Solucionar problemas da estrutura LISP VXLAN nos switches Catalyst 9000 Series

Contents

Introdução

Este documento descreve os componentes básicos de uma estrutura baseada em VXLAN LISP e como verificar sua operação.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Cisco IOS XE 17.9.3 ou posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estrutura baseada em VXLAN LISP

A finalidade de implantar uma rede VXLAN LISP é ser capaz de criar uma arquitetura onde várias redes Overlay, também conhecidas como Redes Virtuais, são definidas sobre uma rede subjacente.

- A rede Underlay nessa topologia atuaria principalmente como uma camada de transporte e não teria conhecimento das topologias de sobreposição que são executadas sobre ela.
- As redes de sobreposição podem ser adicionadas e removidas sem causar impacto na rede subjacente.
- O uso de redes de sobreposição separa efetivamente os usuários da rede subjacente.

Tecnologias usadas para criar uma estrutura LISP VXLAN

Protocolo de separação de identidade de localizador (LISP)

- O protocolo LISP é o protocolo de plano de controle usado dentro da estrutura. Ele é executado em todos os dispositivos de estrutura para criar a estrutura e controlar como o tráfego é enviado através da estrutura.
- LISP cria 2 espaços de endereço. Um é para os Localizadores de Roteamento (RLOCs) que são usados para anunciar a acessibilidade. O outro espaço de endereço é para os EIDs (Endpoint Identifiers Identificadores de Ponto de Extremidade), que são onde os pontos de extremidade residem e são usados para a sobreposição.
- No LISP, os EIDs são anunciados com um RLOC anunciado. Se um EID mover, tudo o que

precisa ser feito será atualizar o Localizador de roteamento associado a ele.
- Para alcançar um endpoint com tráfego LISP em direção a um EID, ele deve ser encapsulado e encapsulado em direção ao RLOC que o desencapsula e o encaminha para o endpoint.

Políticas baseadas em grupo

- Para permitir a segmentação dentro de um grupo de estrutura com base em políticas é usado.
- Quando as políticas baseadas em grupo são implantadas, o tráfego é classificado com Grupo seguro em vez de com base no IP de origem/destino.
- Isso reduz a complexidade de listas de controle de acesso complexas. Em vez de listas de endereços IP que precisam ser mantidos, os endereços IP/sub-redes são atribuídos a uma Tag de grupo segura.
- No ingresso na estrutura, é marcado um SGT quando o tráfego sai da estrutura, o destino do quadro é procurado por seu SGT .
- Com o uso de uma matriz, o SGT de origem e de destino é combinado e uma ACL de grupo segura é aplicada para aplicar o tráfego quando ele sai da malha.

Encapsulamento de VXLAN

- Dentro da estrutura, a VXLAN é usada para encapsular todo o tráfego
- A vantagem de usar VXLAN sobre o encapsulamento LISP legado é que ele permite encapsular todo o quadro da Camada 2, não apenas o quadro da Camada 3. À medida que o quadro inteiro é encapsulado, ele permite que as sobreposições sejam tanto da Camada 2 como da Camada 3.
- A VXLAN usa o UDP com a porta de destino 4789. Isso permite que os quadros VXLAN do LISP sejam transportados também por meio de um dispositivo que não reconheceria a topologia de sobreposição.
- Como a VXLAN encapsula todo o quadro, é importante aumentar a MTU para que não seja necessária nenhuma fragmentação, pois o tráfego é enviado entre RLOCs. Qualquer dispositivo intermediário precisaria suportar uma MTU maior para transportar os quadros encapsulados.

Autenticação

- Para poder atribuir terminais aos seus respectivos recursos, a autenticação pode ser usada.
- Com protocolos como 802.1x, os endpoints MAB e Webauth podem ser autenticados e/ou ter seu perfil criado em um servidor Radius e ter acesso à rede concedido com base em seus perfis de autorização.
- Com seus respectivos atributos do Radius, os endpoints podem ser atribuídos à VLAN, ao SGT e a qualquer outro atributo para fornecer acesso à rede do usuário/endpoint.

Principais componentes na estrutura LISP VXLAN

Nó do plano de controle

- contém a funcionalidade Servidor de Mapa LISP e Resolvedor de Mapa.

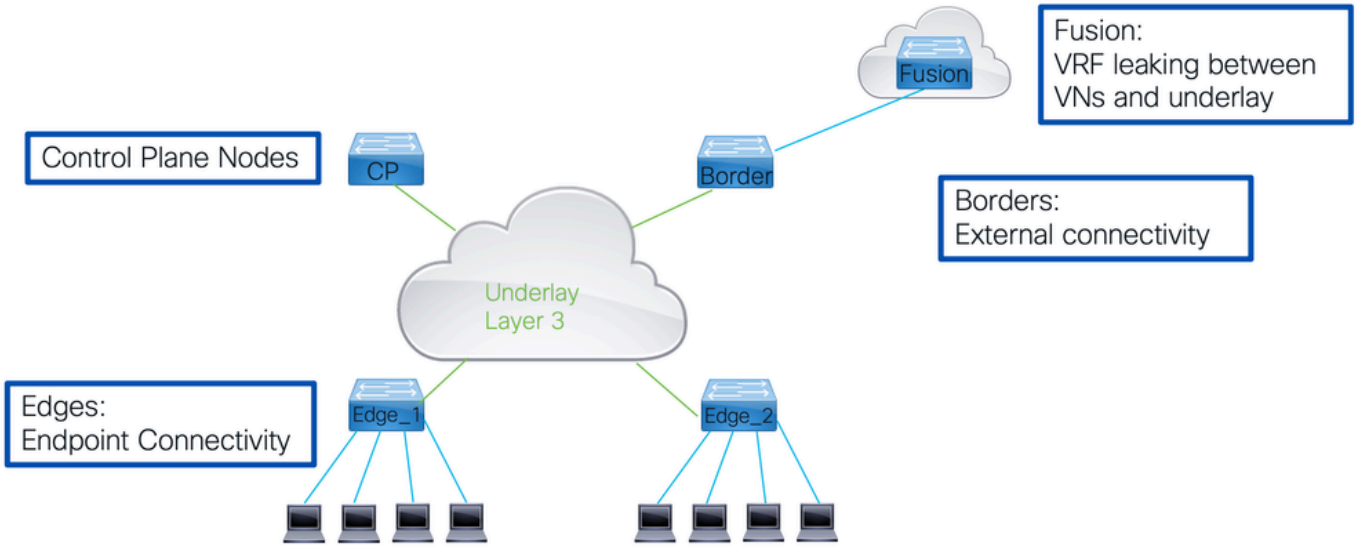
- Todos os outros dispositivos de malha consultam o nó do plano de controle para obter o local do EID e enviam registros para seu EID para os nós do plano de controle.
- Isso dá aos nós do plano de controle uma visão completa da estrutura em relação ao que está por trás do RLOC que os vários EIDs estão.

Nós de Borda

- Fornece conectividade fora da malha para outras malhas ou para o mundo externo.
- As bordas internas importam rotas para a estrutura e as registram nos nós do plano de controle.
- As fronteiras externas conectam-se ao mundo externo e fornecem um caminho padrão fora da malha para destinos IP desconhecidos.

Nós de borda

- Esses nós fornecem conectividade com os endpoints dentro da malha.
- Na definição de LISP, esses seriam XTRs, pois executariam a função de um Ingress Tunnel Router (ITR) e de um Egress Tunnel Router (ETR).



Os nós não estão limitados a apenas executar uma tarefa.

- Eles podem executar uma combinação ou até mesmo todas as funções dentro da estrutura.
- Quando um nó de borda e um nó de plano de controle residem em um dispositivo, eles se referem como colocados.
- Se esse nó também fornecer a funcionalidade de borda, ele será chamado de Fabric In A Box (FIAB).

As fronteiras fornecem handoffs para o restante da rede usando VRF lite.

- Cada sobreposição ou uma rede virtual é associada a uma instância de VRF no nó de borda.

- Para conectar esses vários VRFs, um roteador Fusion é usado. Esse roteador de fusão não faz parte da própria estrutura, mas é crucial para a operação, a fim de poder conectar as redes de Sobreposição à estrutura.

Outro conceito importante dentro de uma estrutura LISP VXLAN é o conceito de usar um Anycast IP.

- Isso significa que em todos os dispositivos de borda o endereço IP e seus endereços MAC para as interfaces virtuais comutadas (SVI) são replicados.
- Cada borda tem a mesma configuração no SVI com relação aos endereços IPv4, IPv6 e MAC.
- Solucionar esse problema impõe alguns desafios.
    - Testar a alcançabilidade com ping funciona com dispositivos locais conectados.
    - Para acessar destinos remotos através da estrutura VXLAN do LISP não retorna uma resposta, pois o dispositivo que envia uma resposta também envia isso para o endereço IP anycast que é direcionado para o dispositivo de estrutura local que não sabe qual outro nó de estrutura enviou o ping original.

Registro de endpoint

Para que uma estrutura LISP VXLAN funcione, é crucial que o nó do plano de controle tenha consciência de como todos os endpoints são alcançáveis através da estrutura.

- Para que o plano de controle aprenda sobre todos os EIDs na rede, ele depende de todos os outros dispositivos de estrutura para registrar todo o EID que conhece no plano de controle.
- Um nó de estrutura envia mensagens de registro de mapa LISP ao nó do plano de controle. Entre as informações que são anunciadas com a mensagem map-register.

Informações importantes

Identificador de instância LISP:

- Esse identificador é transportado pela malha e indica qual rede virtual deve ser usada.
- Dentro de uma estrutura LISP VXLAN por Camada 3 A sobreposição de uma instância é usada por VLAN usada na estrutura, também há uma Instância de Camada 2.

Endpoint Identificado (EID):

- Se esta for uma instância da camada 2 ou 3, este será o endereço MAC, a rota do host IP (/32 ou /128) ou uma sub-rede IP registrada

Localizador de Roteamento (RLOC):

- Esse é o endereço IP do próprio nó de estrutura com o qual ele anuncia a alcançabilidade onde outros dispositivos de estrutura enviam tráfego encapsulado que precisaria alcançar o EID.

