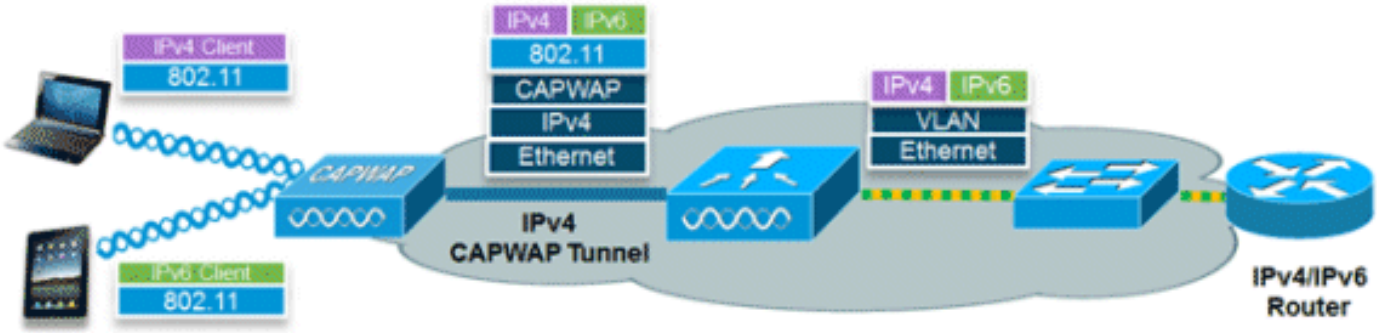
Guia de implantação de cliente IPv6 de LAN sem fio

Contents

Introduction

Este documento fornece informações sobre a teoria da operação e da configuração para a solução Cisco Unified Wireless LAN, enquanto se refere a suporte de clientes IPv6.

Conectividade de Cliente Sem Fio IPv6



O conjunto de recursos IPv6 no software Cisco Unified Wireless Network versão v7.2 permite que a rede sem fio suporte clientes somente IPv4, Dual-Stack e IPv6 na mesma rede sem fio. O objetivo geral para a adição de suporte ao cliente IPv6 para a LAN sem fio unificada da Cisco era manter a paridade de recursos entre clientes IPv4 e IPv6, incluindo mobilidade, segurança, acesso de convidado, qualidade de serviço e visibilidade de endpoint.

Até oito endereços de clientes IPv6 podem ser rastreados por dispositivo. Isso permite que os clientes IPv6 tenham um endereço de link local, de Configuração automática de endereço stateless (SLAAC), de Protocolo de configuração de host dinâmico para endereço IPv6 (DHCPv6) e até mesmo endereços em prefixos alternativos para estar em uma única interface. Os clientes WGB (Work Group Bridge) conectados ao uplink de um ponto de acesso autônomo (AP) no modo WGB também podem suportar IPv6.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controladores de LAN sem fio 2500 Series, 5500 Series ou WiSM2
- APs 1130, 1240, 1250, 1040, 1140, 1260, 3500, 3600 Series APs e 1520 ou 1550 Series Mesh APs
- Roteador compatível com IPv6

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

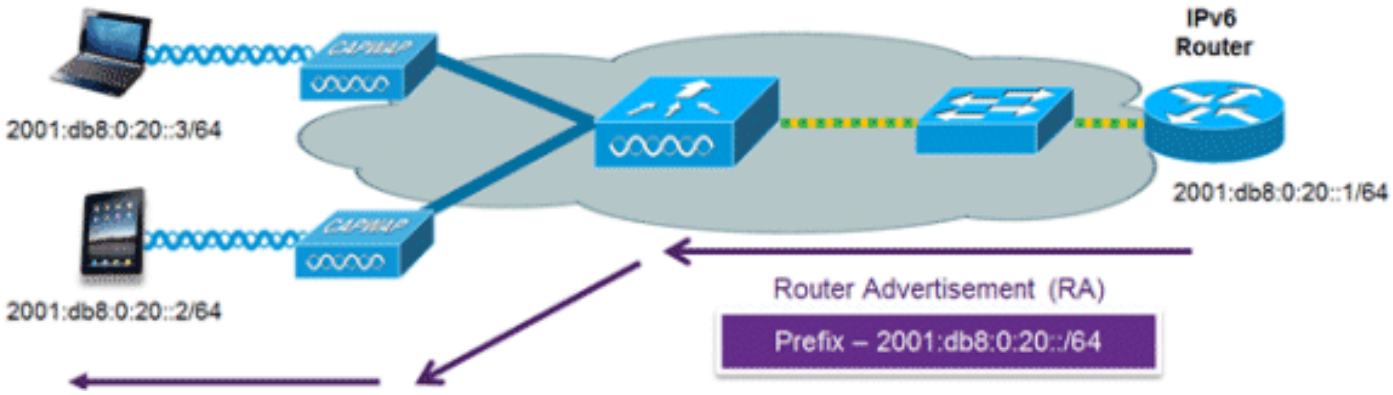
Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Pré-requisitos para conectividade de cliente IPv6 sem fio

Para habilitar a conectividade de cliente IPv6 sem fio, a rede com fio subjacente deve oferecer suporte ao roteamento IPv6 e a um mecanismo de atribuição de endereço, como SLAAC ou DHCPv6. O controlador de LAN sem fio deve ter adjacência L2 com o roteador IPv6, e a VLAN precisa ser marcada quando os pacotes entram no controlador. Os APs não exigem conectividade em uma rede IPv6, pois todo o tráfego é encapsulado dentro do túnel CAPWAP IPv4 entre o AP e o controlador.

Atribuição de endereço SLAAC

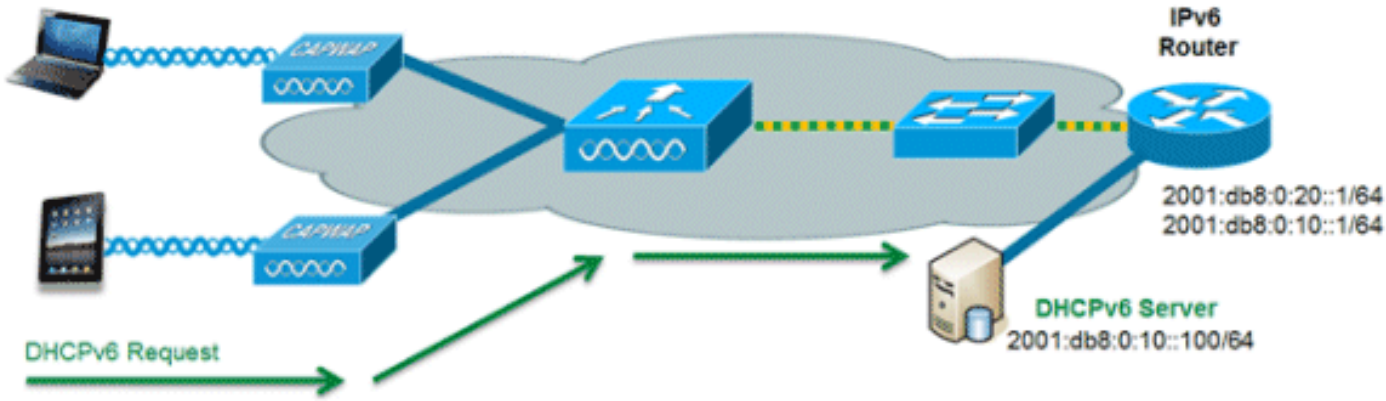


O método mais comum para atribuição de endereço de cliente IPv6 é SLAAC. O SLAAC oferece conectividade plug-and-play simples, em que os clientes atribuem um endereço com base no prefixo IPv6. Esse processo é alcançado quando o roteador IPv6 envia mensagens periódicas de Anúncio de Roteador que informam ao cliente o prefixo IPv6 em uso (os primeiros 64 bits) e o gateway padrão IPv6. A partir desse ponto, os clientes podem gerar os 64 bits restantes de seu endereço IPv6 com base em dois algoritmos: EUI-64, que é baseado no endereço MAC da interface, ou endereços privados que são gerados aleatoriamente. A escolha do algoritmo é da responsabilidade do cliente e é frequentemente configurável. A detecção de endereços duplicados é realizada por clientes IPv6 para garantir que endereços aleatórios que são selecionados não colidam com outros clientes. O endereço do roteador que envia anúncios é usado como gateway padrão para o cliente.

Estes comandos de configuração do Cisco IOS® de um roteador IPv6 com capacidade para Cisco são usados para ativar o endereçamento SLAAC e anúncios de roteador:

```
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
```

Atribuição de endereço DHCPv6



O uso de DHCPv6 não é necessário para conectividade de cliente IPv6 se o SLAAC já estiver implantado. Há dois modos de operação para DHCPv6 chamados **Stateless** e **Stateful**.

