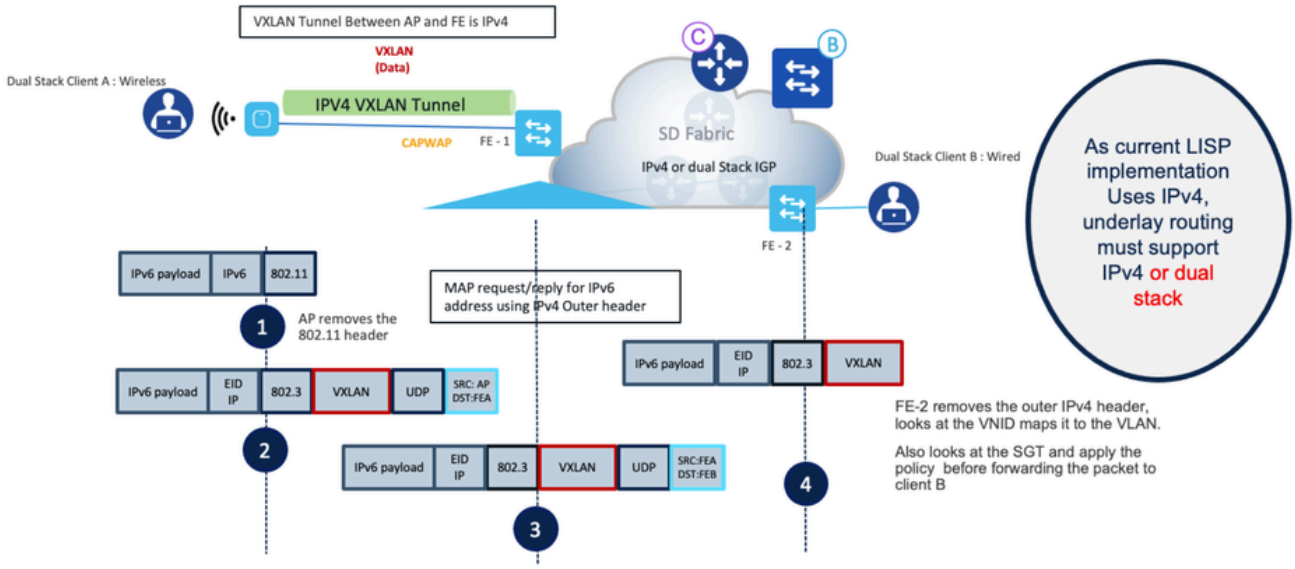
从AP到WLC的数据包捕获（CAPWAP隧道）与WLC到AP的数据包捕获（交换矩阵中的VxLAN隧道）

客户端自注册

双堆栈/IPv6客户端自注册过程保持不变，但客户端使用SLAAC/DHCPv6等IPv6地址分配方法来获取IPv6地址。
1.客户端加入交换矩阵并在AP上启用SSID。
2. WLC知道AP RLOC。
3.客户端身份验证和WLC向CP注册客户端L2详细信息并更新AP。
4.客户端从已配置的方法 — SLAAC/DHCPv6发起IPv6编址。
5. FE触发IPv6客户端注册到CP主机跟踪数据库(HTDB)。AP到FE和FE到其他目的地使用IPv4帧中的VXLAN和LISP IPv6封装。

