Dépannage du fabric LISP VXLAN sur les commutateurs de la gamme Catalyst 9000

Table des matières

Introduction

Ce document décrit les composants de base d'un fabric basé sur LISP VXLAN et comment vérifier son fonctionnement.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Cisco IOS XE 17.9.3 ou version ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Fabric basé sur LISP VXLAN

L'objectif du déploiement d'un réseau LISP VXLAN est de pouvoir créer une architecture dans laquelle plusieurs réseaux superposés, également appelés réseaux virtuels, sont définis au-dessus d'un réseau sous-jacent.

- Dans une telle topologie, le réseau sous-jacent agit principalement comme une couche transport et ignore les topologies de superposition qui sont exécutées sur celle-ci.
- Les réseaux superposés peuvent être ajoutés et supprimés sans impact sur le réseau sous-jacent.
- L'utilisation de réseaux superposés sépare efficacement les utilisateurs du réseau sous-jacent.

Technologies utilisées pour créer un fabric LISP VXLAN

Protocole LISP (Locator Identity Separation Protocol)

- Le protocole LISP est le protocole du plan de contrôle utilisé dans le fabric. Il s'exécute sur tous les périphériques du fabric pour créer le fabric et contrôler la manière dont le trafic est envoyé à travers le fabric.
- LISP crée 2 espaces d'adressage. L'un concerne les RLOC (Routing Locator) qui sont utilisés pour annoncer l'accessibilité. L’autre espace d’adressage est réservé aux identificateurs de point de terminaison (EID) , c’est-à-dire à l’emplacement où résident les points de terminaison et qui est utilisé pour la superposition.

- Dans LISP, les EID sont annoncés avec un RLOC annoncé. Si un EID se déplace, il suffit de mettre à jour le localisateur de routage qui lui est associé.
- Pour atteindre un point d'extrémité avec le trafic LISP vers un EID, il faut l'encapsuler et le tunneler vers le RLOC qui le désencapsule et le transfère au point d'extrémité.

Stratégies basées sur des groupes

- Pour permettre la segmentation à l'intérieur d'un groupe de fabric, des stratégies basées sur des groupes sont utilisées.
- Lorsque des stratégies basées sur des groupes sont déployées, le trafic est classé avec le groupe sécurisé plutôt qu'en fonction de l'adresse IP source/de destination.
- Cela réduit la complexité des listes de contrôle d'accès complexes. Au lieu de listes d’adresses IP devant être mises à jour, les adresses IP/sous-réseaux sont attribués à une balise de groupe sécurisée.
- En entrée dans le fabric est étiqueté avec un SGT lorsque le trafic quitte le fabric, la destination de la trame est recherchée pour son SGT .
- Avec l'utilisation d'une matrice, les balises SGT source et de destination sont mises en correspondance et une liste de contrôle d'accès de groupe sécurisé est appliquée pour appliquer le trafic lorsqu'il quitte le fabric.

Encapsulation VXLAN

- À l’intérieur du fabric, le VXLAN est utilisé pour encapsuler tout le trafic
- L’avantage d’utiliser VXLAN par rapport à l’encapsulation LISP héritée est qu’il permet d’encapsuler la trame de couche 2 entière, et pas seulement la trame de couche 3. À mesure que la trame entière est encapsulée, les superpositions peuvent être à la fois des couches 2 et 3.
- VXLAN utilise UDP avec le port de destination 4789. Cela permet aux trames LISP VXLAN d’être également transportées à travers un périphérique qui ne connaîtrait pas la topologie de superposition.
- Comme VXLAN encapsule la trame entière, il est important d’augmenter la MTU afin qu’aucune fragmentation ne soit nécessaire lorsque le trafic est envoyé entre des RLOC. Tous les périphériques intermédiaires doivent prendre en charge un MTU plus important pour transporter les trames encapsulées.

Authentification

- Pour pouvoir attribuer des terminaux à leurs ressources respectives, l'authentification peut être utilisée.
- Avec des protocoles 802.1x, les points d'extrémité MAB et Webauth peuvent être authentifiés et/ou profilés par rapport à un serveur Radius et se voir accorder l'accès au réseau en fonction de leurs profils d'autorisation.
- Avec leurs attributs Radius respectifs, les terminaux peuvent être affectés à leur VLAN respectif, SGT et tout autre attribut pour fournir un accès réseau terminal/utilisateur.

