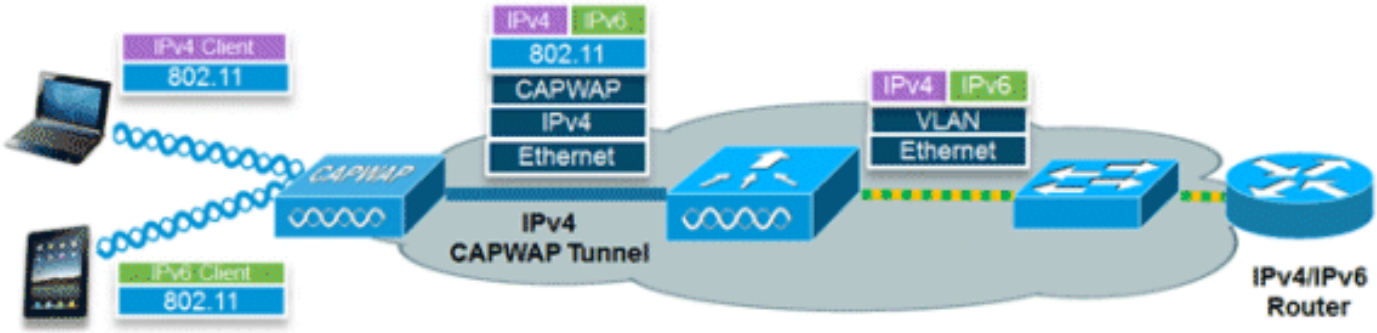
Implementatiehandleiding voor draadloze LAN IPv6-clients

Inhoud

Inleiding

Dit document biedt informatie over de theorie van de werking en configuratie voor de Cisco Unified Wireless LAN-oplossing aangezien deze betrekking heeft op het ondersteunen van IPv6-clients.

IPv6-clientconnectiviteit voor draadloos LAN



Met de IPv6-functieset binnen de Cisco Unified Wireless Network-softwarerelease v7.2 kan het draadloze netwerk IPv4-, dual-stack- en IPv6-clients ondersteunen op hetzelfde draadloze netwerk. Het algemene doel voor de toevoeging van IPv6-clientondersteuning aan Cisco Unified Wireless LAN was functiepariteit te behouden tussen IPv4- en IPv6-clients, inclusief mobiliteit, beveiliging, gasttoegang, kwaliteit van de service en zichtbaarheid van endpoints.

Per apparaat kunnen maximaal acht IPv6-clientadressen worden bijgehouden. Hierdoor kunnen IPv6-clients een link-lokaal, stateless Address Auto Configuration (SLAAC)-adres, Dynamic Host Configuration Protocol voor IPv6 (DHCPv6)-adres en zelfs adressen in alternatieve prefixes hebben om op één interface te staan. Clients voor werkgroepbridge (WGB) die zijn aangesloten op de uplink van een autonoom access point (AP) in de WGB-modus kunnen IPv6 ook ondersteunen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Draadloze LAN-controllers 2500 Series, 5500 Series of WiSM2
- APs 130, 1240, 1250, 1040, 1140, 1260, 3500, 3600 Series APs, en 1520 of 1550 Series mesh APs
- IPv6-enabled router

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

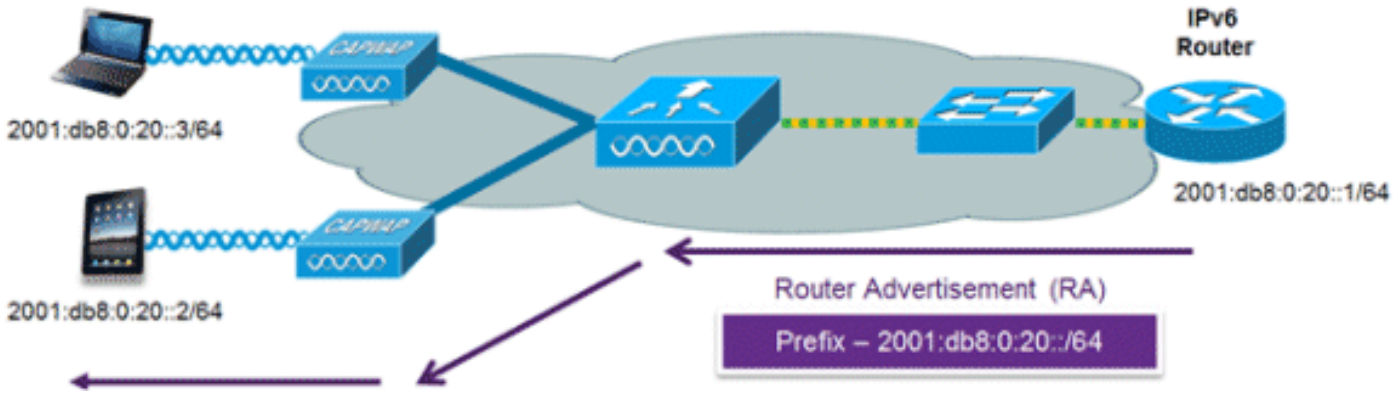
Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Voorwaarden voor draadloze IPv6-clientconnectiviteit

Om draadloze IPv6-clientconnectiviteit mogelijk te maken, moet het onderliggende bekabelde netwerk IPv6-routing en een mechanisme voor adrestoewijzing zoals SLAAC of DHCPv6 ondersteunen. De draadloze LAN-controller moet L2-nabijheid van de IPv6-router hebben en het VLAN moet worden gelabeld wanneer de pakketten de controller binnenkomen. AP's vereisen geen verbinding op een IPv6-netwerk, omdat al het verkeer is ingekapseld in de IPv4 CAPWAP-tunnel tussen het AP en de controller.

TOEWIJZING VAN SLAC-ADRES

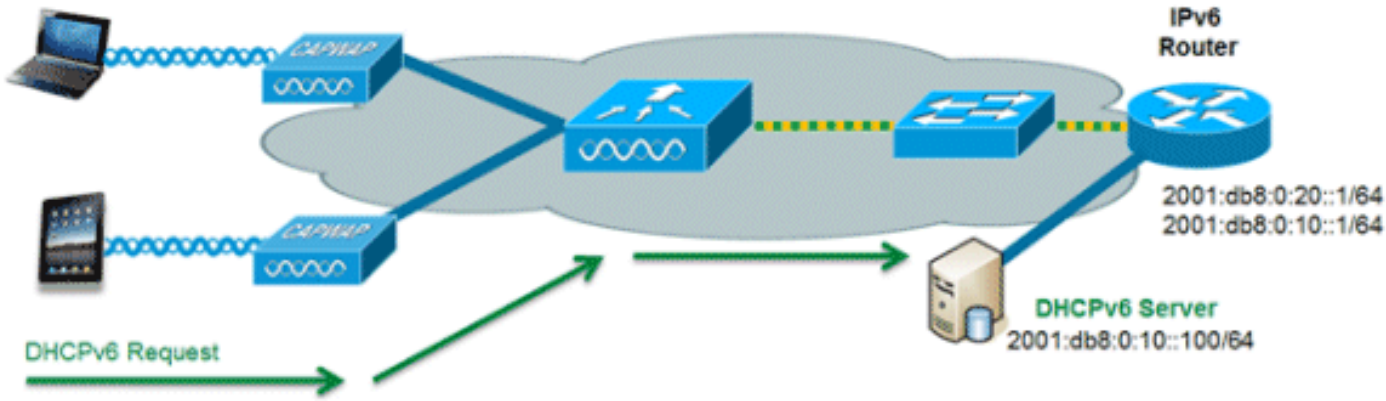


De meest gebruikelijke methode voor de toewijzing van IPv6-clientadressen is SLAAC. SLAAC biedt eenvoudige plug-and-play connectiviteit, waarbij klanten zelf een adres toewijzen op basis van de IPv6-prefix. Dit proces wordt bereikt wanneer de IPv6 router periodieke Router Advertisement-berichten uitstuurt die de client informeren over het in gebruik zijnde IPv6-prefix (de eerste 64 bits) en over de IPv6-standaardgateway. Vanaf dat punt kunnen clients de resterende 64 bits van hun IPv6-adres genereren op basis van twee algoritmen: EUI-64, dat gebaseerd is op het MAC-adres van de interface, of privé-adressen die willekeurig worden gegenereerd. De keuze van het algoritme is aan de client en is vaak configureerbaar. De dubbele adredetectie wordt uitgevoerd door IPv6-clients om ervoor te zorgen dat willekeurige adressen die worden gekozen niet botsen met andere clients. Het adres van de router die advertenties verzenden wordt gebruikt als de standaardgateway voor de client.

Deze Cisco IOS®-configuratieopdrachten van een Cisco-compatibele IPv6-router worden gebruikt om SLAAC-adressering en routeradvertenties in te schakelen:

```
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
```

DHCPv6-adrestoewijzing



Het gebruik van DHCPv6 is niet vereist voor IPv6-clientconnectiviteit als de SLAAC al is geïmplementeerd. Er zijn twee werkingsmodi voor DHCPv6, **Stateless** en **Stateful** genoemd.

De **stateless** modus DHCPv6 wordt gebruikt om clients aanvullende netwerkinformatie te geven die niet beschikbaar is in de routeradvertentie, maar niet in een IPv6-adres, aangezien dit al door SLAAC wordt geleverd. Deze informatie kan de DNS-domeinnaam, DNS-server(s) en andere DHCP-leverancierspecifieke opties bevatten. Deze interfaceconfiguratie is voor een Cisco IOS IPv6-router die stateless DHCPv6 implementeert met SLAAC:

```
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
```

De DHCPv6 **Stateful** optie, ook bekend als beheerde modus, werkt op dezelfde manier als DHCPv4 in die zin dat het unieke adressen aan elke client toewijst in plaats van de client die de laatste 64 bits van het adres genereert zoals in SLAAC. Deze interfaceconfiguratie is voor een Cisco IOS IPv6-router die stateful DHCPv6 implementeert met SLA uitgeschakeld:

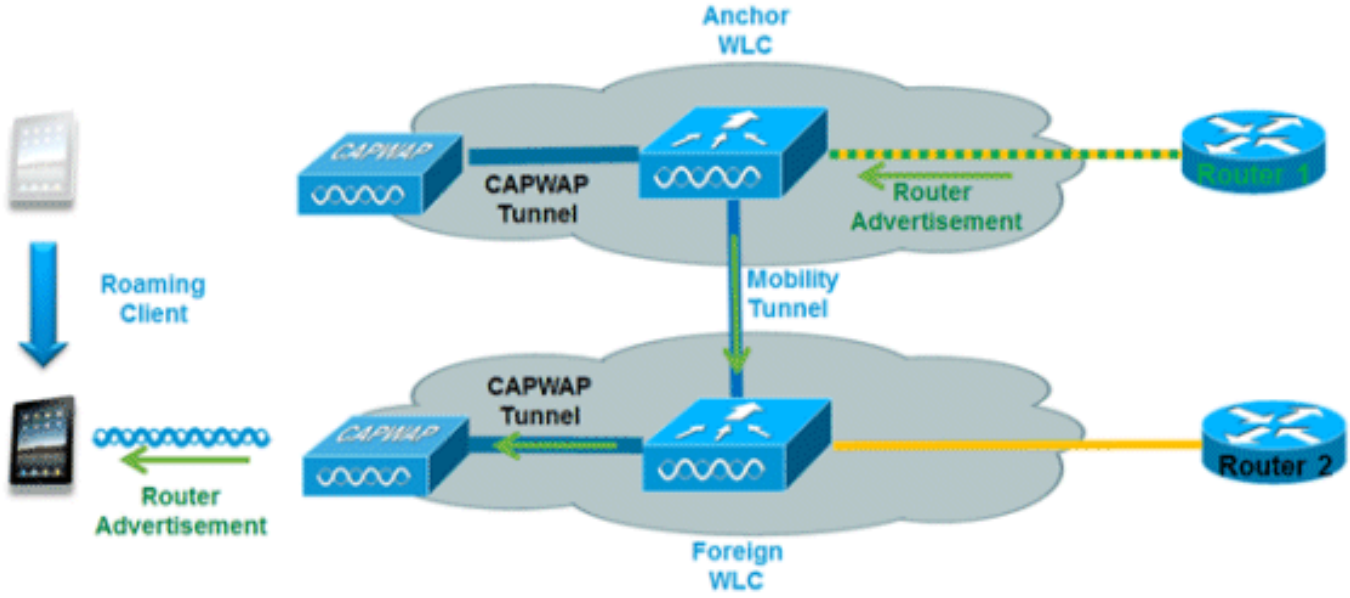
```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateful
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
```

```
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

Aanvullende informatie

Het configureren van het bekabelde netwerk voor volledige IPv6-connectiviteit op de campus met dubbele stack- of tunnelconnectiviteitsmethoden valt buiten het bereik van dit document. Raadpleeg voor meer informatie de Cisco-gevalideerde implementatiegids voor IPv6-implementatie in Campus-netwerken.

IPv6-clientmobiliteit



Om zwervende IPv6-clients over controllers te kunnen verwerken, moeten de ICMPv6-berichten zoals Neighbor Sollicitation (NS), Neighbor Advertisement (NA), Router Advertisement (RA) en Router Solicitation (RS) speciaal worden verwerkt om ervoor te zorgen dat een client op hetzelfde Layer 3-netwerk blijft. De configuratie voor IPv6-mobiliteit is hetzelfde als voor IPv4-mobiliteit en vereist geen afzonderlijke software aan de clientzijde om naadloos zwerven te realiseren. De enige vereiste configuratie is dat de controllers deel moeten uitmaken van dezelfde mobiliteitsgroep/-domein.

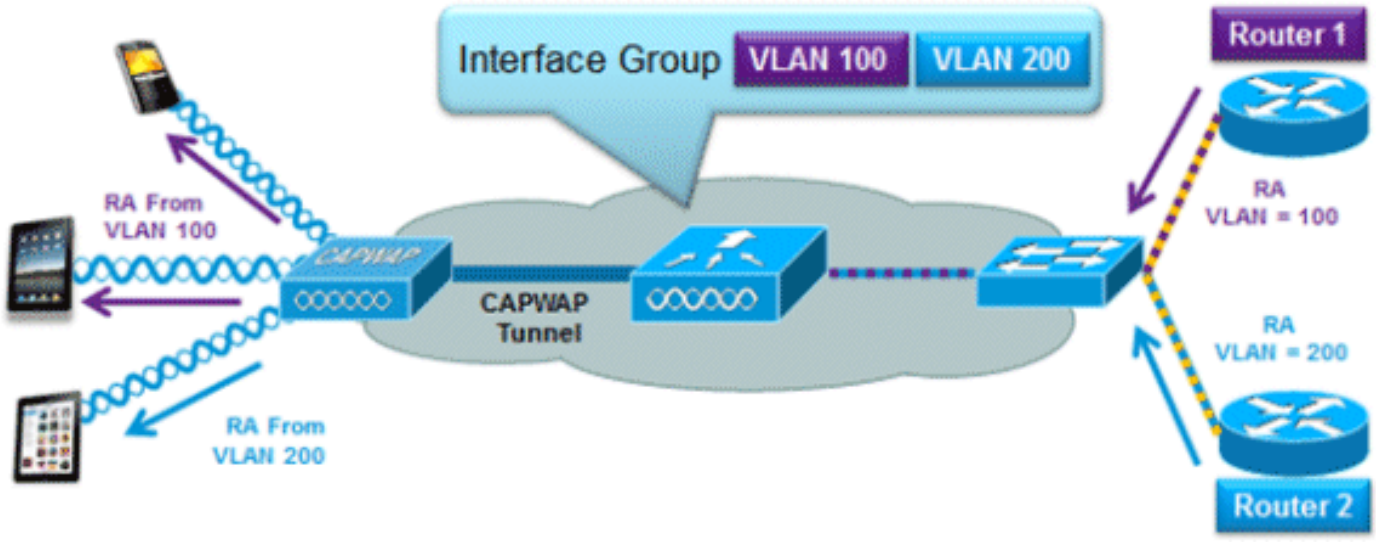
Hier is het proces voor IPv6-clientmobiliteit over controllers:

1. Als beide controllers toegang hebben tot hetzelfde VLAN als de client oorspronkelijk was ingeschakeld, is het zwerven gewoon een Layer 2-roaminggebeurtenis waarbij het clientrecord wordt gekopieerd naar de nieuwe controller en er geen verkeer wordt getunneld naar de ankercontroller.
2. Als de tweede controller geen toegang heeft tot het oorspronkelijke VLAN waarop de client was, zal een Layer 3-roaminggebeurtenis optreden, wat betekent dat al het verkeer van de client via de mobiliteitstunnel (Ethernet over IP) naar de ankercontroller moet worden getunneld.Om ervoor te zorgen dat de client zijn oorspronkelijke IPv6-adres behoudt, worden de RA's van het oorspronkelijke VLAN door de ankercontroller naar de buitenlandse controller gestuurd, waar ze aan de client worden geleverd met L2-unicast van het

toegangspunt.Wanneer de zwervende client zijn adres via DHCPv6 gaat vernieuwen of via SLAAC een nieuw adres gaat genereren, worden de RS-, NA- en NS-pakketten nog steeds getunneld naar het oorspronkelijke VLAN, zodat de client een IPv6-adres ontvangt dat van toepassing is op dat VLAN.

Opmerking: Mobility for IPv6-only clients is gebaseerd op VLAN-informatie. Dit betekent dat IPv6-only clientmobiliteit niet wordt ondersteund op niet-gelabelde VLAN's.

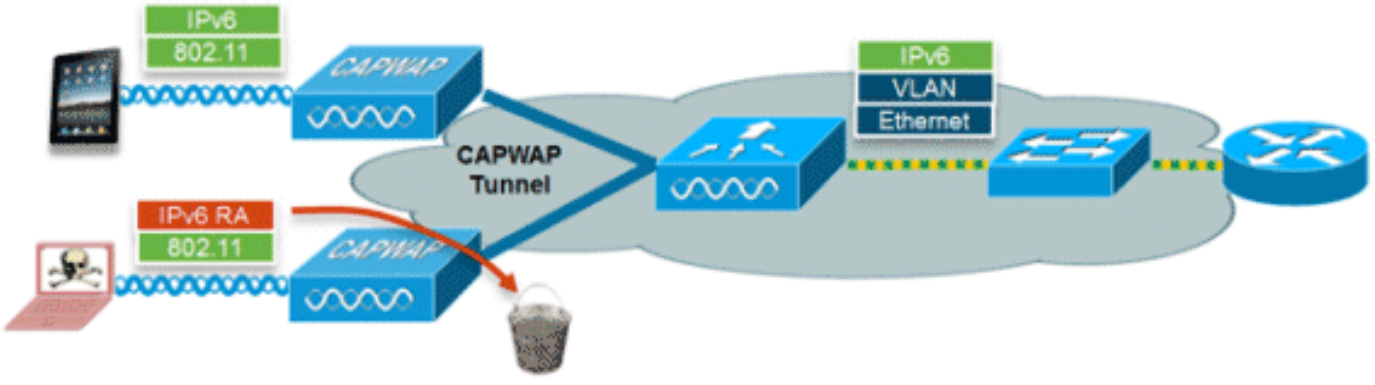
Ondersteuning voor VLAN-selectie (interfacegroepen)



De functie interfacegroepen maakt het voor een organisatie mogelijk om één WLAN met meerdere VLAN's op de controller te hebben geconfigureerd om taakverdeling voor draadloze clients in deze VLAN's mogelijk te maken. Deze eigenschap wordt algemeen gebruikt om IPv4 subnetgrootte klein te houden terwijl het toelaten van WLAN aan schaal aan duizenden gebruikers over veelvoud VLANs in de groep. Om IPv6-clients met interfacegroepen te ondersteunen, is geen extra configuratie nodig, aangezien het systeem automatisch de juiste RA naar de juiste clients stuurt via L2 draadloze unicast. Door de RA uit te schakelen, ontvangen clients op hetzelfde WLAN, maar een ander VLAN, de onjuiste RA niet.

Eerste hopbeveiliging voor IPv6-clients

Router Advertisement Guard



De RA Guard-functie verhoogt de beveiliging van het IPv6-netwerk door RA's die van draadloze clients komen, te laten vallen. Zonder deze functie kunnen slecht geconfigureerd of kwaadaardige IPv6-clients zichzelf aankondigen als een router voor het netwerk, vaak met een hoge prioriteit die

voorrang zou kunnen krijgen over legitieme IPv6-routers.

In de standaardinstelling is RA Guard ingeschakeld op het toegangspunt (maar kan worden uitgeschakeld op het toegangspunt) en is het altijd ingeschakeld op de controller. Het laten vallen van RAs bij AP wordt verkozen aangezien het een schaalbaardere oplossing is en verbeterde Ra-daltellers per cliënt verstrekt. In alle gevallen zal de IPv6 RA op enig moment worden verwijderd, waardoor andere draadloze clients en upstream bekabeld netwerk worden beschermd tegen kwaadaardige of verkeerd geconfigureerde IPv6-clients.

DHCPv6-serverbewaking

De functie DHCPv6 Server Guard voorkomt dat draadloze clients IPv6-adressen upstream kunnen doorgeven aan andere draadloze clients of bekabelde clients. Om te voorkomen dat DHCPv6-adressen worden uitgedeeld, worden alle DHCPv6-advertentiepakketten van draadloze clients verwijderd. Deze functie werkt op de controller, vereist geen configuratie en wordt automatisch ingeschakeld.

IPv6-bronbeveiliging

De functie IPv6 Source Guard voorkomt dat een draadloze client een IPv6-adres van een andere client spooft. Deze functie is analoog aan IPv4 Source Guard. IPv6 Source Guard is standaard ingeschakeld, maar kan via de CLI worden uitgeschakeld.

IPv6-adresaccounting

Voor RADIUS-verificatie en -accounting stuurt de controller één IP-adres terug met behulp van het kenmerk "Framed-IP-adres". In dit geval wordt het IPv4-adres gebruikt.

