Implementazione di IPv6 nell'accesso definito dal software

Sommario

Introduzione

Questo documento descrive come implementare IPv6 in Cisco® Software-Defined Access (SD-Access).

Premesse

Il protocollo IPv4 è stato rilasciato nel 1983 ed è ancora utilizzato per la maggior parte del traffico Internet. L'indirizzamento IPv4 a 32 bit ha consentito oltre 4 miliardi di combinazioni uniche. Tuttavia, a causa dell'aumento del numero di client connessi a Internet, si registra una carenza di indirizzi IPv4 univoci. Negli anni '90, l'esaurimento degli indirizzi IPv4 è diventato inevitabile.
In previsione di questo, Internet Engineering Taskforce ha introdotto lo standard IPv6. IPv6 utilizza 128 bit e offre 340 indirizzi IP univoci senza decimali, più che sufficienti per soddisfare la necessità di dispositivi connessi in crescita. Poiché sempre più dispositivi end-point moderni supportano sia il doppio stack che il singolo stack IPv6, è fondamentale che qualsiasi organizzazione sia pronta all'adozione di IPv6. Ciò significa che l'intera infrastruttura deve essere pronta per IPv6. Cisco SD-Access rappresenta l'evoluzione dai progetti di campus tradizionali alle reti che implementano

direttamente le finalità di un'organizzazione. Software Defined Networks di Cisco è ora pronto per integrare dispositivi dual-stack (dispositivi IPv6).

Una delle principali sfide per qualsiasi organizzazione nell'adozione di IPV6 è rappresentata dalla gestione delle modifiche e dalle complessità associate alla migrazione dei sistemi IPv4 legacy a IPv6. Questo documento tratta tutti i dettagli relativi al supporto delle funzionalità IPv6 su SDN Cisco, strategia e punti critici, di cui è necessario tenere conto quando si adotta IPv6 con reti Cisco definite dal software.

Ad agosto 2019, Cisco Digital Network Architecture (DNA) Center versione 1.3 è stato introdotto per la prima volta con il supporto di IPv6. In questa versione, la rete del campus Cisco SD-Access supporta l'indirizzo IP dell'host con client cablati e wireless in IPv4, IPv6 o IPv4v6 Dual-stack dalla rete del fabric di sovrapposizione. La soluzione è quella di evolversi continuamente per introdurre nuove caratteristiche e funzionalità che possano essere facilmente integrate nell'IPv6 per qualsiasi azienda.

Accesso SD Cisco con architettura IPv6

La tecnologia fabric, parte integrante di SD-Access, fornisce alle reti di campus cablate e wireless sovrapposizioni programmabili e virtualizzazione di rete facile da installare, che consentono a una rete fisica di ospitare una o più reti logiche per soddisfare le finalità di progettazione. Oltre alla virtualizzazione della rete, la tecnologia fabric nella rete del campus migliora il controllo delle comunicazioni, fornendo segmentazione definita dal software e l'applicazione di policy in base all'identità dell'utente e all'appartenenza ai gruppi. L'intera soluzione SDN Cisco viene eseguita sul DNA del fabric. È quindi fondamentale comprendere ogni pilastro della soluzione rispetto al supporto IPv6.

- Underlay - La funzionalità IPv6 per la sovrimpressione ha una dipendenza dalla sovrimpressione, in quanto la sovrimpressione IPv6 utilizza l'indirizzamento IP sottostante IPv4 per creare il control plane Locator/ID Separation Protocol (LISP) e i tunnel del data plane VXLAN (Virtual Extensible LAN). È sempre possibile abilitare il dual-stack per il protocollo di routing dell'overlay. Solo il LISP di overlay di accesso SD dipende dal routing IPv4.
- Overlay - Quando si tratta di overlay, SD-Access supporta sia endpoint cablati che wireless solo IPv6. Il traffico IPv6 è incapsulato nell'intestazione IPv4 e VXLAN all'interno del fabric SD-Access finché non raggiungono i nodi di confine del fabric. I nodi di confine della struttura decapsulano l'intestazione IPv4 e VXLAN, che da allora segue il normale processo di routing unicast IPv6.
- Nodi Control Plane: il nodo Control Plane è configurato per consentire la registrazione nel relativo database di mapping di tutte le subnet host IPv6 e delle route host /128 all'interno degli intervalli di subnet.
- Nodi di confine - Sui nodi di confine, il peering BGP IPv6 con dispositivi di fusione è abilitato. Il nodo di bordo decapsula l'intestazione IPv4 dal traffico in uscita dell'infrastruttura, mentre il traffico IPv6 in entrata viene incapsulato con l'intestazione IPv4 anche dai nodi di bordo.
- Fabric Edge: tutte le interfacce virtuali commutate (SVI) configurate in Fabric Edge devono

essere IPv6. Questa configurazione viene sottoposta a push dal DNA Center Controller.

- Cisco DNA Center - Le interfacce fisiche di Cisco DNA Center non supportano la configurazione a doppio stack al momento della pubblicazione del presente documento. Può essere installato solo in un singolo stack con IPv4 o IPv6 solo nelle interfacce di gestione e/o aziendali di DNA Center.
- Client - Cisco SD-Access supporta lo stack doppio (IPv4 e IPv6) o singolo stack sia IPv4 che IPv6. Tuttavia, nel caso di uno stack singolo IPv6, DNA Center richiede ancora di creare un pool di stack doppio per supportare un client solo IPv6. L'indirizzo IPv4 nel pool a doppio stack è un indirizzo fittizio solo come l'indirizzo IPv6 che il client deve disattivare.

Architettura di overlay IPv6 in Cisco Software-Defined Access.

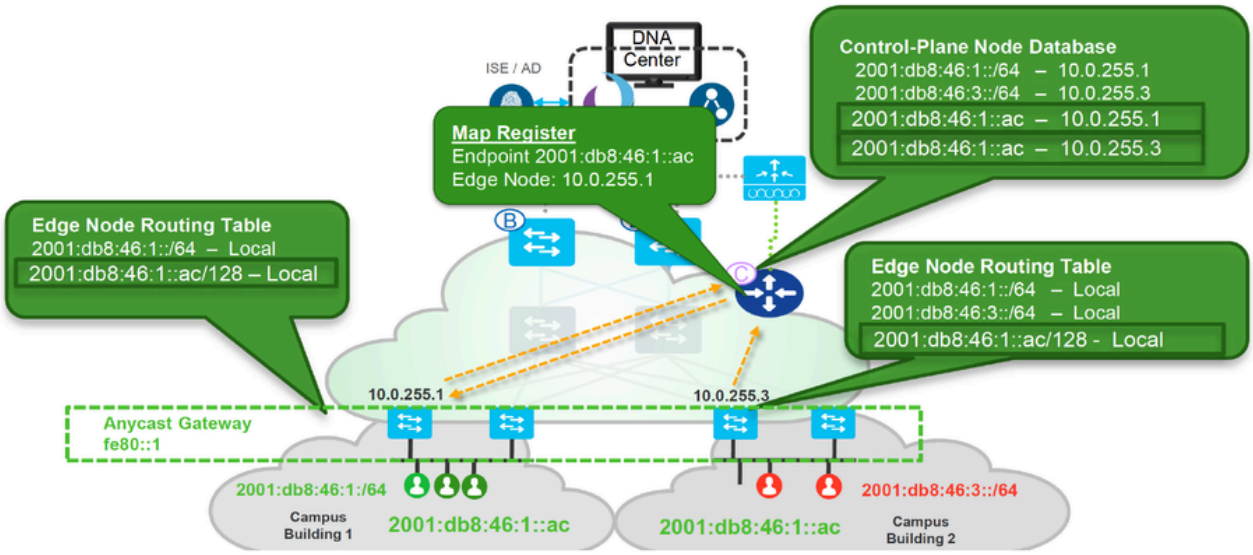


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

Architettura di overlay IPv6

Abilita IPv6 con Cisco DNA-Center

Per abilitare il pool IPv6 in Cisco DNA Center, è possibile procedere in due modi:
1. Creare un nuovo pool IPv4/v6 a doppio stack - greenfield
2. Modificare IPv6 nel pool IPv4 già esistente - migrazione brownfield

La versione corrente (fino a 2.3.x) di DNA Center non supporta IPv6. Solo un pool, se l'utente prevede di supportare un client solo indirizzo IPv6 singolo/nativo. È necessario associare un indirizzo IPv4 fittizio al pool IPv6. Tenere presente che dal pool IPv4 distribuito già esistente con un sito associato e modificare il pool con un indirizzo IPv6. DNA Center fornisce l'opzione di migrazione per SD-Access Fabric che richiede all'utente di effettuare nuovamente il provisioning del fabric per quel sito. Un indicatore di avviso viene visualizzato nell'infrastruttura a cui appartiene

il sito e indica che l'infrastruttura deve essere riconfigurata. Per esempi, vedere le seguenti immagini:

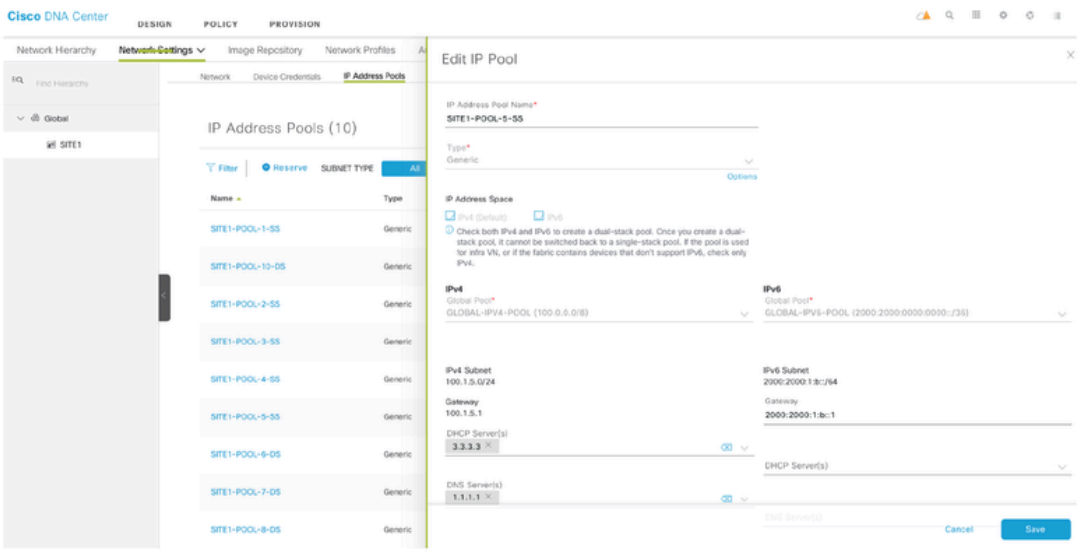


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

Aggiornamento di un singolo pool IPv4 a un pool a doppio stack modificando l'opzione del pool IPv4

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

L'infrastruttura dispone di un indicatore di avviso che deve 'riconfigurare l'infrastruttura'

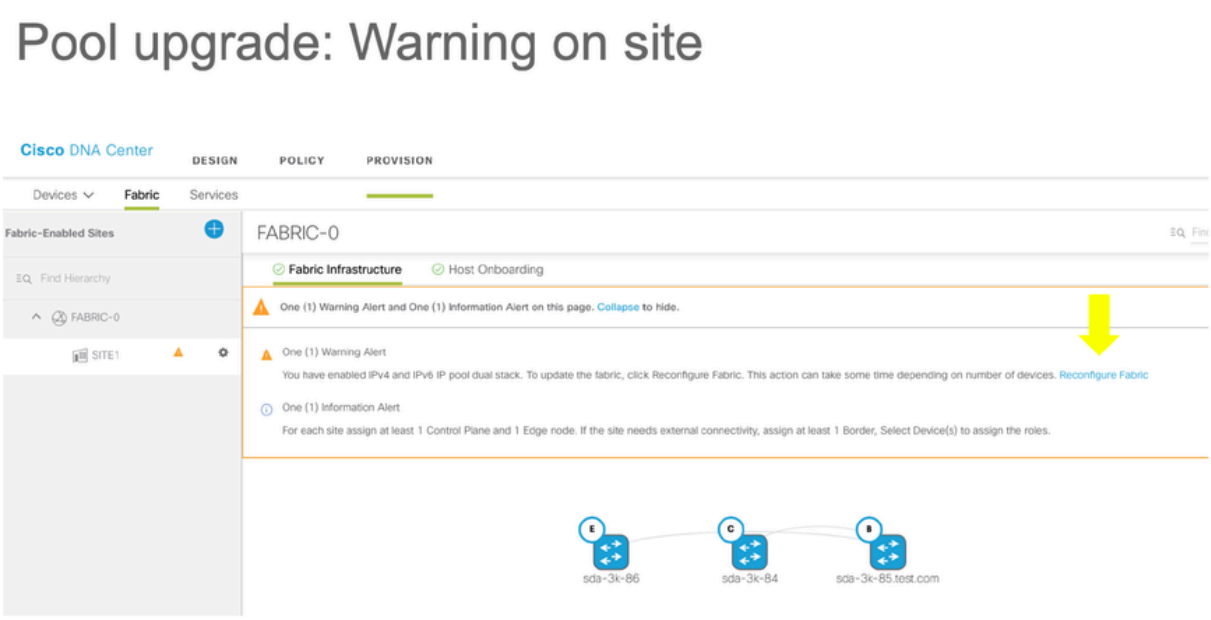


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

Per rendere effettiva la configurazione a doppio stack come parte del processo di migrazione, l'utente deve fare clic su "reconfigure fabric" per effettuare il reprovisioning automatico dei nodi fabric

Considerazioni sulla progettazione con IPv6 in Cisco SD-Access

Anche se per i client Cisco SD-Access possono essere eseguiti con impostazioni di rete a doppio stack o solo IPv6, l'attuale implementazione del fabric SD-Access con DNA Center Switch (SW) versione fino alla 2.3.x.x ha alcune considerazioni sull'implementazione di IPv6.

- Cisco SD-Access supporta i protocolli di routing underlay IPv4. Pertanto, il traffico del client IPv6 viene trasportato quando viene incapsulato nelle intestazioni IPv4. Questo è un requisito per l'attuale distribuzione del software LISP. Ma non significa che l'underlay non possa abilitare il protocollo di routing IPv6, solo il LISP di overlay SD-Access non funziona in base alla sua dipendenza.
- Il multicast nativo IPv6 non è supportato perché l'infrastruttura sottostante può essere solo IPv4 al momento.
- La tecnologia wireless guest può essere eseguita solo con uno stack doppio. A causa della versione corrente di Identity Services Engine (ISE) (ad esempio, fino alla versione 3.2), il portale guest IPv6 non è supportato, pertanto un client guest solo IPv6 non sarà in grado di ottenere l'autenticazione.
- L'automazione dei criteri QoS per applicazioni IPv6 non è supportata nella versione corrente di DNA Center. In questo documento vengono descritti i passaggi necessari per implementare QoS IPv6 per client a doppio stack cablati e wireless in Cisco SD-Access, implementato per uno degli utenti su larga scala.
- La funzionalità di limitazione della velocità dei client wireless per il traffico a valle e a monte per SSID (Service Set Identifier) o per client in base ai criteri è supportata per IPv4

(TCP/UDP) e IPv6 (solo TCP). La limitazione della velocità UDP IPv6 non è ancora supportata.
- Il pool IPv4 può essere aggiornato a pool a doppio stack. Tuttavia, non è possibile effettuare il downgrade di un pool a doppio stack a un pool IPv4. Se si desidera rimuovere il pool di due stack dal pool di un singolo stack IPv4, è necessario rilasciare l'intero pool di due stack.
- L'IPv6 singolo non è ancora supportato, mentre è possibile creare solo pool IPv4 o a doppio stack nel DNA Center corrente.
- La piattaforma Cisco IOS® XE richiede almeno la versione software 16.9.2 e successive.
- IPv6 Guest wireless non è ancora supportato nelle piattaforme Cisco IOS XE, mentre AireOS (8.10.105.0+) supporta una soluzione alternativa.
- Non è possibile assegnare un pool a doppio stack nell'INFRA_VN in cui è possibile assegnare solo un punto di accesso (AP) o un pool di nodi estesi.
- L'automazione LAN non supporta ancora IPv6.

Oltre alle limitazioni descritte in precedenza, quando si progetta un'infrastruttura ad accesso SD con IPv6 abilitato, è sempre necessario tenere presente la scalabilità di ogni componente dell'infrastruttura. Se un endpoint dispone di più indirizzi IPv4 o IPv6, ogni indirizzo viene conteggiato come una singola voce.

Le voci relative all'host dell'infrastruttura includono punti di accesso e nodi classici e nodi estesi in base a criteri.

Ulteriori considerazioni sulla scala dei nodi dei bordi:

Le voci /32 (IPv4) o /128 (IPv6) vengono utilizzate quando il nodo di confine inoltra il traffico dall'esterno dell'infrastruttura a un host nell'infrastruttura.

Per tutti gli switch ad eccezione degli switch Cisco Catalyst serie 9500 ad alte prestazioni e degli switch Cisco Catalyst serie 9600:

- IPv4 utilizza una voce TCAM (Content Addressable Memory) ternaria (voci host fabric) per ogni indirizzo IP IP IPv4.
- IPv6 utilizza due voci TCAM (voci host fabric) per ogni indirizzo IP IP IPv6.

Per gli switch Cisco Catalyst serie 9500 ad alte prestazioni e gli switch Cisco Catalyst serie 9600:

- IPv4 utilizza una voce TCAM (voci host fabric) per ogni indirizzo IP IP IPv4.
- IPv6 utilizza una voce TCAM (voci host fabric) per ogni indirizzo IP IP IPv6.

