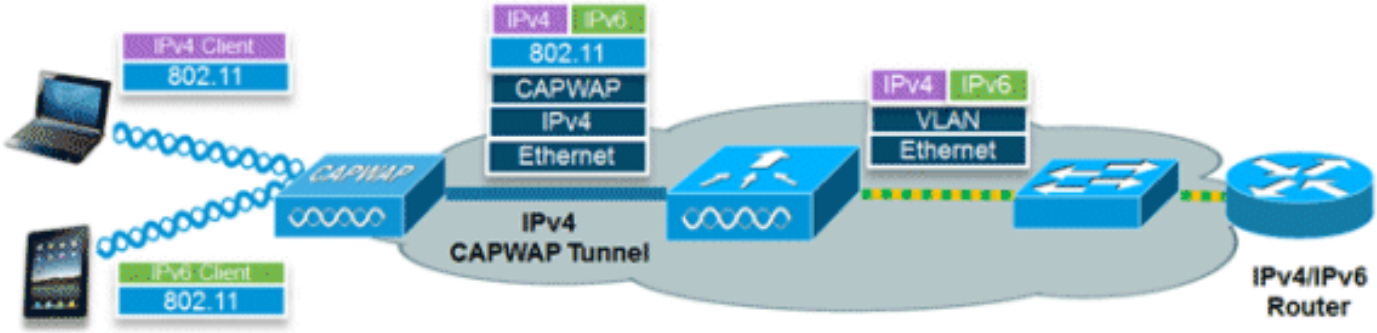
Guide de déploiement du client IPv6 LAN sans fil

Table des matières

Introduction

Ce document fournit des informations sur le fonctionnement théorique et sur la configuration de la solution de réseau local sans fil unifié de Cisco en ce qui concerne la prise en charge des clients IPv6.

Connectivité client sans fil IPv6



Le jeu de fonctions IPv6 de la version 7.2 du logiciel Cisco Unified Wireless Network permet au réseau sans fil de prendre en charge les clients IPv4, Dual-Stack et IPv6 uniquement sur le même réseau sans fil. L'objectif global de l'ajout de la prise en charge des clients IPv6 au réseau local sans fil unifié Cisco était de maintenir la parité des fonctionnalités entre les clients IPv4 et IPv6, notamment la mobilité, la sécurité, l'accès invité, la qualité de service et la visibilité des terminaux.

Jusqu'à huit adresses client IPv6 peuvent être suivies par périphérique. Cela permet aux clients IPv6 de disposer d'une adresse SLAAC (Stateless Address Auto Configuration) link-local, d'une adresse DHCPv6 (Dynamic Host Configuration Protocol for IPv6) et même d'adresses dans d'autres préfixes sur une seule interface. Les clients WGB (Work Group Bridge) connectés à la liaison ascendante d'un point d'accès autonome en mode WGB peuvent également prendre en charge IPv6.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Contrôleurs LAN sans fil, série 2500, série 5500 ou WiSM2
- Points d'accès 1130, 1240, 1250, 1040, 1140, 1260, 3500, 3600 Series AP et 1520 ou 1550 Series Mesh AP
- Routeur compatible IPv6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

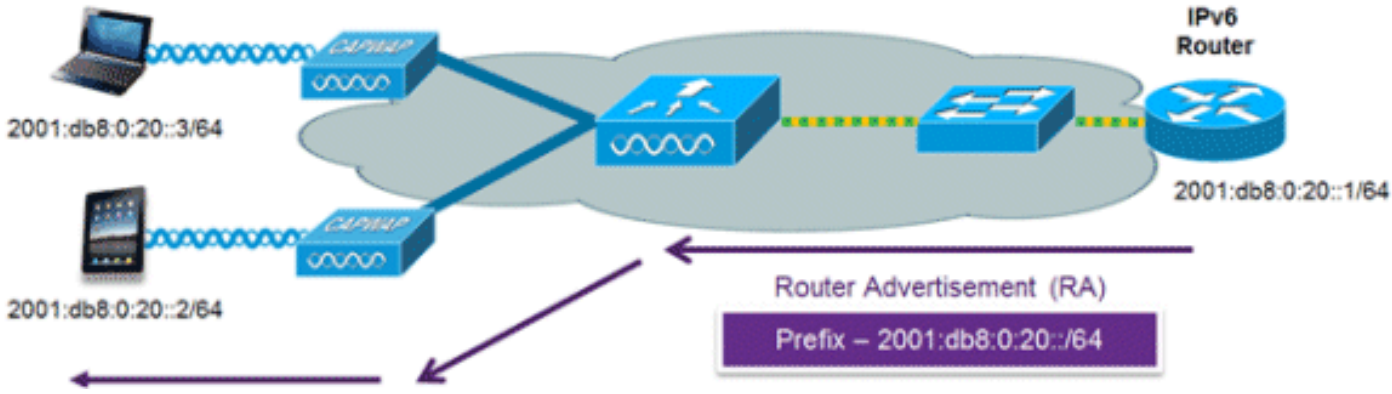
Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Conditions requises pour la connectivité client IPv6 sans fil

Afin d'activer la connectivité client IPv6 sans fil, le réseau câblé sous-jacent doit prendre en charge le routage IPv6 et un mécanisme d'attribution d'adresses tel que SLAAC ou DHCPv6. Le contrôleur LAN sans fil doit avoir une contiguïté de couche 2 avec le routeur IPv6 et le VLAN doit être étiqueté lorsque les paquets entrent dans le contrôleur. Les points d'accès ne nécessitent pas de connectivité sur un réseau IPv6, car tout le trafic est encapsulé à l'intérieur du tunnel CAPWAP IPv4 entre le point d'accès et le contrôleur.

Attribution d'adresses SLAAC



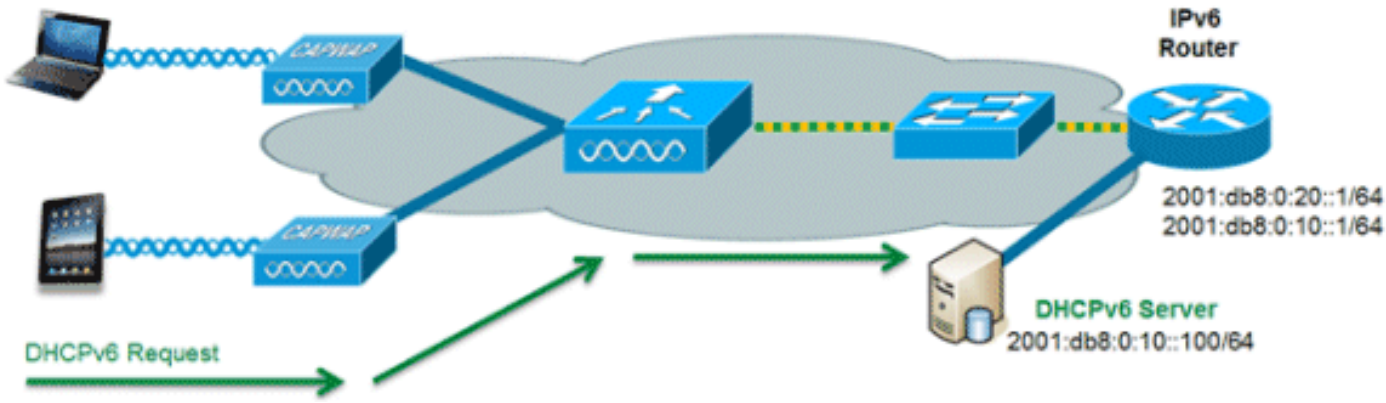
La méthode la plus courante pour l'attribution d'adresses de client IPv6 est SLAAC. SLAAC offre une connectivité plug-and-play simple dans laquelle les clients attribuent eux-mêmes une adresse en fonction du préfixe IPv6. Ce processus est réalisé lorsque le routeur IPv6 envoie des messages d'annonce de routeur périodiques qui informent le client du préfixe IPv6 utilisé (les 64 premiers bits) et de la passerelle par défaut IPv6. À partir de ce moment, les clients peuvent générer les 64 bits restants de leur adresse IPv6 selon deux algorithmes : EUI-64 qui est basé sur l'adresse MAC de l'interface, ou des adresses privées qui sont générées de manière aléatoire. Le choix de l'algorithme appartient au client et est souvent configurable. La détection des adresses en double est effectuée par les clients IPv6 afin de s'assurer que les adresses aléatoires sélectionnées ne entrent pas en collision avec d'autres clients. L'adresse du routeur qui envoie des annonces est utilisée comme passerelle par défaut pour le client.

Les commandes de configuration Cisco IOS® d'un routeur IPv6 compatible Cisco sont utilisées

pour activer l'adressage SLAAC et les annonces de routeur :

```
ipv6 unicast-routing
interface Vlan20
 description IPv6-SLAAC
 ip address 192.168.20.1 255.255.255.0
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 enable
end
```

Attribution d'adresses DHCPv6



L'utilisation de DHCPv6 n'est pas requise pour la connectivité du client IPv6 si SLAAC est déjà déployé. Il existe deux modes de fonctionnement pour DHCPv6, appelés **Stateless** et **Stateful**.

Le mode **sans état** DHCPv6 est utilisé pour fournir aux clients des informations réseau supplémentaires qui ne sont pas disponibles dans l'annonce du routeur, mais pas une adresse IPv6 car elle est déjà fournie par SLAAC. Ces informations peuvent inclure le nom de domaine DNS, le ou les serveurs DNS et d'autres options spécifiques au fournisseur DHCP. Cette configuration d'interface est destinée à un routeur IPv6 Cisco IOS implémentant DHCPv6 sans état avec SLAAC activé :

```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateless
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

L'option DHCPv6 **Stateful**, également connue sous le nom de mode géré, fonctionne de la même manière que DHCPv4 en ce qu'elle attribue des adresses uniques à chaque client au lieu que le client génère les 64 derniers bits de l'adresse comme dans SLAAC. Cette configuration d'interface est destinée à un routeur IPv6 Cisco IOS implémentant DHCPv6 avec état avec SLAAC désactivé :

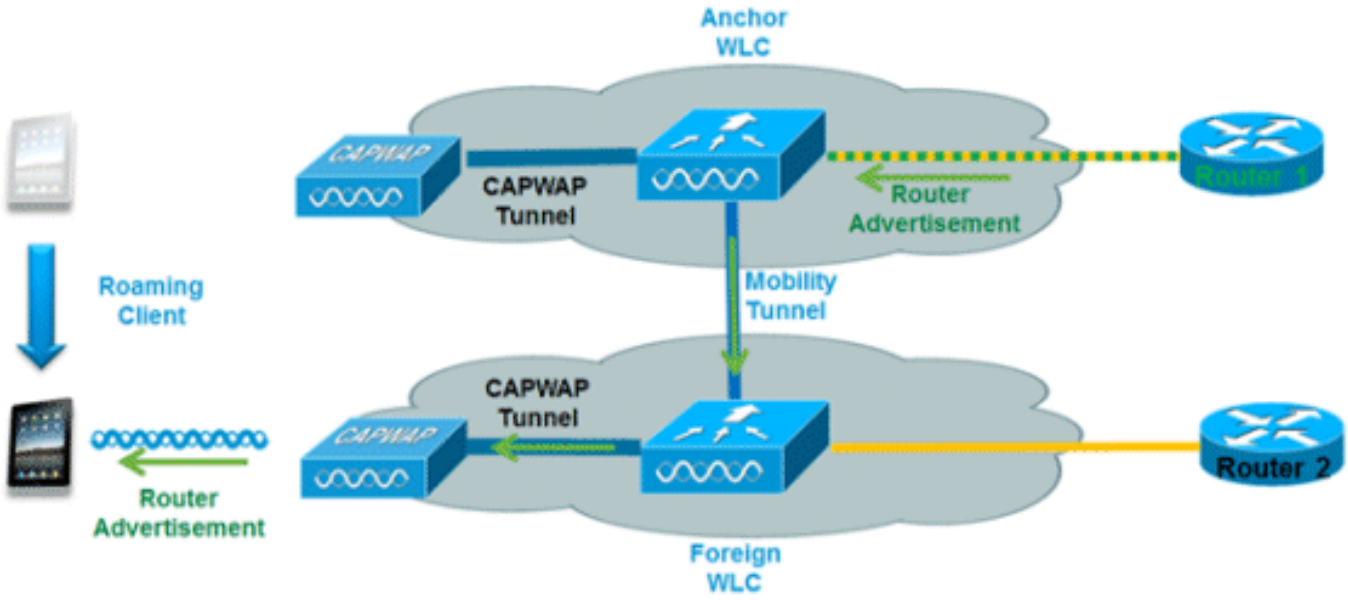
```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateful
```

```
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

Additional Information

La configuration du réseau câblé pour une connectivité IPv6 complète à l'échelle du campus à l'aide de méthodes de connectivité à double pile ou à tunnellisation sort du cadre de ce document. Pour plus d'informations, reportez-vous au guide de déploiement validé par Cisco Déploiement d'IPv6 dans les réseaux de campus.

Mobilité des clients IPv6



Afin de traiter les clients IPv6 itinérants entre les contrôleurs, les messages ICMPv6 tels que la sollicitation de voisin (NS), l'annonce de voisin (NA), l'annonce de routeur (RA) et la sollicitation de routeur (RS) doivent être traités spécialement afin de garantir qu'un client reste sur le même réseau de couche 3. La configuration de la mobilité IPv6 est identique à celle de la mobilité IPv4 et ne nécessite aucun logiciel distinct côté client pour assurer une itinérance transparente. La seule configuration requise est que les contrôleurs doivent faire partie du même groupe/domaine de mobilité.

