在軟體定義訪問中實施IPv6

目錄

簡介

本文檔介紹如何在Cisco®軟體定義訪問(SD-Access)中實施IPv6。

背景資訊

IPv4於1983年發佈，目前仍用於大部分網際網路流量。32位IPv4編址允許超過40億種不同的組合。但是，由於與Internet連線的客戶端數量增加，因此缺乏唯一的IPv4地址。在20世紀90年代，IPv4編址的耗盡已不可避免。
基於此預期，Internet工程任務組引入了IPv6標準。IPv6利用128位元，提供340萬億個唯一IP地址，足以滿足不斷增長的互聯裝置的需求。隨著越來越多的現代終端裝置支援雙堆疊和/或單個IPv6堆疊，任何組織都必須為採用IPv6做好準備。這意味著整個基礎設施必須準備好採用IPv6。Cisco SD-Access是從傳統園區設計到直接實現組織意圖的網路的演變。Cisco軟體定義網路現在已準備就緒，可以加入雙堆疊（IPv6裝置）。

任何組織在採用IPV6時都會面臨一個重大挑戰，即與傳統IPv4系統遷移到IPv6相關的更改管理和複雜性。本文涵蓋有關Cisco SDN上IPv6功能支援、策略和關鍵點的所有詳細資訊，當您採用Cisco軟體定義網路的IPv6時，需要注意這些詳細資訊。

2019年8月，Cisco Digital Network Architecture(DNA)Center 1.3版首次引入了IPv6支援。在此版本中，Cisco SD-Access園區網路支援主機IP地址與重疊交換矩陣網路中的IPv4、IPv6或IPv4v6雙協定棧中的有線和無線客戶端。解決方案是不斷改進，以便為任何企業帶來可輕鬆加入IPv6的新特性和功能。

採用IPv6架構的Cisco SD-Access

交換矩陣技術是SD-Access不可或缺的一部分，為有線和無線園區網路提供可程式設計的重疊和易於部署的網路虛擬化，允許物理網路託管一個或多個邏輯網路以滿足設計意圖。除了網路虛擬化之外，園區網路中的交換矩陣技術增強了通訊控制，從而提供了基於使用者身份和組成員資格的軟體定義分段和策略實施。整個Cisco SDN解決方案在交換矩陣的DNA上運行。因此，瞭解解決方案中有關IPv6支援的各個支柱至關重要。

- 底層 — Overlay的IPv6功能依賴於底層，因為IPv6重疊利用IPv4底層IP編址來建立定位器/ID分離協定(LISP)控制平面和虛擬可擴展LAN(VXLAN)資料平面隧道。您始終可以為底層路由協定啟用雙堆疊，而只有SD-Access重疊LISP僅取決於IPv4路由。
- 重疊 — 在重疊方面，SD-Access支援僅IPv6有線和無線終端。該IPv6流量將封裝在SD-Access交換矩陣中的IPv4和VXLAN報頭中，直到它們到達交換矩陣邊界節點。交換矩陣邊界節點解封IPv4和VXLAN報頭，從那時起，VXLAN報頭會執行正常的IPv6單播路由過程。
- 控制平面節點 — 控制平面節點配置為允許在其對映資料庫中註冊子網範圍內的所有IPv6主機子網和/128主機路由。
- 邊界節點 — 在邊界節點上，已啟用與融合裝置的IPv6 BGP對等。邊界節點將IPv4報頭從交換矩陣出口流量中解除封裝，同時邊界節點也將輸入IPv6流量封裝為IPv4報頭。
- 交換矩陣邊緣 — 交換矩陣邊緣中配置的所有交換虛擬介面(SVI)都必須是IPv6。此配置由DNA中心控制器推送。
- Cisco DNA Center — 截至本文發佈時，Cisco DNA Center物理介面不支援雙堆疊。它只能通過IPv4或IPv6在DNA Center的管理和/或企業介面中部署在一個堆疊中。
- 客戶端 — Cisco SD-Access支援雙堆疊（IPv4和IPv6）或單堆疊（IPv4或IPv6）。但是，在部署了IPv6單堆疊的情況下，DNA Center仍需要建立雙堆疊池來支援僅支援IPv6的客戶端。雙堆疊池中的IPv4隻是虛擬地址，因為客戶端需要禁用IPv4地址。

思科軟體定義訪問中的IPv6重疊架構。

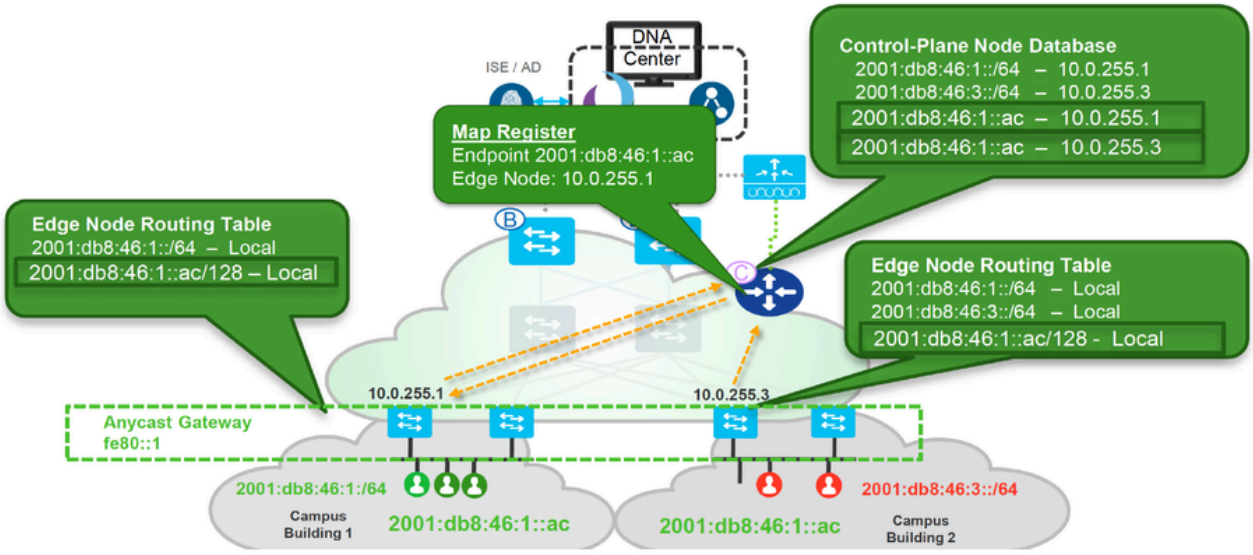


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

IPv6重疊架構

使用Cisco DNA-Center啟用IPv6

在Cisco DNA Center中啟用IPv6池的方法有兩種：
1.建立新的雙堆疊IPv4/v6池 — greenfield
2.在已經存在的IPv4池上編輯IPv6 - brownfield遷移

當前版本的DNA Center（最多2.3.x）不支援IPv6。如果使用者計畫支援單一/本機IPv6僅地址客戶端，則僅支援池。虛擬IPv4地址需要與IPv6池關聯。請注意，從已部署的IPv4池中（該池已存在於與其關聯的站點），並編輯具有IPv6地址的池。DNA Center為SD-Access交換矩陣提供了遷移選項，該選項要求使用者為該站點重新調配交換矩陣。站點所屬的交換矩陣中會顯示一個警告指示符，指示交換矩陣需要「重新配置交換矩陣」。有關示例，請參閱以下影象：

