Implemente o IPv6 no acesso definido por software

Contents

Introdução

Este documento descreve como implementar o IPv6 no Cisco® Software-Defined Access (SD-Access).

Informações de Apoio

O IPv4 foi lançado em 1983 e ainda está em uso para a maioria do tráfego da Internet. O endereçamento IPv4 de 32 bits permitiu mais de 4 bilhões de combinações exclusivas. No entanto, devido ao aumento no número de clientes conectados à Internet, há uma falta de endereços IPv4 exclusivos. Nos anos 90, o esgotamento do endereçamento IPv4 tornou-se inevitável.
Antecipando isso, a Internet Engineering Taskforce introduziu o padrão IPv6. O IPv6 utiliza 128 bits e oferece 340 undecilhões de endereços IP exclusivos, o que é mais do que suficiente para atender à necessidade de dispositivos conectados que crescem. Como cada vez mais dispositivos de ponto final modernos suportam pilha dupla e/ou pilha única de IPv6, é crucial para qualquer organização estar pronta para a adoção do IPv6. Isso significa que toda a infraestrutura

deve estar pronta para o IPv6. O Cisco SD-Access é a evolução dos projetos de campus tradicionais para as redes que implementam diretamente o objetivo de uma organização. As Cisco Software Defined Networks agora estão prontas para integrar dispositivos de pilha dupla (IPv6).

Um grande desafio para qualquer organização na adoção do IPV6 é o gerenciamento de alterações e as complexidades associadas à migração de sistemas IPv4 legados para o IPv6. Este documento abrange todos os detalhes sobre o suporte de recursos do IPv6 no SDN da Cisco, na estratégia e nos pontos críticos, que precisam ser tratados quando você adota o IPv6 com as redes definidas por software da Cisco.

Em agosto de 2019, o Cisco Digital Network Architecture (DNA) Center versão 1.3 foi introduzido pela primeira vez com o suporte do IPv6. Nesta versão, a rede de campus Cisco SD-Access suportava o endereço IP do host com clientes com e sem fio em IPv4, IPv6 ou IPv4v6 Dual-stack da rede de estrutura de sobreposição. A solução é evoluir continuamente para trazer novos recursos e funcionalidades que integrem facilmente o IPv6 para qualquer empresa.

Cisco SD-Access com arquitetura IPv6

A tecnologia de estrutura, parte integrante do SD-Access, fornece redes de campus com e sem fio com sobreposições programáveis e virtualização de rede fácil de implantar, que permitem que uma rede física hospede uma ou mais redes lógicas para atender ao objetivo do projeto. Além da virtualização de rede, a tecnologia de estrutura na rede do campus melhora o controle das comunicações, o que fornece segmentação definida por software e aplicação de políticas com base na identidade do usuário e na associação do grupo. Toda a solução de SDN da Cisco é executada no DNA da malha. Portanto, é fundamental entender cada pilar da solução com relação ao suporte IPv6.

- Subcamada - A funcionalidade IPv6 para Sobreposição depende da subcamada, pois a sobreposição IPv6 usa o endereçamento IP de subcamada IPv4 para criar o plano de controle do Locator/ID Separation Protocol (LISP) e túneis do plano de dados da Virtual Extensible LAN (VXLAN). Você sempre pode habilitar a pilha dupla para o protocolo de roteamento subjacente, apenas o LISP de sobreposição de acesso SD depende do roteamento IPv4.
- Sobreposição - Quando se trata de sobreposição, o SD-Access oferece suporte a endpoints com e sem fio somente IPv6. Esse tráfego IPv6 é encapsulado no cabeçalho IPv4 e VXLAN na estrutura SD-Access até que atinjam os nós de borda da estrutura. Os nós de borda de estrutura desencapsulam o cabeçalho IPv4 e VXLAN, que segue o processo de roteamento unicast IPv6 normal a partir de então.
- Nós do plano de controle - O nó do plano de controle é configurado para permitir que todas as sub-redes de host IPv6 e as rotas de host /128 dentro dos intervalos de sub-rede sejam registradas em seu banco de dados de mapeamento.
- Nós de borda - Nos nós de borda, o peering BGP IPv6 com dispositivos de fusão está habilitado. O nó de borda desencapsula o cabeçalho IPv4 do tráfego de saída de estrutura, enquanto o tráfego IPv6 de entrada é encapsulado com o cabeçalho IPv4 pelos nós de

borda também.

- Borda de malha - todas as interfaces virtuais comutadas (SVIs) configuradas na Borda de malha devem ser IPv6. Essa configuração é enviada pelo Controlador do DNA Center.
- Cisco DNA Center - As interfaces físicas do Cisco DNA Center não são compatíveis com pilha dupla no momento em que este documento é publicado. Ele só pode ser implantado em uma única pilha com IPv4 ou IPv6 apenas nas interfaces de gerenciamento e/ou corporativas do DNA Center.
- Clientes - O Cisco SD-Access oferece suporte a pilha dupla (IPv4 e IPv6) ou pilha única IPv4 ou IPv6. No entanto, no caso de uma pilha única IPv6 implantada, o DNA Center ainda precisará criar um pool de pilha dupla para oferecer suporte a um cliente somente IPv6. O IPv4 no pool de pilha dupla é um endereço fictício apenas porque o IPv6 do cliente deve desabilitar o endereço IPv4.

Arquitetura de sobreposição de IPv6 no Cisco Software-Defined Access.

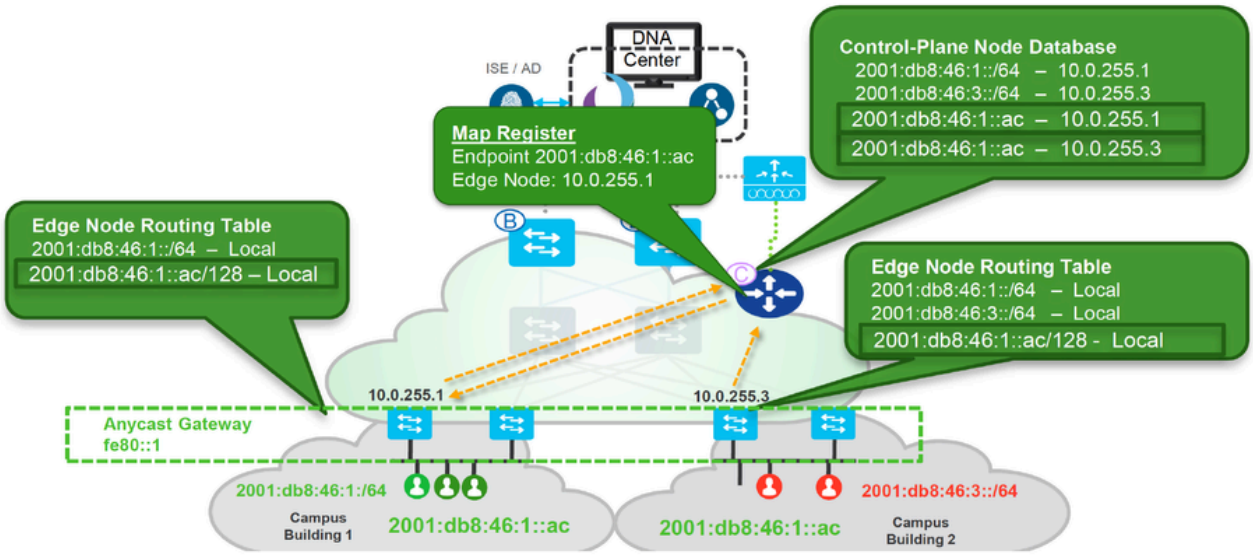


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

Arquitetura de sobreposição de IPv6

Ative o IPv6 com o Cisco DNA-Center

Há duas maneiras de ativar o pool IPv6 no Cisco DNA Center:
1. Crie um novo Pool IPv4/v6 de pilha dupla - iniciante
2. Edite o IPv6 no pool IPv4 que já existe - migração de campo inativo

A versão atual (até 2.3.x) do DNA Center não oferece suporte a IPv6. Apenas um pool, se o usuário planeja oferecer suporte a um único cliente somente de endereço IPv6 nativo/único. Um endereço IPv4 fictício precisa ser associado ao pool IPv6. Observe que no pool IPv4 implantado

que já existe com um site associado a ele e edite o pool com um endereço IPv6. O DNA Center oferece a opção de migração para a malha de acesso SD, que exige que o usuário reprovisione a malha para esse local. Um indicador de aviso é exibido na estrutura à qual o local pertence e indica que a estrutura precisa "reconfigurar a estrutura". Veja estas imagens para obter exemplos:

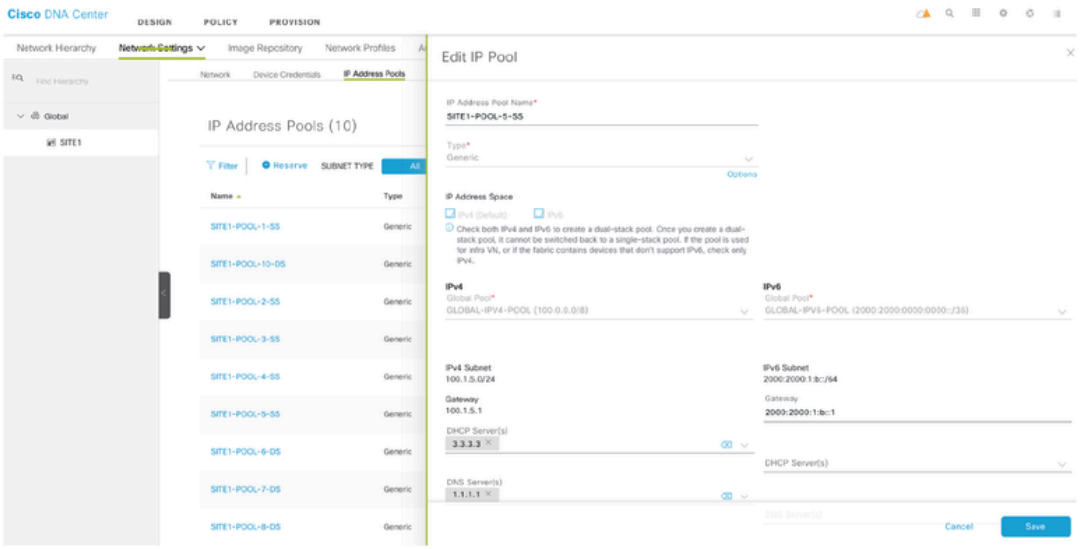


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

Atualização de pool IPv4 único para pool de pilha dupla editando a opção de pool IPv4