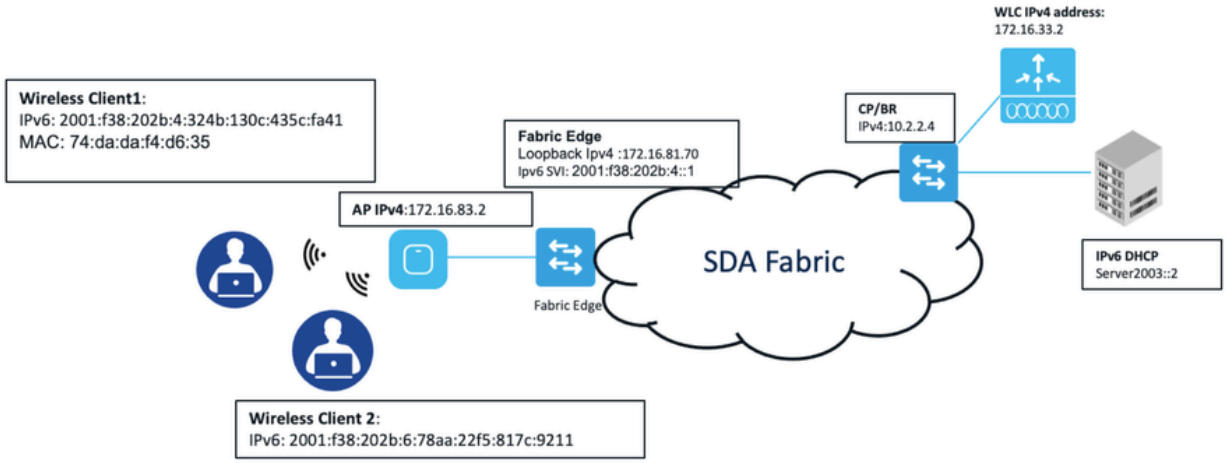
使用IPv6的客户端 — 客户端通信

此图总结了与另一个IPv6有线客户端的IPv6无线客户端通信过程。（这假设客户端已通过身份验证并通过配置的方法获得IPv6地址。）
1.客户端将带IPv6负载的802.11帧发送到AP。
2. AP删除802.11报头并将IPv4 VXAN隧道中的原始IPv6负载发送到交换矩阵边缘。
3.交换矩阵边缘使用消息访问协议(MAP)请求识别目标并将帧通过IPv4 VXLAN发送到目标RLOC。
4.在目的交换机上，IPv4 VXLAN报头被删除，IPv6数据包被发送到客户端。