Composants clés du fabric LISP VXLAN

noeud Plan de contrôle

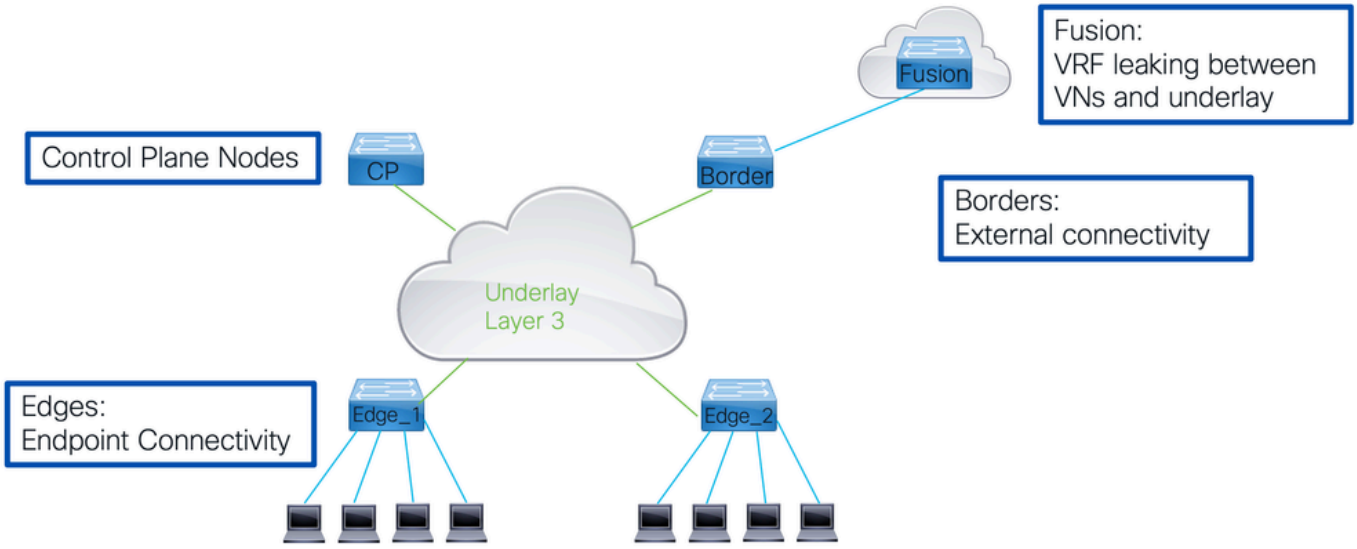
- contient les fonctionnalités LISP Map Server et Map Resolver.
- Tous les autres équipements de fabric demandent au noeud Plan de contrôle l'emplacement de l'EID et envoient les enregistrements de leur EID aux noeuds du Plan de contrôle.
- Les noeuds du plan de contrôle disposent ainsi d'une vue complète du fabric en ce qui concerne le RLOC des différents EID.

Noeuds en limite

- Fournit une connectivité à l'extérieur du fabric, soit vers d'autres fabrics, soit vers le monde extérieur.
- Les bordures internes importent des routes dans le fabric et les enregistrent auprès des noeuds du plan de contrôle.
- Les bordures externes se connectent au monde extérieur et fournissent un chemin par défaut en dehors du fabric pour les destinations IP inconnues.

Noeuds de périphérie

- Ces noeuds assurent la connectivité aux points d'extrémité à l'intérieur du fabric.
- Dans la définition de LISP, il s'agirait de XTR, car ils remplissent à la fois les fonctions de routeur de tunnel d'entrée (ITR) et de routeur de tunnel de sortie (ETR).



Les noeuds ne sont pas limités à une seule tâche.

- Ils peuvent effectuer une combinaison ou même toutes les fonctions à l'intérieur du tissu.
- Lorsqu'un noeud Périphérie et un noeud Plan de contrôle résident sur un périphérique, ils sont appelés colocalisés.
- Si ce noeud fournit également la fonctionnalité de périphérie, il doit être désigné sous le nom de structure dans un boîtier (FIAB).

Les bordures fournissent des transferts au reste du réseau qui utilisent VRF Lite.

- Chaque superposition ou réseau virtuel est associé à une instance VRF sur le noeud périphérique.
- Pour connecter ces différents VRF entre eux, un routeur Fusion est utilisé. Ce routeur de fusion ne fait pas partie du fabric lui-même, mais il est essentiel à son fonctionnement pour pouvoir connecter les réseaux de superposition au fabric.

Un autre concept important au sein d'un fabric VXLAN LISP est celui de l'utilisation d'un Anycast IP.