Sinalizador de proxy:

- Quando esse indicador é definido, ele permite que o nó Plano de controle responda a solicitações de mapa de outros nós de malha diretamente , sem que o indicador de proxy defina todas as solicitações a serem encaminhadas ao nó de malha que registrou o EID.

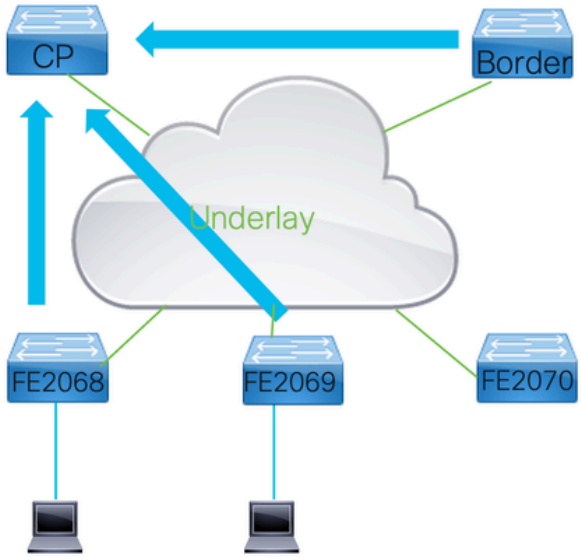
Etapas de registro

Passo 1: Os dispositivos de estrutura aprendem sobre identificadores de ponto final. Isso pode ser feito por meio de configuração, protocolos de roteamento ou quando aprendido nos dispositivos de estrutura.

Etapa 2: os dispositivos de estrutura registram os endpoints aprendidos com cada nó do plano de controle conhecido e acessível dentro da estrutura.

Passo 3: Os nós do plano de controle mantêm uma tabela de EIDs registrados com o ID de instância relacionado, o RLOC e o EID aprendido

Instance	RLOC	EID (mac address)
8189	FE2068	0019.3052.6d7f
8189	FE2069	0019.3052.6d7f
4099	FE2068	172.24.1.4/32
4099	FE2069	172.24.1.3/32
4099	Border	10.48.13.0/24



Verificar

1.1 Aprendizado de Endereços MAC

Para instâncias de camada 2, o EID usado são os endereços MAC aprendidos dentro da VLAN associada. As bordas da estrutura aprendem os endereços da camada 2 através de métodos padrão nos switches.

Localize a VLAN Associada a uma ID de Instância de Camada 2 específica para a qual a configuração pode ser revisada ou o comando

Use "show lisp instance-id <instance> ethernet"

```
<#root>

FE2068#

show lisp instance-id 8191 ethernet


  Instance ID:

8191


  Router-lisp ID:                          0
  Locator table:                           default
  EID table:

Vlan 150


  Ingress Tunnel Router (ITR):             enabled
  Egress Tunnel Router (ETR):              enabled
  ..
  Site Registration Limit:                 0
  Map-Request source:                      derived from EID destination
  ITR Map-Resolver(s):                     172.30.250.19
  ETR Map-Server(s):                       172.30.250.19
```

Como visto na saída, o instance-id 8191 está associado à VLAN 150. Isso faz com que todos os endereços MAC dentro da vlan sejam registrados com LISP e se tornem parte da estrutura LISP VXLAN.

```
<#root>

FE2068#

show mac address-table vlan 150


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

 150    0000.0c9f.f18e    STATIC      Vl150


 150    0050.5693.8930    DYNAMIC     Gi1/0/1


 150    2416.9db4.33fd    STATIC      Vl150


 150    0019.3052.6d7f    CP_LEARN    L2LI0

Total Mac Addresses for this criterion: 3
Total Mac Addresses installed by LISP: REMOTE: 1
```

As entradas estáticas com a interface Vl150 são os endereços MAC da interface virtual do switch (interface vlan 150).

- Esses endereços MAC não são registrados no nó do plano de controle, pois seriam os mesmos em todos os dispositivos de borda.
- A entrada CP_LEARN exibida são as entradas aprendidas através da estrutura. Para todas as outras entradas, se forem dinâmicas ou estáticas, devem ser registradas com o nó do plano de controle.

Uma vez aprendidos através de seus respectivos meios, eles aparecem nas saídas do banco de dados lisp, esta saída contém todas as entradas locais neste dispositivo de estrutura.

<#root>

FE2068#

show lisp instance-id 8191 ethernet database

LISP ETR MAC Mapping Database for LISP 0 EID-table

Vlan 150 (IID 8191)

, LSBs: 0x1
Entries total 3, no-route 0, inactive 0, do-not-register 2

0000.0c9f.f18e/48

, dynamic-eid Auto-L2-group-8191,

do not register

, inherited from default locator-set rloc_hosts
  Uptime: 14:56:40, Last-change: 14:56:40
  Domain-ID: local
  Service-Insertion: N/A
  Locator   Pri/Wgt Source   State

172.30.250.44

  10/10   cfg-intf   site-self, reachable

0050.5693.8930/48

, dynamic-eid Auto-L2-group-8191, inherited from default locator-set rloc_hosts
  Uptime: 14:03:06, Last-change: 14:03:06
  Domain-ID: local
  Service-Insertion: N/A
  Locator   Pri/Wgt Source   State

172.30.250.44

  10/10   cfg-intf   site-self, reachable
2

416.9db4.33fd/48

, dynamic-eid Auto-L2-group-8191, do not register, inherited from default locator-set rloc_hosts
  Uptime: 14:56:50, Last-change: 14:56:50
  Domain-ID: local

```
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State

172.30.250.44
   10/10   cfg-intf   site-self, reachable
```

Para todos os endereços MAC locais conhecidos que são mostrados no banco de dados, o Localizador é mostrado.

- Este é o localizador que deve ser usado para registrar esta entrada com o nó do plano de controle.
- Ele também indicou o estado do localizador.Os 2 endereços MAC que pertenciam à SVI dos Switches também são mostrados, mas são exibidos com o flag "não registrar", que impede que sejam registrados.
- A entrada remota vista no comando show mac address table não é um endereço MAC local e, como tal, não aparece no banco de dados lisp.

Para uma Instância de Camada 2, não apenas os endereços MAC da Camada 2 são aprendidos como EID, mas também há a necessidade de aprender as informações de resolução de endereço dos quadros ARP e ND.

- Isso permite que a estrutura LISP VXLAN possa encaminhar esses quadros, pois eles são normalmente inundados dentro da VLAN.
- Como um Instance-ID de Camada 2 nem sempre tem a capacidade de inundar lá outro mecanismo que permitiria que os endpoints resolvessem informações de resolução de endereço para outros endpoints na mesma instância. Para isso, os dispositivos de estrutura aprendem e registram essas informações que são aprendidas localmente pelo Rastreamento de dispositivos .
- Isso é registrado com os nós do plano de controle também. Devido à espionagem de ND ou ARP, esses pacotes são direcionados para a CPU para disparar uma solicitação para os nós do plano de controle para ver se há algum endereço MAC conhecido associado.
- Se uma resposta positiva voltar, os pacotes ARP/ND serão reescritos para que o endereço MAC de destino seja alterado de broadcast ou multicast para o endereço MAC unicast.
- Esse pacote reescrito pode ser encaminhado através da estrutura LISP VXLAN como um quadro unicast.

Para ver as informações de resolução de endereço conhecidas no switch, o comando show device-tracking database pode ser usado.

- Isso mostra todos os mapeamentos conhecidos pelo rastreamento de dispositivo.
- Os próprios endereços IP dos switches são rotulados como L(Local) e precisam estar presentes no banco de dados de rastreamento de dispositivos.

Entradas remotas também são exibidas nesta saída.

- À medida que são resolvidos após a espionagem da solicitação ND ou ARP, eles são

colocados no banco de dados de rastreamento de dispositivo com um endereço de camada de enlace 000.0000.00fd.

- No momento em que são resolvidas, as informações são alteradas para o endereço MAC resolvido e a porta é alterada para Tu0.

Exibir o banco de dados de rastreamento de dispositivo

<#root>

```
FE2068#

show device-tracking database vlanid 150


vlanDB has 6 entries for vlan 150, 3 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
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      ag

ARP


172.24.1.3                                0050.5693.8930

        Gi1/0/1    150        0005       31s        REACHABLE  213 s try 0
RMT 172.24.1.4

0050.5693.3120

        Tu0    150        0005       51s        REACHABLE


API


172.24.1.99                               0000.0000.00fd

         Gi1/0/1    150        0000       5s         UNKNOWN    try 0 (25 s)
ND  FE80::1AE4:8804:5B8F:50F6                0050.5693.8930         Gi1/0/1    150        0005       12

ND


2001:DB8::E70B:E8E1:E368:BDB7             0050.5693.8930

         Gi1/0/1    150        0005       137s       REACHABLE  110 s try 0
L   172.24.1.254                             0000.0c9f.f18e         Vl150      150        0100       10
L   2001:DB8::1                              0000.0c9f.f18e         Vl150      150        0100       10
L   FE80::200:CFF:FE9F:F18E                  0000.0c9f.f18e         Vl150      150        0100       10
```

Exiba os mapeamentos registrados localmente com o comando 'show lisp instance-id <instance> ethernet database address-resolution'

<#root>

FE2068#

show lisp instance-id 8191 ethernet database address-resolution

LISP ETR Address Resolution for LISP 0 EID-table Vlan 150 (IID 8191)
(*) -> entry being deleted
Hardware Address L3 InstID Host Address

0000.0c9f.f18e 4099 FE80::200:CFF:FE9F:F18E/128

4099 2001:DB8::1/128

0050.5693.8930 4099 172.24.1.3/32

4099 2001:DB8::E70B:E8E1:E368:BDB7/128

4099 FE80::1AE4:8804:5B8F:50F6/128

1.2 Aprendizado de endereços IP dinâmicos

Nos dispositivos de estrutura em uma camada IP, uma rede virtual é formada pela associação de um Instance-id LISP a um VRF.