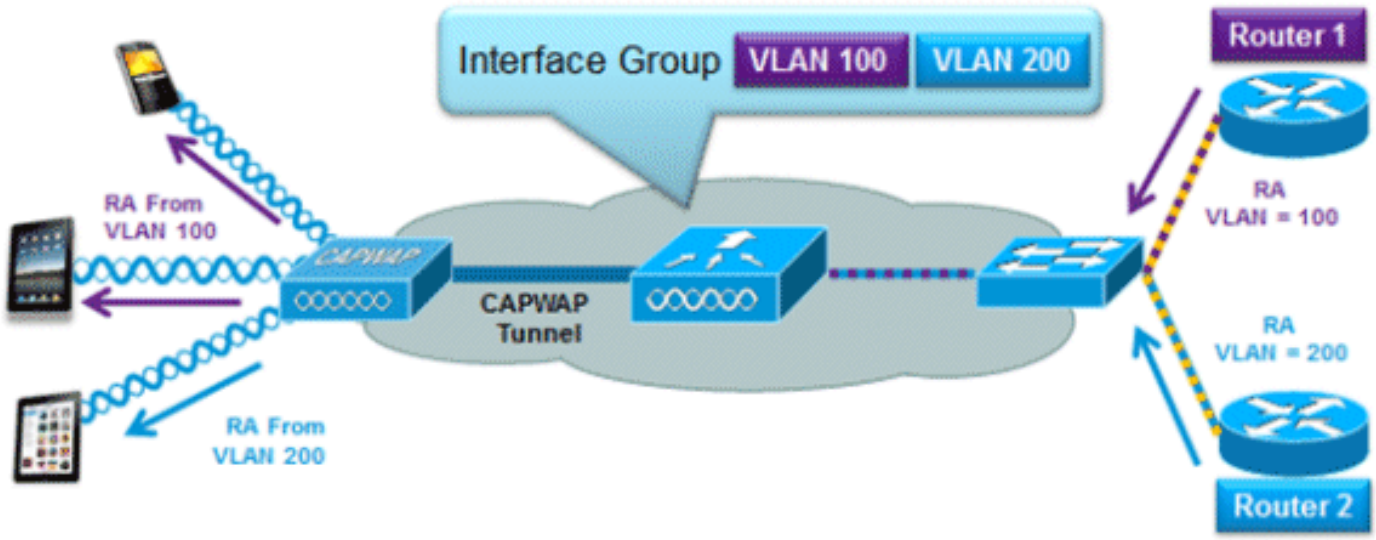
Voici le processus de mobilité des clients IPv6 entre les contrôleurs :

1. Si les deux contrôleurs ont accès au même VLAN que celui sur lequel le client se trouvait à l'origine, l'itinérance est simplement un événement d'itinérance de couche 2 où l'enregistrement du client est copié sur le nouveau contrôleur et aucun trafic n'est renvoyé au contrôleur d'ancrage.
2. Si le second contrôleur n'a pas accès au VLAN d'origine sur lequel le client se trouvait, un événement d'itinérance de couche 3 se produit, ce qui signifie que tout le trafic du client doit être tunnellisé via le tunnel de mobilité (Ethernet sur IP) vers le contrôleur d'ancrage.Afin de

s'assurer que le client conserve son adresse IPv6 d'origine, les RA du VLAN d'origine sont envoyées par le contrôleur d'ancrage au contrôleur étranger où elles sont livrées au client à l'aide de la monodiffusion L2 à partir du point d'accès.Lorsque le client en itinérance va renouveler son adresse via DHCPv6 ou générer une nouvelle adresse via SLAAC, les paquets RS, NA et NS continuent d'être tunnellisés vers le VLAN d'origine afin que le client reçoive une adresse IPv6 applicable à ce VLAN.

Remarque : la mobilité pour les clients IPv6 uniquement est basée sur les informations VLAN. Cela signifie que la mobilité du client IPv6 uniquement n'est pas prise en charge sur les VLAN non balisés.

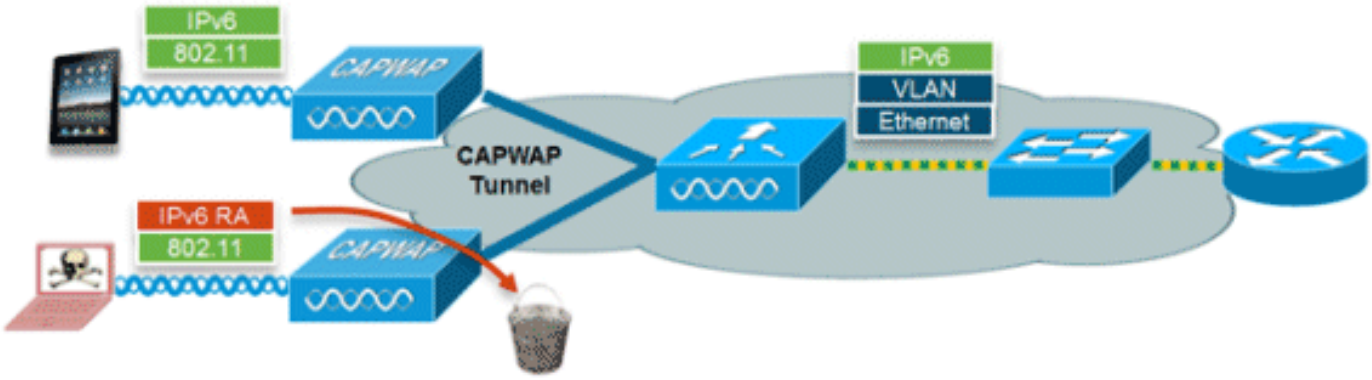
Prise en charge de VLAN Select (groupes d'interfaces)



La fonctionnalité de groupes d'interfaces permet à une organisation d'avoir un seul WLAN avec plusieurs VLAN configurés sur le contrôleur afin de permettre l'équilibrage de charge des clients sans fil sur ces VLAN. Cette fonctionnalité est généralement utilisée pour maintenir des tailles de sous-réseau IPv4 réduites tout en permettant à un WLAN d'évoluer vers des milliers d'utilisateurs sur plusieurs VLAN dans le groupe. Afin de prendre en charge les clients IPv6 avec des groupes d'interfaces, aucune configuration supplémentaire n'est requise car le système envoie automatiquement l'annonce de routeur correcte aux clients corrects via la monodiffusion sans fil de couche 2. En monodiffusion de l'annonce de routeur, les clients du même réseau local sans fil, mais d'un autre réseau local virtuel, ne reçoivent pas l'annonce de routeur incorrecte.

Sécurité au premier saut pour les clients IPv6

Protection contre les annonces de routeur



La fonction RA Guard renforce la sécurité du réseau IPv6 en supprimant les RA provenant de clients sans fil. Sans cette fonctionnalité, les clients IPv6 mal configurés ou malveillants pourraient s'annoncer comme routeur pour le réseau, souvent avec une priorité élevée qui pourrait avoir préséance sur les routeurs IPv6 légitimes.

Par défaut, RA Guard est activé au niveau du point d'accès (mais peut être désactivé au niveau du point d'accès) et est toujours activé sur le contrôleur. Il est préférable d'abandonner les RA au niveau du point d'accès, car il s'agit d'une solution plus évolutive qui fournit des compteurs améliorés d'abandon RA par client. Dans tous les cas, l'annonce de routeur IPv6 sera abandonnée à un moment donné, protégeant ainsi les autres clients sans fil et le réseau câblé en amont des clients IPv6 malveillants ou mal configurés.

Protection du serveur DHCPv6

La fonctionnalité DHCPv6 Server Guard empêche les clients sans fil de distribuer des adresses IPv6 à d'autres clients sans fil ou à des clients câblés en amont. Afin d'empêcher la distribution d'adresses DHCPv6, tous les paquets d'annonce DHCPv6 provenant de clients sans fil sont abandonnés. Cette fonctionnalité fonctionne sur le contrôleur, ne nécessite aucune configuration et est activée automatiquement.

Protection de la source IPv6

La fonction de protection de la source IPv6 empêche un client sans fil d'usurper l'adresse IPv6 d'un autre client. Cette fonctionnalité est analogue à la protection de la source IPv4. La protection de la source IPv6 est activée par défaut, mais elle peut être désactivée via l'interface de ligne de commande.

Gestion des adresses IPv6

Pour l'authentification et la gestion des comptes RADIUS, le contrôleur renvoie une adresse IP à l'aide de l'attribut « Framed-IP-address ». L'adresse IPv4 est utilisée dans ce cas.

L'attribut « Calling-Station-ID » utilise cet algorithme afin de renvoyer une adresse IP lorsque le « Call Station ID Type » sur le contrôleur est configuré sur « IP Address » :

1. Adresse IPv4
2. Adresse IPv6 de monodiffusion globale
3. Adresse IPv6 locale de liaison

Étant donné que les adresses IPv6 des clients peuvent changer fréquemment (adresses temporaires ou privées), il est important de les suivre dans le temps. Cisco NCS enregistre toutes

les adresses IPv6 utilisées par chaque client et les consigne dans l'historique chaque fois que le client se déplace ou établit une nouvelle session. Ces enregistrements peuvent être configurés sur NCS pour être conservés pendant un an maximum.

Remarque : la valeur par défaut du « Call Station ID Type » sur le contrôleur a été remplacée par « System MAC Address » dans la version 7.2. Lors d'une mise à niveau, cette option doit être modifiée pour permettre un suivi unique des clients par adresse MAC, car les adresses IPv6 peuvent changer en cours de session et entraîner des problèmes de comptabilité si l'ID de la station d'appel est défini sur l'adresse IP.

Listes de contrôle d'accès IPv6

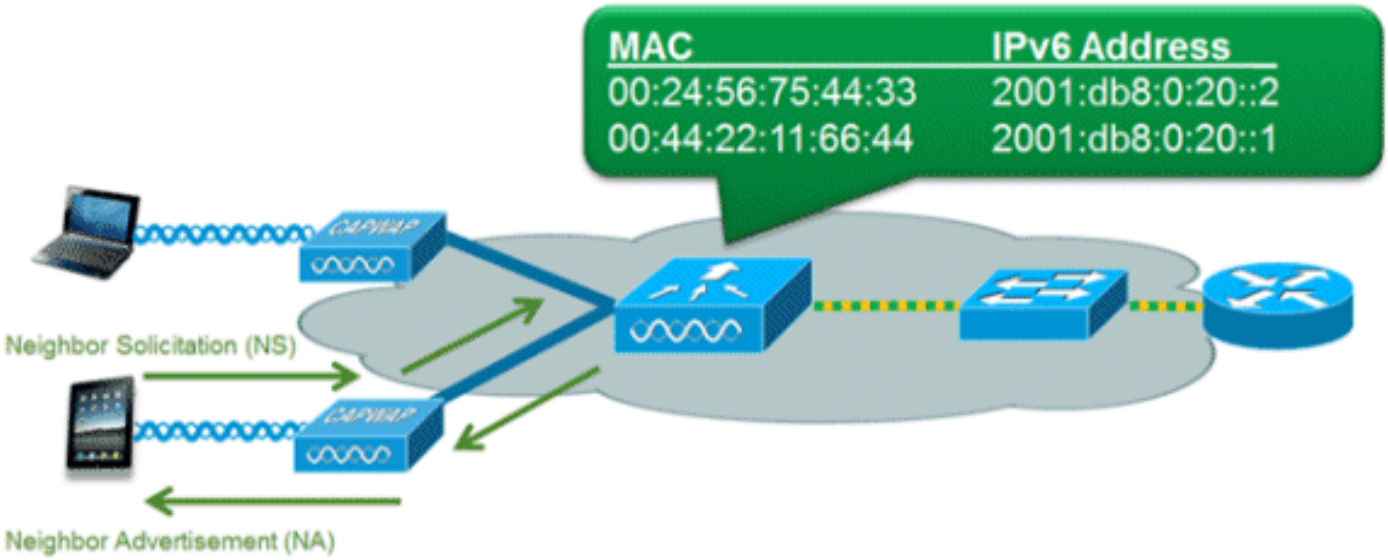
Afin de restreindre l'accès à certaines ressources câblées en amont ou de bloquer certaines applications, des listes de contrôle d'accès IPv6 peuvent être utilisées pour identifier le trafic et l'autoriser ou le refuser. Les listes de contrôle d'accès IPv6 prennent en charge les mêmes options que les listes de contrôle d'accès IPv4, notamment la source, la destination, le port source et le port de destination (les plages de ports sont également prises en charge). Les listes de contrôle d'accès de pré-authentification sont également prises en charge pour prendre en charge l'authentification des invités IPv6 via un serveur Web externe. Le contrôleur sans fil prend en charge jusqu'à 64 listes de contrôle d'accès IPv6 uniques avec 64 règles uniques dans chacune. Le contrôleur sans fil continue de prendre en charge 64 listes de contrôle d'accès IPv4 uniques supplémentaires avec 64 règles uniques dans chacune pour un total de 128 listes de contrôle d'accès pour un client à double pile.

Remplacement AAA pour les ACL IPv6

Afin de prendre en charge le contrôle d'accès centralisé via un serveur AAA centralisé tel que Cisco Identity Services Engine (ISE) ou ACS, la liste de contrôle d'accès IPv6 peut être provisionnée par client à l'aide des attributs AAA Override. Pour utiliser cette fonctionnalité, la liste de contrôle d'accès IPv6 doit être configurée sur le contrôleur et le WLAN doit être configuré avec la fonctionnalité AAA Override activée. L'attribut AAA réellement nommé pour une liste de contrôle d'accès IPv6 est ***Airespace-IPv6-ACL-Name*** similaire à l'attribut *Airespace-ACL-Name* utilisé pour provisionner une liste de contrôle d'accès basée sur IPv4. L'attribut AAA retourné le contenu doit être une chaîne égale au nom de la liste de contrôle d'accès IPv6 telle que configurée sur le contrôleur.

Optimisation des paquets pour les clients IPv6

Mise en cache de découverte voisine



Le protocole NDP (neighbor discovery protocol) IPv6 utilise des paquets NAT et NS à la place du protocole ARP (Address Resolution Protocol) afin de permettre aux clients IPv6 de résoudre l'adresse MAC d'autres clients sur le réseau. Le processus NDP peut être très bavard, car il utilise initialement des adresses de multidiffusion pour effectuer la résolution d'adresse ; cela peut consommer un temps d'antenne sans fil précieux, car les paquets de multidiffusion sont envoyés à tous les clients sur le segment de réseau.

Afin d'augmenter l'efficacité du processus NDP, la mise en cache de découverte de voisins permet au contrôleur d'agir en tant que proxy et de répondre aux requêtes NS qu'il peut résoudre. La mise en cache de découverte de voisin est rendue possible par la table de liaison de voisinage sous-jacente présente dans le contrôleur. La table de liaison de voisinage conserve une trace de chaque adresse IPv6 et de son adresse MAC associée. Lorsqu'un client IPv6 tente de résoudre l'adresse de couche liaison d'un autre client, le paquet NS est intercepté par le contrôleur qui répond avec un paquet NA.

Limitation des annonces de routeur

La limitation des annonces de routeur permet au contrôleur d'appliquer une limitation de débit des RA dirigés vers le réseau sans fil. En activant la limitation de RA, les routeurs qui sont configurés pour envoyer des RA très souvent (par exemple, toutes les trois secondes) peuvent être raccourcis à une fréquence minimale qui maintiendra toujours la connectivité du client IPv6. Cela permet d'optimiser le temps d'antenne en réduisant le nombre de paquets de multidiffusion qui doivent être envoyés. Dans tous les cas, si un client envoie un RS, alors un RA sera autorisé par le contrôleur et monodiffusion au client demandeur. Cela permet de s'assurer que les nouveaux clients ou les clients en itinérance ne sont pas affectés négativement par la limitation RA.