Het attribuut "Calling-Station-ID" gebruikt dit algoritme om een IP-adres te verzenden wanneer het "Call Station ID Type" op de controller is ingesteld op "IP Address":

1. IPv4-adres
2. Wereldwijde Unicast IPv6-adres
3. Lokaal IPv6-adres koppelen

Aangezien IPv6-adressen van clients vaak kunnen veranderen (tijdelijke of privé-adressen), is het belangrijk om ze in de loop der tijd te volgen. Cisco NCS registreert alle IPv6-adressen die door elke client worden gebruikt en registreert deze historisch telkens wanneer de client zwerft of een nieuwe sessie start. Deze records kunnen worden geconfigureerd bij NCS voor een periode tot een jaar.

Opmerking: de standaardwaarde voor het "Call Station ID Type" op de controller is veranderd in "System MAC Address" in versie 7.2. Bij het upgraden moet dit worden gewijzigd om unieke opvolging van clients door MAC-adres mogelijk te maken, aangezien IPv6-adressen kunnen veranderen tijdens de sessie en problemen kunnen veroorzaken bij de accounting als de Calling-Station-ID is ingesteld op IP-adres.

IPv6-toegangscontrolelijsten

Om de toegang tot bepaalde upstream bekabelde bronnen te beperken of bepaalde toepassingen te blokkeren, kunnen IPv6-toegangscontrolelijsten (ACL's) worden gebruikt om verkeer te

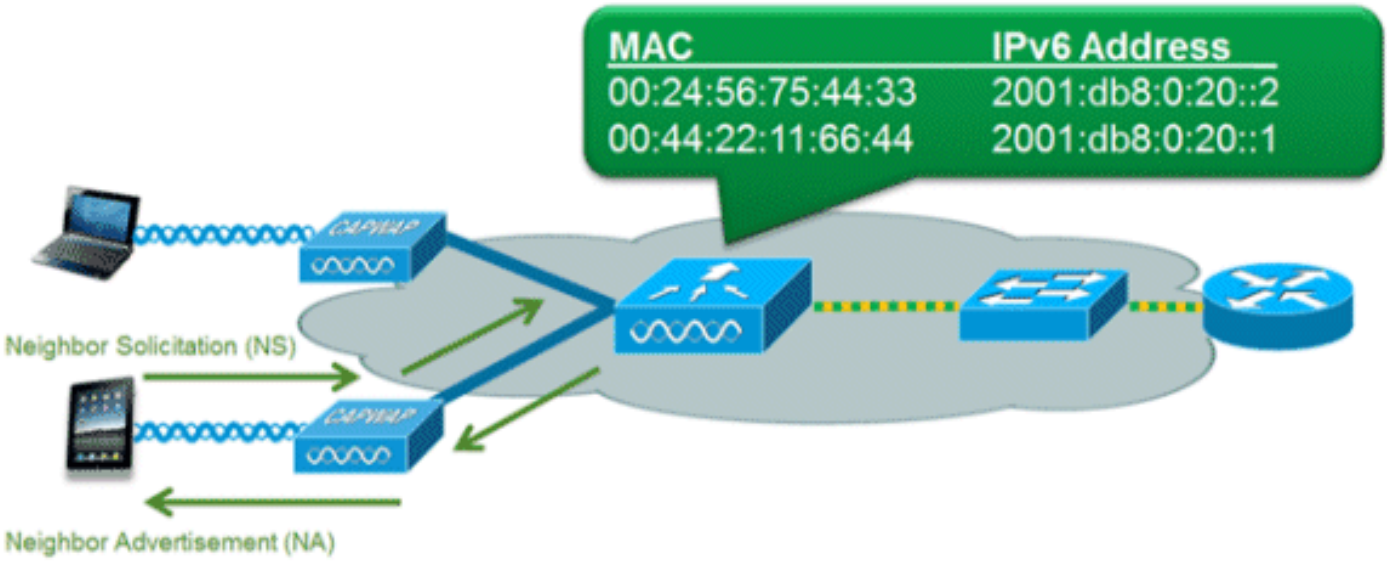
identificeren en verkeer toe te staan of te weigeren. IPv6-ACL's ondersteunen dezelfde opties als IPv4 ACL's, waaronder bron, bestemming, bronpoort en bestemmingshaven (poortbereiken worden ook ondersteund). ACL's voor verificatie vooraf worden ook ondersteund om IPv6-gastverificatie te ondersteunen met een externe webserver. De draadloze controller ondersteunt tot 64 unieke IPv6 ACL's met 64 unieke regels in elk. De draadloze controller blijft 64 unieke IPv4 ACL's ondersteunen met 64 unieke regels in elk van de 64 voor een totaal van 128 ACL's voor een dual-stack client.

AAA-opheffing voor IPv6 ACL's

Om gecentraliseerde toegangscontrole via een gecentraliseerde AAA-server zoals Cisco Identity Services Engine (ISE) of ACS te ondersteunen, kan IPv6-ACL per client worden geleverd met behulp van AAA-kenmerken voor negeren. Om deze functie te kunnen gebruiken, moet IPv6 ACL op de controller worden geconfigureerd en moet WLAN worden geconfigureerd met ingeschakelde AAA-functie voor negeren. Het eigenlijke genoemde AAA-kenmerk voor een IPv6-ACL is ***Airespace-IPv6-ACL-Naam*** vergelijkbaar met het *Airespace-ACL-Name*-attribuut dat wordt gebruikt voor de provisioning van een op IPv4 gebaseerde ACL. Het AAA kenmerk dat wordt teruggegeven moet een string zijn die gelijk is aan de naam van de IPv6 ACL zoals deze is ingesteld op de controller.

Packet optimalisatie voor IPv6-clients

Caching van buurdetectie



Het IPv6-buurdetectieprotocol (NDP) maakt gebruik van NAC- en NS-pakketten in plaats van Address Resolution Protocol (ARP) om IPv6-clients in staat te stellen het MAC-adres van andere clients in het netwerk op te lossen. Het NDP-proces kan erg chatten omdat het in eerste instantie multicast-adressen gebruikt om adresresolutie uit te voeren; dit kan waardevolle draadloze zendtijd in beslag nemen als de multicast-pakketten naar alle clients op het netwerksegment worden verzonden.

Om de efficiëntie van het NDP-proces te verhogen, kan de controller als een proxy fungeren en reageren op NS-vragen die het kan oplossen. Het ontdekken van de buur caching wordt mogelijk gemaakt door de onderliggende buur bindende lijst huidig in het controlemechanisme. De buurbindingstabel houdt elk IPv6-adres en het bijbehorende MAC-adres bij. Wanneer een IPv6-

client probeert het adres van de koppelingslaag van een andere client op te lossen, wordt het NS-pakket onderschept door de controller die terugreageert met een NA-pakket.

Throttling van routeradvertenties

Met Router Advertisement Throttling kan de controller snelheidsbeperking van RA's naar het draadloze netwerk afdwingen. Door RA throttling in te schakelen, kunnen routers die zo zijn geconfigureerd dat ze zeer vaak RA's verzenden (bijvoorbeeld elke drie seconden) worden teruggetrimd naar een minimumfrequentie waarmee de IPv6-clientconnectiviteit nog steeds behouden blijft. Hierdoor kan de zendtijd worden geoptimaliseerd door het aantal multicastpakketten dat moet worden verzonden te verminderen. In alle gevallen, als een klant een RS verstuurt, wordt een RA toegestaan via de controller en unicast naar de verzoekende klant. Dit om ervoor te zorgen dat nieuwe cliënten of roamende cliënten niet negatief worden beïnvloed door verstikkende werking van het RSA.

IPv6-gasttoegang

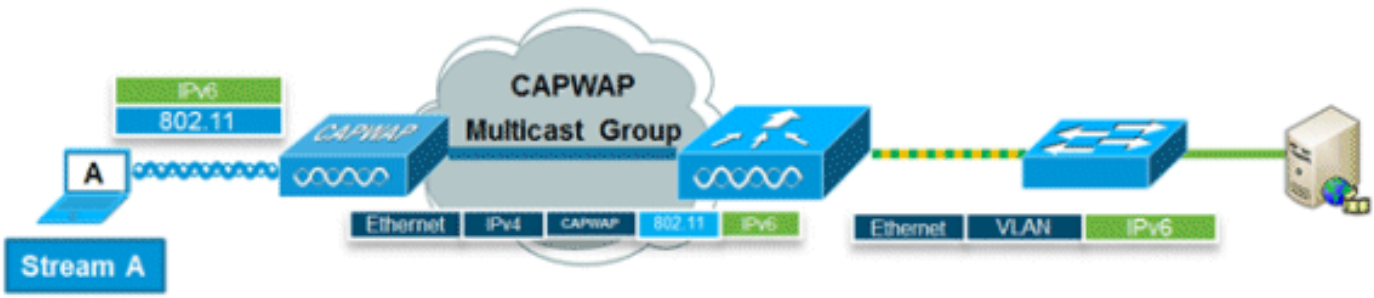
De draadloze en bekabelde gastfuncties voor IPv4-clients werken op dezelfde manier voor clients met dubbele stack en IPv6-clients. Zodra de gastgebruiker associeert, worden ze geplaatst in een "WEB_AUTH_REQ" run state totdat de client is geverifieerd via het IPv4 of IPv6 captive portal. De controller onderschept zowel IPv4- als IPv6 HTTP/HTTPS-verkeer in deze staat en stuurt het door naar het virtuele IP-adres van de controller. Zodra de gebruiker is geverifieerd via het interactieve portal, wordt hun MAC-adres verplaatst naar de uitvoerstatus en kan zowel IPv4- als IPv6-verkeer worden doorgegeven. Voor externe webverificatie kan met pre-authenticatie ACL een externe webserver worden gebruikt.