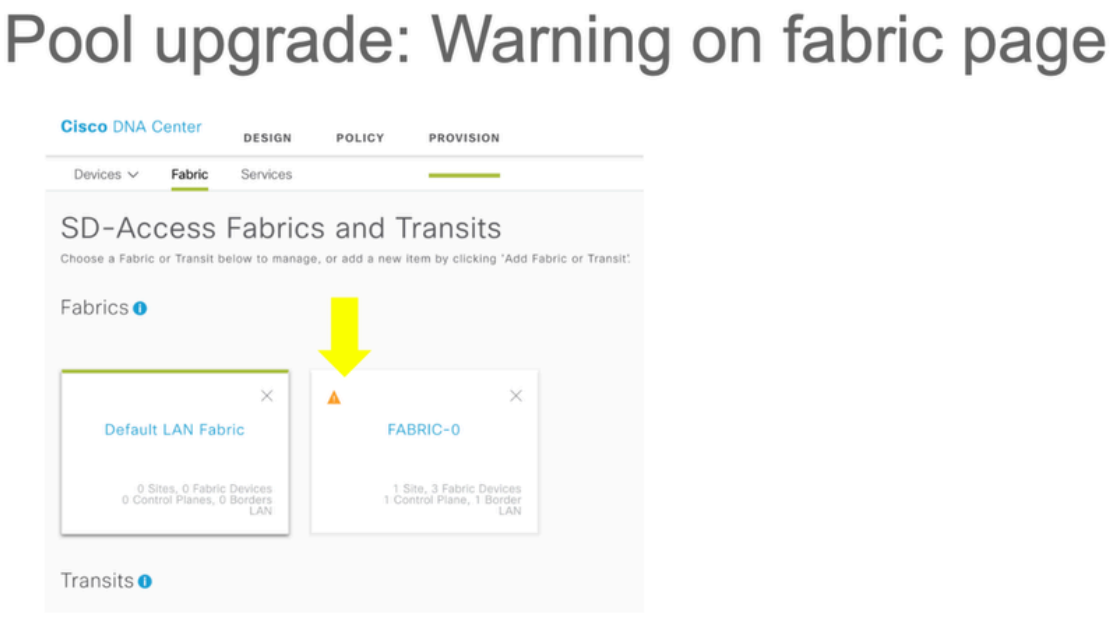


Figure 3.
Fabric has warning indicator which needs to 'reconfigure the fabric'

A malha tem um indicador de aviso que precisa "reconfigurar a malha"

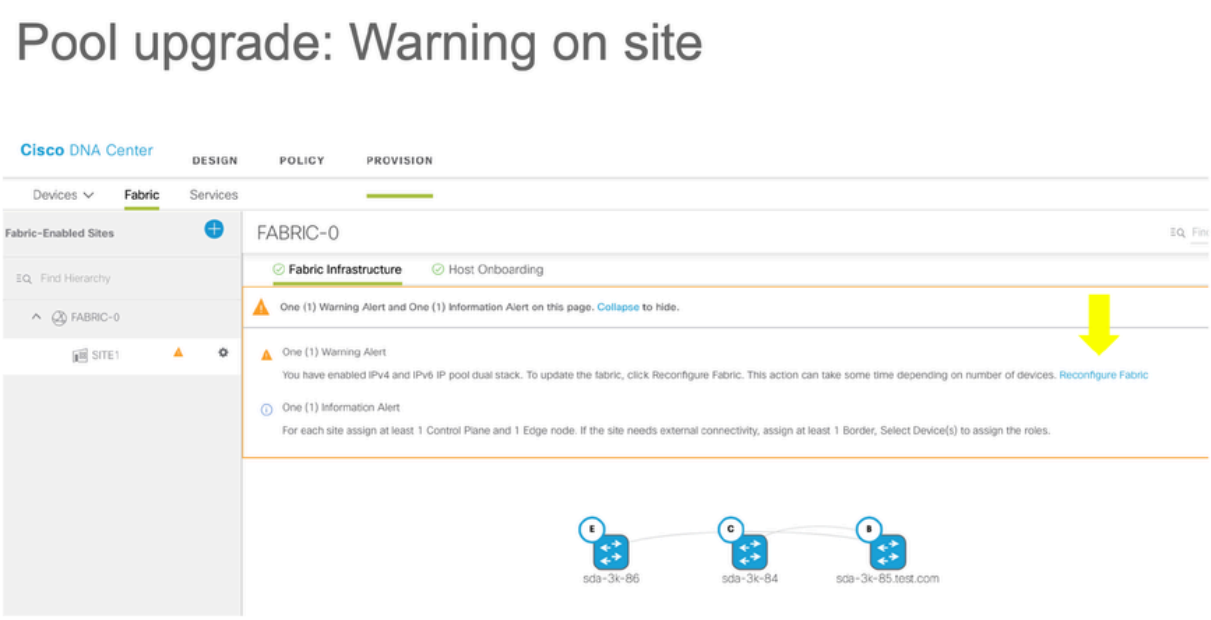


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

O usuário precisa clicar em "reconfigurar estrutura" para reprovisionar automaticamente os nós de estrutura para que a configuração de pilha dupla entre em vigor como parte do processo de migração

Considerações de projeto com IPv6 no Cisco SD-Access

Embora, para os clientes do Cisco SD-Access, eles possam ser executados com configurações de rede de pilha dupla ou somente IPv6, a implementação atual da estrutura do SD-Access com DNA Center Switch (SW) versão até 2.3.x.x tem algumas considerações sobre a implantação do IPv6.

- O Cisco SD-Access oferece suporte a protocolos de roteamento subjacentes IPv4. Assim, o tráfego de cliente IPv6 é transportado quando é encapsulado dentro de cabeçalhos IPv4. Este é um requisito para a implantação de software LISP atual. Mas isso não significa que a subjacência não possa ativar o protocolo de roteamento IPv6, apenas o LISP de sobreposição de acesso SD não é executado em sua dependência.
- Não há suporte para multicast nativo IPv6, pois a estrutura subjacente só pode ser IPv4 no momento.
- O convidado sem fio só pode ser executado com a pilha dupla. Devido à versão atual do Identity Services Engine (ISE) (por exemplo, até 3.2), o portal de convidado IPv6 não é suportado, portanto um cliente convidado somente IPv6 não poderá ser autenticado.
- A automação da Diretiva de QoS do Aplicativo IPv6 não tem suporte na versão atual do DNA Center. Este documento descreve as etapas necessárias para implementar QoS IPv6 para clientes de pilha dupla com e sem fio no Cisco SD-Access que foram implantados para um dos usuários em grande escala.
- O recurso de limitação de taxa de cliente sem fio para tráfego downstream e upstream por Identificador de Conjunto de Serviços (SSID) ou por cliente com base na política é

suportado para IPv4 (TCP/UDP) e IPv6 (somente TCP). Ainda não há suporte para a limitação de taxa de UDP IPv6.
- O pool IPv4 pode ser atualizado para um pool de pilha dupla. Mas um pool de pilha dupla não pode ser submetido a downgrade para um pool IPv4. Se o usuário quiser remover o pool de pilha dupla de volta para o pool de pilha única IPv4, ele precisará liberar todo o pool de pilha dupla.
- Ainda não há suporte para IPv6 único, embora apenas IPv4 ou pool de pilha dupla possa ser criado no DNA Center atual.
- A plataforma do Cisco IOS® XE é um requisito mínimo de versão de software de 16.9.2 e posterior.
- IPv6 Guest wireless ainda não é suportado nas plataformas Cisco IOS XE, enquanto AireOS (8.10.105.0+) suporta uma solução alternativa.
- O pool de pilha dupla não pode ser atribuído no INFRA_VN, onde somente o ponto de acesso (AP) ou o pool de nós estendidos pode ser atribuído.
- A automação de LAN ainda não suporta IPv6.

Além das limitações mencionadas anteriormente, quando você projeta uma malha SD-Access com IPv6 habilitado, você deve sempre manter a escalabilidade de cada componente da malha em mente. Se um ponto de extremidade tiver vários endereços IPv4 ou IPv6, cada endereço será contado como uma entrada individual.

As entradas de host de estrutura incluem pontos de acesso e nós clássicos e estendidos por política.

Considerações adicionais de escala de nó de borda:

As entradas /32 (IPv4) ou /128 (IPv6) são usadas quando o nó de borda encaminha o tráfego de fora da malha para um host na malha.

Para todos os switches, exceto os switches de alto desempenho Cisco Catalyst 9500 Series e os switches Cisco Catalyst 9600 Series:

- O IPv4 usa uma entrada de TCAM (memória endereçável de conteúdo ternário) (entradas de host de estrutura) para cada endereço IP IPv4.
- O IPv6 usa duas entradas TCAM (entradas de host de estrutura) para cada endereço IP IPv6.

Para os switches de alto desempenho Cisco Catalyst 9500 Series e os switches Cisco Catalyst 9600 Series:

- O IPv4 usa uma entrada TCAM (entradas de host de estrutura) para cada endereço IP IPv4.
- O IPv6 usa uma entrada TCAM (entradas de host de estrutura) para cada endereço IP IPv6.

E alguns dos endpoints não suportam DHCPv6, como smartphones baseados em Android OS que dependem da Configuração Automática de Endereço Stateless (SLAAC) para obter endereços IPv6. Um único endpoint pode terminar com mais de dois endereços IPv6. Esse comportamento consome mais recursos de hardware em cada nó de estrutura, especialmente

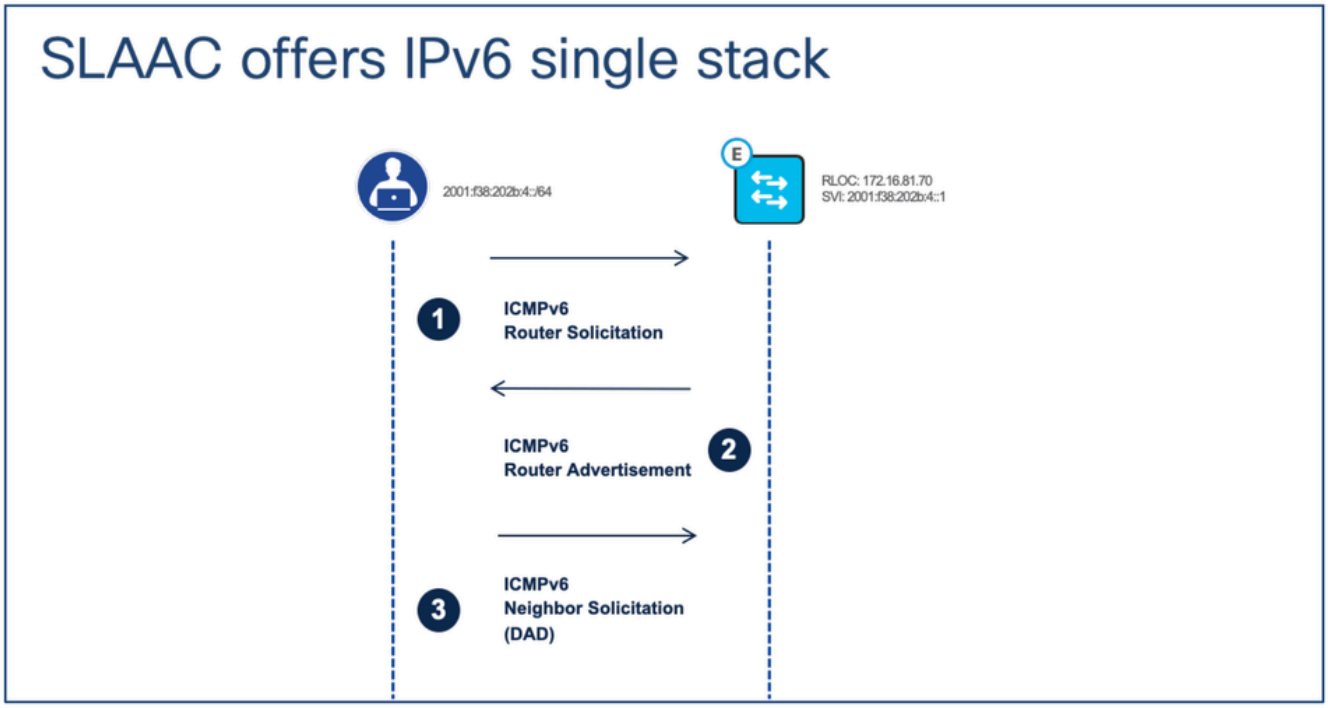
para a borda da estrutura e nós de controle. Por exemplo, sempre que o nó de borda desejar enviar tráfego aos nós de borda para qualquer endpoint, ele instalará uma rota de host na entrada TCAM e gravará uma entrada de adjacência VXLAN no TCAM de Hardware (HW).