Accès invité IPv6

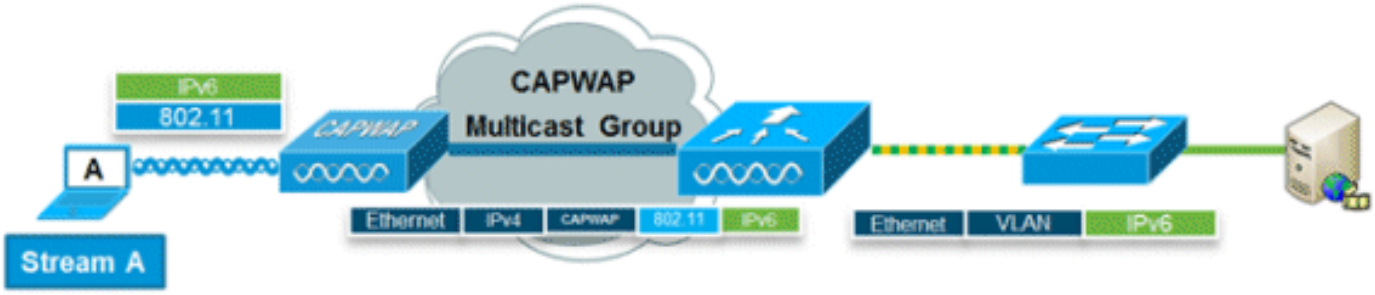
Les fonctionnalités d'invité sans fil et filaire présentes pour les clients IPv4 fonctionnent de la même manière pour les clients à double pile et pour les clients IPv6 uniquement. Une fois l'utilisateur invité associé, il passe à l'état d'exécution « WEB_AUTH_REQ » jusqu'à ce que le client soit authentifié via le portail captif IPv4 ou IPv6. Le contrôleur intercepte le trafic HTTP/HTTPS IPv4 et IPv6 dans cet état et le redirige vers l'adresse IP virtuelle du contrôleur. Une fois que l'utilisateur est authentifié via le portail captif, son adresse MAC passe à l'état d'exécution et le trafic IPv4 et IPv6 est autorisé à passer. Pour l'authentification Web externe, la liste de contrôle d'accès de pré-authentification permet d'utiliser un serveur Web externe.

Afin de prendre en charge la redirection de clients IPv6 uniquement, le contrôleur crée automatiquement une adresse virtuelle IPv6 basée sur l'adresse virtuelle IPv4 configurée sur le contrôleur. L'adresse IPv6 virtuelle respecte la convention de `[::ffff:<adresse IPv4 virtuelle>]`. Par exemple, une adresse IP virtuelle de 1.1.1.1 serait traduite en `[::ffff:1.1.1.1]`.

Lorsque vous utilisez un certificat SSL approuvé pour l'authentification d'accès invité, assurez-vous que les adresses virtuelles IPv4 et IPv6 du contrôleur sont définies dans DNS pour correspondre au nom d'hôte des certificats SSL. Cela garantit que les clients ne reçoivent pas d'avertissement de sécurité indiquant que le certificat ne correspond pas au nom d'hôte du périphérique.

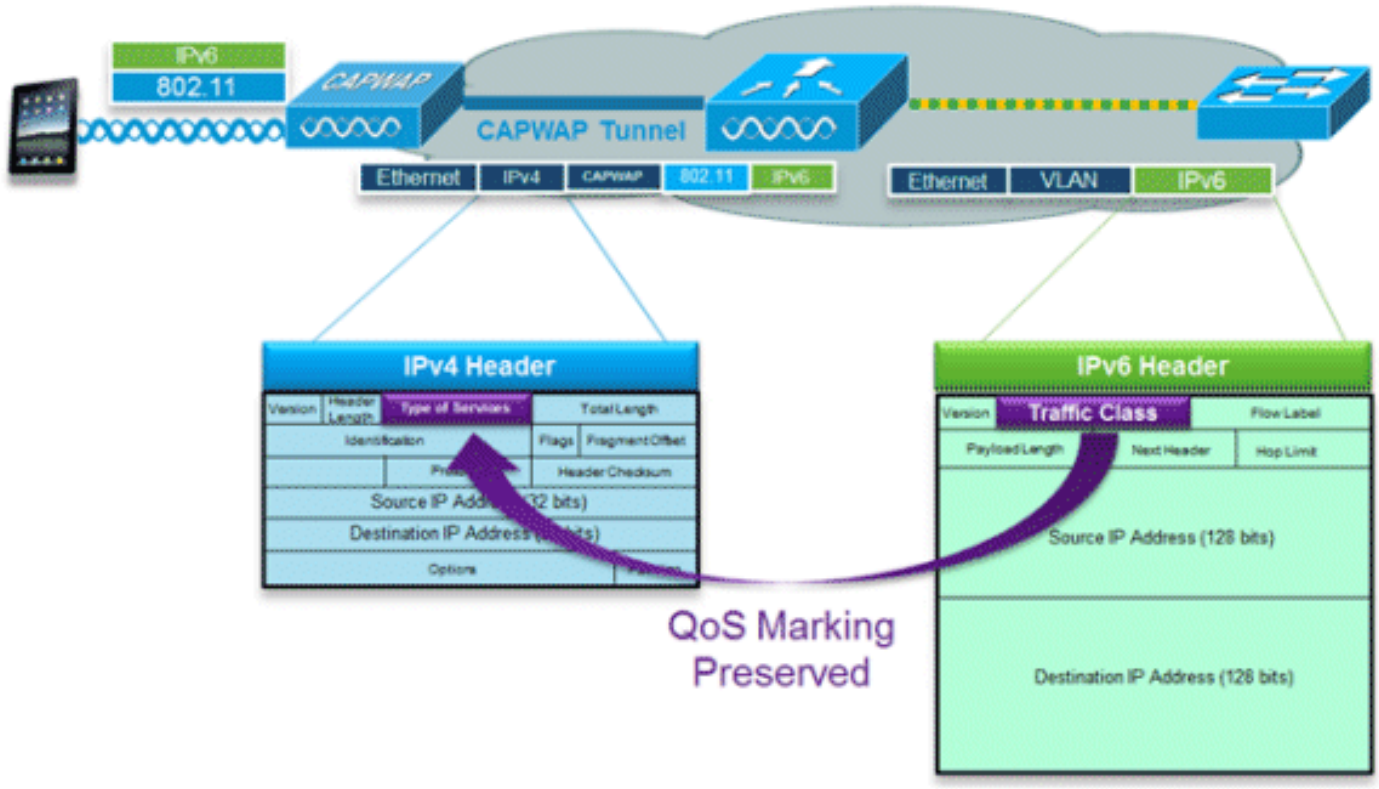
Remarque : le certificat SSL généré automatiquement par le contrôleur ne contient pas l'adresse virtuelle IPv6. Certains navigateurs Web peuvent alors afficher un avertissement de sécurité. Il est recommandé d'utiliser un certificat SSL approuvé pour l'accès invité.

VideoStream IPv6



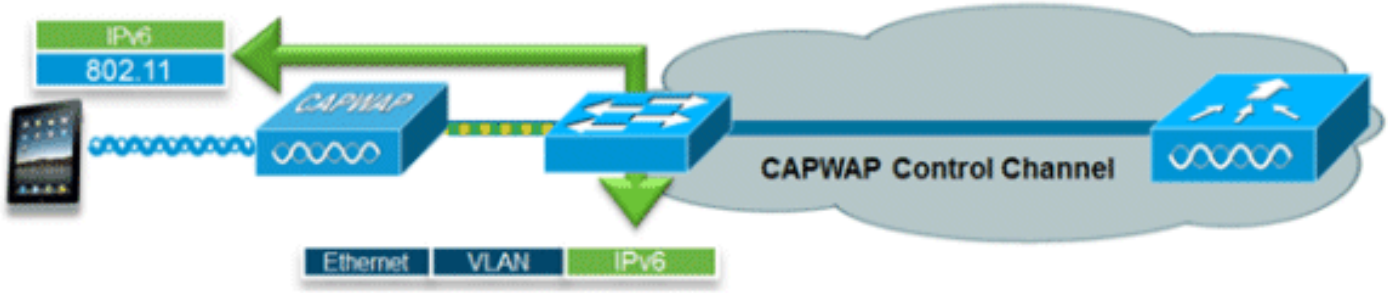
VideoStream permet une diffusion vidéo multidiffusion sans fil fiable et évolutive, envoyant le flux à chaque client dans un format monodiffusion. La conversion de multidiffusion en monodiffusion (de L2) se produit au niveau du point d'accès, fournissant ainsi une solution évolutive. Le contrôleur envoie le trafic vidéo IPv6 à l'intérieur d'un tunnel de multidiffusion CAPWAP IPv4 qui permet une distribution réseau efficace au point d'accès.

Qualité de service IPv6



Les paquets IPv6 utilisent un marquage similaire à l'utilisation par IPv4 des valeurs DSCP prenant en charge jusqu'à 64 classes de trafic différentes (0-63). Pour les paquets en aval du réseau câblé, la valeur de la classe de trafic IPv6 est copiée dans l'en-tête du tunnel CAPWAP afin de garantir que la qualité de service est préservée de bout en bout. En amont, la même chose se produit lorsque le trafic client marqué au niveau de la couche 3 avec la classe de trafic IPv6 sera respecté en marquant les paquets CAPWAP destinés au contrôleur.

IPv6 et FlexConnect



FlexConnect - Commutation locale WLAN

En mode de commutation locale, FlexConnect prend en charge les clients IPv6 en pontant le trafic vers le VLAN local, de la même manière que le fonctionnement IPv4. La mobilité des clients est prise en charge pour l'itinérance de couche 2 dans le groupe FlexConnect.

Les fonctionnalités spécifiques à IPv6 suivantes sont prises en charge en mode de commutation locale FlexConnect :

- Protection RA IPv6
- Pontage IPv6
- Authentification des invités IPv6 (hébergée par un contrôleur)

Ces fonctionnalités spécifiques à IPv6 ne sont pas prises en charge en mode de commutation locale FlexConnect :

- Mobilité de couche 3
- VideoStream IPv6
- Listes de contrôle d'accès IPv6
- Protection de la source IPv6
- Protection du serveur DHCPv6
- Mise en cache de découverte voisine
- Limitation des annonces de routeur

FlexConnect - Commutation centrale WLAN

Pour les points d'accès en mode FlexConnect utilisant la commutation centrale (transmission tunnel du trafic vers le contrôleur), le contrôleur doit être défini sur « Multicast - Unicast Mode » pour le « AP Multicast Mode ». Comme les points d'accès FlexConnect ne rejoignent pas le groupe de multidiffusion CAPWAP du contrôleur, les paquets de multidiffusion doivent être répliqués au niveau du contrôleur et monodiffusés individuellement vers chaque point d'accès. Cette méthode est moins efficace que « Multicast - Multicast Mode » et impose une charge supplémentaire sur le contrôleur.

Cette fonctionnalité spécifique à IPv6 n'est pas prise en charge en mode de commutation FlexConnect Central :

- VideoStream IPv6

Remarque : les WLAN à commutation centrale exécutant IPv6 ne sont pas pris en charge sur le contrôleur Flex 7500.

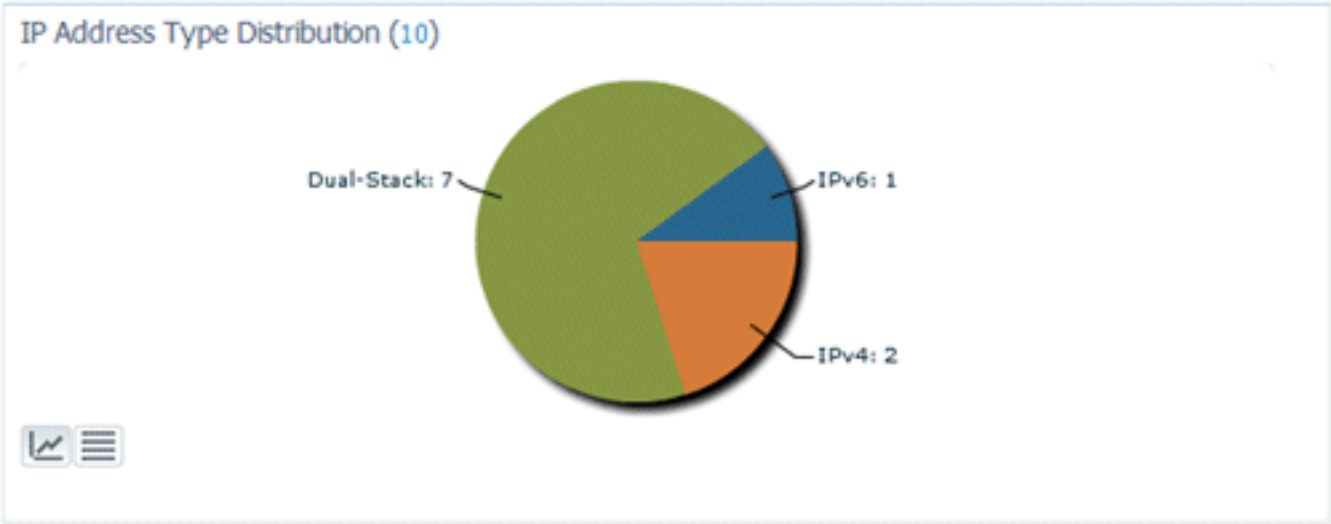
Visibilité des clients IPv6 avec NCS

Avec la version NCS v1.1, de nombreuses fonctionnalités IPv6 supplémentaires sont ajoutées pour surveiller et gérer un réseau de clients IPv6 sur les réseaux filaires et sans fil.

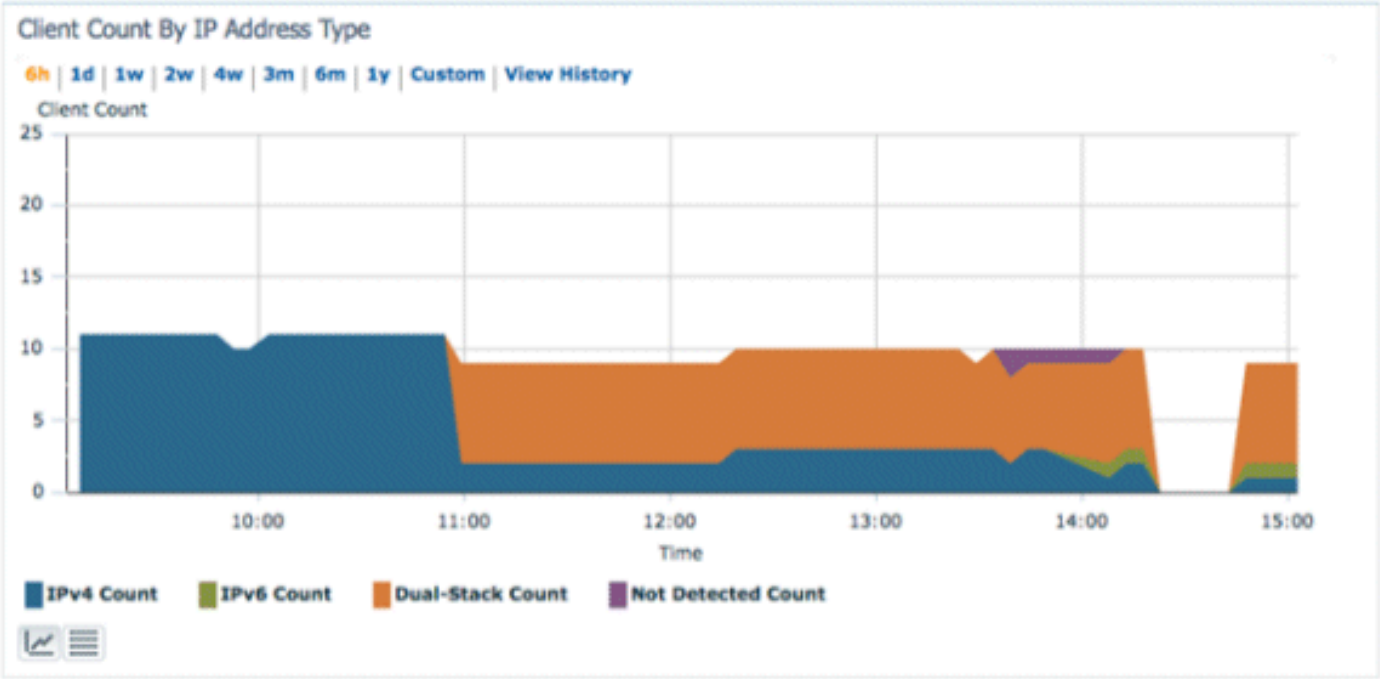
Éléments du tableau de bord IPv6

Afin de visualiser les types de clients présents sur le réseau, un « dashlet » dans NCS est disponible afin de fournir un aperçu des statistiques spécifiques à IPv6 et d'offrir la possibilité d'explorer les clients IPv6 vers le bas.

