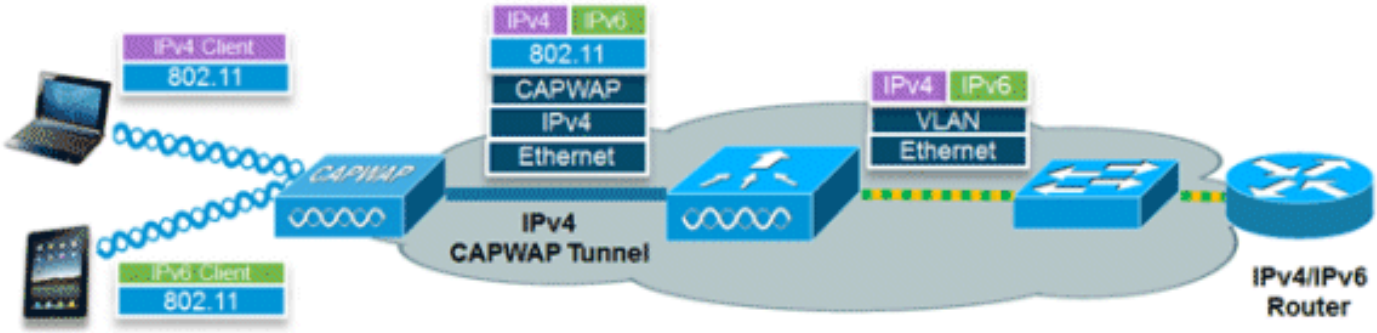
Guía de implementación del cliente IPv6 de LAN inalámbrica

Contenido

Introducción

Este documento proporciona información sobre la teoría del funcionamiento y la configuración de la solución Cisco Unified Wireless LAN en relación al soporte de los clientes IPv6.

Conectividad de cliente inalámbrico IPv6



El conjunto de funciones IPv6 de la versión 7.2 del software Cisco Unified Wireless Network permite que la red inalámbrica admita clientes IPv4, Dual-Stack y solo IPv6 en la misma red inalámbrica. El objetivo general de la adición de compatibilidad con clientes IPv6 a Cisco Unified Wireless LAN era mantener la paridad de funciones entre los clientes IPv4 e IPv6, incluidos movilidad, seguridad, acceso de invitados, calidad de servicio y visibilidad de terminales.

Se puede realizar un seguimiento de hasta ocho direcciones de cliente IPv6 por dispositivo. Esto permite que los clientes IPv6 tengan una dirección de configuración automática de direcciones sin estado (SLAAC) local de vínculo, una dirección de protocolo de configuración dinámica de host para IPv6 (DHCPv6) e incluso direcciones en prefijos alternativos para estar en una única interfaz. Los clientes de puente de grupo de trabajo (WGB) conectados al enlace ascendente de un punto de acceso (AP) autónomo en modo WGB también pueden admitir IPv6.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Controladores de LAN inalámbrica serie 2500, serie 5500 o WiSM2
- APs 1130, 1240, 1250, 1040, 1140, 1260, 3500, 3600 Series APs, y 1520 o 1550 Series Mesh APs
- Router compatible con IPv6

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

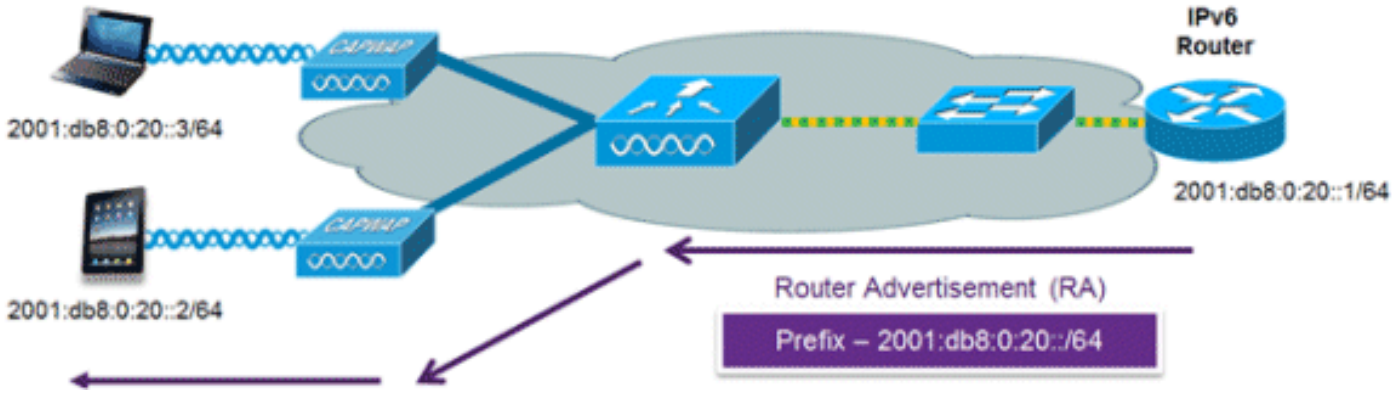
Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Prerrequisitos de Wireless IPv6 Client Connectivity

Para habilitar la conectividad de cliente IPv6 inalámbrica, la red con cables subyacente debe admitir el enrutamiento IPv6 y un mecanismo de asignación de direcciones como SLAAC o DHCPv6. El controlador de LAN inalámbrica debe tener adyacencia de capa 2 al router IPv6 y la VLAN debe etiquetarse cuando los paquetes entran en el controlador. Los AP no requieren conectividad en una red IPv6, ya que todo el tráfico se encapsula dentro del túnel CAPWAP IPv4 entre el AP y el controlador.

Asignación de dirección SLAAC

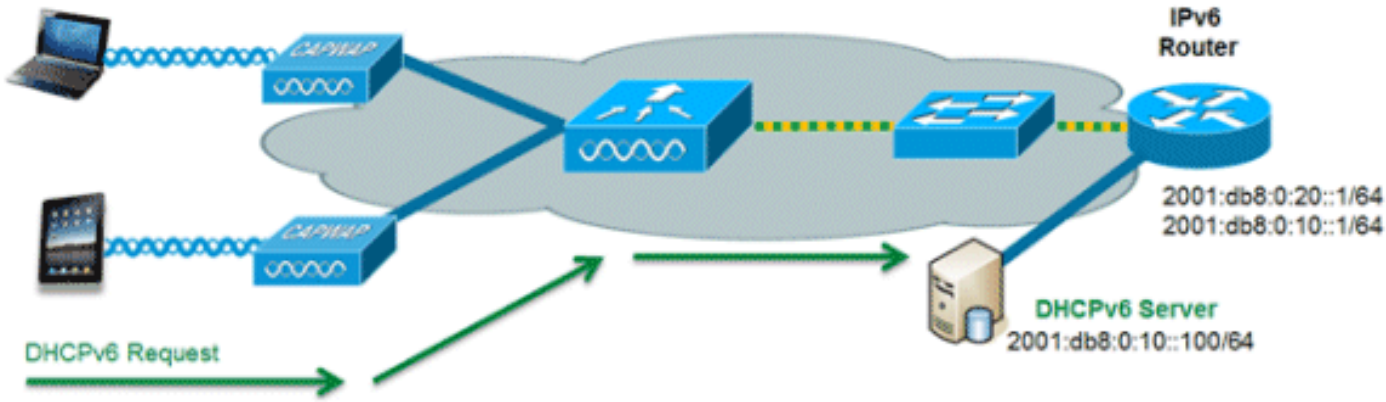


El método más común para la asignación de direcciones de cliente IPv6 es SLAAC. SLAAC proporciona una conectividad Plug and Play sencilla en la que los clientes autoasignan una dirección basándose en el prefijo IPv6. Este proceso se logra cuando el router IPv6 envía mensajes periódicos de anuncio del router que informan al cliente del prefijo IPv6 en uso (los primeros 64 bits) y del gateway predeterminado IPv6. A partir de ese punto, los clientes pueden generar los 64 bits restantes de su dirección IPv6 basándose en dos algoritmos: EUI-64, que se basa en la dirección MAC de la interfaz, o direcciones privadas que se generan aleatoriamente. La elección del algoritmo depende del cliente y suele ser configurable. Los clientes IPv6 realizan la detección de direcciones duplicadas para garantizar que las direcciones aleatorias que se seleccionan no colisionan con otros clientes. La dirección del router que envía anuncios se utiliza como la gateway predeterminada para el cliente.

Estos comandos de configuración de Cisco IOS® de un router IPv6 compatible con Cisco se utilizan para habilitar el direccionamiento de SLAAC y los anuncios de router:

```
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
```

Asignación de dirección DHCPv6



El uso de DHCPv6 no es necesario para la conectividad de cliente IPv6 si SLAAC ya está implementado. Hay dos modos de operación para DHCPv6 llamados **Stateless** y **Stateful**.

El modo DHCPv6 **Stateless** se utiliza para proporcionar a los clientes información de red adicional no disponible en el anuncio del router, pero no una dirección IPv6, ya que esto ya lo proporciona SLAAC. Esta información puede incluir el nombre de dominio DNS, los servidores DNS y otras opciones específicas del proveedor DHCP. Esta configuración de interfaz es para un router IPv6 de Cisco IOS que implementa DHCPv6 sin estado con SLAAC habilitado:

```
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
```

La opción **Stateful** de DHCPv6, también conocida como modo administrado, funciona de manera similar a DHCPv4 en el sentido de que asigna direcciones únicas a cada cliente en lugar de que el cliente genere los últimos 64 bits de la dirección como en SLAAC. Esta configuración de interfaz es para un router IPv6 de Cisco IOS que implementa DHCPv6 con estado con SLAAC desactivado:

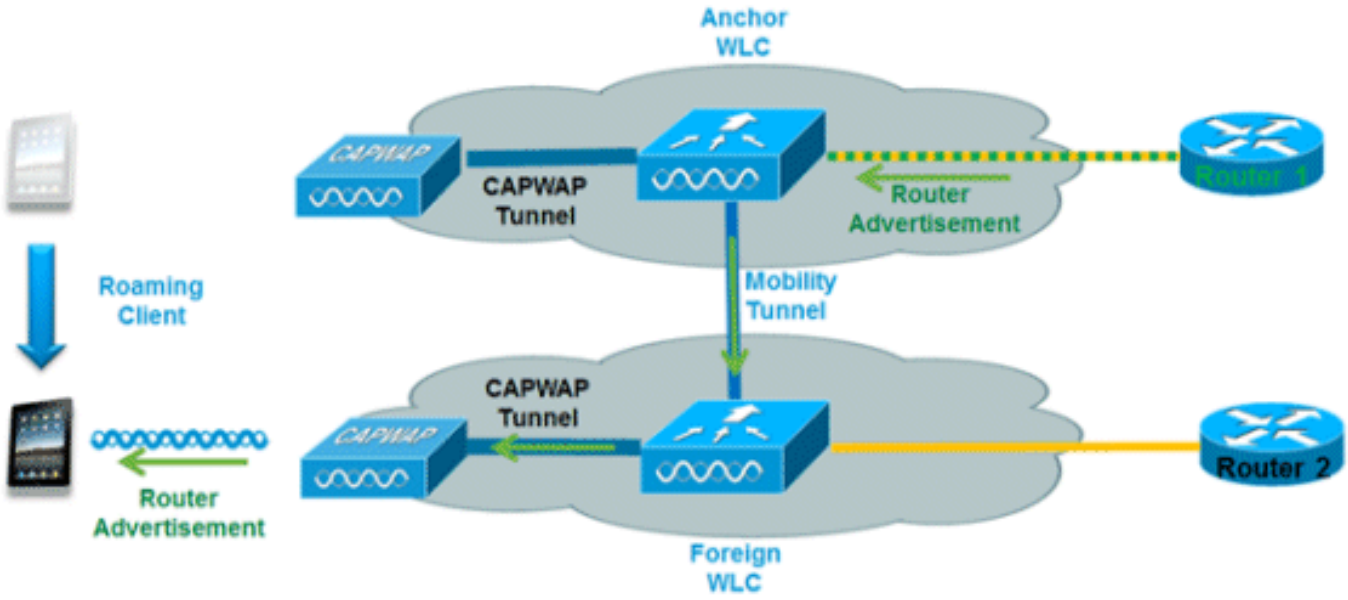
```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateful
```

```
 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 configuración de la red por cable para una conectividad completa de todo el campus IPv6 mediante métodos de conectividad de tunelización o de pila doble está fuera del alcance de este documento. Para obtener más información, consulte la guía de implementación validada de Cisco Implementación de IPv6 en redes de campus.

Movilidad de clientes IPv6



Para lidiar con los clientes IPv6 de roaming a través de los controladores, los mensajes ICMPv6 como la solicitud de vecino (NS), la publicidad de vecino (NA), la publicidad de router (RA) y la solicitud de router (RS) deben tratarse especialmente para garantizar que un cliente permanece en la misma red de capa 3. La configuración para la movilidad IPv6 es la misma que para la movilidad IPv4 y no requiere ningún software independiente en el lado del cliente para lograr una itinerancia sin problemas. La única configuración necesaria es que los controladores deben formar parte del mismo grupo/dominio de movilidad.

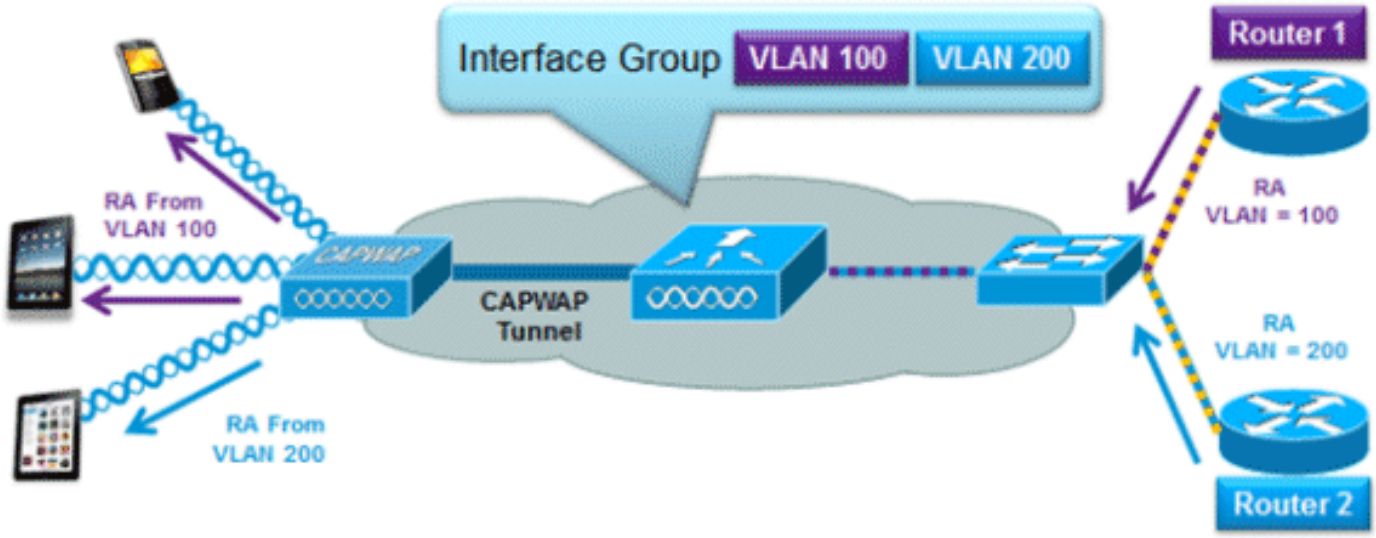
Este es el proceso para la movilidad de clientes IPv6 entre controladores:

1. Si ambos controladores tienen acceso a la misma VLAN en la que estaba originalmente el cliente, la itinerancia es simplemente un evento de itinerancia de Capa 2 donde el registro del cliente se copia al nuevo controlador y no se tuneliza ningún tráfico de regreso al controlador de anclaje.
2. Si el segundo controlador no tiene acceso a la VLAN original en la que estaba el cliente, se producirá un evento de itinerancia de Capa 3, lo que significa que todo el tráfico del cliente debe tunelizarse a través del túnel de movilidad (Ethernet sobre IP) al controlador de

anclaje.Para asegurarse de que el cliente conserve su dirección IPv6 original, los RA de la VLAN original son enviados por el controlador de anclaje al controlador externo donde se entregan al cliente mediante unidifusión L2 desde el AP.Cuando el cliente de roaming va a renovar su dirección a través de DHCPv6 o genera una nueva dirección a través de SLAAC, los paquetes RS, NA y NS continúan siendo tunelados a la VLAN original para que el cliente reciba una dirección IPv6 que sea aplicable a esa VLAN.

Nota: La movilidad de los clientes solo de IPv6 se basa en la información de VLAN. Esto significa que la movilidad del cliente solo de IPv6 no se soporta en las VLAN sin etiqueta.

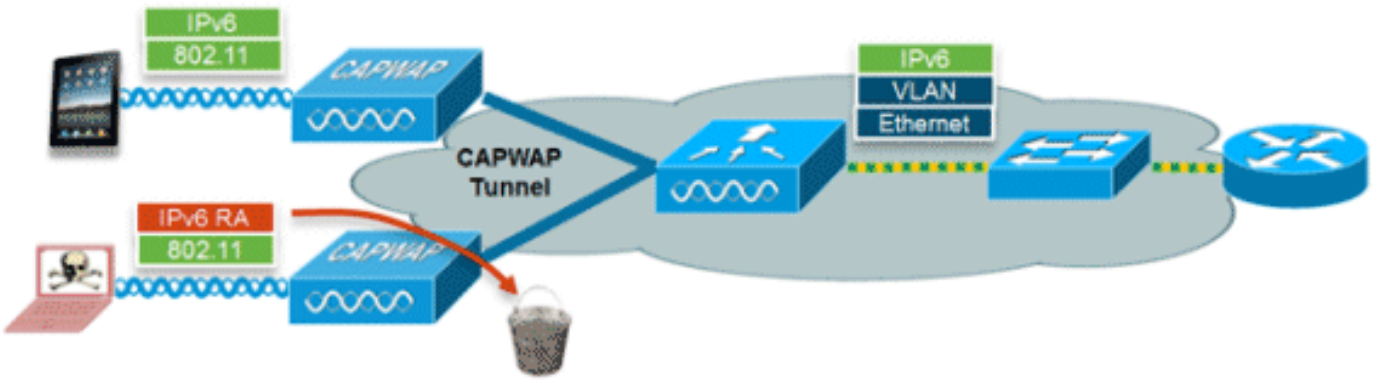
Compatibilidad con VLAN Select (grupos de interfaces)



La función de grupos de interfaz permite que una organización tenga una sola WLAN con varias VLAN configuradas en el controlador para permitir el balanceo de carga de clientes inalámbricos a través de estas VLAN. Esta función se utiliza normalmente para mantener pequeños los tamaños de subred de IPv4 al tiempo que permite que una WLAN se amplíe a miles de usuarios a través de varias VLAN en el grupo. Para admitir clientes IPv6 con grupos de interfaz, no se requiere ninguna configuración adicional, ya que el sistema envía automáticamente el RA correcto a los clientes correctos a través de unidifusión inalámbrica L2. Al unidifusión del RA, los clientes en la misma WLAN, pero en una VLAN diferente, no reciben el RA incorrecto.

Seguridad First Hop para clientes IPv6

Router Advertisement Guard



La función RA Guard aumenta la seguridad de la red IPv6 al descartar los RA procedentes de clientes inalámbricos. Sin esta función, los clientes IPv6 malintencionados o mal configurados podrían anunciarse como routers para la red, a menudo con una prioridad alta que podría tener prioridad sobre los routers IPv6 legítimos.

De forma predeterminada, RA Guard está habilitado en el AP (pero se puede inhabilitar en el AP) y siempre está habilitado en el controlador. Se prefiere descartar RA en el AP ya que es una solución más escalable y proporciona contadores de caídas de RA por cliente mejorados. En todos los casos, el RA IPv6 se descartará en algún momento, lo que protegerá a otros clientes inalámbricos y a la red por cable ascendente de clientes IPv6 malintencionados o mal configurados.

Protección del servidor DHCPv6

La función DHCPv6 Server Guard evita que los clientes inalámbricos entreguen direcciones IPv6 a otros clientes inalámbricos o clientes con cables en sentido ascendente. Para evitar que se distribuyan direcciones DHCPv6, se descartan todos los paquetes de anuncios DHCPv6 de los clientes inalámbricos. Esta función funciona en el controlador, no requiere configuración y se habilita automáticamente.

Protector de origen IPv6

La función IPv6 Source Guard evita que un cliente inalámbrico falsifique una dirección IPv6 de otro cliente. Esta función es análoga a IPv4 Source Guard. La protección de origen IPv6 está activada de forma predeterminada, pero se puede desactivar mediante la CLI.

Contabilización de direcciones IPv6

Para la autenticación y contabilización RADIUS, el controlador devuelve una dirección IP usando el atributo "Framed-IP-address". En este caso se utiliza la dirección IPv4.

El atributo "Calling-Station-ID" utiliza este algoritmo para devolver una dirección IP cuando el "Call Station ID Type" en el controlador está configurado en "IP Address":