O modo DHCPv6 **Stateless** é usado para fornecer aos clientes informações adicionais de rede não disponíveis no anúncio do roteador, mas não um endereço IPv6, pois isso já é fornecido pelo SLAAC. Essas informações podem incluir o nome de domínio DNS, os servidores DNS e outras opções específicas do fornecedor de DHCP. Esta configuração de interface é para um roteador Cisco IOS IPv6 que implementa DHCPv6 stateless com 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
```

A opção DHCPv6 **Stateful**, também conhecida como modo gerenciado, opera de forma semelhante ao DHCPv4, pois atribui endereços exclusivos a cada cliente, em vez de o cliente gerar os últimos 64 bits do endereço como no SLAAC. Esta configuração de interface é para um roteador Cisco IOS IPv6 que implementa DHCPv6 stateful com SLAAC desabilitado:

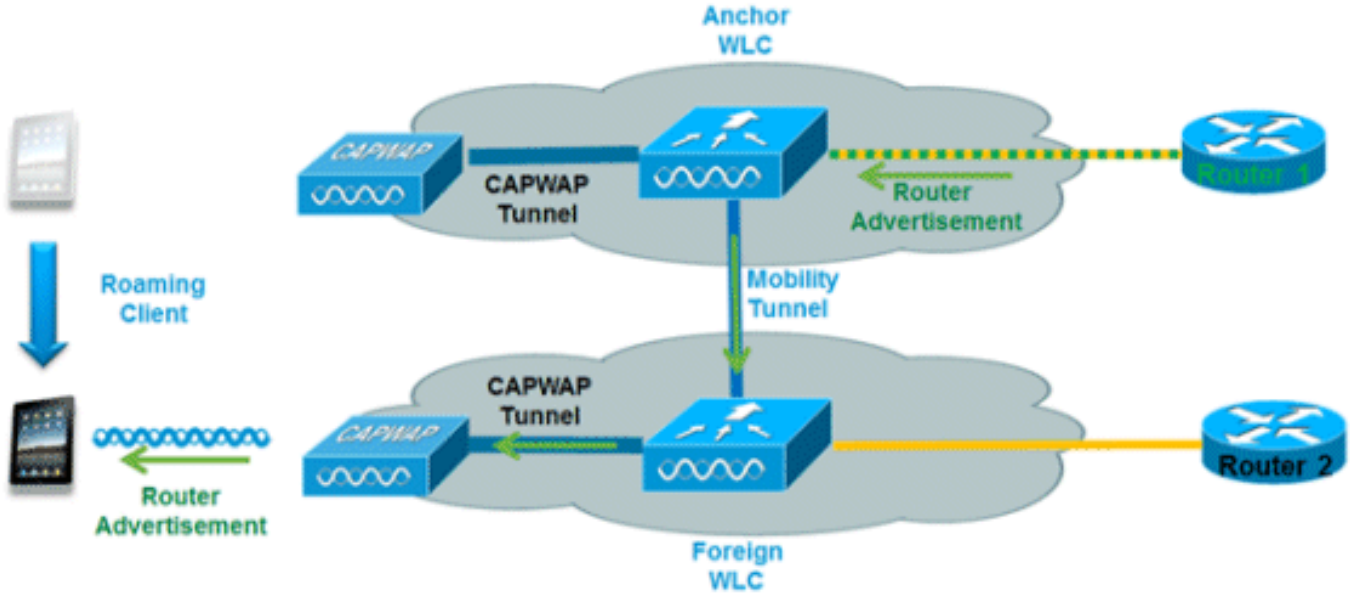
```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateful
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
```

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

Additional Information

A configuração da rede com fio para conectividade completa de todo o campus IPv6 usando métodos de conectividade de pilha dupla ou de túnel está fora do escopo deste documento. Para obter mais informações, consulte o guia de implantação validado da Cisco Implantação de IPv6 em redes de campus.

Mobilidade de cliente IPv6



Para lidar com clientes IPv6 de roaming nos controladores, as mensagens ICMPv6 como Solicitação de Vizinhos (NS), Anúncio de Vizinhos (NA), Anúncio de Roteadores (RA) e Solicitação de Roteadores (RS) devem ser tratadas especialmente para garantir que um cliente permaneça na mesma rede de Camada 3. A configuração para mobilidade IPv6 é a mesma que para mobilidade IPv4 e não requer software separado no lado do cliente para obter roaming contínuo. A única configuração necessária é que os controladores devem fazer parte do mesmo grupo/domínio de mobilidade.

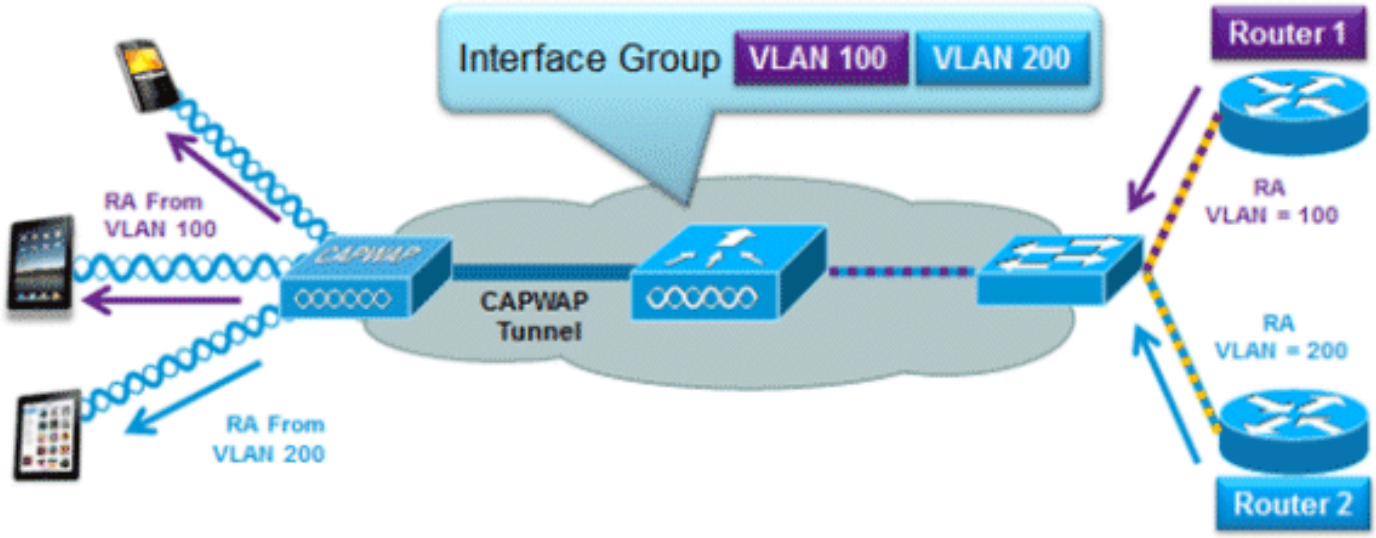
Este é o processo para mobilidade de cliente IPv6 entre controladores:

1. Se ambos os controladores tiverem acesso à mesma VLAN em que o cliente estava originalmente, o roaming é simplesmente um evento de roaming de Camada 2 em que o registro do cliente é copiado para o novo controlador e nenhum tráfego é enviado de volta para o controlador âncora.
2. Se o segundo controlador não tiver acesso à VLAN original em que o cliente estava, ocorrerá um evento de roaming de Camada 3, o que significa que todo o tráfego do cliente deve ser encapsulado através do túnel de mobilidade (Ethernet sobre IP) para o controlador âncora.Para garantir que o cliente retenha seu endereço IPv6 original, os RAs da VLAN original são enviados pelo controlador âncora para o controlador externo, onde são entregues ao cliente usando unicast L2 do AP.Quando o cliente em roaming vai renovar seu

endereço via DHCPv6 ou gerar um novo endereço via SLAAC, os pacotes RS, NA e NS continuam a ser encapsulados na VLAN original para que o cliente receba um endereço IPv6 que seja aplicável a essa VLAN.

Observação: a mobilidade para clientes somente IPv6 é baseada em informações de VLAN. Isso significa que a mobilidade do cliente somente IPv6 não é suportada em VLANs não marcadas.

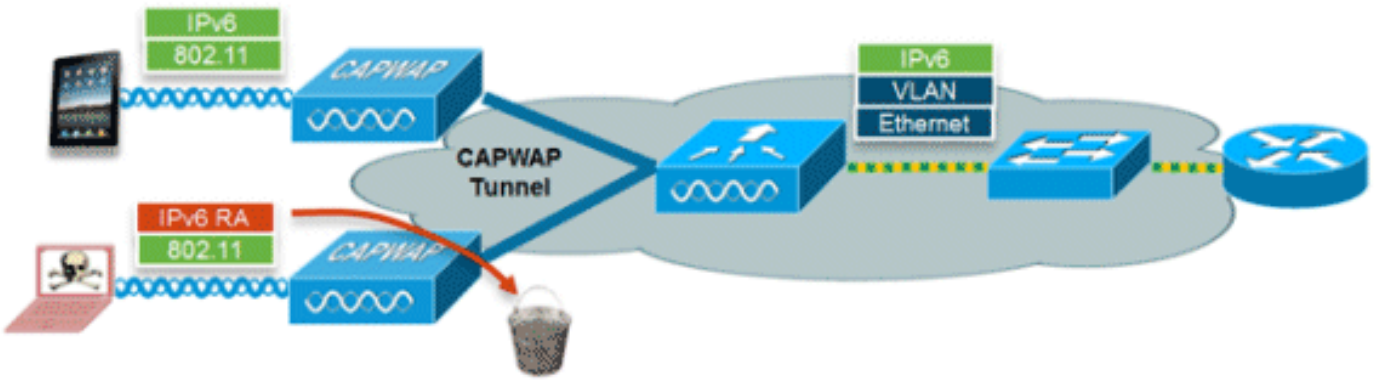
Suporte para seleção de VLAN (grupos de interface)



O recurso de grupos de interface permite que uma organização tenha uma única WLAN com várias VLANs configuradas no controlador para permitir o balanceamento de carga de clientes sem fio nessas VLANs. Esse recurso é comumente usado para manter os tamanhos de sub-rede IPv4 pequenos, ao mesmo tempo em que permite que uma WLAN escale para milhares de usuários em várias VLANs no grupo. Para suportar clientes IPv6 com grupos de interface, nenhuma configuração adicional é necessária, pois o sistema envia automaticamente o RA correto para os clientes corretos através do unicast sem fio L2. Ao unicast do RA, os clientes na mesma WLAN, mas em uma VLAN diferente, não recebem o RA incorreto.

Segurança First Hop para clientes IPv6

Proteção de Anúncio de Roteador



O recurso RA Guard aumenta a segurança da rede IPv6 eliminando RAs provenientes de clientes sem fio. Sem esse recurso, clientes IPv6 mal configurados ou mal-intencionados poderiam anunciar-se como um roteador para a rede, geralmente com uma prioridade alta que poderia ter precedência sobre roteadores IPv6 legítimos.

Por padrão, o RA Guard é ativado no AP (mas pode ser desativado no AP) e sempre é ativado no controlador. Descartar RAs no AP é preferível, pois é uma solução mais escalável e fornece contadores avançados de descarte de RA por cliente. Em todos os casos, o RA IPv6 será descartado em algum momento, protegendo outros clientes sem fio e a rede com fio upstream de clientes IPv6 mal-intencionados ou configurados incorretamente.

Proteção de servidor DHCPv6

O recurso DHCPv6 Server Guard impede que os clientes sem fio distribuam endereços IPv6 para outros clientes sem fio ou clientes com fio upstream. Para impedir que endereços DHCPv6 sejam distribuídos, todos os pacotes de anúncio DHCPv6 de clientes sem fio são descartados. Esse recurso opera no controlador, não requer configuração e é ativado automaticamente.