Conexões e Fluxos de Chamadas de Clientes com e sem Fio

Depois que o cliente estiver conectado à Borda da malha, haverá diferentes maneiras de obter os endereços IPv6. Esta seção aborda a maneira mais comum de endereçamento IPv6 do cliente, ou seja, SLAAC e DHCPv6.

Atribuição de endereço IPv6 - SLAAC

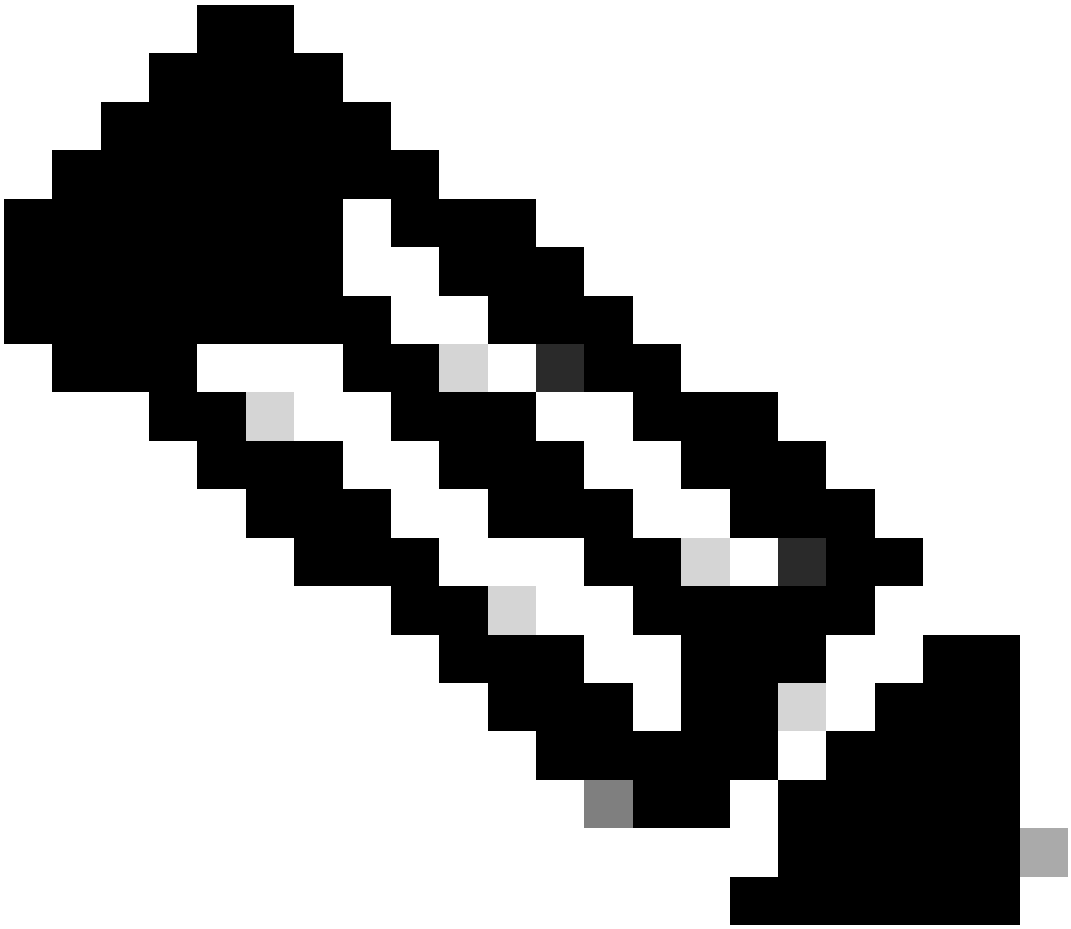
O SLAAC no SDA (Software-Defined Access) não é diferente do fluxo de processo SLAAC padrão. Para que o SLAAC funcione corretamente, o cliente IPv6 deve ser configurado com um endereço de link local em sua interface, como o cliente se configura automaticamente com o endereço de link local está fora do escopo deste documento.



Atribuição de endereço IPv6 - SLAAC

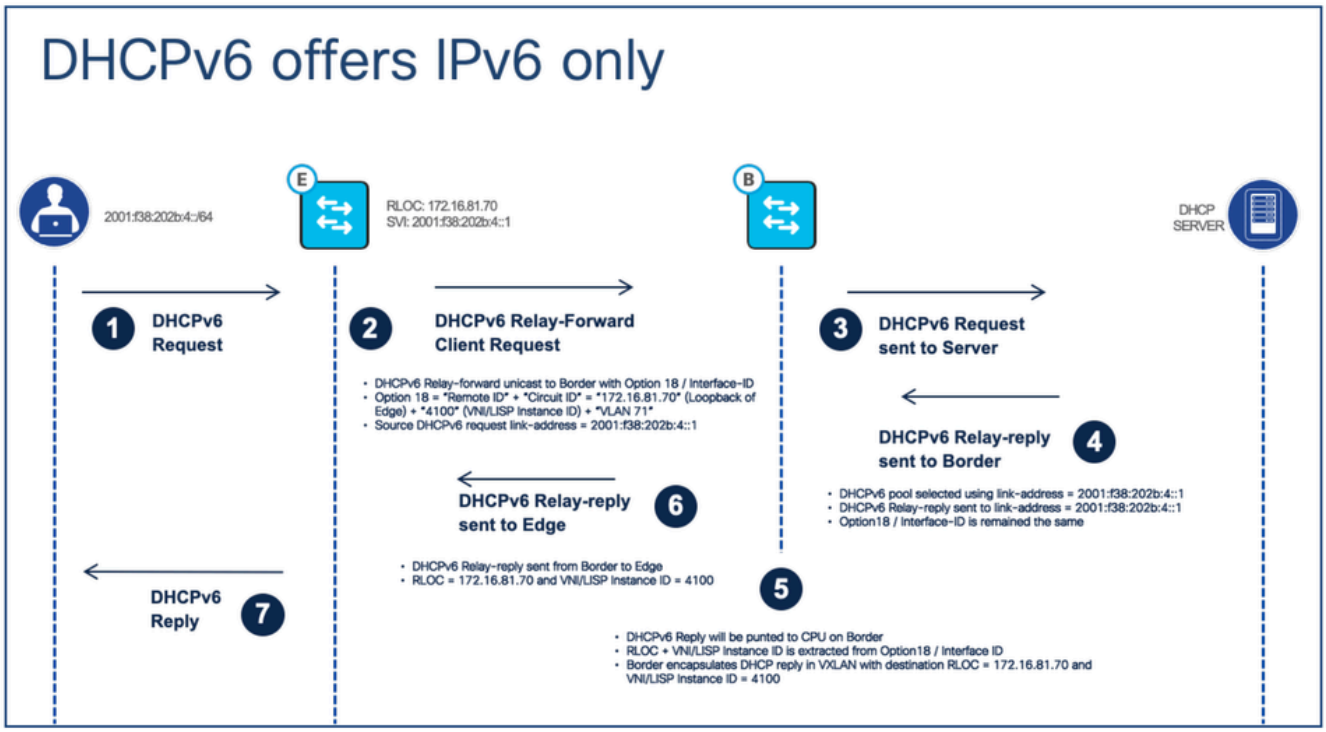
Descrição do fluxo de chamadas:
Etapa 1. Depois que o cliente IPv6 se configura com um endereço de link local IPv6, o cliente envia a mensagem ICMPv6 Router Solicitation (RS) ao Fabric Edge. A finalidade dessa mensagem é obter o prefixo unicast global de seu segmento conectado.
Etapa 2. Depois que a borda da estrutura recebe a mensagem de RS, ela responde com uma mensagem de anúncio de roteador (RA) ICMPv6 que contém o prefixo unicast IPv6 global e seu comprimento interno.
Etapa 3. Depois que o cliente recebe a mensagem do RA, ele combina o prefixo global unicast IPv6 com seu identificador de interface EUI-64 para gerar seu endereço global unicast IPv6

exclusivo e definir seu gateway para o endereço link local do SVI da borda da estrutura que está relacionado ao segmento do cliente. Em seguida, o cliente envia uma mensagem ICMPv6 Neighbor Solicitation para executar a detecção de endereço duplicado (DAD) para garantir que o endereço IPv6 que ele obtém seja exclusivo.



Note: Todas as mensagens relacionadas ao SLAAC são encapsuladas com o endereço link local IPv6 do SVI do cliente e do nó de estrutura.

Atribuição de endereço IPv6 - DHCPv6

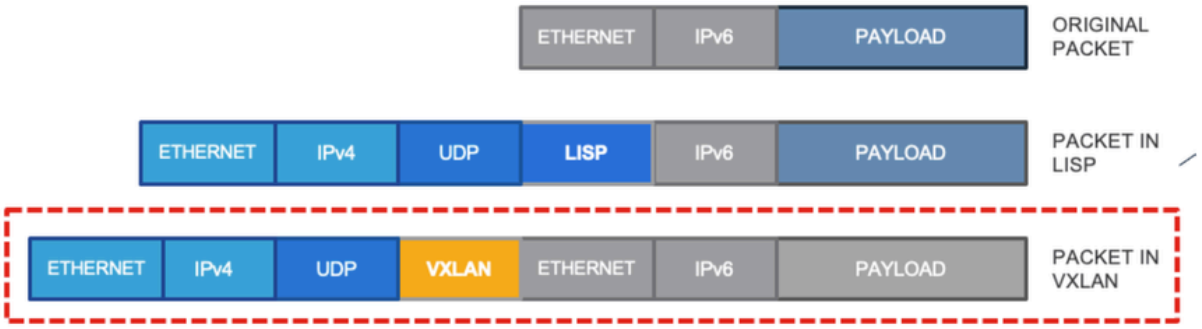


Atribuição de endereço IPv6 - DHCPv6

Descrição do fluxo de chamadas:
Etapa 1. O cliente envia a solicitação DHCPv6 para a borda da malha.
Etapa 2. Quando a borda da malha receber a solicitação de DHCPv6, ela usará a mensagem de encaminhamento de retransmissão de DHCPv6 para transmitir por unicast a solicitação para a borda da malha com a opção 18 de DHCPv6. Em comparação com a opção 82 de DHCP, a opção 18 de DHCPv6 codifica "Circuit ID" e "Remote ID" juntas. O ID/VNI da instância do LISP, o Localizador de roteamento IPv4 (RLOC) e a VLAN do ponto final estão codificando dentro.
Etapa 3. A borda da estrutura desencapsula o cabeçalho da VXLAN e envia por unicast o pacote DHCPv6 para o servidor DHCPv6.
Etapa 4. O servidor DHCPv6 recebe a mensagem de encaminhamento de retransmissão, ele usa o endereço de link de origem (agente de retransmissão DHCPv6/gateway cliente) da mensagem para escolher o pool IPv6 para atribuir o endereço IPv6. Em seguida, envie a mensagem relay-reply de DHCPv6 de volta ao endereço gateway do cliente. A opção 18 permanece inalterada.
Etapa 5. Quando a borda da estrutura recebe a mensagem relay-reply, ela extrai a instância RLOC e LISP/VNI da opção 18. A borda da estrutura encapsula a mensagem relay-reply na VXLAN com um destino que ela extraiu da opção 18.
Etapa 6. A borda da malha envia a mensagem de resposta de retransmissão DHCPv6 para a borda da malha à qual o cliente se conecta.
Etapa 7. Quando a borda da estrutura recebe a mensagem de resposta de relé DHCPv6, ela desencapsula o cabeçalho VXLAN da mensagem e encaminha a mensagem ao cliente. O cliente sabe o endereço IPv6 atribuído.