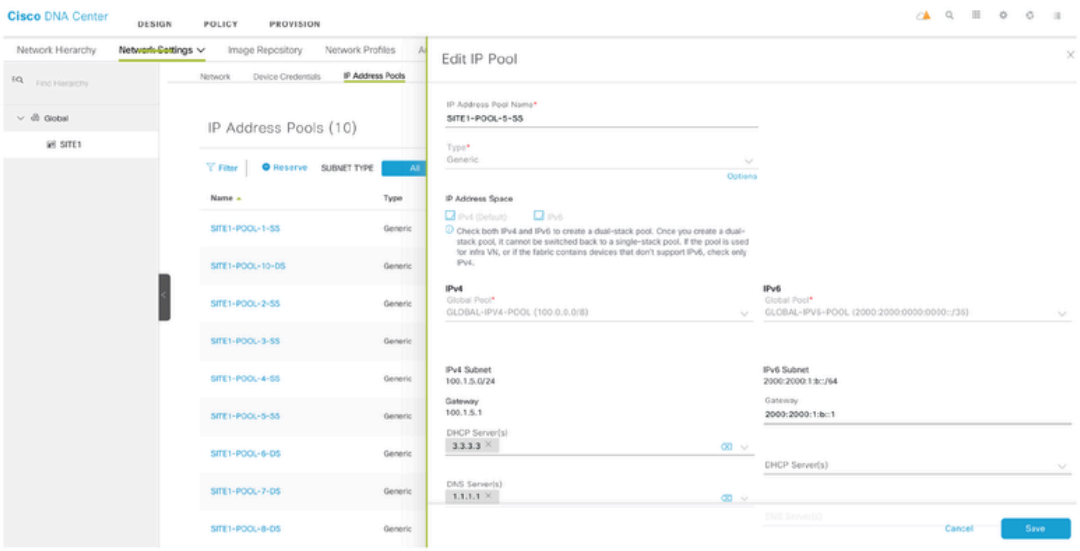


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

通過編輯IPv4池選項將單IPv4池升級到雙堆疊池

Pool upgrade: Warning on fabric page

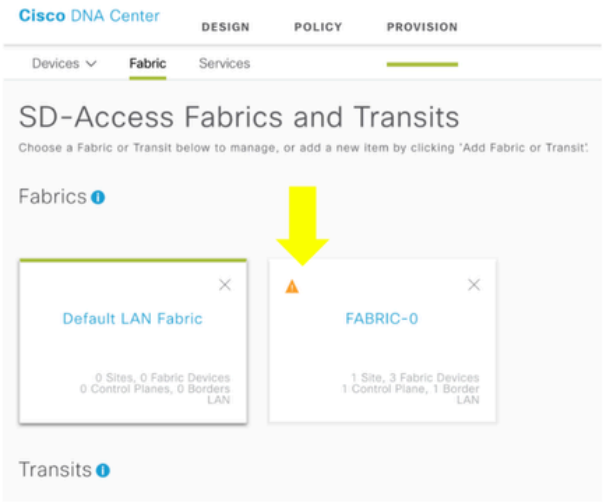


Figure 3.
Fabric has warning indicator which needs to 'reconfigure the fabric'

交換矩陣具有需要「重新配置交換矩陣」的警告指示器

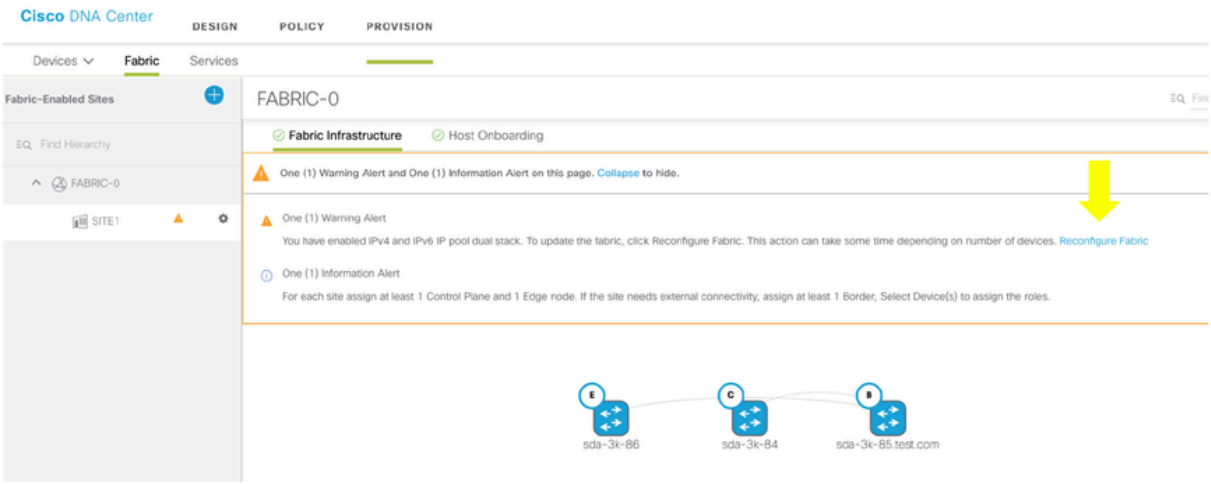


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

使用者需要點選「重新配置交換矩陣」以自動重新調配交換矩陣節點，使雙堆疊配置在遷移過程中生效

Cisco SD-Access中IPv6的設計注意事項

雖然對於Cisco SD-Access客戶端，它們可以使用雙堆疊或僅IPv6網路設定運行，但當前採用DNA中心交換機(SW)版本(2.3.x.x)的SD-Access交換矩陣實施在IPv6部署方面有一些注意事項。

- Cisco SD-Access支援IPv4底層路由協定。因此，將IPv6客戶端流量封裝在IPv4報頭中時，會對其進行傳輸。這是當前LISP軟體部署的要求。但這並不意味著底層無法啟用IPv6路由協定，只是SD-Access重疊LISP不依賴其運行。
- 不支援IPv6本機組播，因為交換矩陣底層目前只能是IPv4。
- 訪客無線功能只能使用雙重堆疊執行。由於當前身份服務引擎(ISE)版本（例如，高達3.2），不支援IPv6訪客門戶，因此僅支援IPv6的訪客客戶端將無法獲得身份驗證。
- 當前DNA Center版本不支援IPv6應用QoS策略自動化。本文檔介紹為某個使用者大規模部署的Cisco SD-Access中的有線和無線雙堆疊客戶端實施IPv6 QoS所需的步驟。
- IPv4(TCP/UDP)和IPv6（僅TCP）支援根據服務集識別符號(SSID)或基於策略的每個客戶端的下游和上游流量的無線客戶端速率限制功能。尚不支援IPv6 UDP速率限制。
- IPv4池可升級為雙堆疊池。但是雙堆疊池不能降級為IPv4池。如果使用者想要將雙堆疊池移除回IPv4單堆疊池，則需要釋放整個雙堆疊池。
- 目前尚不支援單IPv6，但在當前DNA中心中只能建立IPv4或雙堆疊池。
- Cisco IOS® XE平台是16.9.2及更高版本的最低軟體版本要求。
- Cisco IOS XE平台尚不支援IPv6訪客無線，而AireOS(8.10.105.0+)支援解決方法。
- 無法在INFRA_VN中指定雙堆疊池，其中只能指定接入點(AP)或擴展節點池。
- LAN自動化尚不支援IPv6。

除了前面提到的限制之外，在設計啟用了IPv6的SD-Access交換矩陣時，必須始終牢記每個交換矩陣元件的可擴充性。如果某個終端有多個IPv4或IPv6地址，則每個地址都將計為單個條目。

交換矩陣主機條目包括接入點以及經典和策略擴展節點。

其他邊界節點擴展注意事項：

當邊界節點將流量從交換矩陣外部轉發到交換矩陣中的主機時，會使用/32(IPv4)或/128(IPv6)條目。

對於除Cisco Catalyst 9500系列高效能交換機和Cisco Catalyst 9600系列交換機以外的所有交換機：

- IPv4對每個IPv4 IP位址使用一個「三重內容可定址記憶體(TCAM)」專案（光纖主機專案）。
- IPv6對每個IPv6 IP地址使用兩個TCAM條目（交換矩陣主機條目）。