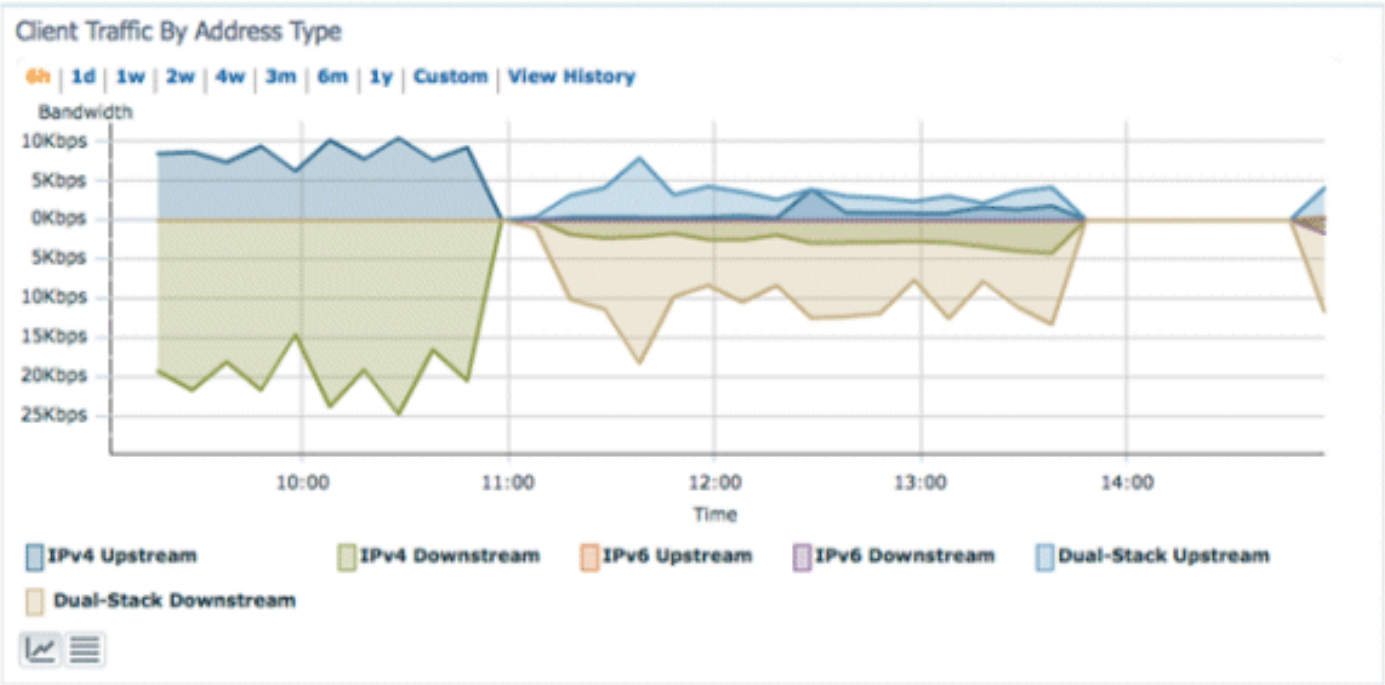
IP Address Type Dashlet : affiche les types de clients IP sur le réseau :



Client Count by IP Address Type : affiche le type de client IP au fil du temps :



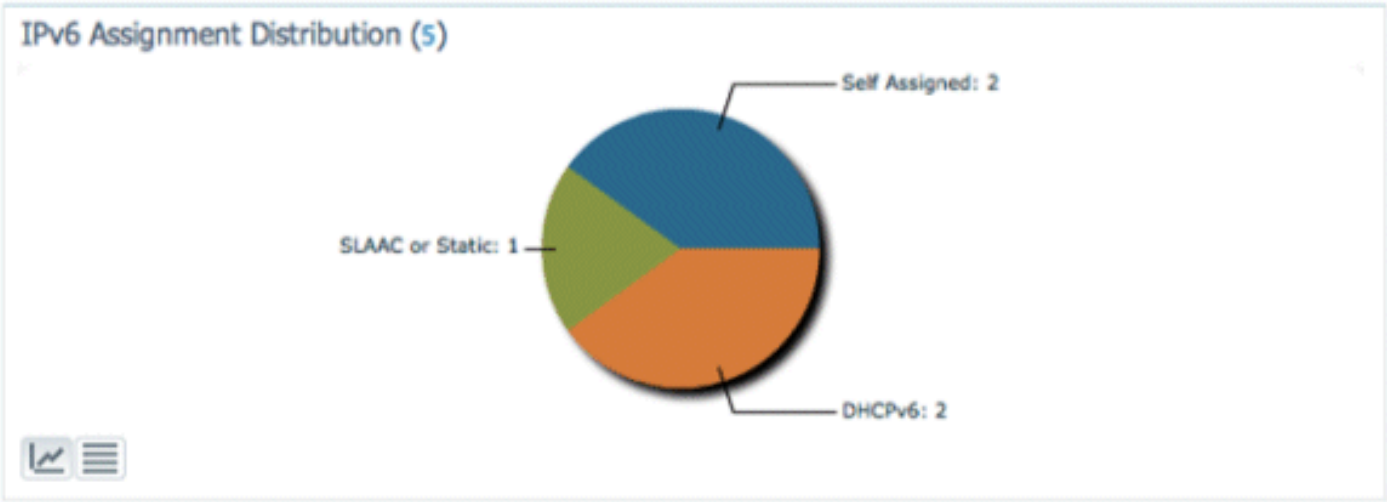
Trafic client par type d'adresse IP - Affiche le trafic de chaque type de client. Les clients de la catégorie dual-stack incluent le trafic IPv4 et IPv6 :



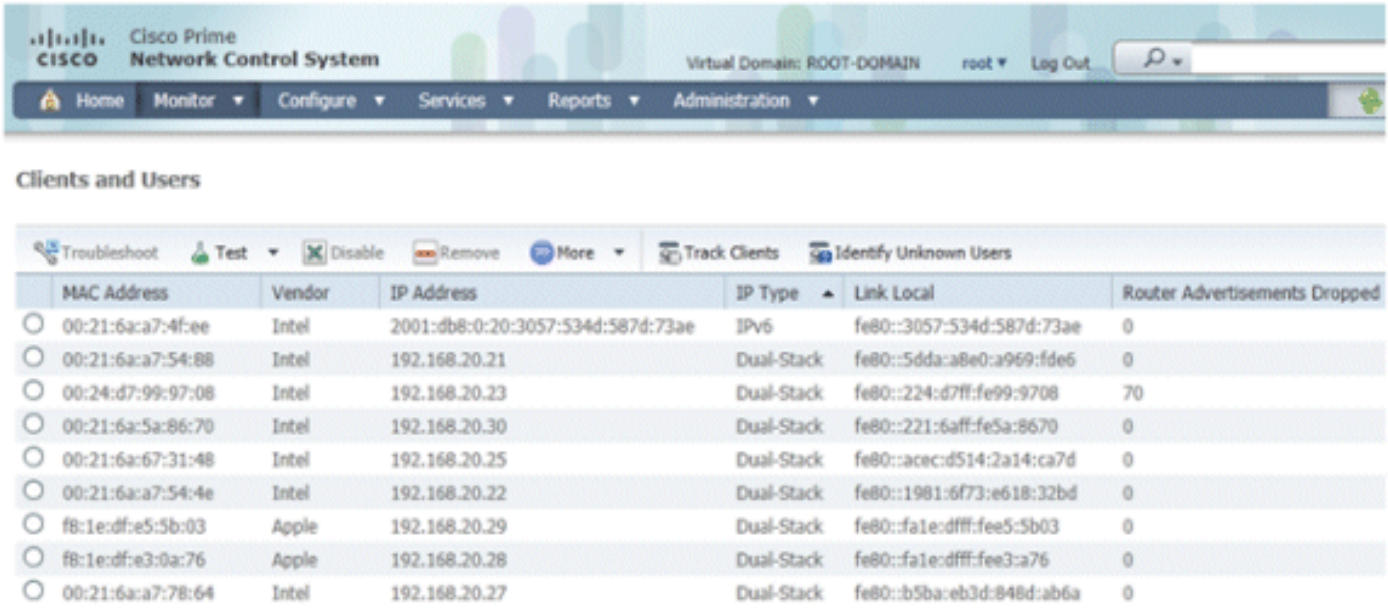
IPv6 Address Assignment : affiche la méthode d'attribution d'adresse pour chaque client dans l'une des quatre catégories suivantes :

- DHCPv6 : pour les clients dont les adresses sont attribuées par un serveur central. Le client peut également avoir une adresse SLAAC.
- SLAAC ou Statique : pour les clients utilisant l'affectation automatique d'adresses sans état ou utilisant des adresses configurées de manière statique.
- Inconnu : dans certains cas, l'attribution d'adresses IPv6 ne peut pas être détectée.Cette condition se produit uniquement sur les clients filaires dans NCS, car certains commutateurs ne surveillent pas les informations d'attribution d'adresse IPv6.
- Auto-assigné : pour les clients dont l'adresse link-local est entièrement auto-assignée.Les clients de cette catégorie peuvent présenter des problèmes de connectivité IPv6, car il leur manque une adresse unique globale ou locale.

Chacune des sections du graphique à secteurs est accessible en cliquant dessus, ce qui permet à l'administrateur d'effectuer une hiérarchisation vers le bas vers une liste de clients.



Surveiller les clients IPv6



Afin de surveiller et de gérer les informations client IPv6, ces colonnes ont été ajoutées à la page Clients et utilisateurs :

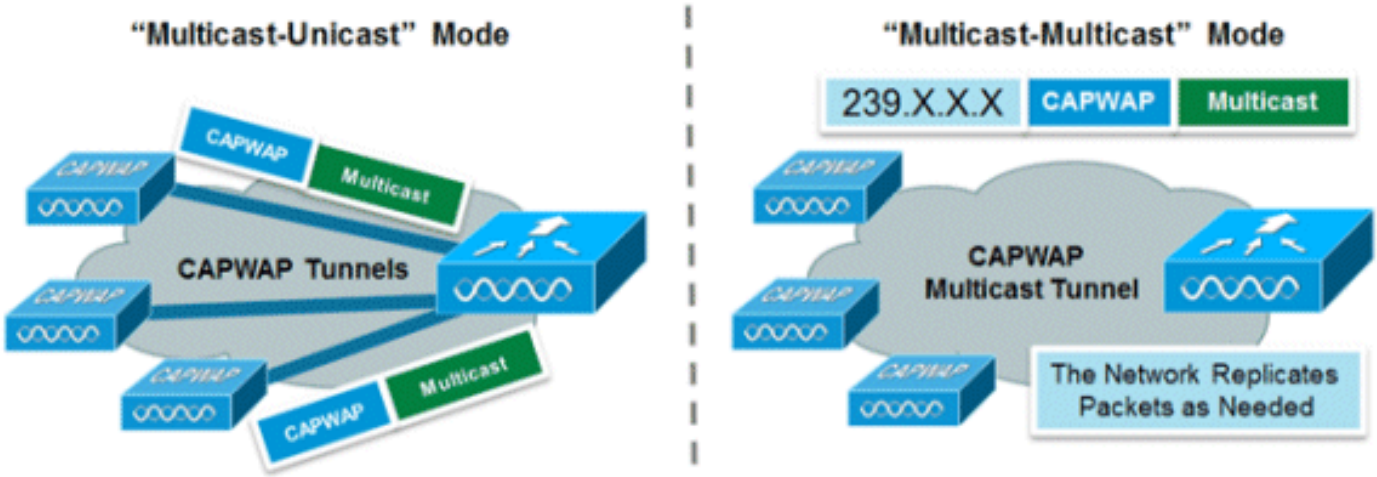
- IP Type (Type IP) : type de client en fonction des adresses IP vues par le client. Les options possibles sont IPv4, IPv6 ou Dual-Stack, ce qui signifie qu'un client possède des adresses IPv4 et IPv6.
- Type d'affectation IPv6 : la méthode d'affectation d'adresse est détectée par NCS comme étant SLAAC ou statique, DHCPv6, auto-affecté ou inconnu.
- Global Unique : adresse globale IPv6 la plus récente utilisée par le client. Le passage de la souris sur le contenu de la colonne indique les adresses uniques globales IPv6 supplémentaires utilisées par le client.
- Local Unique : adresse IPv6 locale unique la plus récente utilisée par le client. Si vous passez le curseur sur le contenu de la colonne, vous voyez les adresses uniques globales IPv6 supplémentaires utilisées par le client.
- Link Local (Liaison locale) : adresse IPv6 du client qui est auto-attribuée et utilisée pour la communication avant toute autre adresse IPv6.
- Annonces de routeur abandonnées : nombre d'annonces de routeur envoyées par le client et abandonnées au niveau du point d'accès. Cette colonne peut être utilisée pour suivre les clients qui peuvent être mal configurés ou configurés de manière malveillante pour agir comme un routeur IPv6. Cette colonne est triable, ce qui permet d'identifier facilement les clients contrevenants.

Outre les colonnes IPv6 spécifiques, la colonne IP Address affiche l'adresse IP actuelle du client avec une priorité pour afficher d'abord l'adresse IPv4 (dans le cas d'un client à double pile) ou l'adresse IPv6 Global Unique dans le cas d'un client IPv6 uniquement.