1. Dirección IPv4
2. Dirección IPv6 de unidifusión global
3. Vincular dirección IPv6 local

Dado que las direcciones IPv6 del cliente pueden cambiar con frecuencia (direcciones temporales o privadas), es importante realizar un seguimiento de ellas a lo largo del tiempo. Cisco NCS registra todas las direcciones IPv6 que utiliza cada cliente y las registra históricamente cada vez que el cliente se desplaza o establece una nueva sesión. Estos registros se pueden configurar en NCS para que se conserven durante un máximo de un año.

Nota: El valor predeterminado para el "Tipo de ID de estación de llamada" en el controlador se ha cambiado a "Dirección MAC del sistema" en la versión 7.2. Al actualizar, esto debe cambiarse para permitir el seguimiento único de los clientes por dirección MAC, ya que las direcciones IPv6 pueden cambiar a mitad de la sesión y causar problemas en la contabilidad si el ID de la estación de llamada se establece en dirección IP.

Listas de control de acceso IPv6

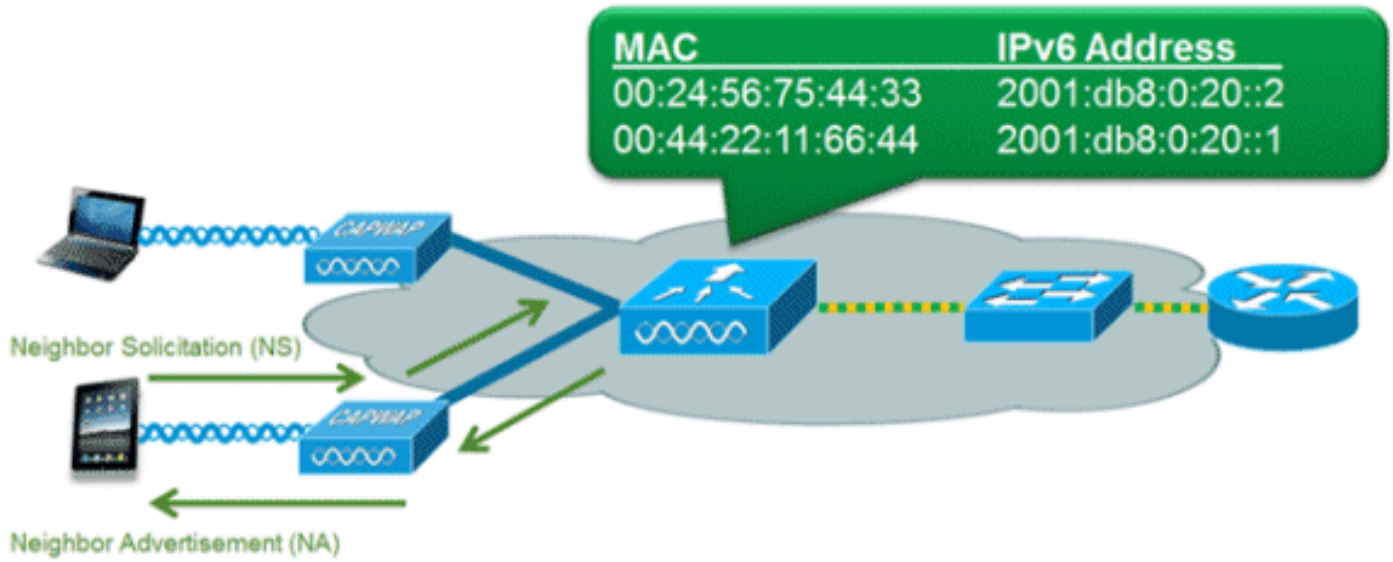
Para restringir el acceso a determinados recursos por cable ascendentes o bloquear determinadas aplicaciones, se pueden utilizar listas de control de acceso (ACL) IPv6 para identificar el tráfico y permitirlo o denegarlo. Las ACL IPv6 admiten las mismas opciones que las ACL IPv4, incluidos el origen, el destino, el puerto de origen y el puerto de destino (también se admiten los intervalos de puertos). Las ACL de autenticación previa también son compatibles con la autenticación de invitado IPv6 mediante un servidor web externo. El controlador inalámbrico admite hasta 64 ACL IPv6 únicas con 64 reglas únicas en cada una. El controlador inalámbrico sigue admitiendo 64 ACL IPv4 únicas adicionales con 64 reglas únicas en cada una para un total de 128 ACL para un cliente de doble pila.

Anulación de AAA para ACL IPv6

Para admitir el control de acceso centralizado a través de un servidor AAA centralizado, como Cisco Identity Services Engine (ISE) o ACS, la ACL IPv6 se puede aprovisionar por cliente mediante atributos de anulación de AAA. Para utilizar esta función, la ACL IPv6 se debe configurar en el controlador y la WLAN se debe configurar con la función AAA Override habilitada. El atributo AAA con nombre real para una ACL IPv6 es ***Airespace-IPv6-ACL-Name*** , similar al atributo *Airespace-ACL-Name* utilizado para aprovisionar una ACL basada en IPv4. El atributo AAA devuelto content debe ser una cadena de caracteres igual al nombre de la ACL IPv6 configurada en el controlador.

Optimización de paquetes para clientes IPv6

Caché de detección de vecino



El protocolo de detección de vecinos (NDP) IPv6 utiliza paquetes NA y NS en lugar del protocolo de resolución de direcciones (ARP) para permitir que los clientes IPv6 resuelvan la dirección MAC de otros clientes de la red. El proceso NDP puede ser muy hablador, ya que utiliza inicialmente direcciones multicast para realizar la resolución de direcciones; esto puede consumir un valioso tiempo de transmisión inalámbrica, ya que los paquetes multicast se envían a todos los clientes en el segmento de red.

Para aumentar la eficiencia del proceso NDP, el almacenamiento en caché de detección de vecinos permite que el controlador actúe como proxy y responda a las consultas NS que puede resolver. El almacenamiento en caché de detección de vecinos es posible gracias a la tabla de

enlace de vecinos subyacente presente en el controlador. La tabla de enlace de vecinos realiza un seguimiento de cada dirección IPv6 y su dirección MAC asociada. Cuando un cliente IPv6 intenta resolver la dirección de la capa de link de otro cliente, el controlador intercepta el paquete NS, que responde con un paquete NA.

Regulación de anuncio de router

La aceleración de anuncio de router permite que el controlador aplique el límite de velocidad de los RA que se dirigen hacia la red inalámbrica. Al habilitar la regulación de RA, los routers configurados para enviar RA con mucha frecuencia (por ejemplo, cada tres segundos) pueden reducirse a una frecuencia mínima que mantendrá la conectividad de cliente IPv6. Esto permite optimizar el tiempo de transmisión al reducir el número de paquetes de multidifusión que se deben enviar. En todos los casos, si un cliente envía un RS, se permitirá un RA a través del controlador y unidifusión al cliente solicitante. Esto es para asegurarse de que los nuevos clientes o clientes de roaming no se vean afectados negativamente por la limitación de RA.

Acceso de invitado IPv6

Las funciones de invitado por cable e inalámbricas presentes para los clientes IPv4 funcionan de la misma manera para los clientes de pila doble y los clientes solo IPv6. Una vez que el usuario invitado se asocia, se colocan en un estado de ejecución "WEB_AUTH_REQ" hasta que el cliente se autentica a través del portal cautivo IPv4 o IPv6. El controlador interceptará el tráfico HTTP/HTTPS IPv4 e IPv6 en este estado y lo redirigirá a la dirección IP virtual del controlador. Una vez que el usuario se autentica a través del portal cautivo, su dirección MAC se mueve al estado de ejecución y se permite el paso del tráfico IPv4 e IPv6. Para la autenticación web externa, la ACL de autenticación previa permite utilizar un servidor web externo.

