Implémenter IPv6 dans l'accès défini par logiciel

Table des matières

Introduction

Ce document décrit comment implémenter IPv6 dans Cisco® Software-Defined Access (SD-Access).

Informations générales

IPv4 a été lancé en 1983 et est toujours utilisé pour la majorité du trafic Internet. L'adressage IPv4 32 bits a permis plus de 4 milliards de combinaisons uniques. Cependant, en raison de l'augmentation du nombre de clients connectés à Internet, il existe une pénurie d'adresses IPv4 uniques. Dans les années 1990, l'épuisement de l'adressage IPv4 est devenu inévitable.
En prévision de cela, Internet Engineering Taskforce a introduit la norme IPv6. IPv6 utilise 128 bits et offre 340 undécillions d'adresses IP uniques, ce qui est largement suffisant pour répondre aux besoins croissants des périphériques connectés. Étant donné que de plus en plus de terminaux modernes prennent en charge la double pile et/ou une seule pile IPv6, il est essentiel que toute organisation soit prête pour l'adoption d'IPv6. Cela signifie que l'ensemble de l'infrastructure doit être prête pour IPv6. Cisco SD-Access est l'évolution des conceptions de campus traditionnelles vers les réseaux qui implémentent directement l'intention d'une organisation. Cisco Software Defined Networks est désormais prêt à intégrer une double pile (périphériques IPv6).

Un défi majeur pour toute entreprise dans l'adoption de l'IPv6 est la gestion des changements et les complexités associées à la migration des systèmes IPv4 existants vers l'IPv6. Ce document couvre tous les détails sur la prise en charge des fonctionnalités IPv6 sur le SDN Cisco, la stratégie et les points de ponctuation critiques, qui doivent être pris en compte lorsque vous adoptez l'IPv6 avec les réseaux définis par logiciel Cisco.

En août 2019, la version 1.3 de Cisco Digital Network Architecture (DNA) Center a été introduite avec la prise en charge d'IPv6. Dans cette version, le réseau de campus Cisco SD-Access prenait en charge l'adresse IP hôte avec les clients filaires et sans fil en IPv4, IPv6 ou IPv4v6 Dual-stack à partir du réseau de fabric de superposition. La solution est d'évoluer en permanence afin d'apporter de nouvelles fonctionnalités qui intègrent facilement l'IPv6 pour toute entreprise.

Cisco SD-Access avec architecture IPv6

La technologie de fabric, qui fait partie intégrante de SD-Access, fournit aux réseaux de campus filaires et sans fil des superpositions programmables et une virtualisation de réseau facile à déployer, qui permettent à un réseau physique d'héberger un ou plusieurs réseaux logiques afin de répondre à l'intention de conception. Outre la virtualisation du réseau, la technologie de fabric du réseau de campus améliore le contrôle des communications, ce qui permet une segmentation définie par logiciel et l'application de politiques en fonction de l'identité de l'utilisateur et de l'appartenance au groupe. L'ensemble de la solution Cisco SDN s'exécute sur l'ADN du fabric. Il est donc essentiel de comprendre chaque pilier de la solution en ce qui concerne la prise en charge IPv6.

- Sous-couche : la fonctionnalité IPv6 de superposition dépend de la sous-couche, car la superposition IPv6 utilise l'adressage IP de sous-couche IPv4 pour créer un plan de contrôle LISP (Locator/ID Separation Protocol) et des tunnels de plan de données VXLAN (Virtual Extensible LAN). Vous pouvez toujours activer la double pile pour le protocole de routage sous-jacent, seul le LISP de superposition SD-Access dépend du routage IPv4.
- Superposition : en matière de superposition, SD-Access prend en charge les terminaux filaires et sans fil IPv6 uniquement. Ce trafic IPv6 est encapsulé dans l'en-tête IPv4 et VXLAN dans le fabric SD-Access jusqu'à ce qu'il atteigne les noeuds de périphérie du fabric. Les noeuds de périphérie de fabric décapsule l'en-tête IPv4 et VXLAN, ce qui suit le processus de routage de monodiffusion IPv6 normal à partir de ce moment.
- Noeuds du plan de contrôle : le noeud du plan de contrôle est configuré pour autoriser l'enregistrement dans sa base de données de mappage de tous les sous-réseaux hôtes IPv6 et des routes hôtes /128 des plages de sous-réseaux.
- Noeuds en limite : sur les noeuds en limite, l'appairage BGP IPv6 avec les périphériques de fusion est activé. Le noeud de périphérie décapsule l'en-tête IPv4 du trafic de sortie du fabric, tandis que le trafic IPv6 entrant est également encapsulé avec l'en-tête IPv4 par les noeuds de périphérie.
- Périphérie du fabric : toutes les interfaces virtuelles commutées (SVI) configurées dans la périphérie du fabric doivent être IPv6. Cette configuration est poussée par le contrôleur DNA Center.
- Cisco DNA Center - Les interfaces physiques de Cisco DNA Center ne prennent pas en

charge la double pile au moment de la publication de ce document. Il ne peut être déployé que dans une seule pile avec IPv4 ou IPv6 uniquement dans les interfaces de gestion et/ou d'entreprise du centre DNA.
- Clients - Cisco SD-Access prend en charge la double pile (IPv4 et IPv6) ou la simple pile IPv4 ou IPv6. Toutefois, dans le cas d'un déploiement d'une seule pile IPv6, DNA Center doit toujours créer un pool de deux piles pour prendre en charge un client IPv6 uniquement. L'adresse IPv4 du pool de deux piles est une adresse fictive uniquement en tant qu'adresse IPv6 que le client est censé désactiver.

Architecture de superposition IPv6 dans Cisco Software-Defined Access.

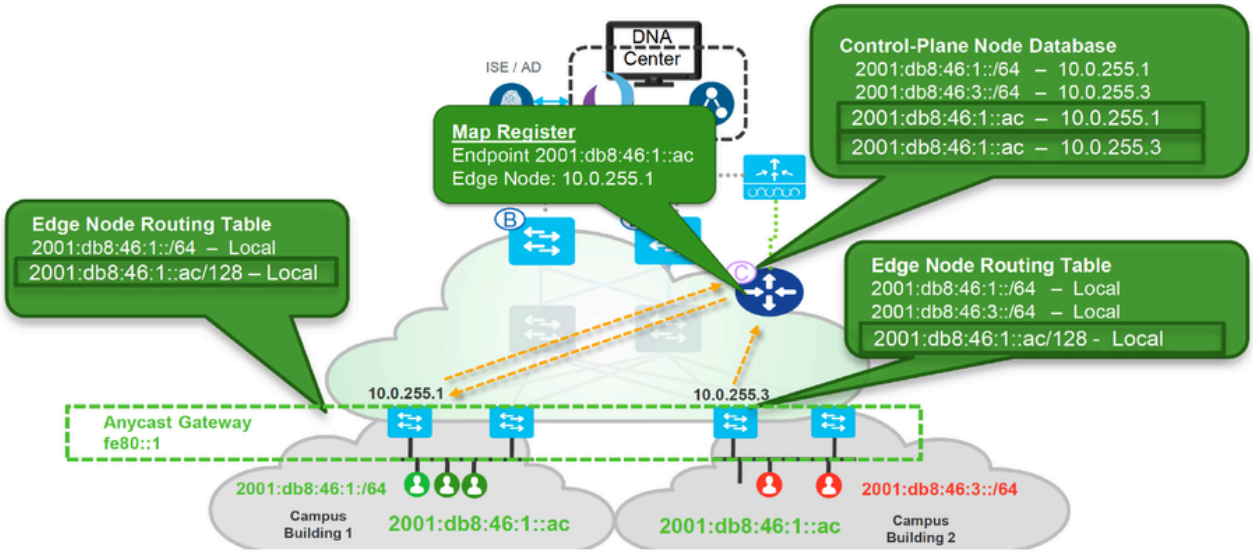


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

Architecture de superposition IPv6

Activer IPv6 avec Cisco DNA-Center

Il existe deux façons d'activer le pool IPv6 dans Cisco DNA Center :
1. Créer un pool IPv4/v6 à double pile - nouveau champ
2. Modifier IPv6 sur le pool IPv4 qui existe déjà - migration du champ de démarrage

La version actuelle (jusqu'à 2.3.x) de DNA Center ne prend pas en charge IPv6. Uniquement un pool, si l'utilisateur prévoit de prendre en charge un client unique/natif avec adresse IPv6 uniquement. Une adresse IPv4 fictive doit être associée au pool IPv6. Notez qu'à partir du pool IPv4 déployé qui existe déjà avec un site qui lui est associé, modifiez le pool avec une adresse IPv6. DNA Center offre l'option de migration pour le fabric SD-Access, qui nécessite que l'utilisateur reprovisionne le fabric pour ce site. Un indicateur d'avertissement s'affiche dans le fabric auquel le site appartient et indique que le fabric doit être « reconfiguré ». Consultez ces

images pour des exemples :