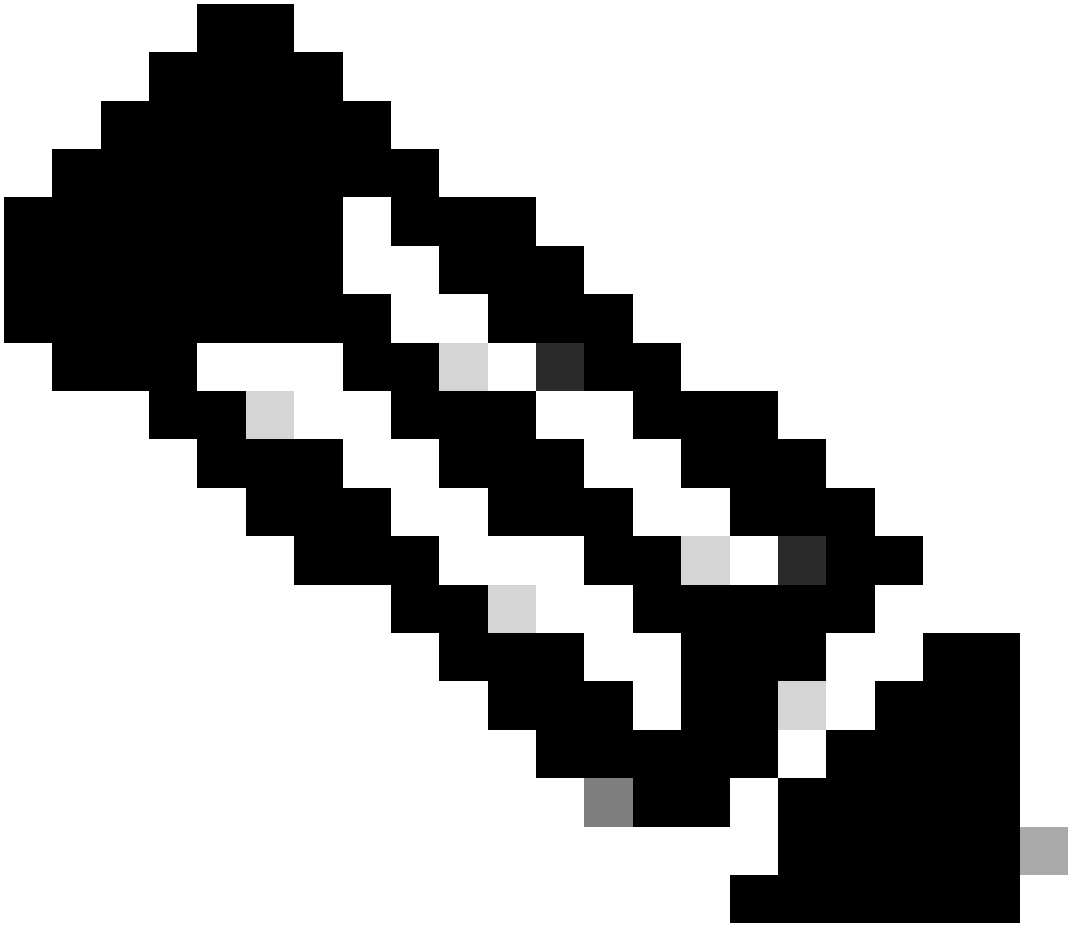


双堆栈无线客户端到双堆栈有线客户端数据包流

通过数据包捕获深入了解此过程，并参阅映像了解IP地址和MAC地址的详细信息。请注意，此设置使用两个双协议栈客户端，这两个客户端连接到相同的接入点，但映射到不同的IPv6子网(SSID)。