Proteção de origem IPv6

O recurso IPv6 Source Guard impede que um cliente sem fio falsifique um endereço IPv6 de outro cliente. Esse recurso é análogo ao IPv4 Source Guard. O IPv6 Source Guard está ativado por padrão, mas pode ser desativado via CLI.

Contabilização de Endereço IPv6

Para autenticação e tarifação RADIUS, o controlador envia de volta um endereço IP usando o atributo "Framed-IP-address". O endereço IPv4 é usado nesse caso.

O atributo "Calling-Station-ID" usa esse algoritmo para enviar de volta um endereço IP quando o "Tipo de ID da estação de chamada" no controlador está configurado como "Endereço IP":

1. endereço IPv4
2. Endereço IPv6 unicast global
3. Endereço IPv6 do link local

Como os endereços IPv6 do cliente podem mudar com frequência (endereços temporários ou privados), é importante rastreá-los ao longo do tempo. O Cisco NCS registra todos os endereços IPv6 em uso por cada cliente e os registra historicamente cada vez que o cliente faz roaming ou estabelece uma nova sessão. Esses registros podem ser configurados no NCS para serem mantidos por até um ano.

Observação: o valor padrão para o "Tipo de ID da estação de chamada" no controlador foi alterado para "Endereço MAC do sistema" na versão 7.2. Durante a atualização, isso deve ser alterado para permitir o rastreamento exclusivo de clientes pelo endereço MAC, pois os endereços IPv6 podem mudar durante a sessão e causar problemas na contabilidade se o ID da estação de chamada estiver definido como endereço IP.

Listas de controle de acesso IPv6

Para restringir o acesso a certos recursos cabeados de upstream ou bloquear certos aplicativos, as Listas de Controle de Acesso (ACLs) IPv6 podem ser usadas para identificar o tráfego e permitir ou negá-lo. As ACLs IPv6 suportam as mesmas opções que as ACLs IPv4, incluindo a origem, o destino, a porta de origem e a porta de destino (os intervalos de porta também são suportados). As ACLs de pré-autenticação também são suportadas para oferecer suporte à autenticação de convidado IPv6 usando um servidor Web externo. O controlador sem fio suporta

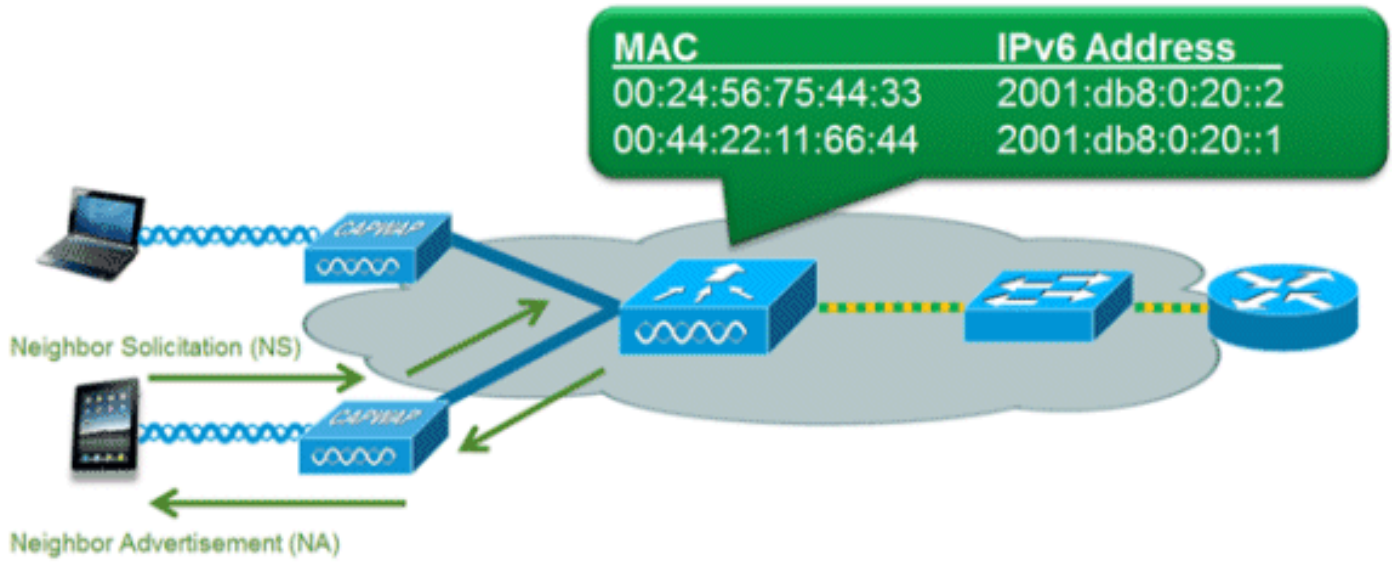
até 64 ACLs IPv6 exclusivas com 64 regras exclusivas em cada uma. O controlador sem fio continua a suportar 64 ACLs IPv4 exclusivas adicionais com 64 regras exclusivas em cada uma, totalizando 128 ACLs para um cliente de pilha dupla.

Substituição de AAA para ACLs IPv6

Para oferecer suporte ao controle de acesso centralizado por meio de um servidor AAA centralizado, como o Cisco Identity Services Engine (ISE) ou o ACS, a ACL IPv6 pode ser provisionada por cliente usando atributos AAA Override. Para usar esse recurso, a ACL IPv6 deve ser configurada no controlador e a WLAN deve ser configurada com o recurso AAA Override habilitado. O atributo de AAA nomeado real para uma ACL IPv6 é ***Airespace-IPv6-ACL-Name*** semelhante ao atributo *Airespace-ACL-Name* usado para provisionar uma ACL baseada em IPv4. O conteúdo retornado do atributo AAA deve ser uma sequência de caracteres igual ao nome da ACL IPv6 conforme configurado no controlador.

Otimização de pacotes para clientes IPv6

Cache de descoberta de vizinhos



O protocolo de descoberta de vizinhos (NDP - Neighbor Discovery Protocol) IPv6 utiliza pacotes NA e NS no lugar do Address Resolution Protocol (ARP) para permitir que os clientes IPv6 resolvam o endereço MAC de outros clientes na rede. O processo NDP pode ser muito tagarela, pois inicialmente usa endereços multicast para executar a resolução de endereços; isso pode consumir tempo de transmissão sem fio valioso, pois os pacotes multicast são enviados a todos os clientes no segmento de rede.

Para aumentar a eficiência do processo NDP, o cache de descoberta de vizinhos permite que o controlador atue como um proxy e responda às consultas NS que ele pode resolver. O cache de descoberta de vizinhos é possibilitado pela tabela de ligação de vizinhos subjacente presente no controlador. A tabela de vinculação de vizinhos rastreia cada endereço IPv6 e seu endereço MAC associado. Quando um cliente IPv6 tenta resolver o endereço da camada de enlace de outro cliente, o pacote NS é interceptado pelo controlador que responde com um pacote NA.

Limitação de Anúncio de Roteador

A limitação de anúncio de roteador permite que o controlador imponha a limitação de taxa de RAs direcionadas para a rede sem fio. Ao habilitar a limitação de RA, os roteadores configurados para enviar RAs com muita frequência (por exemplo, a cada três segundos) podem ser reduzidos a uma frequência mínima que ainda manterá a conectividade do cliente IPv6. Isso permite que o tempo de transmissão seja otimizado reduzindo o número de pacotes multicast que devem ser enviados. Em todos os casos, se um cliente enviar um RS, um RA será permitido através do controlador e unicast para o cliente solicitante. Isso serve para garantir que novos clientes ou clientes de roaming não sejam afetados negativamente pela limitação do RA.