Om de omleiding van IPv6-clients te ondersteunen, maakt de controller automatisch een IPv6 virtueel adres op basis van het IPv4 virtueel adres dat op de controller is geconfigureerd. Het virtuele IPv6-adres voldoet aan de afspraak van `[::ffff:<virtueel IPv4-adres>]`. Een virtueel IP-adres van 1.1.1.1 wordt bijvoorbeeld vertaald naar `[::ffff:1.1.1.1]`.

Wanneer u een vertrouwd SSL-certificaat gebruikt voor gasttoegangsverificatie, zorg er dan voor dat zowel het IPv4- als IPv6-virtuele adres van de controller in DNS is gedefinieerd, zodat dit overeenkomt met de hostnaam van de SSL-certificaten. Dit zorgt ervoor dat de cliënten geen veiligheidswaarschuwing ontvangen die verklaart dat het certificaat niet de hostname van het apparaat aanpast.

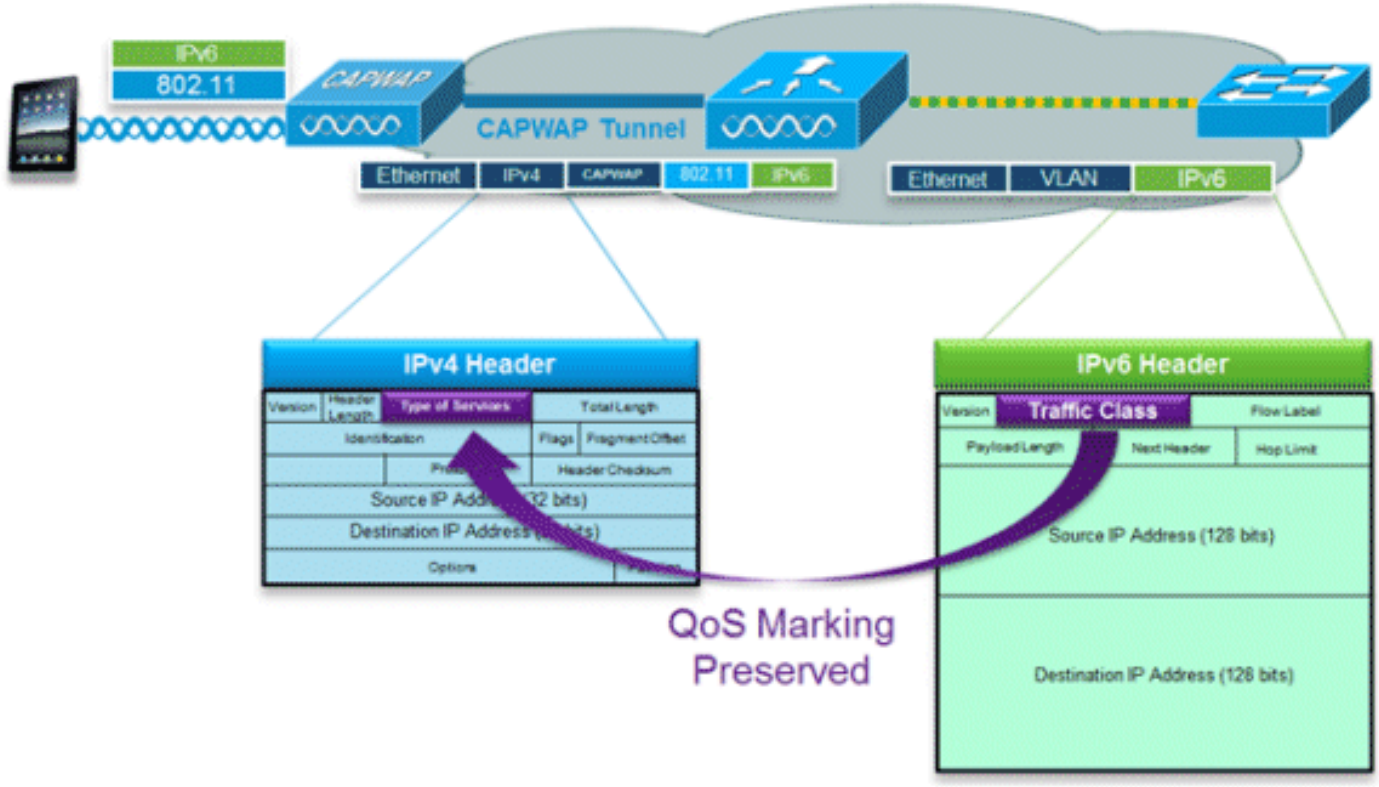
Opmerking: het automatisch gegenereerde SSL-certificaat van de controller bevat niet het IPv6 virtuele adres. Hierdoor kunnen sommige webbrowsers een veiligheidswaarschuwing laten zien. Het gebruik van een vertrouwd SSL-certificaat voor gasttoegang wordt aanbevolen.

IPv6-videostream



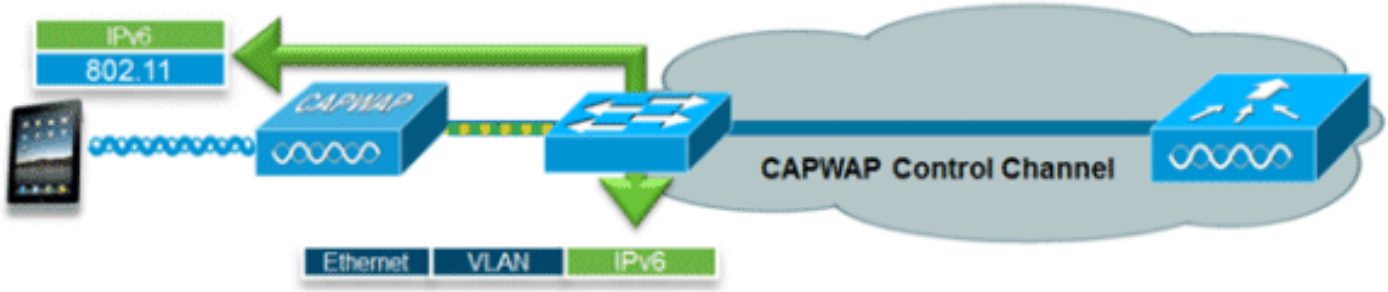
VideoStream maakt betrouwbare en schaalbare draadloze multicast-videolevering mogelijk, waarbij elke client de stream in een unicast-indeling ontvangt. De eigenlijke multicast naar unicast conversie (van L2) vindt plaats op het toegangspunt en biedt een schaalbare oplossing. De controller verzendt het IPv6-videoverkeer in een IPv4 CAPWAP-multicast tunnel die een efficiënte netwerkdistributie naar het toegangspunt mogelijk maakt.

IPv6 Quality-of-Service



IPv6-pakketten gebruiken een markering die vergelijkbaar is met het gebruik van DSCP-waarden door IPv4 en die tot 64 verschillende verkeersklassen (0-63) ondersteunt. Voor stroomafwaartse pakketten van het bekabelde netwerk wordt de waarde van IPv6 Traffic Class gekopieerd naar de header van de CAPWAP-tunnel om ervoor te zorgen dat QoS end-to-end behouden blijft. In de stroomopwaartse richting gebeurt hetzelfde als het clientverkeer dat op Layer 3 met IPv6-verkeersklasse is gemarkeerd, door de CAPWAP-pakketten te markeren die voor de controller zijn bestemd.

IPv6 en FlexConnect



FlexConnect - lokale switching WLAN's

FlexConnect in lokale switchingmodus ondersteunt IPv6-clients door het verkeer naar het lokale VLAN te overbruggen, wat vergelijkbaar is met IPv4-werking. Clientmobiliteit wordt ondersteund voor Layer 2-roaming binnen de FlexConnect-groep.

Deze IPv6-specifieke functies worden ondersteund in FlexConnect-lokale switchingmodus:

- IPv6 RNA-bewaking
- IPv6-overbrugging
- IPv6-gastverificatie (controller-gehost)

Deze IPv6-specifieke functies worden niet ondersteund in FlexConnect-lokale switchingmodus:

- Layer 3 Mobility
- IPv6-videostream
- IPv6-toegangscontrolelijsten
- IPv6-bronbeveiliging
- DHCPv6-serverbewaking
- Caching van buurdetectie
- Throttling van routeradvertenties

FlexConnect - Central-switching WLAN's

Voor AP's in FlexConnect-modus die gebruik maken van centrale switching (tunneling traffic terug naar de controller), moet de controller worden ingesteld op "Multicast - Unicast Mode" voor de "AP Multicast Mode". Aangezien FlexConnect AP's niet tot de CAPWAP multicast-groep van de controller behoren, moeten multicast pakketten op de controller worden gerepliceerd en unicast op elke AP afzonderlijk. Deze methode is minder efficiënt dan "Multicast - Multicast Mode" en plaatst extra belasting op de controller.

Deze IPv6-specifieke functie wordt niet ondersteund in FlexConnect-centrale switchingmodus:

- IPv6-videostream

Opmerking: Centraal switched WLAN's met IPv6 worden niet ondersteund op de Flex 7500 Series controller.

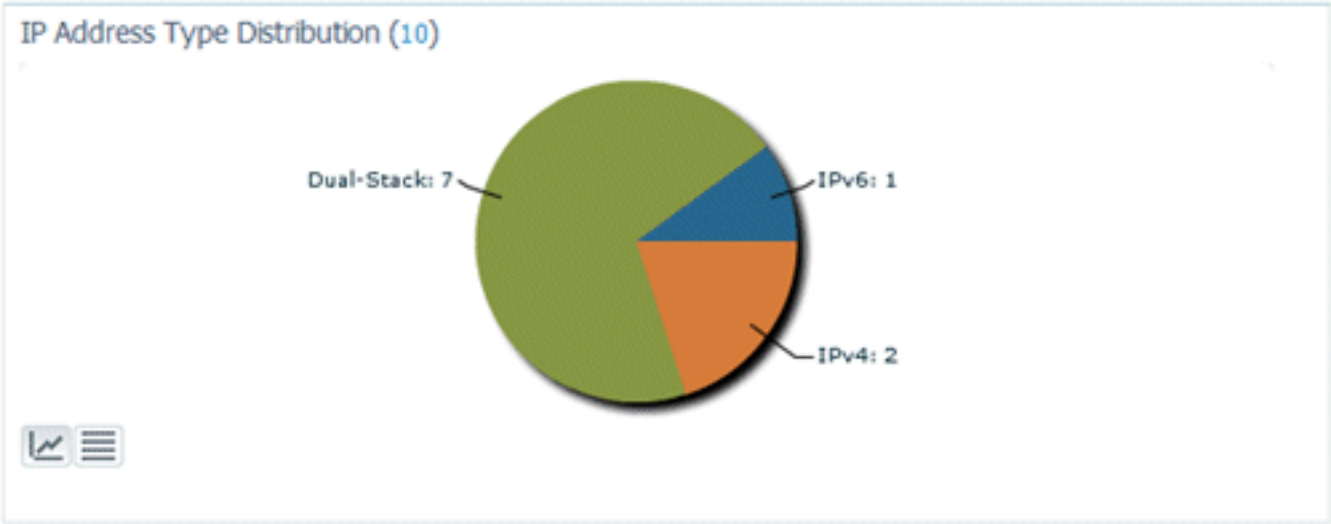
IPv6-clientzichtbaarheid met NCS

Met de release van NCS v1.1 worden veel extra specifieke IPv6-functies toegevoegd om een netwerk van IPv6-clients op zowel bekabelde als draadloze netwerken te bewaken en te beheren.

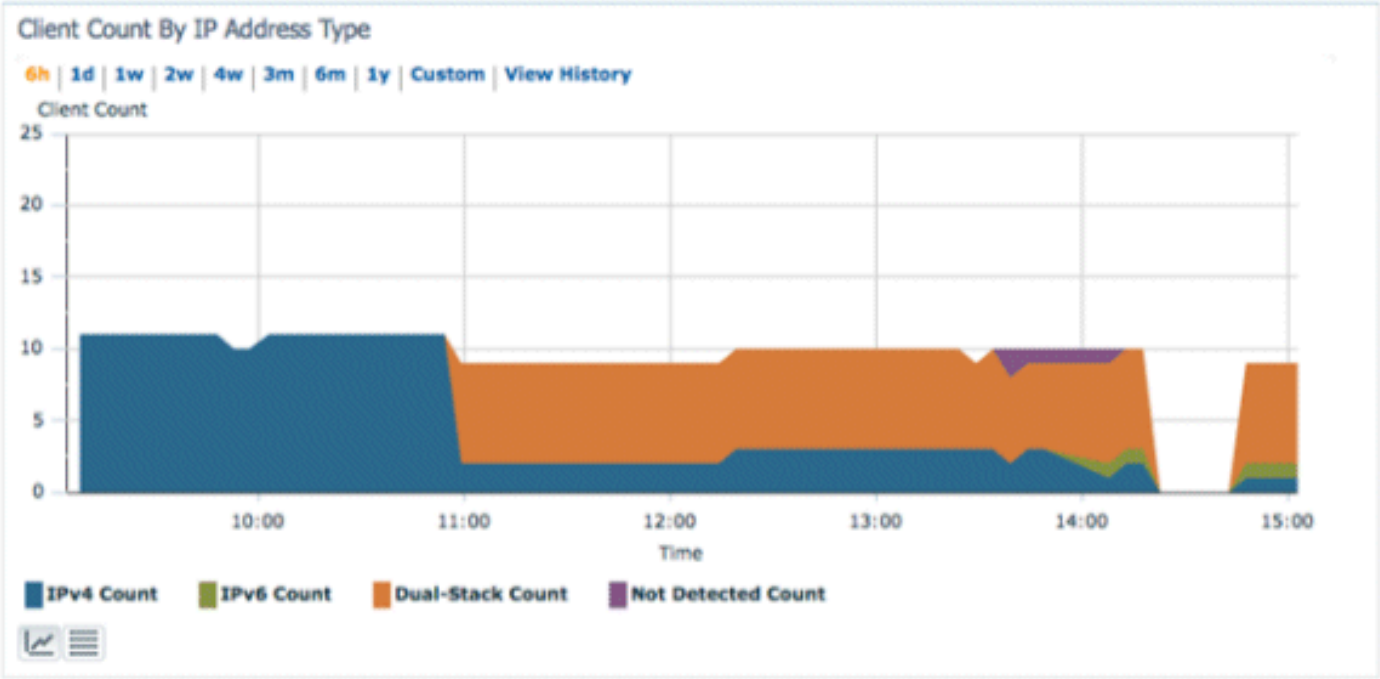
IPv6-dashboard items

Om te zien welke soorten clients op het netwerk aanwezig zijn, is een "Dashlet" in NCS beschikbaar om inzicht te geven in IPv6-specifieke statistieken en biedt de mogelijkheid om af te boren naar IPv6-clients.

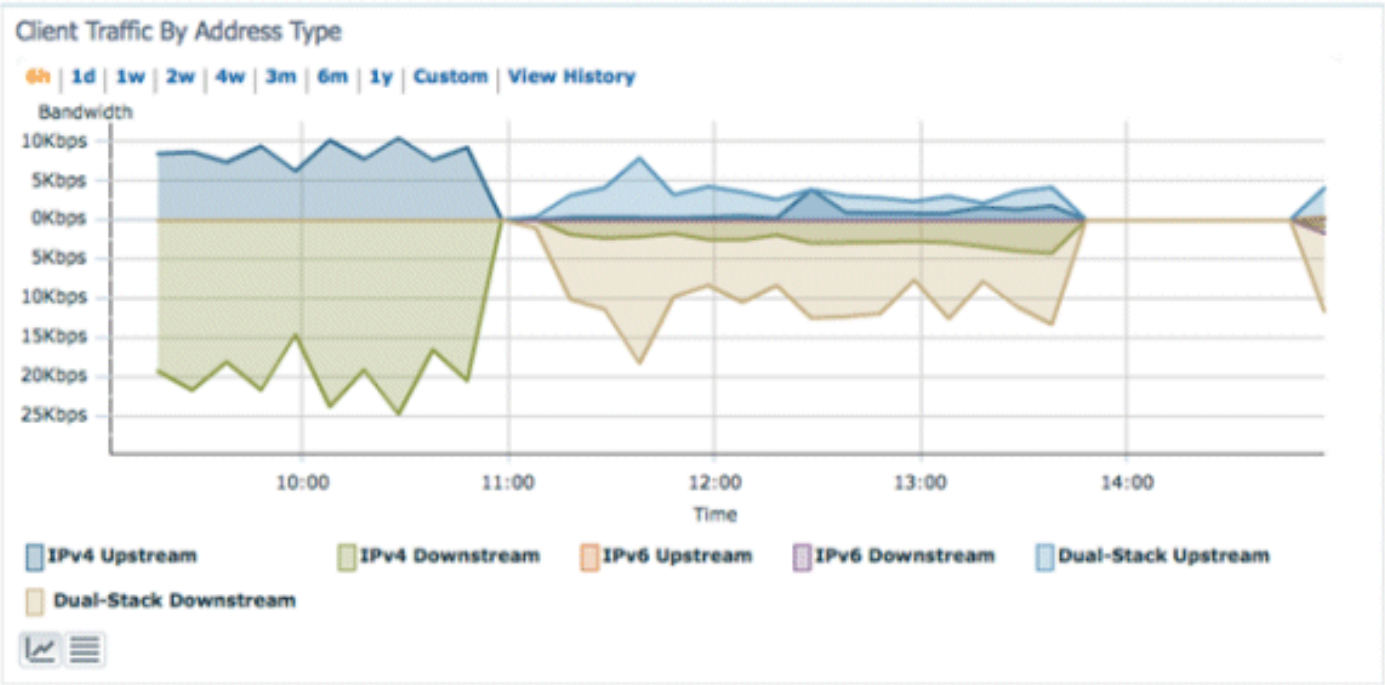
IP Address Type Dashlet - Hier worden de typen IP-clients in het netwerk weergegeven:



Clientaantal op IP-adrestype - hiermee wordt het IP-clienttype in de loop der tijd weergegeven:



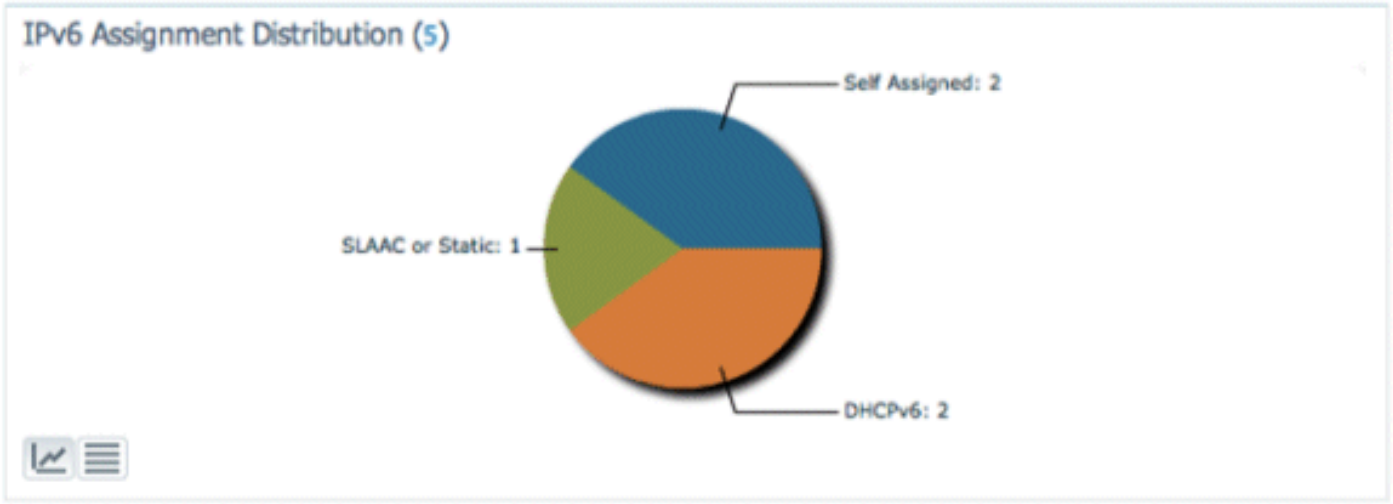
Clientverkeer per IP-adrestype - Hier wordt het verkeer weergegeven van elk type client. Clients in de categorie dual-stack omvatten zowel IPv4- als IPv6-verkeer:



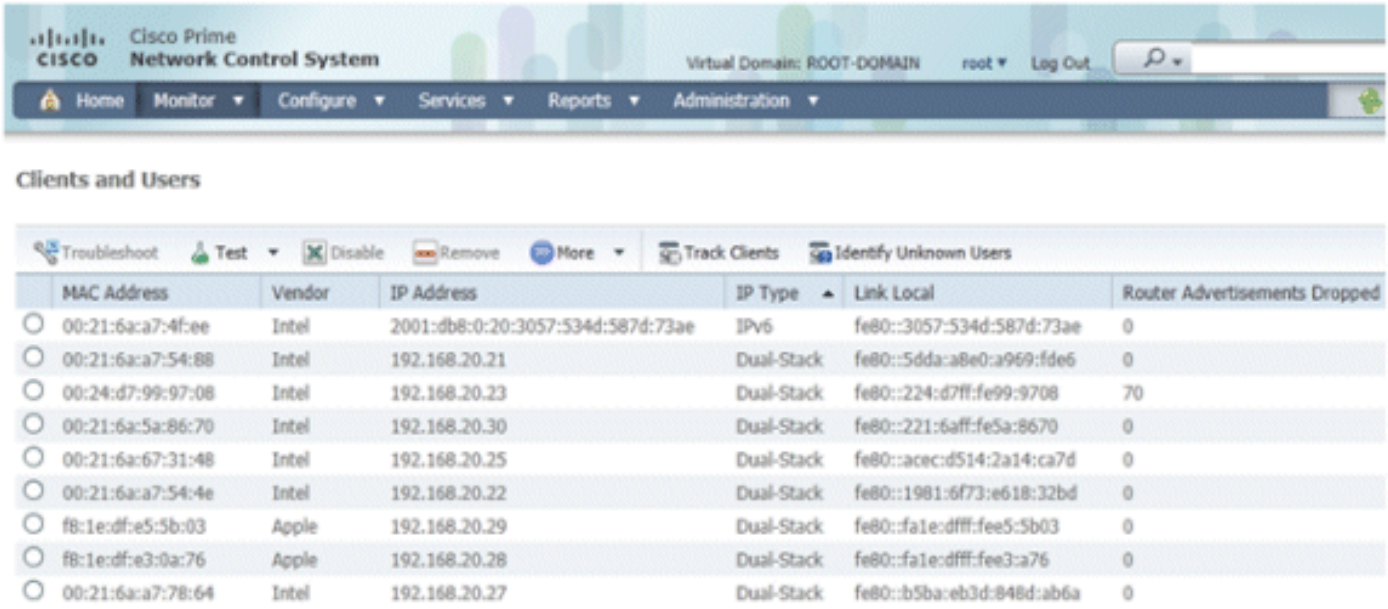