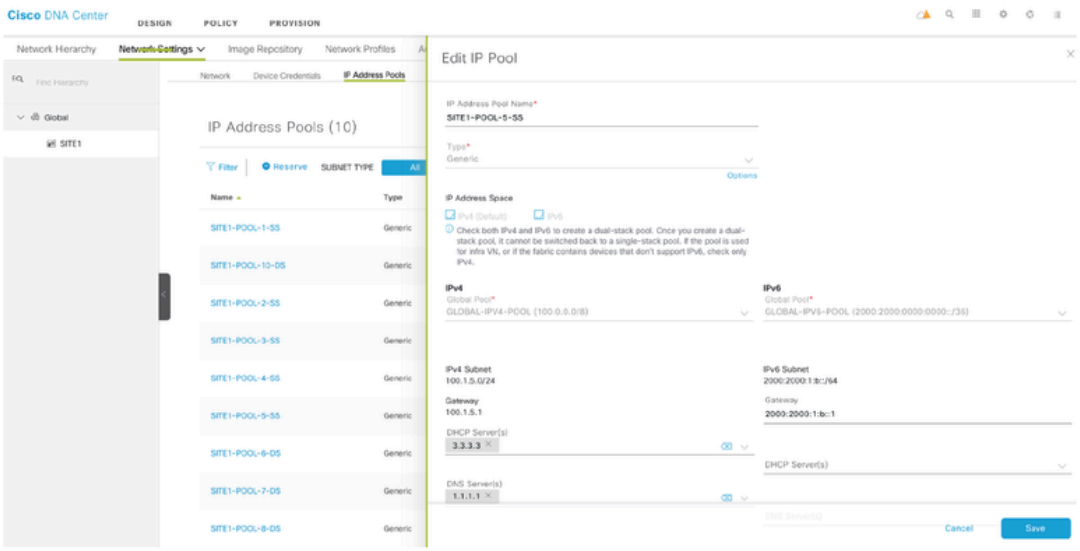


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

Mise à niveau d'un pool IPv4 unique vers un pool à deux piles en modifiant l'option de pool IPv4

Pool upgrade: Warning on fabric page

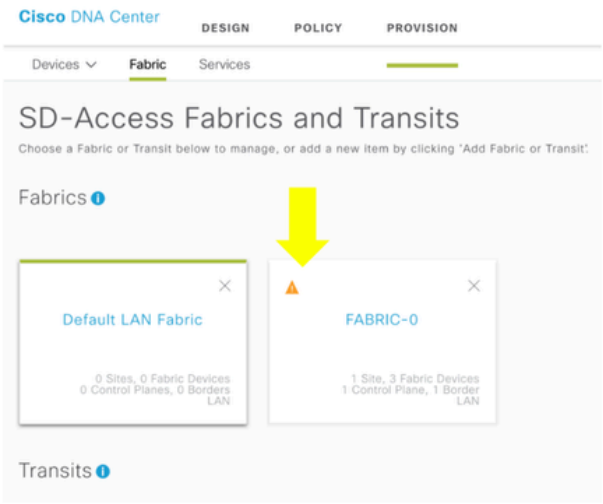


Figure 3.
Fabric has warning indicator which needs to 'reconfigure the fabric'

Le fabric a un indicateur d'avertissement qui doit « reconfigurer le fabric »

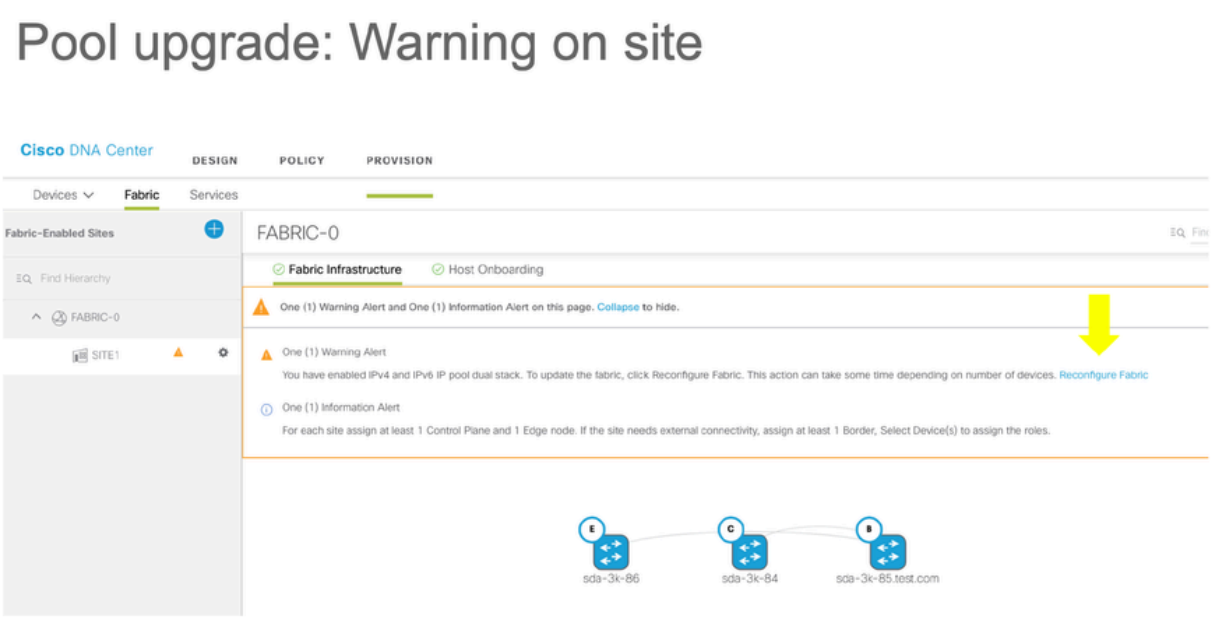


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

L'utilisateur doit cliquer sur « reconfigurer le fabric » pour reconfigurer automatiquement les noeuds du fabric pour que la configuration à double pile prenne effet dans le cadre du processus de migration

Considérations relatives à la conception d'IPv6 dans Cisco SD-Access

Bien que les clients Cisco SD-Access puissent fonctionner avec des paramètres réseau à double pile ou IPv6 uniquement, l'implémentation actuelle du fabric SD-Access avec la version 2.3.x.x du commutateur DNA Center (SW) comporte certaines considérations relatives au déploiement IPv6.

- Cisco SD-Access prend en charge les protocoles de routage IPv4 sous-jacents. Ainsi, le trafic client IPv6 est transporté lorsqu'il est encapsulé dans des en-têtes IPv4. Il s'agit d'une condition requise pour le déploiement actuel du logiciel LISP. Mais cela ne signifie pas que le sous-réseau ne peut pas activer le protocole de routage IPv6, juste le LISP de superposition SD-Access ne fonctionne pas sur sa dépendance.
- La multidiffusion native IPv6 n'est pas prise en charge, car la couche sous-jacente du fabric ne peut être qu'IPv4 pour le moment.
- Le réseau sans fil invité ne peut fonctionner qu'avec la pile double. En raison de la version actuelle d'Identity Services Engine (ISE) (par exemple, jusqu'à 3.2), le portail d'invité IPv6 n'est pas pris en charge. Par conséquent, un client invité IPv6 uniquement ne pourra pas être authentifié.
- L'automatisation de la stratégie QoS des applications IPv6 n'est pas prise en charge dans la version actuelle de DNA Center. Ce document décrit les étapes nécessaires à la mise en oeuvre de la QoS IPv6 pour les clients à double pile filaires et sans fil dans Cisco SD-Access qui avait été déployée pour l'un des utilisateurs à grande échelle.
- La fonctionnalité de limitation du débit du client sans fil pour le trafic en aval et en amont, par

SSID (Service Set Identifier) ou par client, en fonction de la stratégie, est prise en charge pour IPv4 (TCP/UDP) et IPv6 (TCP uniquement). La limitation du débit UDP IPv6 n'est pas encore prise en charge.
- Le pool IPv4 peut être mis à niveau vers un pool à double pile. Mais un pool à deux piles ne peut pas être rétrogradé en pool IPv4. Si l'utilisateur souhaite réintégrer le pool à deux piles dans le pool à une pile IPv4, il doit libérer l'ensemble du pool à deux piles.
- L'IPv6 unique n'est pas encore pris en charge, alors que seul l'IPv4 ou le pool à deux piles peut être créé dans le DNA Center actuel.
- La plate-forme Cisco IOS® XE est une version logicielle minimale requise à partir de la version 16.9.2.
- La technologie sans fil IPv6 Guest n'est pas encore prise en charge sur les plates-formes Cisco IOS XE, tandis qu'AireOS (8.10.105.0+) prend en charge une solution de contournement.
- Le pool à deux piles ne peut pas être attribué dans l'INFRA_VN où seul le point d'accès (AP) ou le pool de noeuds étendus peut être attribué.
- L'automatisation LAN ne prend pas encore en charge IPv6.

Outre les limitations mentionnées précédemment, lorsque vous concevez un fabric SD-Access avec IPv6 activé, vous devez toujours garder à l'esprit l'évolutivité de chaque composant de fabric. Si un point d'extrémité a plusieurs adresses IPv4 ou IPv6, chaque adresse est comptée comme une entrée individuelle.

Les entrées d'hôte de fabric incluent les points d'accès et les noeuds classiques et étendus par stratégie.

Considérations supplémentaires sur l'évolutivité des noeuds périphériques :

Les entrées /32 (IPv4) ou /128 (IPv6) sont utilisées lorsque le noeud périphérique transfère le trafic provenant de l'extérieur du fabric vers un hôte du fabric.

Pour tous les commutateurs, à l'exception des commutateurs hautes performances Cisco Catalyst 9500 et des commutateurs Cisco Catalyst 9600 :

- IPv4 utilise une entrée TCAM (Ternary Content Addressable Memory) (entrées d'hôte de fabric) pour chaque adresse IPv4.
- IPv6 utilise deux entrées TCAM (entrées d'hôte de fabric) pour chaque adresse IPv6.