對於Cisco Catalyst 9500系列高效能交換機和Cisco Catalyst 9600系列交換機：

- IPv4對每個IPv4 IP位址使用一個TCAM專案（光纖主機專案）。
- IPv6對每個IPv6 IP地址使用一個TCAM條目（交換矩陣主機條目）。

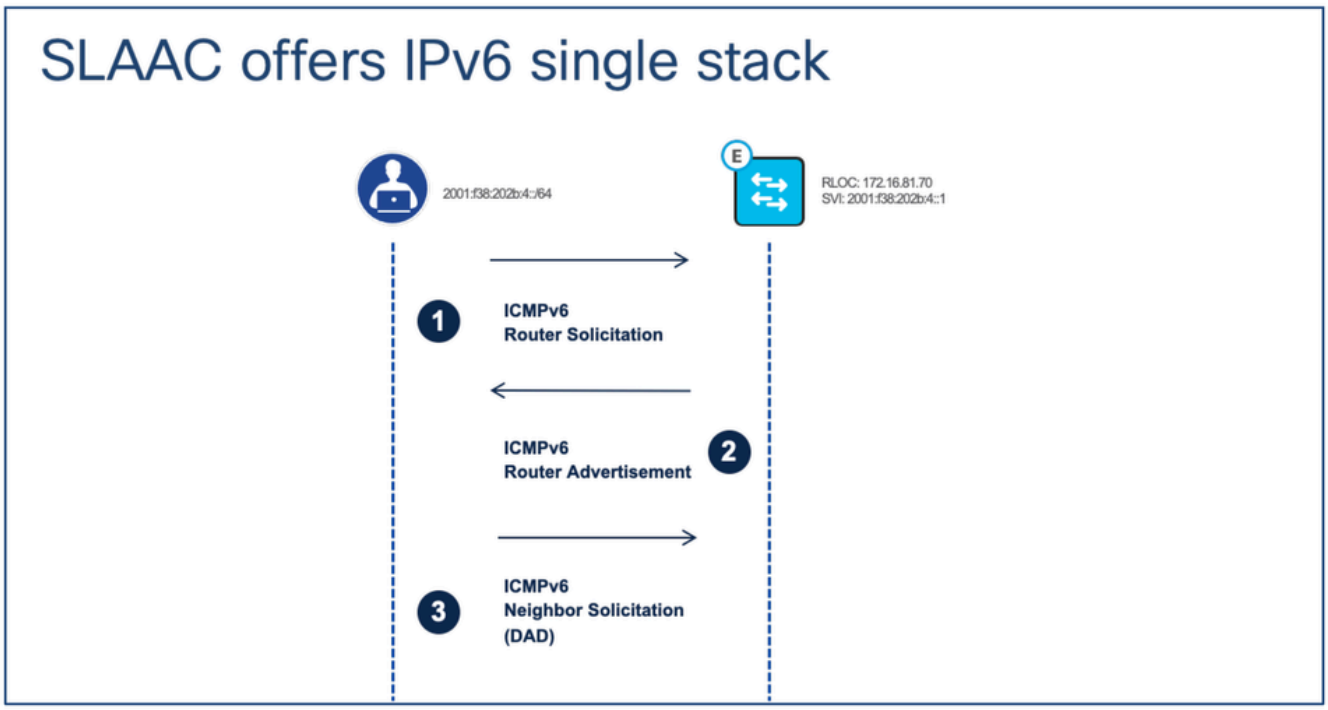
某些終端不支援DHCPv6，例如基於Android OS的智慧手機，它們依靠無狀態地址自動配置(SLAAC)獲取IPv6地址。單個終端可能最終擁有兩個以上的IPv6地址。此行為在每個交換矩陣節點上消耗更多硬體資源，尤其是對於交換矩陣邊界和控制節點。例如，每當邊界節點要將流量傳送到任何端點的邊緣節點時，它都會在TCAM條目中安裝主機路由，並在硬體(HW)TCAM中燒毀VXLAN鄰接條目。

有線和無線客戶端連線和呼叫流程

客戶端連線到交換矩陣邊緣後，可通過多種不同方式獲取IPv6地址。本節介紹客戶端IPv6編址的最常見方法，即SLAAC和DHCPv6。

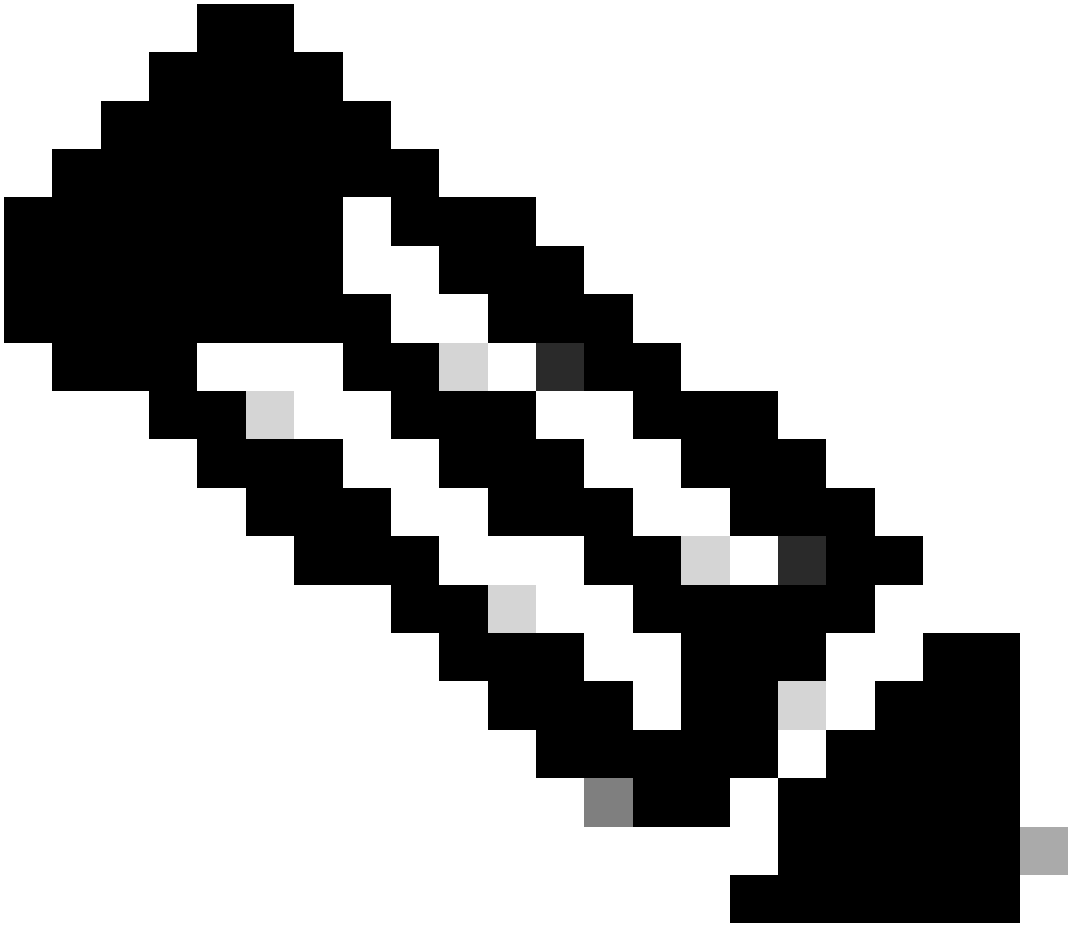
IPv6地址分配 — SLAAC

軟體定義訪問(SDA)中的SLAAC與標準SLAAC流程沒有區別。為了使SLAAC正常工作，必須在IPv6客戶端的介面上配置本地鏈路地址，而客戶端如何使用本地鏈路地址自動配置自己則不在本文檔的討論範圍之內。