IPv6-adrestoewijzing - Hier wordt de adrestoewijzingsmethode voor elke client weergegeven als een van de volgende vier categorieën:

- DHCPv6 - voor clients met adressen die door een centrale server zijn toegewezen. De klant kan ook een SLAAC-adres hebben.
- SLAAC of Static - voor clients die gebruik maken van de automatische toewijzing van stateless adressen of die statisch geconfigureerde adressen gebruiken.
- Onbekend - In sommige gevallen kan de IPv6-adrestoewijzing niet worden ontdekt.Deze voorwaarde komt alleen voor bij bekabelde clients in NCS omdat sommige switches geen informatie over IPv6-adrestoewijzing doorzoeken.
- Zelftoegewezen - Voor klanten met alleen een Link-lokaal adres dat volledig zelftoegewezen is.Klanten in deze categorie kunnen problemen met IPv6-connectiviteit hebben omdat ze geen wereldwijd uniek of lokaal uniek adres hebben.

Elk van de secties van het cirkeldiagram is klikbaar, wat de beheerder toestaat om neer aan een lijst van cliënten te boren.



IPv6-clients controleren



Om IPv6-clientinformatie te bewaken en te beheren, zijn deze kolommen toegevoegd aan de pagina Clients en gebruikers:

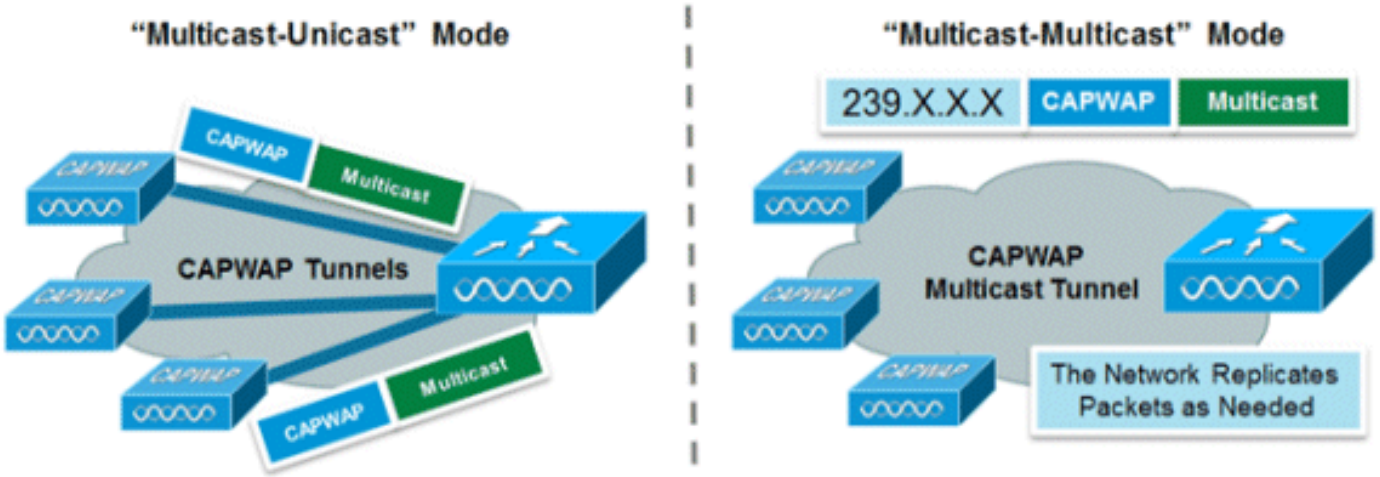
- IP Type - Het type client op basis van welke IP-adressen van de client zijn gezien. De mogelijke opties zijn IPv4, IPv6 of Dual-Stack die een client met zowel IPv4- als IPv6-adressen aanduidt.
- IPv6-toewijzingstype - de methode voor de adrestoewijzing wordt door NCS gedetecteerd als SLAAC of Statisch, DHCPv6, zelftoegewezen of onbekend.
- Wereldwijd uniek - Het meest recente algemene IPv6-adres dat door de client wordt gebruikt. Een muis-over op kolom inhoud onthult eventuele extra IPv6 globale unieke adressen gebruikt door de client.
- Lokale unieke - het meest recente lokale unieke IPv6-adres dat door de client wordt gebruikt. Een muis over op kolom inhoud onthult eventuele extra IPv6 globale unieke adressen gebruikt door de client.
- Link Local - Het IPv6-adres van de client dat zelf wordt toegewezen en wordt gebruikt voor communicatie voordat een ander IPv6-adres wordt toegewezen.
- Routeradvertenties Dropped - Het aantal routeradvertenties dat door de client is verzonden en op het toegangspunt is gedropt. Deze kolom kan worden gebruikt om clients op te sporen die mogelijk verkeerd zijn geconfigureerd of slecht zijn geconfigureerd om te handelen als een IPv6-router. Deze kolom is sorteerbaar, wat het mogelijk maakt om overtredende klanten gemakkelijk te identificeren.

Naast het weergeven van IPv6-specifieke kolommen, zal de kolom IP-adres het huidige IP-adres van de client tonen met een prioriteit om eerst het IPv4-adres weer te geven (in het geval van een Dual-Stack-client) of het globale unieke IPv6-adres in het geval van een client die alleen IPv6 is.

Configuratie voor draadloze IPv6-clientondersteuning

Multicastdistributiemodus naar AP's

Het Cisco Unified Wireless Network ondersteunt twee methoden voor multicast distributie naar AP's die aan de controller zijn gekoppeld. In beide modi wordt het oorspronkelijke multicast pakket van het bekabelde netwerk ingekapseld in een Layer 3 CAPWAP-pakket dat via CAPWAP Unicast of Multicast naar het toegangspunt wordt verzonden. Aangezien het verkeer is ingekapseld met CAPWAP, hoeven AP's niet op hetzelfde VLAN te staan als het clientverkeer. De twee methodes van Multicastdistributie worden hier vergeleken:



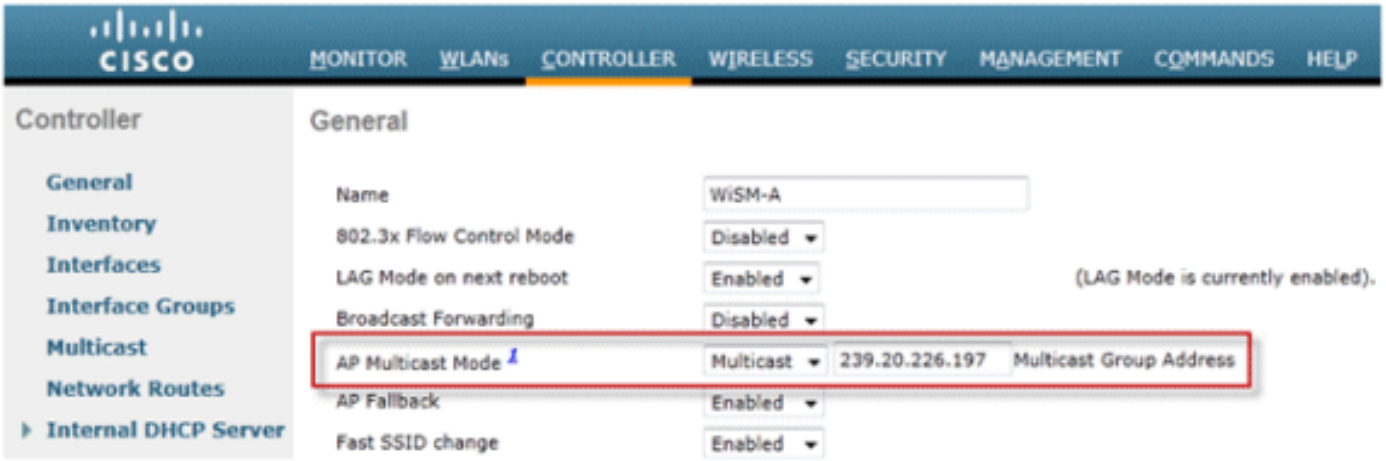
	Multicast-Unicast modus	Multicast-Multicast modus
Leveringsmechanisme	De controller repliceert het multicast pakket en verstuurt het naar elke AP in een Unicast CAPWAP-tunnel	De controller stuurt één kopie van het multicast pakket
Ondersteunde AP-modi	FlexConnect en lokaal	Alleen lokale modus
Vereist L3-multicast routing op bekabeld netwerk	Nee	Ja
Controllerlading	Hoog	Laag
Laden van bekabeld netwerk	Hoog	Laag

Multicast-Multicast distributiemodus configureren

Multicast-multicast modus is de aanbevolen optie voor schaalbaarheid en bekabelde bandbreedte-efficiëntie.

Opmerking: deze stap is alleen absoluut vereist voor de 2500 Series draadloze controller, maar het maakt efficiëntere multicast-transmissie mogelijk en wordt aanbevolen voor alle controller-platforms.

Ga naar het tabblad "Controller" onder de pagina "Algemeen" en zorg ervoor dat de AP Multicast Mode is geconfigureerd om de **Multicast** modus te gebruiken en dat er een geldig groepsadres is ingesteld. Het groepsadres is een IPv4 multicast groep en wordt aanbevolen voor gebruik in het 239.X.X.X-239.255.255.255-bereik, dat is bedoeld voor particuliere multicast toepassingen.

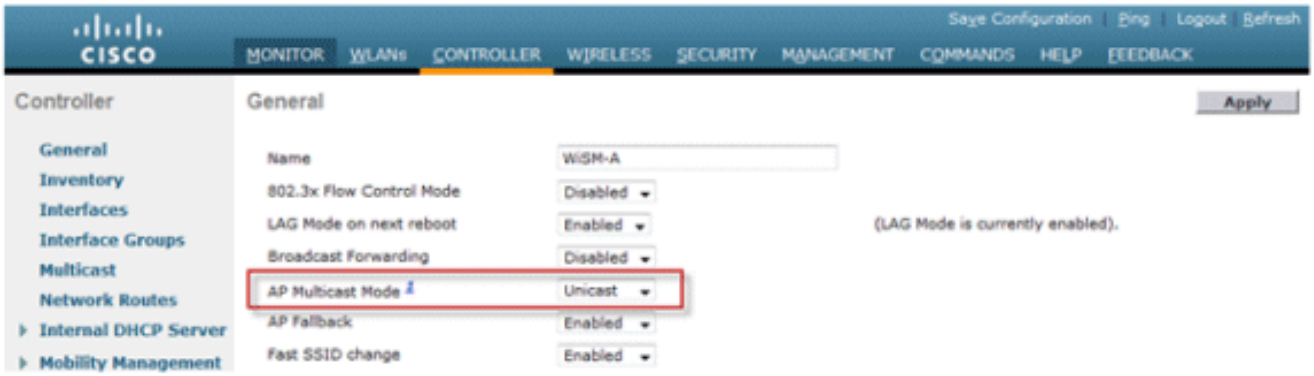


Opmerking: Gebruik de adresbereiken 224.X.X.X, 239.0.0.X of 239.128.0.X niet voor het multicast groepsadres. Adressen in deze bereiken overlappen met de link lokale MAC-adressen en overspoelen alle switch-poorten, zelfs met IGMP-snooping ingeschakeld.

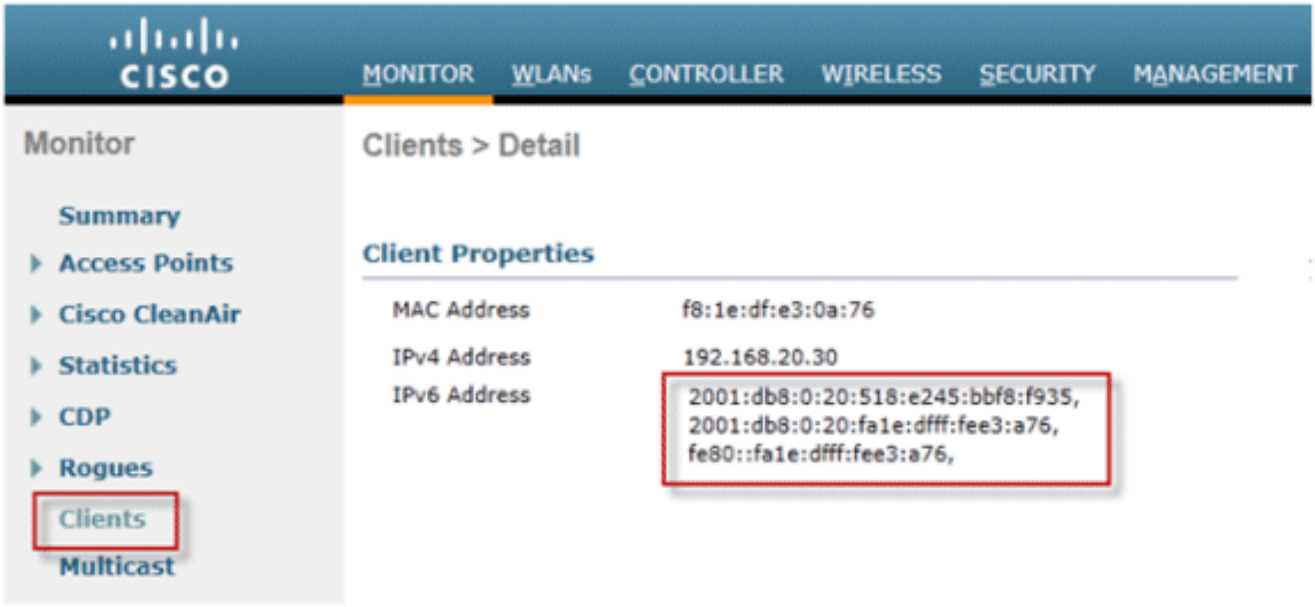
Multicast-Unicast distributiemodus configureren

Als het bekabelde netwerk niet goed is geconfigureerd om de CAPWAP-multicast te leveren tussen de controller en de AP- of FlexConnect-modus, en AP's worden gebruikt voor centraal switched WLAN's die IPv6 ondersteunen, is de unicastmodus vereist.