Pour les commutateurs hautes performances Cisco Catalyst 9500 et les commutateurs Cisco Catalyst 9600 :

- IPv4 utilise une entrée TCAM (entrées d'hôte de fabric) pour chaque adresse IPv4.
- IPv6 utilise une entrée TCAM (entrées d'hôte de fabric) pour chaque adresse IPv6.

Et certains terminaux ne prennent pas en charge DHCPv6, comme les smartphones sous Android OS qui utilisent la configuration automatique des adresses sans état (SLAAC) pour obtenir des adresses IPv6. Un seul point d'extrémité peut aboutir à plus de deux adresses IPv6. Ce comportement consomme davantage de ressources matérielles sur chaque noeud de fabric, en

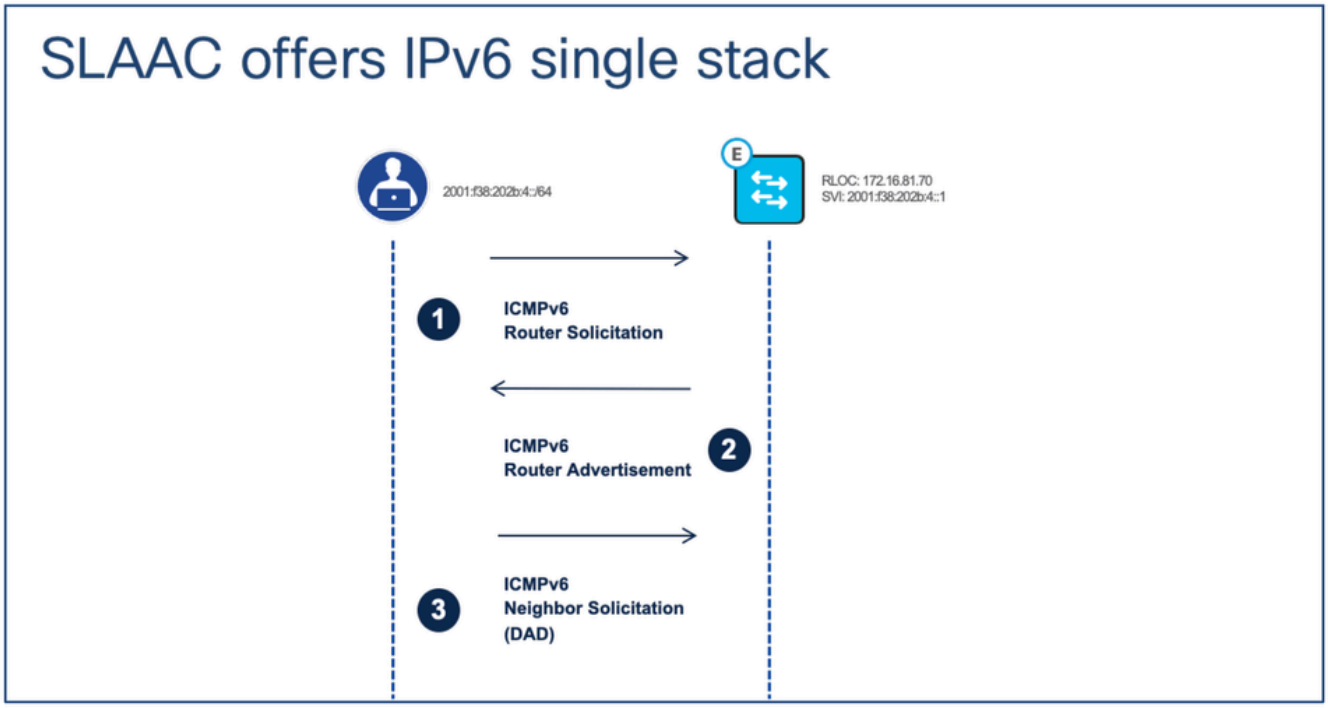
particulier pour les noeuds de contrôle et de périphérie de fabric. Par exemple, chaque fois que le noeud périphérique veut envoyer du trafic aux noeuds de périphérie pour un point d'extrémité, il installe une route hôte dans l'entrée TCAM et brûle une entrée de contiguïté VXLAN dans la TCAM matérielle.

Connexions et flux d'appels des clients filaires et sans fil

Une fois que le client est connecté à la périphérie du fabric, il peut obtenir les adresses IPv6 de différentes manières. Cette section décrit la méthode la plus courante d'adressage IPv6 client, à savoir SLAAC et DHCPv6.

Attribution d'adresses IPv6 - SLAAC

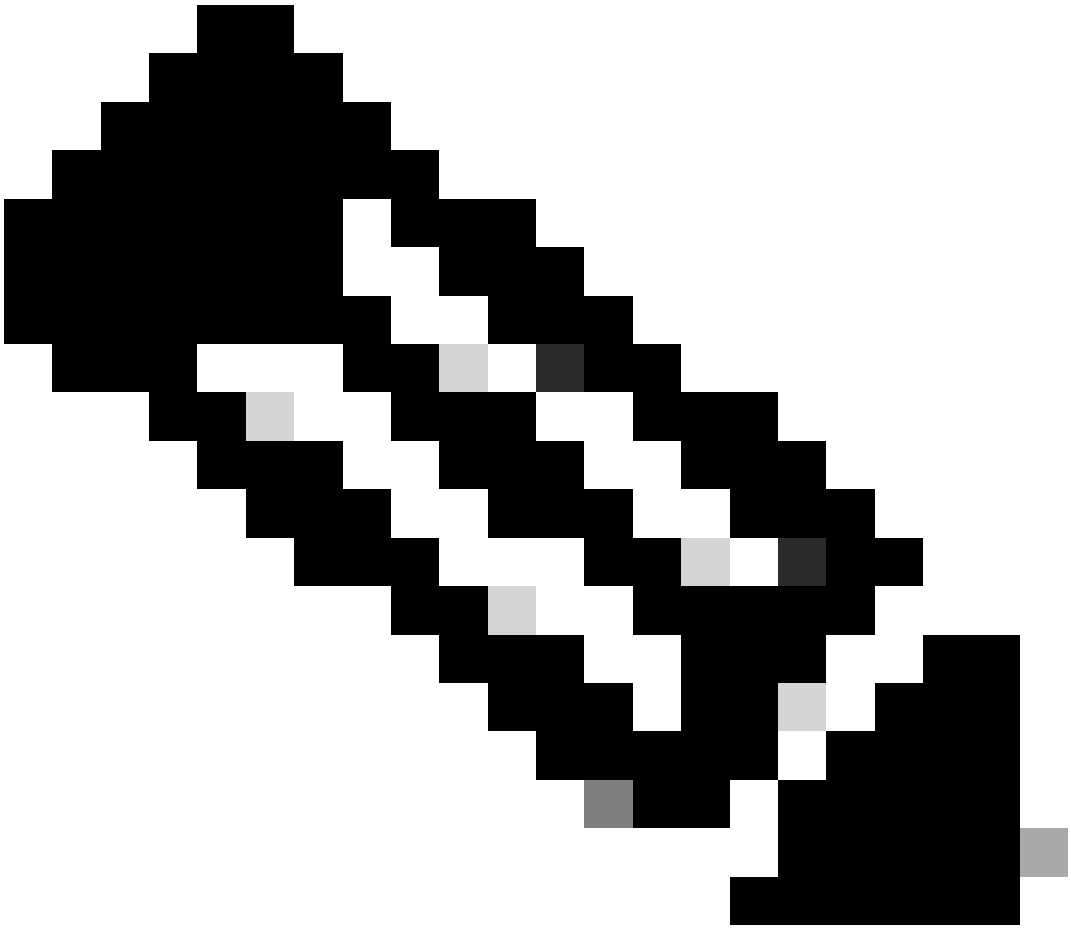
Le SLAAC dans l'accès défini par logiciel (SDA) n'est pas différent du flux de processus SLAAC standard. Pour que la SLAAC fonctionne correctement, le client IPv6 doit être configuré avec une adresse link-local dans son interface, la manière dont le client se configure automatiquement avec l'adresse link-local n'est pas dans le cadre de ce document.