Configuration pour la prise en charge du client IPv6 sans fil

Mode de distribution multidiffusion vers les points d'accès

Le réseau sans fil unifié Cisco prend en charge deux méthodes de distribution multidiffusion vers les points d'accès associés au contrôleur. Dans les deux modes, le paquet multicast d'origine provenant du réseau câblé est encapsulé dans un paquet CAPWAP de couche 3 envoyé au point d'accès par monodiffusion ou multidiffusion CAPWAP. Puisque le trafic est encapsulé CAPWAP, les AP ne doivent pas être sur le même VLAN que le trafic client. Les deux méthodes de distribution multidiffusion sont comparées ici :



	Mode Multicast-unicast	Mode multidiffusion-multidiffusion
Mécanisme D'Émission	Le contrôleur réplique le paquet multicast et l'envoie à chaque point d'accès dans un tunnel CAPWAP monodiffusion	Le contrôleur envoie une copie du paquet de multidiffusion
Modes AP pris en charge	FlexConnect et local	Mode local uniquement
Nécessite un routage multidiffusion de couche 3 sur le réseau câblé	Non	Oui
Chargement du contrôleur	Élevé	Faible
Chargement du réseau câblé	Élevé	Faible

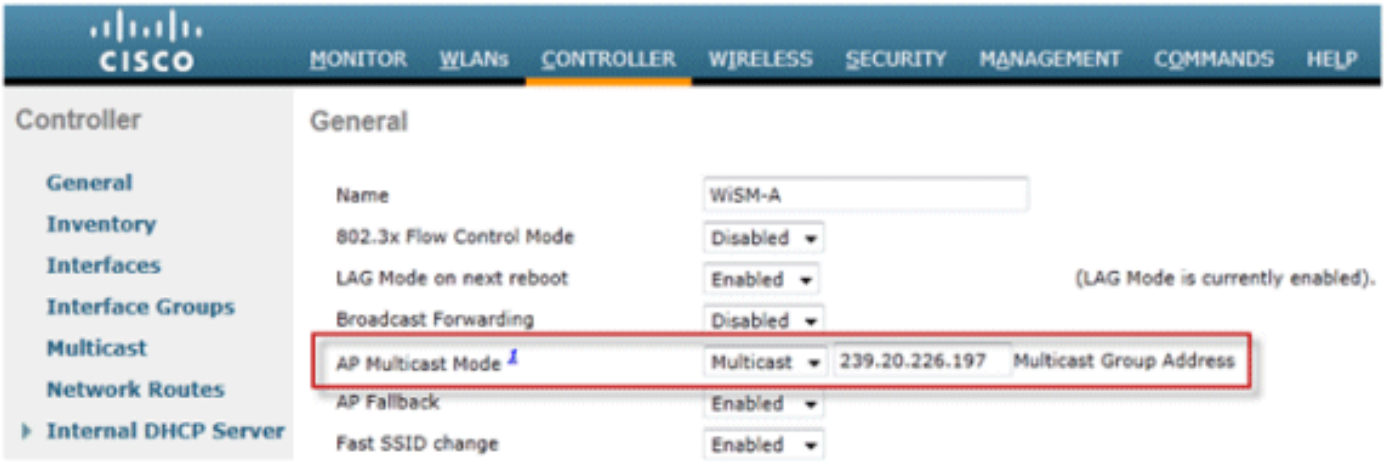
Configuration du mode de distribution multidiffusion-multidiffusion

Le mode multidiffusion est recommandé pour des raisons d'évolutivité et d'efficacité de la bande

passante filaire.

Remarque : cette étape n'est absolument nécessaire que pour le contrôleur sans fil de la gamme 2500, mais elle permet une transmission multidiffusion plus efficace et est recommandée pour toutes les plates-formes de contrôleur.

Accédez à l'onglet « Controller » sous la page « General » et assurez-vous que le mode multidiffusion AP est configuré pour utiliser le mode **multidiffusion** et qu'une adresse de groupe valide est configurée. L'adresse de groupe est un groupe de multidiffusion IPv4 et il est recommandé de l'inclure dans la plage 239.X.X.X-239.255.255.255, qui est étendue pour les applications de multidiffusion privées.

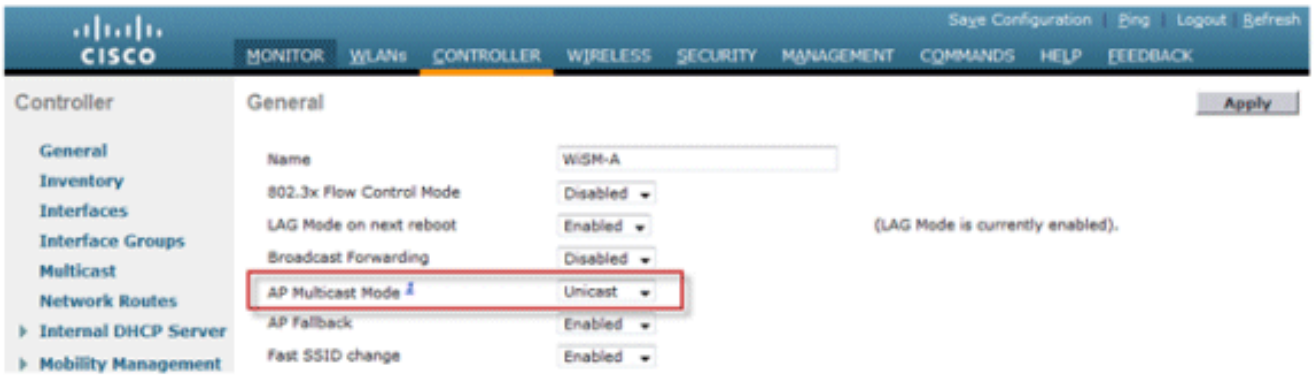


Remarque : n'utilisez pas les plages d'adresses 224.X.X.X, 239.0.0.X ou 239.128.0.X pour l'adresse du groupe de multidiffusion. Les adresses de ces plages chevauchent les adresses MAC locales de la liaison et inondent tous les ports du commutateur, même lorsque la surveillance IGMP est activée.

Configuration du mode de distribution multidiffusion-monodiffusion

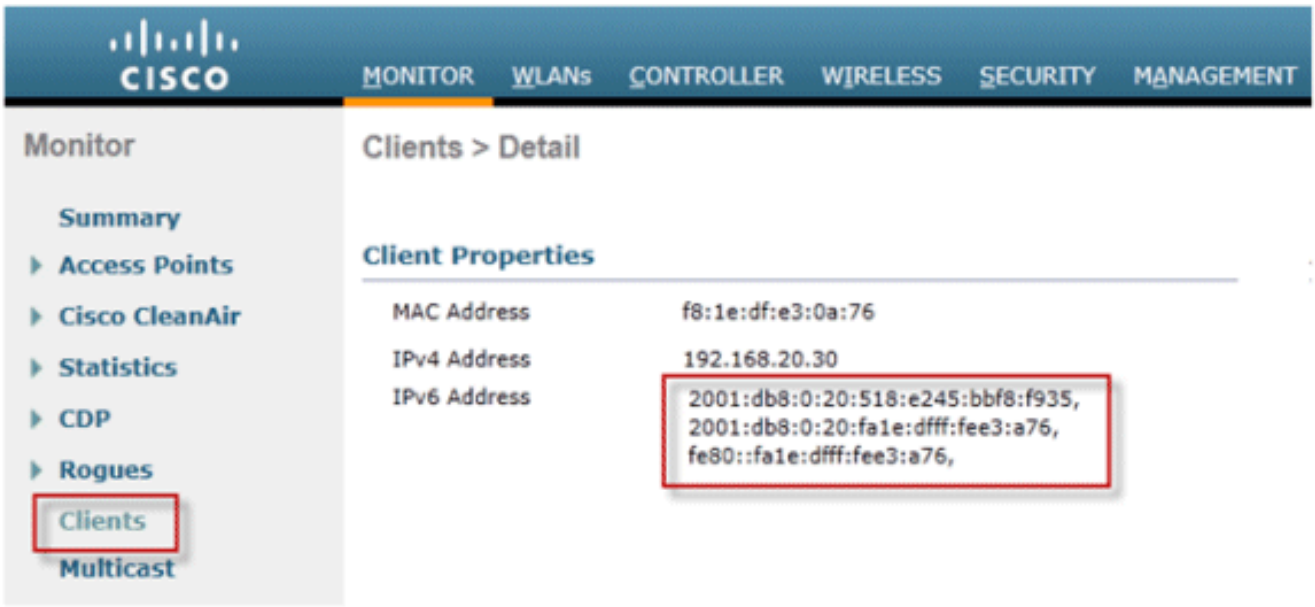
Si le réseau filaire n'est pas correctement configuré pour fournir la multidiffusion CAPWAP entre le contrôleur et le mode AP ou FlexConnect, et que les AP seront utilisés pour les WLAN à commutation centrale prenant en charge IPv6, alors le mode monodiffusion est requis.

1. Accédez à l'onglet **Controller** sous la page General, et assurez-vous que le mode multidiffusion AP est configuré pour utiliser le mode **monodiffusion**.



2. Connectez un client compatible IPv6 au réseau local sans fil. Vérifiez que le client reçoit une adresse IPv6 en accédant à l'onglet **Monitor**, puis au menu

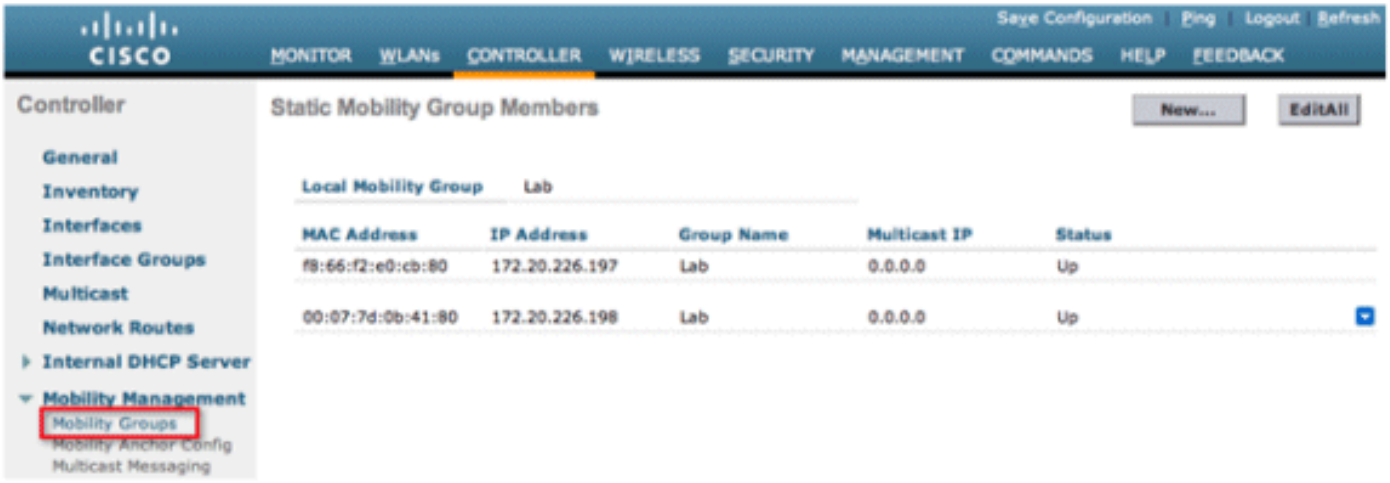
Clients.



Configuration de la mobilité IPv6

Il n'existe aucune configuration spécifique pour la mobilité IPv6, sauf pour placer les contrôleurs dans le même groupe de mobilité ou dans le même domaine de mobilité. Cela permet à un total de 72 contrôleurs de participer à un domaine de mobilité offrant une mobilité transparente, même pour les plus grands campus.

Accédez à l'onglet **Controller > Mobility Groups**, et ajoutez chaque contrôleur par adresse MAC et adresse IP dans le groupe. Cette opération doit être effectuée sur tous les contrôleurs du groupe de mobilité.

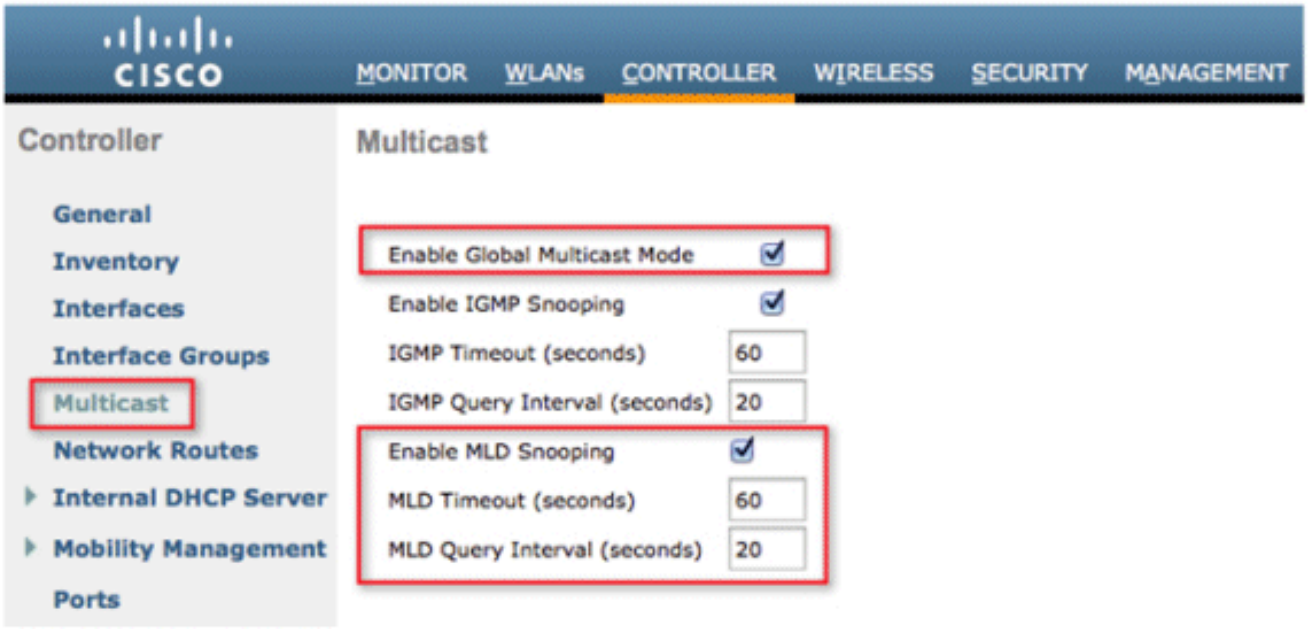


Configuration de la multidiffusion IPv6

Le contrôleur prend en charge la surveillance MLDv1 pour la multidiffusion IPv6, ce qui lui permet d'effectuer un suivi intelligent des flux de multidiffusion et de les transmettre aux clients qui en font la demande.