Acesso de convidado IPv6

Os recursos de convidado com e sem fio presentes para clientes IPv4 funcionam da mesma maneira para clientes de pilha dupla e somente IPv6. Quando o usuário convidado se associar, ele será colocado em um estado de execução "WEB_AUTH_REQ" até que o cliente seja autenticado por meio do portal cativo IPv4 ou IPv6. O controlador interceptará o tráfego HTTP/HTTPS IPv4 e IPv6 nesse estado e o redirecionará para o endereço IP virtual do controlador. Depois que o usuário é autenticado por meio do portal cativo, seu endereço MAC é movido para o estado de execução e o tráfego IPv4 e IPv6 tem permissão para passar. Para a autenticação da Web externa, a ACL de pré-autenticação permite que um servidor Web externo seja usado.

Para suportar o redirecionamento de clientes somente IPv6, o controlador cria automaticamente um endereço virtual IPv6 com base no endereço virtual IPv4 configurado no controlador. O endereço IPv6 virtual segue a convenção de `[::ffff:<endereço IPv4 virtual>]`. Por exemplo, um endereço IP virtual de 1.1.1.1 seria convertido em `[::ffff:1.1.1.1]`.

Ao usar um certificado SSL confiável para autenticação de acesso de convidado, certifique-se de que os endereços virtuais IPv4 e IPv6 do controlador estejam definidos no DNS para corresponder ao nome de host dos certificados SSL. Isso garante que os clientes não recebam um aviso de segurança informando que o certificado não corresponde ao nome de host do dispositivo.

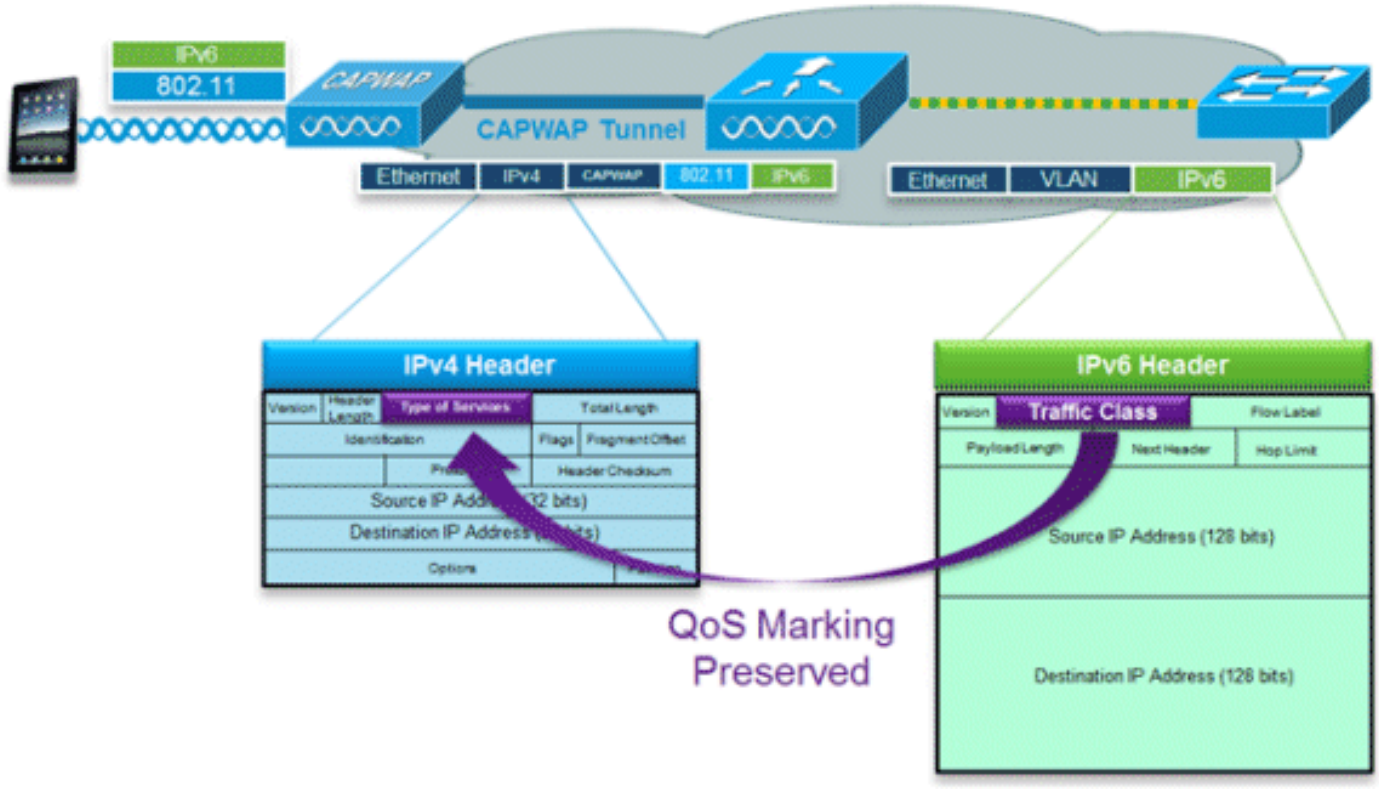
Observação: o certificado SSL gerado automaticamente do controlador não contém o endereço virtual IPv6. Isso pode fazer com que alguns navegadores apresentem um aviso de segurança. É recomendável usar um certificado SSL confiável para acesso de convidado.

Fluxo de vídeo IPv6

O VideoStream permite a entrega de vídeo multicast sem fio confiável e escalável, enviando o fluxo a cada cliente em um formato unicast. A conversão real de multicast para unicast (de L2) ocorre no AP fornecendo uma solução escalável. O controlador envia o tráfego de vídeo IPv6 dentro de um túnel multicast CAPWAP IPv4 que permite a distribuição eficiente da rede para o

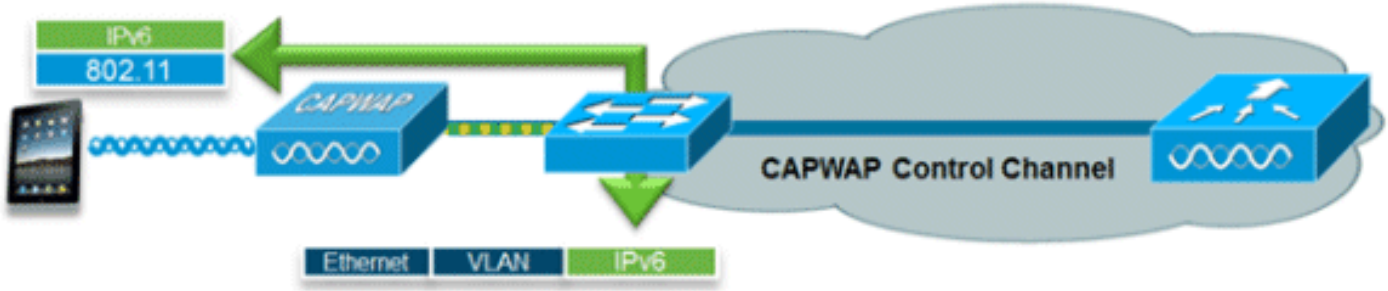
AP.

Qualidade de Serviço IPv6



Os pacotes IPv6 usam uma marcação semelhante ao uso do IPv4 dos valores de DSCP que suportam até 64 classes de tráfego diferentes (0-63). Para pacotes downstream da rede com fio, o valor da classe de tráfego IPv6 é copiado para o cabeçalho do túnel CAPWAP para garantir que a QoS seja preservada de ponta a ponta. No sentido upstream, o mesmo ocorre que o tráfego de cliente marcado na Camada 3 com a classe de tráfego IPv6 será honrado pela marcação dos pacotes CAPWAP destinados ao controlador.

IPv6 e FlexConnect



FlexConnect - WLANs de switching local

O FlexConnect no modo de switching local suporta clientes IPv6 fazendo a ponte do tráfego para a VLAN local, semelhante à operação do IPv4. A mobilidade do cliente é compatível com roaming de camada 2 no grupo FlexConnect.

Esses recursos específicos do IPv6 são suportados no modo de switching local do FlexConnect:

- Proteção de RA IPv6
- Bridging IPv6
- Autenticação de convidado IPv6 (hospedada por controlador)

Esses recursos específicos do IPv6 não são suportados no modo de switching local do FlexConnect:

- Mobilidade da camada 3
- Fluxo de vídeo IPv6
- Listas de controle de acesso IPv6
- Proteção de origem IPv6
- Proteção de servidor DHCPv6
- Cache de descoberta de vizinhos
- Limitação de Anúncio de Roteador

FlexConnect - WLANs de switching central

Para APs no modo FlexConnect que usam switching central (tráfego de tunelamento de volta para o controlador), o controlador deve ser definido como "Multicast - Unicast Mode" para o "AP Multicast Mode". Como os APs FlexConnect não se juntam ao grupo multicast CAPWAP do controlador, os pacotes multicast devem ser replicados no controlador e unicast para cada AP individualmente. Esse método é menos eficiente que o "Multicast - Modo Multicast" e coloca carga adicional no controlador.

Este recurso específico de IPv6 não é suportado no modo de switching central FlexConnect:

- Fluxo de vídeo IPv6

Observação: as WLANs comutadas centralmente que executam IPv6 não são suportadas no Flex 7500 Series Controller.

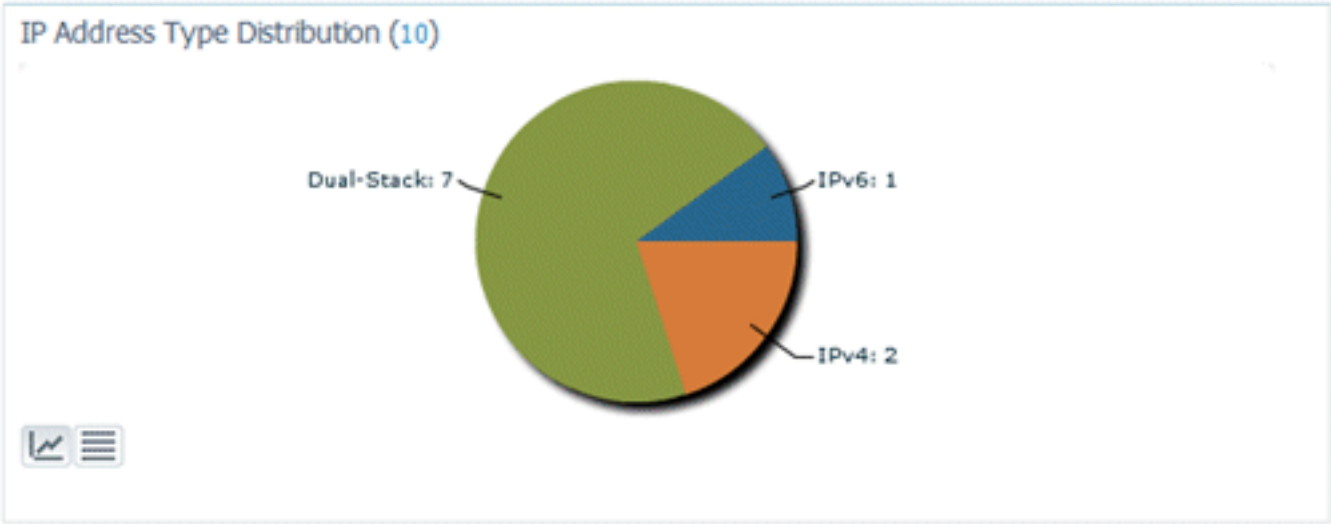
Visibilidade de clientes IPv6 com NCS

Com o lançamento do NCS v1.1, muitos recursos adicionais específicos do IPv6 são adicionados para monitorar e gerenciar uma rede de clientes IPv6 em redes com e sem fio.

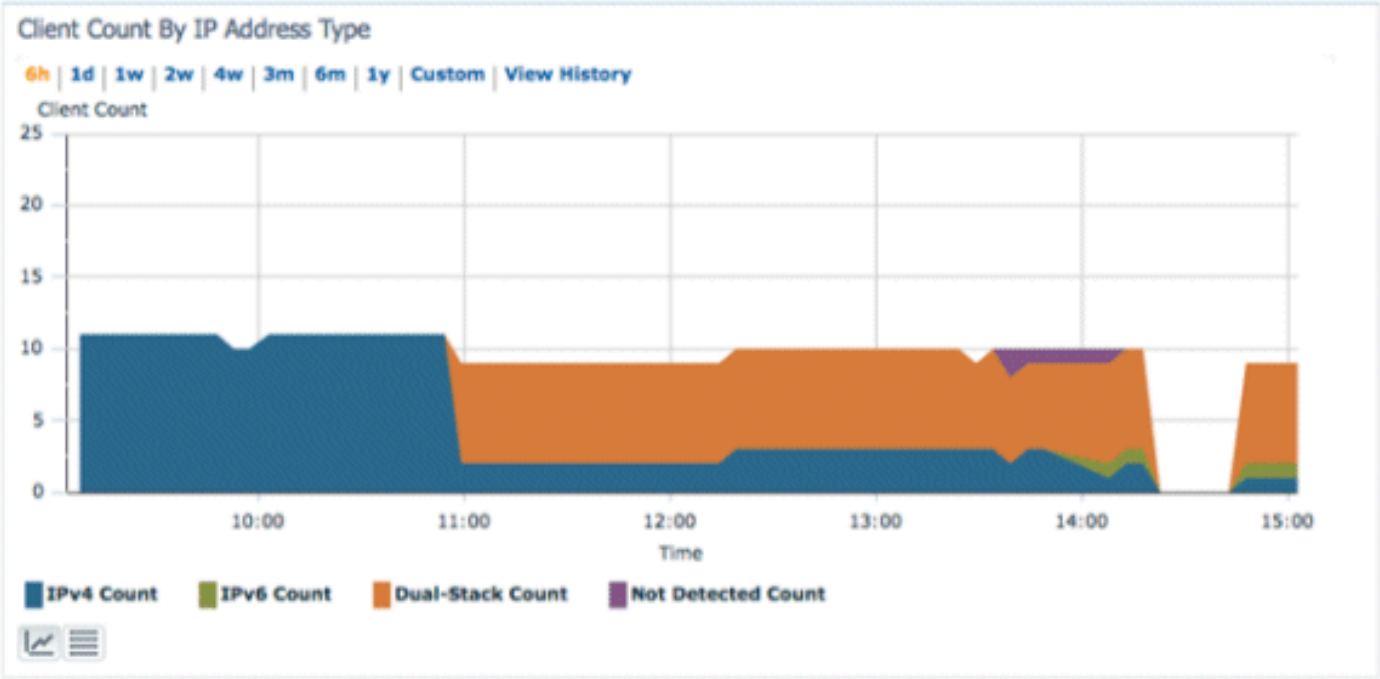
Itens do painel IPv6

Para visualizar que tipos de clientes estão presentes na rede, um "Dashlet" no NCS está disponível para fornecer informações sobre estatísticas específicas de IPv6 e oferecer a capacidade de detalhamento em clientes IPv6.

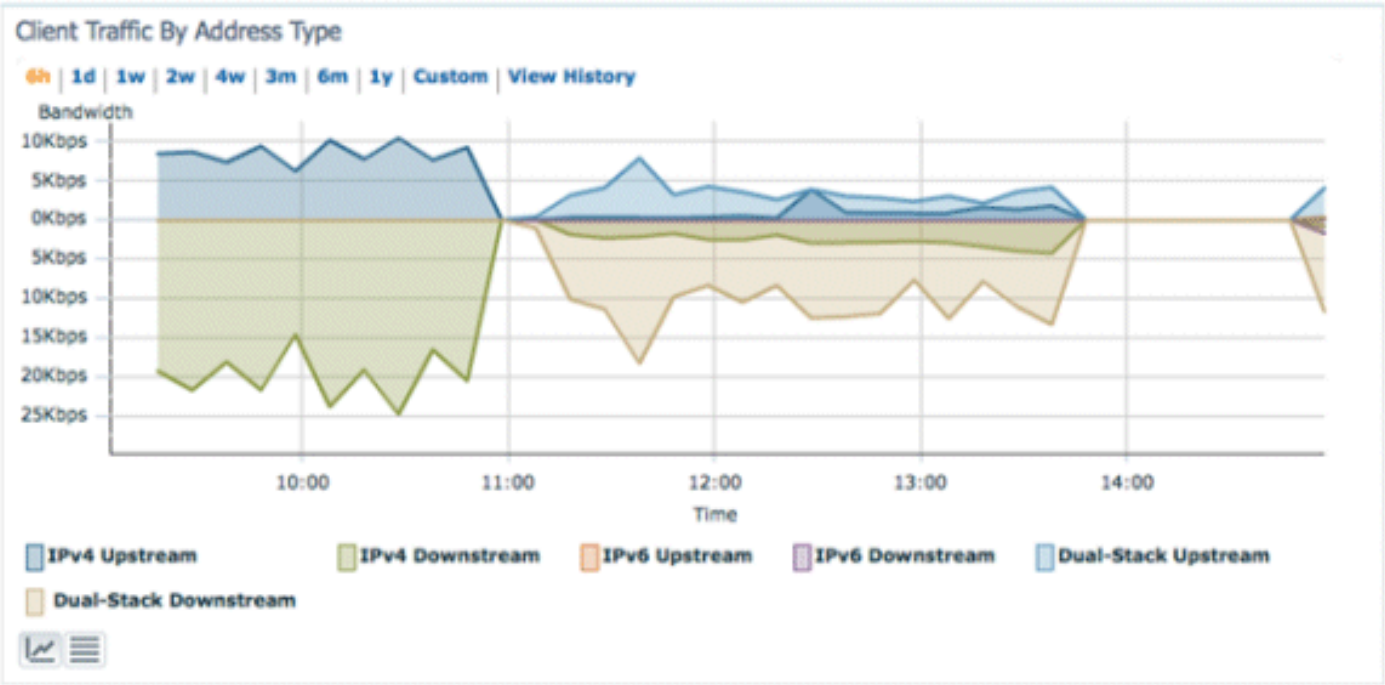
Dashlet de tipo de endereço IP - Exibe os tipos de clientes IP na rede:



Contagem de clientes por tipo de endereço IP - Exibe o tipo de cliente IP ao longo do tempo:



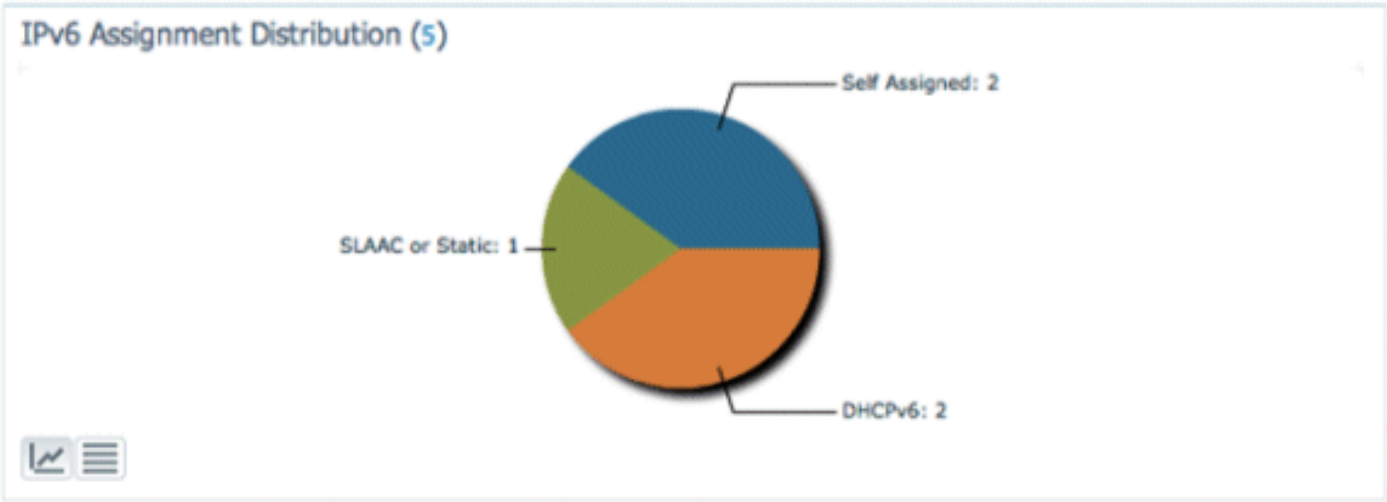