- Esse VRF é então configurado nas várias interfaces virtuais do switch (SVI) e elas se tornam parte da rede de camada 3
- Na maioria dos casos, essas SVI também pertencem a VLANs registradas com suas respectivas instâncias de camada 2.

Localize o mapeamento entre o VRF e o ID da instância do LISP com o comando 'show lisp instance-id <instance> ipv4'

<#root>

FE2068#

sh lisp instance-id 4099 ipv4

Instance ID: 4099

Router-lisp ID: 0
Locator table: default

EID table: vrf Fabric_VN_1

Ingress Tunnel Router (ITR): enabled

```
  Egress Tunnel Router (ETR):               enabled
  ..
  ITR Map-Resolver(s):                      172.30.250.19


  ETR Map-Server(s):                        172.30.250.19
```

Note: Esse comando também pode ser usado para verificar as várias funções que podem ser habilitadas para essa Instância, bem como mostra os nós do plano de controle usados dentro da estrutura LISP VXLAN

Quando uma instância de camada 3 é criada e vinculada a um VRF, uma interface LISP 0 <instance-id> é criada e fica visível na configuração de execução e em show vrf.

- Essa interface NÃO precisa ser criada manualmente e geralmente não precisa de configuração (exceto a Configuração Multicast quando a opção Underlay Multicast é usada).

<#root>

FE2068#

show vrf Fabric_VN_1

```
  Name                              Default RD            Protocols   Interfaces
```

Fabric_VN_1

ipv4,ipv6

LI0.4099

Vl150

Vl151

Diferentemente dos quadros Ethernet, onde todos os endereços MAC em uma VLAN são usados para IP, há uma necessidade de que os endereços IP estejam dentro de um intervalo EID dinâmico a ser aprendido.

Exibir uma instância LISP

<#root>

FE2068#

sh lisp instance-id 4099 dynamic-eid

LISP Dynamic EID Information for router 0,

IID 4099, EID-table VRF "Fabric_VN_1"

Dynamic-EID name:

Fabric_VN_Subnet_1_IPv4

  Database-mapping EID-prefix: 172.24.1.0/24, locator-set rloc_hosts

  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: none configured

  Number of roaming dynamic-EIDs discovered: 2

  Last dynamic-EID discovered: 172.24.1.3, 21:17:45 ago

Dynamic-EID name: Fabric_VN_Subnet_1_IPv6

  Database-mapping EID-prefix: 2001:DB8::/64, locator-set rloc_hosts

  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: none configured

  Number of roaming dynamic-EIDs discovered: 2

  Last dynamic-EID discovered: 2001:DB8::E70B:E8E1:E368:BDB7, 21:17:44 ago

```
Dynamic-EID name: Fabric_VN_Subnet_2_IPv4


  Database-mapping EID-prefix: 172.24.2.0/24, locator-set rloc_hosts


  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: none configured

  Number of roaming dynamic-EIDs discovered: 2


  Last dynamic-EID discovered: 172.24.2.2, 21:55:56 ago
```

Os endereços IP que estão fora desses intervalos definidos são considerados inelegíveis para a estrutura e não são colocados nos bancos de dados LISP e não registrados nos nós do plano de controle.

<#root>

FE2068#

show lisp instance-id 4099 ipv4 database

```
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), LSBs: 0x1
Entries total 4, no-route 0, inactive 0, do-not-register 2
```

172.24.1.3/32, dynamic-eid Fabric_VN_Subnet_1_IPv4

```
, inherited from default locator-set rloc_hosts
  Uptime: 21:28:51, Last-change: 21:28:51
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State
```

172.30.250.44

```
   10/10   cfg-intf   site-self, reachable
```

172.24.1.254/32, dynamic-eid Fabric_VN_Subnet_1_IPv4, do not register,

```
 inherited from default locator-set rloc_hosts
  Uptime: 22:22:35, Last-change: 22:22:35
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State
```

172.30.250.44

```
   10/10   cfg-intf   site-self, reachable
```

172.24.2.2/32, dynamic-eid Fabric_VN_Subnet_2_IPv4

```
, inherited from default locator-set rloc_hosts
  Uptime: 22:07:03, Last-change: 22:07:03
```

```
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.44

  10/10   cfg-intf   site-self, reachable

172.24.2.254/32, dynamic-eid Fabric_VN_Subnet_2_IPv4, do not register

, inherited from default locator-set rloc_hosts
  Uptime: 22:22:35, Last-change: 22:22:35
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.44

 10/10   cfg-intf   site-self, reachable
```

A saída mostra todas as informações de endereço IP localmente conhecidas.

- Para hosts, essas são normalmente rotas de host (/32 ou /128), mas elas também podem ser sub-redes se elas tiverem sido importadas para o banco de dados LISP no nó de borda.
- Os endereços IP da própria SVI são marcados como "não registrar" . Isso evita que todos os dispositivos de estrutura registrem o endereço IP Anycast no nó do plano de controle.

<#root>

```
CP_BN_2071#

sh lisp instance-id 4099 ipv4 database


LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), LSBs: 0x1
Entries total 2, no-route 0, inactive 0, do-not-register 0


0.0.0.0/0

, locator-set rloc_border, auto-discover-rlocs, default-ETR
  Uptime: 2d17h, Last-change: 2d17h
  Domain-ID: local
  Metric: 0
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.19

   10/10   cfg-intf   site-self, reachable


10.48.13.0/24, route-import

, inherited from default locator-set rloc_border, auto-discover-rlocs
  Uptime: 2d17h, Last-change: 2d16h
  Domain-ID: local, tag: 65101
  Service-Insertion: N/A
```

```
  Locator        Pri/Wgt  Source     State

172.30.250.19

   10/10   cfg-intf   site-self, reachable
```

1.3 Registro da identificação eletrônica no plano de controlo

O registro de endpoint em uma estrutura baseada em VXLAN LISP é feito por meio de registro confiável LISP. Isso significa que todos os registros são feitos por meio de uma sessão TCP estabelecida , a sessão LISP. A partir de cada dispositivo de estrutura, uma sessão LISP é estabelecida com cada um dos nós do plano de controle na estrutura. Por meio dessa sessão LISP, todos os registros ocorrem. Se vários nós do plano de controle estiverem presentes dentro de uma malha, todos serão usados para registrar EIDs.

O estado é Desativado quando não há nada para registrar no dispositivo de malha, o que normalmente ocorreria apenas nas fronteiras externas
que não registram intervalos de IP com o nó Plano de controle ou em dispositivos de borda sem nenhum ponto final

O registro de EID acontece através de mensagens de registro LISP
que são enviadas a todos os nós do plano de controle configurados.

Para ver a sessão LISP em um dispositivo de estrutura, o comando show lisp session pode ser usado.
Ele mostra o estado da sessão e a hora em que ela esteve ativa.

<#root>

```
FE2068#

show lisp session


Sessions for VRF default, total: 1, established: 1
Peer                          State      Up/Down        In/Out    Users

172.30.250.19:4342            Up

        22:06:07     9791/6531   10
```

A sessão LISP mostrada como Inativa pode ocorrer em dispositivos que não têm nenhum EID para registrar no nó Plano de controle.
Normalmente, seriam nós de borda que não importam rotas para a estrutura ou para os dispositivos de borda sem nenhum endpoint conectado.

Exiba informações mais detalhadas sobre uma sessão LISP com o comando 'show lisp session vrf default <ip address>'

<#root>

FE2068#

show lisp vrf default session 172.30.250.19

Peer address: 172.30.250.19:4342
Local address: 172.30.250.44:13255
Session Type:

Active

Session State:

Up

(22:07:24)
Messages in/out: 9800/6537
Bytes in/out: 616771/757326
Fatal errors: 0
Rcvd unsupported: 0
Rcvd invalid VRF: 0
Rcvd override: 0
Rcvd malformed: 0
Sent deferred: 1
SSO redundancy: N/A
Auth Type: None
Accepting Users: 0
Users: 10

Type	ID	In/Out	State
Policy subscription	lisp 0 IID 4099 AFI IPv4	2/1	Established
Pubsub subscriber	lisp 0 IID 4099 AFI IPv6	1/0	Idle
Pubsub subscriber	lisp 0 IID 8191 AFI MAC	2/0	Idle
Pubsub subscriber	lisp 0 IID 8192 AFI MAC	0/0	Idle

ETR Reliable Registration lisp 0 IID 4099 AFI IPv4

6/5 TCP

ETR Reliable Registration lisp 0 IID 4099 AFI IPv6

1/3 TCP

ETR Reliable Registration lisp 0 IID 8191 AFI MAC

9769/6517 TCP

ETR Reliable Registration lisp 0 IID 8192 AFI MAC

2/6 TCP

ETR Reliable Registration	lisp 0 IID 16777214 AFI IPv4	4/4	TCP
Capability Exchange	N/A	1/1	waiting

Esta saída detalhada da sessão mostra quais Instâncias estão ativas com EID que estão registradas com os nós do plano de controle.

<#root>

CP_BN_2071#

show lisp session

```
Sessions for VRF default, total: 7, established: 4
Peer                            State      Up/Down        In/Out    Users
```

172.30.250.19:4342   Up

```
         22:10:52   1198618/1198592 4
```

172.30.250.19:49270   Up

```
      22:10:52   1198592/1198618 3
```

172.30.250.30:25780   Up

```
        22:10:38     6534/9805   6
```

172.30.250.44:13255   Up

```
        22:10:44     6550/9820   7
```

Quando se observa o número de sessões em um nó de plano de controle, normalmente há mais sessões ativas.

- Se esse for um nó Border/CP posicionado, também haverá uma sessão LISP estabelecida em relação a si mesmo.
- Nesse caso, há uma sessão de 172.30.250.19:4342 a 172.30.250.19:49270.
- Através desta sessão, o componente Borda registra seu EID com o nó de plano de controle.