Attribution d'adresses IPv6 - SLAAC

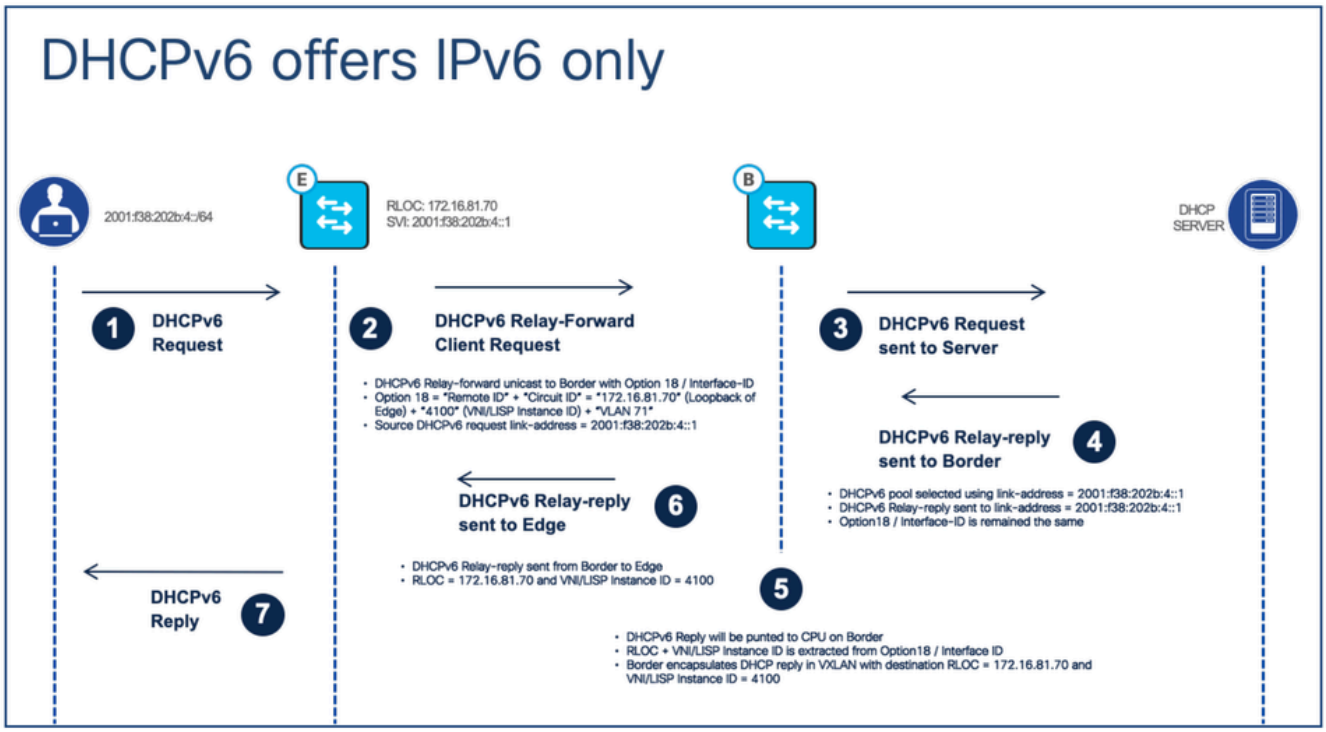
Description du flux d'appels :
Étape 1. Une fois que le client IPv6 s'est configuré avec une adresse link-local IPv6, il envoie un message de sollicitation de routeur ICMPv6 à la périphérie du fabric. L'objectif de ce message est d'obtenir le préfixe de monodiffusion globale de son segment connecté.
Étape 2. Après avoir reçu le message RS, la périphérie du fabric répond par un message d'annonce de routeur ICMPv6 contenant le préfixe de monodiffusion IPv6 global et sa longueur interne.
Étape 3. Une fois que le client reçoit le message RA, il combine le préfixe de monodiffusion

globale IPv6 avec son identificateur d’interface EUI-64 afin de générer son adresse de monodiffusion globale IPv6 unique et de définir sa passerelle sur l’adresse link-local de l’interface SVI de la périphérie du fabric qui est associée au segment du client. Ensuite, le client envoie un message de sollicitation de voisin ICMPv6 afin d'effectuer une détection d'adresse en double (DAD) pour s'assurer que l'adresse IPv6 qu'il obtient est unique.



Remarque : Tous les messages SLAAC sont encapsulés avec l'adresse link-local SVI IPv6 du client et du noeud de fabric.

Attribution d'adresses IPv6 - DHCPv6

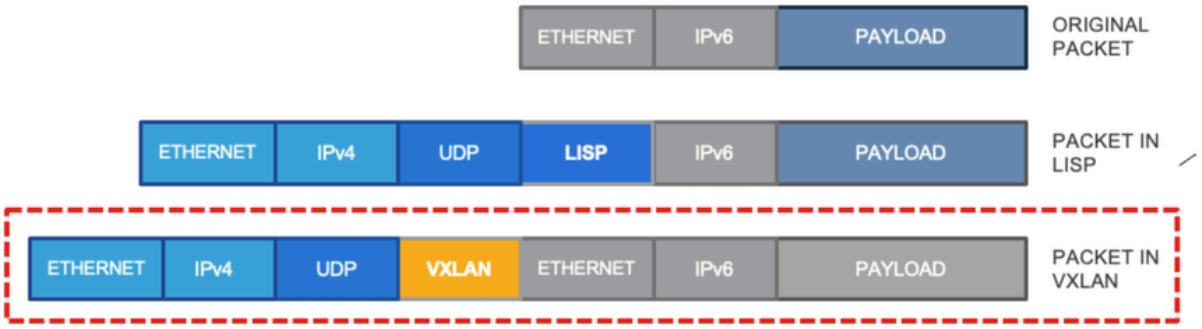


Attribution d'adresses IPv6 - DHCPv6

Description du flux d'appels :
Étape 1. Le client envoie la requête DHCPv6 à la périphérie du fabric.
Étape 2. Lorsque la périphérie du fabric reçoit la demande DHCPv6, elle utilise le message de transfert de relais DHCPv6 pour monodiffuser la demande à la périphérie du fabric avec l'option DHCPv6 18. Par rapport à l'option DHCPv6 82, l'option DHCPv6 18 code à la fois « ID de circuit » et « ID distant ». L'ID d'instance LISP/VNI, le localisateur de routage IPv4 (RLOC) et le VLAN du point d'extrémité sont codés à l'intérieur.
Étape 3. La bordure du fabric décapsule l'en-tête VXLAN et monodiffuse le paquet DHCPv6 au serveur DHCPv6.
Étape 4. Le serveur DHCPv6 reçoit le message de transfert de relais, il utilise l'adresse de liaison source (agent de relais DHCPv6/passerelle client) du message pour choisir le pool IPv6 afin d'attribuer l'adresse IPv6. Ensuite, renvoyez le message de réponse de relais DHCPv6 à l'adresse de la passerelle cliente. L'option 18 reste inchangée.
Étape 5. Lorsque la frontière de fabric reçoit le message de réponse de relais, elle extrait l'instance/VNI RLOC et LISP de l'option 18. La frontière de fabric encapsule le message de réponse de relais dans VXLAN avec une destination qu'elle a extraite de l'option 18.
Étape 6. La bordure du fabric envoie le message de réponse de relais DHCPv6 à la périphérie du fabric à laquelle le client se connecte.
Étape 7. Lorsque la périphérie du fabric reçoit le message de réponse de relais DHCPv6, elle décapsule l'en-tête VXLAN du message et transfère le message au client. Le client connaît alors l'adresse IPv6 qui lui a été attribuée.

Communication IPv6 dans Cisco SD-Access

La communication IPv6 utilise le plan de contrôle LISP standard et les méthodes de communication du plan de données VXLAN. Avec l'implémentation actuelle dans Cisco SD-Access, LISP et VXLAN utilisent l'en-tête IPv4 externe pour transporter les paquets IPv6 à l'intérieur. Cette image illustre ce processus.



En-tête IPv4 externe contenant les paquets IPv6

Cela signifie que toutes les requêtes LISP utilisent le paquet natif IPv4, tandis que la table de noeuds du plan de contrôle contient des détails sur le RLOC avec les adresses IPv6 et IPv4 du point d'extrémité. Ce processus est expliqué en détail dans la section suivante du point de vue des terminaux sans fil.

Communication IPv6 sans fil dans Cisco SD-Access

La communication sans fil repose sur deux composants spécifiques : les points d'accès et les contrôleurs LAN sans fil, à l'exception des composants standard du fabric d'accès SD de Cisco. Les points d'accès sans fil créent un tunnel CAPWAP (Control and Provisioning of wireless access points) avec le contrôleur LAN sans fil (WLC). Alors que le trafic client existe à la périphérie du fabric, d'autres communications du plan de contrôle qui incluent des statistiques radio sont gérées par le WLC. D'un point de vue IPv6, le WLC et le point d'accès doivent avoir les adresses IPv4 et toutes les communications CAPWAP utilisent ces adresses IPv4. Alors que le WLC non-fabric et le point d'accès prennent en charge la communication IPv6, Cisco SD-Access utilise le protocole IPv4 pour toutes les communications qui transportent tout trafic IPv6 client à l'intérieur des paquets IPv4. Cela signifie que les pools d'AP attribués sous Infra VN ne peuvent pas être mappés avec des pools d'IP qui sont à double pile et une erreur est générée si une tentative est faite pour ce mappage. La communication sans fil au sein de Cisco SDA peut être divisée en plusieurs tâches principales :

