Solución de problemas de LISP VXLAN Fabric en switches Catalyst serie 9000

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
  - Fabric basado en LISP VXLAN
    - Tecnologías utilizadas para crear un fabric VXLAN LISP
    - Componentes clave del fabric LISP VXLAN
  - Registro de terminales
    - Información importante
    - Pasos de registro
- Verificación
  - 1.1 Aprendizaje de direcciones MAC
  - 1.2 Aprendizaje dinámico de direcciones IP
  - 1.3 Registro de EID con el plano de control
  - 1.4 Información del plano de control
- Resolver destinos remotos
  - 2.1 Caché de mapas Ethernet
  - 2.2 Caché de mapa IP
- Reenvío de tráfico a través del fabric
  - 3.1 Reenvío de capa 2 o capa 3
  - 3.2 Reenvío de capa 2
  - 3.3 Información de reenvío de capa 3
  - 3.4 Formato de paquete
- Autenticación y aplicación de seguridad
  - 4.1 Autenticación del puerto del switch
  - 4.2 Políticas de tráfico y políticas basadas en grupos (CTS)
  - 4.3 Entorno CTS
- Información Relacionada

Introducción

Este documento describe los componentes básicos de un entramado basado en VXLAN LISP y cómo verificar su funcionamiento.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Fabric basado en LISP VXLAN

El propósito de implementar una red VXLAN LISP es poder crear una arquitectura en la que varias redes superpuestas, también conocidas como redes virtuales, se definan sobre una red subyacente.

- La red subyacente en dicha topología actuaría principalmente como una capa de transporte y no sería consciente de las topologías de superposición que se ejecutan en ella.
- Las redes superpuestas se pueden agregar y eliminar sin que ello afecte a la red subyacente.
- El uso de redes superpuestas separa eficazmente a los usuarios de la red subyacente.

Tecnologías utilizadas para crear un fabric VXLAN LISP

Protocolo de separación de identidades de ubicación (LISP)

- El protocolo LISP es el protocolo del plano de control que se utiliza dentro del fabric. Se ejecuta en todos los dispositivos de fabric para crear el fabric y controlar cómo se envía el tráfico a través del fabric.
- LISP crea 2 espacios de direcciones. Una es para el localizador de routing (RLOC), que se utiliza para anunciar la disponibilidad. El otro espacio de dirección es para los identificadores de punto final (EID) , es decir, donde residen los puntos finales y se utiliza para la superposición.

- Dentro de LISP, los EID se anuncian con un RLOC anunciado. Si un EID mueve todo lo que debe hacerse es actualizar el Localizador de enrutamiento asociado con él.
- Alcanzar un punto final con tráfico LISP hacia un EID debe encapsularse y tunelizarse hacia el RLOC que lo desencapsula y lo reenvía al punto final.

Políticas basadas en grupos

- Para poder permitir la segmentación dentro de un grupo de fabric se utilizan políticas basadas.
- Cuando se implementan políticas basadas en grupos, el tráfico se clasifica con Secure Group en lugar de basarse en la IP de origen/destino.
- Esto reduce la complejidad de las listas de control de acceso complejas. En lugar de las listas de direcciones IP que deben mantenerse, las direcciones IP/subredes se asignan a una etiqueta de grupo seguro.
- Al ingresar al entramado se etiqueta con una SGT cuando el tráfico sale del entramado, el destino de la trama se busca para su SGT .
- Con el uso de una matriz, la SGT de origen y de destino coincide y se aplica una ACL de grupo seguro para aplicar el tráfico a medida que sale del fabric.

Encapsulación VXLAN

- Dentro del fabric, VXLAN se utiliza para encapsular todo el tráfico
- La ventaja de utilizar VXLAN sobre la encapsulación LISP heredada es que permite encapsular toda la trama de Capa 2, no sólo la trama de Capa 3. A medida que toda la trama se encapsula, permite que las superposiciones sean tanto de Capa 2 como de Capa 3.
- VXLAN utiliza UDP con el puerto de destino 4789. Esto permite que las tramas VXLAN LISP se transporten también a través de un dispositivo que no sería consciente de la topología de superposición.
- Dado que VXLAN encapsula toda la trama, es importante aumentar la MTU para que no se necesite fragmentación, ya que el tráfico se envía entre RLOC. Cualquier dispositivo intermedio tendría que soportar una MTU más grande para transportar las tramas encapsuladas.

Autenticación

- Para poder asignar terminales a sus respectivos recursos, se puede utilizar la autenticación.
- Con protocolos como 802.1x, los terminales MAB y Webauth se pueden autenticar y/o crear perfiles en un servidor Radius y se les puede conceder acceso a la red en función de sus perfiles de autorización.
- Con sus respectivos atributos Radius, los terminales se pueden asignar a sus respectivas VLAN, SGT y cualquier otro atributo para proporcionar un acceso a la red de usuario/terminal.

Componentes clave del fabric LISP VXLAN

nodo Plano de control

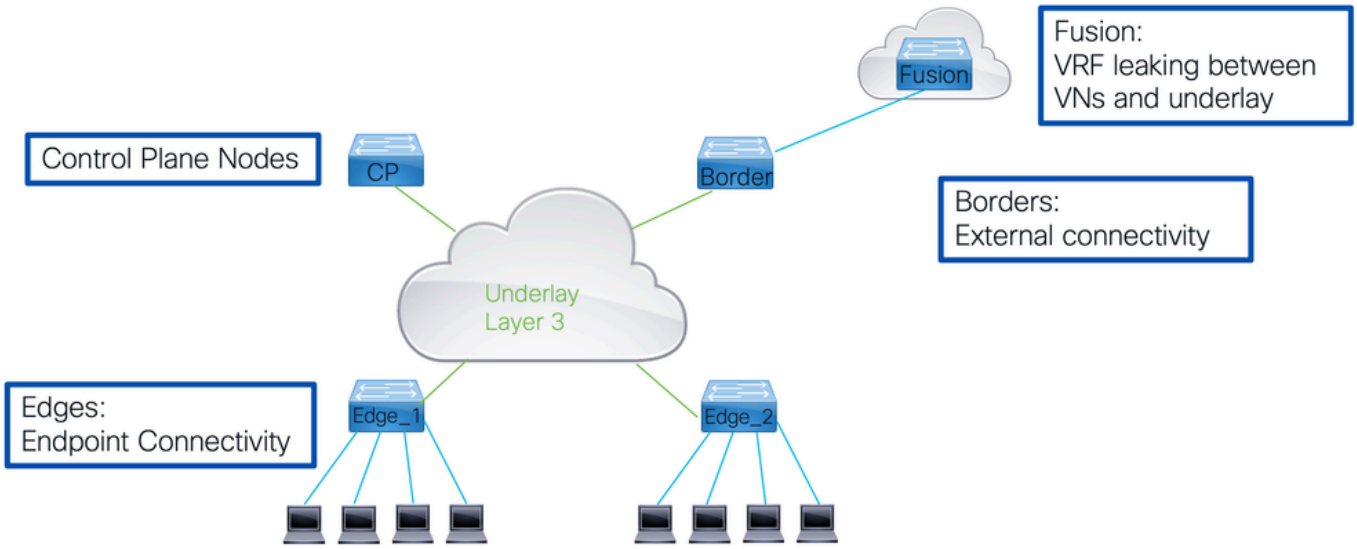
- contiene la funcionalidad de servidor de mapas LISP y de resolución de mapas.
- Todos los demás dispositivos de fabric consultan el nodo del plano de control para la ubicación de EID y envían registros para su EID a los nodos del plano de control.
- Esto proporciona a los nodos del plano de control una vista completa del fabric con respecto a los RLOC detrás de los diversos EID.