Para admitir la redirección de clientes solo de IPv6, el controlador crea automáticamente una dirección virtual de IPv6 basada en la dirección virtual de IPv4 configurada en el controlador. La dirección IPv6 virtual sigue la convención de `[::ffff:<dirección IPv4 virtual>]`. Por ejemplo, una dirección IP virtual de 1.1.1.1 se traduciría a `[::ffff:1.1.1.1]`.

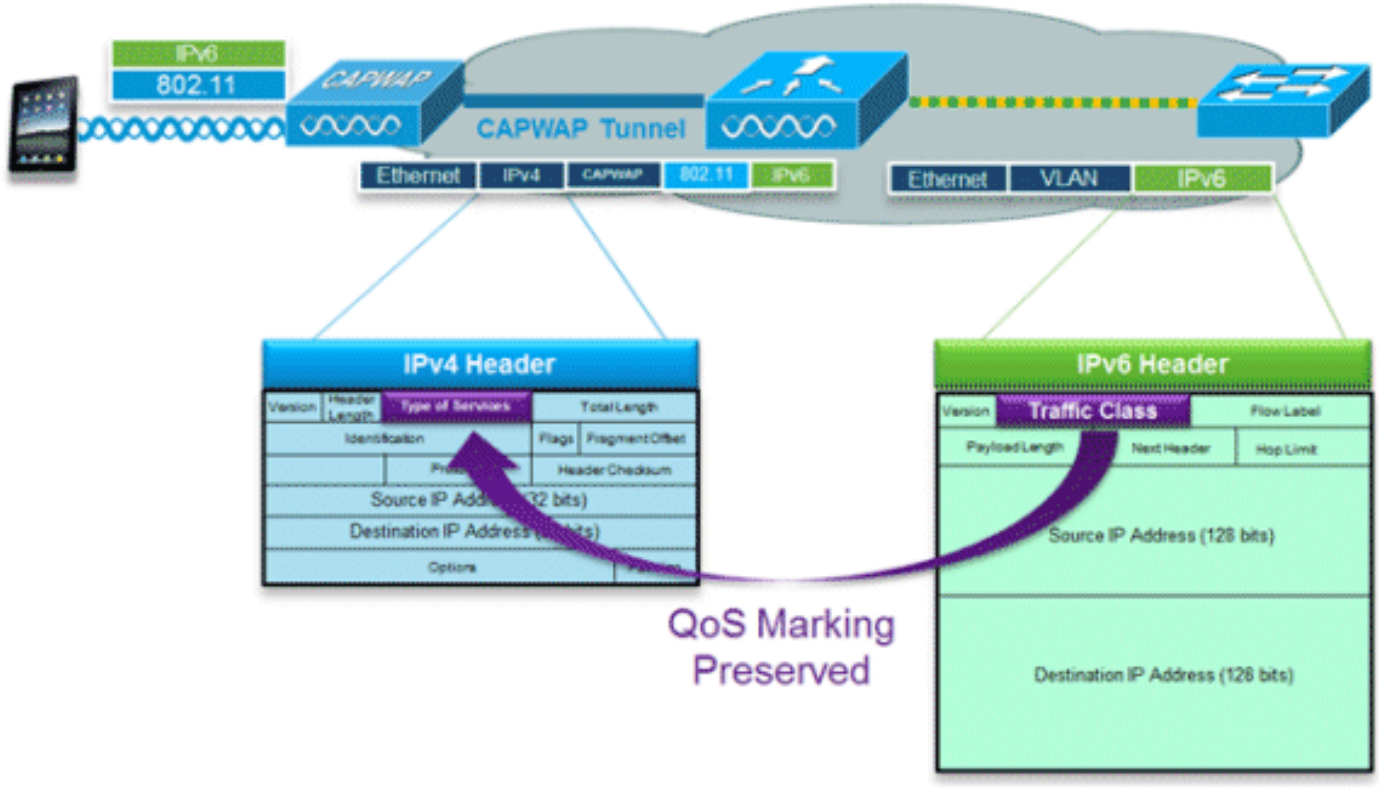
Cuando utilice un certificado SSL de confianza para la autenticación de acceso de invitado, asegúrese de que la dirección virtual IPv4 e IPv6 del controlador esté definida en DNS para que coincida con el nombre de host de los certificados SSL. Esto garantiza que los clientes no reciban una advertencia de seguridad que indique que el certificado no coincide con el nombre de host del dispositivo.

Nota: El certificado SSL generado automáticamente del controlador no contiene la dirección virtual IPv6. Esto puede hacer que algunos navegadores web presenten una advertencia de seguridad. Se recomienda utilizar un certificado SSL de confianza para el acceso de invitados.

VideoStream IPv6

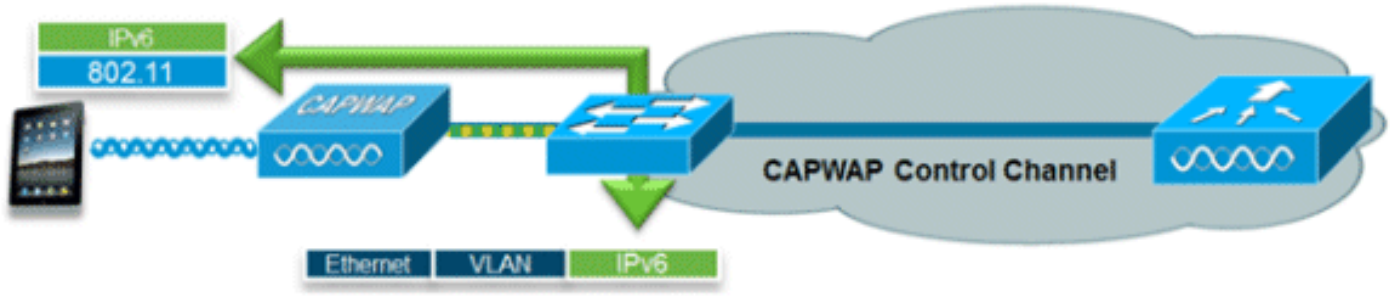
VideoStream permite la entrega de vídeo multidifusión inalámbrico fiable y escalable, enviando a cada cliente la secuencia en un formato de unidifusión. La conversión real de multidifusión a unidifusión (de L2) se produce en el punto de acceso, lo que proporciona una solución escalable. El controlador envía el tráfico de vídeo IPv6 dentro de un túnel de multidifusión CAPWAP IPv4 que permite una distribución de red eficiente al AP.

Calidad de servicio IPv6



Los paquetes IPv6 utilizan un marcado similar al uso que hace IPv4 de los valores DSCP que admiten hasta 64 clases de tráfico diferentes (0-63). Para los paquetes descendentes de la red con cables, el valor de Clase de tráfico IPv6 se copia en el encabezado del túnel CAPWAP para garantizar que QoS se conserve de extremo a extremo. En la dirección ascendente, ocurre lo mismo ya que el tráfico del cliente marcado en la Capa 3 con la clase de tráfico IPv6 se cumplirá al marcar los paquetes CAPWAP destinados al controlador.

IPv6 y FlexConnect



FlexConnect: WLAN de switching local

FlexConnect en el modo de switching local admite clientes IPv6 mediante la conexión en puente del tráfico a la VLAN local, de forma similar al funcionamiento de IPv4. La movilidad del cliente es compatible con el roaming de capa 2 en el grupo FlexConnect.

Estas funciones específicas de IPv6 son compatibles con el modo de switching local de FlexConnect:

- Protección IPv6 RA
- Puente IPv6
- Autenticación de invitado IPv6 (alojada en controlador)

Estas funciones específicas de IPv6 no se admiten en el modo de switching local de FlexConnect:

- Movilidad de capa 3
- VideoStream IPv6
- Listas de control de acceso IPv6
- Protector de origen IPv6
- Protección del servidor DHCPv6
- Caché de detección de vecino
- Regulación de anuncio de router

FlexConnect: WLAN de switching central

En el caso de los AP en modo FlexConnect que utilizan switching central (tunelización del tráfico de vuelta al controlador), el controlador debe configurarse en "Multicast - Unicast Mode" (Multidifusión - Modo unidifusión) para el "AP Multicast Mode" (Modo multidifusión de AP). Dado que los AP FlexConnect no se unen al grupo de multidifusión CAPWAP del controlador, los paquetes de multidifusión deben replicarse en el controlador y unidifusión en cada AP individualmente. Este método es menos eficiente que "Multicast - Multicast Mode" y coloca carga adicional en el controlador.

Esta función específica de IPv6 no se admite en el modo de switching central de FlexConnect:

- VideoStream IPv6

Nota: Las WLAN conmutadas centralmente que ejecutan IPv6 no son compatibles con el controlador Flex 7500 Series.

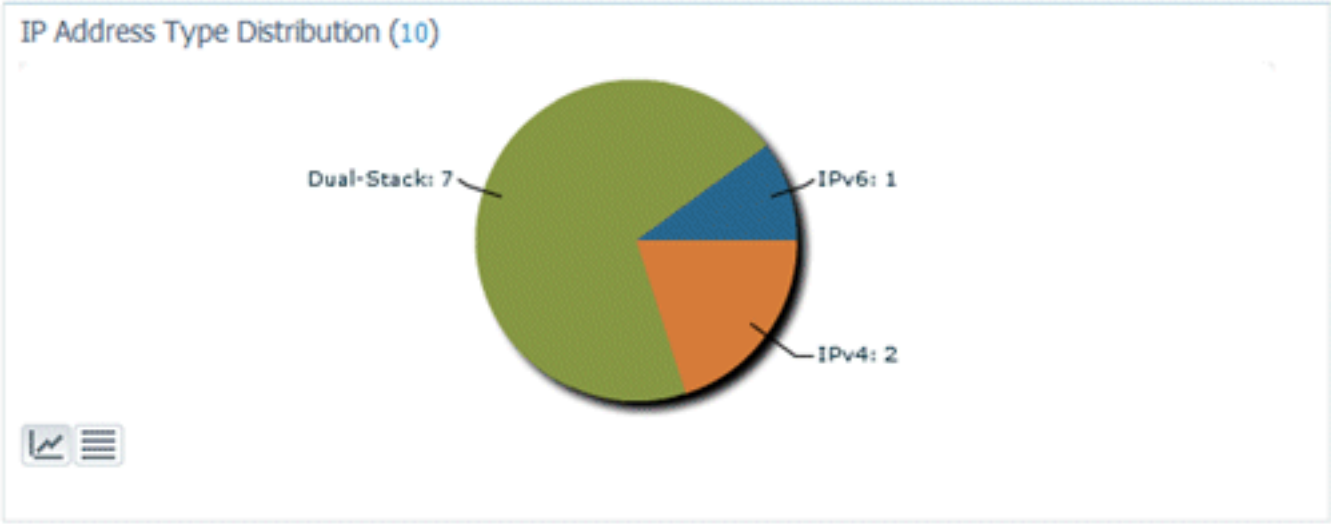
Visibilidad de clientes IPv6 con NCS

Con el lanzamiento de NCS v1.1, se han añadido muchas funciones adicionales específicas de IPv6 para supervisar y gestionar una red de clientes IPv6 en redes por cable e inalámbricas.

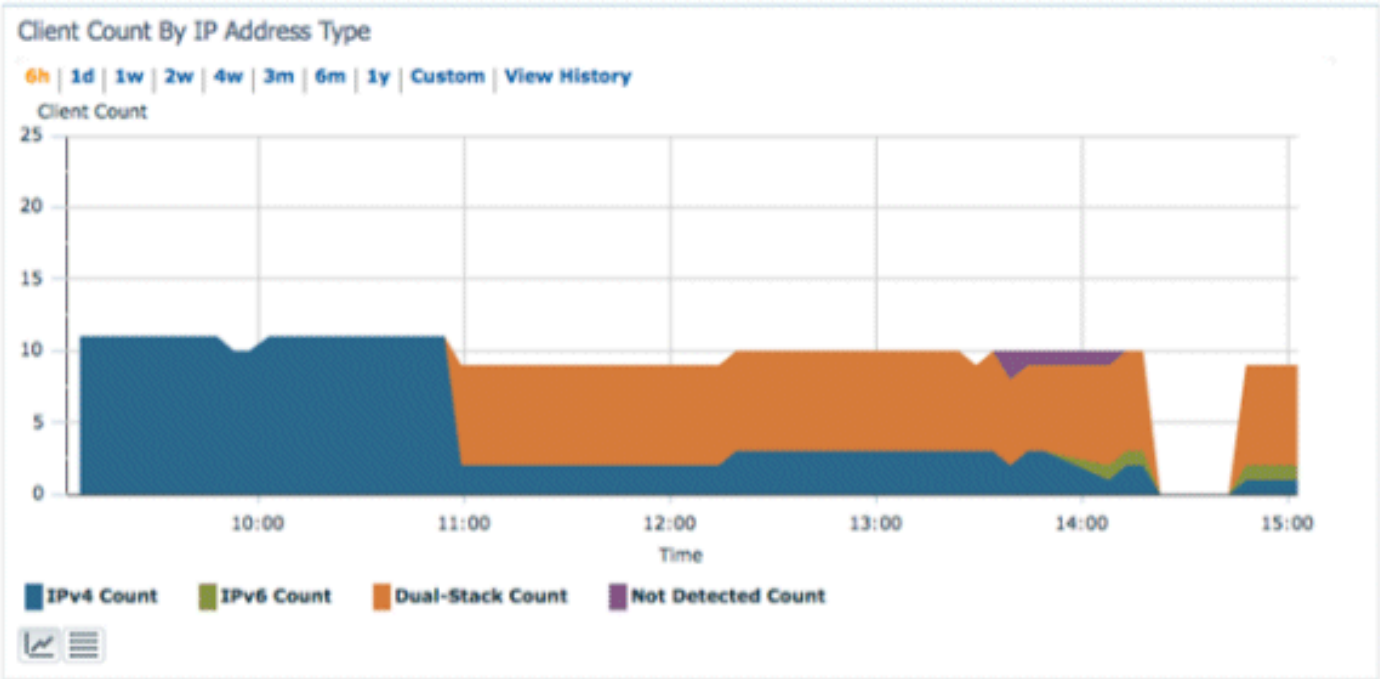
Elementos del panel de IPv6

Para ver qué tipos de clientes están presentes en la red, hay disponible un "Dashlet" en NCS para proporcionar información sobre estadísticas específicas de IPv6 y ofrecer la capacidad de profundizar en clientes IPv6.

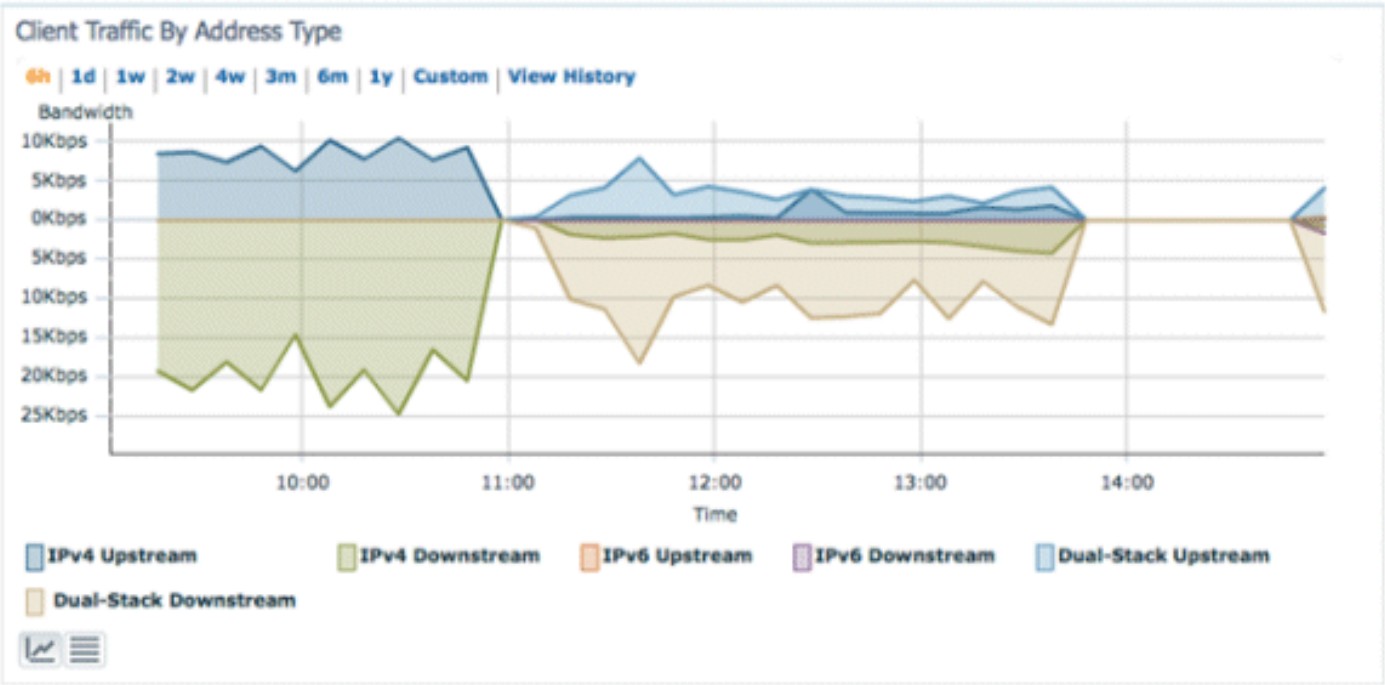
Dashlet de tipo de dirección IP - Muestra los tipos de clientes IP en la red:



Recuento de clientes por tipo de dirección IP: muestra el tipo de cliente IP a lo largo del tiempo:



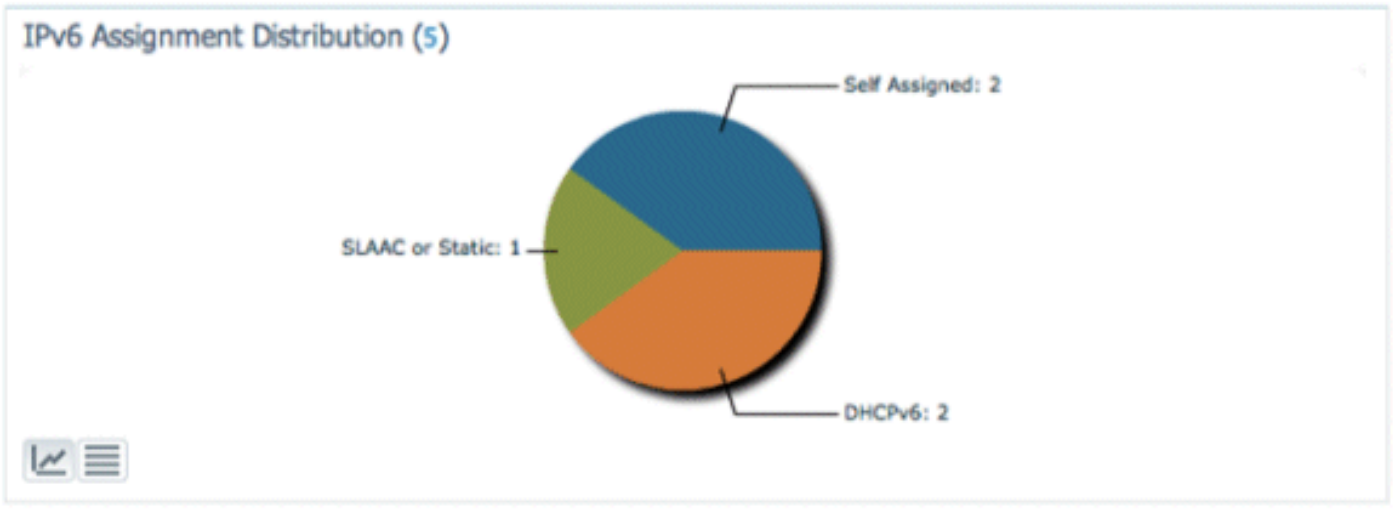
Tráfico del Cliente por Tipo de Dirección IP: Muestra el tráfico de cada tipo de cliente. Los clientes de la categoría de pila doble incluyen tráfico IPv4 e IPv6:



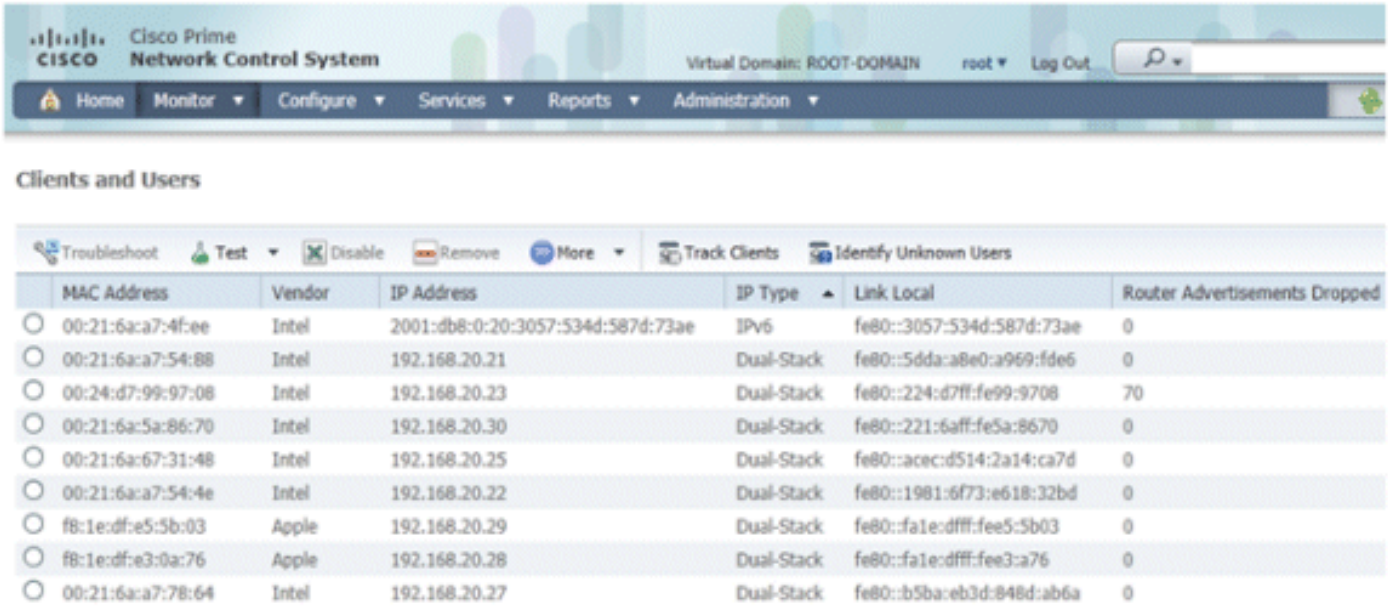
Asignación de dirección IPv6: muestra el método de asignación de dirección para cada cliente como una de estas cuatro categorías:

- DHCPv6: para clientes con direcciones asignadas por un servidor central. El cliente también puede tener una dirección SLAAC.
- SLAAC o Static: para clientes que utilizan la asignación automática de direcciones sin estado o que utilizan direcciones configuradas estáticamente.