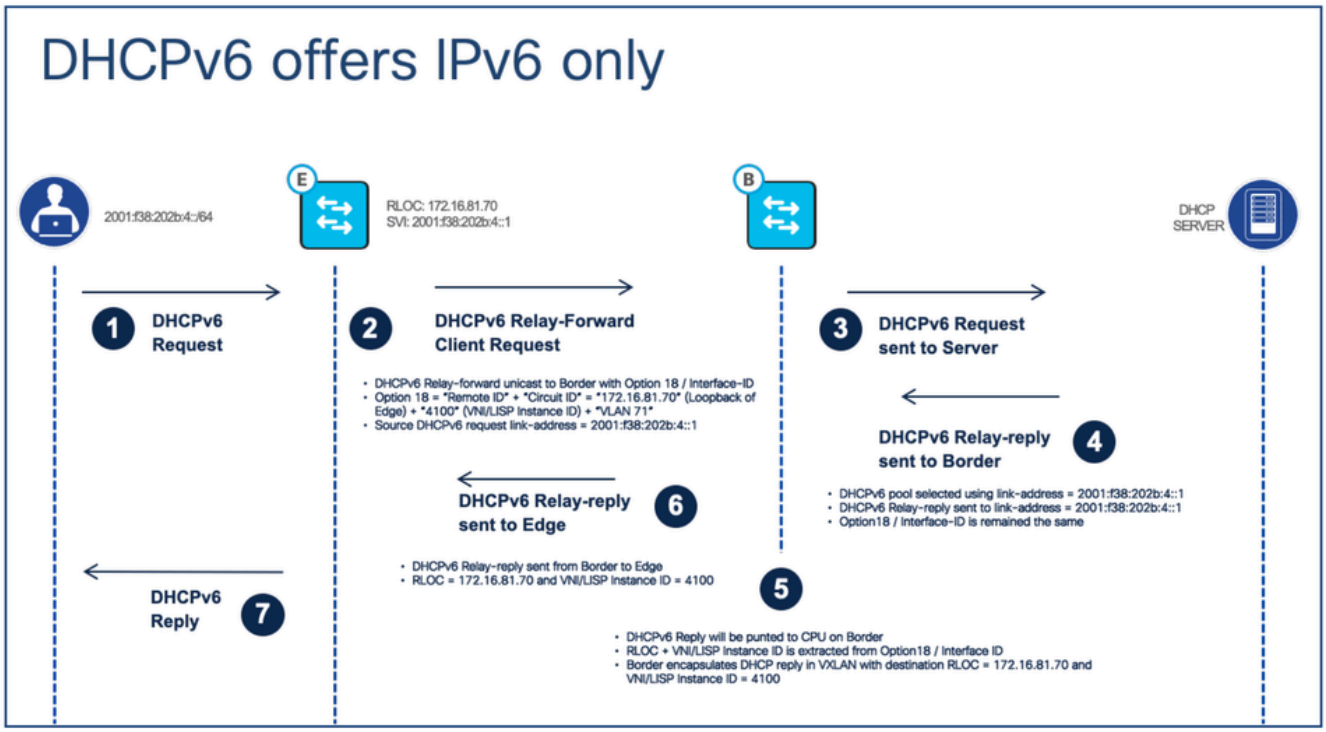
IPv6地址分配 — SLAAC

呼叫流描述：
步驟1. IPv6客戶端使用IPv6本地鏈路地址進行配置後，客戶端會向交換矩陣邊緣傳送ICMPv6路由器請求(RS)消息。此訊息的用途是取得其連線的區段的全域單點傳播首碼。
步驟2.交換矩陣邊緣收到RS消息後，會使用包含全域性IPv6單播字首及其內部長度的ICMPv6路由器通告(RA)消息進行響應。
步驟3.客戶端收到RA消息後，會將IPv6全域性單播字首與其EUI-64介面識別符號相結合，生成唯一的IPv6全域性單播地址，並將其網關設定為與客戶端網段相關的交換矩陣邊緣SVI的本地鏈路地址。然後使用者端會發出ICMPv6鄰居要求訊息，以便執行重複位址偵測(DAD)，以確保其取得的IPv6位址是唯一的。



附註：所有與SLAAC相關的消息均使用客戶端和交換矩陣節點的SVI IPv6本地鏈路地址進行封裝。

IPv6地址分配 — DHCPv6

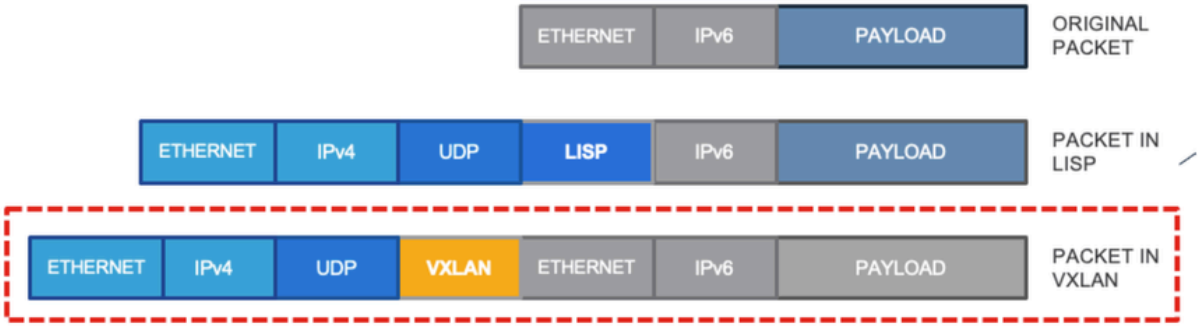


IPv6地址分配 — DHCPv6

呼叫流描述：
步驟1.客戶端向交換矩陣邊緣傳送DHCPv6請求。
步驟2.交換矩陣邊緣收到DHCPv6請求時，它將使用DHCPv6中繼轉發消息將請求單播到交換矩陣邊界，並使用DHCPv6選項18。與DHCP選項82相比，DHCPv6選項18將「電路ID」和「遠端ID」一起編碼。LISP例項ID/VNI、IPv4路由定位器(RLOC)和終端VLAN都在內部編碼。
步驟3.交換矩陣邊界解封VXLAN報頭並將DHCPv6資料包單播到DHCPv6伺服器。
步驟4、DHCPv6伺服器收到中繼轉發消息，使用該消息的源鏈路地址（DHCPv6中繼代理/客戶端網關）選擇IPv6 IP池分配IPv6地址。然後將DHCPv6中繼回覆消息傳送回客戶端網關地址。選項18保持不變。
步驟5.交換矩陣邊界收到中繼回覆消息時，從選項18提取RLOC和LISP例項/VNI。交換矩陣邊界將中繼回覆消息封裝在VXLAN中，目的地為從選項18提取的目標。
步驟6.交換矩陣邊界將DHCPv6中繼回覆消息傳送到客戶端連線的交換矩陣邊緣。
步驟7.交換矩陣邊緣收到DHCPv6中繼回覆消息時，會解除封裝該消息的VXLAN報頭並將該消息轉發給客戶端。然後客戶端知道其分配的IPv6地址。

Cisco SD-Access中的IPv6通訊

IPv6通訊使用標準的基於LISP的控制平面和基於VXLAN的資料平面通訊方法。在Cisco SD-Access LISP和VXLAN中的當前實施中，使用外部IPv4報頭將IPv6資料包傳送至內部。此影象捕獲此過程。



內部承載IPv6資料包的外部IPv4報頭

這意味著所有LISP查詢都使用IPv4本機資料包，而控制平面節點表包含有關具有終端的IPv6和IPv4 IP地址的RLOC的詳細資訊。下一節從無線端點的角度詳細介紹此過程。

Cisco SD-Access中的無線IPv6通訊

除了典型的Cisco SD-Access交換矩陣元件外，無線通訊依賴於兩個特定元件接入點和無線LAN控制器。無線存取點與無線LAN控制器(WLC)建立無線存取點(CAPWAP)通道的控制和布建。 雖然使用者端流量存在於光纖邊緣，但包含無線電統計資料的其他控制平面通訊仍由WLC管理。從IPv6的角度來看，WLC和AP都必須具有IPv4地址，並且所有CAPWAP通訊都使用這些IPv4地址。雖然非交換矩陣WLC和AP支援IPv6通訊，但Cisco SD-Access使用IPv4進行所有在IPv4資料包中傳輸任何客戶端IPv6流量的通訊。這表示在Infra VN下分配的AP池無法用雙堆疊的IP池進行對映，如果對此對映進行任何嘗試，則會引發錯誤。Cisco SDA內的無線通訊可分為以下主要任務：