1. Ga naar het tabblad **Controller** onder de pagina Algemeen en zorg ervoor dat de AP Multicast Mode is geconfigureerd om de **Unicast**-modus te gebruiken.



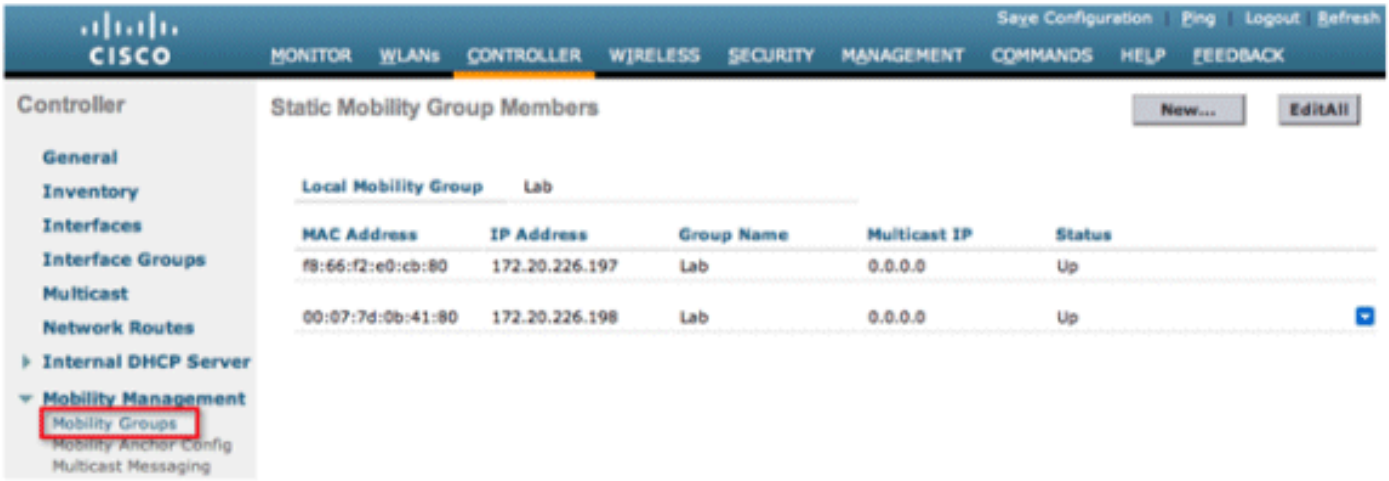
2. Sluit een client die IPv6 ondersteunt aan op het draadloze LAN. Bevestig dat de client een IPv6-adres ontvangt door te navigeren naar het tabblad **Monitor** en vervolgens naar het menu **Clients**.



IPv6-mobiliteit configureren

Er is geen specifieke configuratie voor IPv6-mobiliteit behalve om controllers in dezelfde mobiliteitsgroep of binnen hetzelfde mobiliteitsdomein te plaatsen. Hierdoor kunnen maximaal 72 controllers deelnemen aan een mobiliteitsdomein, wat naadloze mobiliteit biedt voor zelfs de grootste campussen.

Ga naar het **tabblad Controller > Mobiliteitsgroepen**, en voeg elke controller toe per MAC-adres en IP-adres in de groep. Dit moet worden gedaan voor alle controleurs in de mobiliteitsgroep.



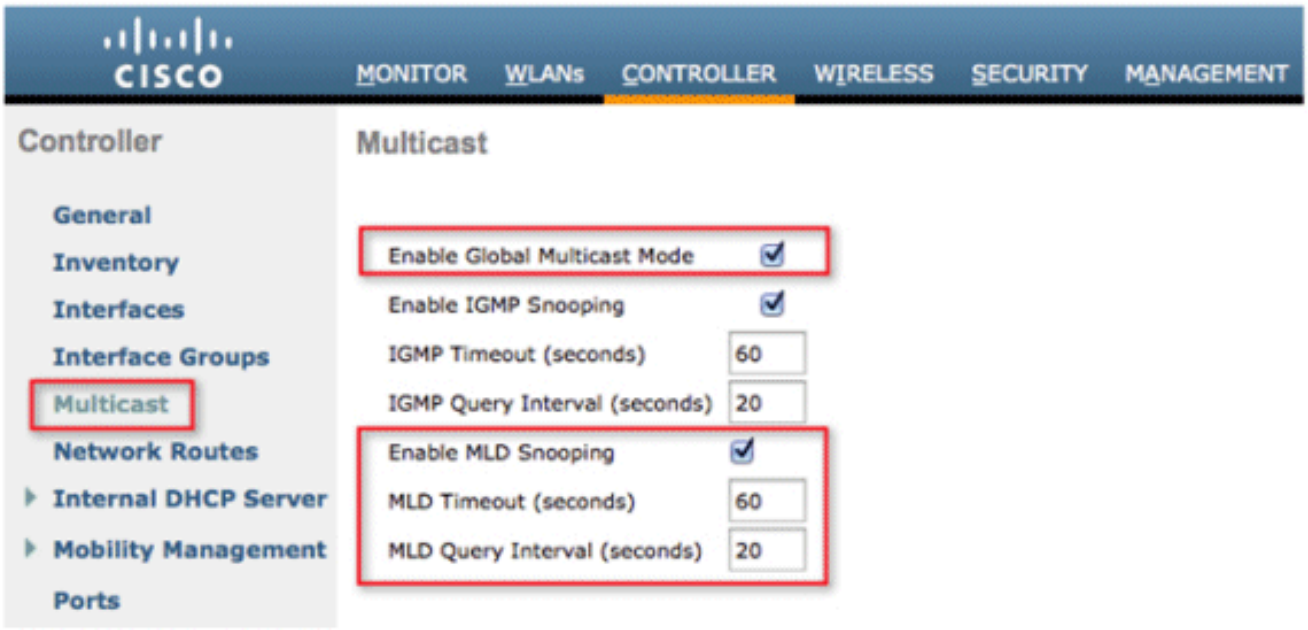
IPv6-multicast configureren

De controller ondersteunt MLDv1 snooping voor IPv6 multicast, waardoor het op intelligente wijze de multicast-stromen kan bijhouden en leveren aan clients die hierom vragen.

Opmerking: in tegenstelling tot eerdere versies van releases vereist IPv6-ondersteuning van unicastverkeer niet dat "Global Multicast Mode" is ingeschakeld op de controller. IPv6-unicastverkeersondersteuning wordt automatisch ingeschakeld.

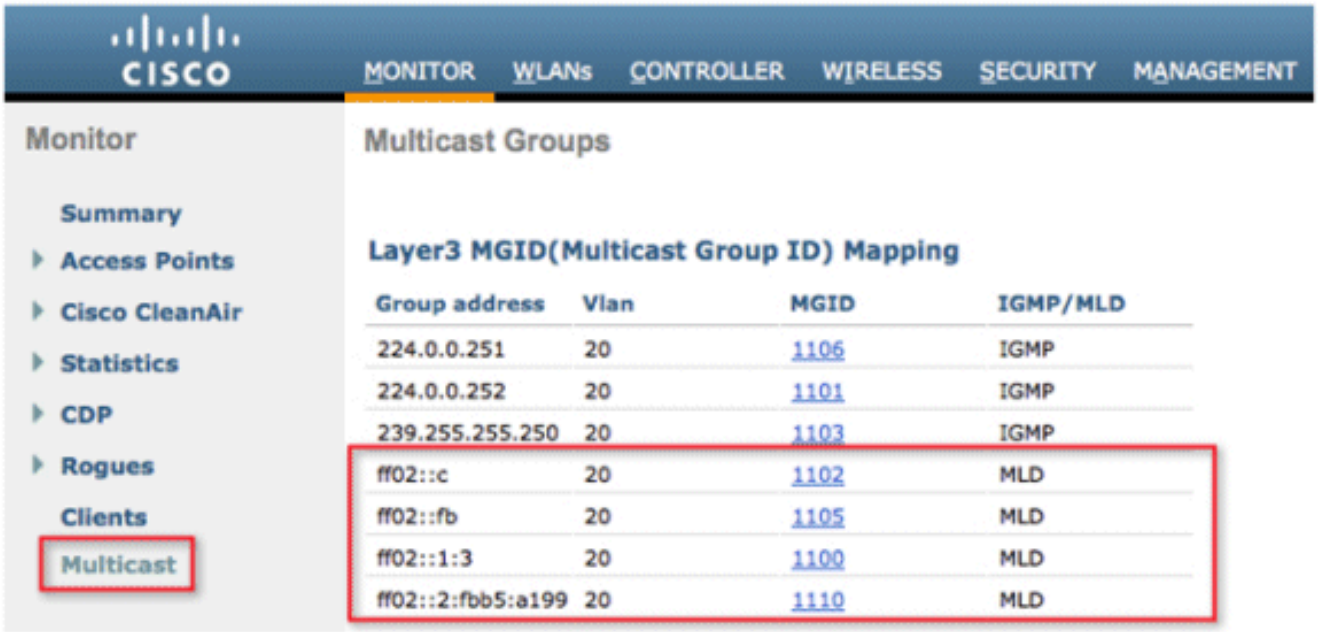
1. Ga naar het tabblad **Controller > Multicast**-pagina en **Schakel MLD Snooping** in om multicast IPv6-verkeer te ondersteunen. Om IPv6 Multicast te kunnen inschakelen, moet de **Global**

Multicast Mode van de controller ook zijn ingeschakeld.



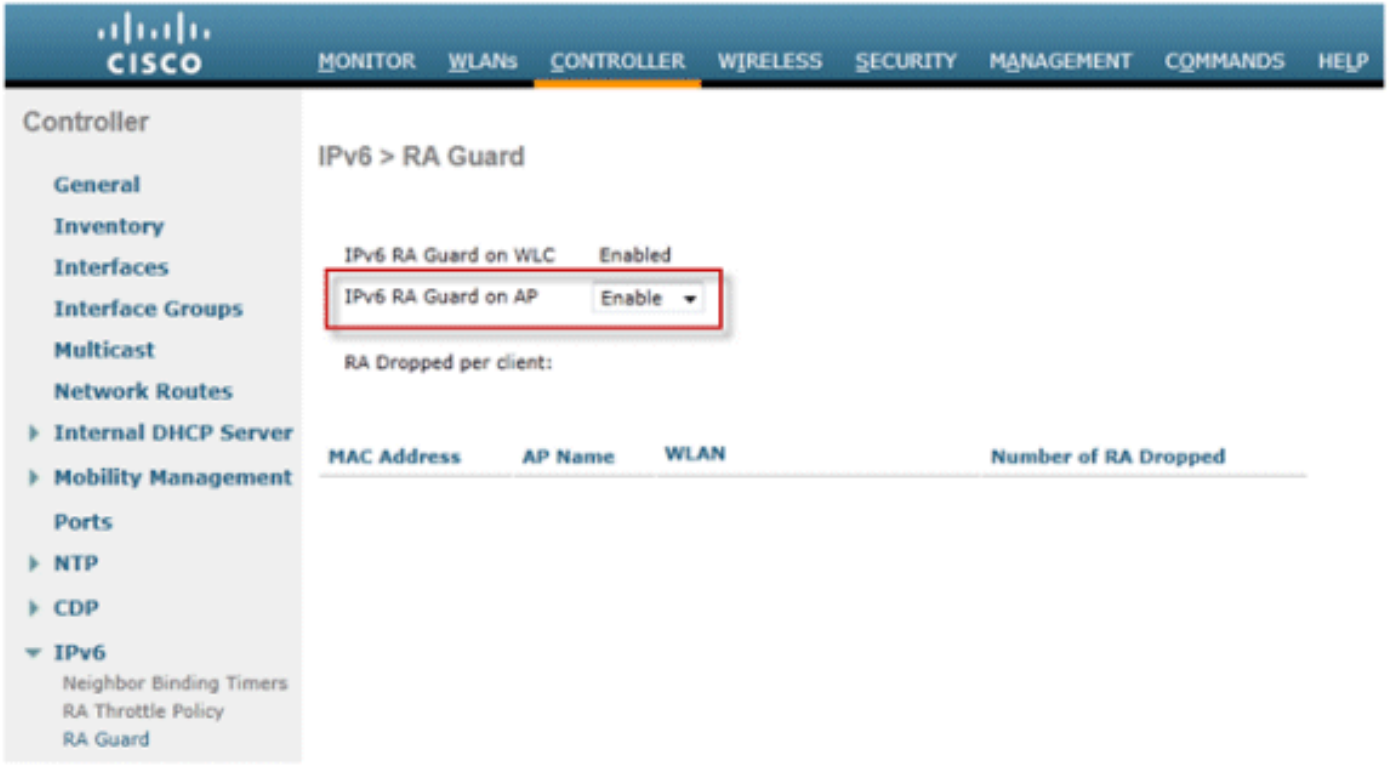
Opmerking: Global Multicast Mode, IGMP en MLD snooping moeten worden ingeschakeld als peer-to-peer detectietoepassingen zoals de Bonjour van Apple nodig zijn.

2. Ga naar het tabblad **Monitor** en de pagina **Multicast** om te controleren of IPv6-multicast verkeer wordt gesnooped. Bericht dat zowel IPv4 (IGMP) als IPv6 (MLD) multicast groepen vermeld zijn. Klik op de MGID om de draadloze clients te bekijken die zijn aangesloten op dat groepsadres.



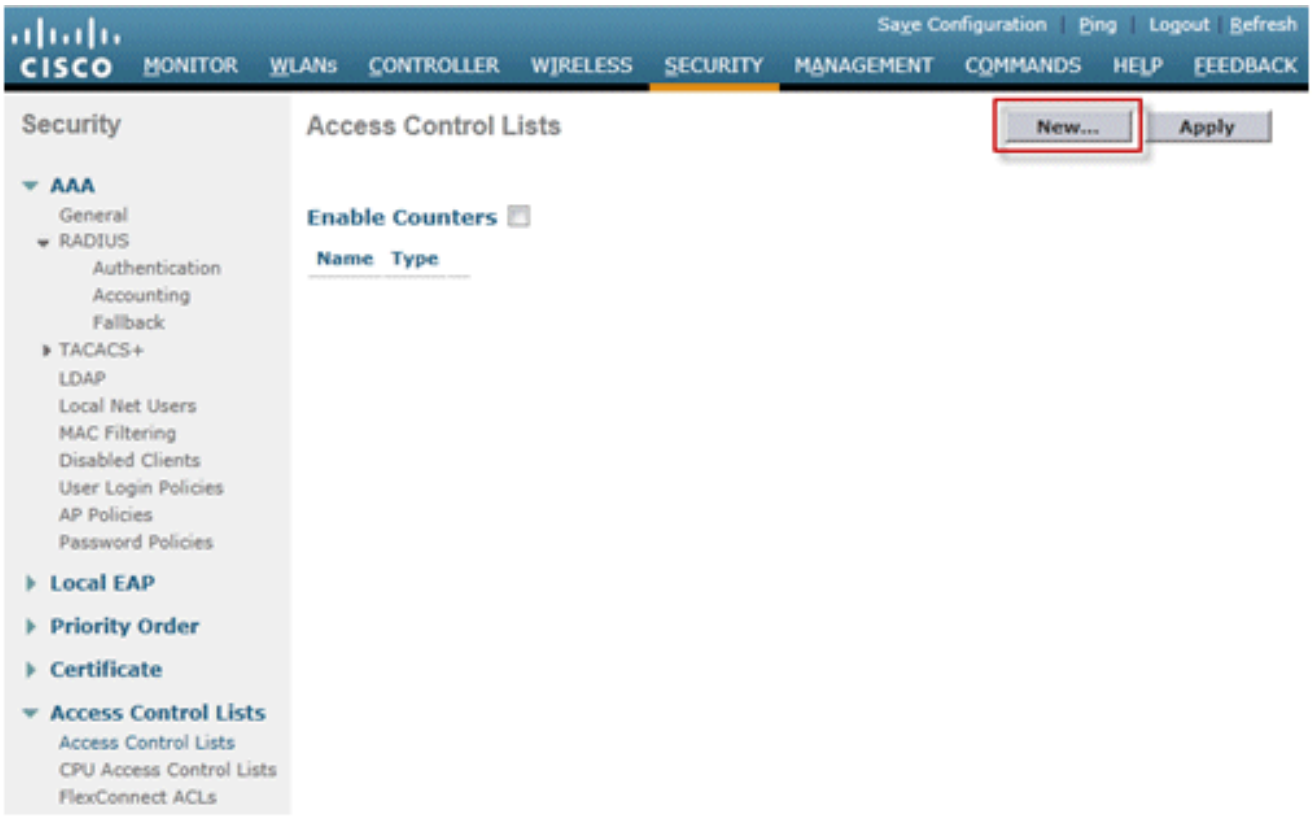
IPv6 RA-bewaking configureren

Navigeer naar het tabblad **Controller** en vervolgens naar **IPv6 > RA Guard** in het linker menu. **Schakel** IPv6 RA Guard op access point in. RA Guard op de controller kan niet worden uitgeschakeld. Naast de configuratie van de RA Guard, toont deze pagina ook alle klanten die als verzendende RA's zijn geïdentificeerd.



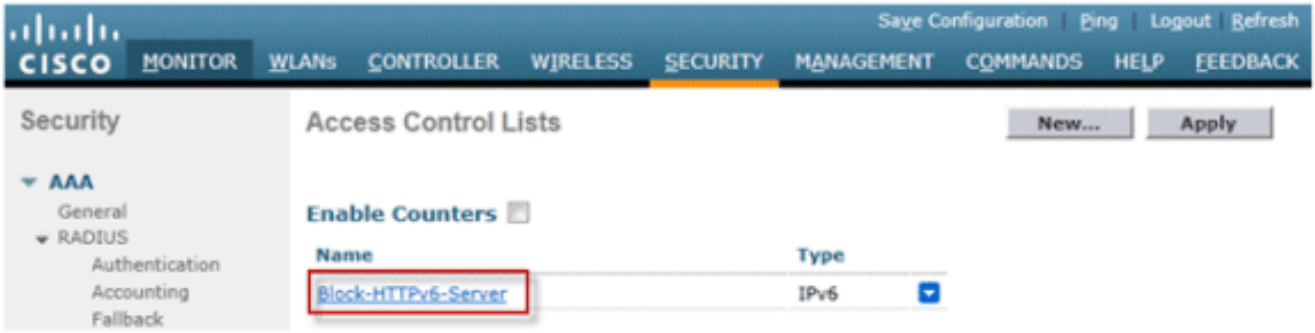
IPv6-toegangscontrolelijsten configureren

1. Ga naar het tabblad **Beveiliging**, open **toegangscontrolelijsten** en klik op **Nieuw**.

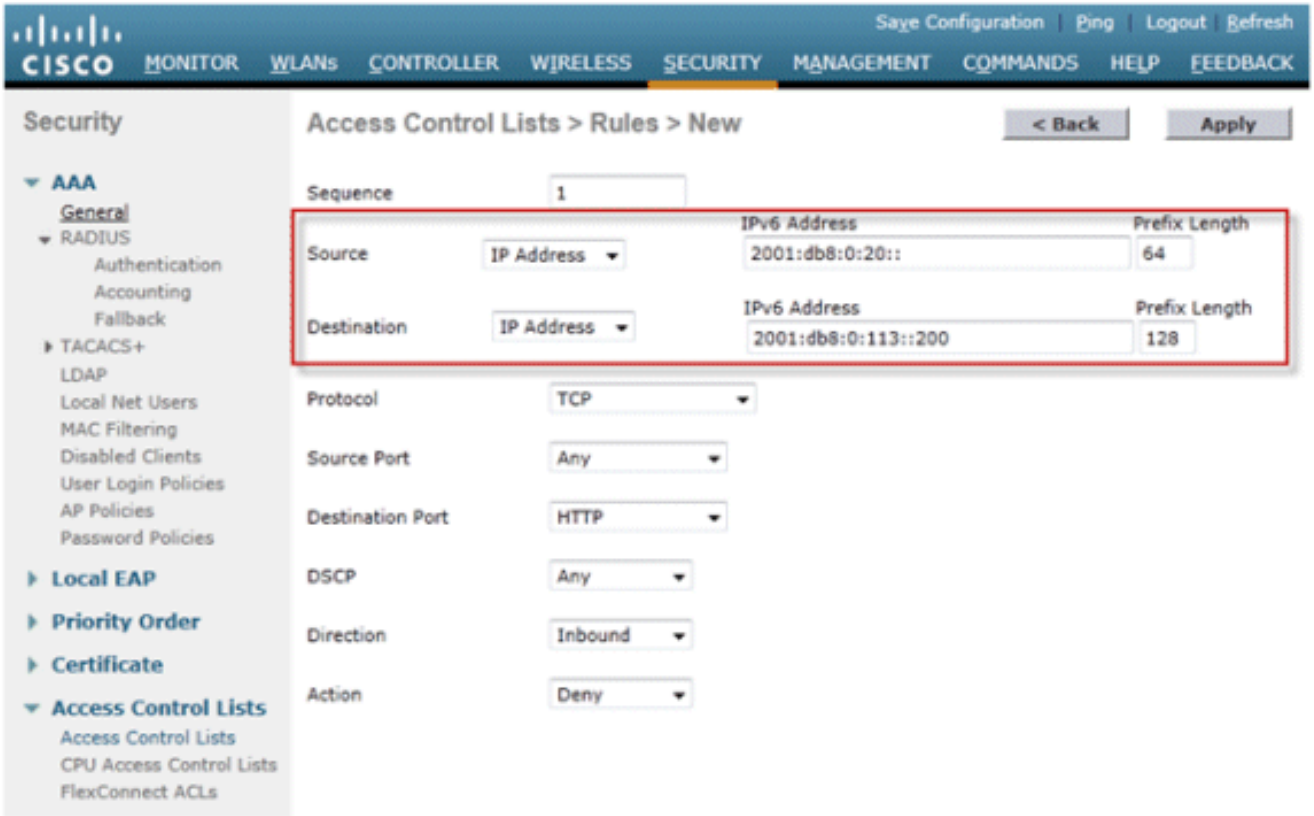


2. Voer een unieke naam in voor de ACL, wijzig het ACL-type in **IPv6** en klik op **Toepassen**.

3. Klik op de nieuwe ACL die in de bovenstaande stappen is gemaakt.

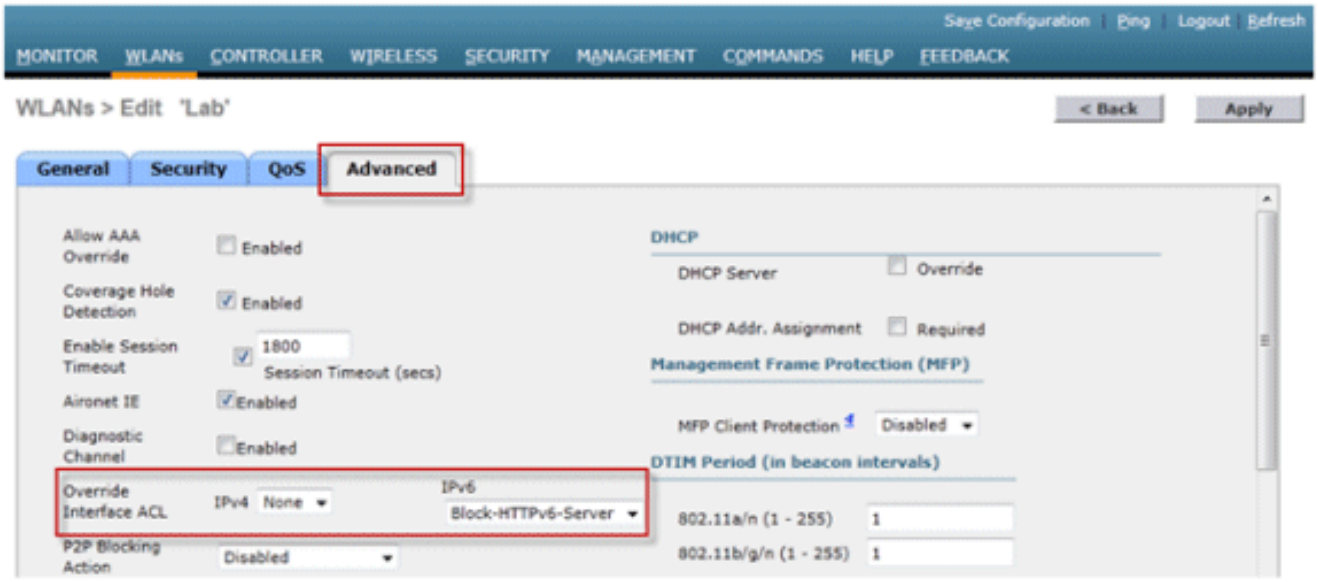


4. Klik op **Nieuwe regel toevoegen**, voer de gewenste parameters voor de regel in en klik op **Toepassen**. Laat het volgnummer leeg om de regel aan het einde van de lijst te plaatsen. De optie "Richting" van "Inbound" wordt gebruikt voor verkeer vanaf het draadloze netwerk en "Outbound" voor verkeer dat voor draadloze clients is bestemd. Herinner me, is de laatste regel in ACL impliciet ontkennen-allen. Gebruik een prefixlengte van 64 om een volledig IPv6-subnetnummer aan te passen en een prefixlengte van 128 om de toegang tot een individueel adres op unieke wijze te beperken.



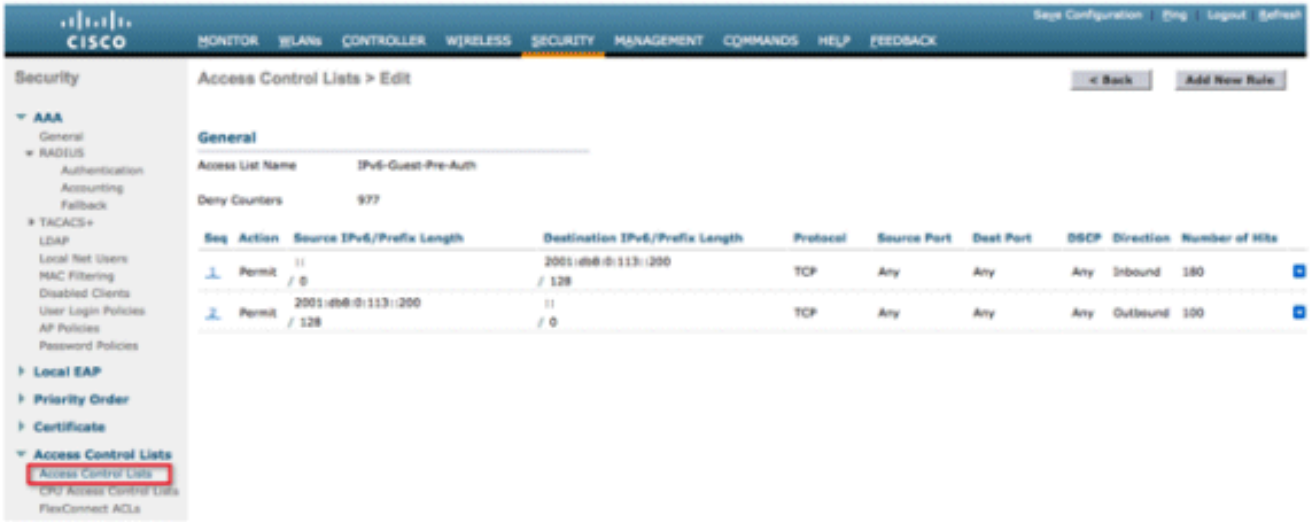
5. IPv6-ACL's worden per WLAN/SSID toegepast en kunnen gelijktijdig op meerdere WLAN's worden gebruikt. Navigeer naar het tabblad **WLAN's** en klik op de WLAN-id van de SSID in

kwestie om de IPv6-ACL toe te passen. Klik op het tabblad **Geavanceerd** en wijzig de ACL met interface negeren voor IPv6 in de ACL-
naam.



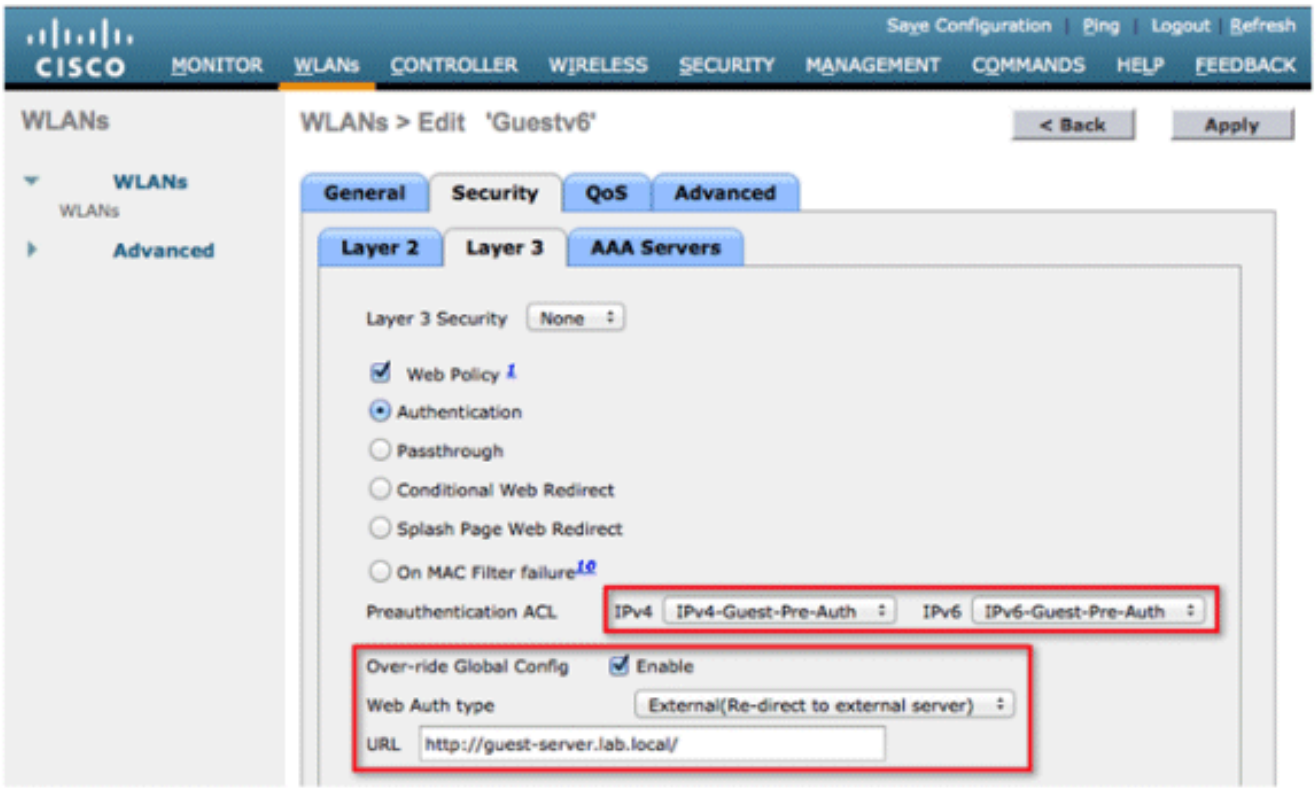
IPv6-gasttoegang configureren voor externe webverificatie

1. Configureer de ACL voor voorafgaande verificatie van IPv4 en IPv6 voor de webserver. Dit maakt verkeer van en naar de externe server mogelijk voordat de client volledig is geverifieerd.



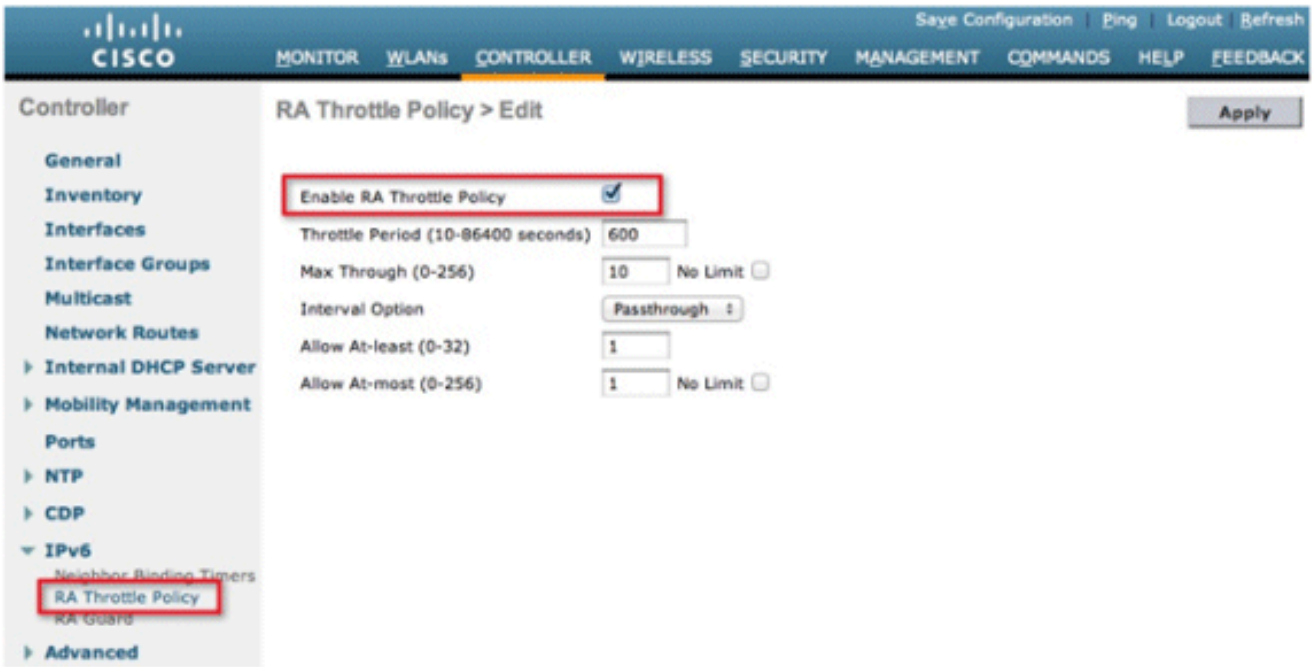
Raadpleeg voor meer informatie over het gebruik van externe webtoegang Configuratievoorbeeld van externe webverificatie met draadloze LAN-controllers.

2. Configureer het WLAN door naar het tabblad WLAN's bovenaan te bladeren. Maak de Guest SSID en gebruik een Layer 3 webbeleid. De vooraf gedefinieerde ACL's in stap 1 worden geselecteerd voor IPv4 en IPv6. Controleer de sectie Over-ride Global Config en selecteer **Extern** in het vervolgkeuzevenster Type Web Auth. Voer de URL van de webserver in. De hostnaam van de externe server moet oplosbaar zijn in IPv4 en IPv6
DNS.



IPv6-RNA-beperking configureren