- Desconocido: en algunos casos, no se puede detectar la asignación de direcciones IPv6.Esta condición solo ocurre en los clientes con cable en NCS, ya que algunos switches no buscan información de asignación de direcciones IPv6.
- Autoasignado: para clientes que sólo tienen una dirección local de vínculo totalmente autoasignada.Los clientes de esta categoría pueden tener problemas de conectividad IPv6, ya que carecen de una dirección única local o global.

Se puede hacer clic en cada una de las secciones del gráfico circular, lo que permite al administrador obtener detalles de una lista de clientes.

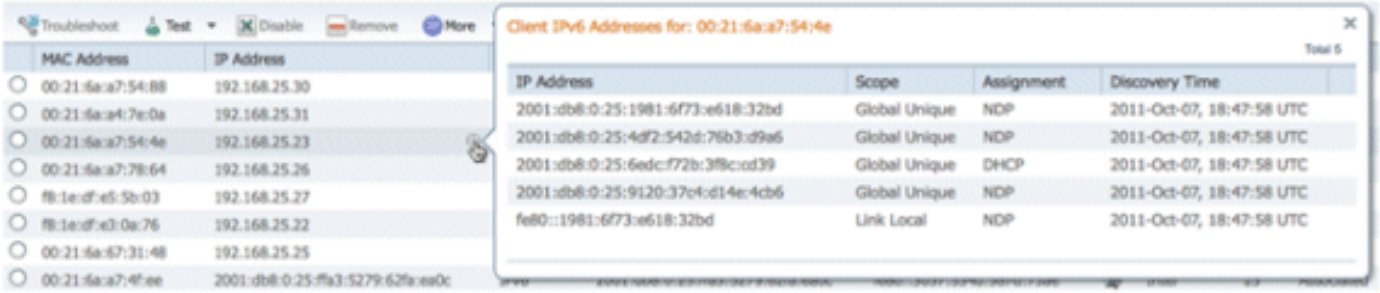


Supervisar clientes IPv6



Para supervisar y administrar la información del cliente IPv6, estas columnas se agregaron a la página Clientes y usuarios:

- Tipo de IP: tipo de cliente basado en las direcciones IP que se han visto desde el cliente. Las opciones posibles son IPv4, IPv6 o Dual-Stack, que significa un cliente con direcciones IPv4 e IPv6.
- Tipo de asignación IPv6: NCS detecta el método de asignación de direcciones como SLAAC o Static, DHCPv6, Self-Assigned o Unknown.
- Global Unique: dirección global IPv6 más reciente utilizada por el cliente. Al pasar el ratón por el contenido de la columna, se muestran las direcciones únicas globales de IPv6 adicionales que utiliza el cliente.
- Local Unique (Única local): Dirección única local IPv6 más reciente utilizada por el cliente. Al pasar el ratón por el contenido de la columna, se muestran las direcciones únicas globales IPv6 adicionales que utiliza el cliente.
- Link Local (Enlace local): Dirección IPv6 del cliente autoasignada y utilizada para la comunicación antes de asignar cualquier otra dirección IPv6.
- Anuncios de router descartados: el número de anuncios de router enviados por el cliente y descartados en el AP. Esta columna se puede utilizar para rastrear clientes que pueden estar mal configurados o maliciosamente configurados para actuar como un router IPv6. Esta columna se puede ordenar, lo que permite identificar fácilmente a los clientes infractores.

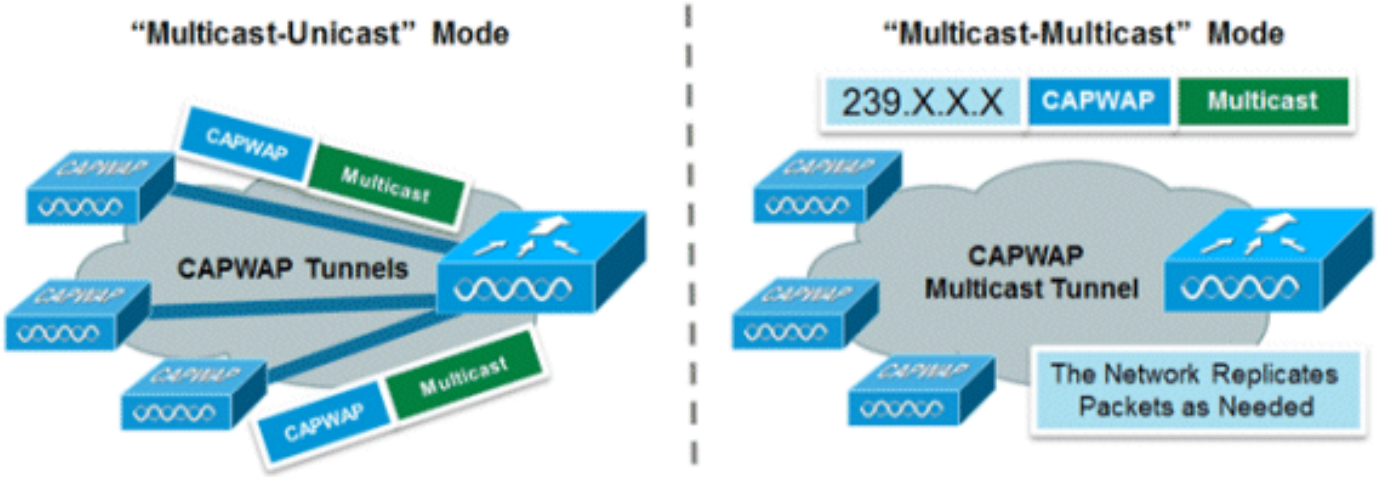


Además de mostrar columnas específicas de IPv6, la columna Dirección IP mostrará la dirección IP actual del cliente con una prioridad para mostrar primero la dirección IPv4 (en el caso de un cliente de doble pila) o la dirección IPv6 Global Unique en el caso de un cliente solo de IPv6.

Configuración de Wireless IPv6 Client Support

Modo de distribución de multidifusión a AP

Cisco Unified Wireless Network admite dos métodos de distribución multidifusión a los puntos de acceso asociados al controlador. En ambos modos, el paquete multicast original de la red cableada se encapsula dentro de un paquete CAPWAP de Capa 3 enviado a través de la unidifusión CAPWAP o la multidifusión al AP. Dado que el tráfico es encapsulado CAPWAP, los AP no tienen que estar en la misma VLAN que el tráfico del cliente. Aquí se comparan los dos métodos de distribución multidifusión:



	Modo multidifusión-unidifusión	Modo multidifusión-multidifusión
Mecanismo de entrega	El controlador replica el paquete de multidifusión y lo envía a cada AP en un túnel CAPWAP de unidifusión	El controlador envía una copia del paquete de multidifusión
Modos de AP admitidos	FlexConnect y local	Sólo modo local
Requiere routing multidifusión de capa 3 en redes con cables	No	Yes
Carga del controlador	Alto	Bajo
Carga de red con cables	Alto	Bajo

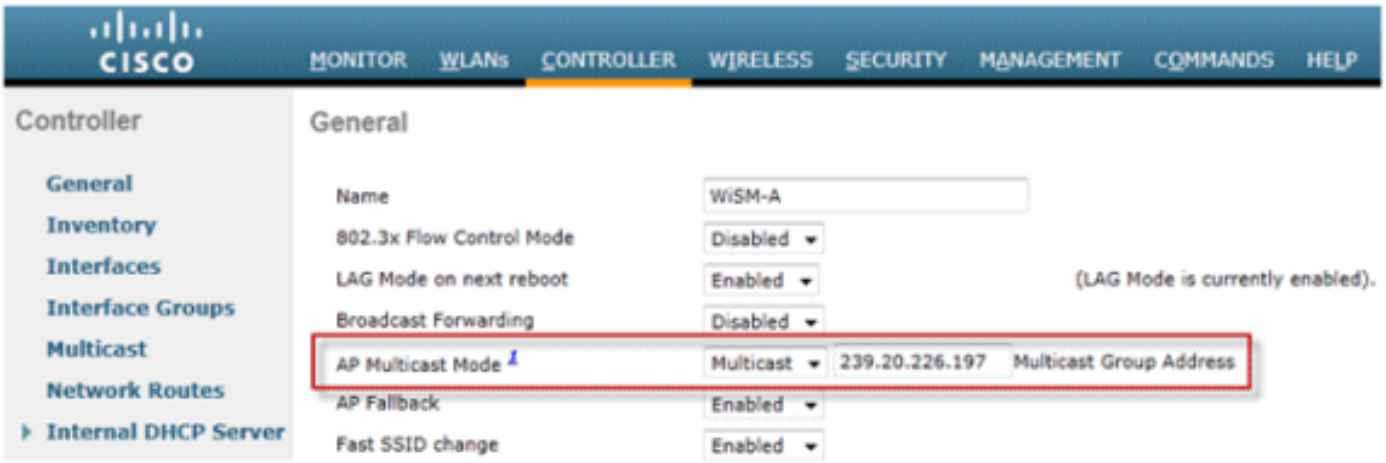
Configuración del modo de distribución multidifusión-multidifusión

El modo multidifusión-multidifusión es la opción recomendada por motivos de escalabilidad y eficacia del ancho de banda por cable.

Nota: Este paso solo es absolutamente necesario para el controlador inalámbrico de la serie 2500, pero permite una transmisión multidifusión más eficiente y se recomienda para todas las

plataformas de controlador.

Vaya a la pestaña "Controlador" debajo de la página "General" y asegúrese de que el Modo Multicast AP esté configurado para utilizar el modo **Multicast** y que se haya configurado una dirección de grupo válida. La dirección de grupo es un grupo de multidifusión IPv4 y se recomienda que se encuentre en el rango 239.X.X.X-239.255.255.255, que está definido para aplicaciones de multidifusión privadas.

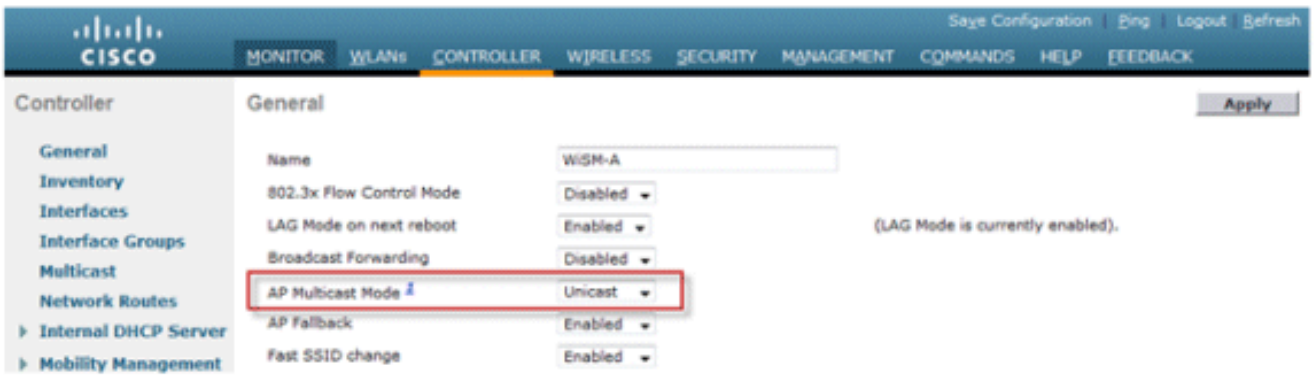


Nota: No utilice los rangos de direcciones 224.X.X.X, 239.0.0.X o 239.128.0.X para la dirección del grupo multicast. Las direcciones de estos rangos se superponen con las direcciones MAC locales del link e inundan todos los puertos del switch, incluso con la indagación IGMP habilitada.

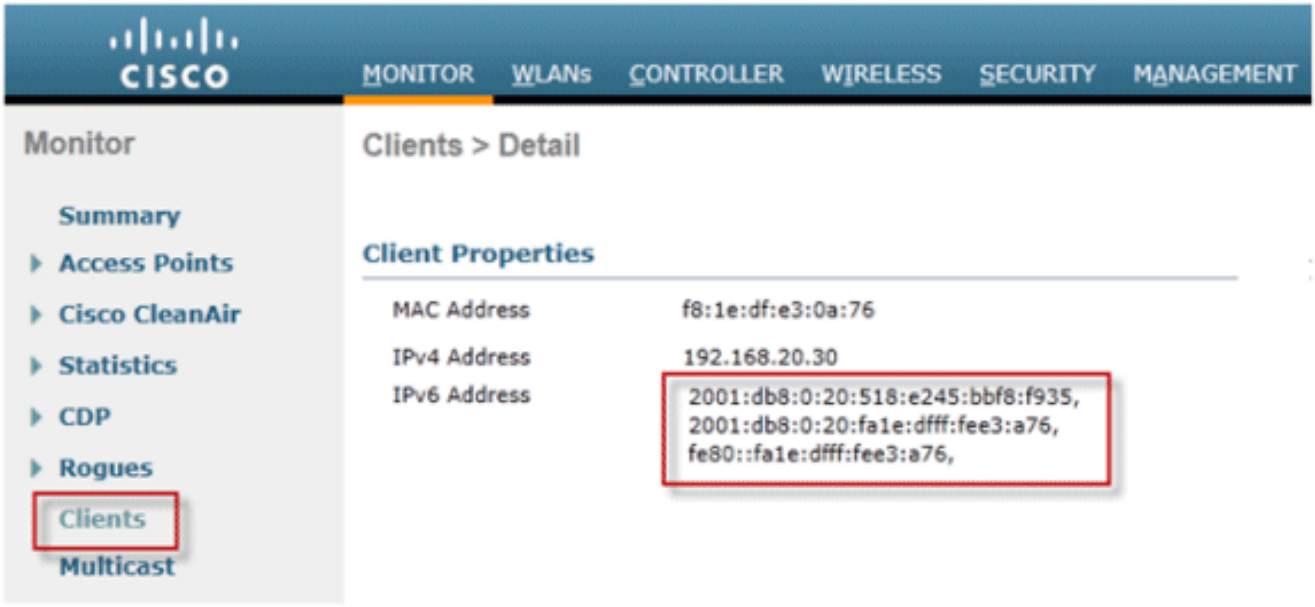
Configuración del modo de distribución multidifusión-unidifusión

Si la red cableada no está configurada correctamente para ofrecer la multidifusión CAPWAP entre el controlador y el modo AP o FlexConnect, y los AP se utilizarán para las WLAN conmutadas centralmente que admiten IPv6, se requiere el modo de unidifusión.

1. Vaya a la pestaña **Controlador** bajo la página General, y asegúrese de que el Modo Multicast AP esté configurado para utilizar el modo **Unicast**.



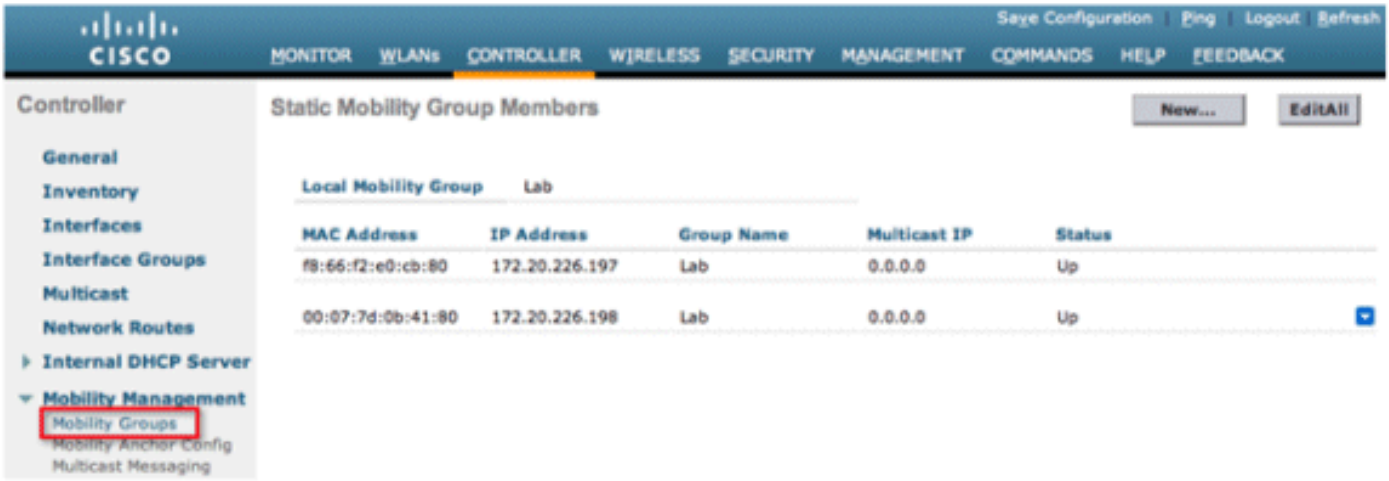