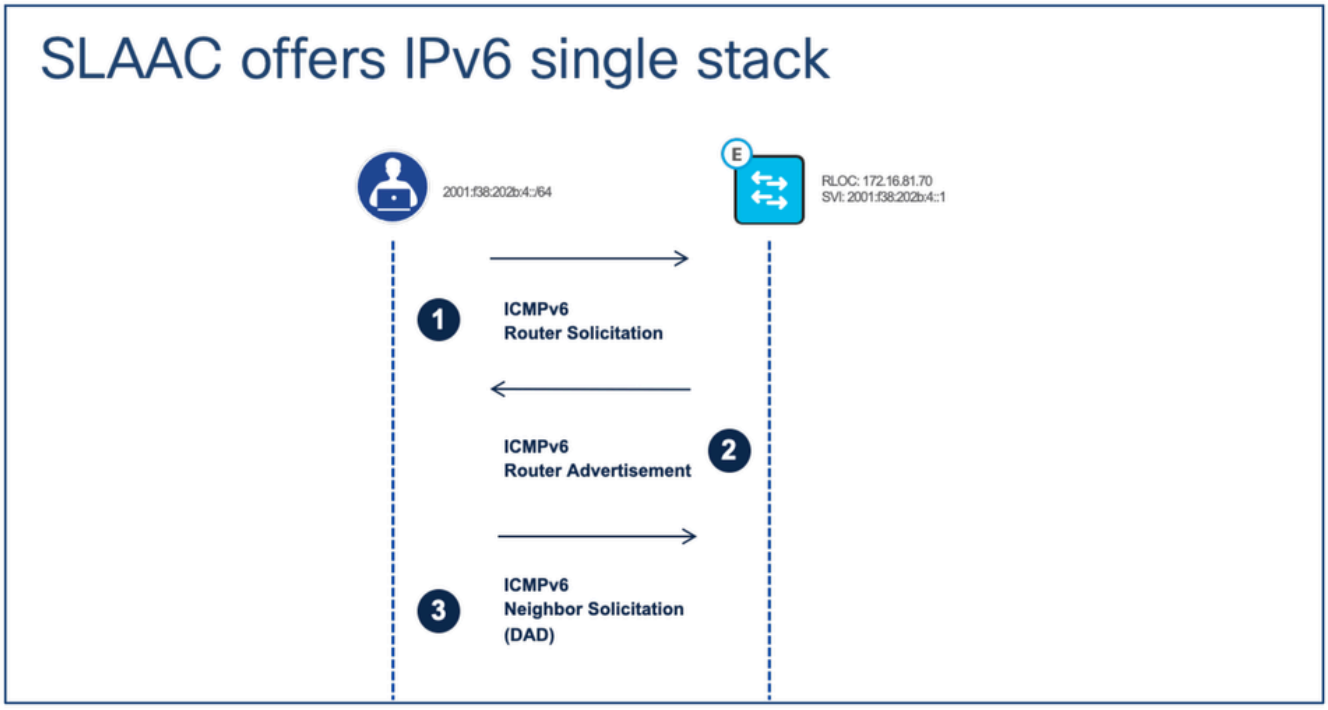
Alcuni endpoint non supportano DHCPv6, ad esempio gli smartphone basati su sistema operativo Android che si basano sulla configurazione automatica degli indirizzi senza stato (SLAAC, Stateless Address Autoconfiguration) per ottenere indirizzi IPv6. Un singolo endpoint può avere più di due indirizzi IPv6. Questo comportamento consuma più risorse hardware su ciascun nodo di fabric, in particolare per i nodi di bordo e di controllo dell'infrastruttura. Ad esempio, ogni volta che il nodo di confine desidera inviare il traffico ai nodi periferici di un endpoint, installa un percorso host nella voce TCAM e masterizza una voce di adiacenza VXLAN nel TCAM hardware (HW).

Connessioni client cablate e wireless e flussi di chiamate

Una volta connesso il client al Fabric Edge, esistono diversi modi in cui ottiene gli indirizzi IPv6. In questa sezione viene descritto il modo più comune per indirizzare gli indirizzi IPv6 dei client, ovvero SLAAC e DHCPv6.

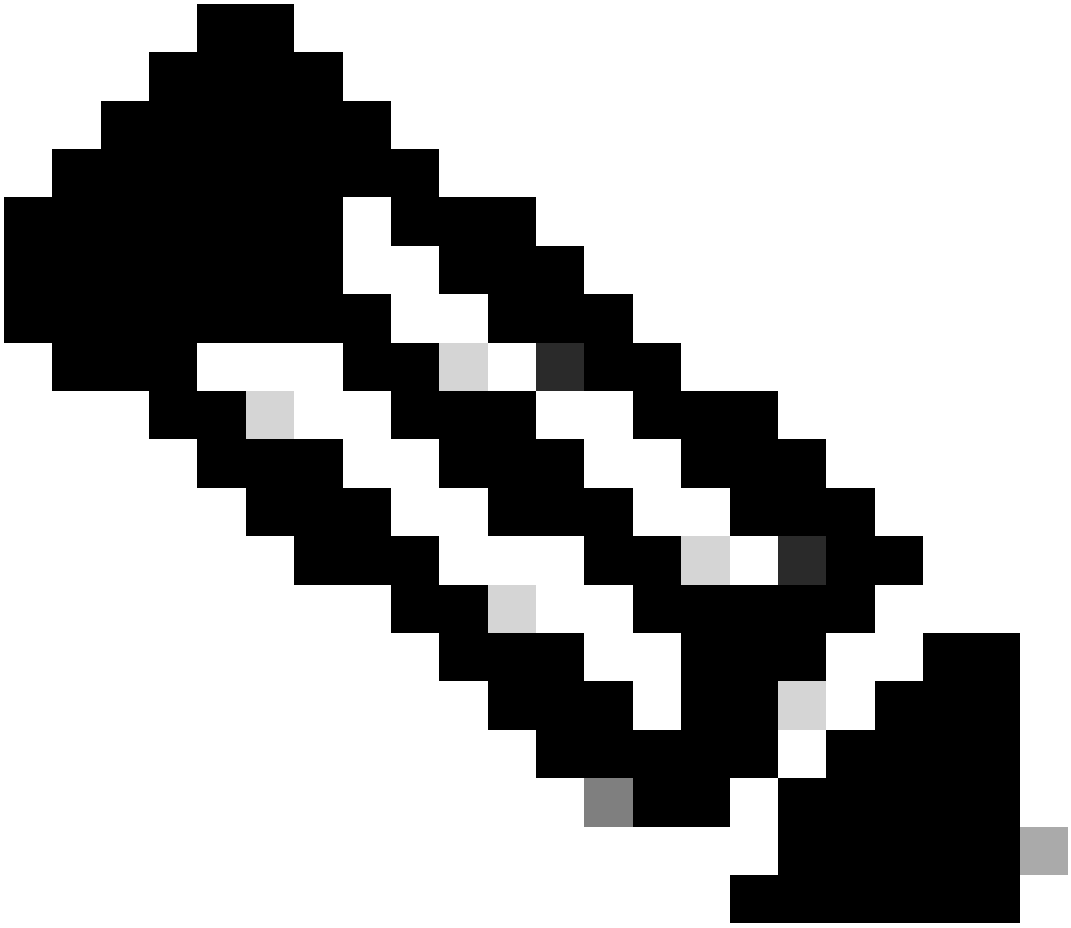
Assegnazione indirizzo IPv6 - SLAAC

Lo SLAAC in SDA (Software-Defined Access) non è diverso dal flusso di processo SLAAC standard. Per il corretto funzionamento di SLAAC, è necessario configurare il client IPv6 con un indirizzo locale del collegamento nell'interfaccia. La modalità di configurazione automatica del client con l'indirizzo locale del collegamento non rientra nell'ambito di questo documento.



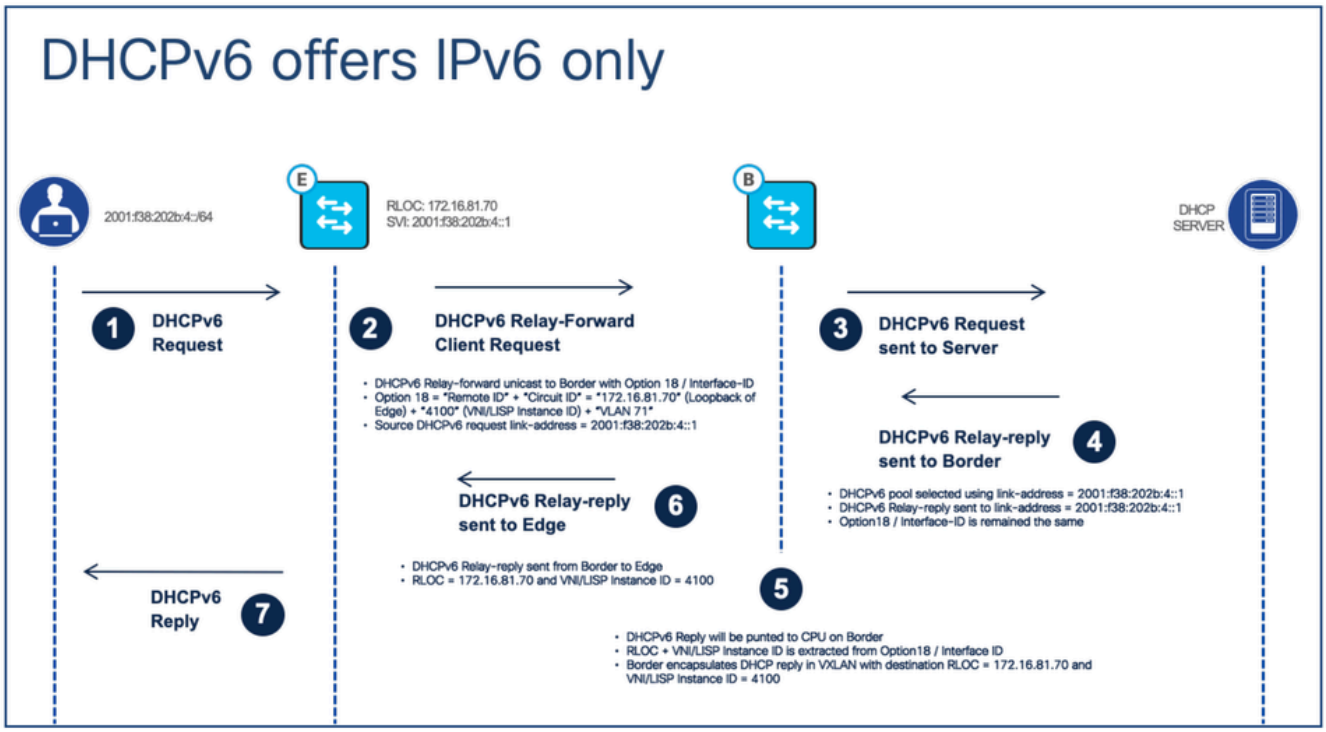
Assegnazione indirizzo IPv6 - SLAAC

Descrizione flusso di chiamata:
Passaggio 1. Dopo aver configurato il client IPv6 con un indirizzo locale del collegamento IPv6, invia un messaggio ICMPv6 Router Request (RS) a Fabric Edge. Lo scopo di questo messaggio è ottenere il prefisso unicast globale del relativo segmento connesso.
Passaggio 2. Dopo aver ricevuto il messaggio RS, il lato dell'infrastruttura risponde con un messaggio di annuncio router ICMPv6 (RA) contenente il prefisso unicast IPv6 globale e la relativa lunghezza all'interno.
Passaggio 3. Dopo aver ricevuto il messaggio RSA, il client combina il prefisso unicast globale IPv6 con il relativo identificatore di interfaccia EUI-64 per generare il proprio indirizzo unicast globale IPv6 univoco e impostare il gateway sull'indirizzo locale del collegamento della SVI del lato dell'infrastruttura correlato al segmento del client. Il client invia quindi un messaggio ICMPv6 Neighbor Request per eseguire il rilevamento degli indirizzi duplicati (DAD, Duplicate Address Detection) per garantire l'univocità dell'indirizzo IPv6 ottenuto.