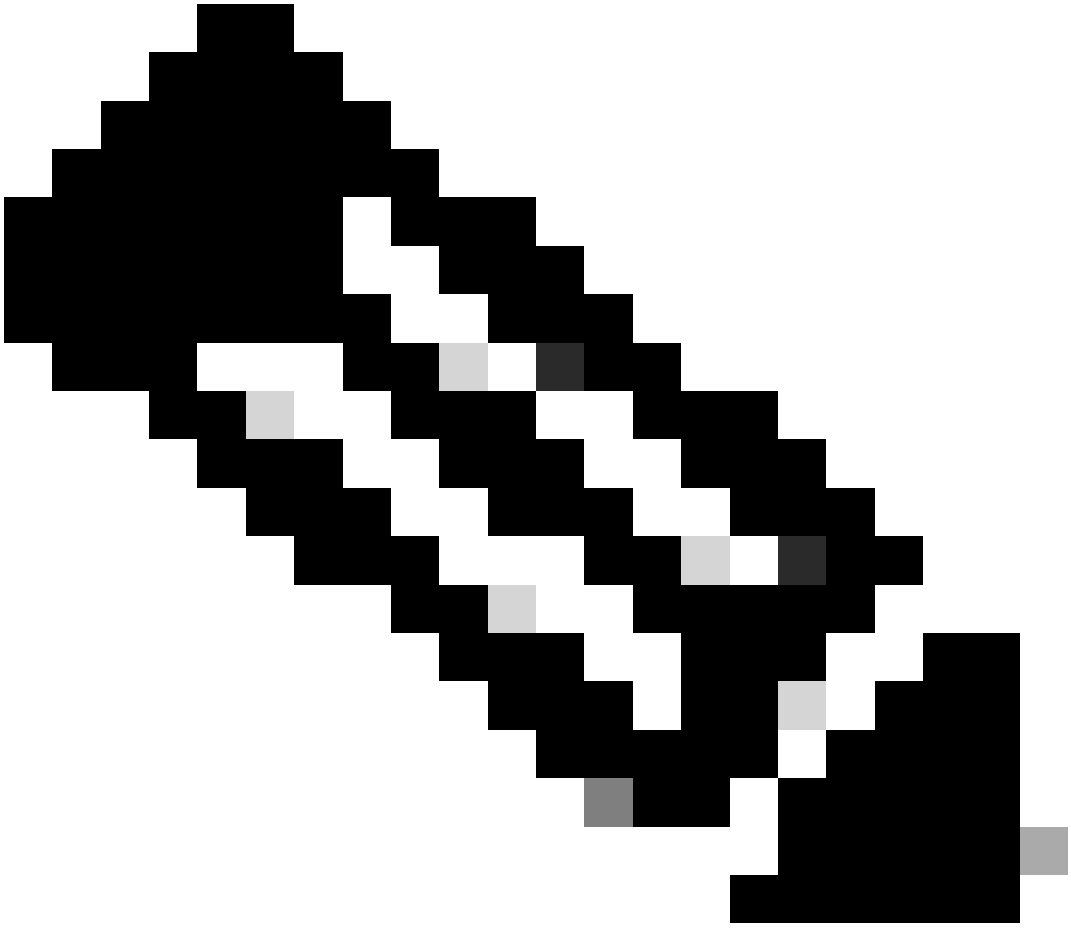
- 接入點自註冊
- 客戶端入站

從IPv6的角度看這些事件。

接入點自註冊

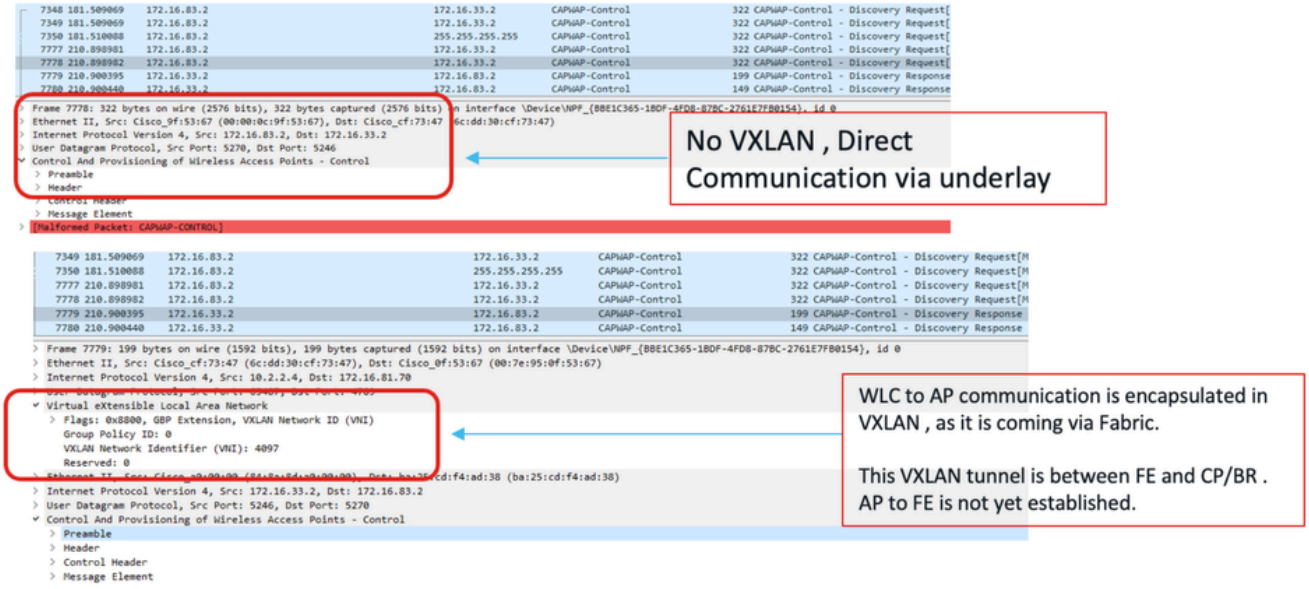
對於IPv6和IPv4，此過程保持不變，因為WLC和AP都具有IPv4地址以及此處包含的步驟：
1.將交換矩陣邊緣(FE)埠配置為板載AP。
2. AP連線到FE埠，並通過CDP AP通知FE其存在（這允許FE分配正確的VLAN）。
3. AP從DHCP伺服器獲取IPv4地址，FE註冊AP並使用AP詳細資訊更新控制平面(控制平面(CP)節點)。
4. AP通過傳統方法（如DHCP選項43）加入WLC。
5. WLC檢查AP是否支援交換矩陣，並在控制平面中查詢AP RLOC資訊（例如，請求的RLOC/接收的響應）。
6. CP會使用AP的RLOC IP回覆WLC。
7. WLC在CP中註冊AP介質訪問控制（地址）(MAC)。
8. CP使用WLC提供的有關AP的詳細資訊更新FE（這指示FE通過AP啟動VXLAN隧道）。

FE會處理該資訊並建立帶AP的VXLAN隧道。此時，AP會通告啟用交換矩陣的SSID。



附註：如果AP廣播非交換矩陣SSID而不廣播交換矩陣SSID，請檢查接入點和交換矩陣邊緣節點之間的VXLAN隧道。

另請注意，AP到WLC的通訊始終通過襯底CAPWAP進行，而所有WLC到AP的通訊都通過重疊使用VXLAN CAPWAP。這表示如果擷取從AP到WLC的封包，則只有在反向流量具有VXLAN通道時，才會看到CAPWAP。有關AP和WLC之間的通訊，請參閱以下示例。



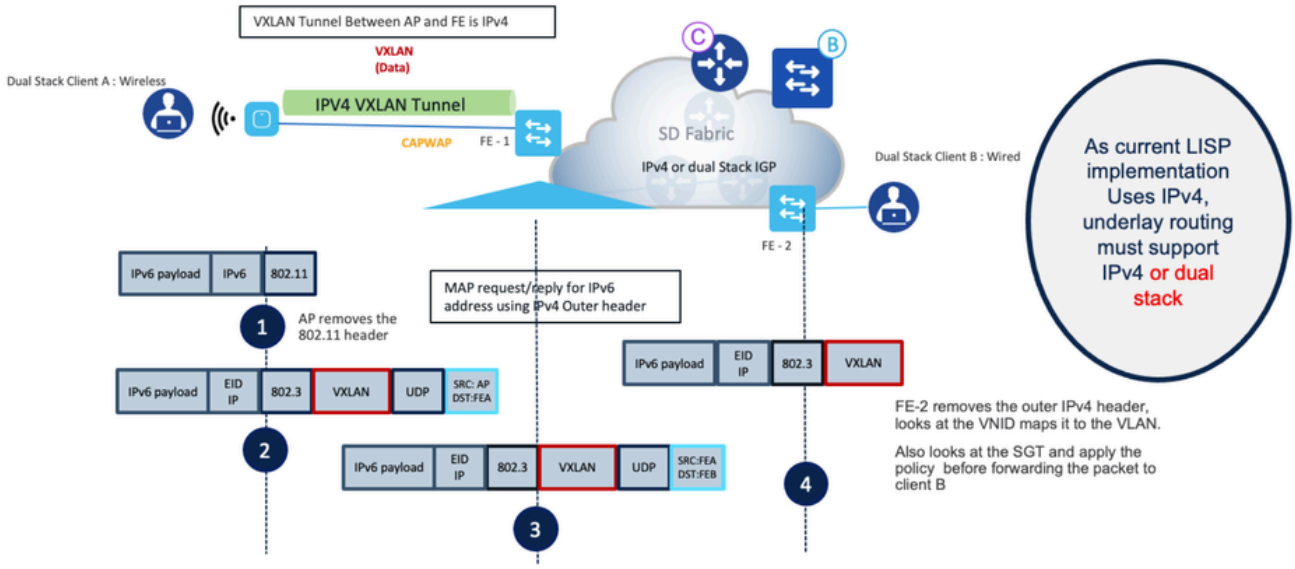
從AP到WLC的封包擷取（CAPWAP通道）與WLC到AP的封包擷取（光纖中的VxLAN通道）