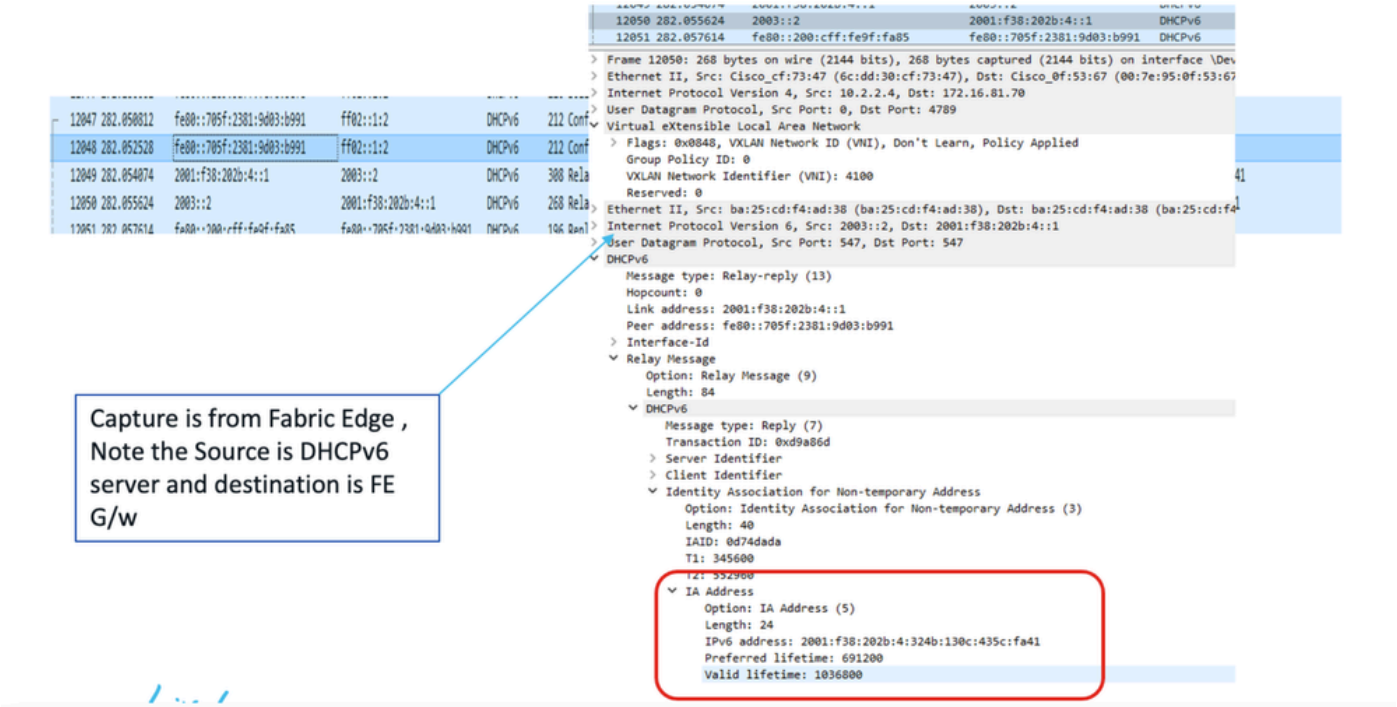


示例SD访问交换矩阵网络IP地址和MAC地址详细信息



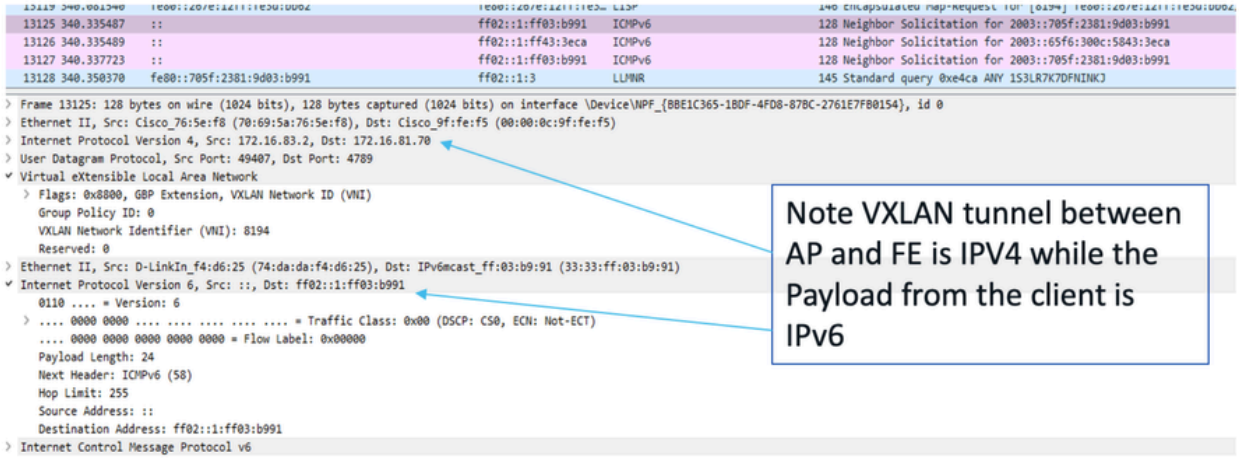
注意：对于交换矩阵外部的任何IPv6通信（例如，DHCP/DNS），必须在边界基础设施和非交换矩阵基础设施之间启用IPv6路由。