Nota: Tutti i messaggi relativi a SLAAC sono incapsulati con l'indirizzo locale del collegamento IPv6 SVI del client e il nodo dell'infrastruttura.

Assegnazione indirizzo IPv6 - DHCPv6

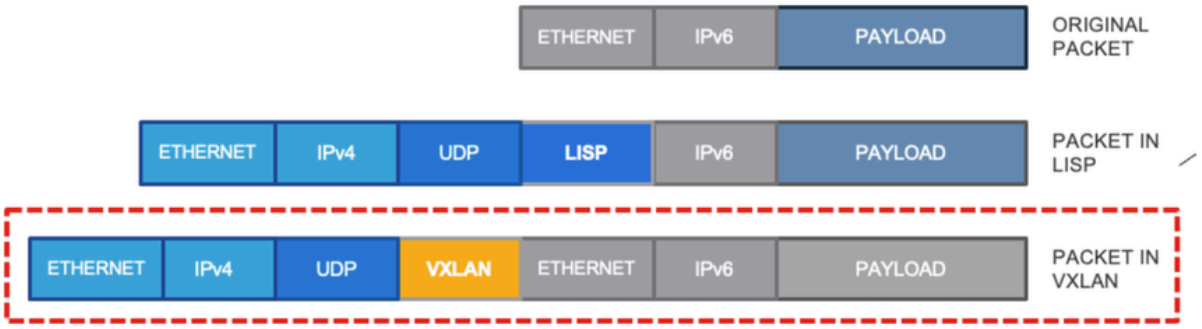


Assegnazione indirizzo IPv6 - DHCPv6

Descrizione flusso di chiamata:
Passaggio 1. Il client invia la richiesta DHCPv6 al perimetro dell'infrastruttura.
Passaggio 2. Quando il perimetro dell'infrastruttura riceve la richiesta DHCPv6, utilizzerà il messaggio di inoltro di inoltro DHCPv6 per trasmettere in unicast la richiesta al bordo dell'infrastruttura con l'opzione DHCPv6 18. Rispetto all'opzione DHCP 82, l'opzione DHCPv6 18 codifica insieme 'ID circuito' e 'ID remoto'. L'ID istanza/VNI del LISP, la funzionalità RLOC (IPv4 Routing Locator) e la VLAN dell'endpoint sono codificati all'interno.
Passaggio 3. Il bordo dell'infrastruttura decapsula l'intestazione VXLAN e invia in unicast il pacchetto DHCPv6 al server DHCPv6.
Passaggio 4. Il server DHCPv6 riceve il messaggio di inoltro, utilizza l'indirizzo del collegamento di origine (agente di inoltro DHCPv6/gateway client) del messaggio per scegliere il pool IPv6 per assegnare l'indirizzo IPv6. Inviare quindi il messaggio di risposta inoltro DHCPv6 all'indirizzo del gateway client. L'opzione 18 rimane invariata.
Passaggio 5. Quando il bordo dell'infrastruttura riceve il messaggio relay-reply, estrae l'istanza RLOC e LISP o il VNI dall'opzione 18. Il bordo dell'infrastruttura incapsula il messaggio relay-reply in VXLAN con una destinazione estratta dall'opzione 18.
Passaggio 6. Il bordo dell'infrastruttura invia il messaggio di risposta di inoltro DHCPv6 al bordo dell'infrastruttura a cui si connette il client.
Passaggio 7. Quando Fabric Edge riceve il messaggio di risposta di inoltro DHCPv6, decapsula l'intestazione VXLAN del messaggio e inoltra il messaggio al client. Il client conosce quindi l'indirizzo IPv6 assegnato.

Comunicazione IPv6 in Cisco SD-Access

La comunicazione IPv6 utilizza il control plane standard basato su LISP e i metodi di comunicazione Data plane basati su VXLAN. Con l'implementazione corrente in Cisco SD-Access LISP e VXLAN, l'intestazione IPv4 esterna viene utilizzata per trasportare i pacchetti IPv6 all'interno. Questa immagine acquisisce questo processo.



Intestazione IPv4 esterna contenente i pacchetti IPv6

Ciò significa che tutte le query LISP utilizzano il pacchetto nativo IPv4, mentre la tabella del nodo del control plane contiene dettagli sulla RLOC con indirizzi IP IPv6 e IPv4 dell'endpoint. Questo processo viene descritto in dettaglio nella sezione successiva dalla prospettiva di un endpoint wireless.

Comunicazione IPv6 wireless in Cisco SD-Access

La comunicazione wireless si basa su due componenti specifici: i punti di accesso e i controller LAN wireless, a parte i tipici componenti fabric Cisco SD-Access. I punti di accesso wireless creano un tunnel CAPWAP (Control and Provisioning of Wireless Access Point) con il controller WLC. Mentre il traffico client esiste sul perimetro della struttura, altre comunicazioni del control plane, che includono le statistiche della radio, vengono gestite dal WLC. Dal punto di vista IPv6, sia il WLC che l'access point devono avere gli indirizzi IPv4 e tutte le comunicazioni CAPWAP utilizzano questi indirizzi IPv4. Mentre il WLC e l'access point non fabric supportano la comunicazione IPv6, Cisco SD-Access utilizza l'IPv4 per tutte le comunicazioni che trasportano qualsiasi traffico IPv6 client all'interno dei pacchetti IPv4. Ciò significa che i pool AP assegnati nella rete VN ad infrarossi non possono essere mappati con pool IP a doppio stack e viene generato un errore se si tenta di eseguire questa mappatura. La comunicazione wireless all'interno di Cisco SDA può essere suddivisa in queste attività principali:

- Caricamento Access Point
- On-boarding client

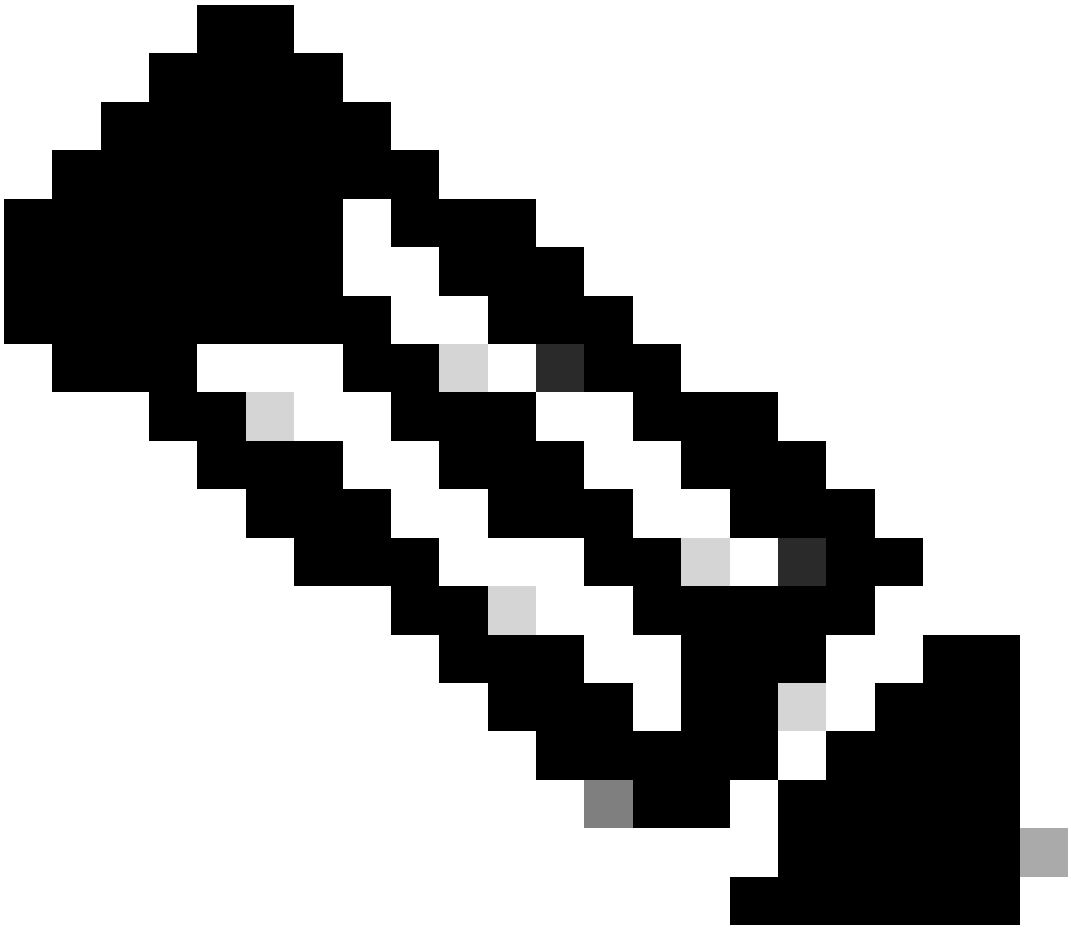
Osservare questi eventi da una prospettiva IPv6.