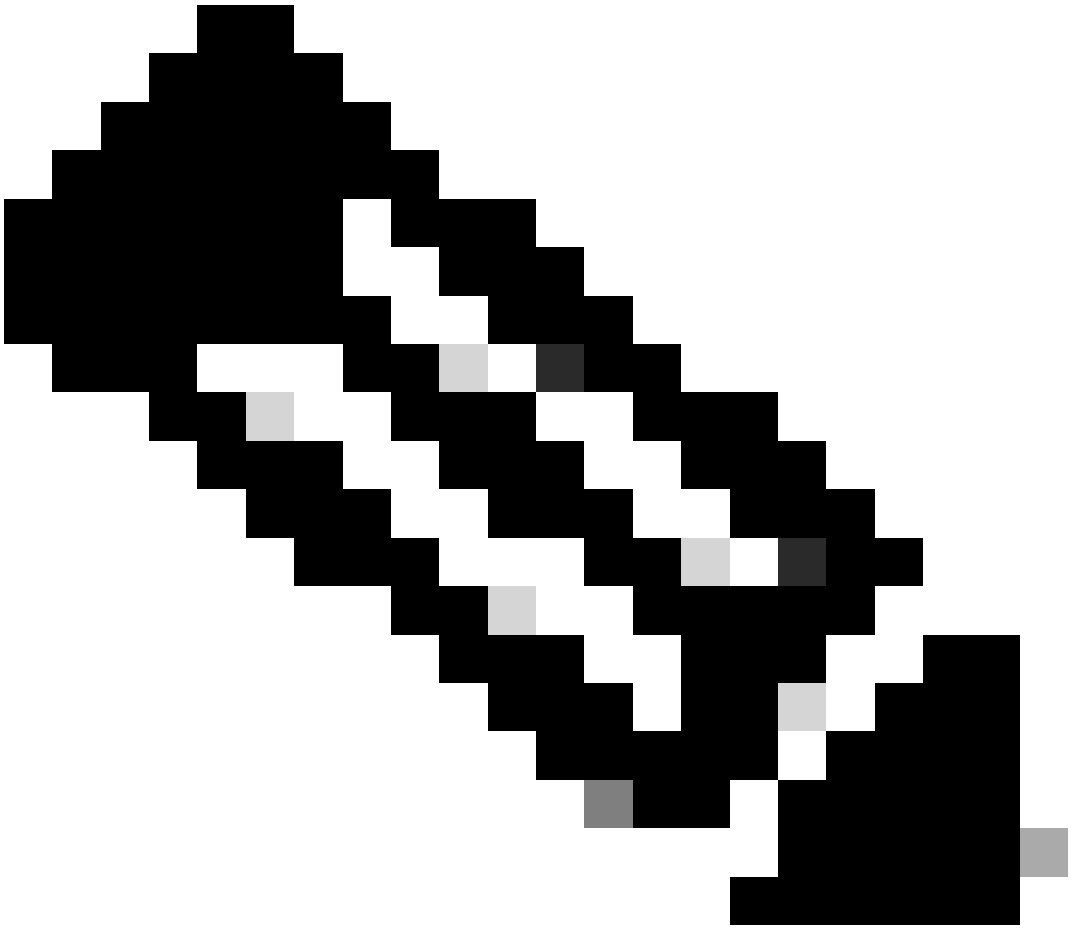
- Intégration des points d'accès
- Intégration du client

Observez ces événements du point de vue de l'IPv6.

Intégration des points d'accès

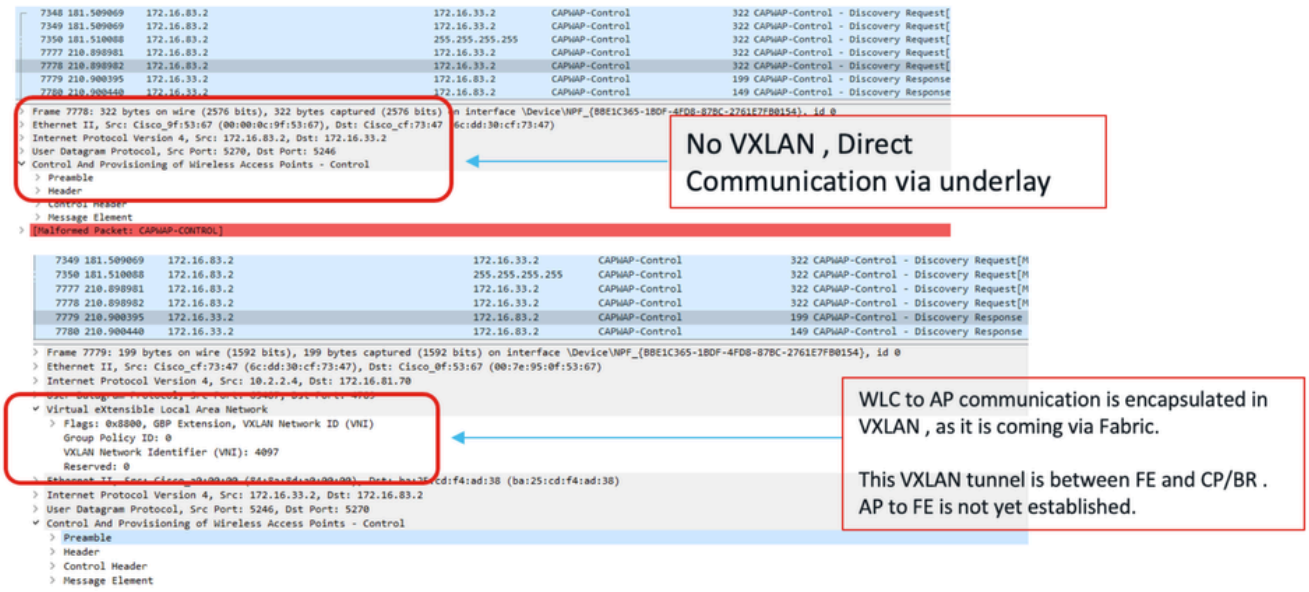
Ce processus reste le même pour IPv6 et IPv4, car les adresses IPv4 du WLC et du point d'accès sont incluses ici :
1. Le port de périphérie de fabric (FE) est configuré pour le point d'accès intégré.
2. Le point d’accès se connecte au port FE et, via le point d’accès CDP, informe FE de sa présence (ce qui permet à FE d’attribuer le bon VLAN).
3. Le point d’accès obtient l’adresse IPv4 du serveur DHCP et FE enregistre le point d’accès et met à jour le plan de contrôle (noeud Plan de contrôle) avec les détails du point d’accès.
4. Le point d’accès rejoint le WLC via des méthodes traditionnelles (comme l’option 43 du DHCP).
5. WLC vérifie si AP est compatible avec le fabric et interroge le plan de contrôle pour les informations RLOC AP (par exemple, RLOC demandé/réponse reçue).
6. CP répond avec l'IP RLOC de l'AP au WLC.
7. WLC enregistre le contrôle d’accès au support (adresse) (MAC) AP dans CP.
8. CP met à jour le FE avec les détails du WLC sur le AP (ceci indique à FE d'initier le tunnel VXLAN avec le AP).

FE traite les informations et crée un tunnel VXLAN avec AP. À ce stade, le point d’accès annonce le SSID activé par le fabric.



Remarque : Si le point d'accès diffuse les SSID non-fabric et ne diffuse pas le SSID du fabric, vérifiez le tunnel VXLAN entre le point d'accès et le noeud de périphérie du fabric.

Notez également que la communication AP à WLC se fait toujours via le CAPWAP sous-jacent et que toutes les communications WLC à AP utilisent le CAPWAP VXLAN via la superposition. Cela signifie que si vous capturez des paquets qui vont d'AP à WLC, vous ne voyez que CAPWAP alors que le trafic inverse a un tunnel VXLAN. Voir cet exemple pour la communication entre AP et WLC.



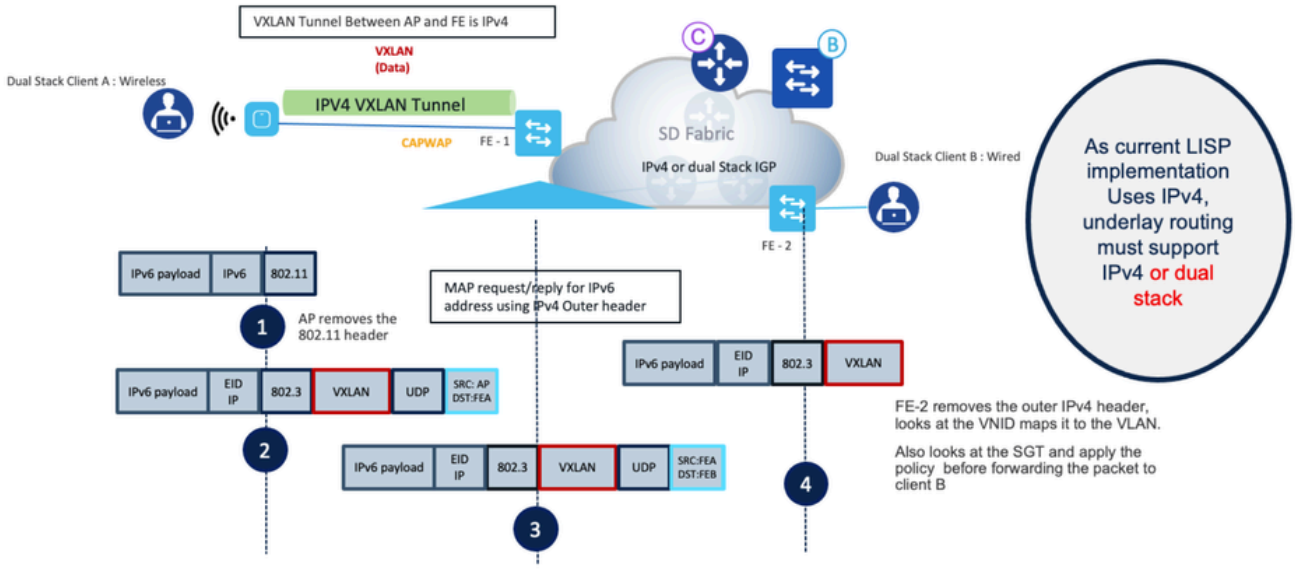
Captures de paquets du point d'accès au WLC (tunnel CAPWAP) par rapport au WLC au point d'accès (tunnel VxLAN dans le fabric)

Intégration client

Le processus d'intégration du client double pile/IPv6 reste le même, mais le client utilise les méthodes d'attribution d'adresses IPv6 telles que SLAAC/DHCPv6 afin d'obtenir les adresses IPv6.
1. Le client rejoint le fabric et active le SSID sur le point d'accès.
2. WLC connaît le RLOC AP.
3. Le client authentifie et le WLC enregistre les détails du client L2 auprès du CP et met à jour le point d'accès.
4. Le client lance l'adressage IPv6 à partir des méthodes configurées : SLAAC/DHCPv6.
5. FE déclenche l'enregistrement du client IPv6 dans la base de données de suivi de l'hôte (HTDB) CP. AP vers FE et FE vers d'autres destinations utilisent l'encapsulation IPv6 VXLAN et LISP dans les trames IPv4.