1.4 Informações do plano de controle

Com as informações fornecidas pelos dispositivos de estrutura por meio do registro, o nó do plano de controle é capaz de criar uma visão completa da estrutura. Por Instance-id, ele mantém uma tabela com os EIDs aprendidos e seus Localizadores de Roteamento associados.

Exiba isso para as instâncias de Camada 3 do comando show lisp site

<#root>

CP_BN_2071#

show 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     0.0.0.0/0
               never     no     --                   4097     172.23.255.0/24
               never     no     --                   4097     172.24.255.0/24
               never     no     --                   4099     0.0.0.0/0
               00:00:00
yes#   172.30.250.19:49270  4099     10.48.13.0/24

               never     no     --                   4099     172.23.1.0/24
               never     no     --                   4099     172.24.1.0/24
               21:35:06
yes#   172.30.250.44:13255  4099     172.24.1.3/32

               22:11:46
yes#   172.30.250.30:25780  4099     172.24.1.4/32

               never     no     --                   4099     172.24.2.0/24
               22:11:52
yes#   172.30.250.44:13255  4099     172.24.2.2/32
```

Esse comando mostra todos os EID registrados e o último que registrou o EID. É importante observar que isso normalmente também seria o RLOC que está em uso, mas isso pode diferir. Além disso, os EIDs podem ser registrados com vários RLOCs .

Para exibir todos os detalhes, o comando inclui o EID e a instância

<#root>

```
CP_BN_2071#
show lisp site 172.24.1.3/32 instance-id 4099

LISP Site Registration Information
Site name: site_uci
Description: map-server
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:
172.24.1.3/32 instance-id 4099

    First registered:     21:35:53
    Last registered:      21:35:53
    Routing table tag:    0
    Origin:               Dynamic, more specific of 172.24.1.0/24
    Merge active:         No
    Proxy reply:
Yes
```

```
    Skip Publication:     No
    Force Withdraw:       No
    TTL:
```

1d00h

```
    State:
```

complete

```
    Extranet IID:         Unspecified
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.30.250.44:13255, last registered 21:35:53, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0x6ED7000E-0xD4C608C5
                             xTR-ID 0x88F15053-0x40C0253D-0xAE5EA874-0x2551DB71
                             site-ID unspecified
                             Domain-ID local
                             Multihoming-ID unspecified
                             sourced by reliable transport
      Locator        Local  State      Pri/Wgt  Scope
```

172.30.250.44 yes   up

```
          10/10   IPv4 none
```

Note: Na saída detalhada, alguns itens são importantes:

- Proxy, com esse conjunto, o nó Plano de controle responde diretamente a uma solicitação de Mapa. No LISP tradicional, uma solicitação de mapa é encaminhada para o XTR que registrou o EID, mas com Proxy definido, o nó do plano de controle responde diretamente
- TTL, este é o Time To Live do registro EID. Por padrão, são 24 horas
- informação ETR, refere-se ao dispositivo de estrutura que enviou o registro EID
- RLOC, esse é o RLOC a ser usado para acessar o EID. Ele também contém informações de estado como ativo/inativo. se o RLOC estiver inativo, ele não será usado. Ele também contém um peso e uma prioridade que podem ser usados quando existem vários RLOCs para que um EID dê preferência a um deles.

Para ver o histórico de registro no nó Plano de controle, o comando show lisp server registration history pode ser usado.

- Ele fornece uma visão geral da EID que foi registrada e cancelada.

Exibir histórico de registro

<#root>

CP_BN_2071#

show lisp server registration-history last 10

```
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event
Timestamp (UTC)      Instance Proto Roam WLC Source
                                            EID prefix / Locator
*Mar 24 20:49:51.490     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.491     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.621     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.622     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.752     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.754     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.884     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.886     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:52.017     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:52.019     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
```

Exiba o EID registrado para Ethernet. O comando é show lisp instance-id <instance> ethernet server (Isso gera uma saída semelhante à da Camada 3)

<#root>

CP_BN_2071#

show lisp instance-id 8191 ethernet server

```
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     --                   8191     any-mac
               00:00:04
```

yes#   172.30.250.44:13255 8191   0019.3052.6d7f/48

```
               21:36:41
```

yes#   172.30.250.44:13255 8191   0050.5693.8930/48

```
               22:13:20
```

yes# 172.30.250.30:25780 8191 0050.5693.f1b2/48

Acrescentar o endereço MAC para obter informações mais detalhadas sobre um registro

<#root>

CP_BN_2071#

show lisp instance-id 8191 ethernet server 0019.3052.6d7f

LISP Site Registration Information
Site name: site_uci
Description: map-server
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:

0019.3052.6d7f/48 instance-id 8191

    First registered: 22:14:38
    Last registered: 00:00:03
    Routing table tag: 0
    Origin: Dynamic, more specific of any-mac
    Merge active: No
    Proxy reply:

Yes

    Skip Publication: No
    Force Withdraw: No
    TTL:

1d00h

    State:

complete

    Extranet IID: Unspecified
    Registration errors:
      Authentication failures: 0
      Allowed locators mismatch: 0
    ETR 172.30.250.30:25780, last registered 00:00:03, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0x0465A327-0xA3A2974C
                             xTR-ID 0x280403CF-0x598BAAF1-0x3E70CE52-0xE8F09E6E
                             site-ID unspecified
                             Domain-ID local
                             Multihoming-ID unspecified
                             sourced by reliable transport
      Locator   Local State   Pri/Wgt Scope

172.30.250.30 yes

```
up          10/10   IPv4 none
```

Acrescente 'registration history' para ver o histórico de registro da EEthernet EID

Note: Esse comando é muito útil quando os dispositivos fazem roaming na malha para ver onde e quando o endereço MAC foi registrado

---

<#root>

```
CP_BN_2071#
```

show lisp instance-id 8191 ethernet server registration-history

```
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event
Timestamp (UTC)      Instance Proto Roam WLC Source
                                            EID prefix / Locator
*Mar 24 20:47:10.291     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:10.296     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:18.644     8191 TCP   Yes  No  172.30.250.30
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:18.647     8191 TCP   No   No  172.30.250.44
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:20.700     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:20.702     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:31.914     8191 TCP   Yes  No  172.30.250.30
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:31.918     8191 TCP   No   No  172.30.250.44
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:40.206     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:40.210     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
```

Para ver as informações registradas de resolução de endereço no nó do plano de controle, o comando é anexado com address-resolution.

- Isso mostra apenas os mapeamentos entre o endereço MAC e suas informações de Camada 3 e deve ser usado principalmente para os Fabric Edges para regravar os endereços MAC de destino da camada 2 de broadcast/multicast para unicast.
- O RLOC que corresponde àquele endereço MAC de Camada 2 seria resolvido separadamente .

Acrescente 'address-resolution' para ver as informações registradas de resolução de endereços

no nó do plano de controle

<#root>

```
CP_BN_2071#
sh lisp instance-id 8191 ethernet server address-resolution

Address-resolution data for router lisp 0 instance-id 8191
L3 InstID    Host Address                                Hardware Address