客戶端自註冊

雙堆疊/IPv6客戶端自註冊過程保持不變，但客戶端使用SLAAC/DHCPv6等IPv6地址分配方法獲取IPv6地址。
1.客戶端加入交換矩陣並在AP上啟用SSID。
2. WLC知道AP RLOC。
3.客戶端身份驗證和WLC使用CP註冊客戶端L2詳細資訊並更新AP。
4.客戶端從已配置的方法(SLAAC/DHCPv6)起始IPv6編址。
5. FE觸發IPv6客戶端註冊到CP主機跟蹤資料庫(HTDB)。AP到FE和FE到其他目的地使用IPv4幀中的VXLAN和LISP IPv6封裝。

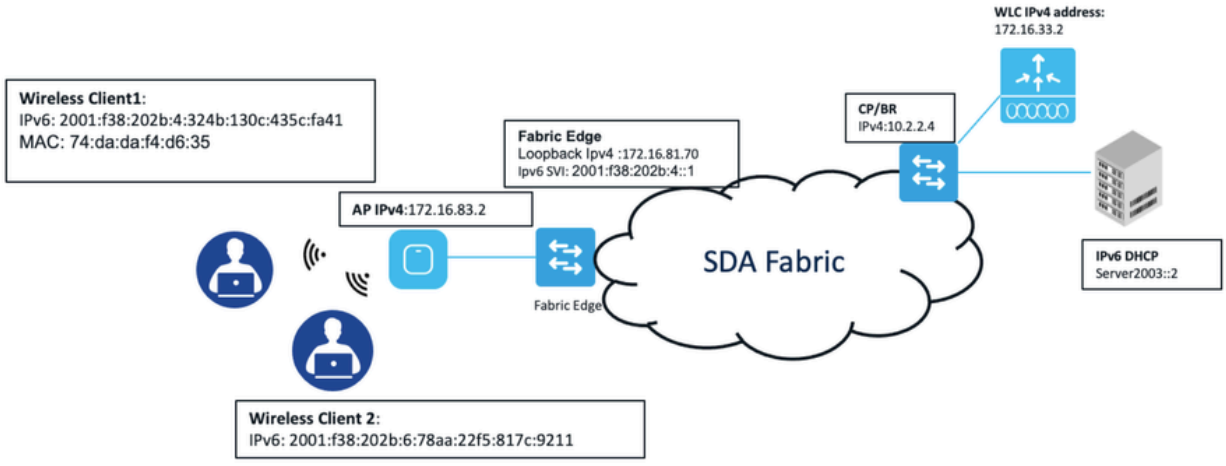
使用IPv6的客戶端 — 客戶端通訊

此處的影象總結了與另一個IPv6有線客戶端的IPv6無線客戶端通訊過程。（這假設客戶端通過身份驗證並通過配置的方法獲得IPv6地址。）
1.客戶端使用IPv6負載將802.11幀傳送到AP。
2. AP刪除802.11報頭並將IPv4 VXAN隧道中的原始IPv6負載傳送到交換矩陣邊緣。
3. Fabric Edge使用消息訪問協定(MAP)請求來標識目標，並使用IPv4 VXLAN將幀傳送到目標RLOC。
4.在目的交換機上，IPv4 VXLAN報頭被刪除，IPv6資料包被傳送到客戶端。

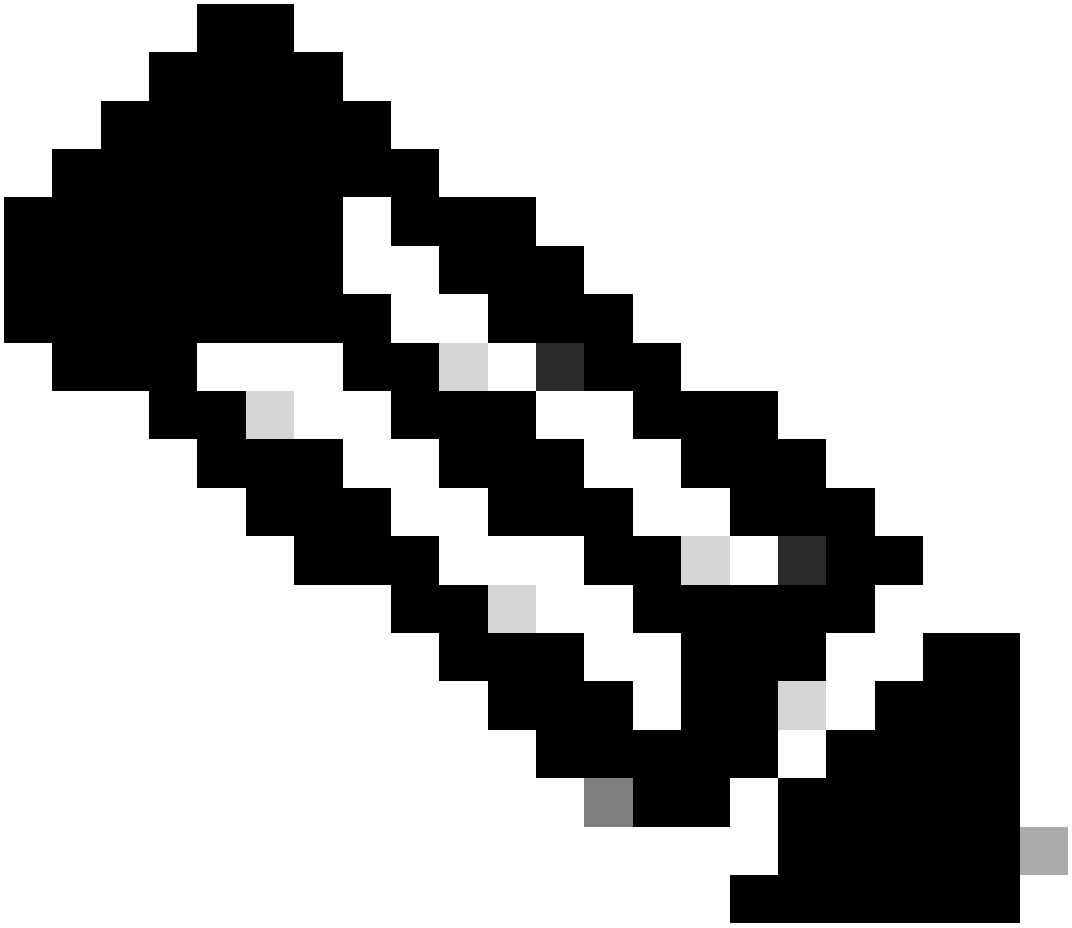


雙堆疊無線客戶端到雙堆疊有線客戶端資料包流

使用封包擷取深入瞭解此程式，並參閱映像瞭解IP位址和MAC位址詳細資訊。注意：此設定使用兩個雙協定棧客戶端，它們通過相同的接入點連線，但對映為不同的IPv6子網(SSID)。