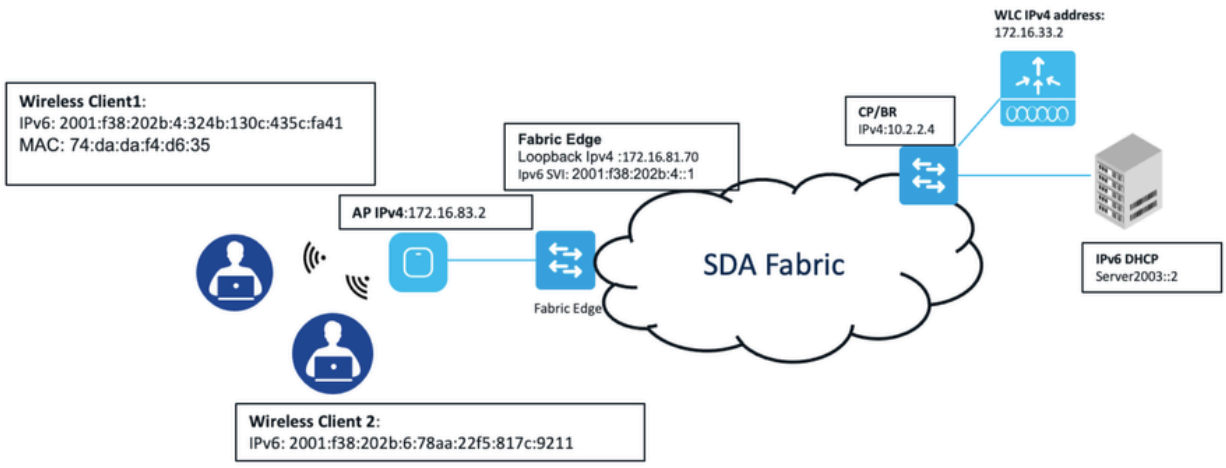
Communication client-client avec IPv6

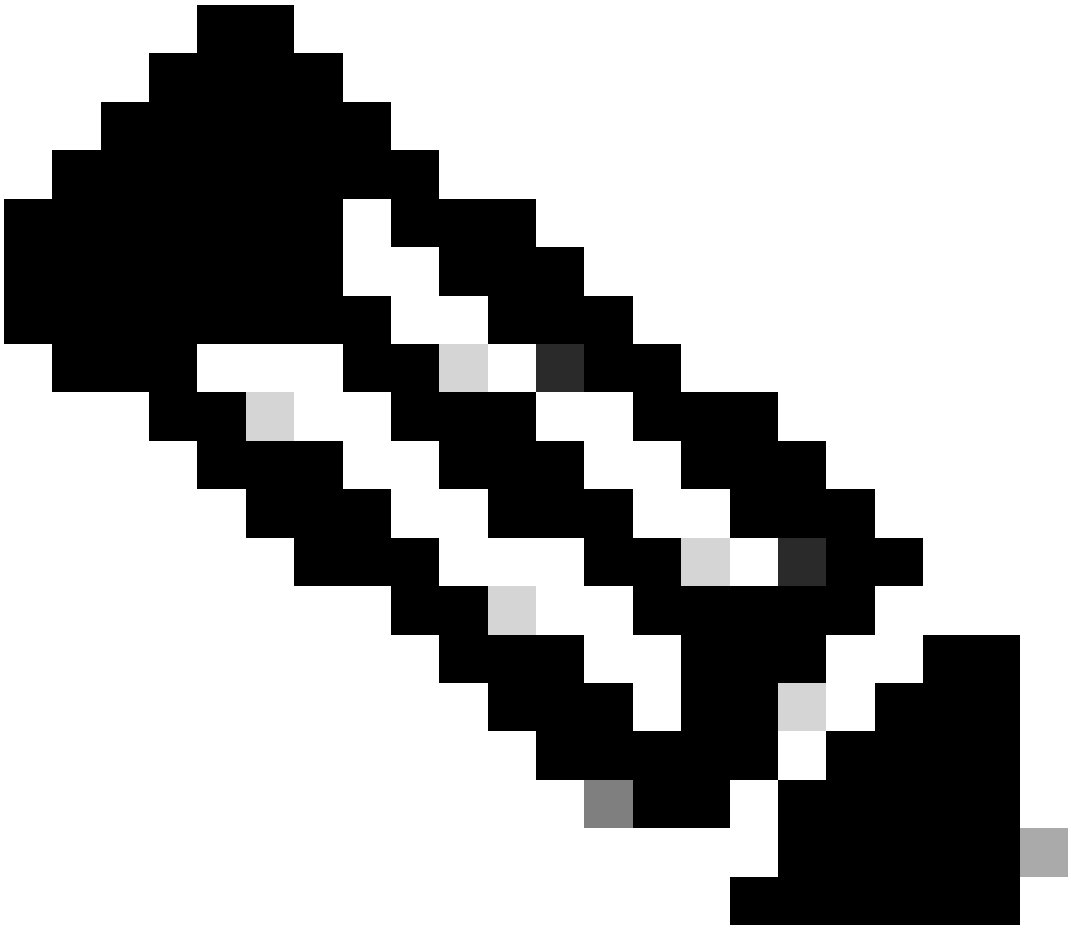
L'image ci-dessous résume le processus de communication du client sans fil IPv6 avec un autre client câblé IPv6. (Cela suppose que le client est authentifié et a obtenu l'adresse IPv6 via des méthodes configurées.)
1. Le client envoie les trames 802.11 au point d'accès avec la charge utile IPv6.
2. Le point d'accès supprime les en-têtes 802.11 et envoie la charge utile IPv6 d'origine dans le tunnel VXAN IPv4 vers le fabric Edge.
3. Fabric Edge utilise la requête MAP (Message Access Protocol) pour identifier la destination et envoie la trame au RLOC de destination avec le VXLAN IPv4.
4. Au niveau du commutateur de destination, l'en-tête VXLAN IPv4 est supprimé et le paquet IPv6 est envoyé au client.



Flux de paquets client sans fil double pile vers client filaire double pile

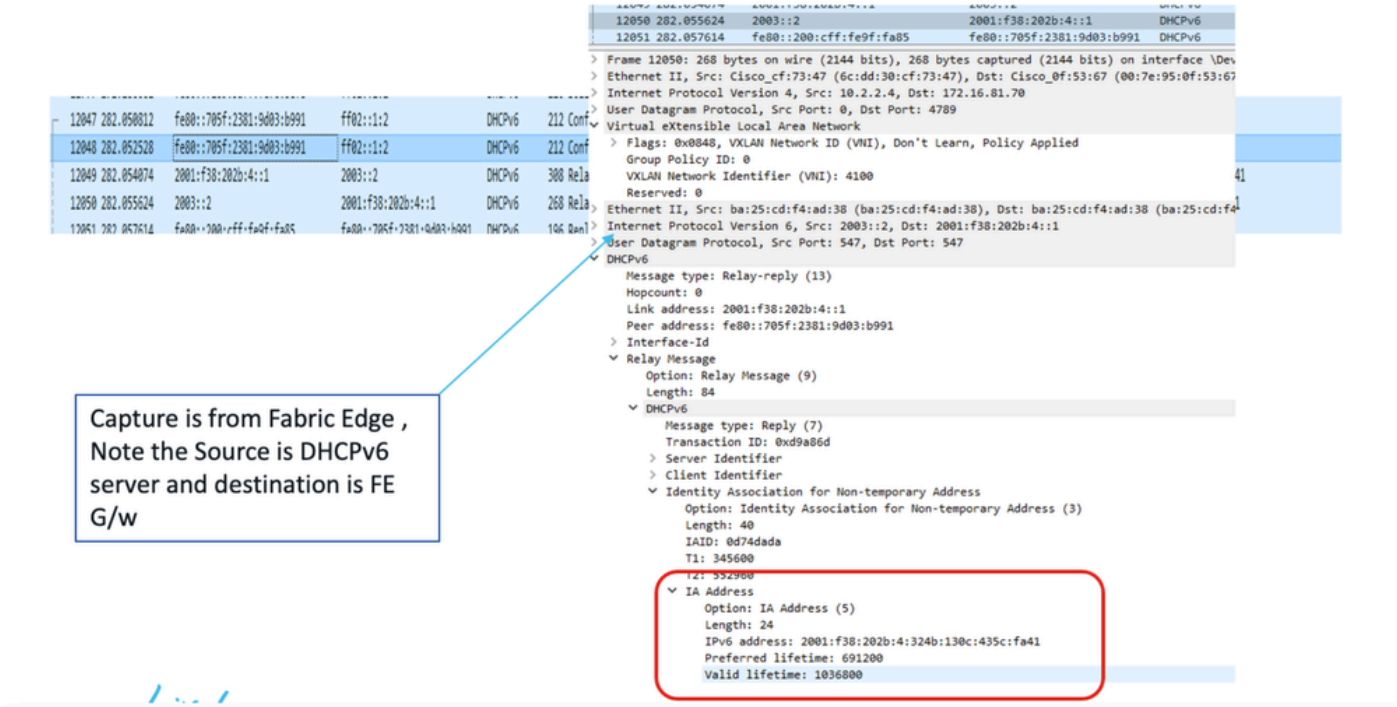
Examinez en détail ce processus avec les captures de paquets et reportez-vous à l'image pour obtenir des informations détaillées sur les adresses IP et MAC. Notez que cette configuration utilise les deux clients à double pile connectés aux mêmes points d'accès mais mappés avec des sous-réseaux IPv6 (SSID) différents.