- Cela signifie que sur tous les périphériques Edge, l'adresse IP et ses adresses MAC pour les interfaces virtuelles commutées (SVI) sont répliquées.
- Chaque périphérie a la même configuration sur l'interface SVI en ce qui concerne les adresses IPv4, IPv6 et MAC.
- Pour résoudre ce problème, il faut relever certains défis.
    - Pour tester l'accessibilité avec la commande ping, utilisez des périphériques connectés localement.
    - Pour atteindre des destinations distantes via le fabric VXLAN LISP, ne renvoie pas de réponse, car le périphérique qui envoie une réponse l’envoie également à l’adresse IP anycast qui est envoyée au périphérique local du fabric qui ne sait pas quel autre noeud du fabric a envoyé la requête ping d’origine.

Enregistrement des terminaux

Pour qu'un fabric VXLAN LISP fonctionne, il est essentiel que le noeud Plan de contrôle sache comment tous les terminaux sont accessibles via le fabric.

- Pour que le plan de contrôle connaisse tous les EID du réseau, il faut que tous les autres périphériques du fabric enregistrent tous les EID qu'il connaît avec le plan de contrôle.
- Un noeud de matrice envoie des messages LISP map-register au noeud du plan de contrôle. Parmi les informations qui sont annoncées avec le message map-register.

Informations importantes

Identificateur d'instance LISP :

- Cet identificateur est transmis à travers le fabric et indique le réseau virtuel à utiliser.
- Dans un fabric VXLAN LISP par superposition de couche 3, une instance est utilisée par VLAN utilisé dans le fabric et il existe également une instance de couche 2.

Terminaux identifiés (EID) :

- S'il s'agit d'une instance de couche 2 ou de couche 3, il s'agit de l'adresse MAC, de la route d'hôte IP (/32 ou /128) ou d'un sous-réseau IP enregistré

Emplacement de routage (RLOC) :

- Il s'agit de l'adresse IP propre au noeud de fabric avec laquelle il annonce l'accessibilité lorsque d'autres périphériques de fabric envoient du trafic encapsulé qui devrait atteindre l'EID.

Indicateur de proxy :

- Lorsque cet indicateur est défini, il permet au noeud Plan de contrôle de répondre directement aux requêtes de mappage provenant d'autres noeuds de fabric , sans que l'indicateur proxy ne définisse toutes les requêtes à transmettre au noeud de fabric qui a enregistré l'EID.

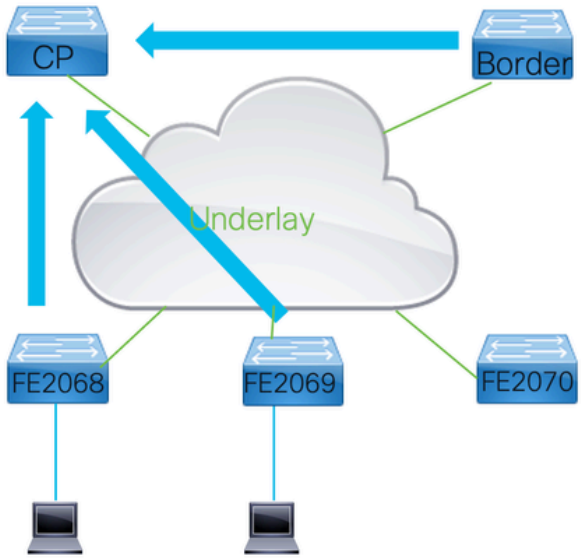
Étapes d'inscription

Étape 1: Les périphériques de fabric découvrent les identificateurs de point final. Cela peut se faire par le biais de la configuration, des protocoles de routage ou lors de l'apprentissage sur les périphériques de fabric.

Étape 2 : les périphériques du fabric enregistrent les terminaux appris auprès de chaque noeud du plan de contrôle connu et accessible à l'intérieur du fabric.

Étape 3: Les noeuds du plan de contrôle gèrent une table des EID enregistrés avec l'ID d'instance associé, le RLOC et l'EID appris

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



Vérifier

1.1 Apprentissage des adresses MAC

Pour les instances de couche 2, l'EID utilisé correspond aux adresses MAC apprises à l'intérieur du VLAN associé. Les arêtes de fabric apprennent les adresses de couche 2 par le biais de méthodes standard sur les commutateurs.

Localisez le VLAN associé à une instance de couche 2 spécifique ID de la configuration peut être

examinée ou la commande

Utilisez "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
```

Comme le montre le résultat, l'ID d'instance 8191 est associé au VLAN 150. Cela a pour conséquence que toutes les adresses MAC à l'intérieur du VLAN sont enregistrées avec LISP et deviennent partie intégrante du fabric VXLAN 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
```

Les entrées statiques avec l'interface Vl150 sont les adresses MAC de l'interface virtuelle du commutateur (interface vlan 150).