4099    172.24.1.3/32                                0050.5693.8930

     4099    172.24.1.4/32                                0050.5693.f1b2

     4099    2001:DB8::E70B:E8E1:E368:BDB7/128            0050.5693.8930

     4099    2001:DB8::F304:BCCD:6BF3:BFAF/128            0050.5693.f1b2

     4099    FE80::3EE:5111:BA77:E37D/128                 0050.5693.f1b2

     4099    FE80::1AE4:8804:5B8F:50F6/128                0050.5693.8930
```

Note: Embora os endereços IPv6 de link local não correspondam ao EID dinâmico IPv6, eles devem ser aprendidos para a resolução de endereço e isso apareceria no nó do plano de controle. Eles não seriam registrados na ID de instância da camada 3, mas estão disponíveis para a resolução de endereços.

Resolver destinos remotos

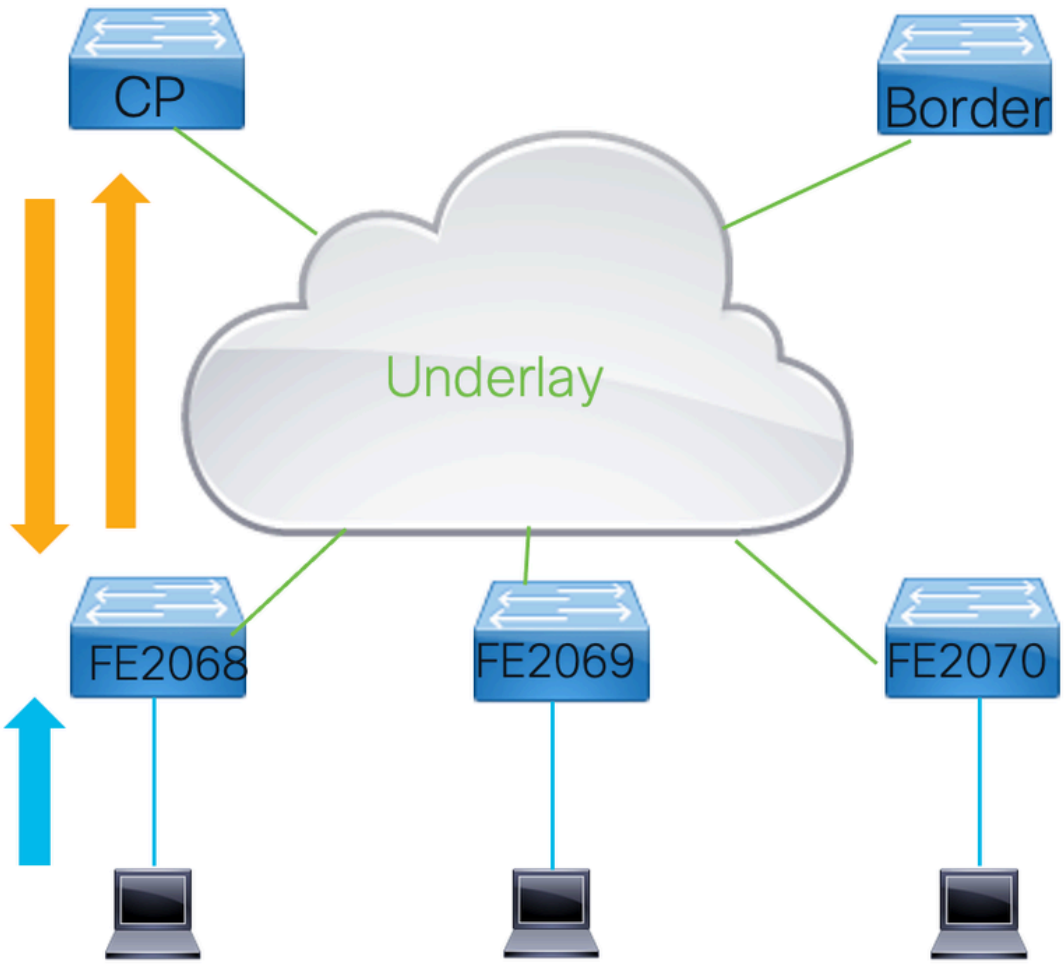
Para que o tráfego seja encaminhado através de uma estrutura LISP VXLAN, o RLOC de um destino precisa ser resolvido. Dentro de uma estrutura LISP VXLAN, isso é feito com o uso de um cache de mapas a partir do qual as informações são colocadas na base de informações de encaminhamento (FIB) do dispositivo de estrutura.

Com o LISP VXLAN, os caches de mapa de estruturas devem ser acionados devido a sinais de dados.

- Isso significa que o tráfego é encaminhado para a CPU e a CPU cria uma solicitação de mapa em direção ao nó do plano de controle para consultar as informações de RLOC para as quais os quadros em direção a esse EID precisariam ser enviados.
- Quando recebe uma solicitação de mapa, o plano de controle fornece as informações do Localizador de Roteamento associadas a esse EID ou envia uma resposta de mapa negativa.
- Quando envia uma resposta negativa ao mapa, o nó do plano de controle não indicaria apenas que a identificação eletrônica solicitada não é conhecida, ele ofereceria todo o bloco de identificações eletrônicas ao qual essa identificação pertenceria e para o qual não teria nenhum registro.

Com as informações dentro da resposta de mapa do nó do plano de controle, o cache de mapa é atualizado.

- O TTL para respostas de mapa é geralmente de 24 horas. (Para respostas de mapa negativas, normalmente é de apenas 15 minutos).
- Para Ethernet EID, as respostas negativas de mapa não são colocadas no cache de mapas. (Isso só é feito para instâncias da camada 3).



2.1 Cache de mapas Ethernet

Exiba o map-cache Ethernet com o comando show lisp instance-id <instance> map-cache

<#root>

```
FE2067#
show lisp instance-id 8191 ethernet map-cache

LISP MAC Mapping Cache for LISP 0 EID-table
Vlan 150 (IID 8191)
, 1 entries
0
019.3052.6d7f/48
, uptime: 00:00:07, expires: 23:59:52, via map-reply, complete
  Locator        Uptime    State  Pri/Wgt     Encap-IID

172.30.250.44
 00:00:07  up      10/10        -
```

Esse comando mostra a entrada do endereço MAC remoto que teria sido resolvida.

- Para disparar uma entrada de cache de mapa para uma instância Ethernet, o tráfego precisa ser enviado para um destino desconhecido.
- Isso faria com que o dispositivo de estrutura tentasse resolvê-lo por meio do LISP.
- Uma vez aprendido por meio de uma resposta de mapa, ele seria colocado no cache de mapas e os quadros subsequentes em direção ao destino da camada 2 seriam enviados diretamente ao Localizador de Roteamento aprendido.

Opcionalmente, em instâncias de camada 2 está o uso de inundação de tráfego de BUM .

- LISP/VXLAN não inunda o tráfego por padrão, pois usa uma tecnologia de sobreposição, mas um grupo Multicast IP pode ser configurado na rede subjacente (GRT) através da qual os quadros da camada 2 podem ser inundados.

Exibir o endereço do grupo subjacente de broadcast

<#root>

```
FE2068#
sh run | sec instance-id 8191

 instance-id 8191
  remote-rloc-probe on-route-change
```

```
  service ethernet
   eid-table vlan 150

broadcast-underlay 239.0.1.19

   database-mapping mac locator-set rloc_hosts
   exit-service-ethernet
  !
  exit-instance-id
```

2.2 Cache do mapa IP

Para instâncias de Camada 3, as informações do cache de mapas são semelhantes à criação de ethernet pelo tráfego enviado à CPU para sinalizar faz com que uma solicitação de mapa seja enviada.

- No entanto, para os pacotes de Camada 3, somente os pacotes são direcionados para a CPU para sinalizarem quando isso deve ser configurado. Isso é feito pelo comando map-cache configurado. Para IPv4, é 0.0.0.0/0 e ::0/0 para IPv6.
- A configuração dessa entrada do cache de mapas nos nós de borda deve ser feita com cuidado. Se um nó de borda estiver configurado com essa entrada map-cache 0.0.0.0/0 ou ::0/0 map-cache, ele tentará resolver destinos desconhecidos por meio da malha, em vez de roteá-la para fora da malha.

Exibir a configuração do cache de mapas

<#root>

FE2068#

sh run | sec instance-id 4099

```
 instance-id 4099
  remote-rloc-probe on-route-change
  dynamic-eid Fabric_VN_Subnet_1_IPv4
   database-mapping 172.24.1.0/24 locator-set rloc_hosts
   exit-dynamic-eid
  !
  dynamic-eid Fabric_VN_Subnet_1_IPv6
   database-mapping 2001:DB8::/64 locator-set rloc_hosts
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf Fabric_VN_1

map-cache 0.0.0.0/0 map-request

   exit-service-ipv4
  !
  service ipv6
   eid-table vrf Fabric_VN_1
```

```
   map-cache ::/0 map-request


   exit-service-ipv6
  !
  exit-instance-id
```

Os comandos map-cache 0.0.0.0/0 e ::/0 map-request fazem com que uma entrada map-cache seja configurada no map-cache com as ações "send-map-request". O tráfego que atinge esse aciona solicitações de mapa. Como as entradas do cache de mapas devem ser colocadas no FIB que funciona com base na correspondência mais longa, isso é aplicado a todo o tráfego IP roteado que não atinge nenhuma das entradas mais específicas.

- Em plataformas suportadas para evitar que o primeiro pacote seja descartado, a ação mostrada é send-map-request + encapsulate para o proxy ETR.
  Isso faz com que o primeiro pacote para um destino desconhecido dispare uma solicitação de mapa, bem como que o pacote seja encaminhado para o proxy-etr, se presente.

<#root>

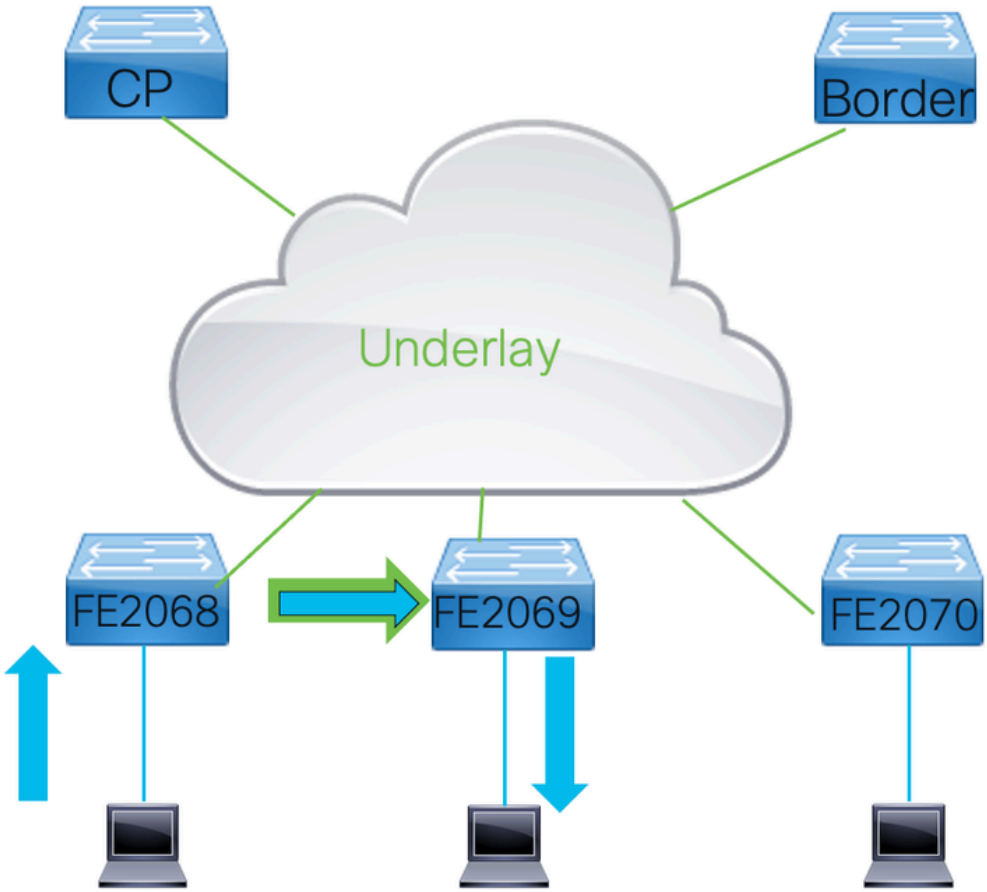
```
FE2067#

show lisp instance-id 4099 ipv4 map-cache


LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), 6 entries

0.0.0.0/0,

 uptime: 22:28:18, expires: 00:13:41, via map-reply, unknown-eid-forward
 action:

send-map-request + Encapsulating to proxy ETR


  PETR           Uptime    State      Pri/Wgt     Encap-IID  Metric
  172.30.250.19  22:28:18  up          10/10        -         0