Nodos de borde

- Proporciona conectividad fuera del fabric a otros fabrics o al mundo exterior.
- Los bordes internos importan rutas en el fabric y las registran con los nodos del plano de control.
- Las fronteras externas se conectan con el mundo exterior y proporcionan una ruta predeterminada fuera del fabric para destinos IP desconocidos.

Nodos de borde

- Estos nodos proporcionan conectividad a los terminales dentro del fabric.
- En la definición de LISP, estos serían XTRs, ya que realizarían la función de un router de túnel de entrada (ITR) y un router de túnel de salida (ETR).



Los nodos no se limitan a realizar una sola tarea.

- Pueden realizar una combinación o incluso todas las funciones dentro del fabric.
- Cuando un nodo de borde y un nodo de plano de control residen en un dispositivo, se denominan "colocados".
- Si ese nodo también proporciona la funcionalidad Edge, se le denominará Fabric In A Box (FIAB).

Los bordes proporcionan transferencias al resto de la red y utilizan VRF Lite.

- Cada superposición o red virtual está asociada a una instancia VRF en el nodo de borde.

- Para conectar los distintos VRF entre sí se utiliza un router Fusion. Ese router de fusión no es parte del fabric en sí, pero es crucial para la operación para poder conectar las redes superpuestas al fabric.

Otro concepto importante dentro de un fabric LISP VXLAN es el concepto de utilizar un Anycast IP.

- Esto significa que en todos los dispositivos periféricos se replican la dirección IP y sus direcciones MAC para las interfaces virtuales conmutadas (SVI).
- Cada Edge tiene la misma configuración en la SVI con respecto a las direcciones IPv4, IPv6 y MAC.
- Solucionar este problema plantea algunos retos.
    - Para probar la disponibilidad con ping funciona con dispositivos conectados locales.
    - Para llegar a destinos remotos a través del fabric VXLAN LISP, no devuelve una respuesta, ya que el dispositivo que envía una respuesta también envía esto a la dirección IP de difusión por proximidad que se envía al dispositivo de fabric local que no sabe qué otro nodo de fabric ha enviado el ping original.

Registro de terminales

Para que un fabric VXLAN LISP funcione, es fundamental que el nodo del plano de control sea consciente de cómo se puede acceder a todos los terminales a través del fabric.

- Para que el plano de control obtenga información sobre todos los EID de la red, es necesario que todos los demás dispositivos de fabric registren todos los EID que conozca en el plano de control.
- Un nodo de fabric envía mensajes de registro de mapa LISP al nodo del plano de control. Entre la información que se anuncia con el mensaje map-register.

Información importante

Identificador de instancia de LISP:

- Este identificador se transporta a través del fabric e indica qué red virtual se va a utilizar.
- Dentro de un fabric VXLAN LISP por superposición de capa 3, se utiliza una instancia por VLAN utilizada en el fabric y también hay una instancia de capa 2.

Terminales identificados (EID):

- Si se trata de una instancia de capa 2 o capa 3, se trata de la dirección MAC, la ruta de host IP (/32 o /128) o una subred IP registrada

Localizador de routing (RLOC):

- Se trata de la dirección IP propia del nodo de fabric con la que anuncia la disponibilidad en el lugar donde otros dispositivos de fabric envían tráfico encapsulado que tendría que alcanzar el EID.

Indicador de proxy:

- Cuando se establece este indicador, permite que el nodo del plano de control responda a las solicitudes de asignación de otros nodos de fabric directamente , sin que el indicador proxy establezca todas las solicitudes que se reenviarán al nodo de fabric que registró el EID.

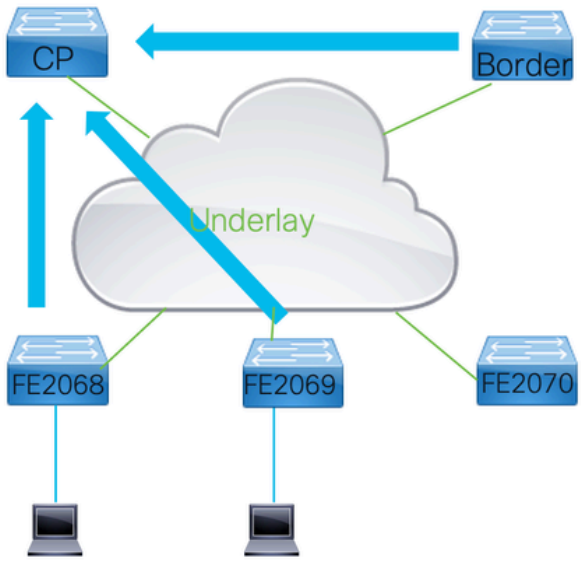
Pasos de registro

Paso 1: Los dispositivos de fabric obtienen información sobre los identificadores de terminales. Esto puede hacerse a través de la configuración, los protocolos de routing o cuando se detecta en los dispositivos de fabric.

Paso 2: los dispositivos de fabric registran los terminales aprendidos con cada nodo del plano de control conocido y accesible dentro del fabric.

Paso 3: Los nodos del plano de control mantienen una tabla de EID registrados con el ID de instancia relacionado, el RLOC y el 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



Verificación

1.1 Aprendizaje de direcciones MAC

Para las Instancias de Capa 2, el EID que se utiliza son las direcciones MAC que se aprenden dentro de la VLAN asociada. Los bordes del fabric aprenden las direcciones de capa 2 a través de los métodos estándar en los switches.