1. Navigeer naar het bovenste menu van de **controller** en klik op de optie **IPv6 > RA Throttle Policy** aan de linkerkant. Schakel RA Throttling in door op het selectievakje te klikken.



Opmerking: Wanneer RA Throttling optreedt, is alleen de eerste IPv6-compatibele router toegestaan. Voor netwerken met meerdere IPv6-prefixes die door verschillende routers worden bediend, moet RA-beperking worden uitgeschakeld.

2. Pas de gaspedaal en andere opties aan enkel onder advies van TAC. De standaardinstelling wordt echter voor de meeste implementaties aanbevolen. De verschillende configuratieopties van het RA Throttling-beleid moeten met dit in gedachten worden aangepast:De numerieke waarden van "Ten minste toestaan" moeten kleiner zijn dan "Ten hoogste toestaan", wat

minder zou moeten zijn dan "Tot max.".Het RA-gaspedaalbeleid mag geen gaspedaal gebruiken die langer is dan 1800 seconden, aangezien dit de standaardlevensduur van de meeste RA's is.

Elke RA Throttling optie wordt hieronder beschreven:

- De periode van het gaspedaal - de periode waarin het gaspedaal plaatsvindt. RA-beperking wordt pas van kracht nadat de "Max Through"-limiet voor VLAN is bereikt.
- Max Through - Dit is het maximale aantal RA's per VLAN voordat het gaspedaal wordt ingeschakeld. De "No Limit"-optie maakt een onbeperkt aantal RA's zonder beperking mogelijk.
- Interval Option - Met de intervaloptie kan de controller anders handelen op basis van de RFC 3775-waarde die in de IPv6-RA is ingesteld.Passthrough - Met deze waarde kunnen RA's met een RFC3775-intervaloptie zonder throttling doorlopen.Negeren - Deze waarde zorgt ervoor dat de RA throttler pakketten met de interval optie als een normale RA en onderhevig aan throttling als in feite.Throttle - Deze waarde zorgt ervoor dat de RA's met de intervaloptie altijd onderhevig zijn aan snelheidsbeperking.
- Minimaal toestaan - Het minimumaantal RA's per router dat als multicast wordt verzonden.
- Toestaan Hoogste - Het maximale aantal RA's per router dat als multicast wordt verzonden voordat throttling van kracht wordt. De "No Limit" optie zal een onbeperkt aantal RA's doorlaten voor die router.

De bindende tabel voor de IPv6-buur configureren

1. Ga naar het bovenste menu van de controller en klik op **IPv6 > Bindingstimers voor** de **buur** in het
linkermenu.

2. Pas omlaag Leven, Bereikbare Leven, en Verblijfelijke Leven aan zoals nodig. Voor implementaties met clients die zeer mobiel zijn, moeten de timers voor een verouderde adrestimer worden aangepast. De aanbevolen waarden zijn:Levenslang - 30 secondenReachable Lifetime - 300 secondenState Lifetime - 86400 secondenElke levensduur timer verwijst naar de status waarin een IPv6-adres kan zijn:**Down Lifetime** - De down timer specificeert hoe lang de IPv6 cache-ingangen moeten worden bewaard als de uplink-interface van de controller uitvalt.**Reachable Lifetime** - Deze timer geeft aan hoe lang een IPv6-adres actief wordt gemarkeerd, wat betekent dat er onlangs verkeer van dit adres is ontvangen. Als deze timer is verlopen, wordt het adres naar de status "Verkoop" verplaatst.**Stale Lifetime** - Deze timer geeft aan hoe lang IPv6-adressen in het cache moeten blijven die niet in de "Reachable Lifetime" worden gezien. Na dit leven, wordt het adres verwijderd uit de bindende lijst.

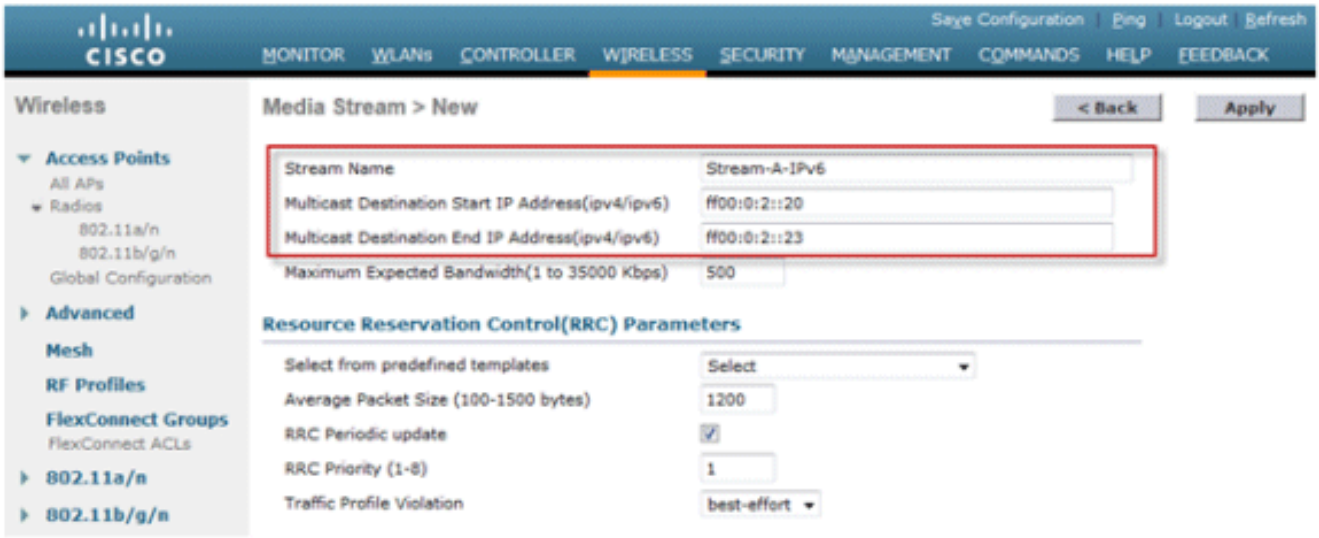
IPv6-videostream configureren

1. Zorg ervoor dat Global VideoStream-functies zijn ingeschakeld op de controller. Raadpleeg Cisco Unified Wireless Network Solution: implementatiegids voor videoStream voor

informatie over het inschakelen van VideoStream op het 802.11a/g/n-netwerk en op de WLAN-SSID.

2. Ga naar het tabblad **Draadloos** op de controller en kies in het menu links **Media Stream** > **Streams**. Klik op **Add New** om een nieuwe stream te maken.

3. Geef de stream een naam en voer de begin- en eindadressen van IPv6 in. Wanneer u slechts één stream gebruikt, zijn de begin- en eindadressen gelijk. Na het toevoegen van de adressen, klik op **Toepassen** om de stream te maken.



Probleemoplossing voor IPv6-clientconnectiviteit

Bepaalde clients kunnen IPv6-verkeer niet doorgeven

Sommige IPv6-netwerkstackimplementaties van clients maken zichzelf niet goed bekend wanneer ze op het netwerk komen en daarom wordt hun adres niet correct gesnooped door de controller voor plaatsing in de buurbindingstabel. Alle adressen die niet voorkomen in de bindingstabel van de buur worden geblokkeerd volgens de functie IPv6-bronbeveiliging. Om deze cliënten toe te staan om verkeer over te gaan, moeten deze opties worden gevormd:

1. Schakel de functie IPv6-bronbeveiliging uit via de CLI:

   config network ip-mac-binding disable

2. Doorsturen van multicastvragen via de CLI inschakelen:

   config ipv6 ns-mcast-fwd enable

Controleer succesvolle Layer 3-roaming voor een IPv6-client:

Geef deze **debug** commando's uit op zowel de anker als de buitenlandse controller:

debug client

debug mobility handoff enable

debug mobility packet enable

Debug resultaten op ankercontroller:

```
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
```

Debug resultaten op Foreign Controller:

```
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
```

Handige IPv6 CLI-opdrachten:

Show ipv6 neighbor-binding summary

Debug ipv6 neighbor-binding filter client enable

Debug ipv6 neighbor-binding filter errors enable

Veelgestelde vragen

Q: Wat is de optimale IPv6 prefixgrootte om het uitzendingsdomein te beperken?

A: Hoewel een IPv6-subnetverbinding kan worden onderverdeeld onder een /64, zal deze configuratie SLAAC verbreken en problemen met de clientconnectiviteit veroorzaken. Als segmentatie nodig is om het aantal hosts te verminderen, kan de functie Interfacegroepen worden gebruikt om clients te laden en te balanceren tussen verschillende back-end VLAN's, elk met een andere IPv6-prefix.

V: Zijn er enige schaalbaarheidsbeperkingen als het gaat om het ondersteunen van IPv6-clients?

A: De belangrijkste schaalbaarheidsbeperking voor IPv6-clientondersteuning is de buurbindingstabel die alle IPv6-adressen van draadloze clients bijhoudt. Deze tabel wordt per controller platform geschaald om het maximale aantal clients te ondersteunen, vermenigvuldigd met acht (het maximale aantal adressen per client). De toevoeging van de IPv6-bindingstabel kan het geheugengebruik van de controller met ongeveer 10-15% verhogen onder volle belasting, afhankelijk van het platform.

Draadloze controller	Maximum aantal clients	IPv6-buur, bindend tabelformaat
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

V: Wat is de impact van IPv6-functies op de CPU en het geheugen van de controller?

A: De impact is minimaal omdat de CPU over meerdere kernen beschikt om het besturingsplane te verwerken. Bij testen met maximaal ondersteunde clients, elk met 8 IPv6-adressen, was het CPU-gebruik minder dan 30% en het geheugengebruik minder dan 75%.

V: Kan IPv6-clientondersteuning worden uitgeschakeld?

A: Voor klanten die alleen IPv4 in hun netwerk willen inschakelen en IPv6 willen blokkeren, kan een IPv6 ACL van deny-all verkeer worden gebruikt en per WLAN worden toegepast.

V: Is het mogelijk om een WLAN te hebben voor IPv4 en een WLAN voor IPv6?

A: Het is niet mogelijk om dezelfde SSID-naam en hetzelfde beveiligingstype te hebben voor twee verschillende WLAN's die op dezelfde AP werken. Voor segmentatie van IPv4-clients van IPv6-clients moeten twee WLAN's worden gemaakt. Elk WLAN moet worden geconfigureerd met een ACL die al het IPv4- of IPv6-verkeer blokkeert.

V: Waarom is het belangrijk om meerdere IPv6-adressen per client te ondersteunen?

A: Clients kunnen meerdere IPv6-adressen per interface hebben die statisch, SLAAC of DHCPv6 kunnen zijn toegewezen, naast het altijd hebben van een zelf toegewezen Link-Local adres. Clients kunnen ook extra adressen hebben met verschillende IPv6-prefixes.

Q: Wat zijn IPv6 privé adressen en waarom zijn zij belangrijk om te volgen?

A: Privé-adressen (ook wel bekend als tijdelijke adressen) worden willekeurig gegenereerd door de klant wanneer de SLAAC-adrestoewijzing in gebruik is. Deze adressen worden vaak geroteerd met een frequentie van een dag of zo, om de traceerbaarheid van de host te voorkomen die zou komen van het gebruik van dezelfde host postfix (laatste 64 bits) te allen tijde. Het is belangrijk deze privéadressen te volgen voor auditdoeleinden zoals het traceren van inbreuken op auteursrechten. Cisco NCS registreert alle IPv6-adressen die door elke client worden gebruikt en registreert deze historisch telkens wanneer de client zwerft of een nieuwe sessie start. Deze records kunnen worden geconfigureerd bij NCS voor een periode tot een jaar.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.