步骤1.客户端通过身份验证并从配置的方法获取IPv6地址。



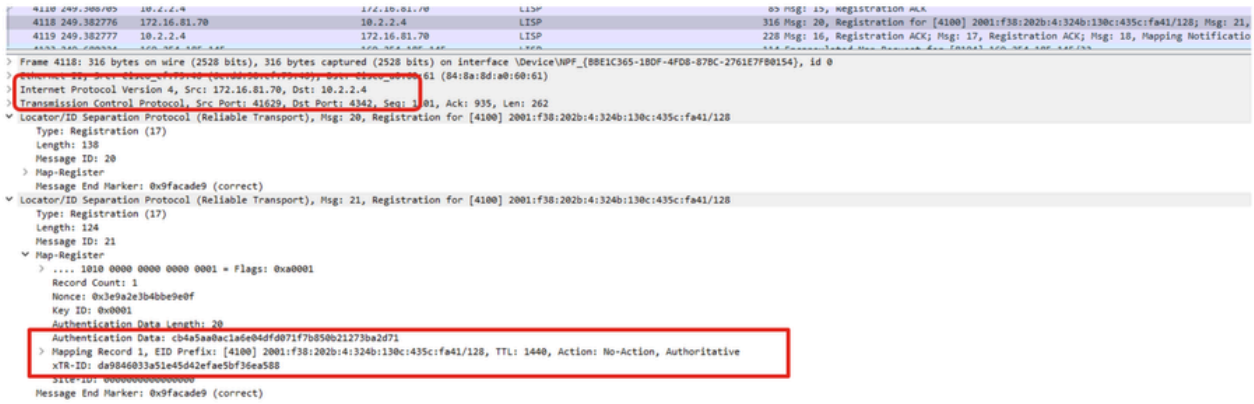
从DHCPv6服务器到交换矩阵边缘节点的数据包捕获

步骤2.无线客户端使用IPv6负载将802.11帧发送到接入点。
步骤3.接入点删除无线报头并将数据包发送到交换矩阵边缘。这使用基于IPv4的VXLAN隧道报头，因为接入点具有IPv4地址。



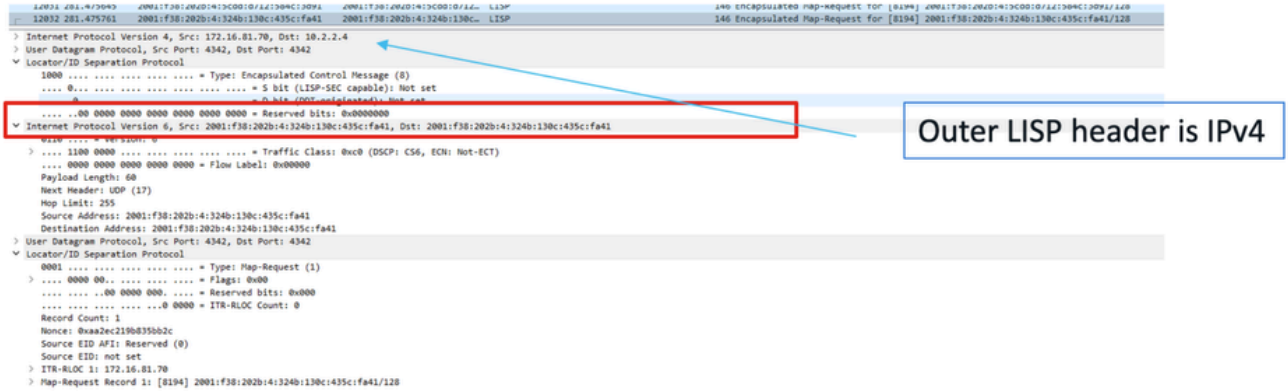
FE和AP之间VxLAN隧道的数据包捕获

步骤3.1.交换矩阵边缘将IPv6客户端注册到控制平面。这使用IPv4注册方法，其中包含IPv6客户端的详细信息。



FE注册的数据包捕获与IPv6客户端的控制平面

步骤3.2. FE将MAP请求发送到控制平面以标识目标RLOC。



使用MAP注册消息从FE到CP的数据包捕获

Fabric Edge还维护已知IPv6客户端的MAP缓存，如下图所示。

```
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#
```