Localice la VLAN asociada con un ID de instancia de capa 2 específico cuando se pueda revisar la configuración o el comando

Utilice "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 se ve en el resultado, el instance-id 8191 está asociado con VLAN 150. Esto hace que todas las direcciones MAC dentro de la vlan se registren con LISP y pasen a formar parte del fabric VXLAN de LISP.

```
<#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
```

Las entradas estáticas con la interfaz Vl150 son las direcciones MAC de la interfaz virtual del switch (interfaz vlan 150).

- Esas direcciones MAC no están registradas con el nodo del plano de control ya que serían las mismas en todos los dispositivos de borde.
- La entrada CP_LEARN mostrada son entradas que se aprenden a través del fabric. Para todas las demás entradas, si son dinámicas o estáticas, se registrarán con el nodo del plano de control.

Una vez que se aprenden a través de sus respectivos medios, aparecen en las salidas de la base de datos lisp, esta salida contiene todas las entradas locales en este dispositivo de fabric.

<#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 todas las direcciones MAC locales conocidas que se muestran en la base de datos, se muestra Locator.

- Esta es la ubicación que se utilizará para registrar esta entrada con el nodo del plano de control.
- También indicó el estado del Localizador.Las 2 direcciones MAC que pertenecían a la SVI de los Switches también se muestran pero se muestran con el indicador "no registrar" que impide que se registren.
- La entrada remota que se vio en el comando show mac address table no es una dirección MAC local y, como tal, no se muestra en la base de datos lisp.

Para una instancia de capa 2, no solo las direcciones MAC de capa 2 se aprenden como EID, sino que también es necesario aprender la información de resolución de direcciones de las tramas ARP y ND.

- Esto permite que el entramado VXLAN LISP pueda reenviar esas tramas ya que normalmente se inundan dentro de la VLAN.
- Como un ID de instancia de Capa 2 no siempre tiene la capacidad de inundar allí otro mecanismo que permitiría a los terminales resolver la información de resolución de direcciones para otros terminales en la misma instancia. Para esto, los dispositivos de fabric aprenden y registran esta información que se aprende localmente mediante el rastreo de dispositivos .
- Esto también se registra con los nodos del plano de control. Debido a la indagación ND o ARP, esos paquetes se envían a la CPU para activar una solicitud a los nodos del plano de control para ver si hay alguna dirección MAC conocida asociada.
- Si se recibe una respuesta positiva, los paquetes ARP/ND se reescriben de modo que la dirección MAC de destino se cambia de difusión o multidifusión a la dirección MAC de unidifusión.
- Este paquete reescrito se puede reenviar a través del fabric VXLAN LISP como una trama de unidifusión.

Para ver la información de resolución de direcciones que se conoce en el switch, se puede utilizar el comando show device-tracking database.

- Esto muestra todos los mapeos conocidos por el rastreo de dispositivos.
- Las direcciones IP propias de los switches se etiquetan como L(Local) y deben estar presentes en la base de datos de seguimiento de dispositivos.

Las entradas remotas también se muestran en esta salida.

- A medida que se resuelven después de que se ha indagado la solicitud ND o ARP, se colocan en la base de datos de seguimiento de dispositivos con una dirección de capa de enlace de 0000.0000.00fd.
- En el momento en que se resuelven, la información se cambia hacia la dirección mac resuelta y el puerto se cambia a Tu0.

Mostrar la base de datos de seguimiento de dispositivos

<#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
```

Muestre las asignaciones registradas localmente con el 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 Aprendizaje de direcciones IP dinámicas

En los dispositivos de fabric de una capa IP, una red virtual se forma asociando un ID de instancia de LISP con un VRF.

- A continuación, este VRF se configura en las distintas interfaces virtuales de switch (SVI) y pasan a formar parte de la red superpuesta de capa 3
- En la mayoría de los casos, estas SVI también pertenecen a las VLAN registradas con sus respectivas instancias de Capa 2.

Busque la asignación entre VRF e ID de instancia de LISP con el 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
```

Nota: Este comando también se puede utilizar para verificar las diversas funciones que se podrían habilitar para esta instancia, así como para mostrar los nodos del plano de control usados dentro del fabric VXLAN de LISP

Una vez que se crea una instancia de Capa 3 y se vincula a un VRF, se crea una interfaz LISP 0 <instance-id> que es visible en la configuración en ejecución y en show vrf.

- Esta interfaz NO necesita crearse manualmente y normalmente no necesita configuración (aparte de la configuración de multidifusión cuando se utiliza multidifusión subyacente).

<#root>

FE2068#

show vrf Fabric_VN_1

```
  Name                              Default RD            Protocols   Interfaces
```

Fabric_VN_1

ipv4,ipv6

LI0.4099

Vl150

Vl151

A diferencia de las tramas Ethernet donde todas las direcciones MAC en una VLAN se utilizan para IP, existe la necesidad de que las direcciones IP estén dentro de un rango EID dinámico para ser aprendidas.

Mostrar una instancia de 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

Las direcciones IP que se encuentran fuera de estos rangos definidos no se consideran aptas para el fabric y no se colocan en las bases de datos LISP ni se registran con los nodos del plano de control.

<#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
```

El resultado muestra toda la información de dirección IP conocida localmente.

- En el caso de los hosts, se trata normalmente de rutas de host (/32 o /128), pero también podrían ser subredes si se hubieran importado a la base de datos LISP en el nodo de borde.
- Las direcciones IP de la propia SVI se marcan como "no registrar" . Esto evita que todos los dispositivos de fabric registren la dirección IP de difusión ilimitada con el nodo del plano de control.

<#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 de EID con el plano de control

El registro de terminales en un fabric basado en LISP VXLAN se realiza mediante un registro fiable de LISP. Esto significa que todos los registros se realizan a través de una sesión TCP establecida , la sesión LISP. Desde cada dispositivo de fabric se establece una sesión LISP con cada uno de los nodos del plano de control en el fabric. A través de esta sesión LISP, se producen todos los registros. Si hay varios nodos del plano de control dentro de un fabric, se utilizarán para registrar los EID.

El estado es Inactivo cuando no hay nada que registrar en el dispositivo de fabric, lo que normalmente solo se produciría en las fronteras externas
que no registran ningún rango de IP con el nodo del plano de control o en dispositivos periféricos sin ningún terminal

El registro de EID se realiza a través de mensajes de registro LISP
que se envían a todos los nodos del plano de control configurados.

Para ver la sesión LISP en un dispositivo de fabric, se puede utilizar el comando show lisp session.
Muestra el estado de la sesión y el tiempo que ha estado activa.

<#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
```

La sesión LISP que se muestra como Caída puede ocurrir en dispositivos que no tienen ningún EID para registrarse con el nodo del plano de control.
Por lo general, se trata de nodos de borde que no importan rutas en el fabric o en los dispositivos

periféricos sin ningún terminal conectado.