Comunicação IPv6 no Cisco SD-Access

A comunicação IPv6 usa o plano de controle padrão baseado em LISP e os métodos de comunicação de plano de dados baseados em VXLAN. Com a implementação atual no Cisco SD-Access LISP e VXLAN usa o cabeçalho IPv4 externo para transportar os pacotes IPv6 para dentro. Esta imagem captura este processo.



Cabeçalho IPv4 externo que transporta os pacotes IPv6 para dentro

Isso significa que todas as consultas LISP usam o pacote nativo IPv4, enquanto a tabela de nós do plano de controle tem detalhes sobre o RLOC com os endereços IP IP IPv6 e IPv4 do ponto de extremidade. Esse processo é explicado em detalhes na próxima seção a partir de uma perspectiva de endpoint sem fio.

Comunicação IPv6 sem fio no Cisco SD-Access

A comunicação sem fio depende de dois componentes específicos, Pontos de acesso e controladores de LAN sem fio, além dos componentes típicos da malha de acesso SD da Cisco. Os pontos de acesso sem fio criam um túnel de controle e provisionamento de pontos de acesso sem fio (CAPWAP) com a controladora Wireless LAN (WLC). Enquanto o tráfego do cliente existe na borda da malha, outra comunicação do plano de controle, que inclui estatísticas de rádio, é gerenciada pela WLC. De uma perspectiva do IPv6, a WLC e o AP devem ter os endereços IPv4 e toda a comunicação CAPWAP usa esses endereços IPv4. Enquanto a WLC e o AP sem estrutura suportam a comunicação IPv6, o Cisco SD-Access usa o IPv4 para todas as comunicações que transportam qualquer tráfego IPv6 de cliente dentro de pacotes IPv4. Isso significa que os pools de AP atribuídos no Infra VN não podem ser mapeados com pools de IP que são de pilha dupla e um erro será lançado se qualquer tentativa for feita para esse mapeamento. A comunicação sem fio no Cisco SDA pode ser dividida nestas tarefas principais:

- Integração de ponto de acesso
- Integração do cliente

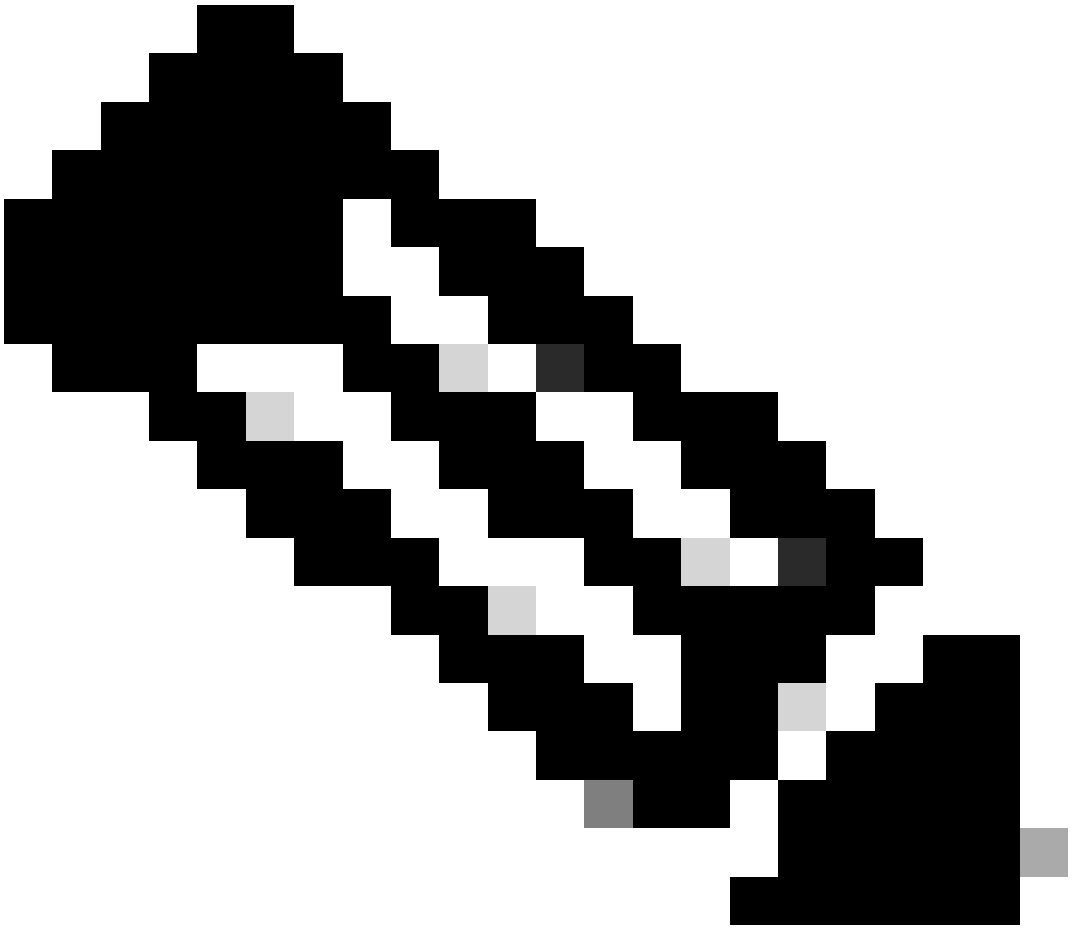
Examine esses eventos de uma perspectiva do IPv6.

Integração de ponto de acesso

Esse processo permanece o mesmo para IPv6 e IPv4, pois tanto a WLC quanto o AP têm

endereços IPv4 e etapas incluídas aqui:
1. A porta Fabric Edge (FE) está configurada para AP integrado.
2. O AP se conecta à porta FE e, via CDP, o AP notifica o FE sobre sua presença (isso permite que o FE atribua a VLAN correta).
3. O AP obtém o endereço IPv4 do servidor DHCP e o FE registra o AP e atualiza o plano de controle (nó do plano de controle (CP)) com os detalhes do AP.
4. O AP une a WLC através de métodos tradicionais (como a Opção de DHCP 43).
5. A WLC verifica se o AP é compatível com a estrutura e consulta o plano de controle para obter informações de RLOC do AP (por exemplo, RLOC solicitado/resposta recebida).
6. CP responde com o IP RLOC do AP para a WLC.
7. A WLC registra o Controle de Acesso ao Meio (MAC) (Endereço) do AP no CP.
8. O CP atualiza o FE com os detalhes do WLC sobre o AP (isso diz ao FE para iniciar o túnel VXLAN com o AP).

O FE processa as informações e cria um túnel VXLAN com o AP. Neste ponto, o AP anuncia o SSID habilitado para malha.

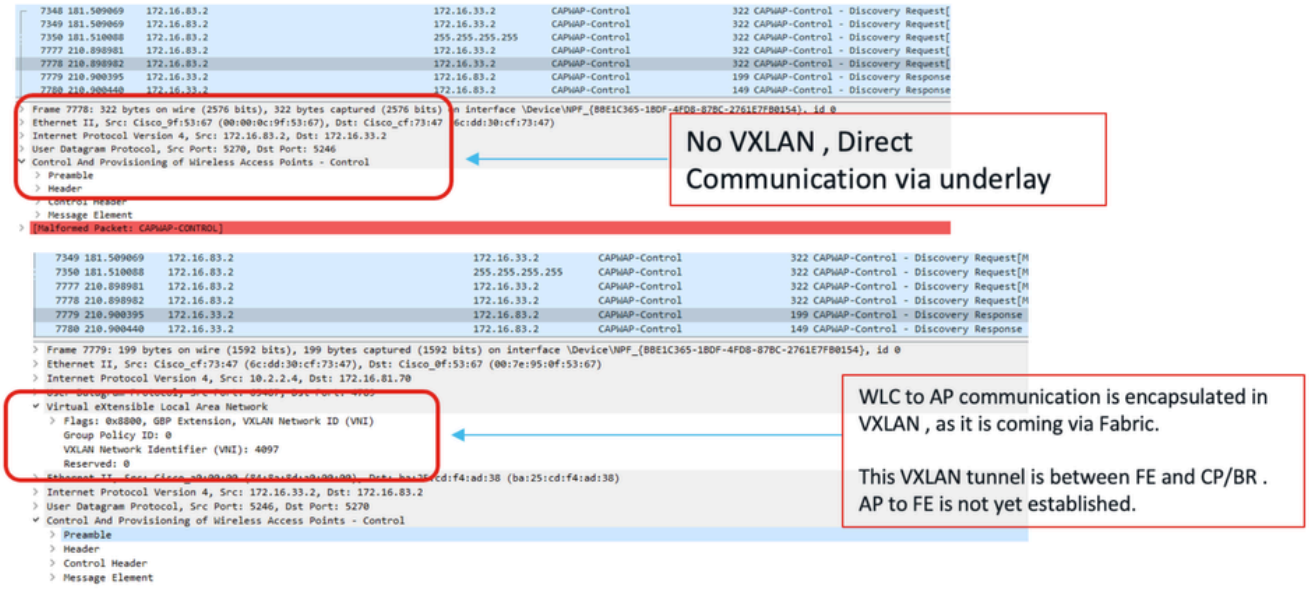


Note: Caso o AP transmita os SSIDs que não são da estrutura e não transmita o SSID da

---

estrutura, verifique o túnel VXLAN entre o ponto de acesso e o nó da borda da estrutura.

Além disso, observe que a comunicação de AP para WLC sempre acontece através de Underlay CAPWAP e toda a comunicação de WLC para AP usa VXLAN CAPWAP via sobreposição. Isso significa que, se você capturar pacotes que vão de AP para WLC, verá apenas CAPWAP enquanto o tráfego reverso tiver um túnel VXLAN. Veja este exemplo para comunicação entre AP e WLC.