Tráfego do cliente por tipo de endereço IP - Exibe o tráfego de cada tipo de cliente. Os clientes na categoria de pilha dupla incluem tráfego IPv4 e IPv6:



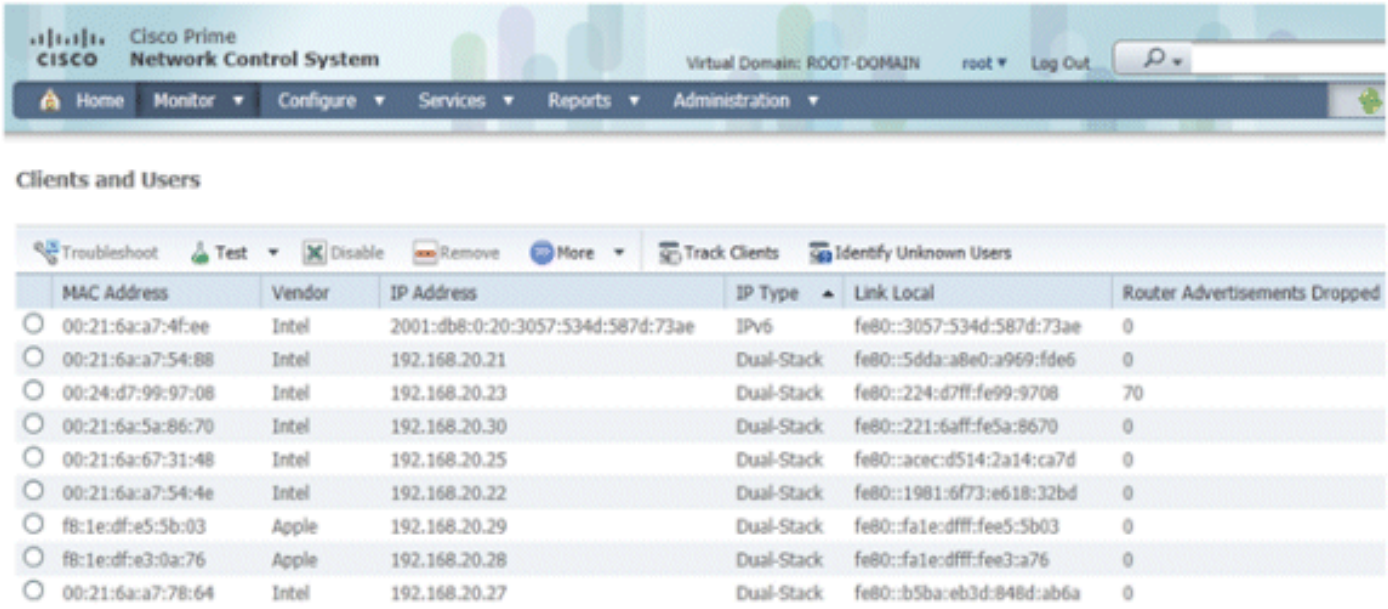
Atribuição de endereço IPv6 - Exibe o método de atribuição de endereço para cada cliente como uma destas quatro categorias:

- DHCPv6 - Para clientes com endereços atribuídos por um servidor central. O cliente também pode ter um endereço SLAAC.
- SLAAC ou Estático - Para clientes que usam atribuição automática de endereço stateless ou endereços configurados estaticamente.
- Desconhecido - Em alguns casos, a atribuição de endereço IPv6 não pode ser descoberta.Essa condição ocorre apenas em clientes com fio no NCS, pois alguns switches não rastreiam informações de atribuição de endereço IPv6.
- Autoatribuído - Para clientes com apenas um endereço de link local que é totalmente autoatribuído.Os clientes nesta categoria podem ter problemas de conectividade IPv6, pois não têm um endereço exclusivo global ou exclusivo local.

Cada uma das seções do gráfico de pizza pode ser clicada, o que permite que o administrador faça drill-down para uma lista de clientes.

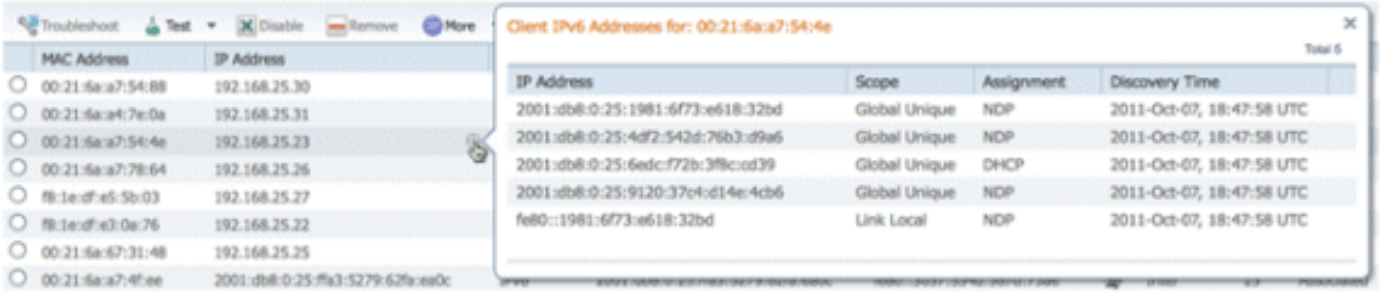


Monitorar Clientes IPv6



Para monitorar e gerenciar as informações do cliente IPv6, estas colunas foram adicionadas à página Clientes e usuários:

- Tipo de IP - O tipo de cliente com base nos endereços IP que foram vistos do cliente. As opções possíveis são IPv4, IPv6 ou Pilha Dupla, o que significa um cliente com endereços IPv4 e IPv6.
- Tipo de atribuição de IPv6 - o método de atribuição de endereço é detectado pelo NCS como SLAAC ou estático, DHCPv6, autoatribuído ou desconhecido.
- Global Exclusivo - O endereço global IPv6 mais recente usado pelo cliente. Passe o mouse sobre o conteúdo da coluna para ver todos os endereços IPv6 exclusivos globais adicionais usados pelo cliente.
- Exclusivo local - o endereço exclusivo local IPv6 mais recente usado pelo cliente. Passe o mouse sobre o conteúdo da coluna para ver todos os endereços IPv6 exclusivos globais adicionais usados pelo cliente.
- Link Local - O endereço IPv6 do cliente que é autoatribuído e usado para comunicação antes que qualquer outro endereço IPv6 seja atribuído.
- Anúncios do roteador descartados - O número de anúncios do roteador enviados pelo cliente e descartados no AP. Essa coluna pode ser usada para rastrear clientes que podem estar configurados incorretamente ou mal-intencionados para agir como um roteador IPv6. Essa coluna é classificável, o que permite que clientes ofensivos sejam identificados facilmente.

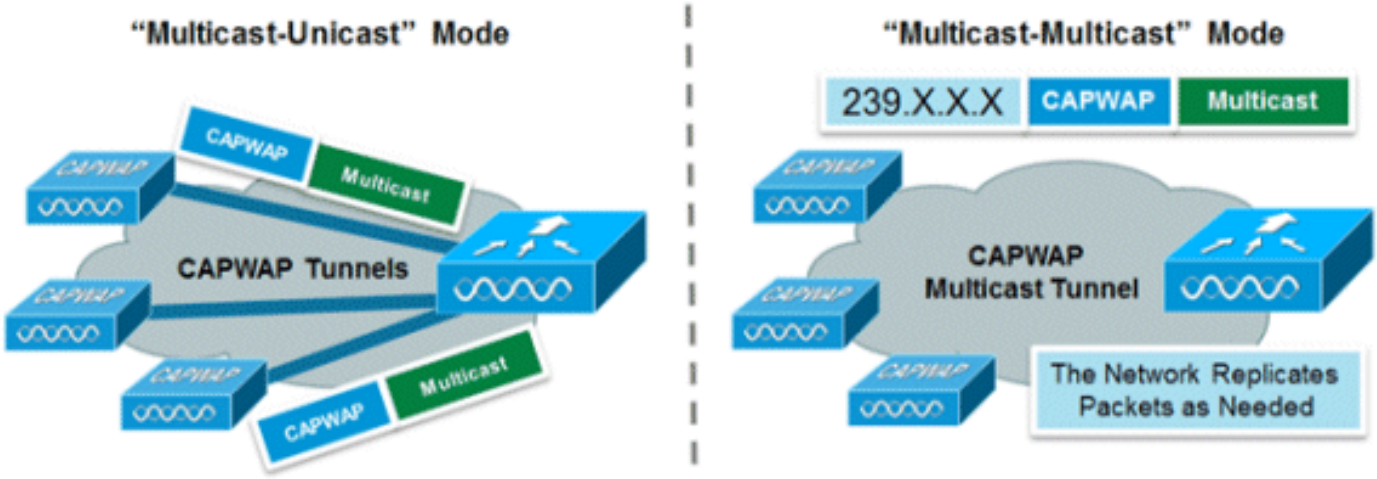


Além de exibir colunas específicas de IPv6, a coluna Endereço IP mostrará o endereço IP atual do cliente com uma prioridade para exibir primeiro o endereço IPv4 (no caso de um cliente de Pilha Dupla) ou o endereço exclusivo global de IPv6 no caso de um cliente somente IPv6.

Configuração para suporte ao cliente IPv6 sem fio

Modo de distribuição multicast para APs

O Cisco Unified Wireless Network suporta dois métodos de distribuição multicast para APs associados ao controlador. Em ambos os modos, o pacote multicast original da rede com fio é encapsulado dentro de um pacote CAPWAP de Camada 3 enviado via Unicast CAPWAP ou Multicast para o AP. Como o tráfego é encapsulado pelo CAPWAP, os APs não precisam estar na mesma VLAN que o tráfego do cliente. Os dois métodos de distribuição Multicast são comparados aqui:



	Modo Multicast-Unicast	Modo Multicast-Multicast
Mecanismo de entrega	O controlador replica o pacote multicast e o envia para cada AP em um túnel CAPWAP Unicast	O controlador envia uma cópia do pacote multicast
Modos de AP suportados	FlexConnect e local	Somente modo local
Requer roteamento multicast L3 em rede com fio	No	Yes
Carregamento do controlador	Alto	Baixa
Carregamento de rede com fio	Alto	Baixa

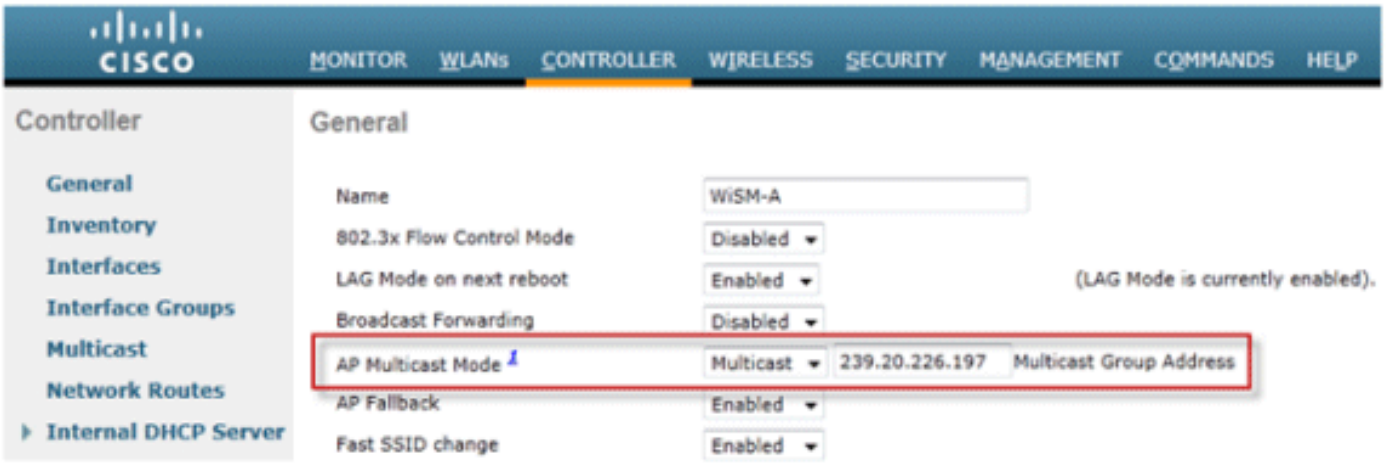
Configurar o modo de distribuição multicast-multicast

O modo multicast-multicast é a opção recomendada por motivos de escalabilidade e eficiência de largura de banda com fio.

Observação: esta etapa só é absolutamente necessária para o 2500 Series Wireless Controller,

mas permite transmissão multicast mais eficiente e é recomendada para todas as plataformas de controlador.

Acesse a guia "Controller" na página "General" e verifique se o AP Multicast Mode está configurado para usar o **Multicast** e se um endereço de grupo válido está configurado. O endereço de grupo é um grupo multicast IPv4 e é recomendado estar no intervalo 239.X.X-239.255.255.255, que tem escopo para aplicativos multicast privados.

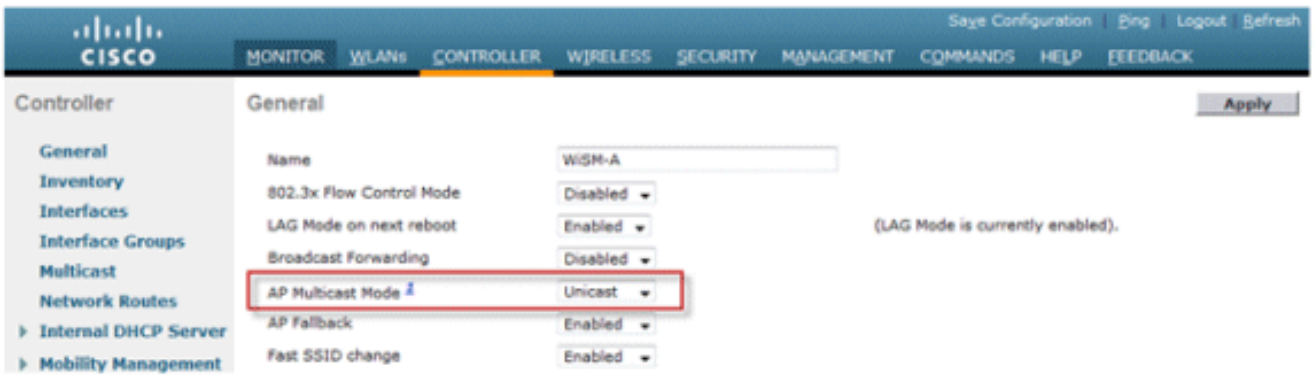


Observação: não use os intervalos de endereço 224.X.X.X, 239.0.0.X ou 239.128.0.X para o endereço do grupo multicast. Os endereços nesses intervalos se sobrepõem aos endereços MAC locais do link e inundam todas as portas do switch, mesmo com o snooping IGMP habilitado.

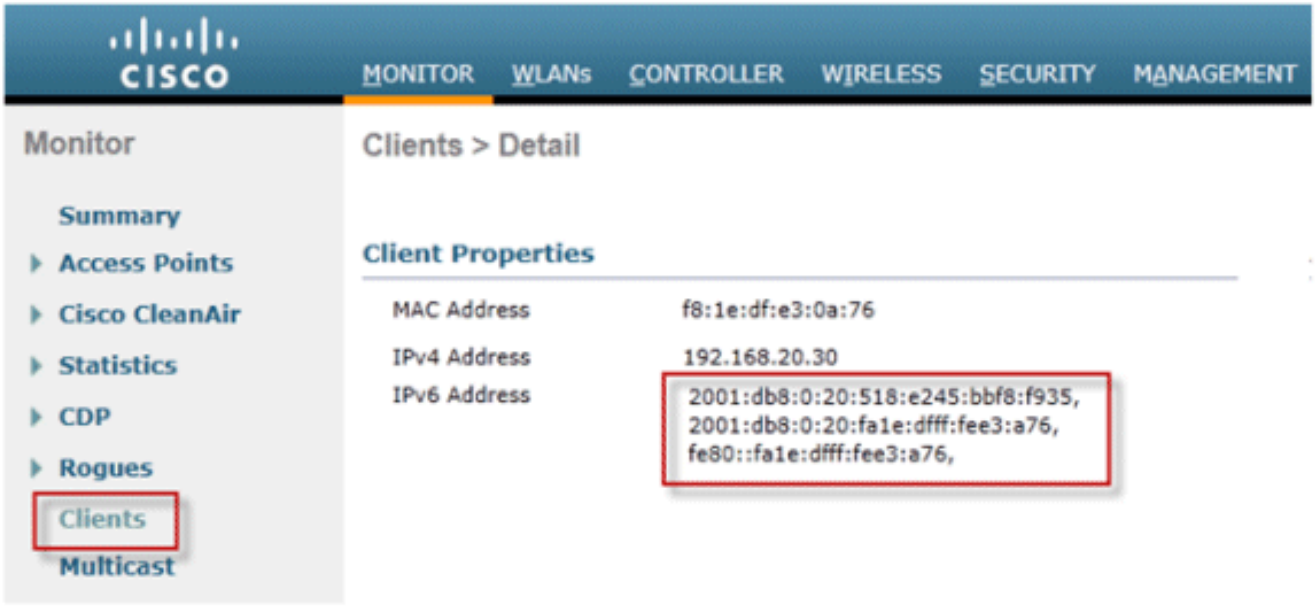
Configurar o modo de distribuição multicast-unicast