Mostrar información más detallada sobre una sesión LISP con el 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 salida detallada de la sesión muestra qué instancias están activas con EID que están registradas con los nodos del plano de control.

<#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

Cuando se observa el número de sesiones en un nodo del plano de control, normalmente se muestran más sesiones que están activas.

- Si se trata de un nodo de frontera/CP colocado, también hay una sesión LISP establecida hacia sí misma.
- En este caso hay una sesión de 172.30.250.19:4342 a 172.30.250.19:49270.
- A través de esta sesión, el componente de borde registra su EID con el nodo del plano de control.

1.4 Información del plano de control

Con la información proporcionada por los dispositivos de fabric mediante el registro, el nodo del plano de control puede crear una vista completa del fabric. Por Instance-id mantiene una tabla con los EID aprendidos y sus Ubicaciones de Ruteo asociadas.

Muestre esto para las instancias de Capa 3 con el 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
```

Este comando muestra todos los EID registrados y el último que registró el EID. Es importante tener en cuenta que normalmente también se utilizarían los RLOC, pero esto puede diferir. También los EID se pueden registrar con varios RLOC .

Para mostrar todos los detalles, el comando incluye el EID y la instancia

<#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
```

Nota: En el resultado detallado, es importante tener en cuenta algunas cosas:

- Proxy, con este conjunto el nodo del plano de control responde directamente a una solicitud de mapa. En el LISP tradicional se reenvía una solicitud de mapa al XTR que registró el EID, pero con el conjunto de proxy el nodo del plano de control responde directamente
- TTL, éste es el tiempo de vida del registro EID. De forma predeterminada, es de 24 horas
- ETR, esto se relaciona con el dispositivo de fabric que ha enviado el registro EID
- Información de RLOC, éste es el RLOC que se utilizará para alcanzar el EID. Esto también contiene información de estado como en up/down. si el RLOC está inactivo, no se utilizará. También contiene un peso y una prioridad que se pueden utilizar cuando existen múltiples RLOC para que un EID dé preferencia a uno de ellos.

Para ver el historial de registro en el nodo del plano de control, se puede utilizar el comando show lisp server registration history.

- Ofrece una descripción general de los EID que se han registrado y anulado.

Mostrar historial 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
```

Mostrar el EID registrado para Ethernet el comando es show lisp instance-id <instance> servidor Ethernet (Esto da un resultado similar al de la Capa 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
```

Añada la dirección MAC para obtener información más detallada sobre un 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
```

Añada 'historial de registro' para ver el historial de registro para EID Ethernet

---

Nota: Este comando es muy útil cuando los dispositivos se desplazan por el fabric para ver dónde y cuándo se ha registrado la dirección MAC

<#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 la información de resolución de direcciones registrada en el nodo del plano de control, el comando se agrega con la resolución de direcciones.

- Esto sólo muestra las asignaciones entre la dirección MAC y su información de capa 3 y se debe utilizar principalmente para que los bordes del entramado reescriban las direcciones

MAC de destino de capa 2 de difusión/multidifusión a unidifusión.
- El RLOC que corresponde a esa dirección MAC de Capa 2 se resolvería por separado .

Anexe 'address-resolution' para ver la información de la resolución de direcciones registrada en el nodo del plano de control

<#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
```

Nota: Aunque las direcciones IPv6 locales del vínculo no coincidan con el EID dinámico de IPv6, deben aprenderse para la resolución de direcciones y esto se mostrará en el nodo del plano de control. Estos no se registrarían por sí mismos bajo el ID de instancia de capa 3, pero están disponibles para la resolución de direcciones.

Resolver destinos remotos

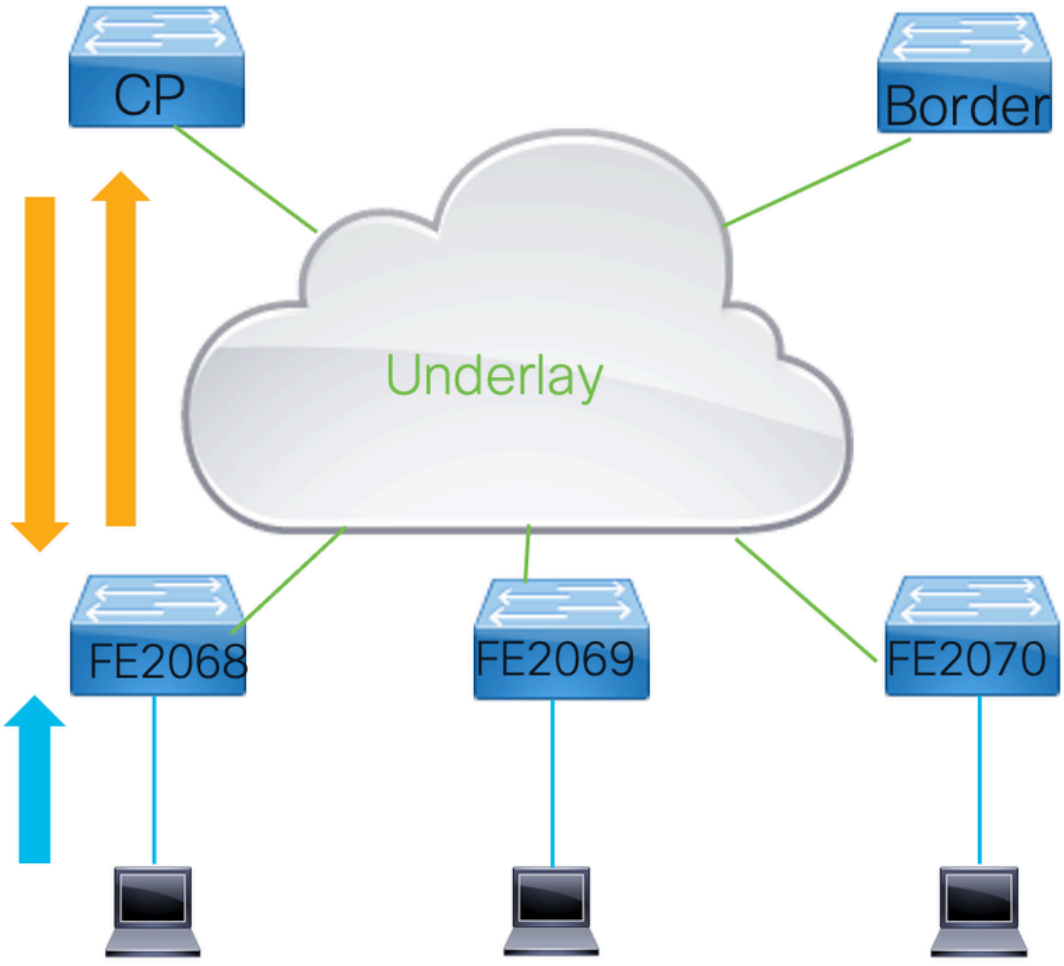
Para que el tráfico se reenvíe a través de un fabric VXLAN LISP, debe resolverse el RLOC de un destino. Dentro de un fabric VXLAN LISP, esto se realiza mediante el uso de una memoria caché de mapas desde la cual se coloca la información en la Base de información de reenvío (FIB) del dispositivo Fabric.