Capturas de pacotes de AP para WLC (túnel CAPWAP) vs WLC para AP (túnel VxLAN na estrutura)

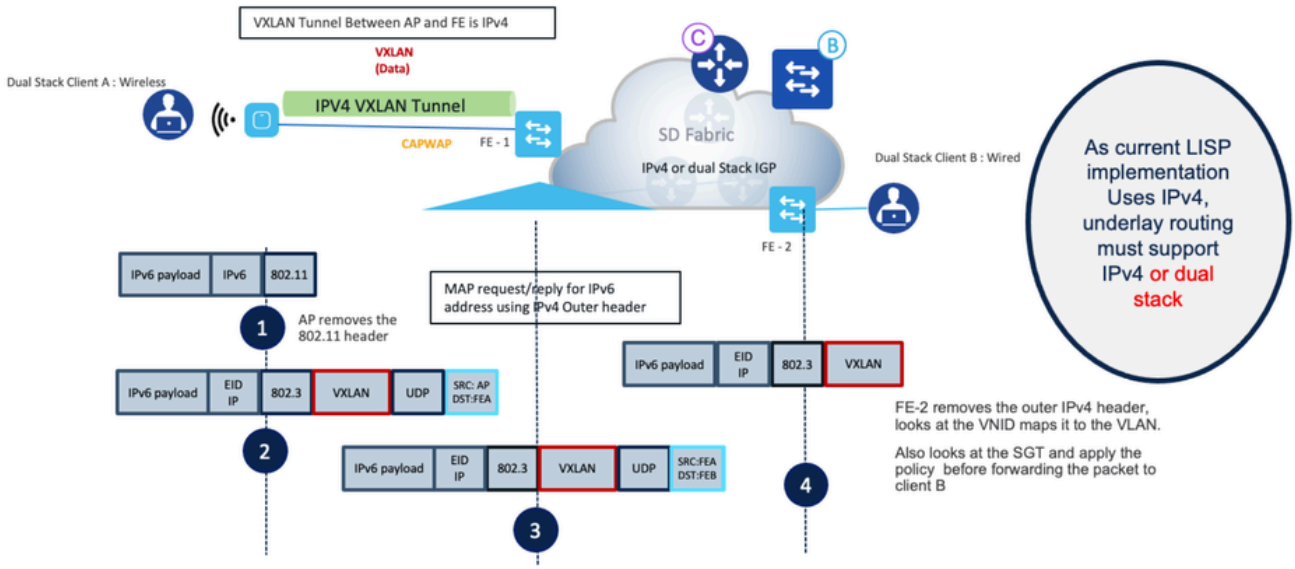
Integração do cliente

O processo de integração do cliente Dual-Stack/IPv6 permanece o mesmo, mas o cliente usa os métodos de atribuição de endereço IPv6, como SLAAC/DHCPv6, para obter os endereços IPv6.
1. O cliente se une à estrutura e ativa o SSID no AP.
2. A WLC conhece o AP RLOC.
3. O Cliente Autentica e a WLC registra os detalhes da L2 do Cliente com o CP e atualiza o AP.
4. O cliente inicia o endereçamento IPv6 a partir dos métodos configurados - SLAAC/DHCPv6.
5. FE dispara o registro de cliente IPv6 para o banco de dados de rastreamento de host (HTDB) CP. O AP para o FE e o FE para outros destinos usam o encapsulamento VXLAN e LISP IPv6 nos quadros IPv4.

Comunicação Cliente-Cliente com IPv6

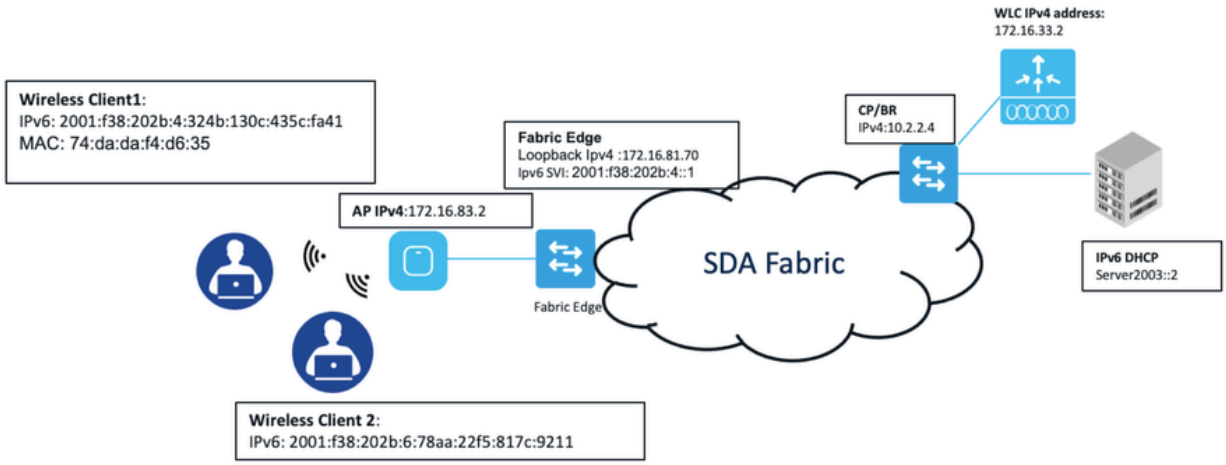
A imagem aqui resume o processo de comunicação do cliente sem fio IPv6 com outro cliente com fio IPv6. (Isso pressupõe que o cliente esteja autenticado e tenha o endereço IPv6 por meio de métodos configurados.)

1. O cliente envia os quadros 802.11 ao AP com payload IPv6.
2. O AP remove os cabeçalhos 802.11 e envia o payload IPv6 original no túnel VXAN IPv4 para a Borda da malha.
3. A Borda de Malha usa a solicitação do Protocolo de Acesso a Mensagens (MAP) para identificar o destino e envia o quadro ao RLOC de destino com VXLAN IPv4.
4. No Switch de destino, o cabeçalho VXLAN IPv4 é removido e o pacote IPv6 é enviado ao cliente.

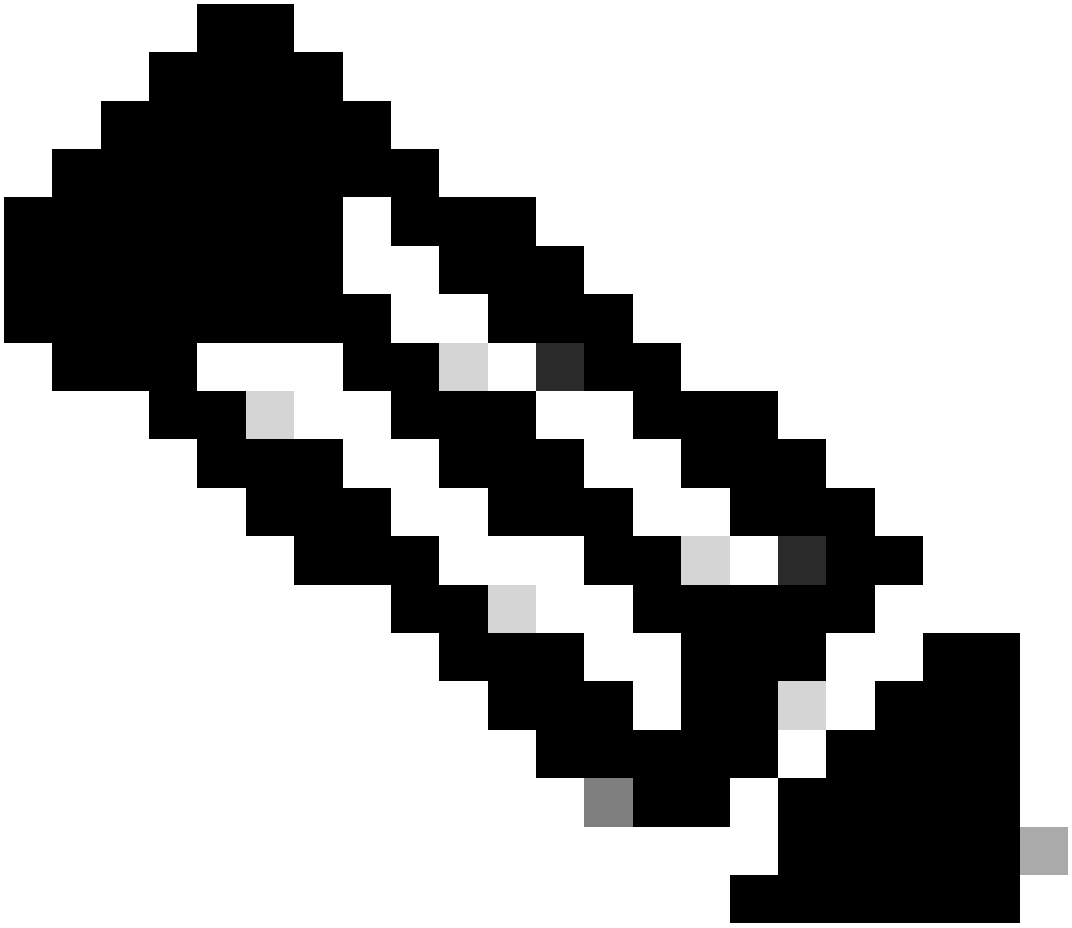


Fluxos de pacotes de cliente sem fio de pilha dupla para cliente com fio de pilha dupla

Examine em detalhes esse processo com as capturas de pacotes e consulte a imagem para obter os detalhes dos endereços IP e MAC. Observe que essa configuração usa clientes Dual-Stack conectados com os mesmos pontos de acesso, mas mapeados com diferentes sub-redes IPv6 (SSIDs).