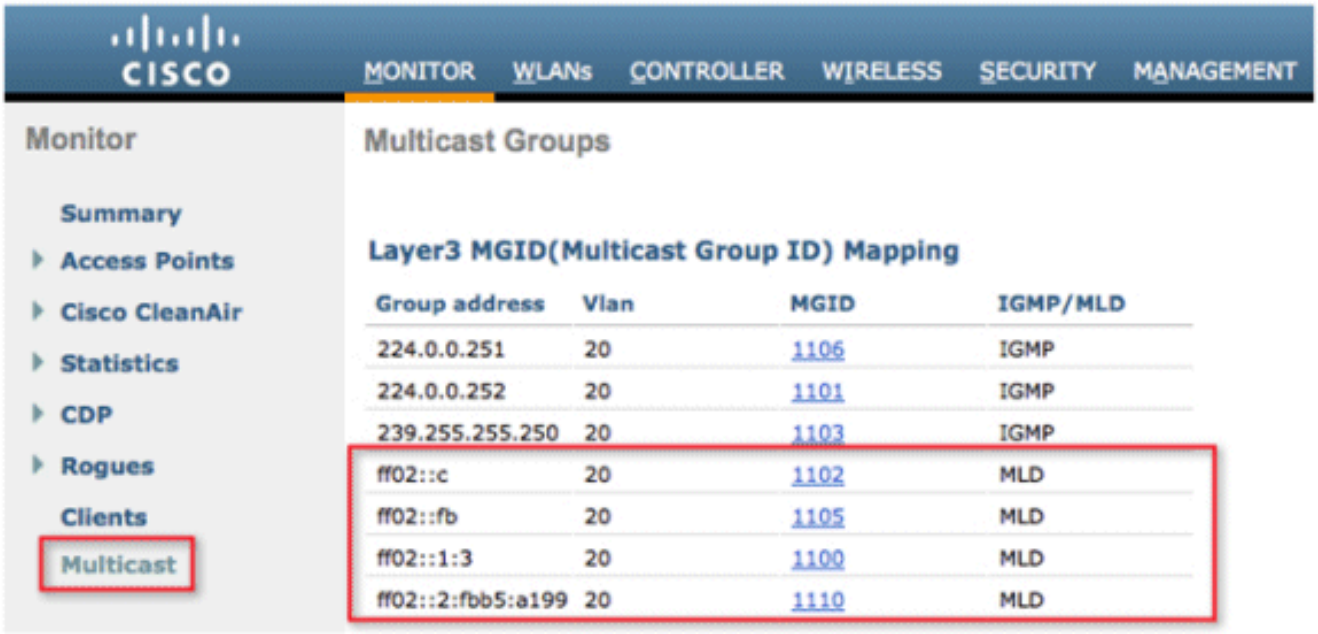
Remarque : contrairement aux versions précédentes, la prise en charge du trafic de monodiffusion IPv6 ne nécessite pas l'activation du mode de multidiffusion globale sur le contrôleur. La prise en charge du trafic de monodiffusion IPv6 est activée automatiquement.

1. Accédez à l'onglet **Controller > Multicast** page et **Enable MLD Snooping** afin de prendre en charge le trafic IPv6 de multidiffusion. Pour que la multidiffusion IPv6 soit activée, le **mode multidiffusion globale** du contrôleur doit également être activé.



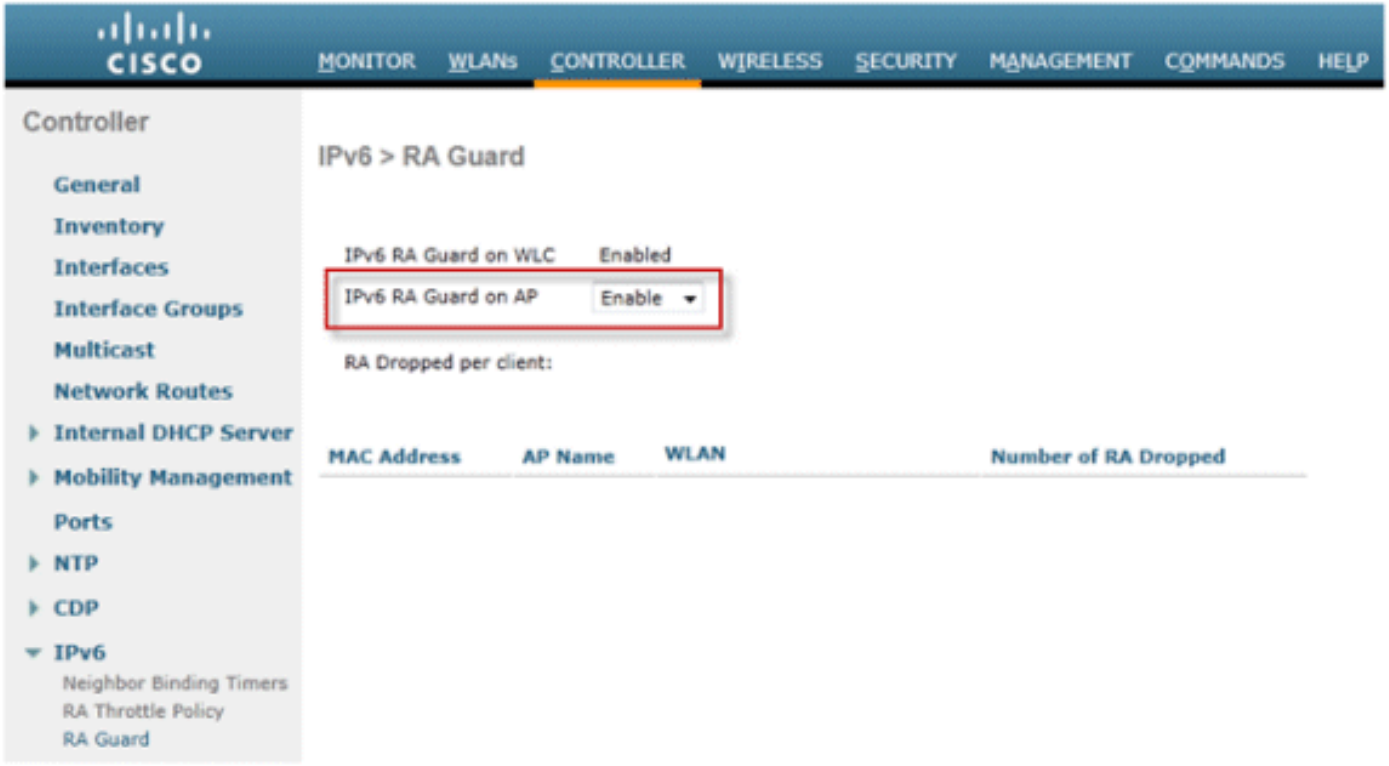
Remarque : le mode multidiffusion globale, IGMP et la surveillance MLD doivent être activés si des applications de détection peer-to-peer, telles que Bonjour d'Apple, sont requises.

2. Afin de vérifier que le trafic de multidiffusion IPv6 est surveillé, accédez à l'onglet **Monitor** et à la page **Multicast**. Notez que les groupes de multidiffusion IPv4 (IGMP) et IPv6 (MLD) sont répertoriés. Cliquez sur le MGID afin d'afficher les clients sans fil joints à cette adresse de groupe.



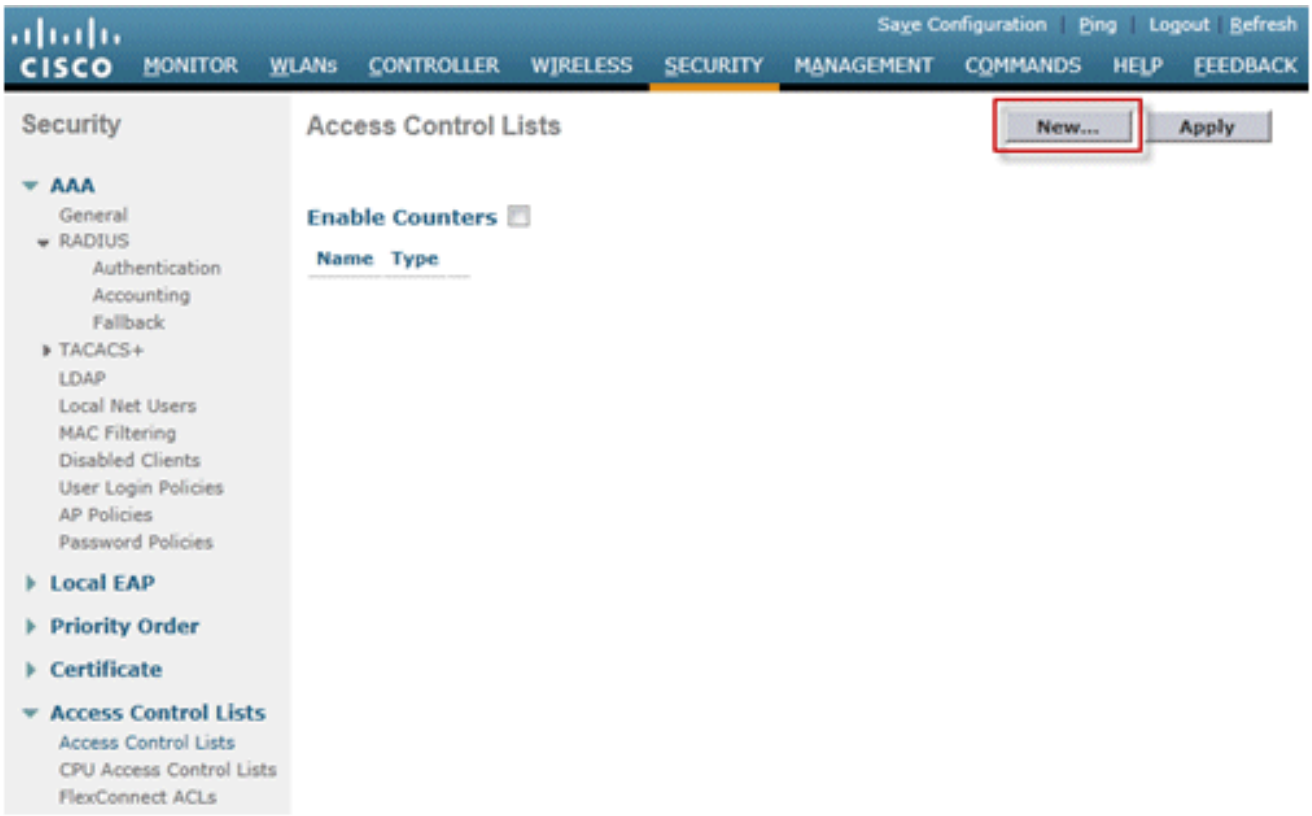
Configuration de la protection RA IPv6

Accédez à l'onglet **Controller**, puis à **IPv6 > RA Guard** dans le menu de gauche. **Activez** IPv6 RA Guard sur le point d'accès. Impossible de désactiver RA Guard sur le contrôleur. Outre la configuration de RA Guard, cette page présente également tous les clients identifiés comme étant des RA émetteurs.



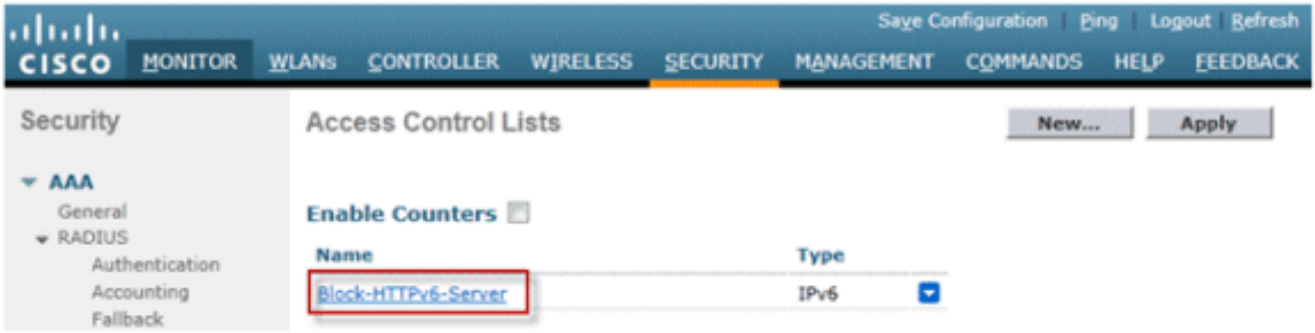
Configuration des listes de contrôle d'accès IPv6

1. Accédez à l'onglet **Security**, ouvrez **Access Control Lists**, et cliquez sur **New**.

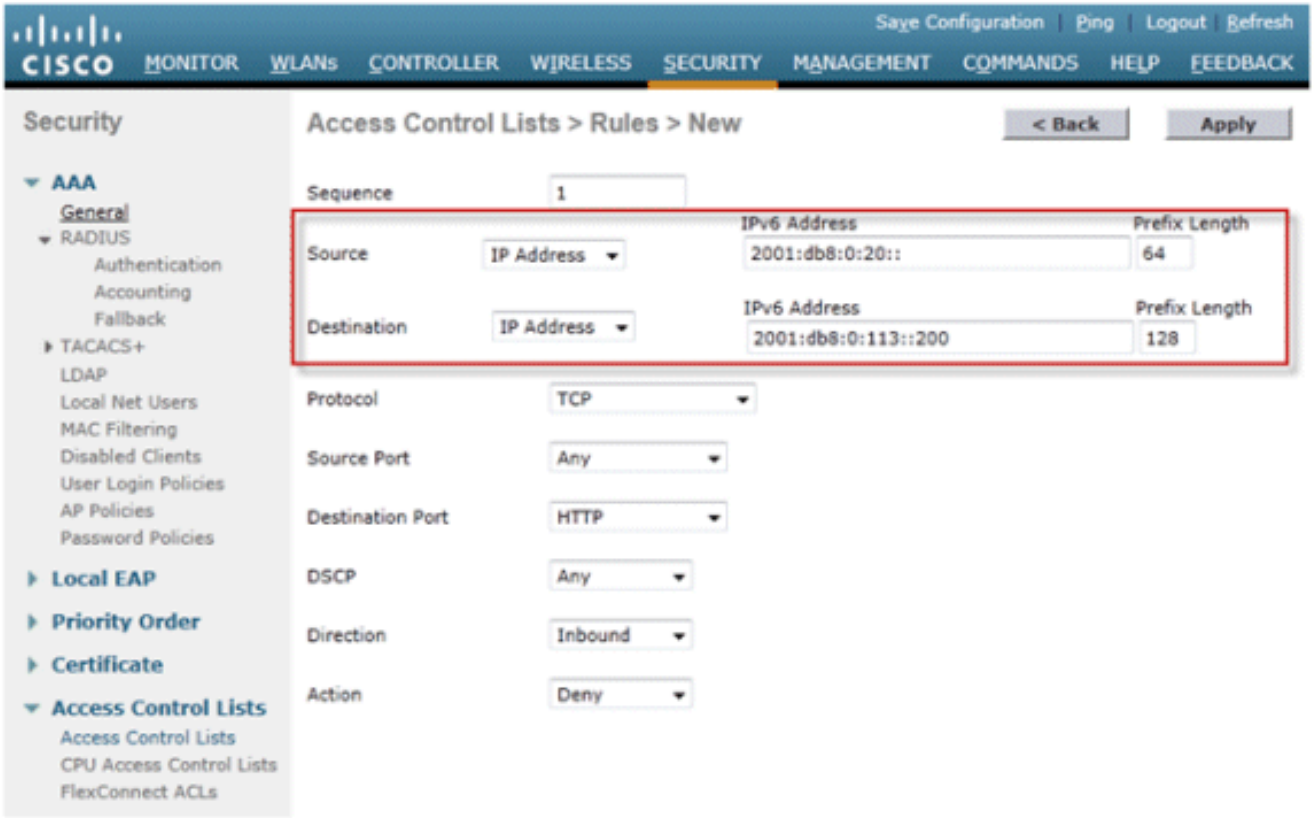


2. Entrez un nom unique pour la liste de contrôle d'accès, changez le type de liste de contrôle d'accès en **IPv6**, et cliquez sur **Apply**.