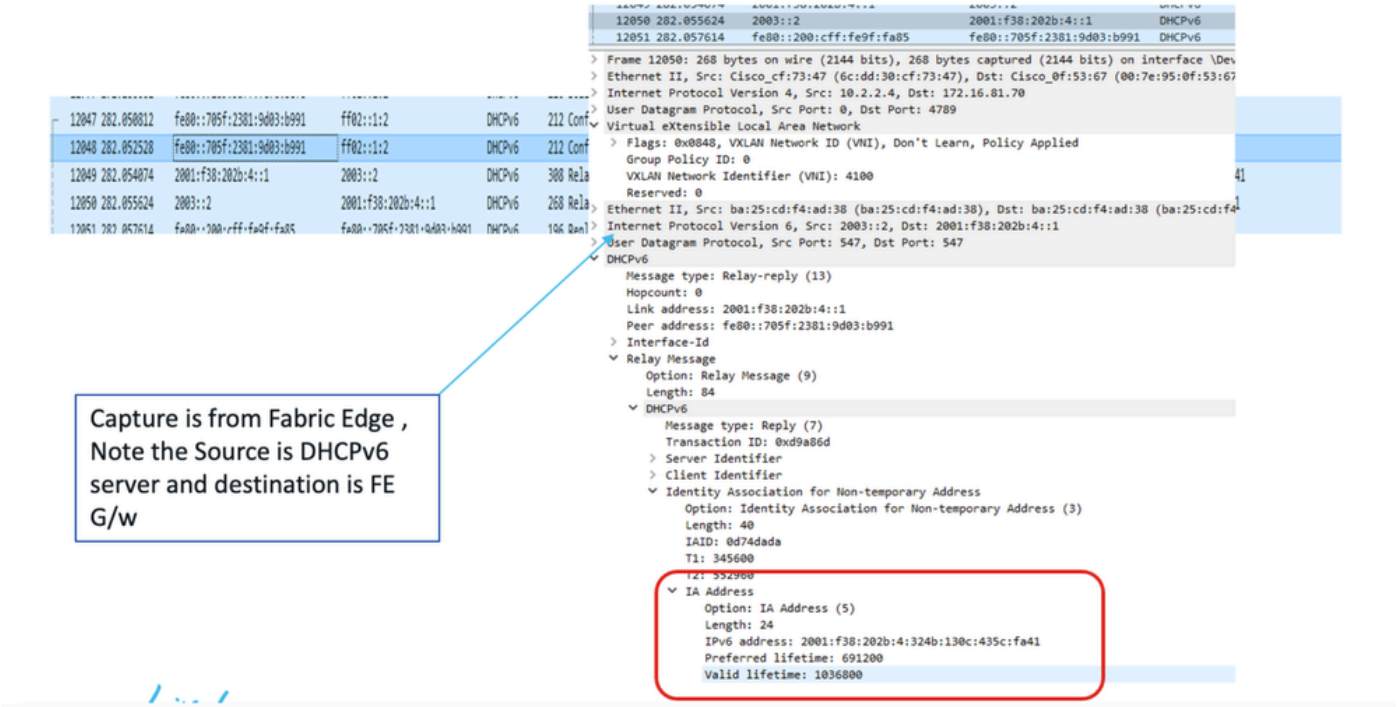


示例SD-Access交換矩陣網路IP地址和MAC地址詳細資訊



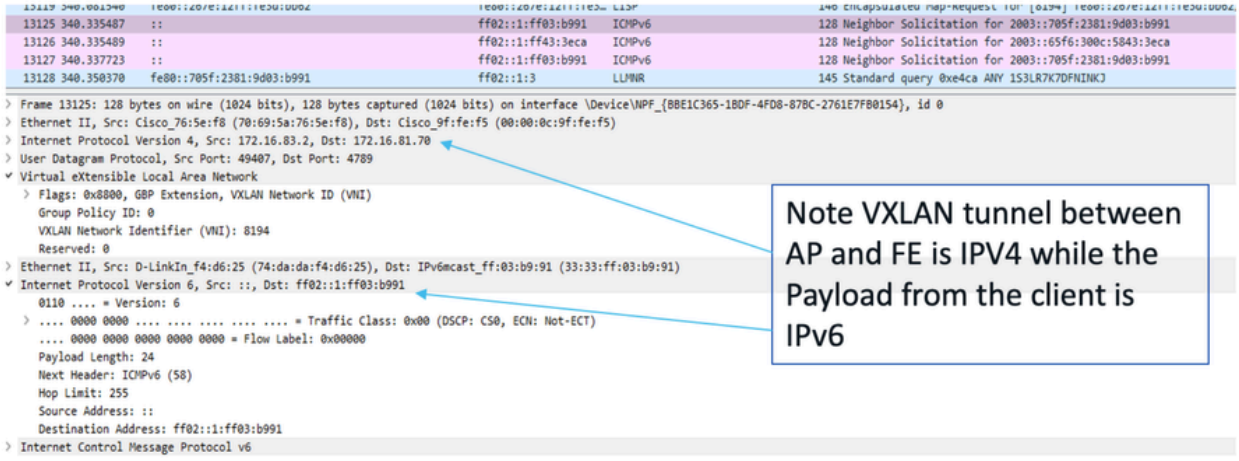
附註：對於交換矩陣之外的任何IPv6通訊（例如DHCP/DNS），必須在邊界和非交換矩陣基礎設施之間啟用IPv6路由。

步驟1.客戶端驗證並從配置的方法獲取IPv6地址。



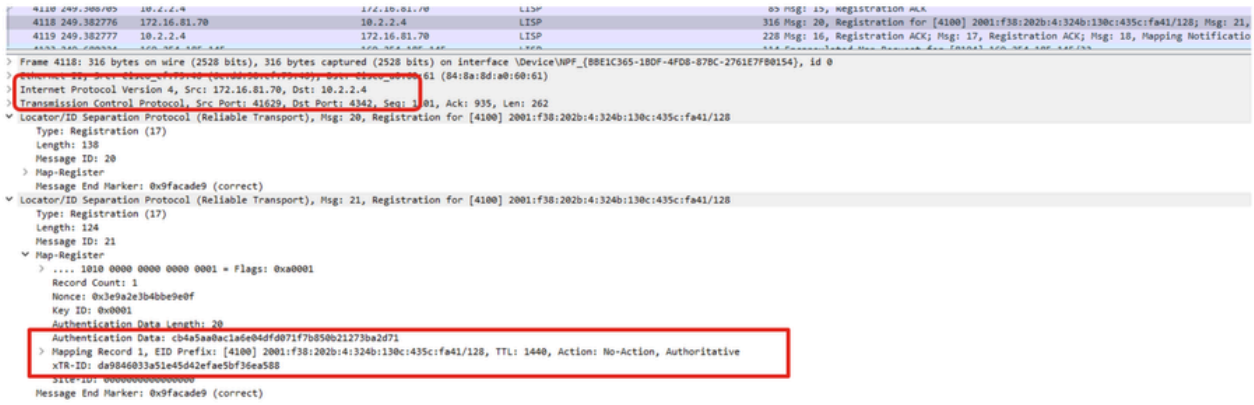
從DHCPv6伺服器到交換矩陣邊緣節點的資料包捕獲

步驟2.無線客戶端使用IPv6負載將802.11幀傳送到接入點。
步驟3.接入點刪除無線報頭並將資料包傳送到交換矩陣邊緣。這會使用基於IPv4的VXLAN通道標頭，因為存取點具有IPv4位址。



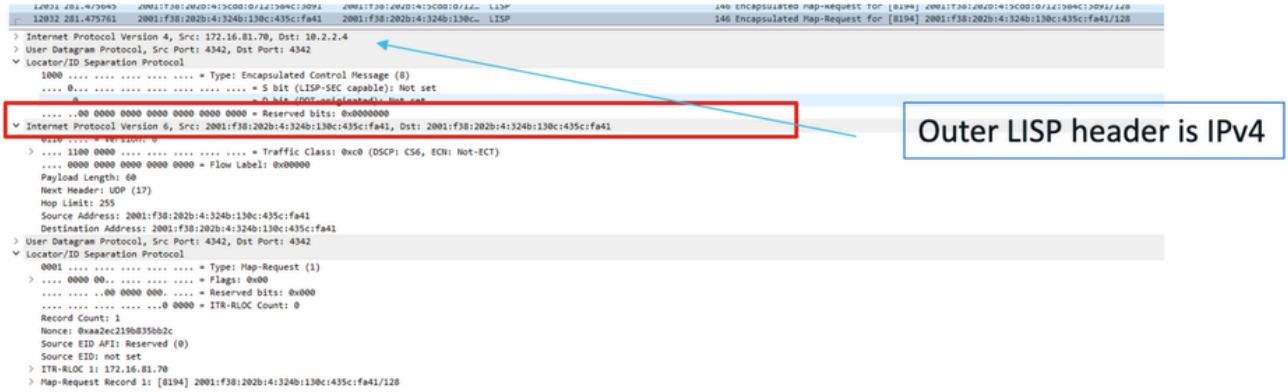
FE和AP之間VxLAN隧道的資料包捕獲

步驟3.1.交換矩陣邊緣向控制平面註冊IPv6客戶端。這使用包含內部IPv6客戶端詳細資訊的IPv4註冊方法。



用於FE註冊的資料包捕獲通過IPv6客戶端的控制平面

步驟3.2. FE將MAP請求傳送到控制平面以標識目標RLOC。



使用MAP註冊消息從FE到CP的資料包捕獲

Fabric Edge還維護已知IPv6客戶端的MAP快取，如下圖所示。

```
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#
```