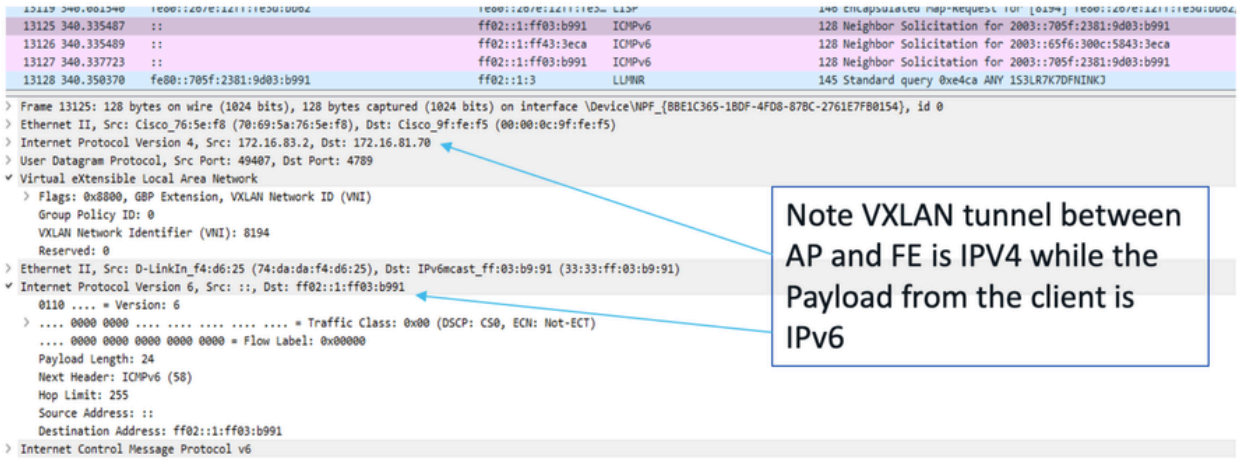
Remarque : Pour toute communication IPv6 en dehors du fabric, par exemple, DHCP/DNS, le routage IPv6 doit être activé entre l'infrastructure de périphérie et l'infrastructure hors fabric.

Étape 1. Le client authentifie et obtient l’adresse IPv6 à partir des méthodes configurées.



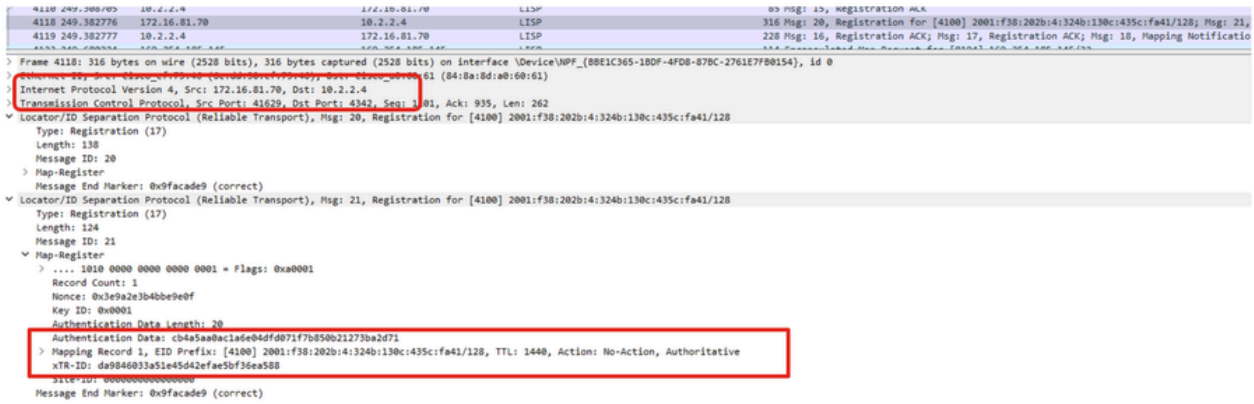
Capture de paquets du serveur DHCPv6 vers le noeud de périphérie de fabric

Étape 2. Le client sans fil envoie les trames 802.11 au point d'accès avec la charge utile IPv6.
Étape 3. Le point d'accès supprime l'en-tête sans fil et envoie le paquet à la périphérie du fabric. Il utilise l'en-tête de tunnel VXLAN basé sur IPv4, car le point d'accès possède l'adresse IPv4.



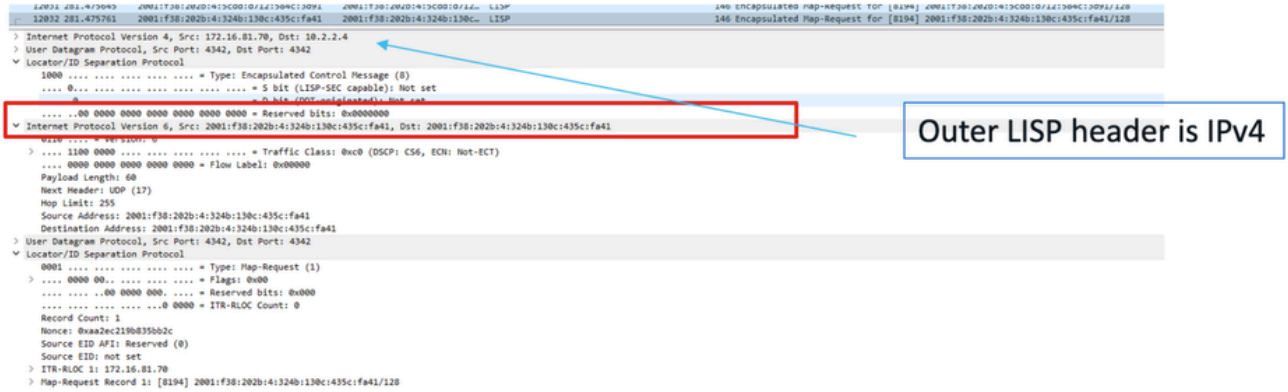
Capture de paquets pour le tunnel VxLAN entre FE et AP

Étape 3.1. Fabric Edge enregistre le client IPv6 dans le plan de contrôle. Elle utilise la méthode d'enregistrement IPv4 avec les détails du client IPv6 à l'intérieur.



Packet Capture pour FE s'enregistre avec le plan de contrôle pour le client IPv6

Étape 3.2. FE envoie la requête MAP au plan de contrôle pour identifier le RLOC de destination.



Capture de paquets de FE à CP avec messages d'enregistrement MAP

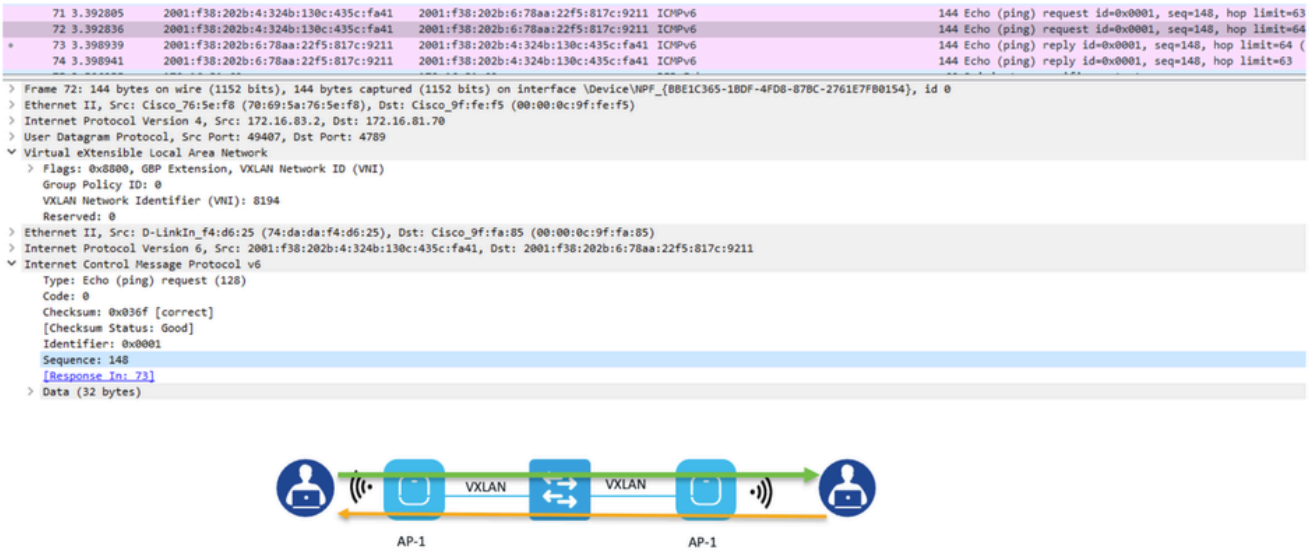
Fabric Edge gère également le cache MAP pour les clients IPv6 connus, comme illustré dans cette image.

```
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#
```