10.48.13.0/24,

 uptime: 02:31:26, expires: 21:28:34, via map-reply, complete
  Locator        Uptime    State  Pri/Wgt     Encap-IID


172.30.250.19

  02:31:26  up      10/10        -

172.24.1.0/24

, uptime: 22:31:34, expires: never, via dynamic-EID, send-map-request


Negative cache entry, action: send-map-request



172.24.2.0/24

, uptime: 22:31:34, expires: never, via dynamic-EID, send-map-request
```

```
 Negative cache entry, action: send-map-request


172.24.2.2/32

, uptime: 00:00:21, expires: 23:59:38,

via map-reply, complet

e
  Locator        Uptime    State   Pri/Wgt     Encap-IID


172.30.250.44

  00:00:21  up      10/10        -

172.28.0.0/14,

 uptime: 22:28:22, expires: 00:13:39, via map-reply, unknown-eid-forward
  PETR           Uptime    State      Pri/Wgt     Encap-IID  Metric


172.30.250.19

  22:28:19  up          10/10        -         0
```

Nesta saída, algumas entradas são mostradas.

- 10.48.13.0/24 e 172.24.2.2/32 nesta saída são aprendidos por meio de resposta de mapa e são concluídos. O tráfego para esses destinos deve ser encapsulado e encaminhado para os respectivos localizadores.
- 172.28.0.0/14 é um exemplo de uma resposta de mapa negativa que foi recebida e um bloco de endereços IP que foi retornado. O tráfego em direção a essa sub-rede não dispara uma solicitação de mapa enquanto essa entrada estiver no cache de mapas.

Encaminhamento de tráfego através da malha



3.1 Encaminhamento de Camada 2 ou Camada 3

O tráfego em uma estrutura LISP/VXLAN pode ser encaminhado através de instâncias de camada 2 ou camada 3.

- A determinação de qual instância é usada depende do endereço MAC de destino dos quadros.
- Os quadros que são enviados para qualquer endereço MAC diferente daquele registrado no switch e que o quadro deve ser encaminhado devem usar a camada 2. Se o destino do pacote for o switch, ele será encaminhado através da camada 3.
- Essa é a mesma lógica que se aplicaria ao encaminhamento normal através de um switch da série Catalyst 9000.

3.2 Encaminhamento de Camada 2

O encaminhamento da camada 2 através de uma estrutura VXLAN LISP é feito com base no endereço MAC de destino da camada 2. Os destinos remotos são inseridos na tabela de endereços MAC com a interface de saída L2LI0.

Exibir as interfaces locais e remotas da camada 2

<#root>

FE2068#

show mac address-table vlan 150

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 150    0000.0c9f.f18e    STATIC      Vl150
 150    0050.5693.8930    DYNAMIC     Gi1/0/1
 150    2416.9db4.33fd    STATIC      Vl150
```

<- Local

```
 150    0019.3052.6d7f    CP_LEARN
```

L2LI0 <- Remote

```
Total Mac Addresses for this criterion: 3
Total Mac Addresses installed by LISP: REMOTE: 1
```

Para destinos desconhecidos, se configurado, o tráfego é enviado através do grupo Multicast IP configurado na subjacência.

- Para garantir a inundação correta de tráfego de broadcast, unicast e multicast desconhecidos (somente inundação de multicast seletivo), é necessário um ambiente multicast operacional corretamente na subjacência.
- O tráfego que seria enviado através desse grupo de subjacência de multicast deve ser encapsulado em VXLAN.
- Todas as outras bordas devem se unir ao grupo multicast, receber tráfego e desencapsular o tráfego para instâncias conhecidas da camada 2.

Exibir o grupo Multicast IP subjacente

<#root>

FE2068#

sh ip mroute 239.0.19.1

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
```

```
       x - VxLAN group, c - PFP-SA cache created entry,
       * - determined by Assert, # - iif-starg configured on rpf intf,
       e - encap-helper tunnel flag, l - LISP decap ref count contributor
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
                          t - LISP transit group
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.0.1.19), 00:02:36/stopped, RP 172.31.255.1, flags: SJCF
  Incoming interface: GigabitEthernet1/0/23, RPF nbr 172.30.250.42
  Outgoing interface list:
    L2LISP0.8191, Forward/Sparse-Dense, 00:02:35/00:00:24, flags:
(
```

172.30.250.44, 239.0.1.19

```
), 00:02:03/00:00:56, flags: FT
  Incoming interface:
```

Null0

```
, RPF nbr 0.0.0.0
  Outgoing interface list:
```

GigabitEthernet1/0/23

```
, Forward/Sparse, 00:02:03/00:03:23, flags:
(
```

172.30.250.30, 239.0.1.19

```
), 00:02:29/00:00:30, flags: JT
  Incoming interface:
```

GigabitEthernet1/0/23

```
, RPF nbr 172.30.250.42
  Outgoing interface list:
```

L2LISP0.8191

```
, Forward/Sparse-Dense, 00:02:29/00:00:30, flags:
```

Esta saída mostra uma entrada S,G para todas as outras bordas na estrutura em que os clientes estão configurados para enviar tráfego inundado. Ele também mostra uma entrada S,G com o Loopback0 desse dispositivo Edge como a origem.

Para o lado do receptor do tráfego através do grupo de multicast subjacente, o comando show ip mroute também mostra o L2LISP0.<instance>
isso indicaria para quais instâncias da camada 2 esse dispositivo de borda desencapsularia o tráfego inundado e o encaminharia para seu
interfaces relevantes.

3.3 Informações de encaminhamento de Camada 3

Para determinar como o tráfego é encaminhado quando uma estrutura LISP VXLAN é implantada,

é importante verificar o CEF.

- O LISP, ao contrário dos protocolos de roteamento tradicionais, insere a direção de roteamento não na tabela de roteamento, mas interage diretamente com o CEF para atualizar o FIB.

Para um determinado destino remoto, as informações do cache de mapas contêm as informações de localizador a serem usadas.

Exibir as informações de localizador

<#root>

```
FE2067#
sh lisp instance-id 4099 ipv4 map-cache 172.24.2.2

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), 1 entries

172.24.2.2/32
, uptime: 11:19:02, expires: 12:40:57, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 11:19:02, map-source: 172.30.250.44
  Idle, Packets out: 2(1152 bytes), counters are not accurate (~ 11:18:35 ago)
  Encapsulating dynamic-EID traffic
  Locator        Uptime    State  Pri/Wgt     Encap-IID

172.30.250.44
  11:19:02  up      10/10        -
    Last up-down state change:         11:19:02, state change count: 1
    Last route reachability change:    11:19:02, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            11:19:02 (rtt 2ms)
```

A partir do cache de mapas, o localizador a ser usado para esse EID é 172.30.250.44. Portanto, o tráfego para esse destino deve ser encapsulado e o cabeçalho IP externo tem um endereço IP de destino 172.30.250.44.

Na tabela de roteamento para o VRF usado para essa instância, essa entrada não é mostrada.

<#root>

```
FE2067#
show ip route vrf Fabric_VN_1

Routing Table: Fabric_VN_1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
Gateway of last resort is not set
      172.24.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.24.1.0/24 is directly connected, Vlan150
l        172.24.1.4/32 [10/1] via 172.24.1.4, 06:11:02, Vlan150
L        172.24.1.254/32 is directly connected, Vlan150
C        172.24.2.0/24 is directly connected, Vlan151
L        172.24.2.254/32 is directly connected, Vlan151
```

As saídas de CEF fornecem mais informações sobre o encaminhamento através da estrutura LISP VXLAN.

- Quando a palavra-chave detail do comando show ip cef é adicionada, ela não apenas fornece o destino do quadro encapsulado a ser enviado.
- A interface de saída com essa saída é LISP 0.<instance> indica que o tráfego é enviado encapsulado.

<#root>

```
FE2067#
```

sh ip cef vrf Fabric_VN_1 172.24.2.2 detail

```
172.24.2.2/32, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 2 packets 1152 bytes
```

fwd action encap

```
, dynamic EID need encap
  SC inherited: LISP cfg dyn-EID - LISP configured dynamic-EID
  LISP EID attributes: localEID No, c-dynEID Yes, d-dynEID No, a-dynEID No
  SC inherited: LISP generalised SMR - [enabled, inheriting, 0x7FF95B3E0BE8 locks: 5]
  LISP source path list
```

nexthop 172.30.250.44 LISP0.4099

```
  2 IPL sources [no flags]
```

nexthop 172.30.250.44 LISP0.4099

Como o tráfego seria enviado encapsulado em direção ao próximo salto, a próxima etapa é

executar um show ip cef <próximo salto> para ver a interface de saída na qual o pacote também seria roteado.

Execute para ver a interface de saída

<#root>

```
FE2067#
sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23
```

Note: Há dois níveis diferentes de roteamento ECMP (Equal Cost Multiple Path) possíveis.

- O tráfego pode ter a carga balanceada na sobreposição caso haja 2 RLOCs anunciados e pode ter a carga balanceada na rede subjacente se existirem caminhos redundantes para alcançar um endereço IP RLOC.
- Como a porta de destino UDP é fixa a 4789 e os endereços IP de origem e de destino para todos os fluxos entre dois dispositivos de estrutura são os mesmos, alguma forma de mecanismo antipolarização precisa ocorrer para evitar todos os pacotes roteados no mesmo caminho.
- Com a LISP VXLAN, essa é a porta de origem UDP no cabeçalho externo que seria diferente para diferentes fluxos na rede de estouro.

3.4 Formato do pacote

- Dentro das estruturas LISP VXLAN, todo o tráfego é completamente encapsulado em VXLAN. Isso inclui todo o quadro da Camada 2 para poder suportar as sobreposições da Camada 2 e da Camada 3.
  Para quadros de Camada 2, o cabeçalho original é encapsulado. Para quadros enviados através de uma ocorrência de Camada 3, um cabeçalho fictício de Camada 2 é usado.

<#root>