Caricamento Access Point

Questo processo rimane lo stesso per IPv6 e IPv4, in quanto sia WLC che AP includono indirizzi

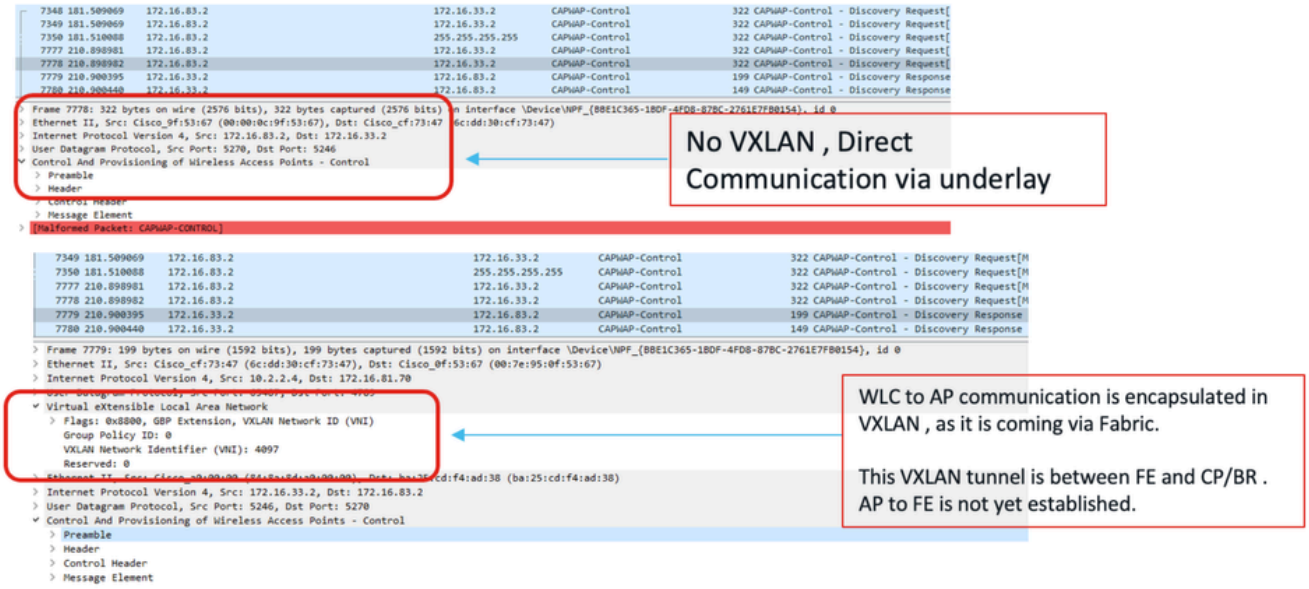
IPv4 e passaggi:
1. La porta Fabric Edge (FE) è configurata per l'access point integrato.
2. Il punto di accesso si connette alla porta FE e, tramite il punto di accesso CDP, notifica la presenza di FE (consentendo a FE di assegnare la VLAN corretta).
3. L'access point ottiene l'indirizzo IPv4 dal server DHCP e registra l'access point e aggiorna il Control Plane (nodo Control Plane (CP)) con i dettagli dell'access point.
4. L'access point viene aggiunto al WLC tramite metodi tradizionali (come l'opzione DHCP 43).
5. Il WLC verifica se l'access point è compatibile con Fabric ed esegue una query sul Control Plane per ottenere le informazioni sull'access point relativo alla ricezione (ad esempio, richiesta/risposta ricevuta).
6. La CP risponde al WLC con l'indirizzo IP della RLOC dell'AP.
7. Il WLC registra l'indirizzo MAC (Media Access Control) dell'access point in CP.
8. CP aggiorna il FE con i dettagli del WLC sull'AP (in questo modo FE avvia il tunnel VXLAN con l'AP).

FE elabora le informazioni e crea un tunnel VXLAN con punto di accesso. A questo punto, AP annuncia SSID abilitato per Fabric.



Nota: Se l'access point trasmette gli SSID non fabric e non trasmette l'SSID fabric, verificare la presenza del tunnel VXLAN tra il punto di accesso e il nodo Fabric Edge.

Inoltre, la comunicazione da AP a WLC avviene sempre tramite Underlay CAPWAP e tutte le comunicazioni da WLC a AP utilizzano VXLAN CAPWAP tramite overlay. Ciò significa che, se si catturano pacchetti che vanno da AP a WLC, viene visualizzato CAPWAP solo quando il traffico inverso ha un tunnel VXLAN. Vedere questo esempio per la comunicazione tra AP e WLC.



Acquisizione di pacchetti da AP a WLC (tunnel CAPWAP) rispetto a WLC a AP (tunnel VxLAN nel fabric)

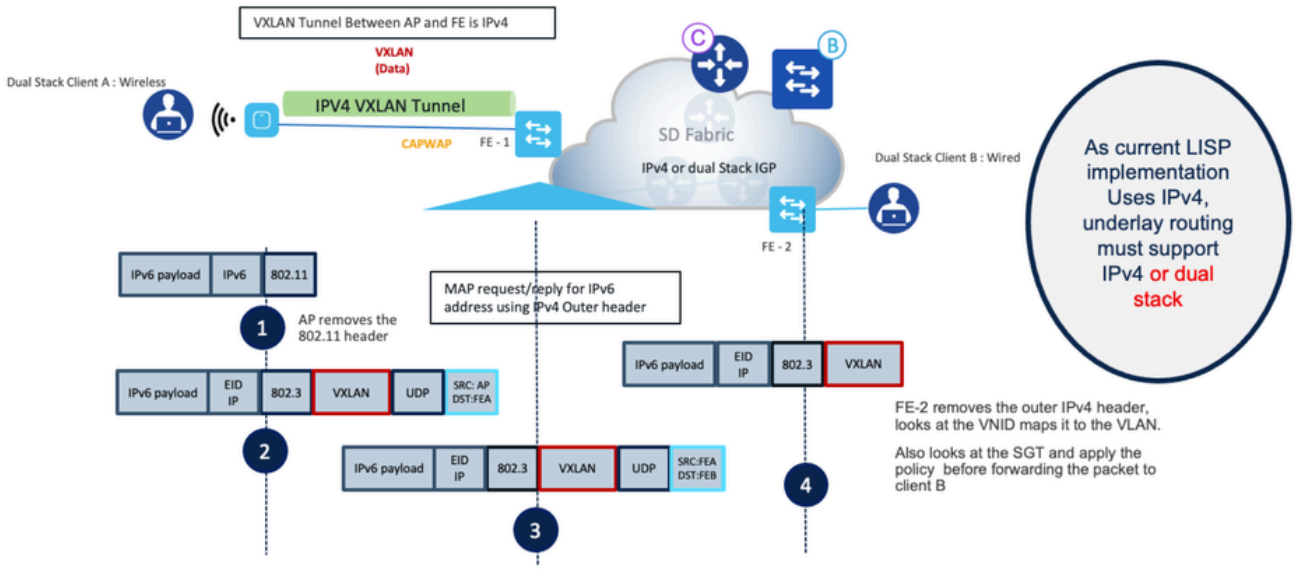
Caricamento client

Il processo di caricamento del client Dual-Stack/IPv6 rimane lo stesso, ma il client utilizza i metodi di assegnazione degli indirizzi IPv6 come SLAAC/DHCPv6 per ottenere gli indirizzi IPv6.
1. Il client si unisce all'infrastruttura e abilita SSID sull'access point.
2. Il WLC conosce l'AP RLOC.
3. Il client esegue l'autenticazione e il WLC registra i dettagli L2 del client con l'access point e gli aggiornamenti.
4. Il client avvia l'indirizzamento IPv6 dai metodi configurati - SLAAC/DHCPv6.
5. FE attiva la registrazione del client IPv6 nel database di rilevamento dell'host del provider di servizi terminal (HTDB). I punti di accesso a FE e i punti di accesso a FE per altre destinazioni utilizzano l'incapsulamento IPv6 VXLAN e LISP all'interno dei frame IPv4.