2. Conecte un cliente compatible con IPv6 a la red LAN inalámbrica. Valide que el cliente reciba una dirección IPv6 desplazándose a la ficha **Monitor** y, a continuación, al menú **Clientes**.



Configuración de la movilidad IPv6

No existe ninguna configuración específica para la movilidad IPv6, excepto colocar los controladores en el mismo grupo de movilidad o en el mismo dominio de movilidad. Esto permite que un total de 72 controladores participen en un dominio de movilidad, lo que proporciona una movilidad perfecta incluso para los campus más grandes.

Vaya a la ficha **Controlador > Grupos de movilidad**, y agregue cada controlador por dirección MAC e IP al grupo. Esto debe hacerse en todos los controladores del grupo de movilidad.



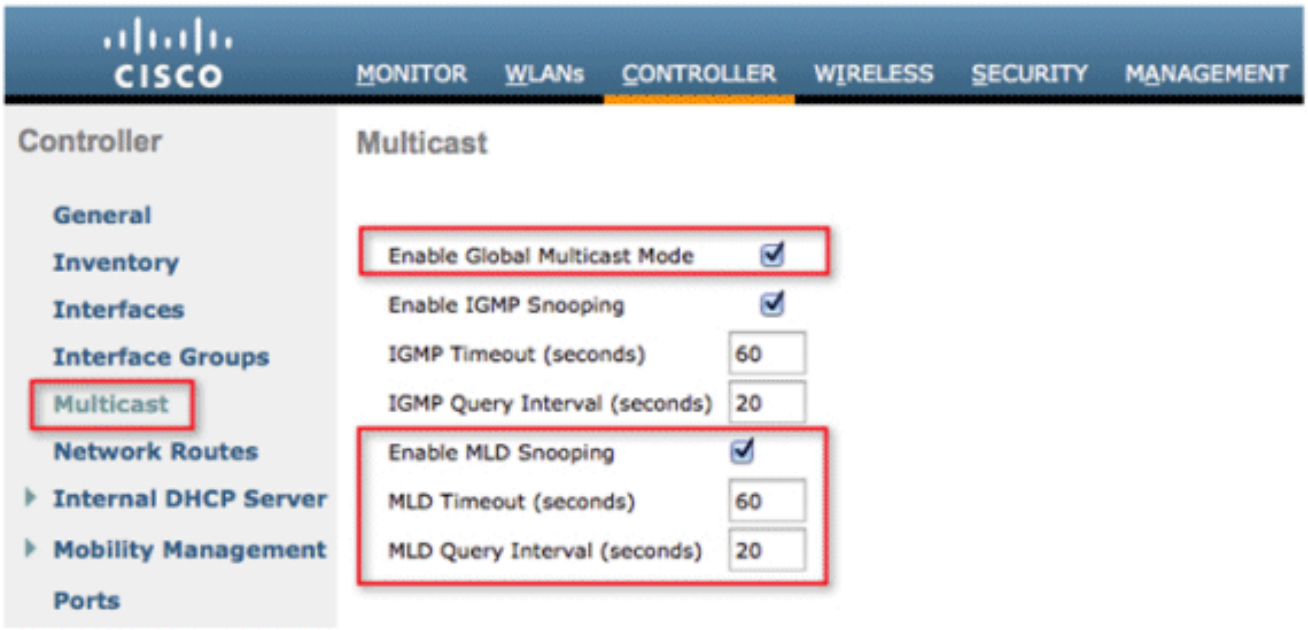
Configuración de multidifusión IPv6

El controlador admite la indagación MLDv1 para multidifusión IPv6, lo que le permite realizar un seguimiento inteligente de los flujos de multidifusión y entregarlos a los clientes que los soliciten.

Nota: A diferencia de las versiones anteriores de las versiones, la compatibilidad con el tráfico unidifusión IPv6 no exige que se active el "modo de multidifusión global" en el controlador. La compatibilidad con tráfico unidifusión IPv6 se habilita automáticamente.

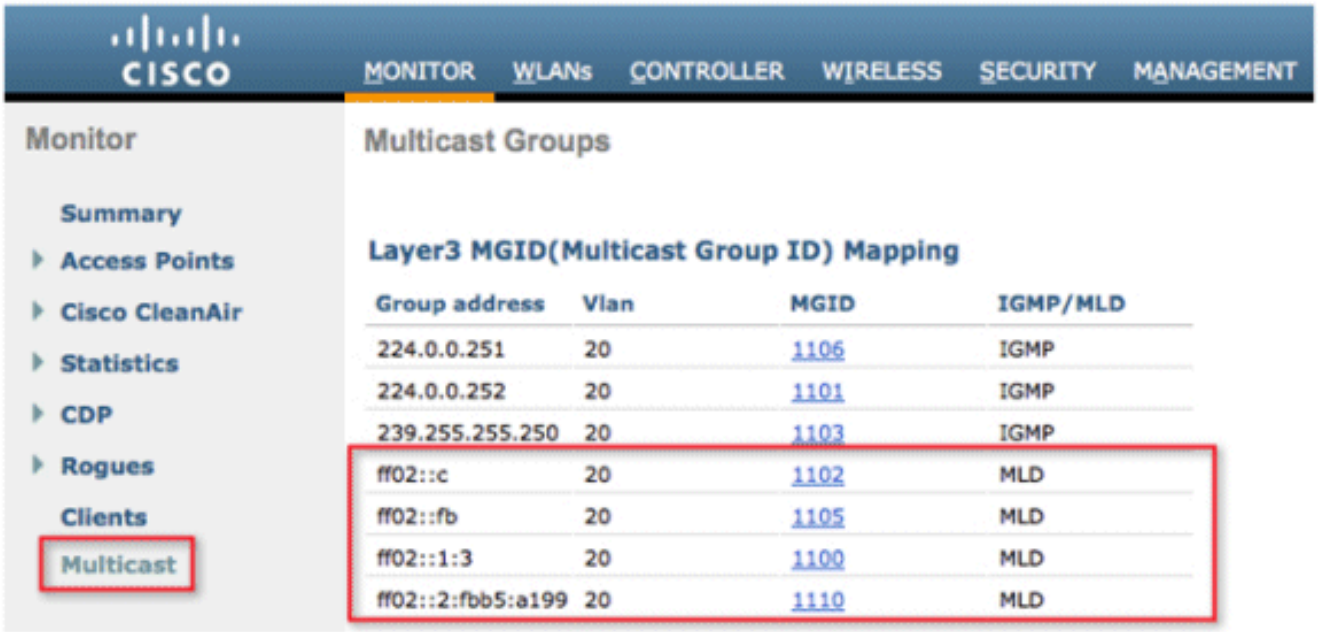
1. Vaya a la ficha **Controlador** > página **Multicast** y **Habilite la indagación MLD** para soportar el tráfico IPv6 multicast. Para habilitar la multidifusión IPv6, también debe habilitarse el **modo**

de multidifusión global del controlador.



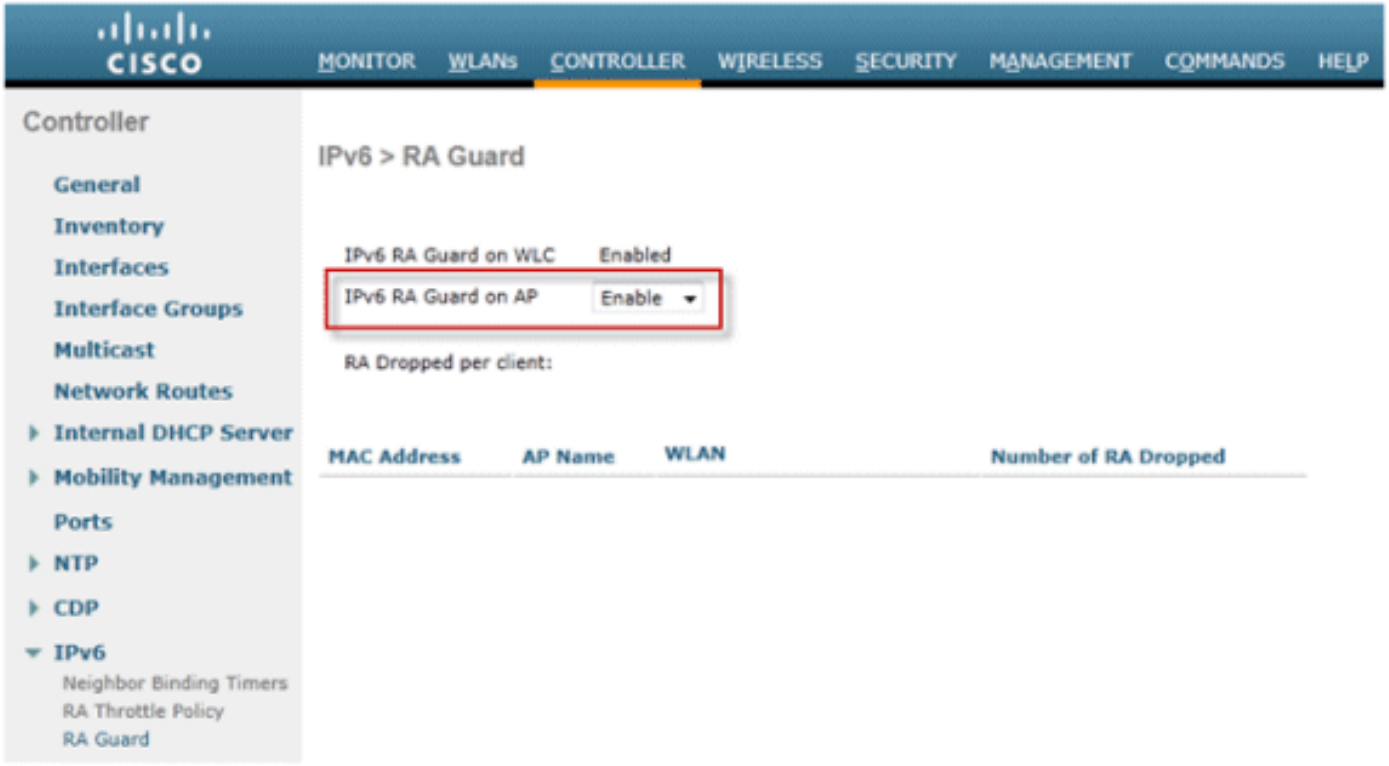
Nota: El modo de multidifusión global, IGMP y el snooping MLD deben activarse si se requieren aplicaciones de detección P2P, como Bonjour de Apple.

2. Para verificar que el tráfico multicast IPv6 está siendo rastreado, vaya a la pestaña **Monitor** y a la página **Multicast**. Observe que se enumeran los grupos de multidifusión IPv4 (IGMP) e IPv6 (MLD). Haga clic en MGID para ver los clientes inalámbricos unidos a esa dirección de grupo.



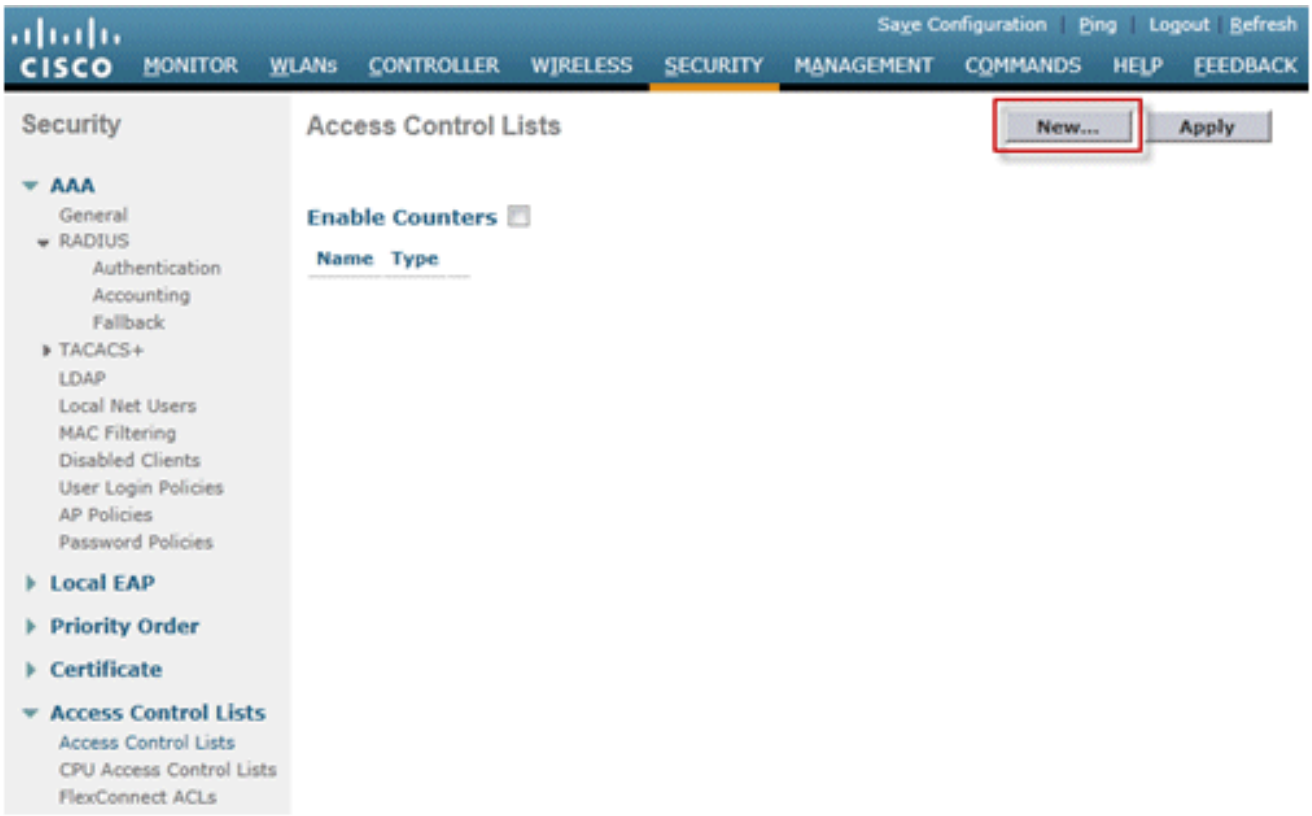
Configuración de IPv6 RA Guard

Vaya a la pestaña **Controlador** y luego a **IPv6 > RA Guard** en el menú de la izquierda. **Habilite** IPv6 RA Guard en AP. La protección de RA en el controlador no se puede inhabilitar. Además de la configuración de RA Guard, esta página también muestra cualquier cliente que haya sido identificado como el envío de RAs.



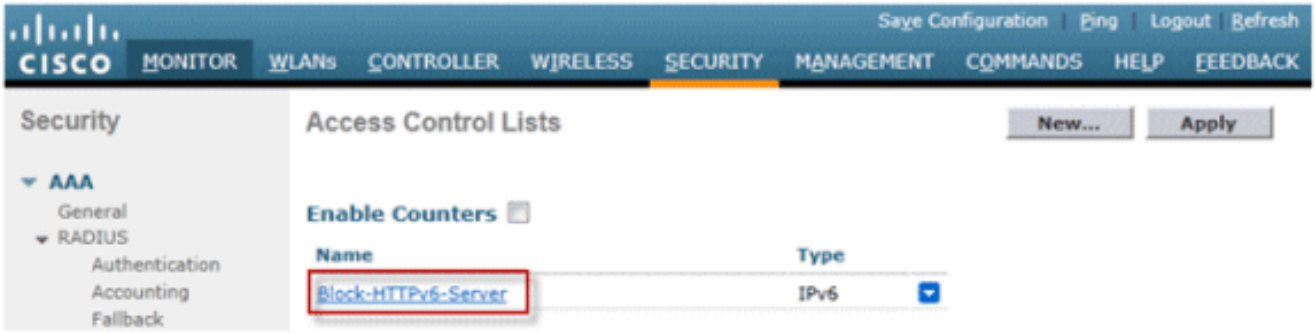
Configurar listas de control de acceso IPv6

1. Vaya a la pestaña **Seguridad**, abra **Listas de control de acceso** y haga clic en **Nuevo**.

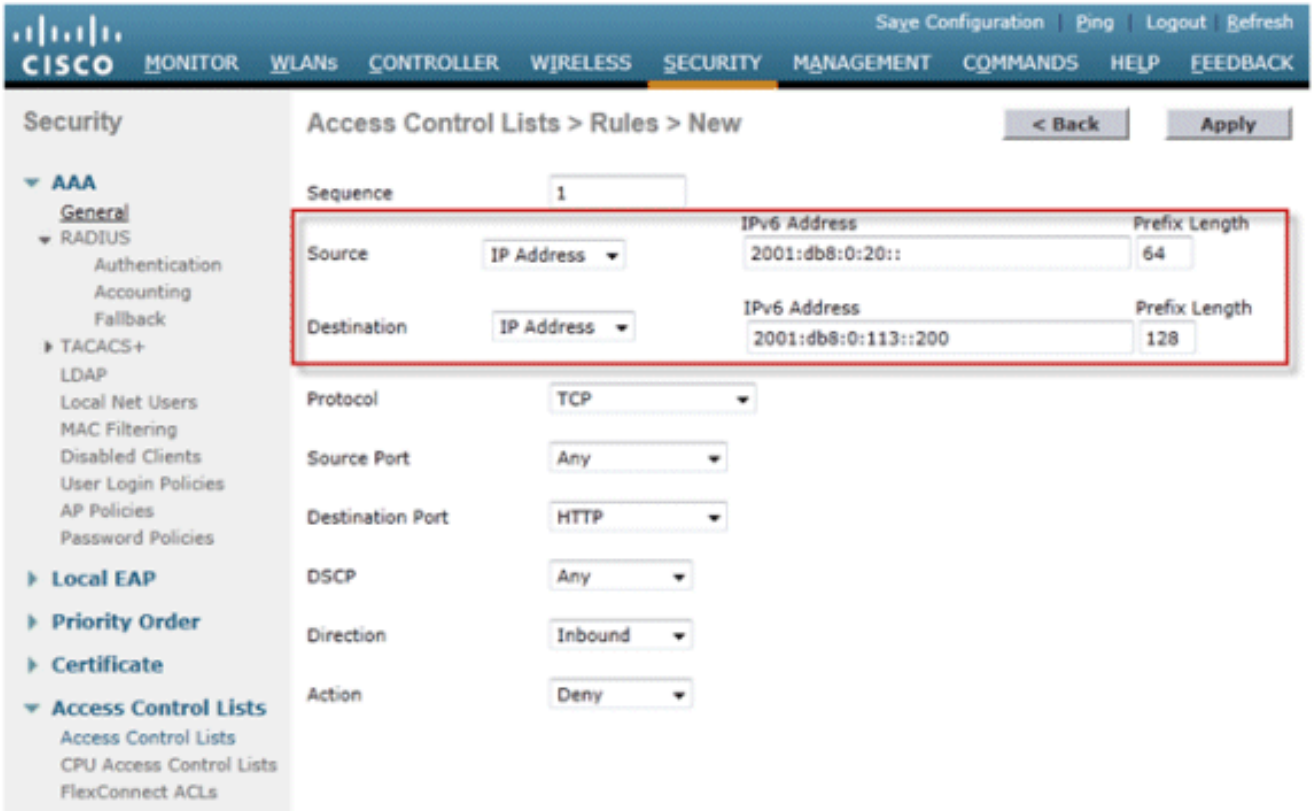


2. Introduzca un nombre único para la ACL, cambie el tipo de ACL a **IPv6** y haga clic en **Apply**.

3. Haga clic en la nueva ACL que se creó en los pasos anteriores.

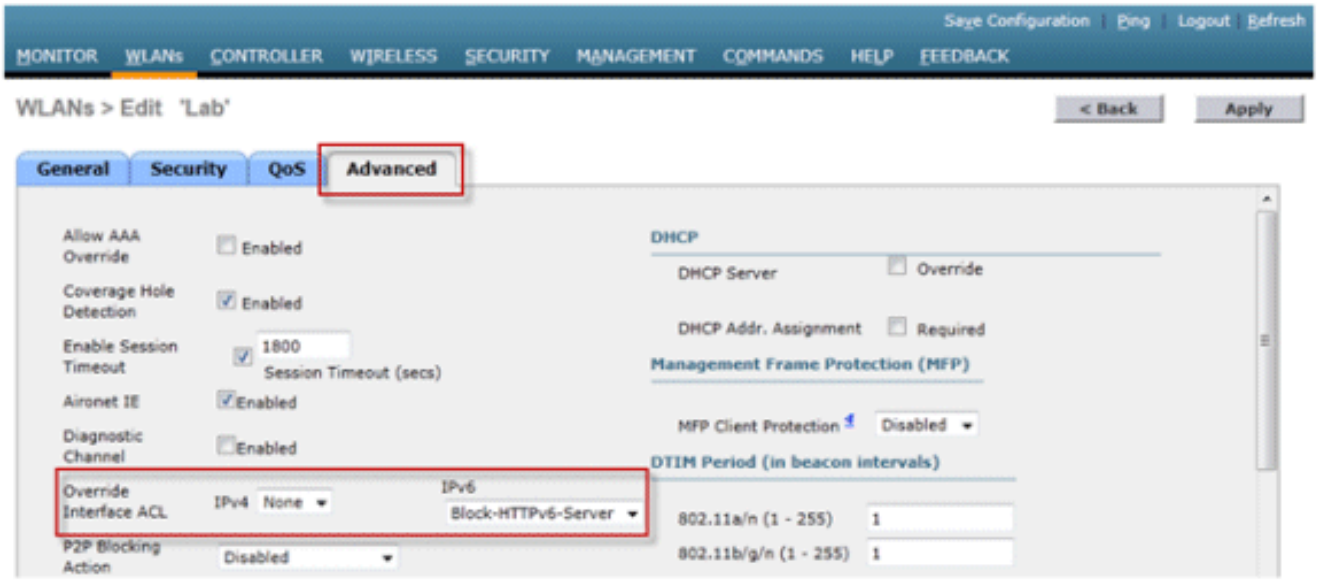


4. Haga clic en **Add New Rule**, ingrese los parámetros deseados para la regla y haga clic en **Apply**. Deje el número de secuencia en blanco para colocar la regla al final de la lista. La opción "Direction" (Dirección) de "Inbound" (Entrante) se utiliza para el tráfico procedente de la red inalámbrica y "Outbound" (Saliente) para el tráfico destinado a los clientes inalámbricos. Recuerde que la última regla en una ACL es una negación de todo implícita. Utilice una longitud de prefijo de 64 para coincidir con una subred IPv6 completa, y una longitud de prefijo de 128 para restringir de forma exclusiva el acceso a una dirección individual.



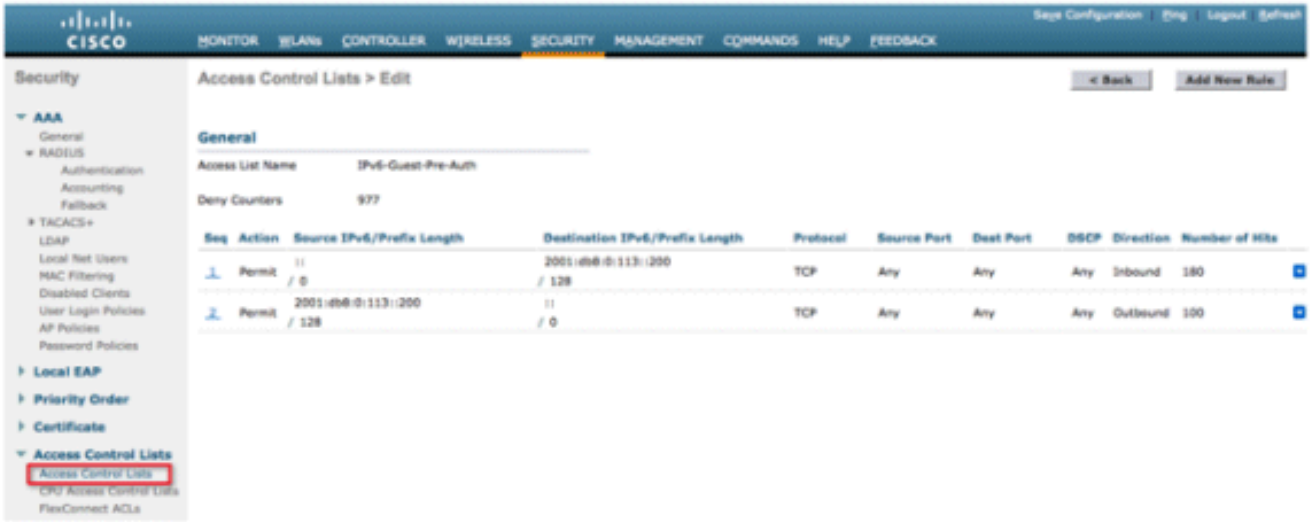
5. Las ACL IPv6 se aplican por WLAN/SSID y se pueden utilizar en varias WLAN de forma simultánea. Navegue hasta la pestaña **WLANs** y haga clic en el ID de WLAN del SSID en

cuestión para aplicar la ACL IPv6. Haga clic en la pestaña **Advanced** y cambie la ACL de interfaz de anulación para IPv6 por el nombre de
ACL.

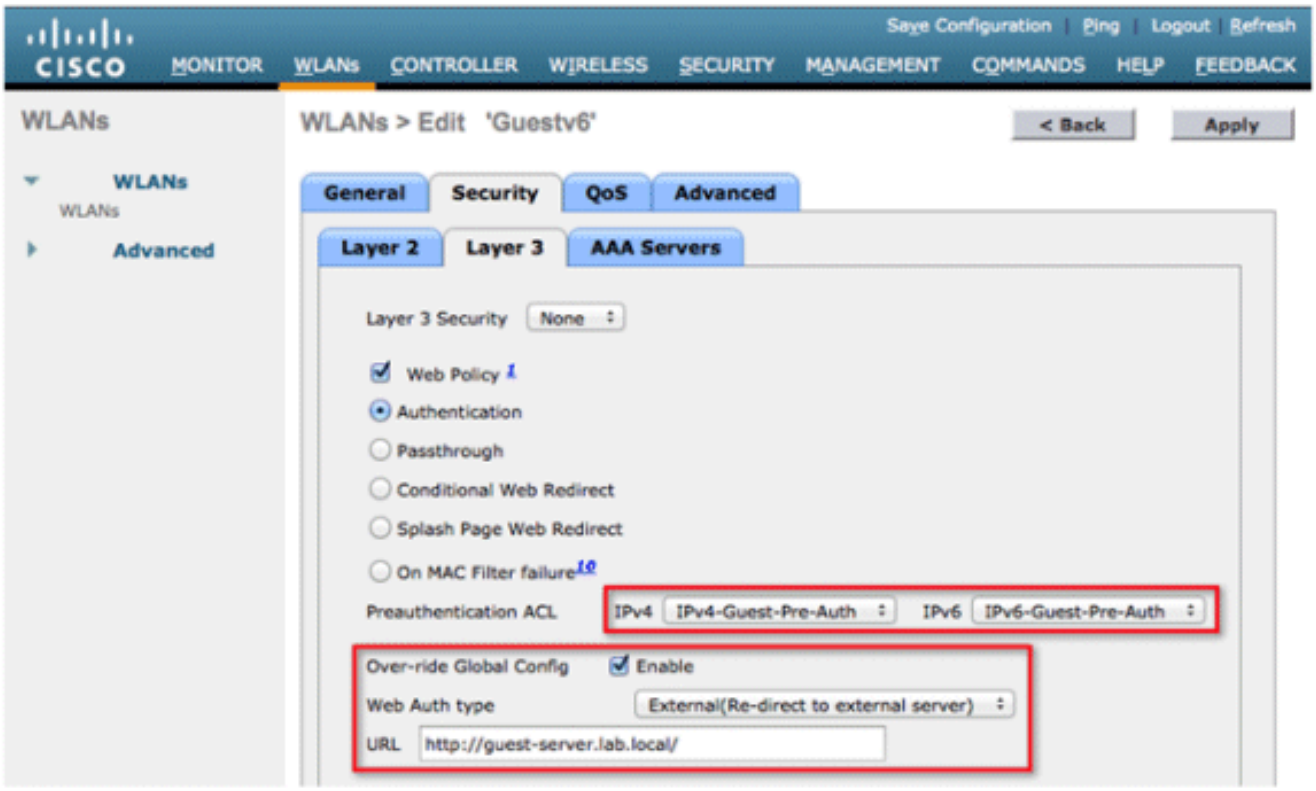


Configurar el acceso de invitado IPv6 para la autenticación Web externa

1. Configure la ACL de autenticación previa de IPv4 e IPv6 para el servidor web. Esto permite el tráfico hacia y desde el servidor externo antes de que el cliente se autentique completamente.

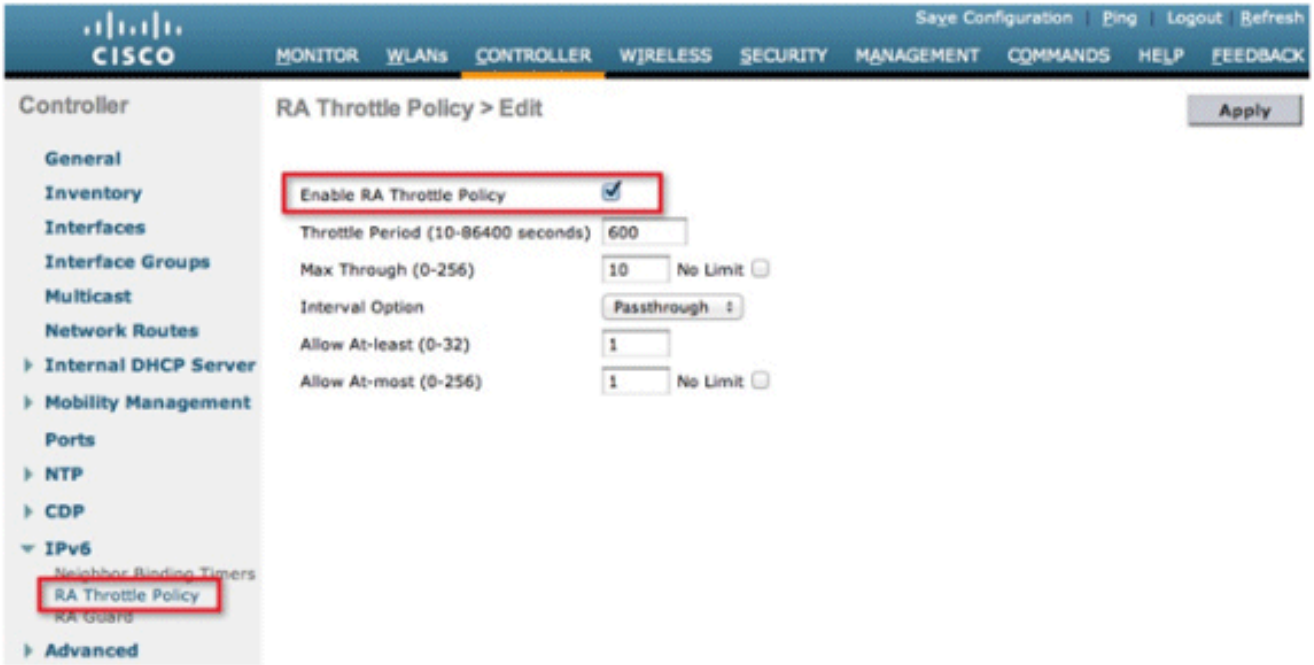


   Para obtener más información sobre el funcionamiento del acceso web externo, consulte Ejemplo de Configuración de Autenticación Web Externa con Controladores de LAN Inalámbrica.
2. Configure la WLAN de invitado navegando a la pestaña WLANs en la parte superior. Cree el SSID de invitado y utilice una política web de capa 3. Las ACL de autenticación previa definidas en el paso 1 se seleccionan para IPv4 e IPv6. Verifique la sección Override Global Config y seleccione **External** en el cuadro desplegable Web Auth type . Introduzca la URL del servidor Web. El nombre de host del servidor externo debe poder resolverse en DNS IPv4 e
   IPv6.



Configuración de la Regulación de RA IPv6

1. Navegue hasta el menú de nivel superior **Controller** y haga clic en la opción **IPv6 > RA Throttle Policy** en el lado izquierdo. Active la aceleración de RA haciendo clic en la casilla de verificación.