```
Ethernet II, Src: 24:16:9d:3d:56:67 (24:16:9d:3d:56:67), Dst: 6c:31:0e:f6:21:c7 (6c:31:0e:f6:21:c7)
 Internet Protocol Version 4, Src: 172.30.250.30, Dst: 172.30.250.44
  User Datagram Protocol, Src Port: 65288, Dst Port: 4789
   Virtual eXtensible Local Area Network
   Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
   1... .... .... .... = GBP Extension: Defined
   .... .... .0.. .... = Don't Learn: False
```

```
.... 1... .... .... = VXLAN Network ID (VNI): True
.... .... .... 0... = Policy Applied: False
.000 .000 0.00 .000 = Reserved(R): 0x0000

Group Policy ID: 16


VXLAN Network Identifier (VNI): 4099


Reserved: 0
 Ethernet II, Src: 00:00:00:00:80:a3 (00:00:00:00:80:a3), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
  Internet Protocol Version 4, Src: 172.24.1.4, Dst: 172.24.2.2
   Internet Control Message Protocol
```

Como visto pela captura de amostra de um quadro transportado através de uma estrutura LISP VXLAN, há o quadro totalmente encapsulado dentro do pacote vxlan. Como seu quadro de camada 3, o cabeçalho ethernet é um cabeçalho fictício.

No cabeçalho VXLAN, o campo Identificador de Rede VLAN transporta o ID de instância LISP ao qual o quadro pertence.

- Por meio do campo Group Policy ID (ID da política de grupo), é transportada a marca SGT dos quadros.
- Isso é definido no ingresso na malha e levado em direção à malha até que a aplicação da política baseada em grupo seja feita.

Autenticação e aplicação de segurança

4.1 Autenticação da porta do switch

Para atribuir dinamicamente endpoints às respectivas VLANs e atribuir a elas uma autenticação de tag SGT pode ser usada.

- Os protocolos de autenticação como Dot1x/MAB/central webauth podem ser implantados para autenticar e autorizar usuários e endpoints em um servidor Radius que envia atributos de volta ao switch para permitir acesso à rede para o cliente/endpoint no pool correto e com a autorização de acesso à rede correta.

Para a estrutura LISP VXLAN, existem alguns atributos comuns de radius:

- Atribuição De Vlan: Esses atributos são definidos como ID ou nome da VLAN do servidor radius para os switches em que um ponto final pode ser atribuído a uma instância específica do LISP de Camada 2/Camada 3.
- Valor SGT: Este atributo define um SGT e atribui um ponto final a este SGT. Isso seria usado para políticas baseadas em grupos em relação a esse ponto final, bem como atribui um valor SGT a todos os quadros enviados através da estrutura originada por esse ponto final.

- Autorização de voz: Os dispositivos de voz operam na vlan de voz. Isso define a autorização de voz que o endpoint teria permissão para enviar e receber tráfego na vlan de voz configurada em uma porta. Isso para separar o tráfego de voz e dados em suas respectivas VLANs
- Intervalo de sessão: Vários endpoints têm seus próprios timeouts para as sessões. Um tempo limite pode ser enviado do servidor radius para indicar com que frequência um cliente precisa reautenticar
- Modelo: Para alguns endpoints, um modelo diferente precisa ser aplicado em uma porta para operar corretamente. Um nome de modelo pode ser enviado do servidor Radius, indicando o que precisa ser aplicado à porta

Verifique o resultado da autenticação em uma porta usando o comando show access-session

<#root>

FE2067#

show access-session interface Gi1/0/1 details

Interface: GigabitEthernet1/0/1
IIF-ID: 0x1FF97CF7
MAC Address: 0050.5693.f1b2
IPv6 Address: FE80::3EE:5111:BA77:E37D
IPv4 Address: 172.24.1.4
User-Name: 00-50-56-93-F1-B2
Device-type: Microsoft-Workstation
Device-name: W7180-PC
Status:

Authorized

Domain:

DATA

Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Acct update timeout: 172800s (local), Remaining: 172678s
Common Session ID: 9256300A000057B8376D924C
Acct Session ID: 0x00016d77
Handle: 0x85000594
Current Policy: PMAP_DefaultWiredDot1xClosedAuth_1X_MAB

Local Policies:

Server Policies:

Vlan Group: Vlan: 150

SGT Value: 16

```
Method status list:
Method State
dot1x
```

Stopped

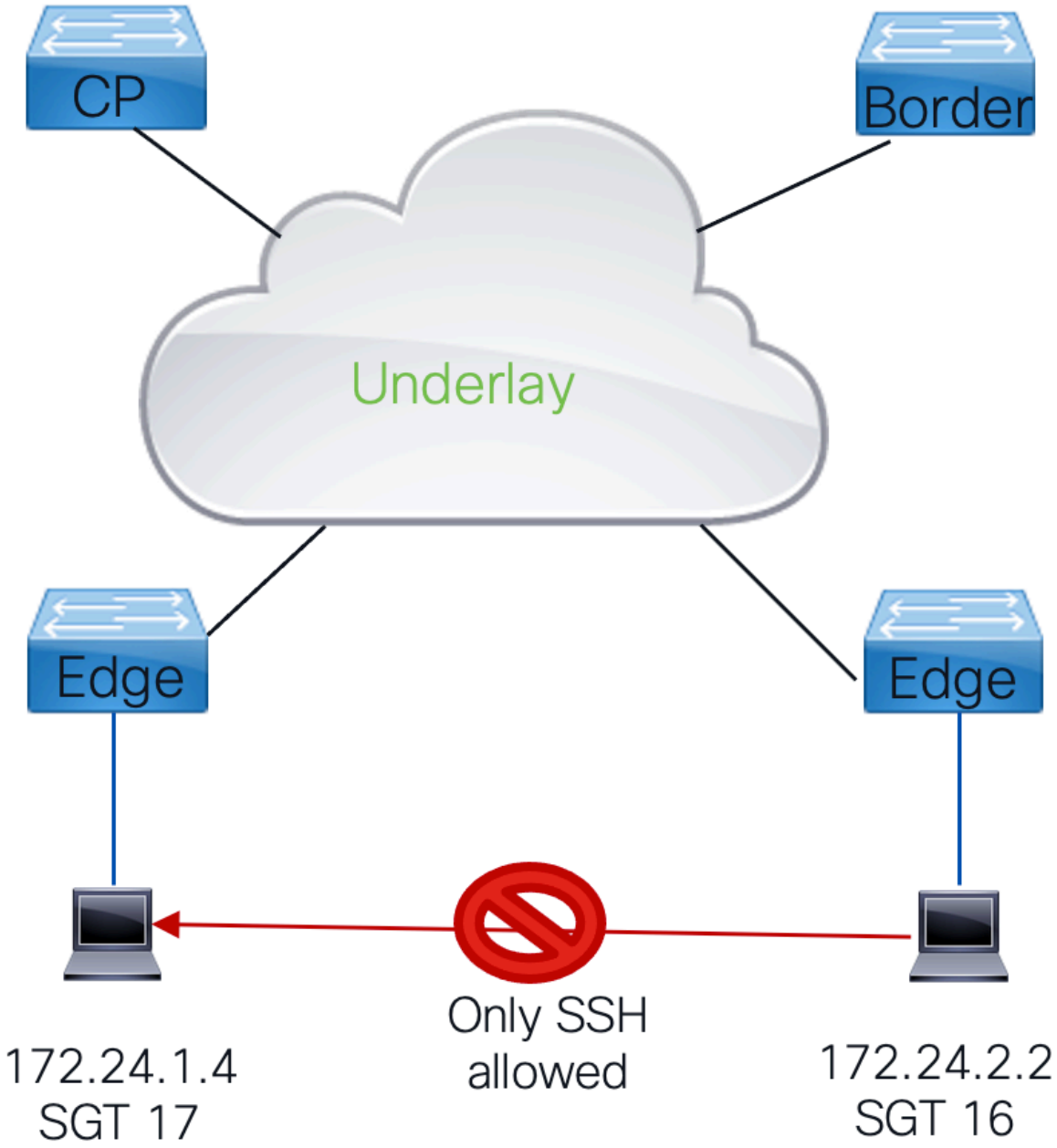
```
mab Authc
```

Success

Observe estes campos-chave:

- Endereços IPv4 e IPv6: Tipicamente aprendido através de rastreamento de dispositivos.
- Nome de usuário: Este é o nome de usuário usado para autenticação.
    - Para Dot1x, este normalmente é o usuário que autentica.
    - Quando MAB é usado, este é o endereço MAC da estação que é enviada para Radius como nome de usuário e senha para autenticação.
- Status: Indica o status da autenticação e o resultado da autenticação.
- Domínio: Para endpoints normais, esse seria o domínio de dados, de modo que o tráfego seria enviado/recebido sem marcação na porta. (Para dispositivos de voz, pode ser definido como Voz)
- Políticas de servidor: Este é o local onde as informações do servidor Radius, como atribuição de Vlan e atribuição de SGT
- Lista de status do método: Isso mostra uma visão geral dos métodos executados.
    - O dot1x padrão é executado antes do MAB.
    - Se um endpoint não respondesse a quadros EAPOL, o método falharia em mab.
    - Isso mostraria o dot1x como tendo falhado.
    - O MAB mostra que o sucesso da autenticação indica que ele conseguiu se autenticar, ele não reflete se o resultado da autenticação seria uma aceitação ou rejeição de acesso.

4.2 Políticas de tráfego e políticas baseadas em grupo (CTS)



Dentro de uma estrutura LISP VXLAN, o CTS é usado para aplicar políticas de tráfego:

- A arquitetura da política baseada em grupos é baseada em Tags de grupo seguras.
- Todo o tráfego dentro da estrutura é atribuído na entrada e na marca SGT, que é transportada pela estrutura em cada quadro.
- Quando esse tráfego sai da malha, as políticas de tráfego são aplicadas.
- Isso é feito em Políticas baseadas em grupos que verificam as tags de grupo de origem e destino do pacote em relação à matriz que consiste em SGTs de origem e destino, onde o resultado é um SGACL que define qual tráfego seria ou não permitido.
- Quando não houver correspondência específica dentro da matriz para o SGT Origem-Destino, a ação padrão definida será aplicada.

4.3 Ambiente CTS

Para operar com políticas baseadas em grupo, a primeira coisa que é necessária para um dispositivo de estrutura é obter um pacote CTS.

- Este pacote deve ser usado dentro de quadros radius para autorizar os quadros RADIUS no Cisco ISE. Isso é usado para definir o campo cts-pac-opaque dentro dos quadros Radius.

Exibir as informações do pacote CTS