Comunicazione client-client con IPv6

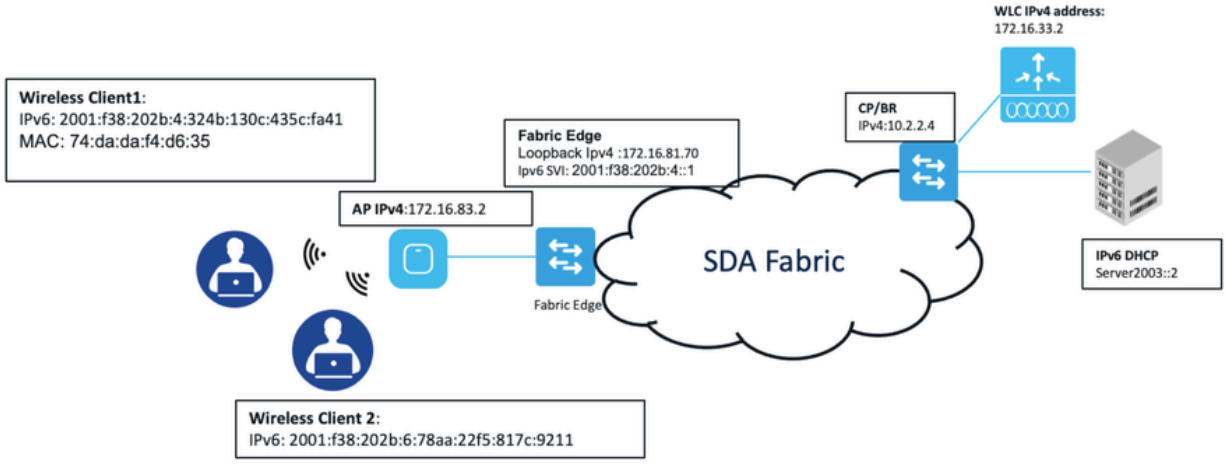
L'immagine riepiloga il processo di comunicazione del client wireless IPv6 con un altro client cablato IPv6. Si presuppone che il client sia autenticato e che l'indirizzo IPv6 sia stato ottenuto

tramite metodi configurati.
1. Il client invia i frame 802.11 all'access point con payload IPv6.
2. AP rimuove le intestazioni 802.11 e invia il payload IPv6 originale nel tunnel VXAN IPv4 al fabric Edge.
3. Fabric Edge utilizza la richiesta MAP (Message Access Protocol) per identificare la destinazione e invia il frame alla RLOC di destinazione con VXLAN IPv4.
4. Sullo switch di destinazione, l'intestazione VXLAN IPv4 viene rimossa e il pacchetto IPv6 viene inviato al client.

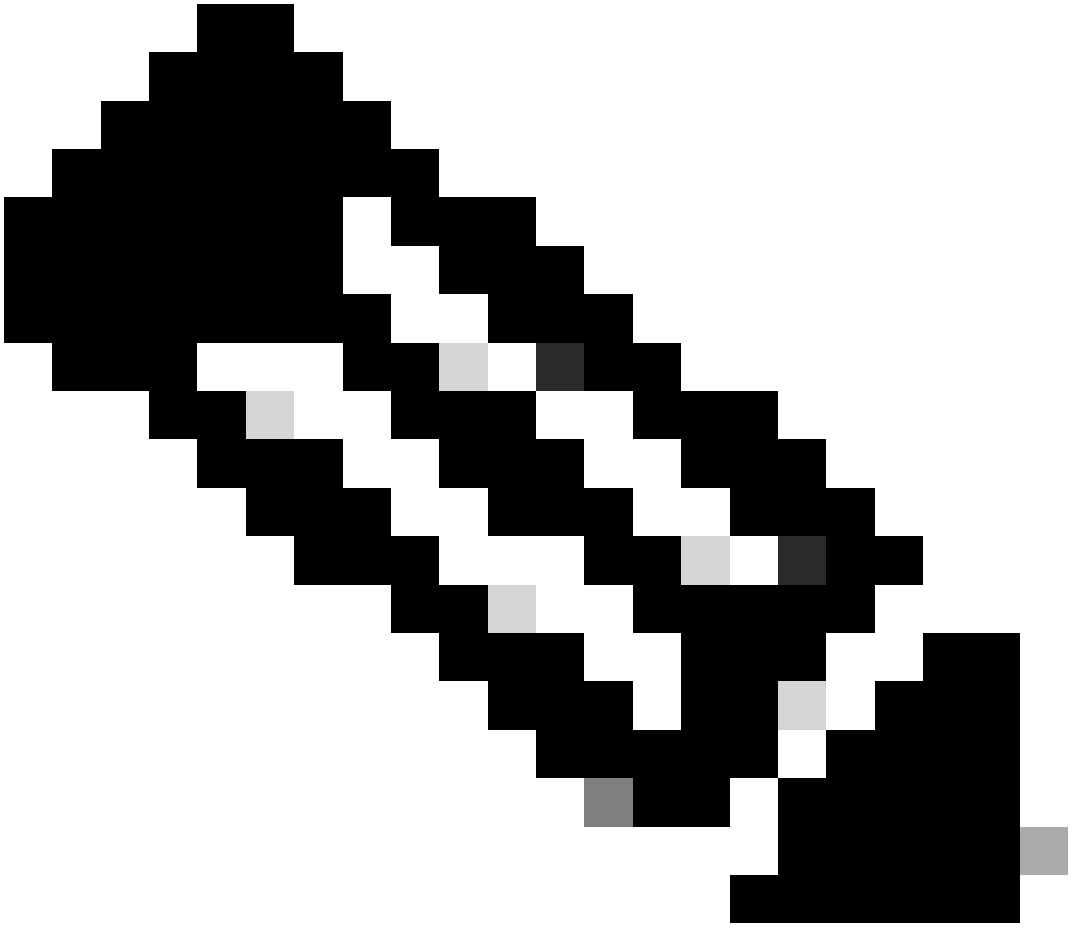


Flussi di pacchetti da client wireless a doppio stack a client cablati

Esaminare attentamente questo processo con le acquisizioni dei pacchetti e fare riferimento all'immagine per gli indirizzi IP e i dettagli dell'indirizzo MAC. Nota: questa installazione utilizza client Dual-Stack connessi con gli stessi punti di accesso ma mappati con subnet IPv6 (SSID) diverse.

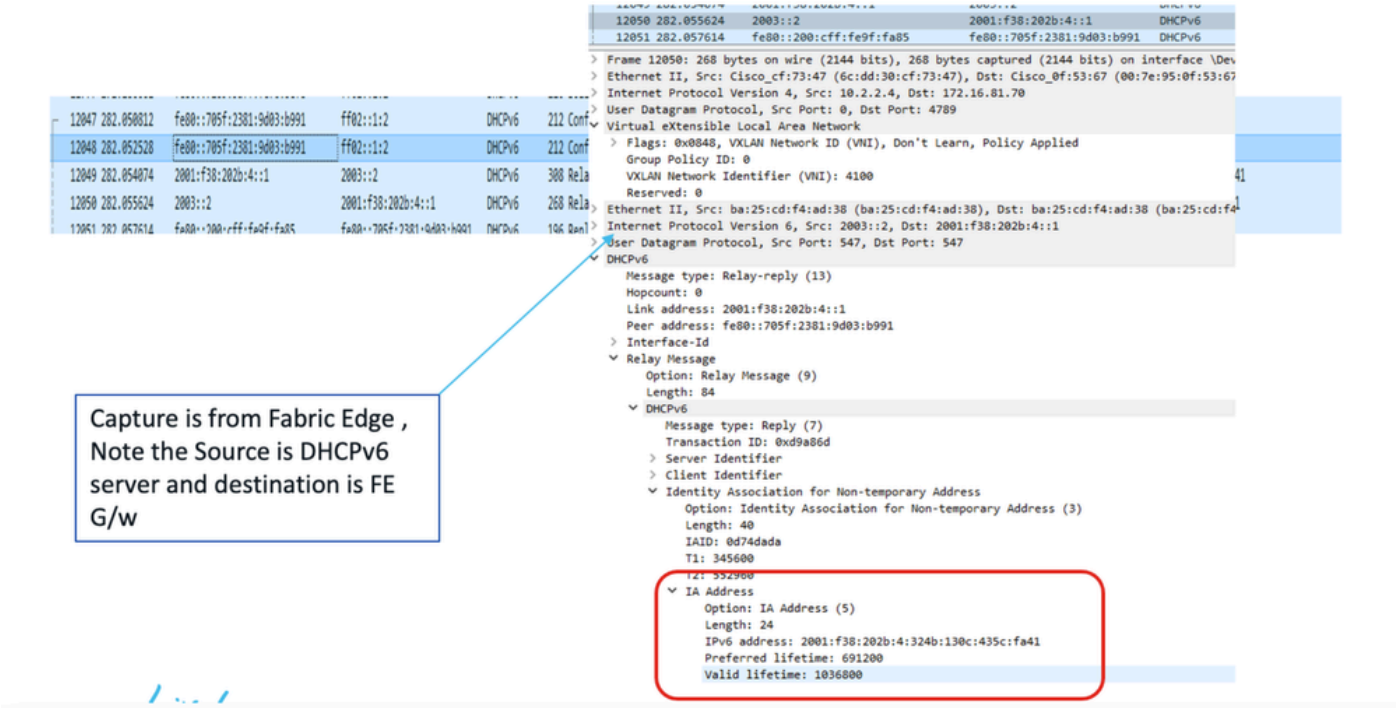


Dettagli sugli indirizzi IP e sugli indirizzi MAC di rete del fabric ad accesso SD di esempio



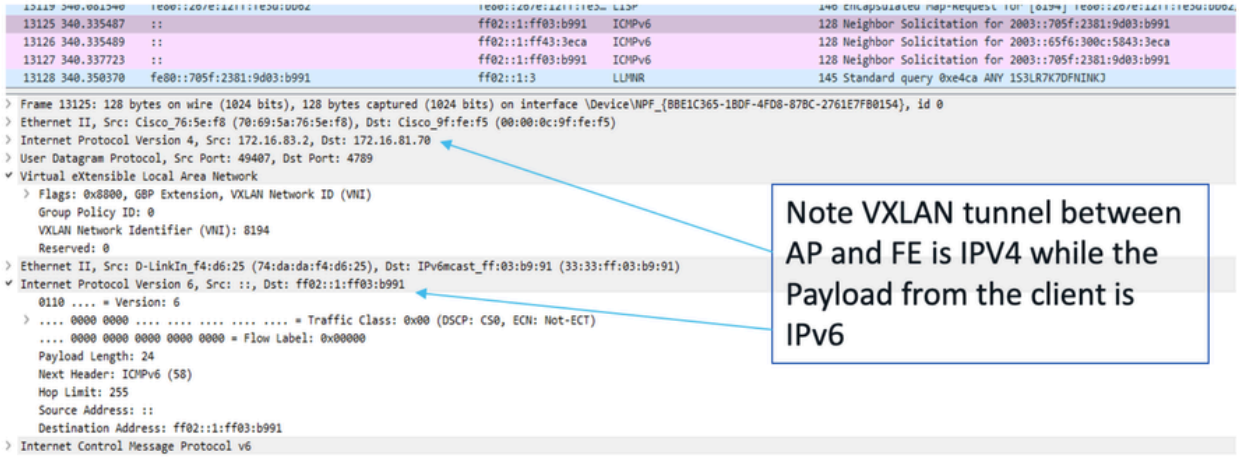
Nota: Per le comunicazioni IPv6 all'esterno dell'infrastruttura, ad esempio DHCP/DNS, è necessario abilitare il routing IPv6 tra l'infrastruttura di confine e quella non dell'infrastruttura.