Con los fabrics LISP VXLAN, las memorias caché de mapas deben activarse debido a las señales de datos.

- Esto significa que el tráfico se reenvía a la CPU y la CPU crea una solicitud de mapa hacia el nodo del plano de control para consultar la información de RLOC a la que deberían enviarse las tramas hacia ese EID.
- El plan de control cuando recibe una solicitud de asignación proporcionaría la información de la ubicación de enrutamiento asociada a este EID o devolvería una respuesta de asignación negativa.
- Cuando envía una respuesta de mapa negativa, el nodo del plano de control no solo indicaría que el EID solicitado no es conocido, sino que ofrecería el bloque completo de EID a los que pertenecería este EID y para los que no tendría ningún registro.

Con la información dentro de map-reply del nodo del plano de control, map-cache se actualiza.

- El TTL para respuestas de mapa suele ser de 24 horas. (Para las respuestas negativas al mapa, normalmente son solo 15 minutos).
- Para Ethernet EID, las respuestas de mapa negativas no se colocan en la memoria caché de mapa. (Esto solo se hace para las instancias de la capa 3).



2.1 Caché de mapas Ethernet

Mostrar la memoria caché de mapa Ethernet con el 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        -
```

Este comando muestra la entrada de dirección MAC remota que se habría resuelto.

- Para activar una entrada de caché de mapas para una instancia de tráfico Ethernet debe enviarse a un destino desconocido.
- Esto daría como resultado que el dispositivo de fabric intentara resolverlo a través de LISP.
- Una vez que se aprende a través de una respuesta de mapa, se colocaría en la memoria caché de mapa y las tramas subsiguientes hacia ese destino de capa 2 se enviarían directamente al localizador de ruteo aprendido.

Opcionalmente, en las Instancias de Capa 2 está el uso de la inundación de tráfico BUM .

- LISP/VXLAN no inunda el tráfico de forma predeterminada, ya que utiliza una tecnología de superposición, pero se puede configurar un grupo de multidifusión IP en la red subyacente (GRT) a través del cual se podrían inundar las tramas de capa 2.

Mostrar la dirección del grupo subyacente de difusión

<#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 Caché de mapa IP

Para las instancias de la Capa 3, la información de la memoria caché de mapas es similar a la construcción de Ethernet por el tráfico enviado a la CPU para señalizar que hace que se envíe una solicitud de mapa.

- Sin embargo, para los paquetes de Capa 3 sólo se los envía a la CPU para indicar cuándo se debe configurar. Esto se realiza mediante el comando map-cache que se configura. Para IPv4 es 0.0.0.0/0 y ::0/0 para IPv6.
- La configuración de esta entrada en la memoria caché de mapas en los nodos de borde debe realizarse con cuidado. Si un nodo de borde se configura con esta entrada map-cache 0.0.0.0/0 o ::0/0 map-cache, intenta resolver destinos desconocidos a través del entramado en lugar de rutearlo fuera del entramado.

Mostrar la configuración de map-cache

<#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
```

La map-cache 0.0.0.0/0 y ::/0 map-request hacen que se configure una entrada de map-cache en la map-cache con las acciones "send-map-request". El tráfico que llega a esto activa las solicitudes de mapa. Dado que las entradas de la memoria caché de mapas deben colocarse en la FIB que funciona según la coincidencia más larga, esto se aplica a todo el tráfico IP ruteado que no llegue a ninguna de las entradas más específicas.

- En las plataformas soportadas para evitar que se descarte el primer paquete, la acción mostrada es send-map-request + encapsulate to proxy ETR.
  Esto hace que el primer paquete a un destino desconocido active una solicitud de mapa, así como que el paquete se reenvíe al servidor proxy si está presente.

<#root>

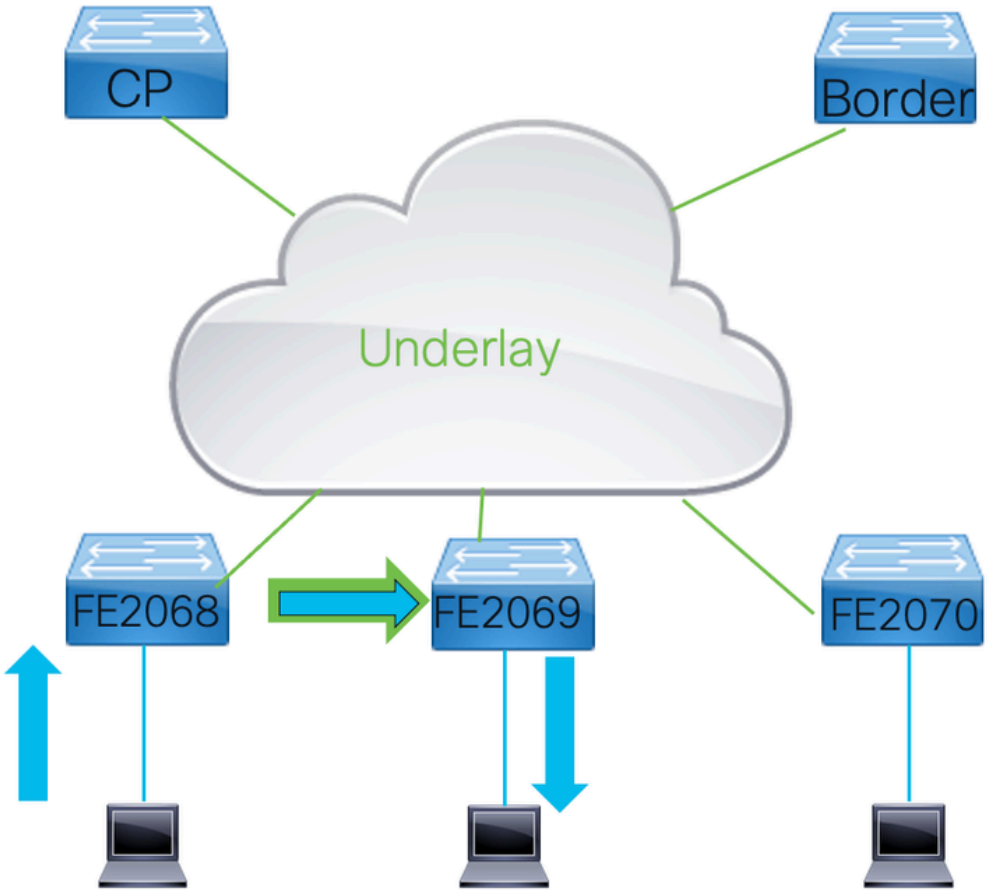
```
FE2067#
show lisp instance-id 4099 ipv4 map-cache

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
```

En esta salida se muestran algunas entradas.