```
<#root>

FE2067#

sh cts pacs

AID:

C7105D0DA108B6AE0FB00499233B9C6A

PAC-Info:
PAC-type = Cisco Trustsec
AID: C7105D0DA108B6AE0FB00499233B9C6A
I-ID: FOC2410L1ZZ
A-ID-Info: Identity Services Engine
Credential Lifetime:

18:05:51 UTC Sat Jun 24 2023

PAC-Opaque: 000200B80003000100040010C7105D0DA108B6AE0FB00499233B9C6A0006009C00030100C5C0B998FB5E8C106F6

Refresh timer is set for 12w0d
```

É importante garantir que o pacote CTS esteja configurado e seja válido. Isso é atualizado automaticamente pelo dispositivo Fabric.

Note: Para disparar manualmente uma atualização, o comando "cts refresh pac" pode ser emitido.

Para que as políticas baseadas em grupo operem, ele faz o download dos dados do ambiente, bem como das informações de política necessárias.

- Esses dados de ambiente contêm a marca CTS que o próprio switch usa, bem como o download da tabela de todos os grupos de política baseados em grupos conhecidos no servidor Radius.

Exibir dados do ambiente cts

<#root>

FE2067#

sh cts environment-data

CTS Environment Data
====================
Current state =

COMPLETE

Last status =

Successful

Service Info Table:
Local Device SGT:
SGT tag =

2-00:TrustSec_Devices

Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server:

10.48.13.221

, port 1812,

A-ID C7105D0DA108B6AE0FB00499233B9C6A

Status = ALIVE
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
0-00:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:Production_Users
8-00:Developers
9-00:Auditors
10-00:Point_of_Sale_Systems
11-00:Production_Servers
12-00:Development_Servers
13-00:Test_Servers
14-00:PCI_Servers
15-00:BYOD
16-00:Fabric_Client_1
17-00:Fabric_Client_2
255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 11:46:41 UTC Fri Mar 31 2023
Env-data expires in 0:19:17:04 (dd:hr:mm:sec)
Env-data refreshes in 0:19:17:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
Retry_timer (60 secs) is not running

Quando políticas baseadas em grupo são usadas, as únicas políticas que são baixadas são as marcas CTS com as quais o dispositivo tem endpoints locais que ele precisa aplicar.

- Para poder verificar o mapeamento do endereço IP (ou sub-rede) para um grupo de políticas baseado em grupos, o comando "show cts role-based sgt-map vrf <vrf> all" pode ser usado.

Exibir todas as informações de IP para SGT conhecidas para um VRF

<#root>

```
FE2067#

sh cts role-based sgt-map vrf Fabric_VN_1 all


Active IPv4-SGT Bindings Information
IP Address SGT Source
========================================

172.24.1.4 17 LOCAL



172.24.1.254 2 INTERNAL



172.24.2.254 2 INTERNAL


IP-SGT Active Bindings Summary
========================================
Total number of LOCAL bindings = 1
Total number of INTERNAL bindings = 2
Total number of active bindings = 3
Active IPv6-SGT Bindings Information
IP Address SGT Source
============================================================

2001:DB8::1 2 INTERNAL



2001:DB8::F304:BCCD:6BF3:BFAF 17 LOCAL


IP-SGT Active Bindings Summary
========================================
Total number of LOCAL bindings = 1
Total number of INTERNAL bindings = 1
Total number of active bindings = 2
```

Esta saída mostra todos os endereços IP conhecidos (e sub-redes) para um determinado VRF e suas associações de política baseadas em grupo.

- Como pode ser visto, há um endereço IP de um endpoint atribuído ao grupo 17 de políticas baseadas em grupos e que tem origem local.
- Este é o resultado da autenticação que ocorre na porta e onde os resultados indicaram que a marca está associada a esse ponto final.
- Ele também destaca os próprios endereços IP dos switches que recebem a marca device-sgt como origem interna.
- As marcas de política baseadas em grupo também podem ser atribuídas por meio de configuração ou por meio de uma sessão SXP em direção ao ISE.

Quando um dispositivo toma conhecimento de uma marca SGT, ele tenta fazer o download das políticas associadas a ele a partir do servidor ISE.

- O comando show cts authorization entries dá uma visão geral de quando houve uma tentativa de fazer o download e se eles foram ou não baixados sucessivamente.

Note: As políticas devem ser atualizadas periodicamente em caso de alterações nas políticas. O ISE também pode enviar um comando CoA para que o switch seja acionado para fazer o download de novas políticas quando forem feitas alterações. Para atualizar manualmente as diretivas, o comando "cts refresh policy" é emitido.

Exibir uma visão geral das políticas que tentaram ser baixadas e se elas foram ou não baixadas sucessivamente

<#root>

```
FE2067#
show cts authorization entries

Authorization Entries Info
==========================
Peer name = Unknown-0
Peer SGT =
0-00:Unknown

Entry State =
COMPLETE

Entry last refresh = 22:14:46 UTC Thu Mar 30 2023
SGT policy last refresh = 22:14:46 UTC Thu Mar 30 2023
SGT policy refresh time = 86400
Policy expires in 0:05:23:44 (dd:hr:mm:sec)
Policy refreshes in 0:05:23:44 (dd:hr:mm:sec)
Retry_timer = not running
Cache data applied = NONE
Entry status =
```

SUCCEEDED

AAA Unique-ID = 11

Peer name = Unknown-17
Peer SGT =

17-01:Fabric_Client_2

Entry State =

COMPLETE

Entry last refresh = 11:47:31 UTC Fri Mar 31 2023
SGT policy last refresh = 11:47:31 UTC Fri Mar 31 2023
SGT policy refresh time = 86400
Policy expires in 0:18:56:29 (dd:hr:mm:sec)
Policy refreshes in 0:18:56:29 (dd:hr:mm:sec)
Retry_timer = not running
Cache data applied = NONE
Entry status =

SUCCEEDED

AAA Unique-ID = 4031

Se houver políticas baixadas, elas poderão ser exibidas com o comando "show cts rolebased policies".

<#root>

FE2067#

sh cts role-based permissions

IPv4 Role-based permissions

default

:

Permit IP-00

IPv4 Role-based permissions from

group 17:Fabric_Client_2 to group 16:Fabric_Client_1

:

PermitWeb-02

RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Esse comando mostra todas as políticas que o dispositivo aprendeu. No servidor ISE existem potencialmente mais políticas presentes para grupos diferentes, mas o dispositivo tenta fazer download apenas de políticas para as quais ele conhece endpoints. Isso preserva recursos valiosos de hardware.

Esse comando também mostra a ação padrão que deve ser aplicada ao tráfego para o qual nenhuma entrada mais específica é conhecida. Nesse caso, o IP de permissão, para que todo o tráfego que não corresponder a uma entrada específica na tabela possa passar.

Execute show cts rbacl <name>para obter mais detalhes sobre o conteúdo exato do RBACL que foi baixado

<#root>

```
FE2067#

sh cts rbacl permitssh


CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
name =

permitssh

-03
IP protocol version = IPV4
refcnt = 2
flag = 0x41000000
stale = FALSE
RBACL ACEs:

permit tcp dst eq 22


permit tcp dst eq 23


deny ip
```

Nesse caso, o único tráfego permitido para ser enviado ao ponto final com esse RBACL aplicado a ele são pacotes tcp para 22 (SSH) e 23 (Telnet).

Note: RBACL só funciona em uma direção. A menos que haja uma política no tráfego de retorno, ela é aplicada com a política padrão. O tráfego que entra na estrutura não é imposto, ele envia através da estrutura com a marca SGT conhecida no nó de entrada. Ele só é imposto quando sai da malha e deve ser imposto nas políticas presentes nesse dispositivo. Normalmente, essas políticas seriam as mesmas, mas é possível estender o domínio CTS, por exemplo, com um firewall onde outras políticas poderiam ter sido

---

definidas, dependendo das políticas de segurança implantadas.

Execute 'show cts role-based counters' para validar se os quadros são ou não descartados

- Esse comando mostra os contadores cumulativos para o switch inteiro. Não há nenhum comando equivalente para cada interface.

<#root>

FE2067#

sh cts role-based counters

Role-based IPv4 counters
From To SW-Denied HW-Denied SW-Permitt HW-Permitt SW-Monitor HW-Monitor

*** ***

0 0 3565235 7777106

0 0

17 16

0

3 0 3412 0

0

16 17

0 5812 0 871231 0

0

Esta visão geral mostra todas as entradas conhecidas que o switch conhece neste caso para poder corresponder o tráfego de 17 a 16 e de 16 a 17.

- Qualquer outra correspondência que se enquadre no * * e obtenha a ação padrão aplicada, portanto, se qualquer tráfego, por exemplo, de 18 a 16, vier, ele não corresponderá à matriz conhecida no switch e terá a ação padrão aplicada.

Mesmo que os contadores sejam cumulativos, eles dão uma boa indicação se o tráfego é descartado.

- Para determinar qual tráfego atingiria uma entrada, a palavra-chave log poderia ser adicionada no servidor ISE às respectivas políticas, o que faz com que o switch forneça mensagens de log quando essa entrada for atingida.
- Isso pode ser feito para a ação padrão (* *) ou para uma das entradas mais específicas na matriz.

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.