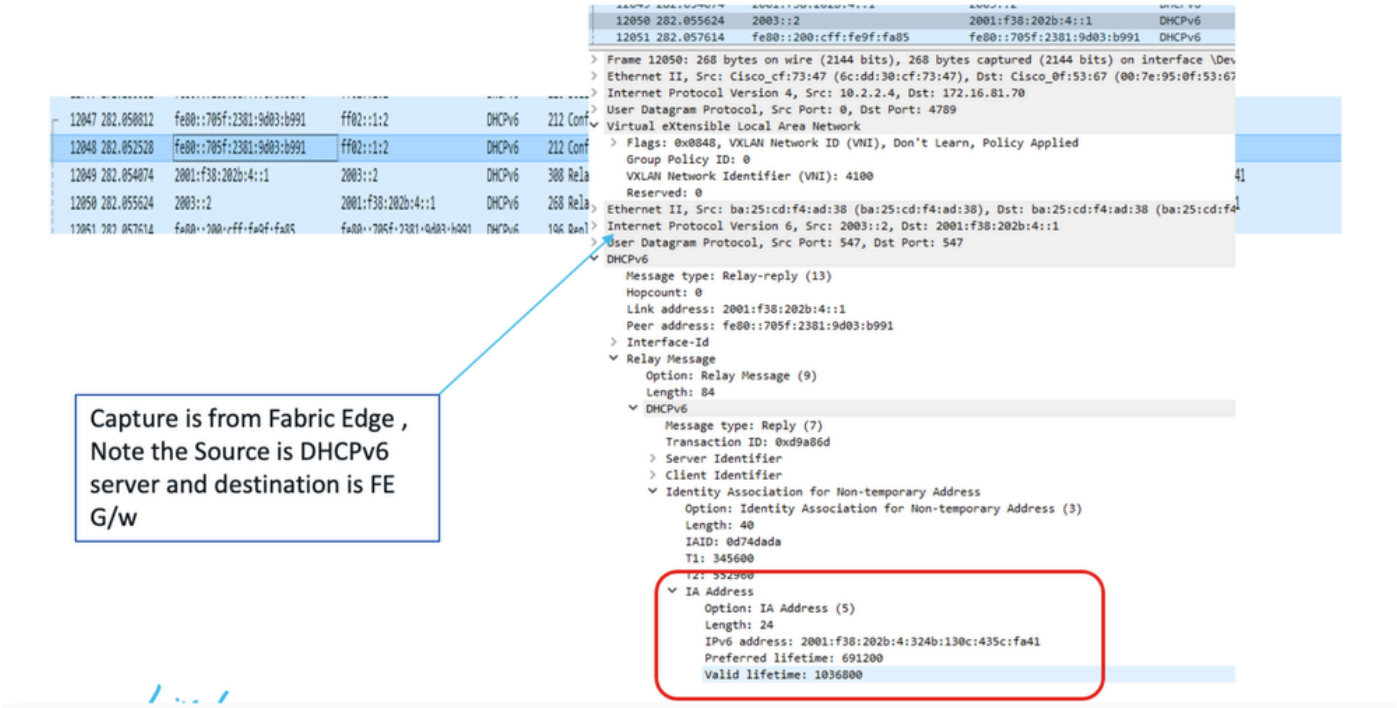


Amostra de detalhes de endereços IP e endereços MAC da malha de acesso SD



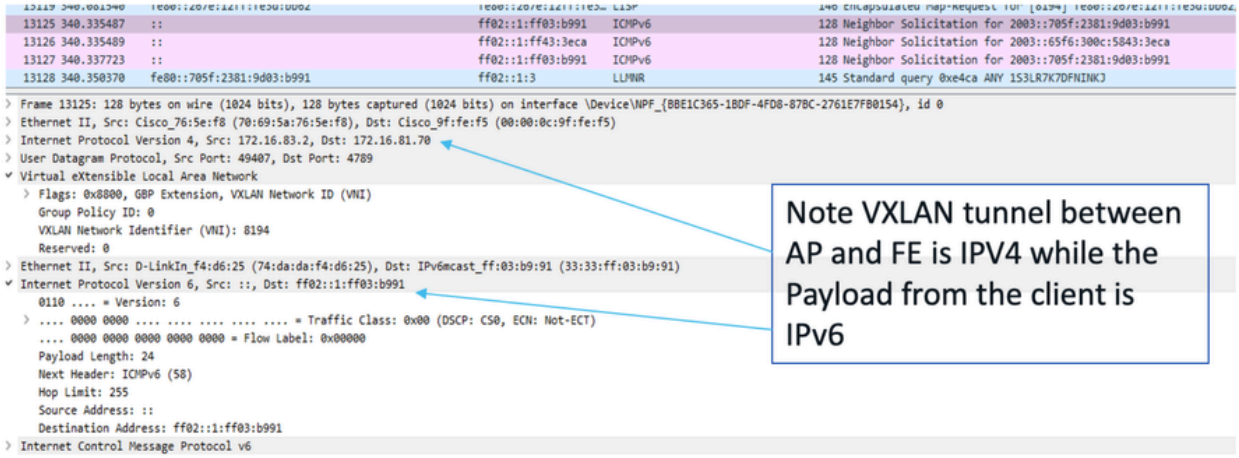
Note: Para qualquer comunicação IPv6 fora da malha, por exemplo, DHCP/DNS, o roteamento IPv6 deve ser ativado entre a infraestrutura de borda e a não malha.

Etapa 1. O cliente autentica e obtém o endereço IPv6 dos métodos configurados.



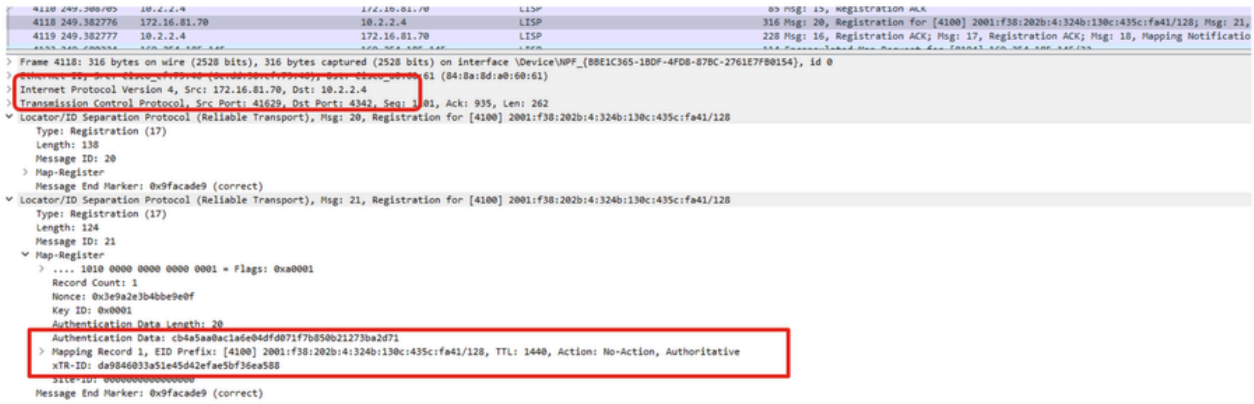
Captura de pacotes do servidor DHCPv6 para o nó de borda de malha

Etapa 2. O cliente sem fio envia os quadros 802.11 ao ponto de acesso com o payload IPv6.
Etapa 3. O ponto de acesso remove o cabeçalho sem fio e envia o pacote para a borda da estrutura. Isso usa o cabeçalho do túnel VXLAN que é baseado em IPv4, pois o Ponto de acesso tem o endereço IPv4.



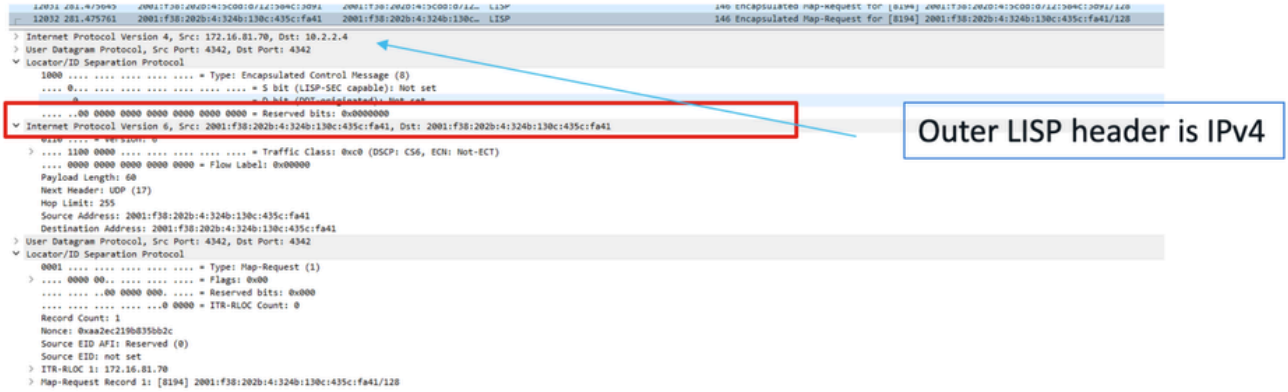
Captura de pacotes para o túnel VxLAN entre FE e AP

Etapa 3.1. Fabric Edge registra o cliente IPv6 com o plano de controle. Ele usa o método de registro IPv4 com detalhes do cliente IPv6 interno.



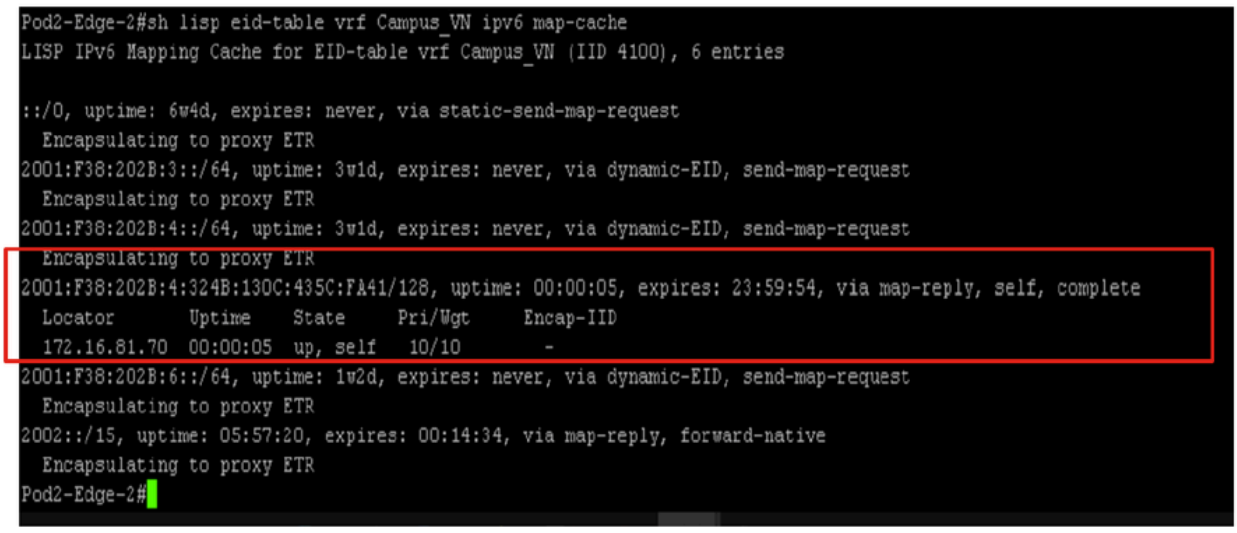
Captura de pacotes para registros FE com plano de controle para cliente IPv6

Etapa 3.2. O FE envia a solicitação MAP ao plano de controle para identificar o RLOC de destino.