Nota: Cuando se produce la aceleración de RA, sólo se permite el acceso al primer router compatible con IPv6. Para redes con varios prefijos IPv6 servidos por routers diferentes, la limitación de RA debe estar inhabilitada.

2. Ajuste el período de aceleración y otras opciones sólo bajo recomendación del TAC. Sin embargo, el valor predeterminado se recomienda para la mayoría de las implementaciones. Las diversas opciones de configuración de la política de aceleración de RA deben ajustarse teniendo esto en cuenta:Los valores numéricos de "Permitir al menos" deben ser inferiores a

"Permitir al menos", que deben ser inferiores a "Pasante máximo".La política del acelerador RA no debe utilizar un período de aceleración superior a 1800 segundos, ya que es la duración predeterminada de la mayoría de RA.

A continuación se describen las opciones de aceleración de RA:

- Período de aceleración: período de tiempo durante el cual tiene lugar la aceleración. La regulación de RA tiene efecto solamente después de que se alcance el límite "Max Through" para la VLAN.
- Max Through (Pasante máximo): Es el número máximo de RA por VLAN antes de que se active la aceleración. La opción "Sin límite" permite una cantidad ilimitada de RAs sin limitación.
- Opción de intervalo: la opción de intervalo permite que el controlador actúe de forma diferente en función del valor RFC 3775 establecido en el RA IPv6.Passthrough (Paso a través): Este valor permite que cualquier RA con una opción de intervalo RFC3775 pase sin limitación.Ignore - Este valor hará que el regulador RA trate a los paquetes con la opción de intervalo como un RA regular y sujeto a regulación si está vigente.Acelerador: este valor hará que los RA con la opción de intervalo estén siempre sujetos a límites de velocidad.
- Permitir como mínimo: el número mínimo de RA por router que se enviarán como multidifusión.
- Permitir como máximo: el número máximo de RA por router que se enviarán como multidifusión antes de que la regulación surta efecto. La opción "Sin límite" permitirá el paso de un número ilimitado de RA para ese router.

Configurar la tabla de enlace de vecino IPv6

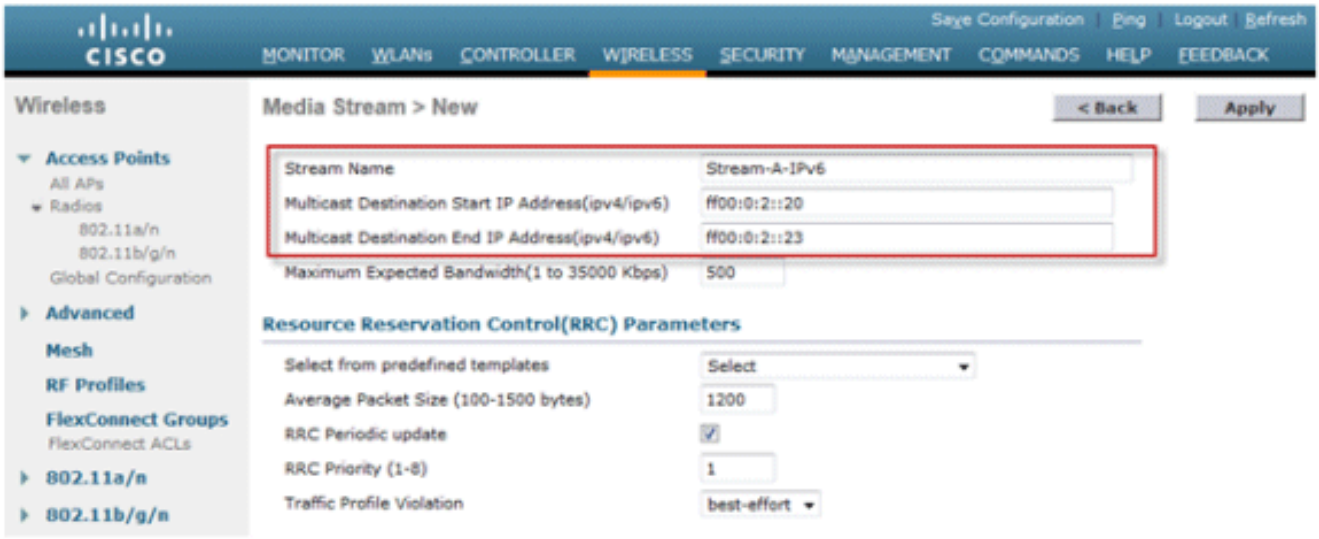
1. Vaya al menú de nivel superior de Controller y haga clic en **IPv6 > Neighbor Binding Timers** en el menú de la izquierda.

2. Ajuste la vida útil hacia abajo, la vida útil alcanzable y la vida útil obsoleta según sea necesario. Para implementaciones con clientes que son altamente móviles, los temporizadores para un temporizador de dirección obsoleto deben ajustarse. Los valores recomendados son:Vida útil inactiva: 30 segundosVida útil alcanzable: 300 segundosDuración del estado: 86400 segundosCada temporizador de duración se refiere al estado en el que puede estar una dirección IPv6:**Tiempo de vida inactivo**: el temporizador de inactividad especifica cuánto tiempo deben conservarse las entradas de caché IPv6 si la interfaz de enlace ascendente del controlador deja de funcionar.**Reachable Lifetime** (Duración alcanzable): Este temporizador especifica cuánto tiempo se marcará como activa una dirección IPv6, lo que significa que se ha recibido tráfico desde esta dirección recientemente. Una vez que este temporizador caduca, la dirección pasa al estado "obsoleto".**Stale Lifetime** - Este temporizador especifica cuánto tiempo se deben mantener las direcciones IPv6 en la memoria caché que no se han visto dentro del "Reachable Lifetime". Después de esta duración, la dirección se quita de la tabla de enlace.

Configurar VideoStream IPv6

1. Asegúrese de que las funciones de Global VideoStream están activadas en Controller. Consulte Cisco Unified Wireless Network Solution: VideoStream Deployment Guide para obtener información sobre cómo habilitar VideoStream en la red 802.11a/g/n, así como el SSID de WLAN.
2. Vaya a la ficha **Wireless** en el controlador y en el menú de la izquierda, elija **Media Stream** > **Streams**. Haga clic en **Add New** para crear una nueva secuencia.

3. Asigne un nombre a la secuencia e introduzca las direcciones IPv6 inicial y final. Cuando se utiliza una sola secuencia, las direcciones inicial y final son iguales. Después de agregar las direcciones, haga clic en **Apply** para crear la secuencia.



Solucionar problemas de conectividad de cliente IPv6

Algunos clientes no pueden pasar tráfico IPv6

Algunas implementaciones de pila de red IPv6 de cliente no se anuncian correctamente al entrar en la red y, por lo tanto, el controlador no indaga su dirección de forma adecuada para colocarla en la tabla de enlace de vecinos. Las direcciones que no estén presentes en la tabla de

vinculación de vecinos se bloquean según la función de protección de origen IPv6. Para permitir que estos clientes pasen el tráfico, estas opciones deben configurarse:

1. Inhabilite la función IPv6 Source Guard a través de la CLI:

   config network ip-mac-binding disable

2. Habilitación del Reenvío de Solicitudes de Vecino Multicast a través de la CLI:

   config ipv6 ns-mcast-fwd enable

Verifique el Roaming de Capa 3 Exitoso para un Cliente IPv6:

Ejecute estos comandos **debug** en el ancla y en el controlador externo:

debug client

debug mobility handoff enable

debug mobility packet enable

Resultados de depuración en controlador de anclaje:

```
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
```

Resultados de depuración en controlador externo:

```
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
```

Comandos útiles de IPv6 CLI:

Show ipv6 neighbor-binding summary

Debug ipv6 neighbor-binding filter client enable

Debug ipv6 neighbor-binding filter errors enable

Preguntas Frecuentes

P: ¿Cuál es el tamaño óptimo del prefijo IPv6 para limitar el dominio de difusión?

R: Aunque una subred IPv6 se puede subdividir por debajo de /64, esta configuración interrumpirá el SLAAC y causará problemas con la conectividad del cliente. Si se necesita segmentación para reducir el número de hosts, la función Interface Groups se puede utilizar para equilibrar la carga de clientes entre diferentes VLAN de back-end, cada una usando un prefijo IPv6 diferente.

P: ¿Existe alguna limitación en cuanto a escalabilidad a la hora de admitir clientes IPv6?

R: La principal limitación de escalabilidad para la compatibilidad con clientes IPv6 es la tabla de enlace de vecinos, que realiza un seguimiento de todas las direcciones IPv6 de clientes inalámbricos. Esta tabla se escala por plataforma de controlador para admitir el número máximo de clientes multiplicado por ocho (el número máximo de direcciones por cliente). La adición de la tabla de enlace IPv6 puede aumentar el uso de memoria del controlador hasta aproximadamente un 10-15% con carga completa, dependiendo de la plataforma.

Controlador inalámbrico	Número máximo de clientes	Tamaño de tabla de enlace de vecino IPv6
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

P: ¿Cuál es el impacto de las funciones de IPv6 en la CPU y la memoria del controlador?

R: El impacto es mínimo ya que la CPU tiene varios núcleos para procesar el plano de control. Cuando se probó con el número máximo de clientes admitidos, cada uno con 8 direcciones IPv6, el uso de la CPU fue inferior al 30% y el uso de la memoria fue inferior al 75%.

P: ¿Se puede desactivar la compatibilidad con el cliente IPv6?

R: Para los clientes que solo desean habilitar IPv4 en su red y bloquear IPv6, se puede utilizar y aplicar una ACL IPv6 de tráfico denegado para cada WLAN.

P: ¿Es posible tener una WLAN para IPv4 y otra para IPv6?

R: No es posible tener el mismo nombre SSID y el mismo tipo de seguridad para dos WLAN diferentes que funcionan en el mismo AP. Para la segmentación de clientes IPv4 de clientes IPv6, se deben crear dos WLAN. Cada WLAN debe configurarse con una ACL que bloquee todo el tráfico IPv4 o IPv6 respectivamente.

P: ¿Por qué es importante admitir varias direcciones IPv6 por cliente?

R: Los clientes pueden tener varias direcciones IPv6 por interfaz que pueden ser estáticas, SLAAC o DHCPv6 asignadas además de tener siempre una dirección Link-Local autoasignada. Los clientes también pueden tener direcciones adicionales mediante prefijos IPv6 diferentes.

P: ¿Qué son las direcciones privadas IPv6 y por qué es importante realizar un seguimiento de ellas?

R: Las direcciones privadas (también conocidas como temporales) son generadas aleatoriamente por el cliente cuando la asignación de direcciones SLAAC está en uso. Estas direcciones suelen rotarse con una frecuencia aproximada de un día, para evitar la trazabilidad del host que resultaría de utilizar el mismo sufijo del host (últimos 64 bits) en todo momento. Es importante realizar un seguimiento de estas direcciones privadas con fines de auditoría, como el seguimiento de la infracción de los derechos de autor. Cisco NCS registra todas las direcciones IPv6 que utiliza cada cliente y las registra históricamente cada vez que el cliente se desplaza o establece una nueva sesión. Estos registros se pueden configurar en NCS para que se conserven durante un máximo de un año.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).