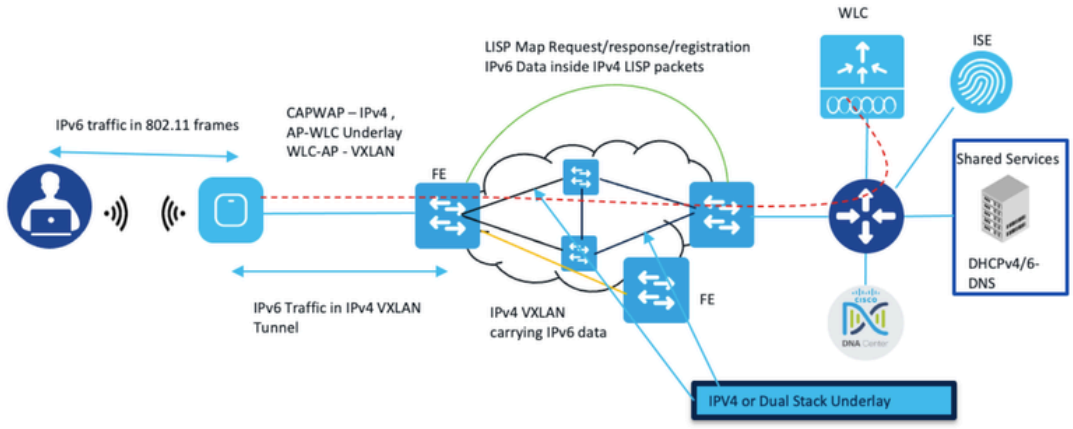
IPv6重叠映射缓存信息的交换矩阵边缘屏幕输出

步骤4.将数据包转发到目标RLOC，其中的IPv4 VXLAN承载了原始IPv6负载。由于两个客户端都连接到同一个AP，因此IPv6 ping会采用此路径。

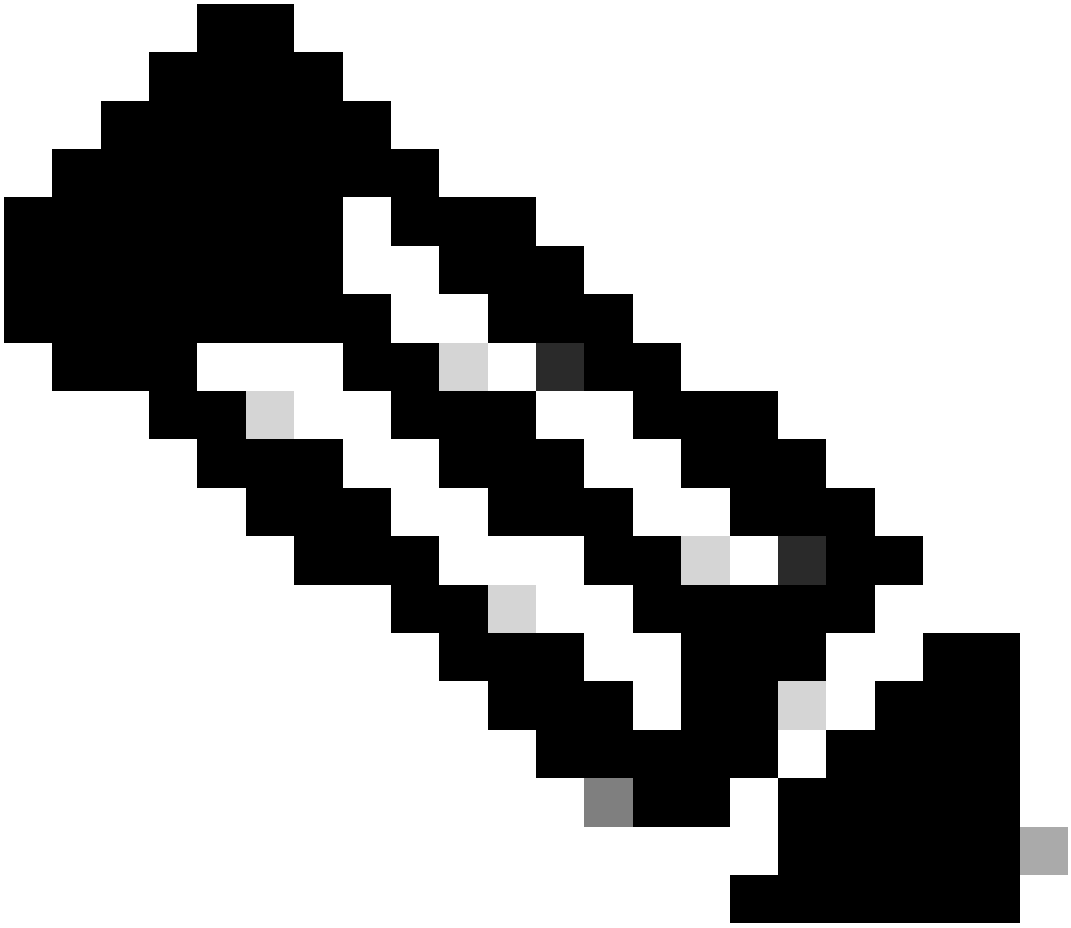
```
    71 3.392805     2001:f38:202b:4:324b:130c:435c:fa41   2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001, seq=148, hop limit=63
    72 3.392836     2001:f38:202b:4:324b:130c:435c:fa41   2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001, 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)
```