- 10.48.13.0/24 y 172.24.2.2/32 en este resultado se aprende a través de map-reply y se completan. El tráfico a esos destinos debe encapsularse y reenviarse a los respectivos localizadores.
- El 172.28.0.0/14 es un ejemplo de una respuesta de mapa negativa que se ha recibido y un bloque de direcciones IP que se ha devuelto. El tráfico hacia esta subred no activa una solicitud de mapa mientras esta entrada esté en la memoria caché de mapa.

Reenvío de tráfico a través del fabric



3.1 Reenvío de capa 2 o capa 3

El tráfico de un fabric LISP/VXLAN se puede reenviar a través de instancias de capa 2 o capa 2.

- La determinación de qué instancia se utiliza depende de la dirección MAC de destino de las tramas.
- Las tramas que se envían a cualquier dirección MAC que no sea la que está registrada con el switch, la trama que se reenviará es para utilizar la Capa 2. Si el destino del paquete es el switch, se reenvía a través de la Capa 3.
- Esta es la misma lógica que se aplicaría al reenvío normal a través de un Catalyst 9000 Series Switch.

3.2 Reenvío de capa 2

El reenvío de la capa 2 a través de un fabric VXLAN LISP se realiza en función de la dirección MAC de destino de la capa 2. Los destinos remotos se insertan en la tabla de direcciones MAC con la interfaz de salida L2LI0.

Mostrar las interfaces de capa 2 local y remota

<#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 desconocidos, si se configura, el tráfico se envía a través del grupo de multidifusión IP configurado en la capa subyacente.

- Para garantizar un flujo correcto de tráfico de difusión, unidifusión desconocida y multidifusión (solo saturación de multidifusión selectiva), se necesita un entorno de multidifusión correctamente operativo en la capa subyacente.
- El tráfico que se enviaría a través de este grupo subyacente de multidifusión se encapsulará en VXLAN.
- El resto de los bordes deben unirse al grupo multicast y recibir tráfico y desencapsular el tráfico para las Instancias de Capa 2 conocidas.

Mostrar el grupo de multidifusión IP subyacente

<#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:
```

Este resultado muestra una entrada S,G para todos los demás bordes del fabric en los que se configuran clientes que enviarían tráfico inundado. También muestra una entrada S,G con el Loopback0 de este dispositivo Edge como origen.

Para el lado del receptor del tráfico a través del grupo multicast subyacente, el comando show ip mroute también muestra el L2LISP0.<instance>
esto indicaría para qué instancias de la capa 2 este dispositivo de borde se desencapsularía del tráfico inundado y lo reenviaría a su
interfaces relevantes.

3.3 Información de reenvío de capa 3

Para determinar cómo se reenvía el tráfico cuando se implementa un fabric VXLAN LISP, es importante verificar CEF.

- A diferencia de los protocolos de ruteo tradicionales, LISP inserta la dirección de ruteo no en la tabla de ruteo, pero interactúa directamente con CEF para actualizar la FIB.

Para un destino remoto determinado, la información de la memoria caché de mapas contiene la información del localizador que se va a utilizar.

Mostrar la información del 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)

Desde la memoria caché de mapas, el Localizador que se utilizará para este EID es 172.30.250.44. Por lo tanto, el tráfico hacia este destino se encapsulará y el encabezado IP externo tendrá una dirección IP de destino de 172.30.250.44.

En la tabla de ruteo para el VRF utilizado para esta instancia, esta entrada no se muestra.

<#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
```

Las salidas CEF proporcionan más información sobre el reenvío a través del fabric VXLAN de LISP.

- Cuando se agrega la palabra clave detail al comando show ip cef, no sólo proporciona el destino para que se envíe la trama encapsulada.
- La interfaz de salida con este resultado es LISP 0.<instance> indica que el tráfico se envía 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

Dado que el tráfico se enviaría encapsulado hacia el siguiente salto, el siguiente paso es ejecutar un comando show ip cef <next hop> para ver la interfaz de egreso donde el paquete también sería enrutado.

Ejecutar para ver la interfaz de salida

<#root>

FE2067#

sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23

Nota: Existen 2 niveles diferentes de routing de múltiples rutas de igual coste (ECMP).

- El tráfico podría equilibrarse en la carga en la superposición en caso de que haya 2 RLOC anunciados y se puede equilibrar en la carga en la red subyacente si existen rutas redundantes para alcanzar una dirección IP de RLOC.
- Como el puerto de destino UDP está fijado en 4789 y las direcciones IP de origen y destino para todos los flujos entre dos dispositivos de fabric son los mismos, debe producirse algún tipo de mecanismo antipolarización para evitar todos los paquetes enrutados en la misma ruta.
- Con LISP VXLAN, este es el puerto de origen UDP en el encabezado externo que sería diferente para los diferentes flujos en la red de desbordamiento.

3.4 Formato de paquete

- En los fabrics LISP VXLAN, todo el tráfico se encapsula por completo en VXLAN. Esto incluye la trama completa de la Capa 2 para ser capaz de soportar superposiciones tanto de la Capa 2 como de la Capa 3.
  Para las tramas de Capa 2, el encabezado original se encapsula. Para las tramas que se envían a través de una instancia de Capa 3, se utiliza un encabezado de Capa 2 ficticio.

<#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 se observa en la captura de ejemplo de una trama transportada a través de un entramado VXLAN LISP, existe la trama totalmente encapsulada dentro del paquete vxlan. Como trama de capa 3, el encabezado Ethernet es un encabezado ficticio.

En el encabezado VXLAN, el campo Identificador de Red VLAN lleva el identificador de instancia LISP al que pertenece la trama.

- A través del campo Group Policy ID se transporta la etiqueta SGT de tramas.
- Se establece en la entrada en el fabric y se traslada al fabric hasta que se debe realizar la aplicación de políticas basadas en grupos.