Passaggio 1. Il client autentica e ottiene l'indirizzo IPv6 dai metodi configurati.



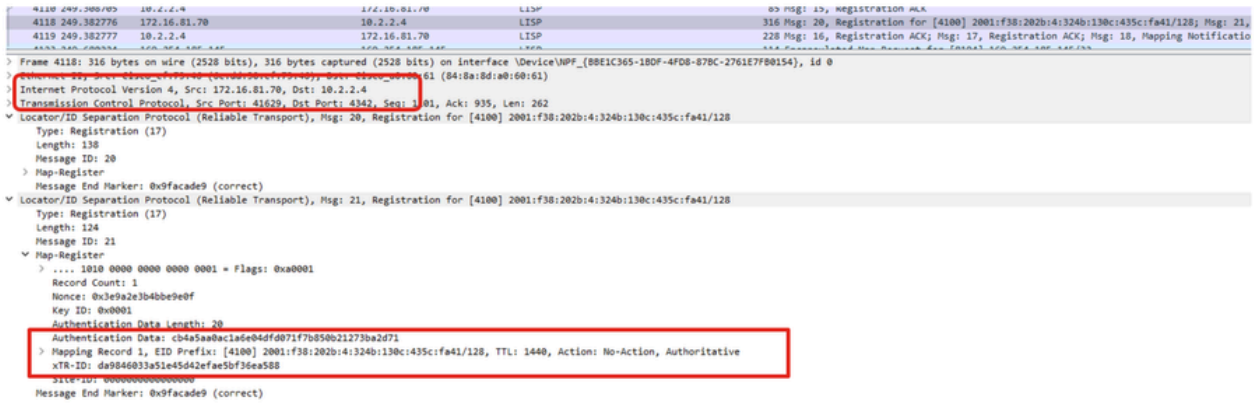
Acquisizione pacchetti dal server DHCPv6 al nodo perimetrale dell'infrastruttura

Passaggio 2. Il client wireless invia i frame 802.11 al punto di accesso con il payload IPv6.
Passaggio 3. Il punto di accesso rimuove l'intestazione wireless e invia il pacchetto al bordo dell'infrastruttura. Viene usata l'intestazione del tunnel VXLAN basata su IPv4 perché il punto di accesso ha l'indirizzo IPv4.



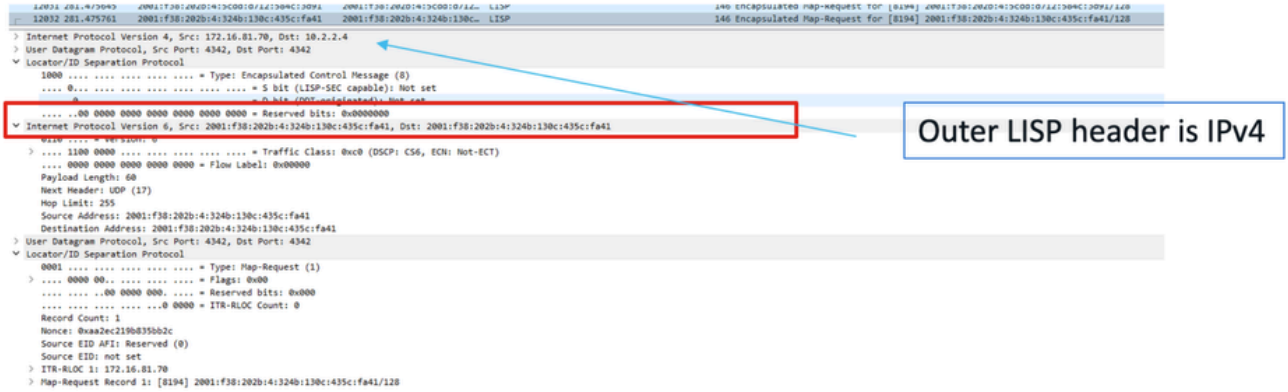
Acquisizione pacchetti per il tunnel VxLAN tra FE e AP

Passaggio 3.1. Fabric Edge registra il client IPv6 con il Control Plane. In questo modo viene utilizzato il metodo di registrazione IPv4 con i dettagli del client IPv6.



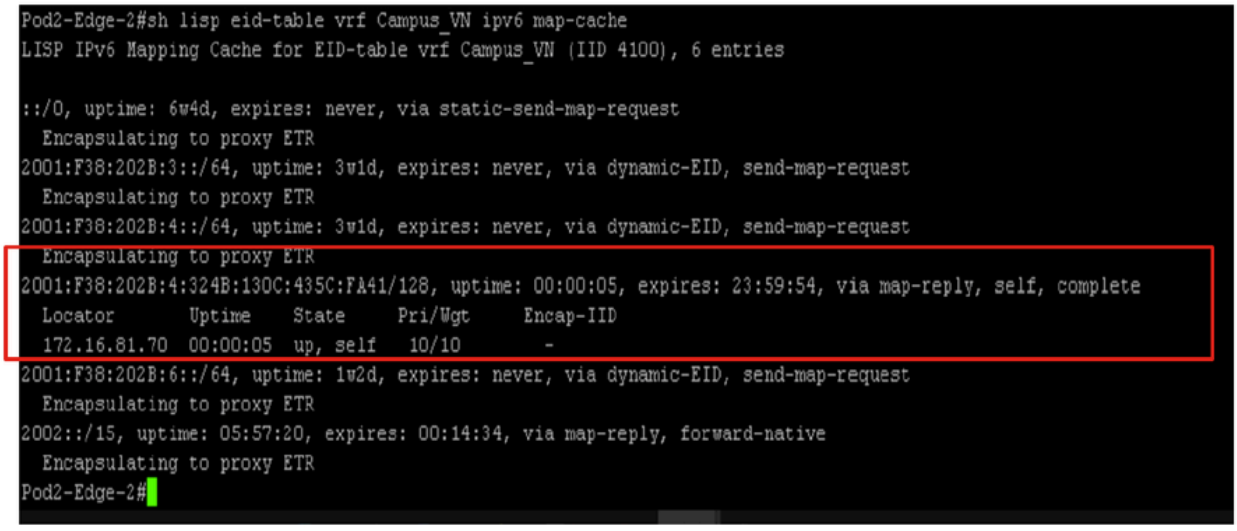
Acquisizione pacchetti per FE con il client Control Plane per IPv6

Passaggio 3.2. FE invia la richiesta MAP al control plane per identificare l'RLOC di destinazione.



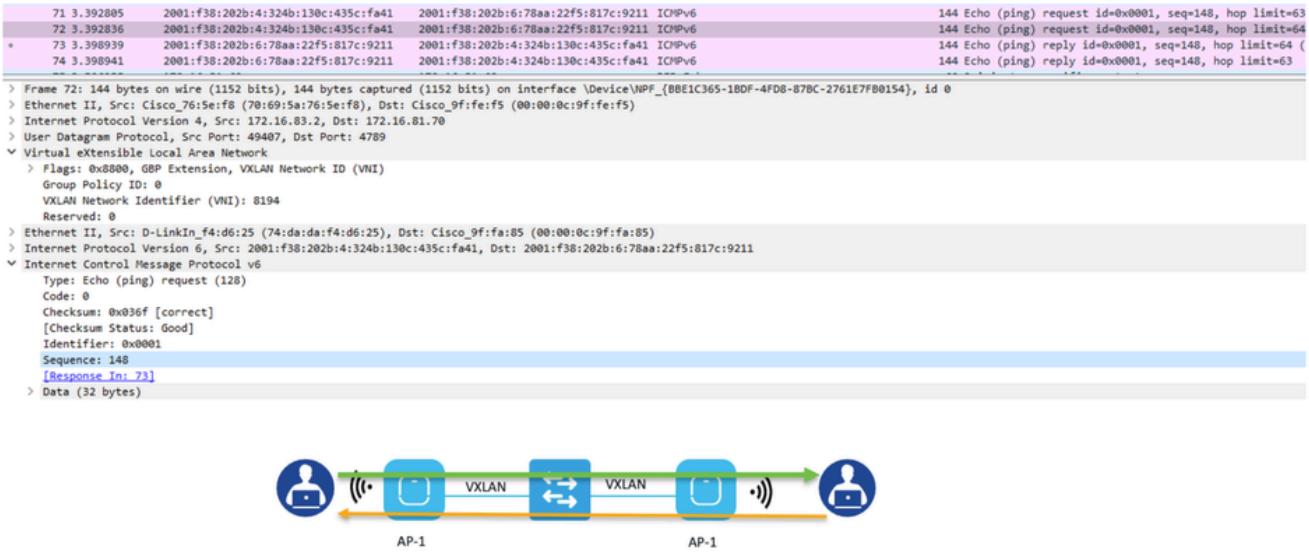
Acquisizione pacchetti da FE a CP con messaggi di registrazione MAP

Fabric Edge mantiene inoltre la cache MAP per i client IPv6 noti, come illustrato in questa immagine.