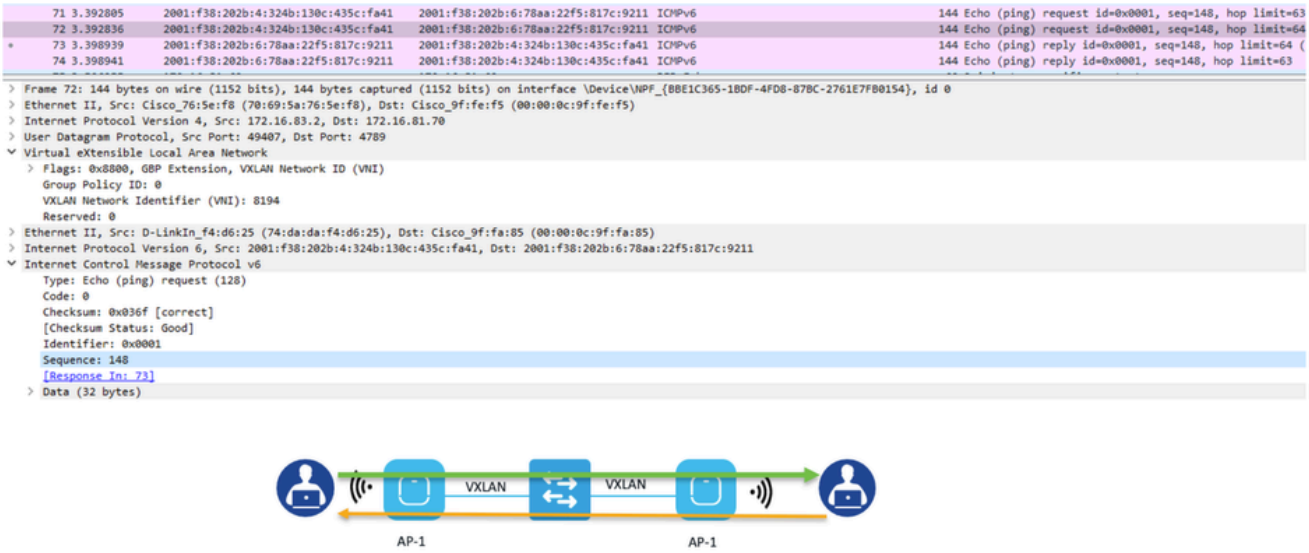
Captura de pacotes de FE para CP com mensagens de registro MAP

O Fabric Edge também mantém o cache MAP para clientes IPv6 conhecidos, como mostrado nesta imagem.



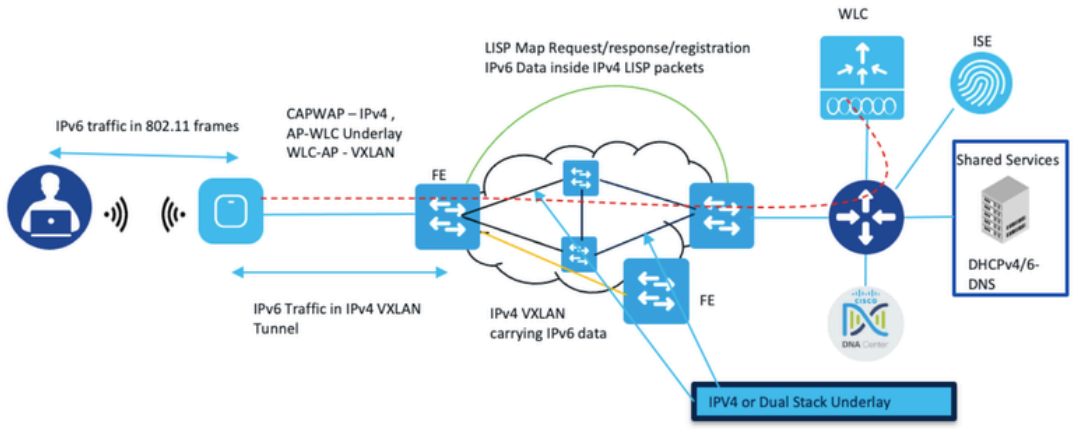
Saída de tela Fabric Edge de informações de cache de mapa de sobreposição IPv6

Etapa 4. O pacote é encaminhado para o RLOC de destino com a VXLAN IPv4 que transporta a carga útil IPv6 original para dentro. Como ambos os clientes estão conectados ao mesmo AP, o ping IPv6 toma esse caminho.

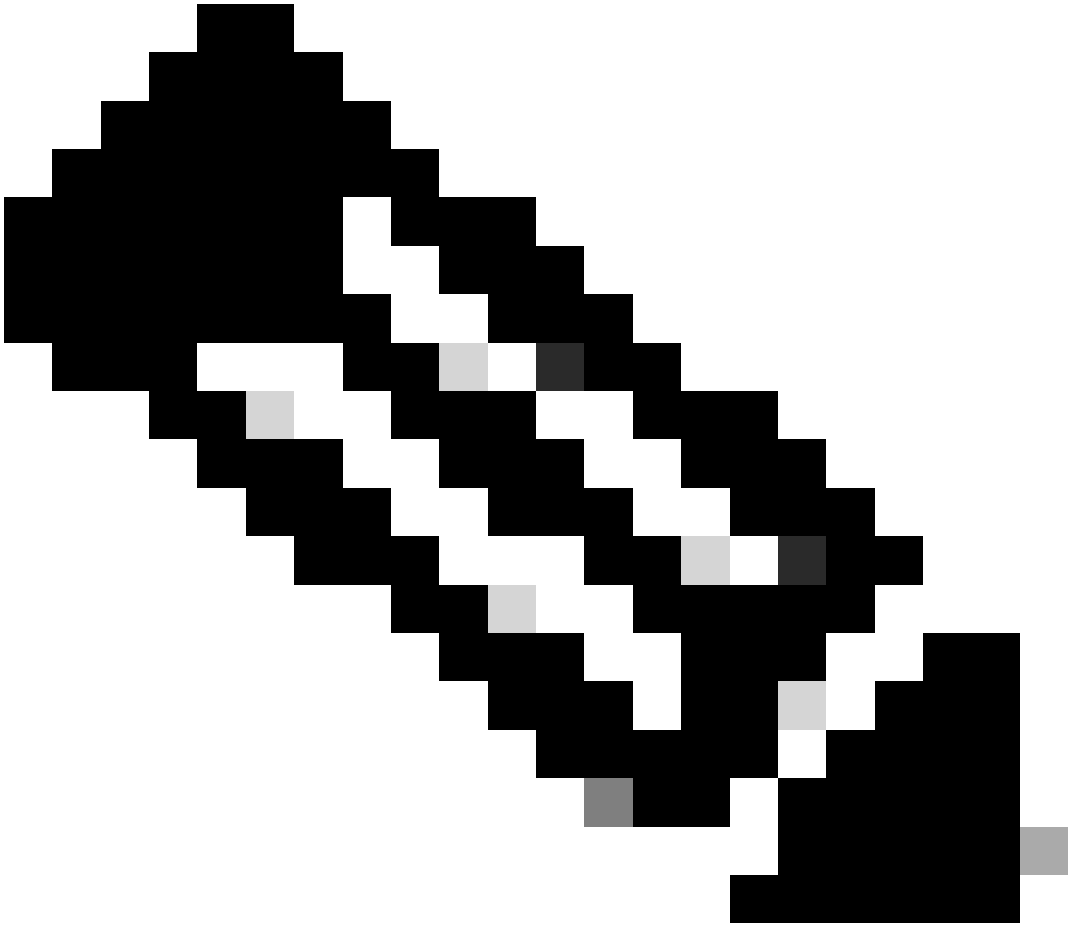


Captura de pacotes para ping IPv6 entre dois clientes sem fio registrados no mesmo AP

Esta imagem resume a comunicação IPv6 da perspectiva do cliente sem fio.



A figura resume a comunicação IPv6 da perspectiva do cliente sem fio



Note: Não há suporte para acesso de convidado IPv6 (portal da Web) via Cisco Identity Services devido a limitações no ISE.

Matriz de Dependências

É importante observar as dependências e o suporte para IPv6 de diferentes componentes sem fio que fazem parte do Cisco SD-Access. A tabela nesta imagem resume essa matriz de recursos.

C9800 IPv6 Features by Release

Feature		AireOS	16.12	17.1
Infra IPv6 (CAPWAP over IPv6)				
	Local	YES	YES	YES
	Flex	YES	YES	YES
	Fabric	NO	YES	YES
Infra IPv6 (WLC Platforms)				
	Hardware Wireless Controller	YES	YES	YES
	Wireless Controller in the switches	NO	YES	YES
	Public Cloud: AWS	NO	NO	NO
	Public Cloud: GCP	NO	NO	NO
	Private Cloud: ESXi	YES	YES	YES
	Private Cloud: KVM	YES	YES	YES
	Private Cloud: NFVIs	NO	YES	YES
Interop IPv6 support				
	C9800 <-> DNA-C (Infra IPv6)	NO	TBD	NO
	C9800 <-> CMX (Infra IPv6)	NO	TBD	YES
	C9800 <-> ISE (Infra IPv6)	NO	TBD	YES
	WLC<->PI(Infra IPv6)	YES(Over SNMP)	YES	YES
	OpenDNS(Infra iPv6)	NO	YES	YES
	Netflow over IPv6	NO	YES	YES
	ETA for IPv6	NO	NO	YES

Recursos do Cat9800 WLC IPv6 por versão

Monitore o plano de controle para IPv6

Depois de habilitar o IPv6, você começa a ver entradas adicionais sobre o host IPv6 nos servidores do servidor de mapa (MS)/resolvedor de mapa (MR). Como um host pode ter vários endereços IP IPv6, sua tabela de pesquisa MS/MR tem entradas para todos os endereços IP. Isso é combinado com a tabela IPv4 que já existe.
Você deve fazer login na CLI do dispositivo e executar esses comandos para verificar todas as entradas.

```
Pod2-Border#sh lisp site

LISP Site Registration Information

* = Some locators are down or unreachable

# = Some registrations are sourced by reliable transport


Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   4097     172.16.83.0/24
               2w1d      yes#   172.16.81.70:41629   4097     172.16.83.2/32
```

```
              never     no     --                  4099     172.16.79.0/24

              never     no     --                  4100     172.16.71.0/24

              never     no     --                  4100     172.16.72.0/24

              never     no     --                  4100     172.16.78.0/24

              never     no     --                  4100     2001:F38:202B:3::/64

              1w0d      yes#   172.16.81.65:16775  4100     2001:F38:202B:3:5B84:C9B0:1271:D4B/128

              1w0d      yes#   172.16.81.70:41629  4100     2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128

              never     no     --                  4100     2001:F38:202B:4::/64

              6d14h     yes#   172.16.81.70:41629  4100     2001:F38:202B:4:324B:130C:435C:FA41/128

              6d15h     yes#   172.16.81.70:41629  4100     2001:F38:202B:4:705F:2381:9D03:B991/128

              14:10:42  yes#   172.16.81.70:41629  4100     2001:F38:202B:4:B8AE:8711:5852:BE6A/128

              never     no     --                  4100     2001:F38:202B:6::/64
```

```
Pod2-Border#sh lisp site summary

                    ----------- IPv4 ----------- ----------- IPv6 ----------- ----------- MAC -----------

Site name           Configured Registered Incons Configured Registered Incons Configured Registered Incons

site_uci                     5          1      0          3          5      0          5          5      0



Site-registration limit for router lisp 0:              0

Site-registration count for router lisp 0:             11

Number of address-resolution entries:                  14

Number of configured sites:                             1

Number of registered sites:                             1

Sites with inconsistent registrations:                  0

IPv4

  Number of configured EID prefixes:                    5

  Number of registered EID prefixes:                    1

  Maximum MS entries allowed:                       81920

IPv6

  Number of configured EID prefixes:                    3
```

```
  Number of registered EID prefixes:                5

  Maximum MS entries allowed:                   81920

MAC

  Number of configured EID prefixes:                5

  Number of registered EID prefixes:                5

  Maximum MS entries allowed:                   81920
```

Você também pode verificar os detalhes sobre os detalhes do host IPv6 por meio da garantia.