Se a rede com fio não estiver configurada corretamente para fornecer o multicast CAPWAP entre o controlador e o AP ou o modo FlexConnect, e os APs forem usados para WLANs com comutação central que suportam IPv6, o modo unicast será necessário.

1. Vá até a guia **Controller** na página General e certifique-se de que o AP Multicast Mode esteja configurado para usar o modo **Unicast**.



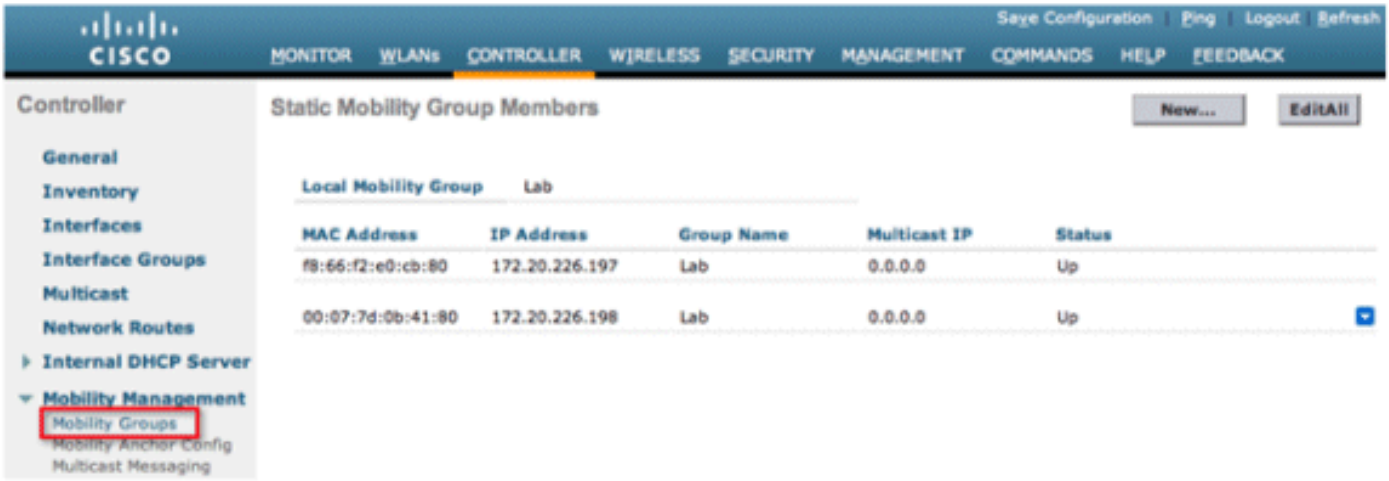
2. Conecte um cliente compatível com IPv6 à LAN sem fio. Valide se o cliente recebe um endereço IPv6 navegando até a guia **Monitor** e depois até o menu **Clients**.



Configurar a mobilidade do IPv6

Não há configuração específica para mobilidade IPv6, exceto para colocar controladores no mesmo grupo de mobilidade ou no mesmo domínio de mobilidade. Isso permite que até 72 controladores no total participem de um domínio de mobilidade, fornecendo mobilidade contínua até mesmo para o maior dos campi.

Acesse a guia **Controller > Mobility Groups** e adicione cada controlador por endereço MAC e endereço IP no grupo. Isso deve ser feito em todos os controladores no grupo de mobilidade.



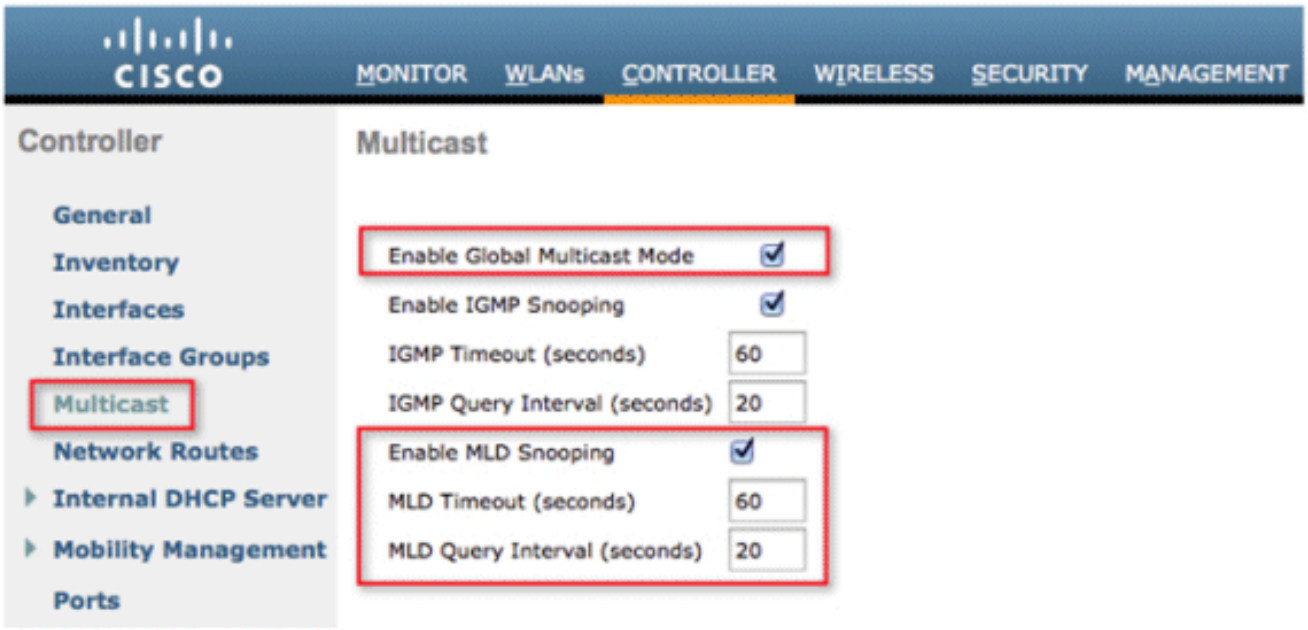
Configurar multicast IPv6

O controlador oferece suporte à espionagem de MLDv1 para multicast IPv6, o que permite que ele acompanhe e forneça fluxos multicast de forma inteligente aos clientes que os solicitam.

Observação: ao contrário das versões anteriores, o suporte ao tráfego unicast IPv6 não exige que o "Modo Multicast Global" seja ativado no controlador. O suporte ao tráfego unicast IPv6 é habilitado automaticamente.

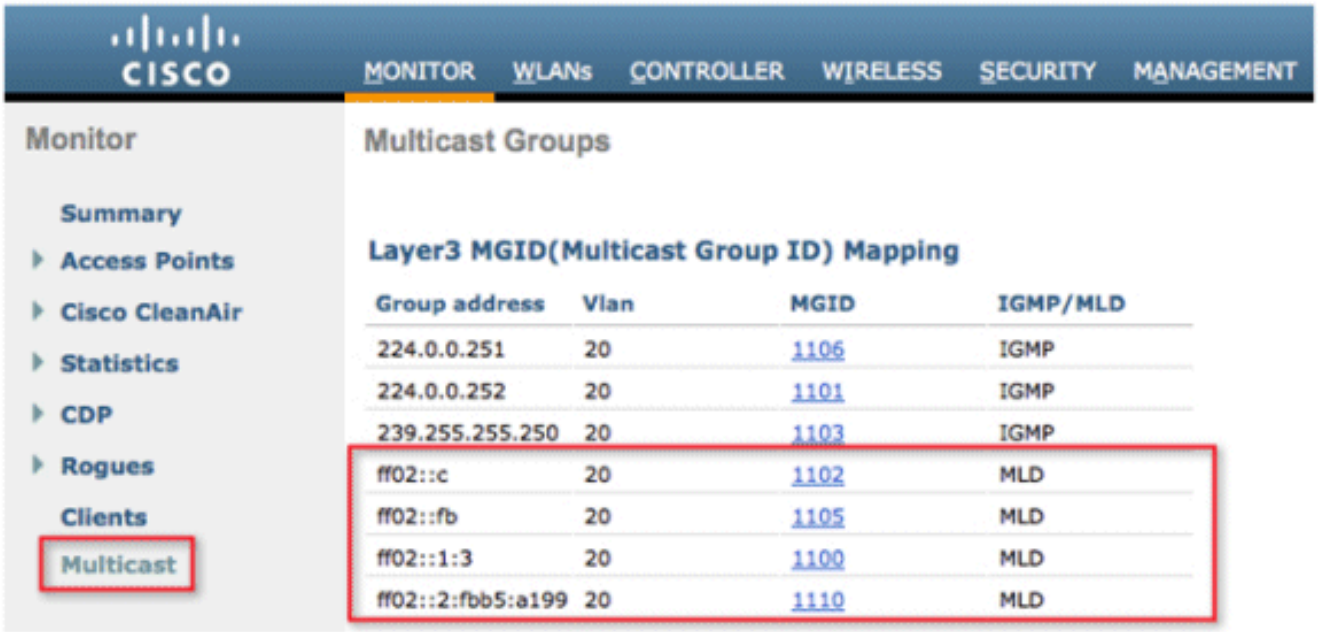
1. Vá para a página **Controller > Multicast** e **Enable MLD Snooping** para oferecer suporte ao tráfego IPv6 multicast. Para que o Multicast IPv6 seja habilitado, o **Modo Multicast Global** do

controlador também deve ser habilitado.



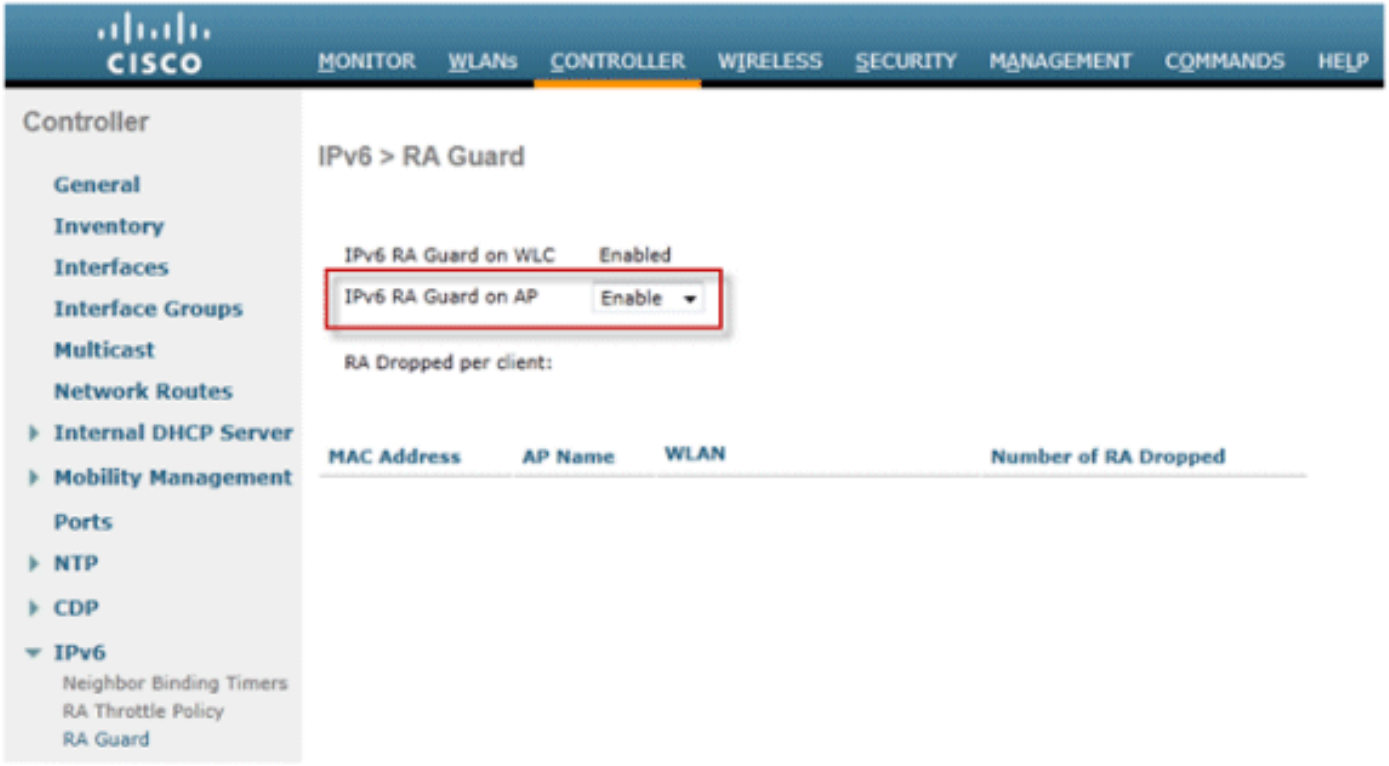
Observação: o modo multicast global, o IGMP e a espionagem de MLD devem ser ativados se forem necessários aplicativos de descoberta ponto a ponto, como o Bonjour da Apple.

2. Para verificar se o tráfego de multicast IPv6 está sendo rastreado, vá para a guia **Monitor** e a página **Multicast**. Observe que os grupos multicast IPv4 (IGMP) e IPv6 (MLD) estão listados. Clique no MGID para exibir os clientes sem fio que ingressaram nesse endereço de grupo.



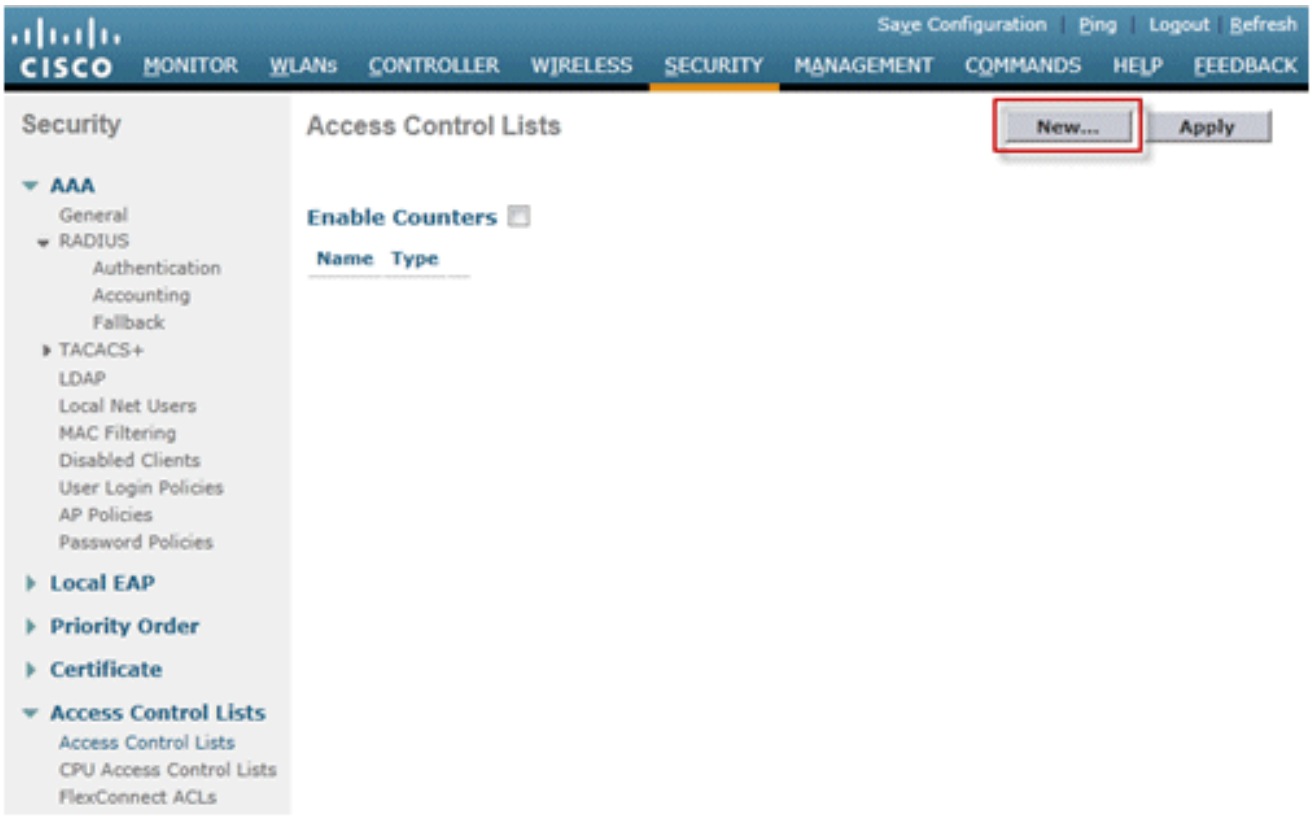
Configurar o IPv6 RA Guard

Navegue até a guia **Controller** e depois **IPv6 > RA Guard** no menu à esquerda. **Ative o** IPv6 RA Guard no AP. O RA Guard no controlador não pode ser desativado. Além da configuração do RA Guard, esta página também mostra todos os clientes que foram identificados como enviando RAs.



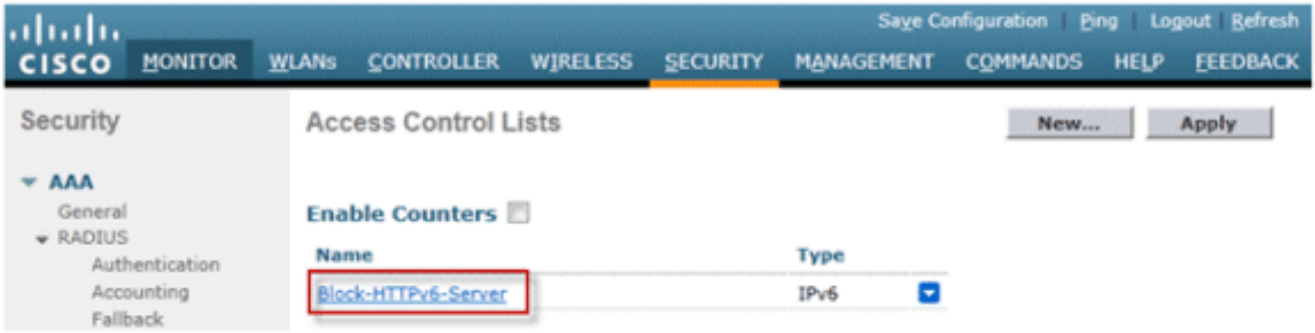
Configurar Listas de Controle de Acesso IPv6

1. Vá até a guia **Segurança**, abra **Listas de controle de acesso** e clique em **Novo**.

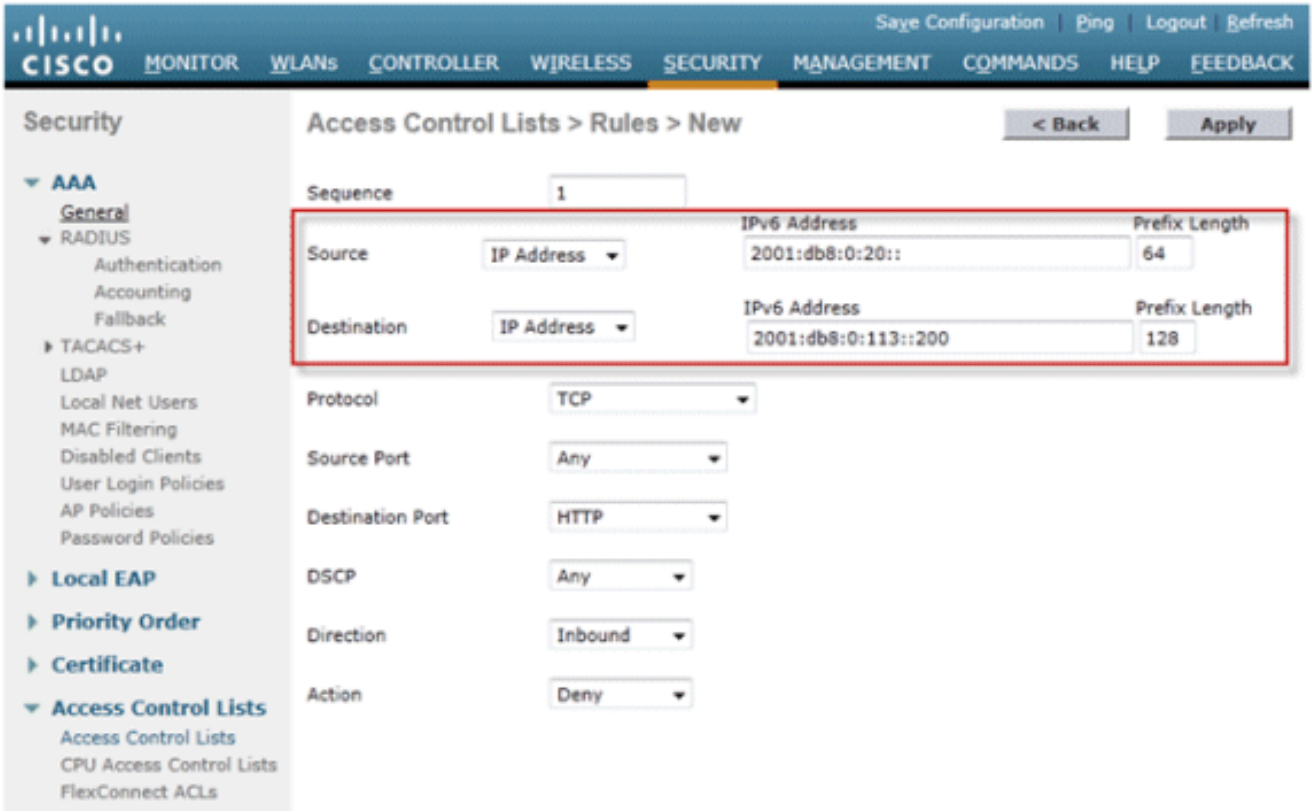


2. Insira um nome exclusivo para a ACL, altere o Tipo de ACL para **IPv6** e clique em **Aplicar**.

3. Clique na nova ACL criada nas etapas acima.

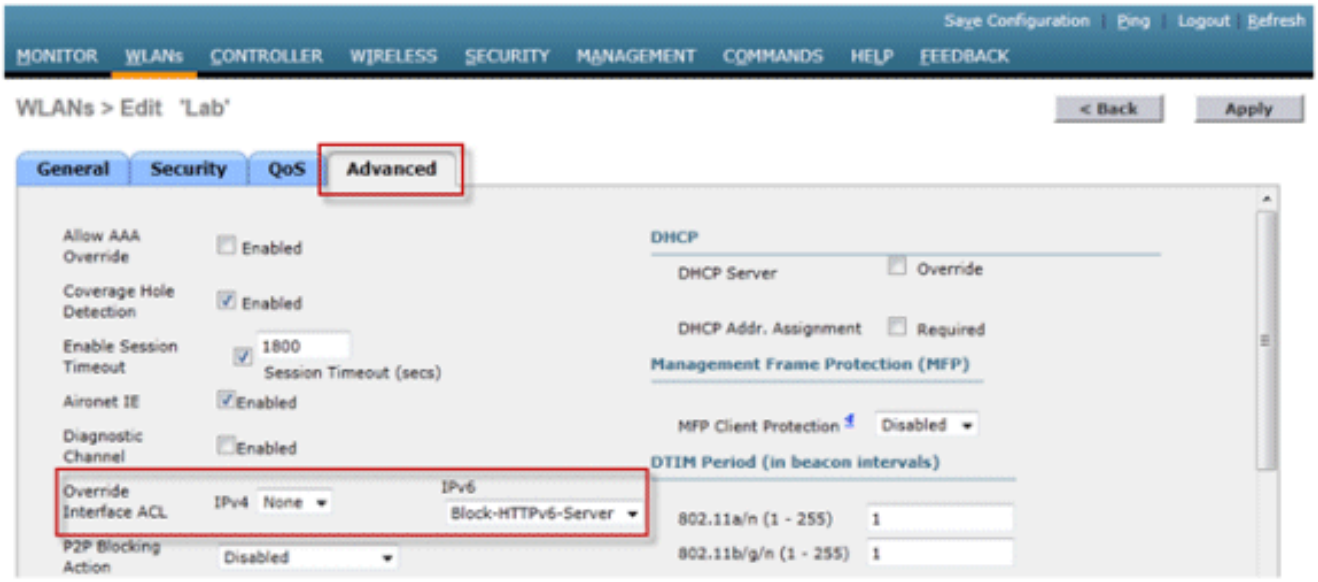


4. Clique em **Adicionar nova regra**, insira os parâmetros desejados para a regra e clique em **Aplicar**. Deixe o número de sequência em branco para colocar a regra no final da lista. A opção "Direção" de "Entrada" é usada para o tráfego proveniente da rede sem fio e "Saída" para o tráfego destinado a clientes sem fio. Lembre-se de que a última regra em uma ACL é um deny-all implícito. Use um comprimento de prefixo de 64 para corresponder a uma sub-rede IPv6 inteira e um comprimento de prefixo de 128 para restringir exclusivamente o acesso a um endereço
individual.



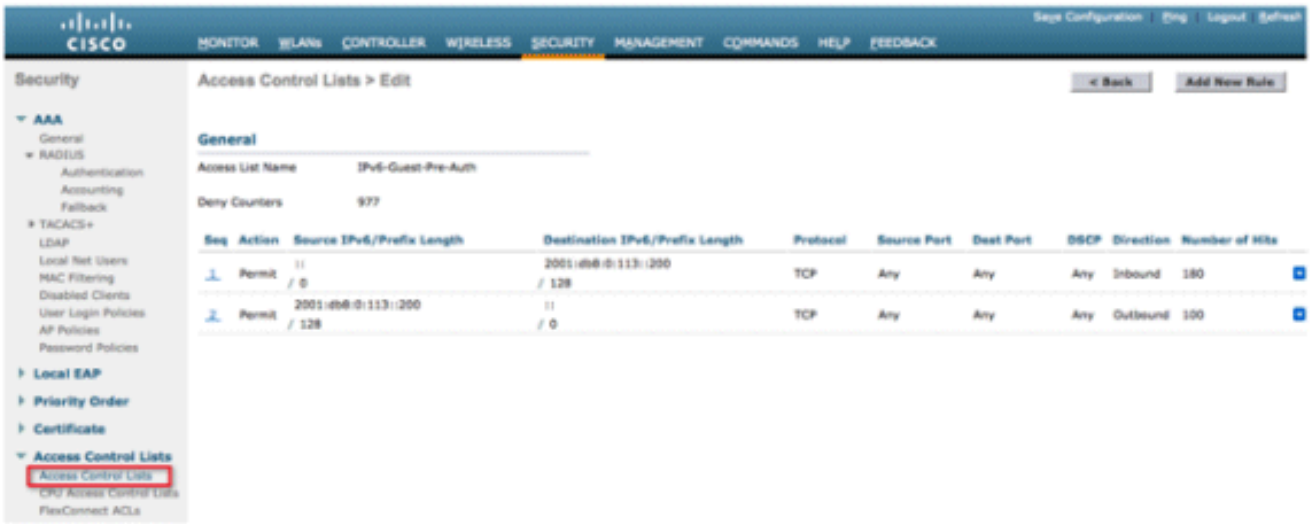
5. As ACLs IPv6 são aplicadas por WLAN/SSID e podem ser usadas em várias WLANs simultaneamente. Navegue até a guia **WLANs** e clique no ID da WLAN do SSID em questão

para aplicar a ACL IPv6. Clique na guia **Avançado** e altere a ACL de interface de substituição para IPv6 para o nome da ACL.

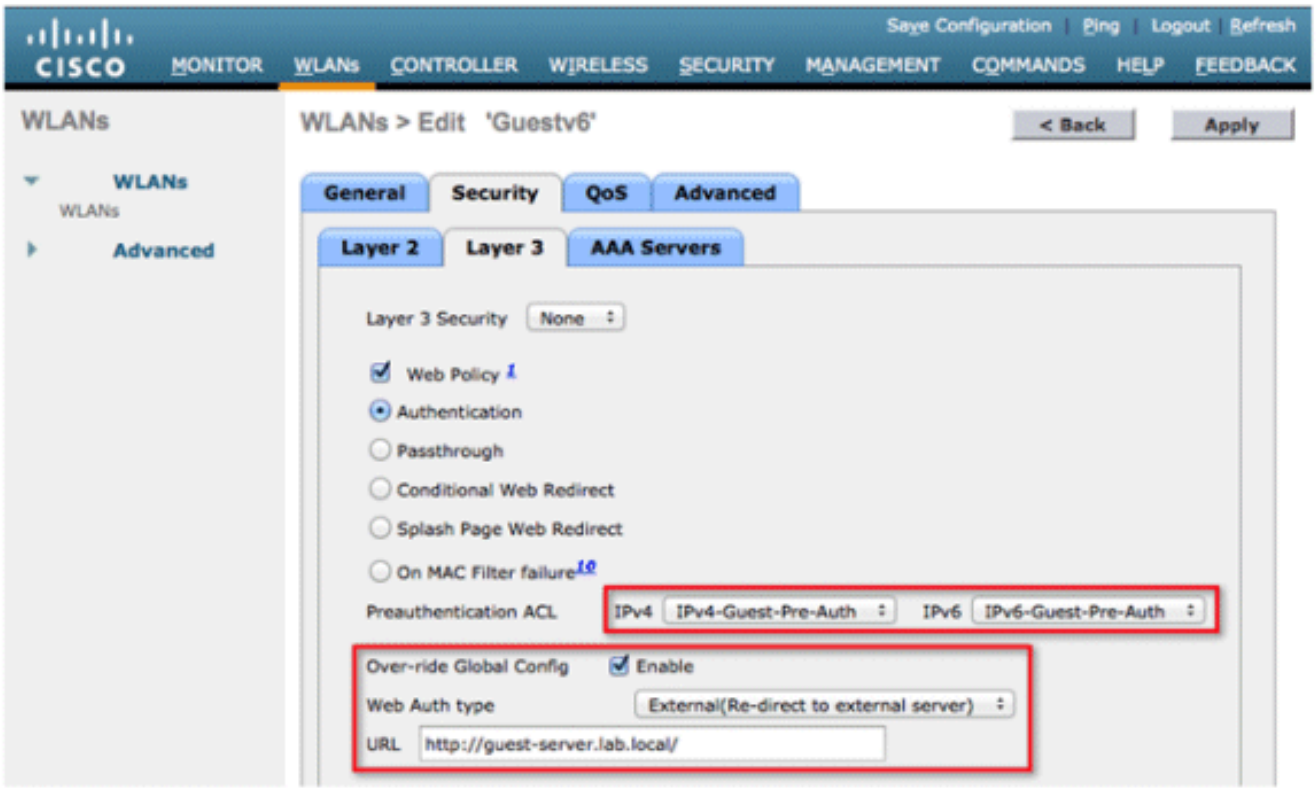


Configurar o acesso de convidado IPv6 para autenticação da Web externa

1. Configure a ACL de pré-autenticação IPv4 e IPv6 para o servidor Web. Isso permite o tráfego de e para o servidor externo antes que o cliente seja totalmente autenticado.

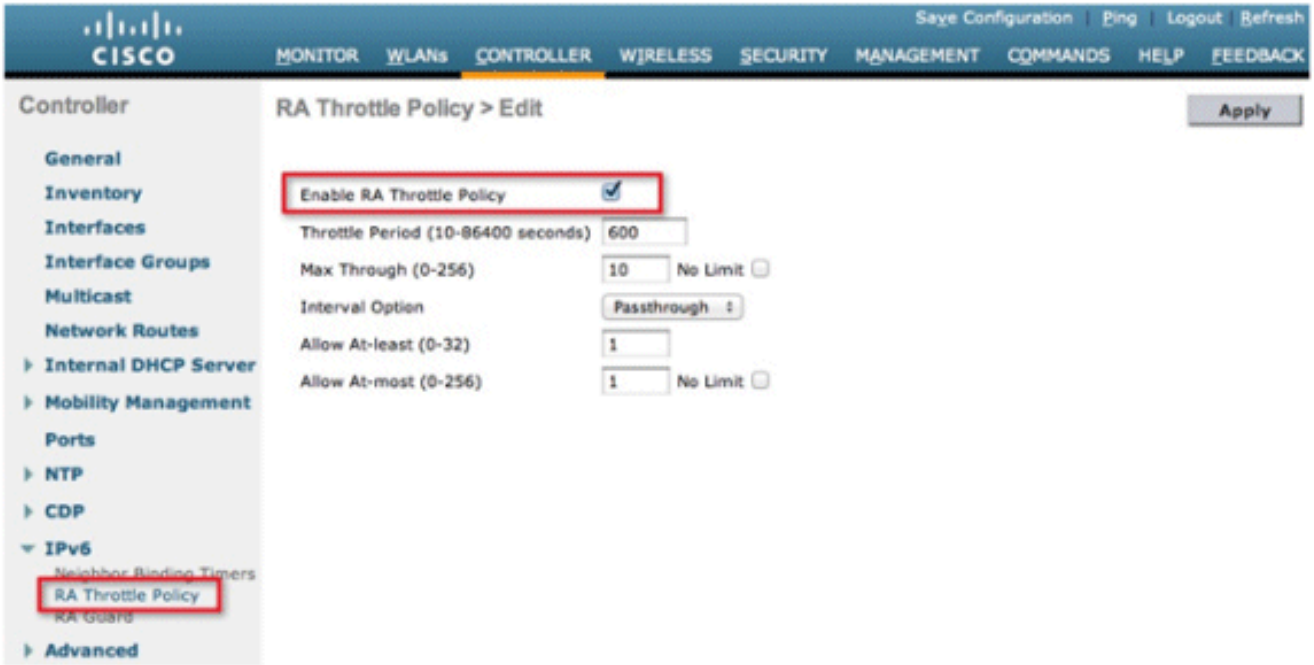


   Para obter mais informações sobre a operação do acesso externo à Web, consulte Exemplo de Configuração de Autenticação Externa da Web com Controladoras Wireless LAN.
2. Configure a Guest WLAN navegando até a guia WLAN na parte superior. Crie o SSID convidado e use uma política da Web de Camada 3. As ACLs de pré-autenticação definidas na Etapa 1 são selecionadas para IPv4 e IPv6. Marque a seção Over-ride Global Config e selecione **External** na caixa suspensa Web Auth type. Insira a URL do servidor Web. O nome de host do servidor externo deve poder ser resolvido no DNS IPv4 e IPv6.



Configurar a limitação de RA IPv6

1. Navegue até o menu de nível superior **Controller** e clique na opção **IPv6 > RA Throttle Policy** no lado esquerdo. Habilite a limitação de RA clicando na caixa de seleção.