Autenticación y aplicación de seguridad

4.1 Autenticación del puerto del switch

Para asignar puntos finales dinámicamente a sus respectivas VLAN y asignarles una autenticación de etiqueta SGT se puede utilizar.

- Los protocolos de autenticación como Dot1x/MAB/webauth central se pueden implementar para autenticar y autorizar usuarios y terminales en un servidor Radius que envía atributos de vuelta al switch para permitir el acceso de red al cliente/terminal en el conjunto correcto y con la autorización de acceso a la red correcta.

Para el fabric VXLAN de LISP hay pocos atributos de radio comunes:

- Asignación De Vlan: Estos atributos se definen como ID de VLAN o nombre desde el servidor RADIUS a los switches; un extremo se puede asignar a una instancia LISP de capa 2/capa 3 específica.
- Valor de SGT: Este atributo establece que una SGT asigna un punto final a esta SGT. Esto se utilizaría para las políticas basadas en grupos hacia este terminal, así como para asignar un valor SGT a todas las tramas enviadas a través del fabric originadas por este terminal.
- Autorización de voz: Los dispositivos de voz funcionan en la VLAN de voz. Esto configura la autorización de voz para que el terminal pueda enviar y recibir tráfico en la vlan de voz configurada en un puerto. Esto permite separar el tráfico de voz y de datos en sus respectivas VLAN
- Tiempo de espera de sesión: Varios terminales tienen sus propios tiempos de espera para las sesiones. Se puede enviar un tiempo de espera desde el servidor RADIUS para indicar

la frecuencia con que un cliente necesita volver a autenticarse
- Plantilla: Para algunos terminales, se debe aplicar una plantilla diferente en un puerto para que funcione correctamente. Se podría enviar un nombre de plantilla desde el servidor Radius que indicaría lo que se debe aplicar al puerto

Verifique el resultado de la autenticación en un puerto mediante el 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

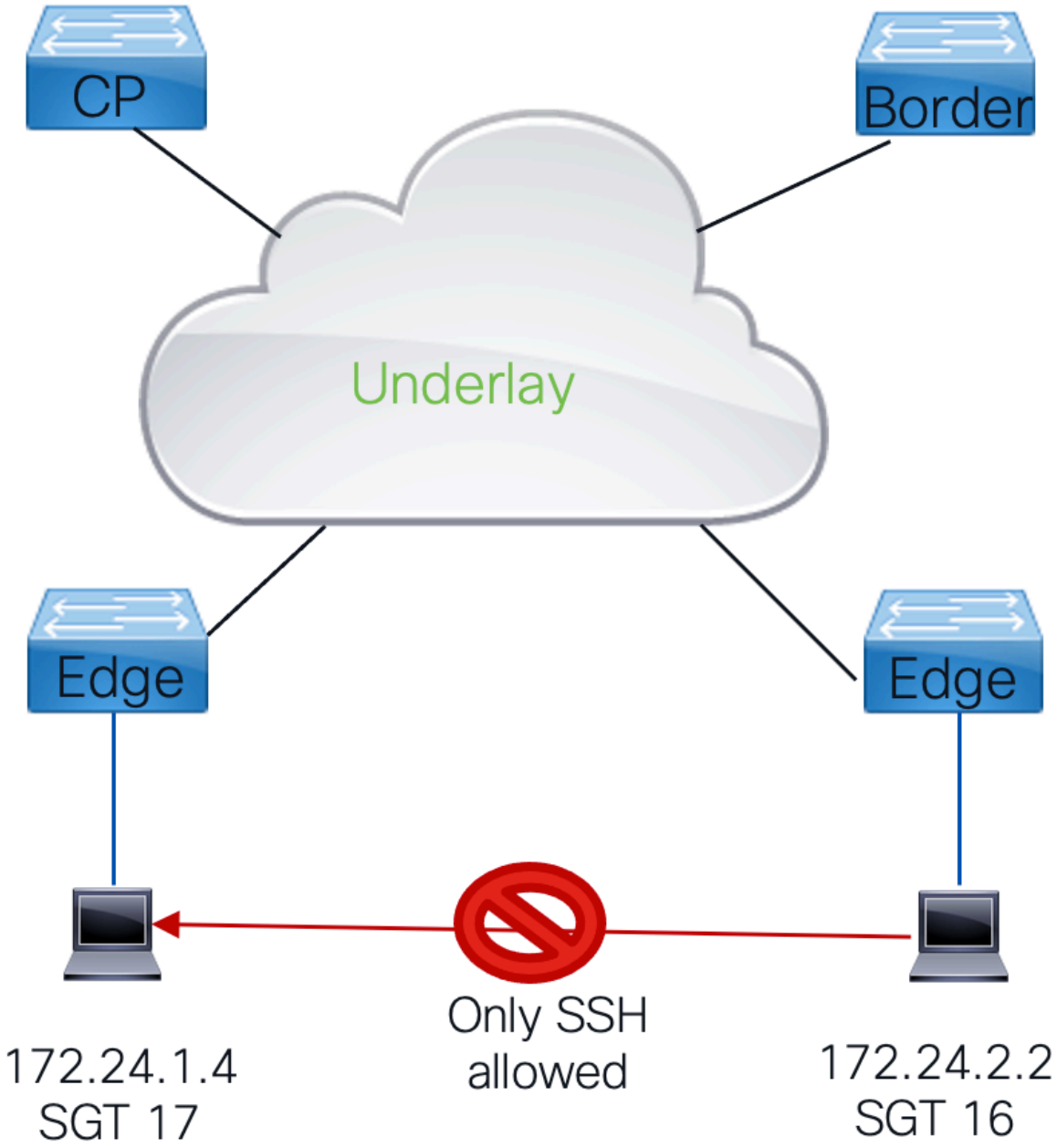
mab Authc

Success

Tenga en cuenta estos campos clave:

- Direcciones IPv4 e IPv6: Normalmente se aprende a través del seguimiento de dispositivos.
- Nombre de usuario: Este es el nombre de usuario utilizado para la autenticación.
    - Para Dot1x, normalmente sería el usuario que se autentica.
    - Cuando se utiliza MAB, esta es la dirección MAC de la estación que se envía a Radius como nombre de usuario y contraseña para la autenticación.
- Estado: Esto indica el estado de la Autenticación y el resultado de la Autenticación.
- Dominio: Para los terminales normales, este sería el dominio de datos, por lo que el tráfico se enviaría/recibiría sin etiquetar en el puerto. (En el caso de los dispositivos de voz, esta opción se puede establecer en Voz)
- Directivas de servidor: Aquí es donde la información del servidor Radius, como la asignación Vlan y la asignación SGT
- Lista de estados de método: Esto muestra una descripción general de los métodos ejecutados.
    - El dot1x estándar se ejecuta antes del MAB.
    - Si un punto final no respondiera a las tramas EAPOL, el método conmutaría por error a mab.
    - Esto luego mostraría que dot1x ha fallado.
    - El MAB muestra que el éxito auténtico indica que se logró autenticar, no refleja si el resultado de la autenticación sería un acceso-aceptación o rechazo.