3. Cliquez sur la nouvelle liste de contrôle d'accès créée au cours des étapes ci-dessus.

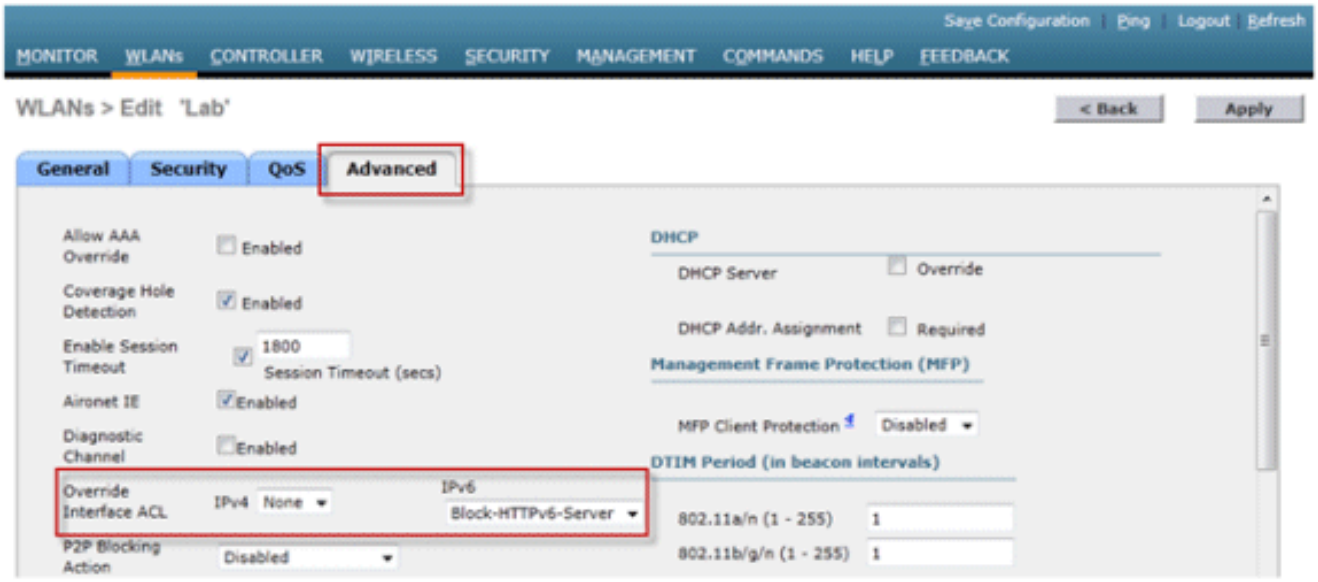


4. Cliquez sur **Add New Rule**, entrez les paramètres souhaités pour la règle, puis cliquez sur **Apply**. Laissez le numéro d'ordre vide afin de placer la règle à la fin de la liste. L'option « Direction » de « Inbound » est utilisée pour le trafic provenant du réseau sans fil et « Outbound » pour le trafic destiné aux clients sans fil. N'oubliez pas que la dernière règle d'une liste de contrôle d'accès est un refus global implicite. Utilisez une longueur de préfixe de 64 pour faire correspondre un sous-réseau IPv6 entier et une longueur de préfixe de 128 pour restreindre de manière unique l'accès à une adresse individuelle.



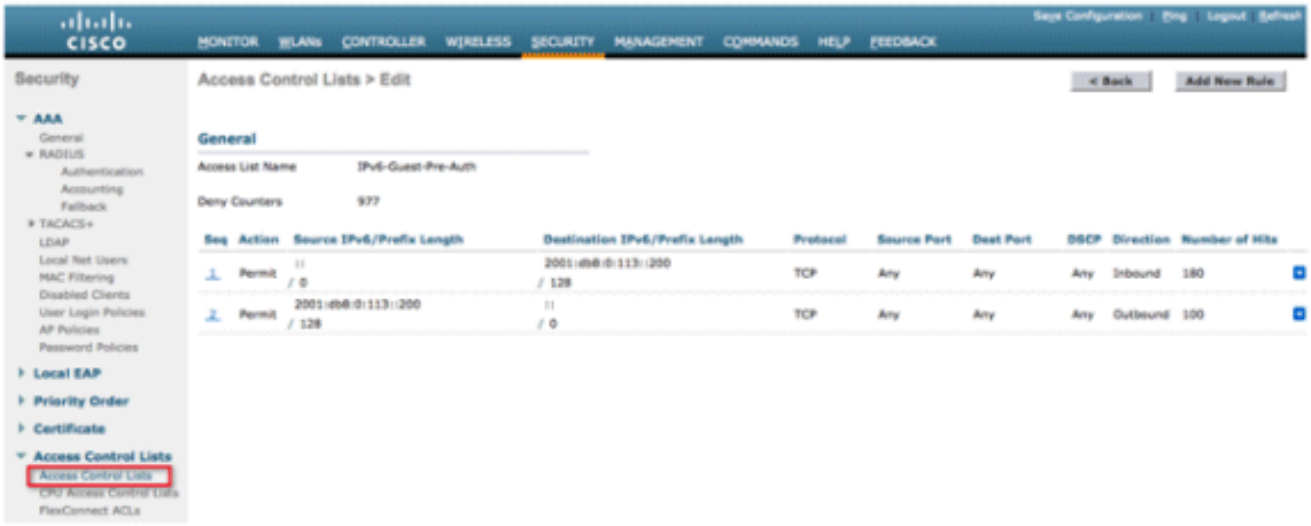
5. Les listes de contrôle d'accès IPv6 sont appliquées par WLAN/SSID et peuvent être utilisées simultanément sur plusieurs WLAN. Accédez à l'onglet **WLANs** et cliquez sur l'ID WLAN du

SSID en question afin d'appliquer la liste de contrôle d'accès IPv6. Cliquez sur l'onglet **Advanced** et remplacez l'ACL Override Interface pour IPv6 par le nom de l'ACL.



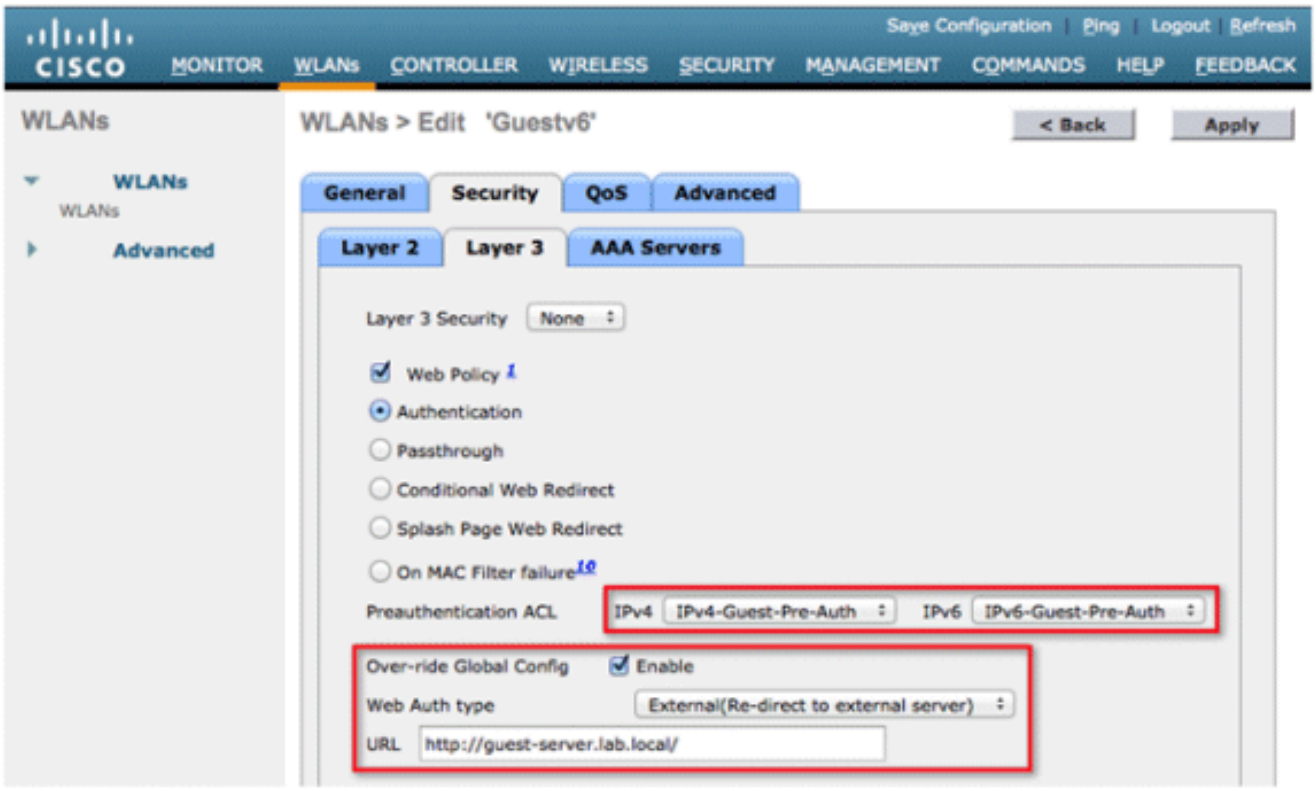
Configurer l'accès invité IPv6 pour l'authentification Web externe

1. Configurez la liste de contrôle d'accès de pré-authentification IPv4 et IPv6 pour le serveur Web. Ceci permet le trafic vers et depuis le serveur externe avant que le client ne soit entièrement
authentifié.



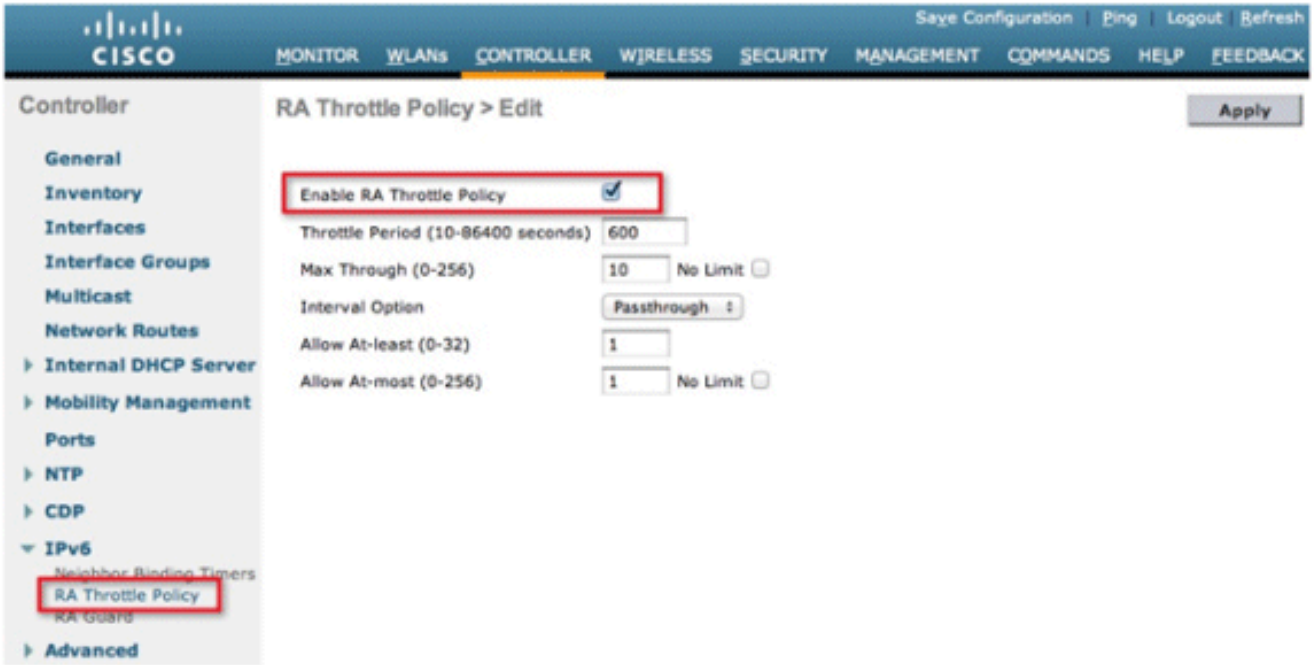
Pour plus d'informations sur le fonctionnement de l'accès Web externe, référez-vous à Exemple de configuration de l'authentification Web externe avec des contrôleurs LAN sans fil.

2. Configurez le WLAN invité en accédant à l'onglet WLAN situé en haut de la page. Créez le SSID invité et utilisez une stratégie Web de couche 3. Les listes de contrôle d'accès de pré-authentification définies à l'étape 1 sont sélectionnées pour IPv4 et IPv6. Cochez la section Override Global Config et sélectionnez **External** dans la liste déroulante Web Auth type. Saisissez l'URL du serveur Web. Le nom d'hôte du serveur externe doit pouvoir être résolu dans les DNS IPv4 et
IPv6.



Configurer la limitation IPv6 RA

1. Accédez au menu de niveau supérieur **Controller** et cliquez sur l'option **IPv6 > RA Throttle Policy** sur le côté gauche. Activez la limitation RA en cochant la case correspondante.



Remarque : en cas de limitation RA, seul le premier routeur IPv6 est autorisé à passer. Pour les réseaux avec plusieurs préfixes IPv6 desservis par différents routeurs, la limitation RA doit être désactivée.

2. Ajuster la période d'accélération et les autres options uniquement en accord avec le TAC. Cependant, la valeur par défaut est recommandée pour la plupart des déploiements. Les différentes options de configuration de la politique de limitation de RA doivent être ajustées en gardant à l'esprit ce qui suit :Les valeurs numériques de « Allow At-least » doivent être

inférieures à « Allow At-most », qui doit être inférieur à « Max Through ».La politique de limitation des RA ne doit pas utiliser une période de limitation supérieure à 1800 secondes, car il s'agit de la durée de vie par défaut de la plupart des RA.