Implementação de QoS IPv6 no Cisco SD-Access

A versão atual do Cisco DNA Center (até 2.3.x) não oferece suporte à automação da política de aplicativos de QoS IPv6. No entanto, os usuários podem criar manualmente modelos com e sem fio IPv6 e enviar o modelo de QoS para os nós de Borda de Estrutura. Como o DNA Center automatiza a política de QoS IPv4 em todas as interfaces físicas, uma vez aplicada, você pode inserir manualmente um mapa de classe (que corresponda à ACL (Access Control List, lista de controle de acesso) IPv6) antes de usar o 'padrão de classe' por meio de um modelo.

Este é um exemplo de modelo habilitado para QoS IPv6 com fio integrado à configuração de política gerada pelo DNA Center:

```
!
interface GigabitEthernetx/y/z
service-policy input DNA-APIC_QOS_IN
class-map match-any DNA-APIC_QOS_IN#SCAVENGER <<< Provisioned by DNAC
match access-group name DNA-APIC_QOS_IN#SCAVENGER__acl
match access-group name IPV6_QOS_IN#SCAVENGER__acl <<< Manually add
!
ipv6 access-list IPV6_QOS_IN#SCAVENGER__acl <<< Manually add
sequence 10 permit icmp any any
!
Policy-map DNA-APIC_QOS_IN
class IPV6_QOS_IN#SCAVENGER__acl <<< manually add
set dscp cs1
For wireless QoS policy, Cisco DNA Center with current release (up to 2.3.x) will provision IPv4 QoS on
and apply IPv4 QoS into the WLC (Wireless LAN Controller). It doesn’t automate IPv6 QoS.
© 2021 Cisco and/or its affiliates. All rights reserved. Page 20 of 24
Below is the sample wireless IPv6 QoS template. Please make sure to apply the QoS policy into the wirel
interface from the wireless VLAN:
ipv6 access-list extended IPV6_QOS_IN#TRANS_DATA__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#REALTIME
remark ### a placeholder ###
```

```
!
ipv6 access-list extended IPV6-QOS_IN#TUNNELED__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#VOICE
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#SCAVENGER__acl
permit icmp any any
!
ipv6 access-list extended IPV6_QOS_IN#SIGNALING__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#BROADCAST__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#BULK_DATA__acl
permit tcp any any eq ftp
permit tcp any any eq ftp-data
permit tcp any any eq 21000
permit udp any any eq 20
!
ipv6 access-list extended IPV6_QOS_IN#MM_CONF__acl
remark ms-lync
permit tcp any any eq 3478
permit udp any any eq 3478
permit tcp range 5350 5509
permit udp range 5350 5509
!
ipv6 access-list extended IPV6_QOS_IN#MM_STREAM__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#OAM__acl
remark ### a placeholder ###
!
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
!
class-map match-any IPV6_QOS_IN#TRANS_DATA
match access-group name IPV6_QOS_IN#TRANS_DATA__acl
!
class-map match-any IPV6_QOS_IN#REALTIME
match access-group name IPV6_QOS_IN#TUNNELED__acl
!
class-map match-any IPV6_QOS_IN#TUNNELED
match access-group name IPV6_QOS_IN#TUNNELED__acl
!
class-map match-any IPV6_QOS_IN#VOICE
match access-group name IPV6_QOS_IN#VOICE
!
class-map match-any IPV6_QOS_IN#SCAVENGER
match access-group name IPV6_QOS_IN#SCAVENGER__acl
!
class-map match-any IPV6_QOS_IN#SIGNALING
match access-group name IPV6_QOS_IN#SIGNALING__acl
class-map match-any IPV6_QOS_IN#BROADCAST
match access-group name IPV6_QOS_IN#BROADCAST__acl
!
class-map match-any IPV6_QOS_IN#BULK_DATA
match access-group name IPV6_QOS_IN#BULK_DATA__acl
!
class-map match-any IPV6_QOS_IN#MM_CONF
```


```
match access-group name IPV6_QOS_IN#MM_CONF__acl
!
class-map match-any IPV6_QOS_IN#MM_STREAM
match access-group name IPV6_QOS_IN#MM_STREAM__acl
!
class-map match-any IPV6_QOS_IN#OAM
match access-group name IPV6_QOS_IN#OAM__acl
!
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
policy-map IPV6_QOS_IN
class IPV6_QOS_IN#VOICE
set dscp ef
class IPV6_QOS_IN#BROADCAST
set dscp cs5
class IPV6_QOS_IN#REALTIME
set dscp cs4
class IPV6_QOS_IN#MM_CONF
set dscp af41
class IPV6_QOS_IN#MM_STREAM
set dscp af31
class IPV6_QOS_IN#SIGNALING
set dscp cs3
class IPV6_QOS_IN#OAM
set dscp cs2
class IPV6_QOS_IN#TRANS_DATA
set dscp af21
class IPV6_QOS_IN#BULK_DATA
set dscp af11
class IPV6_QOS_IN#SCAVENGER
set dscp cs1
class IPV6_QOS_IN#TUNNELED
class class-default
set dscp default
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
interface Vlan1xxx < = = (wireless VLAN)
service-policy input IPV6_QOS_IN
end
```

Identificar e solucionar problemas do IPv6 no Cisco SD-Access

Troubleshooting SD-Access IPv6 é bastante semelhante ao IPv4, você pode sempre usar o mesmo comando com diferentes opções de palavra-chave para alcançar o mesmo objetivo. Isso mostra alguns comandos que são usados com frequência para solucionar problemas do Acesso ao SD.

```
Pod2-Edge-2#sh device-tracking database
Binding Table has 24 entries, 12 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match 0002:Orig trunk 0004:Orig access
0008:Orig trusted trunk 0010:Orig trusted access 0020:DHCP assigned

0040:Cga authenticated 0080:Cert authenticated 0100:Statically assigned
```

```
Network Layer Address Link Layer Address Interface vlan prlvl age state Time left
DH4 172.16.83.2 7069.5a76.5ef8 Gi1/0/1 2045 0025 5s REACHABLE 235 s(653998 s)
L 172.16.83.1 0000.0c9f.fef5 Vl2045 2045 0100 22564mn REACHABLE
ARP 172.16.79.10 74da.daf4.d625 Ac0 71 0005 49s REACHABLE 201 s try 0
L 172.16.79.1 0000.0c9f.f886 Vl79 79 0100 22562mn REACHABLE
L 172.16.78.1 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
DH4 172.16.72.101 000c.29c3.16f0 Gi1/0/3 72 0025 9803mn STALE 101187 s
L 172.16.72.1 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
L 172.16.71.1 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
ND FE80::7269:5AFF:FE76:5EF8 7069.5a76.5ef8 Gi1/0/1 2045 0005 12s REACHABLE 230 s
ND FE80::705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 107s REACHABLE 145 s try 0
L FE80::200:CFF:FE9F:FA85 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
L FE80::200:CFF:FE9F:FA09 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
L FE80::200:CFF:FE9F:F886 0000.0c9f.f886 Vl79 79 0100 87217mn DOWN
L FE80::200:CFF:FE9F:F1AE 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
ND 2003::B900:53C0:9656:4363 74da.daf4.d625 Ac0 71 0005 26mn STALE 451 s
ND 2003::705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 3mn REACHABLE 49 s try 0
ND 2003::5925:F521:C6A7:927B 74da.daf4.d625 Ac0 71 0005 3mn REACHABLE 47 s try 0
L 2001:F38:202B:6::1 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
ND 2001:F38:202B:4:B8AE:8711:5852:BE6A 74da.daf4.d625 Ac0 71 0005 83s REACHABLE 164 s try 0
ND 2001:F38:202B:4:705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 112s REACHABLE 133 s try 0
DH6 2001:F38:202B:4:324B:130C:435C:FA41 74da.daf4.d625 Ac0 71 0024 107s REACHABLE 135 s try 0(985881 s)
L 2001:F38:202B:4::1 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
DH6 2001:F38:202B:3:E6F4:68B3:D2A6:59E6 000c.29c3.16f0 Gi1/0/3 72 0024 9804mn STALE 367005 s
L 2001:F38:202B:3::1 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
Pod2-Edge-2#sh lisp eid-table Campus_VN ipv6 database
LISP ETR IPv6 Mapping Database for EID-table vrf Campus_VN (IID 4100), LSBs: 0x1
Entries total 5, no-route 0, inactive 1
© 2021 Cisco and/or its affiliates. All rights reserved. Page 23 of 24
2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128, dynamic-eid InfraVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:324B:130C:435C:FA41/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:705F:2381:9D03:B991/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:ACAF:7DDD:7CC2:F1B6/128, Inactive, expires: 10:14:48
2001:F38:202B:4:B8AE:8711:5852:BE6A/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
Pod2-Edge-2#show lisp eid-table Campus_VN ipv6 map-cache
LISP IPv6 Mapping Cache for EID-table vrf Campus_VN (IID 4100), 6 entries
::/0, uptime: 1w3d, expires: never, via static-send-map-request
Encapsulating to proxy ETR
2001:F38:202B:3::/64, uptime: 5w1d, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128, uptime: 00:00:04, expires: 23:59:55, via map-reply, self, comp
Locator Uptime State Pri/Wgt Encap-IID
172.16.81.70 00:00:04 up, self 10/10 -
2001:F38:202B:4::/64, uptime: 5w1d, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2001:F38:202B:6::/64, uptime: 6d15h, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2002::/15, uptime: 00:05:04, expires: 00:09:56, via map-reply, forward-native
© 2021 Cisco and/or its affiliates. All rights reserved. Page 24 of 24
Encapsulating to proxy ETR
```

Do nó de borda para verificar a sobreposição do ping do servidor DHCPv6:

```
Pod2-Border#ping vrf Campus_VN 2003::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2003::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Perguntas frequentes rápidas sobre o design do IPv6 com o Cisco SD-Access

P. A Cisco Software Defined Network oferece suporte a IPv6 para redes de sobreposição e subjacentes?
R. Somente a sobreposição é suportada com a versão atual (2.3.x) no momento em que este documento é escrito.

P. O Cisco SDN é compatível com IPv6 nativo para clientes com e sem fio?
R. Sim. Isso requer pools de pilha dupla criados no DNA Center, enquanto IPv4 é o pool fictício, pois os clientes desabilitam solicitações DHCP IPv4 e somente endereços DHCP ou SLAAC IPv6 são oferecidos.

P. Posso ter uma rede de campus somente IPv6 nativa na minha malha de acesso SD da Cisco?
R. Não com a versão atual (até 2.3.x). Está no roteiro.

P. O Cisco SD-Access oferece suporte à entrega L2 IPv6?
A. Atualmente não. Apenas handoff L2 IPv4 e/ou hand-off L3 Dual-Stack são suportados.

P. O Cisco SD-Access suporta multicast para IPv6?
R. Sim, somente a sobreposição de IPv6 com multicast de replicação de fim de cabeçalho é suportada. Ainda não há suporte para multicast IPv6 nativo.

Q. O Cisco SD-Access Fabric Enabled Wireless suporta convidados em pilha dupla?
R. Ainda não suportado no Cisco IOS XE (Cat9800) WLC. O AireOS WLC é suportado por meio de uma solução alternativa. Para obter detalhes sobre a implementação da solução alternativa, entre em contato com a equipe de experiência do cliente da Cisco.

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.