4.2 Políticas de tráfico y políticas basadas en grupos (CTS)



Dentro de un fabric VXLAN LISP, CTS se utiliza para aplicar políticas de tráfico:

- La arquitectura de la política basada en grupos se basa en etiquetas de grupo seguras.
- Todo el tráfico dentro del fabric se asigna en la etiqueta de entrada y SGT, que se transporta a través del fabric en cada trama.
- Cuando este tráfico abandona el fabric, se aplican las políticas de tráfico.
- Esto se hace en las políticas basadas en grupo que verifican las etiquetas de grupo de origen y destino del paquete contra la matriz que consiste en SGT de origen-destino donde el resultado es una SGACL que define qué tráfico se permitiría o no.
- Cuando no hay una coincidencia específica dentro de la matriz para la SGT de origen-destino, se debe aplicar la acción predeterminada que se ha definido.

4.3 Entorno CTS

Para funcionar con políticas basadas en grupos, lo primero que se necesita para un dispositivo Fabric es obtener un paquete CTS.

- Este paquete se debe utilizar dentro de las tramas de RADIUS para autorizar las tramas RADIUS en Cisco ISE. Esto se utiliza para establecer el campo cts-pac-opaque dentro de las tramas Radius.

Mostrar la información del paquete 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

Es importante asegurarse de que el paquete CTS esté configurado y sea válido. El dispositivo Fabric lo actualiza automáticamente.

Nota: Para activar manualmente una actualización, se puede ejecutar el comando "cts refresh pac".

En el caso de las políticas basadas en grupos para su funcionamiento, se descargan datos de entorno, así como la información de política necesaria.

- Estos datos de entorno contienen tanto la etiqueta CTS que utiliza el propio switch como la tabla de todos los grupos de políticas basadas en grupos que se conocen en el servidor Radius.

Mostrar datos del entorno 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
```

Cuando se utilizan políticas basadas en grupos, las únicas políticas que se descargan son las etiquetas CTS con las que el dispositivo tiene terminales locales que debe aplicar.

- Para poder verificar la asignación de una dirección IP (o subred) a un grupo de políticas basadas en grupo, se puede utilizar el comando "show cts role-based sgt-map vrf <vrf> all".

Mostrar toda la información de IP a SGT conocida para un 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
```

Este resultado muestra todas las direcciones IP (y subredes) conocidas para un VRF determinado y sus asociaciones de políticas basadas en grupos.

- Como se puede ver, hay una dirección IP de un terminal al que se le asigna el grupo de políticas basadas en el grupo 17 y que tiene origen local.
- Éste es el resultado de la autenticación que ocurre en el puerto y donde los resultados indican que la etiqueta está asociada con ese punto final.
- También resalta las direcciones IP propias de los switches a las que se les asigna la etiqueta device-sgt como origen interno.
- Las etiquetas de políticas basadas en grupos también se podrían asignar mediante la configuración o una sesión SXP hacia ISE.

Cuando un dispositivo detecta una etiqueta SGT, intenta descargar las políticas asociadas a ella desde el servidor ISE.

- El comando show cts authorization entries brinda una descripción general de cuándo se intentaron descargar y si se descargaron o no sucesivamente.

Nota: Las políticas deben actualizarse periódicamente en caso de que se produzcan cambios en ellas. ISE también puede aplicar un comando CoA para que el switch se active para descargar nuevas políticas cuando se realicen cambios. Para actualizar manualmente las directivas, se ejecuta el comando "cts refresh policy".

Mostrar una descripción general de las políticas que se han intentado descargar y si se han descargado o no de forma sucesiva

<#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
```

Si hay alguna política descargada, se puede mostrar con el comando "show cts role based 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
```

Este comando muestra todas las políticas que el dispositivo ha aprendido. En el servidor ISE hay potencialmente más políticas presentes para diferentes grupos, pero el dispositivo solo intenta descargar las políticas para las que conoce los terminales. Esto permite conservar valiosos recursos de hardware.

Este comando también muestra la acción predeterminada que debe aplicarse al tráfico para la que no se conoce ninguna entrada específica. En este caso, su IP permitida, por lo que se permitirá el paso de todo el tráfico que no coincida con una entrada específica de la tabla.

Ejecute show cts rbacl <name>para obtener más detalles sobre el contenido exacto de la RBACL que se ha descargado

<#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

En este caso, el único tráfico permitido para ser enviado al terminal con esta RBACL aplicada a él son los paquetes tcp hacia 22 (SSH) y 23 (Telnet).

Nota: RBACL sólo funciona en una dirección. A menos que haya una política en el tráfico de retorno, se aplica con la política predeterminada. El tráfico que entra en el fabric no se

---

aplica, sino que se envía a través del fabric con la etiqueta SGT conocida en el nodo de entrada. Sólo se aplica cuando sale del fabric y se debe aplicar en las políticas que están presentes en ese dispositivo. Normalmente, esas políticas serían las mismas, pero es posible ampliar el dominio CTS, por ejemplo, con un firewall en el que se podrían haber definido otras políticas depende de las políticas de seguridad implementadas.

Ejecute 'show cts role-based counters' para validar si las tramas se descartan o no

- Este comando muestra los contadores acumulativos para todo el switch. No existe un comando equivalente para cada interfaz.

<#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 descripción general muestra todas las entradas conocidas que el switch conoce en este caso para poder hacer coincidir el tráfico de 17 a 16 y de 16 a 17.

- Cualquier otra coincidencia que caiga bajo el * * y obtenga la acción predeterminada aplicada de modo que si cualquier tráfico por ejemplo de 18 a 16 fuera a venir no coincide con la matriz conocida en el switch y tiene la acción predeterminada aplicada.

Aunque los contadores son acumulativos, dan una buena indicación si se descarta el tráfico.

- Para determinar qué tráfico afectaría a una entrada, se podría agregar la palabra clave log en el servidor ISE a las políticas respectivas, lo que hace que el switch proporcione mensajes de registro cuando se accede a esta entrada.
- Esto se puede hacer tanto para la acción predeterminada (* *) como para una de las entradas más específicas de la matriz.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems

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

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

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