Chaque option de limitation RA est décrite ci-dessous :

- Période d'étranglement - La période pendant laquelle l'étranglement a lieu. La limitation de la RA prend effet uniquement après que la limite « Max Through » a été atteinte pour le VLAN.
- Max Through : nombre maximal de RA par VLAN avant l'entrée en vigueur de la limitation. L'option « No Limit » autorise un nombre illimité de RA sans limitation.
- Option d'intervalle : l'option d'intervalle permet au contrôleur d'agir différemment en fonction de la valeur RFC 3775 définie dans l'annonce de routeur IPv6.Passthrough (Passthrough) : cette valeur permet à toutes les RA disposant d'une option d'intervalle RFC3775 de passer sans limitation.Ignorer - Cette valeur amènera le limiteur RA à traiter les paquets avec l'option d'intervalle comme un RA régulier et soumis à la limitation si elle est active.Limitation - Cette valeur fera en sorte que les RA avec l'option d'intervalle seront toujours soumis à une limitation de débit.
- Allow At-least : nombre minimal d'adresses de routeur par routeur qui seront envoyées en multidiffusion.
- Allow At-most (Autoriser au maximum) : nombre maximal de RA par routeur qui seront envoyées en multidiffusion avant que la limitation ne prenne effet. L'option « No Limit » autorise un nombre illimité d'adresses de routeur pour ce routeur.

Configuration de la table de liaison de voisinage IPv6

1. Accédez au menu de niveau supérieur du contrôleur et cliquez sur **IPv6 > Neighbor Binding Timers** sur le menu de
gauche.

2. Ajustez les durées de vie Down, Reachable Lifetime et Stale Lifetime selon vos besoins. Pour les déploiements avec des clients très mobiles, les minuteurs d'un minuteur d'adresse obsolète doivent être modifiés. Les valeurs recommandées sont :Durée de vie - 30 secondesDurée de vie accessible : 300 secondesDurée de vie de l'état - 86400 secondesChaque compteur de durée de vie fait référence à l'état dans lequel une adresse IPv6 peut se trouver :**Down Lifetime** : le compteur down spécifie la durée pendant laquelle les entrées du cache IPv6 doivent être conservées en cas de défaillance de l'interface de liaison ascendante du contrôleur.**Reachable Lifetime** - Ce compteur spécifie la durée pendant laquelle une adresse IPv6 sera marquée active, ce qui signifie que du trafic a été reçu de cette adresse récemment. Une fois ce délai expiré, l'adresse passe à l'état « Stale ».**Stale Lifetime** - Ce compteur spécifie la durée pendant laquelle les adresses IPv6 qui n'ont pas été vues dans la « Durée de vie accessible » doivent rester dans le cache. Après cette durée de vie, l'adresse est supprimée de la table de liaison.

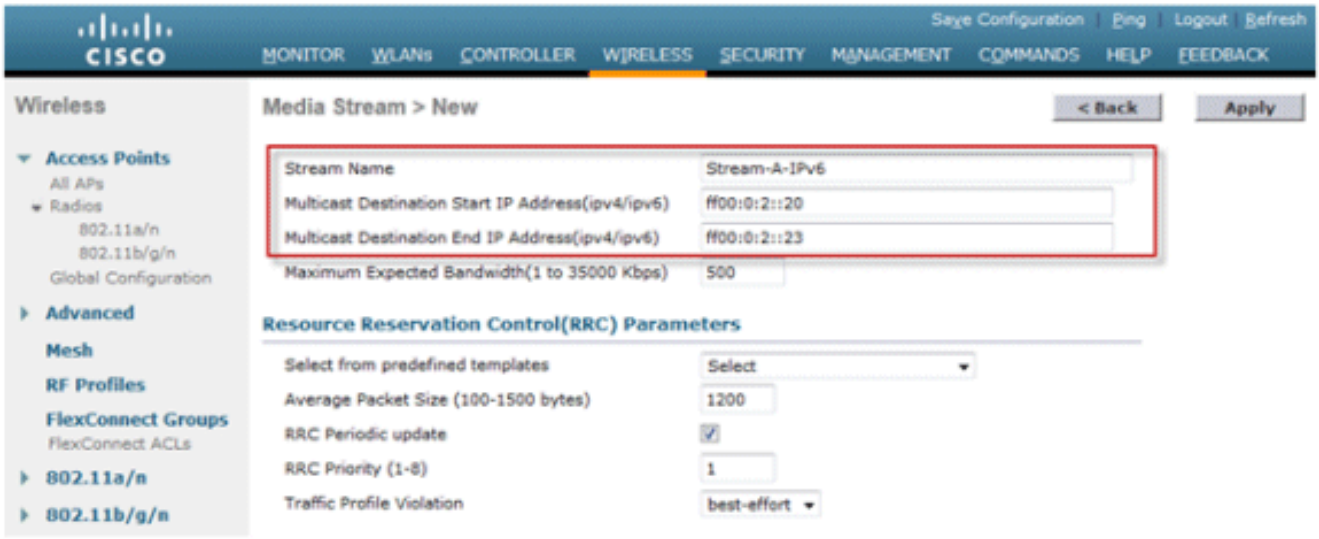
Configuration de VideoStream IPv6

1. Assurez-vous que les fonctionnalités Global VideoStream sont activées sur le contrôleur.

Référez-vous à Solution de réseau sans fil unifié Cisco : Guide de déploiement VideoStream pour des informations sur l'activation de VideoStream sur le réseau 802.11a/g/n ainsi que le SSID WLAN.

2. Accédez à l'onglet **Wireless** sur le contrôleur, et dans le menu de gauche, choisissez **Media Stream > Streams**. Cliquez sur **Add New** afin de créer un nouveau flux.

3. Nommez le flux et entrez les adresses IPv6 de début et de fin. Lorsque vous utilisez un seul flux, les adresses de début et de fin sont identiques. Après avoir ajouté les adresses, cliquez sur **Apply** afin de créer le flux.



Dépannage de la connectivité client IPv6

Certains clients ne peuvent pas transmettre le trafic IPv6

Certaines implémentations de pile réseau IPv6 cliente ne s'annoncent pas correctement lorsqu'elles arrivent sur le réseau et par conséquent leur adresse n'est pas surveillée de manière appropriée par le contrôleur pour être placée dans la table de liaison de voisinage. Toutes les adresses absentes de la table de liaison de voisinage sont bloquées conformément à la

fonctionnalité de protection de la source IPv6. Afin d'autoriser ces clients à transmettre le trafic, ces options doivent être configurées :

1. Désactivez la fonction de protection de la source IPv6 via l'interface de ligne de commande :

   config network ip-mac-binding disable

2. Activez le transfert de sollicitation de voisin multidiffusion via l'interface de ligne de commande :

   config ipv6 ns-mcast-fwd enable

Vérification de l'itinérance de couche 3 réussie pour un client IPv6 :

Émettez ces commandes **debug** sur le contrôleur d'ancrage et le contrôleur étranger :

debug client

debug mobility handoff enable

debug mobility packet enable

Résultats du débogage sur le contrôleur d'ancrage :

```
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Complete to
  Mobility-Incomplete
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Setting handles to 0x00000000
00:21:6a:a7:4f:ee pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE =
  0.
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Deleted mobile LWAPP rule on AP
  [04:fe:7f:49:03:30]
00:21:6a:a7:4f:ee Updated location for station old AP 04:fe:7f:49:03:30-1, new
  AP 00:00:00:00:00:00-0
00:21:6a:a7:4f:ee Stopping deletion of Mobile Station: (callerId: 42)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
  Mobility-Complete, mobility role=Anchor, client state=APF_MS_STATE_ASSOCIATED
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Adding Fast Path rule type = Airespace AP
  Client on AP 00:00:00:00:00:00, slot 0, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID = 255,
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP =
  0, TokenID = 7006  Local Bridging Vlan = 20, Local Bridging intf id = 13
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
  255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee 0.0.0.0 Removed NPU entry.
00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Anchor role
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
```

```
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee 0.0.0.0, VLAN Id 20 Not sending gratuitous ARP
00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:0, apMac 0x0:0:0:0:0:0
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:0 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
  w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x5
  statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:2, anchorip:0xac14e2c6
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
```

Résultats du débogage sur le contrôleur étranger :

```
00:21:6a:a7:4f:ee Adding mobile on LWAPP AP f0:25:72:3c:0f:20(1)
00:21:6a:a7:4f:ee Reassociation received from mobile on AP f0:25:72:3c:0f:20
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1697)
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1864)
00:21:6a:a7:4f:ee Applying site-specific Local Bridging override for station
  00:21:6a:a7:4f:ee - vapId 3, site 'default-group', interface 'client-b1'
00:21:6a:a7:4f:ee Applying Local Bridging Interface Policy for station
  00:21:6a:a7:4f:ee - vlan 25, interface id 12, interface 'client-b1'
00:21:6a:a7:4f:ee processSsidIE  statusCode is 0 and status is 0
00:21:6a:a7:4f:ee processSsidIE  ssid_done_flag is 0 finish_flag is 0
00:21:6a:a7:4f:ee STA - rates (8): 140 18 152 36 176 72 96 108 0 0 0 0 0 0 0 0
*apfMsConnTask_4: Jan 22 20:37:45.370: 00:21:6a:a7:4f:ee suppRates  statusCode
  is 0 and gotSuppRatesElement is 1
00:21:6a:a7:4f:ee Processing RSN IE type 48, length 22 for mobile
  00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Initializing policy
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state
  AUTHCHECK (2)
00:21:6a:a7:4f:ee 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last
  state 8021X_REQD (3)
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee apfMsAssoStateInc
00:21:6a:a7:4f:ee apfPemAddUser2 (apf_policy.c:268) Changing state for mobile
  00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Idle to Associated
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 49) in 1800
  seconds
00:21:6a:a7:4f:ee Sending Assoc Response to station on BSSID f0:25:72:3c:0f:20
  (status 0) ApVapId 3 Slot 1
00:21:6a:a7:4f:ee apfProcessAssocReq (apf_80211.c:6290) Changing state for
  mobile 00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Associated to Associated
<…SNIP…>
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last
  state L2AUTHCOMPLETE (4)
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last
```

```
  state DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 5253, Adding TMP rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IP
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Stopping retransmission timer for mobile 00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Sent an XID frame
00:21:6a:a7:4f:ee Username entry () already exists in name table, length = 253
00:21:6a:a7:4f:ee Username entry () created in mscb for mobile, length = 253
00:21:6a:a7:4f:ee Applying post-handoff policy for station 00:21:6a:a7:4f:ee -
  valid mask 0x1000
00:21:6a:a7:4f:ee QOS Level: -1, DSCP: -1, dot1p: -1, Data Avg: -1, realtime
  Avg: -1, Data Burst -1, Realtime Burst -1
00:21:6a:a7:4f:ee     Session: -1, User session: -1, User elapsed -1 Interface:
  N/A, IPv4 ACL: N/A, IPv6 ACL:
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to DHCP_REQD (7) last state
  DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemCreateMobilityState 6370, Adding TMP
  rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule type =
  Airespace AP - Learn IP address on AP f0:25:72:3c:0f:20, slot 1, interface =
  13, QOS = 0 IPv4 ACL ID = 255,
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 55) in 1800
  seconds
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee apfMsRunStateInc
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to RUN (20) last state RUN
  (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 5776
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
  Mobility-Complete, mobility role=Foreign, client state=APF_MS_STATE_ASSOCIATED
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Replacing Fast Path rule
  type = Airespace AP Client
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID = 25
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP =
  0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id = 12
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
  255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Foreign role
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
```

```
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:1, apMac 0xf0:25:72:3c:f:20
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:1 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
  w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x7
  statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:3, anchorip:0xac14e2c5
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
00:21:6a:a7:4f:ee Copy IPv6 LOCP: 2001:db8:0:20:3057:534d:587d:73ae
```

Commandes CLI IPv6 utiles :

Show ipv6 neighbor-binding summary

Debug ipv6 neighbor-binding filter client enable

Debug ipv6 neighbor-binding filter errors enable

Forum aux questions

Q : Quelle est la taille de préfixe IPv6 optimale pour limiter le domaine de diffusion ?

R : Bien qu'un sous-réseau IPv6 puisse être subdivisé en sous-réseaux /64, cette configuration interrompt la SLAAC et entraîne des problèmes de connectivité client. Si la segmentation est nécessaire afin de réduire le nombre d'hôtes, la fonctionnalité Groupes d'interfaces peut être utilisée pour équilibrer la charge des clients entre différents VLAN back-end, chacun utilisant un préfixe IPv6 différent.

Q : Existe-t-il des limites d'évolutivité en matière de prise en charge des clients IPv6 ?

R : La principale limite d'évolutivité pour la prise en charge des clients IPv6 est la table de liaison de voisinage qui conserve une trace de toutes les adresses IPv6 des clients sans fil. Cette table est mise à l'échelle par plate-forme de contrôleur afin de prendre en charge le nombre maximal de clients multiplié par huit (le nombre maximal d'adresses par client). L'ajout de la table de liaison IPv6 peut augmenter l'utilisation de la mémoire du contrôleur d'environ 10 à 15 % à pleine charge, selon la plate-forme.

Contrôleur sans fil	Nombre maximal de clients	Taille de la table de liaison de voisins IPv6
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

Q : Quel est l'impact des fonctionnalités IPv6 sur le processeur et la mémoire du contrôleur ?

R : L'impact est minime, car le processeur dispose de plusieurs coeurs pour traiter le plan de contrôle. Lors de tests avec un maximum de clients pris en charge, chacun avec 8 adresses IPv6, l'utilisation du processeur était inférieure à 30 % et l'utilisation de la mémoire inférieure à 75 %.

Q : La prise en charge du client IPv6 peut-elle être désactivée ?

R : Pour les clients qui souhaitent activer uniquement IPv4 sur leur réseau et bloquer IPv6, une liste de contrôle d'accès IPv6 de type « refuser tout » peut être utilisée et appliquée par WLAN.

Q : Est-il possible d'avoir un WLAN pour IPv4 et un autre pour IPv6 ?

R : Il n’est pas possible d’avoir le même nom SSID et le même type de sécurité pour deux WLAN différents fonctionnant sur le même AP. Pour la segmentation des clients IPv4 à partir des clients IPv6, deux WLAN doivent être créés. Chaque WLAN doit être configuré avec une liste de contrôle d'accès qui bloque respectivement tout le trafic IPv4 ou IPv6.

Q : Pourquoi est-il important de prendre en charge plusieurs adresses IPv6 par client ?

R : Les clients peuvent avoir plusieurs adresses IPv6 par interface qui peuvent être statiques, SLAAC ou DHCPv6 attribuées en plus d'avoir toujours une adresse link-local auto-attribuée. Les clients peuvent également avoir des adresses supplémentaires utilisant des préfixes IPv6 différents.

Q : Que sont les adresses privées IPv6 et pourquoi sont-elles importantes à suivre ?

R : Les adresses privées (également appelées temporaires) sont générées aléatoirement par le client lorsque l’affectation d’adresses SLAAC est utilisée. Ces adresses sont souvent tournées à une fréquence d'environ un jour, afin d'empêcher la traçabilité de l'hôte qui proviendrait de l'utilisation du même suffixe d'hôte (64 derniers bits) à tout moment. Il est important de suivre ces adresses privées à des fins d'audit, telles que le suivi des violations de droits d'auteur. Cisco NCS enregistre toutes les adresses IPv6 utilisées par chaque client et les consigne dans l'historique chaque fois que le client se déplace ou établit une nouvelle session. Ces enregistrements peuvent être configurés sur NCS pour être conservés pendant un an maximum.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

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.

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.