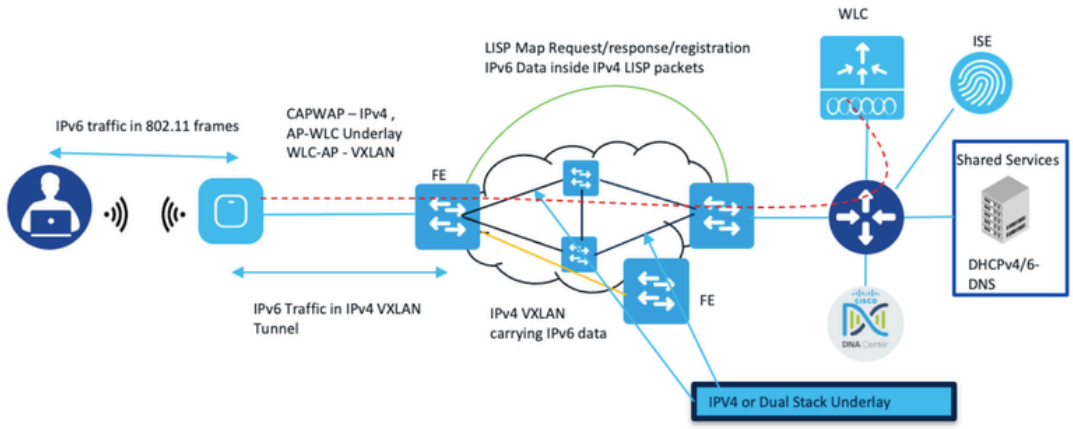
Output dello schermo di Fabric Edge con le informazioni sulla cache delle mappe di overlay IPv6

Passaggio 4. Il pacchetto viene inoltrato alla RLOC di destinazione con la VXLAN IPv4 che contiene il payload IPv6 originale. Poiché entrambi i client sono connessi allo stesso punto di accesso, il ping IPv6 utilizza questo percorso.

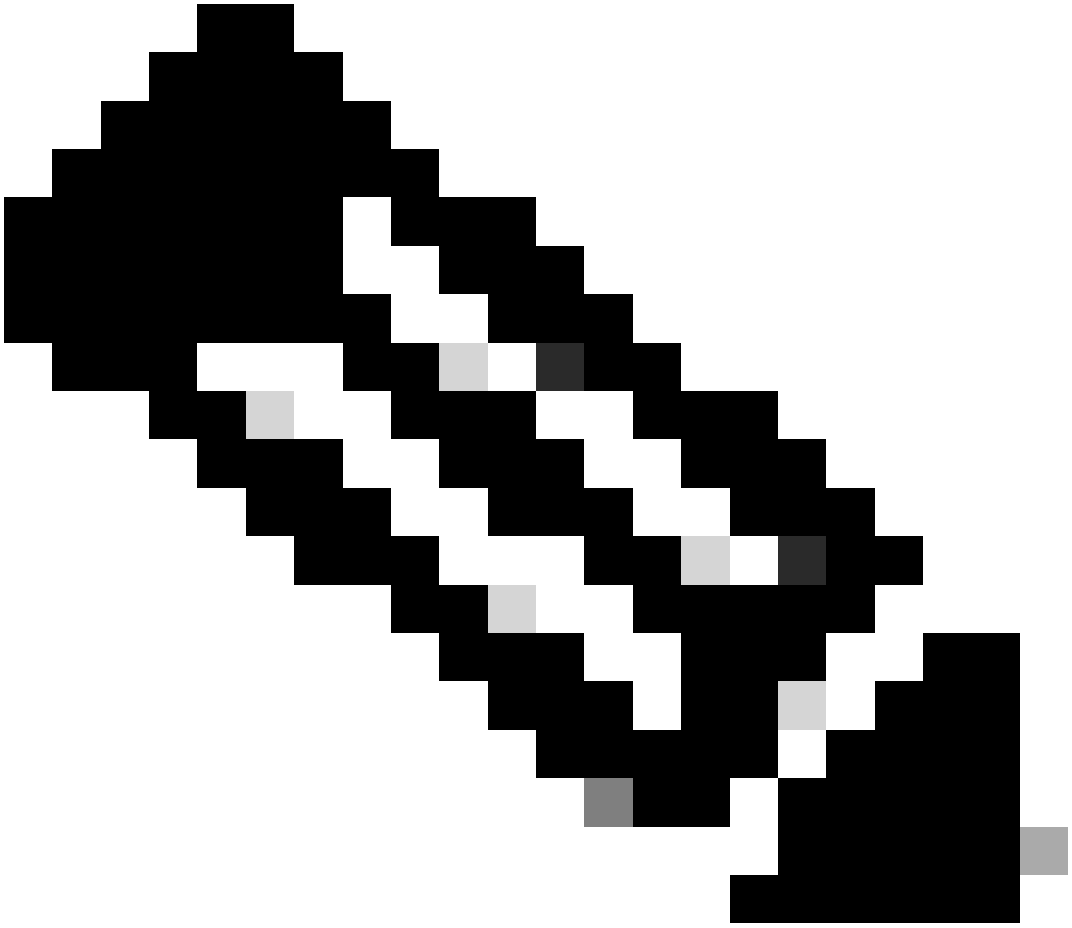


Acquisizione pacchetti per ping IPv6 tra due client wireless registrati nello stesso punto di accesso

Questa immagine riepiloga la comunicazione IPv6 dal punto di vista del client wireless.



La figura riepiloga la comunicazione IPv6 dal punto di vista del client wireless



Nota: L'accesso guest IPv6 (portale Web) tramite Cisco Identity Services non è supportato a causa delle limitazioni di ISE.

Matrice dipendenze

È importante notare le dipendenze e il supporto per IPv6 da diversi componenti wireless che fanno parte di Cisco SD-Access. La tabella in questa immagine riepiloga questa matrice di funzionalità.

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

Funzioni Cat9800 WLC IPv6 per release

Monitoraggio del Control Plane per IPv6

Dopo aver attivato IPv6, verranno visualizzate ulteriori voci relative all'IPv6 host nei server Mapping Server/Map Resolver (MR). Poiché un host può avere più indirizzi IP IPv6, la tabella di ricerca MS/MR contiene voci per tutti gli indirizzi IP. Questo valore viene combinato con la tabella IPv4 già esistente.
È necessario accedere alla CLI del dispositivo e usare questi comandi per controllare tutte le voci.

```
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
```

È inoltre possibile controllare i dettagli relativi all'IPv6 dell'host tramite la garanzia.

Implementazione QoS IPv6 in Cisco SD-Access

L'attuale versione di Cisco DNA Center (fino a 2.3.x) non supporta l'automazione dei criteri di applicazione QoS IPv6. Tuttavia, gli utenti possono creare manualmente modelli wireless e cablati IPv6 e inserire il modello QoS nei nodi Fabric Edge. Poiché DNA Center automatizza il criterio QoS IPv4 su tutte le interfacce fisiche una volta applicato, è possibile inserire manualmente una mappa di classe (corrispondente all'elenco di controllo di accesso (ACL) IPv6) prima di "class-default" tramite un modello.

Di seguito è riportato un esempio di modello abilitato per QoS IPv6 cablato integrato con la configurazione dei criteri generata da DNA Center:

```
!
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
```

Risoluzione dei problemi relativi a IPv6 in Cisco SD-Access

La risoluzione dei problemi relativi a SD-Access IPv6 è molto simile a IPv4: per raggiungere lo stesso obiettivo, è sempre possibile utilizzare lo stesso comando con opzioni di parole chiave diverse. Di seguito vengono illustrati alcuni comandi utilizzati di frequente per risolvere i problemi relativi a SD-Access.

```
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
```

Da Border Node per controllare il ping del server DHCPv6 sovrapposto:

```
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
```

Domande frequenti per la progettazione di IPv6 con Cisco SD-Access

D. La rete definita dal software Cisco supporta IPv6 per le reti di sovrapposizione e underlay?
R. Al momento della stesura del presente documento, è supportata solo la sovrimpressione nella release corrente (2.3.x).

D. Cisco SDN supporta IPv6 nativo per client sia cablati che wireless?
R. Sì. Ciò richiede pool a doppio stack creati nel DNA Center mentre IPv4 è il pool fittizio in quanto i client disabilitano le richieste DHCP IPv4 e vengono offerti solo indirizzi DHCP o SLAAC IPv6.

D. Posso avere una rete campus nativa solo IPv6 nel mio Cisco SD-Access Fabric?
R. Non nella release corrente (fino a 2.3.x). È sulla roadmap.

D. Cisco SD-Access supporta l'handoff IPv6 L2?
R. Non al momento. Sono supportati solo handoff L2 IPv4 e/o handoff L3 Dual-Stack.

D. Cisco SD-Access supporta il multicast per IPv6?
R. Sì, è supportata solo la sovrapposizione di IPv6 con multicast di replica headend. Multicast IPv6 nativo non ancora supportato.

D. Cisco SD-Access Fabric Enabled Wireless supporta gli utenti guest in uno stack doppio?
R. Non ancora supportato in Cisco IOS XE (Cat9800) WLC. AireOS WLC è supportato tramite una soluzione. Per i dettagli sull'implementazione della soluzione alternativa, contattare il team Cisco Customer Experience.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).