Observação: quando ocorre a limitação de RA, somente o primeiro roteador com capacidade para IPv6 pode passar. Para redes com vários prefixos IPv6 que estão sendo atendidos por roteadores diferentes, a limitação do RA deve ser desabilitada.

2. Ajuste o período de aceleração e outras opções somente sob orientação do TAC. No entanto, o padrão é recomendado para a maioria das implantações. As várias opções de configuração da política de Limitação de RA devem ser ajustadas com isso em mente:Os valores numéricos de "Permitir pelo menos" devem ser menores que "Permitir no máximo",

que deve ser menor que "Máximo até".A política de limitação de RA não deve usar um período de limitação superior a 1800 segundos, pois esse é o tempo de vida padrão da maioria dos RAs.

Cada opção de Limitação de RA é descrita abaixo:

- Período de Aceleração - O período de tempo em que a limitação ocorre. A limitação do RA entra em vigor somente depois que o limite "Max Through" é atingido para a VLAN.
- Max Through - Esse é o número máximo de RAs por VLAN antes de a limitação começar. A opção "No Limit" permite uma quantidade ilimitada de RAs sem limitação.
- Opção Interval - A opção interval permite que o controlador atue de forma diferente com base no valor RFC 3775 definido no RA IPv6.Passagem - Este valor permite que qualquer RA com uma opção de intervalo RFC3775 passe sem limitação.Ignorar - esse valor fará com que o acelerador de RA trate pacotes com a opção de intervalo como um RA regular e estará sujeito à limitação se estiver em vigor.Aceleração - Esse valor fará com que os RAs com a opção de intervalo estejam sempre sujeitos à limitação de taxa.
- Permitir pelo menos - O número mínimo de RAs por roteador que serão enviados como multicast.
- Permitir no máximo - O número máximo de RAs por roteador que serão enviados como multicast antes que a limitação entre em vigor. A opção "No Limit" permitirá a passagem de um número ilimitado de RAs para esse roteador.

Configurar a Tabela de Associação de Vizinhos IPv6

1. Vá para o menu de nível superior da controladora e clique em **IPv6 > Neighbor Binding Timers** no menu à
esquerda.

2. Ajuste Down Lifetime, Reachable Lifetime e Stale Lifetime conforme necessário. Para implantações com clientes altamente móveis, os temporizadores de um temporizador de endereço obsoleto devem ser ajustados. Os valores recomendados são:Tempo de vida inativo - 30 segundosTempo de vida acessível - 300 segundosVida útil do estado - 86400 segundosCada temporizador de vida útil se refere ao estado em que um endereço IPv6 pode estar:**Down Lifetime** - O temporizador de inatividade especifica quanto tempo as entradas de cache IPv6 devem ser mantidas se a interface de uplink do controlador ficar inativa.**Tempo de vida acessível** - Esse temporizador especifica quanto tempo um endereço IPv6 será marcado como ativo, o que significa que o tráfego foi recebido desse endereço recentemente. Quando esse temporizador expirar, o endereço será movido para o status "Obsoleto".**Tempo de Vida Obsoleto** - Esse temporizador especifica por quanto tempo manter endereços IPv6 no cache que não foram vistos dentro do "Tempo de Vida Acessível". Após esse tempo de vida, o endereço é removido da tabela de ligação.

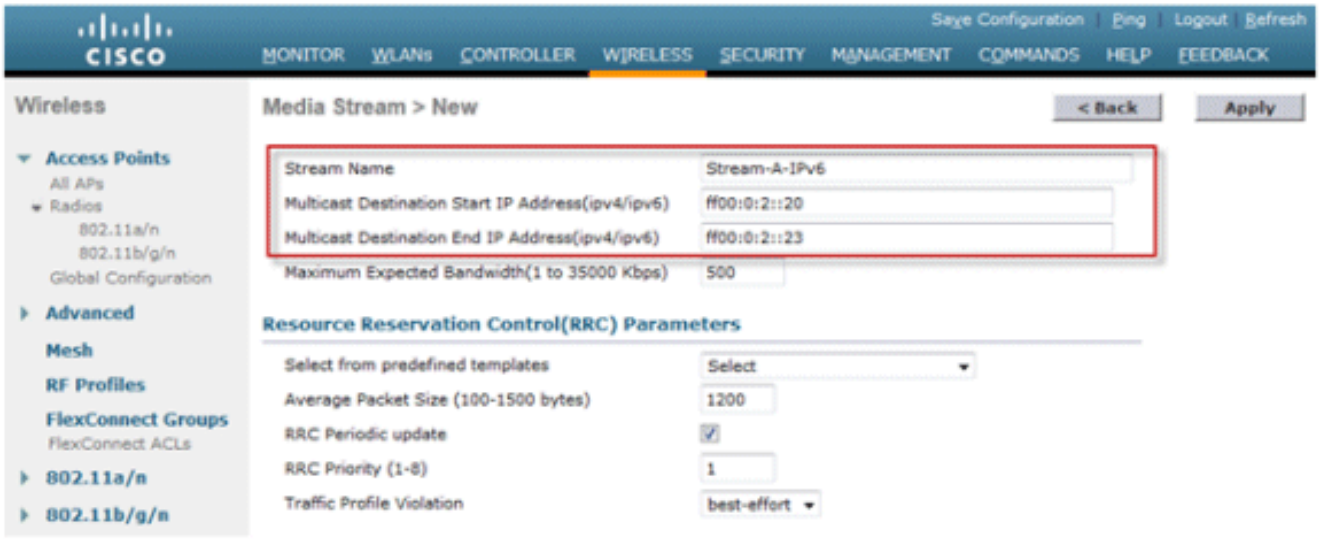
Configurar VideoStream IPv6

1. Verifique se os recursos Global VideoStream estão habilitados no controlador. Consulte a

Solução Cisco Unified Wireless Network: Guia de implantação do VideoStream para obter informações sobre como habilitar o VideoStream na rede 802.11a/g/n, bem como o SSID da WLAN.

2. Vá até a guia **Wireless** no controlador e, no menu à esquerda, escolha **Media Stream > Streams**. Clique em **Add New** para criar um novo fluxo.

3. Nomeie o fluxo e insira os endereços IPv6 inicial e final. Ao usar apenas um único fluxo, os endereços inicial e final são iguais. Depois de adicionar os endereços, clique em **Apply** para criar o fluxo.



Solucionar problemas de conectividade do cliente IPv6

Determinados clientes não podem passar tráfego IPv6

Algumas implementações da pilha de rede IPv6 do cliente não se anunciam corretamente ao entrar na rede e, portanto, seu endereço não é rastreado adequadamente pelo controlador para colocação na tabela de ligação de vizinhos. Todos os endereços que não estão presentes na tabela de ligação de vizinhos são bloqueados de acordo com o recurso de proteção de origem

IPv6. Para permitir que esses clientes passem tráfego, estas opções precisam ser configuradas:

1. Desative o recurso de proteção de origem IPv6 por meio da CLI:

   config network ip-mac-binding disable

2. Habilitar Encaminhamento de Solicitação de Vizinho Multicast via CLI:

   config ipv6 ns-mcast-fwd enable

Verifique se o roaming de camada 3 teve êxito para um cliente IPv6:

Emita estes comandos **debug** na âncora e na controladora externa:

debug client

debug mobility handoff enable

debug mobility packet enable

Depurar resultados no controlador de âncora:

```
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
```

Depurar resultados em 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 CLI IPv6 úteis:

Show ipv6 neighbor-binding summary

Debug ipv6 neighbor-binding filter client enable

Debug ipv6 neighbor-binding filter errors enable

Perguntas mais freqüentes

P: Qual é o tamanho de prefixo IPv6 ideal para limitar o domínio de broadcast?

R: Embora uma sub-rede IPv6 possa ser subdividida abaixo de um /64, essa configuração interromperá o SLAAC e causará problemas com a conectividade do cliente. Se a segmentação for necessária para reduzir o número de hosts, o recurso Grupos de interface pode ser usado para balancear a carga de clientes entre VLANs de back-end diferentes, cada um usando um prefixo IPv6 diferente.

P: Há alguma limitação de escalabilidade quando se trata de oferecer suporte a clientes IPv6?

R: A principal limitação de escalabilidade para suporte ao cliente IPv6 é a tabela de vinculação de vizinhos que controla todos os endereços IPv6 do cliente sem fio. Esta tabela é escalada por plataforma de controlador para suportar o número máximo de clientes multiplicado por oito (o número máximo de endereços por cliente). A adição da tabela de vinculação IPv6 pode elevar o uso de memória do controlador em cerca de 10 a 15% sob carga total, dependendo da plataforma.

Controlador sem fio	Número máximo de clientes	Tamanho da Tabela de Associação de Vizinhos IPv6
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

P: Qual é o impacto dos recursos IPv6 na CPU e na memória do controlador?

R: O impacto é mínimo, pois a CPU tem vários núcleos para processar o plano de controle. Quando testado com o máximo de clientes suportados, cada um com 8 endereços IPv6, o uso da CPU foi inferior a 30% e o uso da memória foi inferior a 75%.

P: O suporte ao cliente IPv6 pode ser desativado?

R: Para clientes que desejam ativar somente o IPv4 em sua rede e bloquear o IPv6, uma ACL IPv6 de tráfego deny-all pode ser usada e aplicada por WLAN.

P: É possível ter uma WLAN para IPv4 e outra para IPv6?

R: Não é possível ter o mesmo nome SSID e tipo de segurança para duas WLANs diferentes operando no mesmo AP. Para segmentação de clientes IPv4 de clientes IPv6, duas WLANs devem ser criadas. Cada WLAN deve ser configurada com uma ACL que bloqueie todo o tráfego IPv4 ou IPv6, respectivamente.

P: Por que é importante suportar vários endereços IPv6 por cliente?

R: Os clientes podem ter vários endereços IPv6 por interface, que podem ser estáticos, SLAAC ou DHCPv6 atribuídos, além de sempre ter um endereço de link local autoatribuído. Os clientes também podem ter endereços adicionais usando prefixos IPv6 diferentes.

P: O que são endereços IPv6 privados e por que eles são importantes para rastrear?

R: Os endereços privados (também conhecidos como temporários) são gerados aleatoriamente pelo cliente quando a atribuição de endereço SLAAC está em uso. Esses endereços são frequentemente girados em uma frequência de um dia ou mais, para evitar a rastreabilidade de host que viria de usar o mesmo sufixo de host (últimos 64 bits) em todos os momentos. É importante rastrear esses endereços privados para fins de auditoria, como rastrear violações de direitos autorais. O Cisco NCS registra todos os endereços IPv6 em uso por cada cliente e os registra historicamente cada vez que o cliente faz roaming ou estabelece uma nova sessão. Esses registros podem ser configurados no NCS para serem mantidos por até um ano.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.