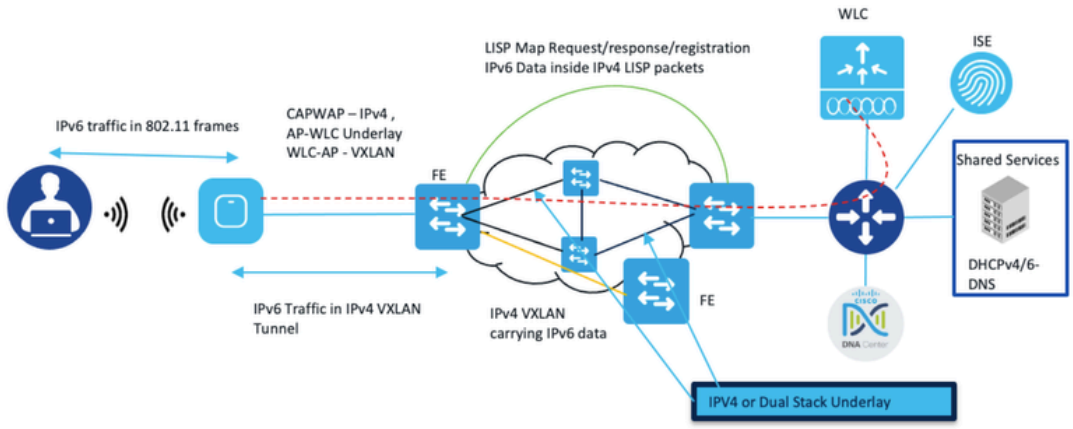
Sortie d'écran Fabric Edge des informations de cache de mappage de superposition IPv6

Étape 4. Le paquet est transmis au RLOC de destination avec le VXLAN IPv4 qui transporte la charge utile IPv6 d'origine à l'intérieur. Comme les deux clients sont connectés au même AP, la requête ping IPv6 emprunte ce chemin.

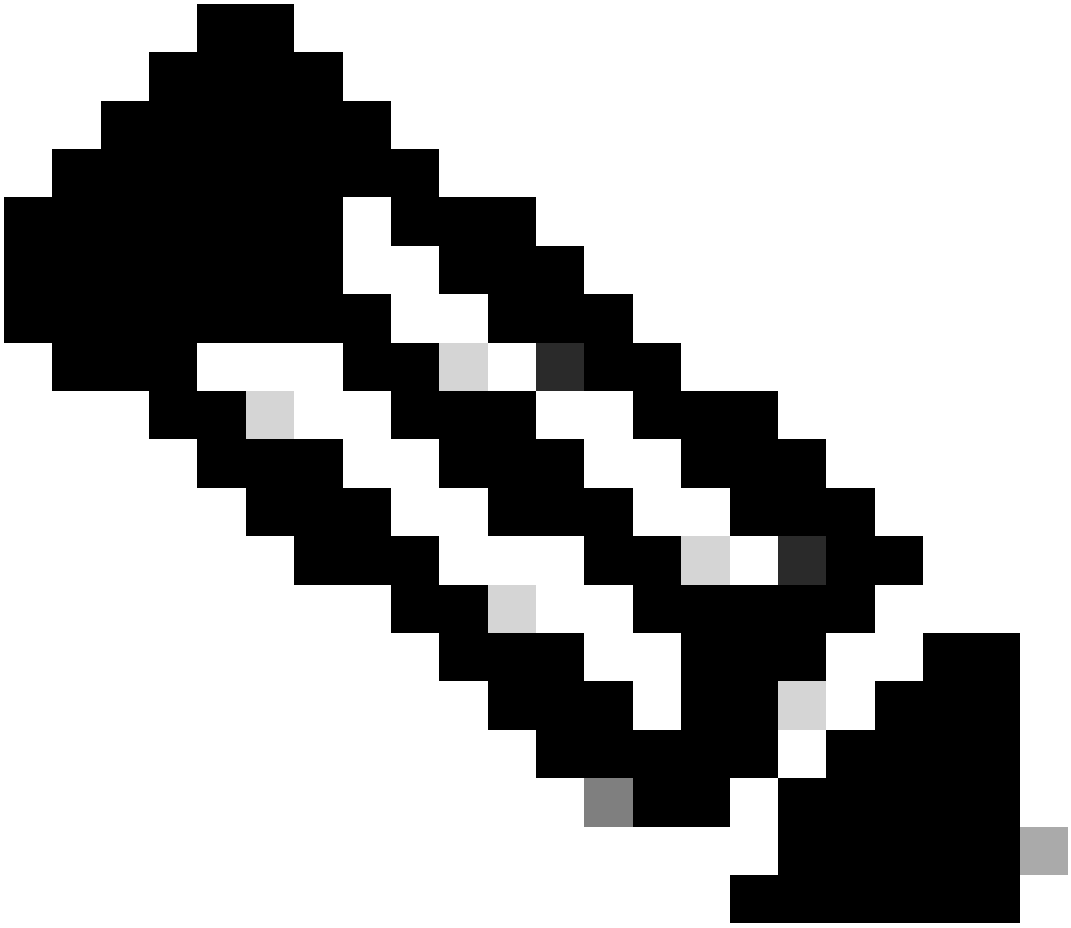


Capture de paquets pour la requête ping IPv6 entre deux clients sans fil enregistrés sur le même point d'accès

Cette image résume la communication IPv6 du point de vue du client sans fil.



La figure résume la communication IPv6 du point de vue du client sans fil



Remarque : L'accès invité IPv6 (portail Web) via Cisco Identity Services n'est pas pris en charge en raison des limitations d'ISE.

Matrice des dépendances

Il est important de noter les dépendances et la prise en charge d'IPv6 à partir de différents composants sans fil qui font partie de Cisco SD-Access. Le tableau de cette image résume cette matrice de fonctions.

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

Fonctionnalités du WLC IPv6 du Cat9800 par version

Surveillance du plan de contrôle pour IPv6

Une fois que vous avez activé IPv6, vous commencez à voir des entrées supplémentaires sur l'hôte IPv6 dans les serveurs Map server (MS)/Map resolver (MR). Comme un hôte peut avoir plusieurs adresses IPv6, votre table de recherche MS/MR contient des entrées pour toutes les adresses IP. Elle est associée à la table IPv4 qui existe déjà.
Vous devez vous connecter à l'interface de ligne de commande du périphérique et exécuter ces commandes afin de vérifier toutes les entrées.

```
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
```

Vous pouvez également vérifier les détails de l'hôte IPv6 via l'assurance.

Implémentation de la QoS IPv6 dans Cisco SD-Access

La version actuelle de Cisco DNA Center (jusqu'à 2.3.x) ne prend pas en charge l'automatisation de la politique d'application QoS IPv6. Toutefois, les utilisateurs peuvent créer manuellement des modèles filaires et sans fil IPv6 et insérer le modèle QoS dans les noeuds de périphérie de fabric. Étant donné que DNA Center automatise la stratégie QoS IPv4 sur toutes les interfaces physiques une fois appliquée, vous pouvez insérer manuellement une carte de classe (qui correspond à la liste de contrôle d'accès IPv6) avant « class-default » via un modèle.

Voici un exemple de modèle filaire compatible IPv6 QoS intégré à la configuration de politiques générée par 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
```

Dépannage d'IPv6 dans Cisco SD-Access

Dépannage SD-Access IPv6 est tout comme IPv4, vous pouvez toujours utiliser la même commande avec différentes options de mots clés afin d'atteindre le même objectif. Ceci montre quelques commandes qui sont fréquemment utilisées pour dépanner 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
```

À partir de Border Node pour vérifier la requête ping du serveur DHCPv6 de superposition :

```
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
```

FAQ rapide sur la conception IPv6 avec Cisco SD-Access

Q. Cisco Software Defined Network prend-il en charge IPv6 pour les réseaux sous-jacents et superposés ?
R. Seule la superposition est prise en charge avec la version actuelle (2.3.x) au moment où ce document est écrit.

Q. Cisco SDN prend-il en charge le protocole IPv6 natif pour les clients filaires et sans fil ?
R. Oui. Cela nécessite des pools à double pile qui sont créés dans le centre DNA tandis que IPv4 est le pool fictif car les clients désactivent les requêtes DHCP IPv4 et seules les adresses DHCP ou SLAAC IPv6 sont proposées.

Q. Puis-je avoir un réseau de campus IPv6 uniquement natif dans mon fabric Cisco SD-Access ?
R. Pas avec la version actuelle (jusqu'à 2.3.x). Elle figure sur la feuille de route.

Q. Cisco SD-Access prend-il en charge le transfert L2 IPv6 ?
R. Pas pour le moment. Seuls les transferts L2 IPv4 et/ou L3 Dual-Stack sont pris en charge.

Q. Cisco SD-Access prend-il en charge la multidiffusion pour IPv6 ?
R. Oui, seule la superposition IPv6 avec la multidiffusion de réplication de tête de réseau est prise en charge. La multidiffusion IPv6 native n'est pas encore prise en charge.

Q. Cisco SD-Access Fabric Enabled Wireless prend-il en charge les invités en double pile ?
R. Pas encore pris en charge dans le WLC Cisco IOS XE (Cat9800). Le WLC AireOS est pris en charge via une solution de contournement. Pour plus d'informations sur la mise en oeuvre de la solution de contournement, contactez l'équipe Cisco Customer Experience.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.