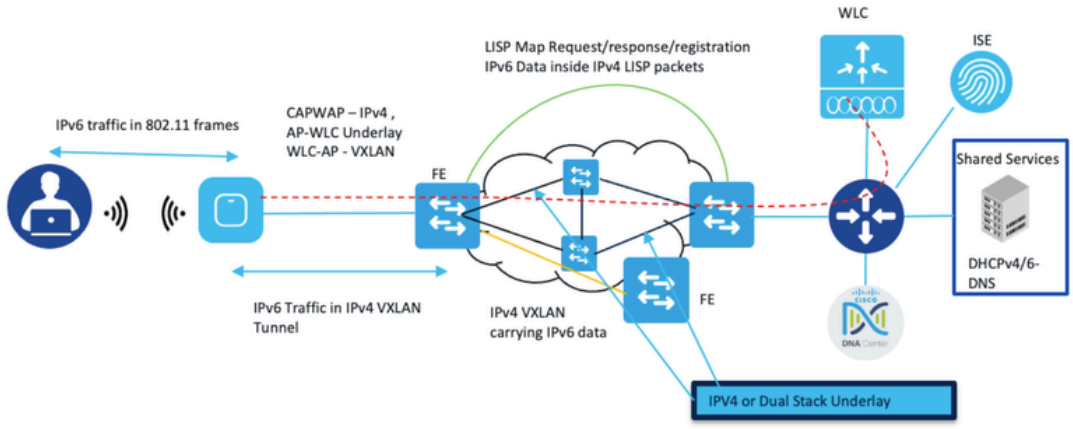
IPv6重疊對映快取資訊的交換矩陣邊緣螢幕輸出

步驟4.將資料包轉發到目標RLOC，其中的IPv4 VXLAN承載了原始IPv6負載。由於兩個客戶端都連線到同一個AP，因此IPv6 ping會採用此路徑。

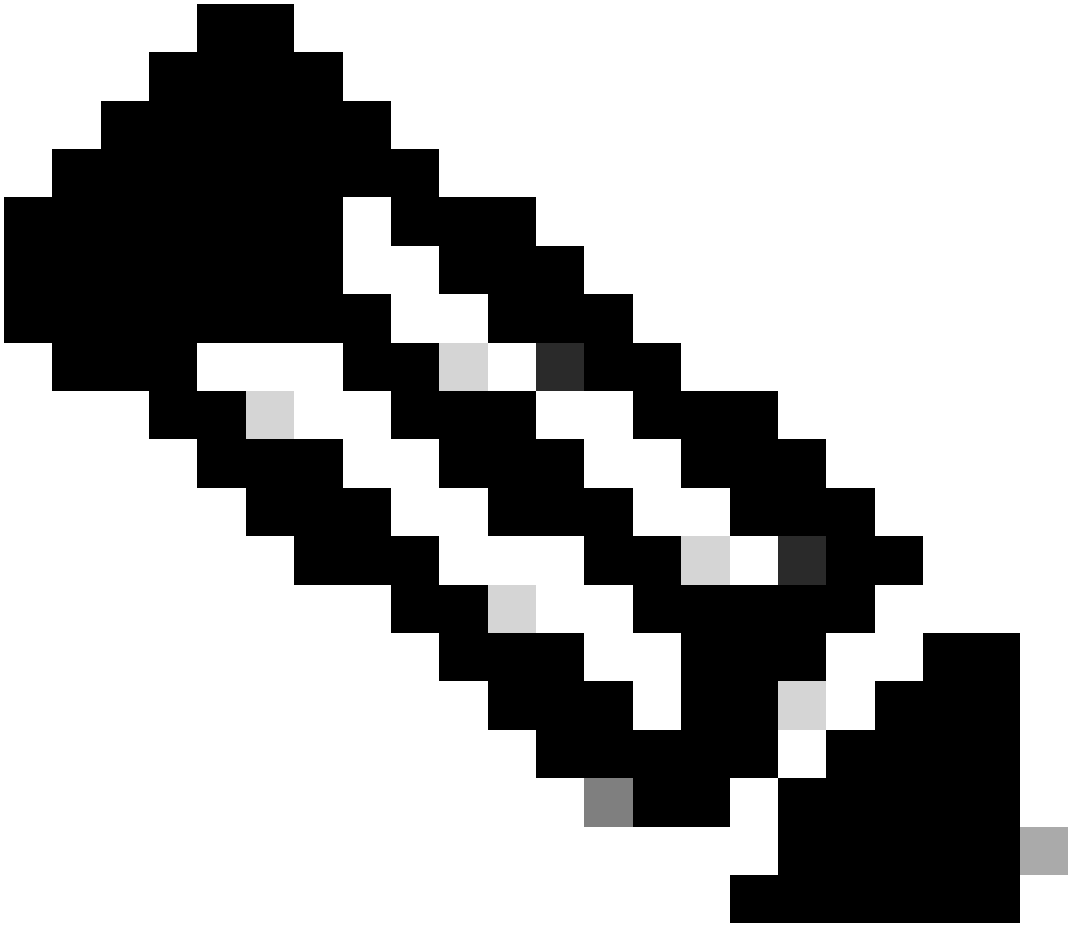
```
    71 3.392805     2001:f38:202b:4:324b:130c:435c:fa41    2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001, seq=148, hop limit=63
    72 3.392836     2001:f38:202b:4:324b:130c:435c:fa41    2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001,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

在註冊到同一AP的兩個無線客戶端之間進行IPv6 ping的資料包捕獲

此圖從無線客戶端的角度總結了IPv6通訊。



圖中從無線客戶端的角度總結了IPv6通訊



附註：由於ISE的限制，不支援通過Cisco Identity Services進行IPv6訪客訪問（Web門戶）。

依賴矩陣

必須注意Cisco SD-Access中的不同無線元件對IPv6的依賴性和支援。本圖中的表格總結了此功能矩陣。

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）

監控IPv6的控制平面

啟用IPv6後，您開始在對映伺服器(MS)/對映解析器(MR)伺服器中看到有關主機IPv6的其他條目。由於主機可以有多個IPv6 IP地址，您的MS/MR查詢表包含所有IP地址的條目。這會與已經存在的IPv4表結合使用。
您必須登入裝置CLI並發出這些命令以檢查所有條目。

```
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
```

您還可以通過保證檢查有關主機IPv6的詳細資訊。

Cisco SD-Access中的IPv6 QoS實施

當前的Cisco DNA Center版本（高達2.3.x）不支援IPv6 QoS應用策略自動化。但是，使用者可以手動建立IPv6有線和無線模板，並將QoS模板推入交換矩陣邊緣節點。由於DNA Center在應用後在所有物理介面上自動執行IPv4 QoS策略，因此可以通過模板在「class-default」之前手動插入一個類對映(匹配IPv6訪問控制清單(ACL))。

以下是與DNA Center生成的策略配置整合的有線支援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故障與IPv4非常相似，您始終可以使用帶有不同關鍵字選項的相同命令來實現相同的目標。此處顯示一些常用於對SD-Access進行故障排除的命令。

```
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
```

從邊界節點檢查重疊DHCPv6伺服器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設計快速常見問題解答

問：思科軟體定義網路是否支援底層網路和重疊網路的IPv6?
A.編寫本檔案時，目前的版本(2.3.x)僅支援重疊專案。

問：Cisco SDN是否支援有線和無線客戶端的本機IPv6?
是。這要求在DNA中心中建立雙堆疊池，而IPv4是虛擬池，因為客戶端禁用IPv4 DHCP請求，且僅提供IPv6 DHCP或SLAAC地址。

問：我的思科SD接入交換矩陣中是否可以擁有僅限於IPv6的本機園區網路？
A.當前版本（最高2.3.x）不適用。 它已經在規劃圖上了。

問：Cisco SD-Access是否支援L2 IPv6轉接？
目前還沒有。僅支援L2 IPv4切換和/或L3 Dual-Stack切換。

問：Cisco SD-Access是否支援用於IPv6的組播？
答：是，僅支援頭端複製組播的重疊IPv6。尚未支援本地IPv6組播。

問：Cisco SD-Access Fabric Enabled Wireless是否支援雙堆疊中的訪客？
A.在Cisco IOS XE(Cat9800)WLC中尚未支援。AireOS WLC通過變通方法受支援。有關變通方法實施的詳細資訊，請聯絡思科客戶體驗團隊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。