在注册到同一AP的两个无线客户端之间进行IPv6 ping的数据包捕获

此图从无线客户端的角度总结了IPv6通信。



图中从无线客户端的角度总结了IPv6通信



注意：由于ISE的限制，不支持通过思科身份服务进行IPv6访客访问（Web门户）。

依赖矩阵

请注意Cisco SD-Access中不同无线组件对IPv6的依赖性和支持，这一点非常重要。本图中的表格总结了此功能矩阵。

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功能（按版本）

监控IPv6的控制平面

启用IPv6后，您开始在映射服务器(MS)/映射解析器(MR)服务器中看到有关主机IPv6的其他条目。由于主机可以有多个IPv6 IP地址，您的MS/MR查找表包含所有IP地址的条目。这将与已经存在的IPv4表结合使用。
您必须登录设备CLI并发出这些命令以检查所有条目。

```
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
```

您还可以通过保证检查有关主机IPv6的详细信息。

Cisco SD-Access中的IPv6 QoS实施

当前的Cisco DNA Center版本（高达2.3.x）不支持IPv6 QoS应用策略自动化。但是，用户可以手动创建IPv6有线和无线模板，并将QoS模板推送到交换矩阵边缘节点。由于DNA Center会在应用所有物理接口上自动执行IPv4 QoS策略，因此您可以通过模板在“class-default”之前手动插入类映射(匹配IPv6访问控制列表(ACL))。

以下是与DNA Center生成的策略配置集成的支持IPv6 QoS的模板示例：

```
!
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-Access中的IPv6故障排除

排除SD-Access IPv6故障与IPv4非常相似，您可以始终使用包含不同关键字选项的相同命令以实现相同目标。此处显示一些常用于排除SD-Access故障的命令。

```
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
```

从边界节点检查重叠DHCPv6服务器ping:

```
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-Access IPv6设计快速常见问题

问：思科软件定义网络是否支持底层网络和重叠网络的IPv6?
答：在撰写本文档时，当前版本(2.3.x)仅支持重叠。

问：思科SDN是否支持有线和无线客户端的本机IPv6?
答：是的。这要求在DNA中心中创建双堆栈池，而IPv4是虚拟池，因为客户端禁用IPv4 DHCP请求，且仅提供IPv6 DHCP或SLAAC地址。

问：我的思科SD接入交换矩阵中能否拥有纯IPv6的本机园区网络？
A.不适用于当前版本（最高为2.3.x）。 它正在规划中。

问：Cisco SD-Access是否支持L2 IPv6转接？
目前还没有。仅支持L2 IPv4切换和/或L3双栈切换。

问：Cisco SD-Access是否支持IPv6的组播？
答：是，仅支持头端复制组播的重叠IPv6。尚不支持本地IPv6组播。

问：思科SD接入交换矩阵支持无线支持双堆栈中的访客吗？
A.尚不支持Cisco IOS XE(Cat9800)WLC。AireOS WLC通过一种变通方法受到支持。有关解决方案的实施详情，请联系思科客户体验团队。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。