- Ces adresses MAC ne sont pas enregistrées avec le noeud du plan de contrôle, car elles seraient identiques sur tous les périphériques de périphérie.
- Les entrées CP_LEARN affichées sont des entrées apprises par le biais du fabric. Pour toutes les autres entrées, si elles sont dynamiques ou statiques, elles doivent être enregistrées avec le noeud du plan de contrôle.

Une fois qu'ils sont appris par leurs moyens respectifs, ils apparaissent dans les sorties de la base de données lisp, cette sortie contient toutes les entrées locales sur ce périphérique 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
```

Pour toutes les adresses MAC locales connues qui sont affichées dans la base de données, le localisateur est affiché.

- Il s'agit du localisateur qui doit être utilisé pour enregistrer cette entrée avec le noeud du plan de contrôle.
- Il indique également l'état du localisateur.Les 2 adresses MAC qui appartenaient à l'interface SVI des commutateurs sont également affichées, mais avec l'indicateur « ne pas enregistrer » qui empêche leur enregistrement.
- L'entrée distante qui a été vue dans la commande show mac address table n'est pas une adresse MAC locale et n'apparaît donc pas dans la base de données lisp.

Pour une instance de couche 2, les adresses MAC de couche 2 ne sont pas seulement apprises en tant qu'EID, il est également nécessaire d'apprendre les informations de résolution d'adresse à partir des trames ARP et ND.

- Cela permet au fabric VXLAN LISP de pouvoir transférer ces trames car elles sont normalement diffusées à l’intérieur du VLAN.
- Comme un ID d'instance de couche 2 n'a pas toujours la capacité d'inonder là un autre mécanisme qui permettrait aux terminaux de résoudre les informations de résolution d'adresse pour d'autres terminaux dans la même instance. Pour cela, les périphériques de fabric apprennent et enregistrent ces informations qui sont apprises localement par Device-Tracking .
- Cette opération est ensuite enregistrée avec les noeuds du plan de contrôle également. En raison de la surveillance ND ou ARP, ces paquets sont dirigés vers le processeur pour déclencher une requête vers les noeuds du plan de contrôle pour voir si une adresse MAC connue est associée.
- En cas de réponse positive, les paquets ARP/ND sont réécrits de sorte que l'adresse MAC de destination passe de la diffusion ou de la multidiffusion à l'adresse MAC de monodiffusion.
- Ce paquet réécrit peut ensuite être transféré via le fabric VXLAN LISP en tant que trame de monodiffusion.

Pour afficher les informations de résolution d’adresse connues sur le commutateur, la commande

show device-tracking database peut être utilisée.

- Ceci n'affiche pas tous les mappages connus par le suivi de périphérique.
- Les adresses IP propres aux commutateurs sont étiquetées L(Local) et doivent être présentes dans la base de données de suivi des périphériques.

Les entrées distantes sont également affichées dans cette sortie.

- Lorsqu'ils sont résolus après avoir été surveillés par la requête ND ou ARP, ils sont placés dans la base de données de suivi des périphériques avec l'adresse de couche liaison 0000.0000.00fd.
- Au moment où elles sont résolues, les informations sont changées vers l'adresse MAC résolue et le port est changé en Tu0.

Afficher la base de données de suivi des périphériques

<#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
```

Affichez les mappages enregistrés localement avec la commande « 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 Apprentissage des adresses IP dynamiques

Sur les périphériques de fabric d'une couche IP, un réseau virtuel est formé en associant un ID d'instance LISP à un VRF.

- Ce VRF est ensuite configuré sous les diverses interfaces virtuelles de commutateur (SVI) et elles deviennent partie intégrante du réseau de couche 3 Overlay
- Dans la plupart des cas, ces interfaces SVI appartiennent également à des VLAN qui sont enregistrés avec leurs instances de couche 2 respectives.

Recherchez le mappage entre VRF et LISP Instance id à l'aide de la commande '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
```

Remarque : Cette commande peut également être utilisée pour vérifier les différentes fonctions qui pourraient être activées pour cette instance, ainsi qu'elle montre les noeuds du plan de contrôle utilisés dans le fabric VXLAN LISP

Une fois qu'une instance de couche 3 est créée et liée à un VRF, une interface LISP 0 **<**id-instance**>** est créée et est visible dans la configuration en cours et sous show vrf.

- Cette interface n'a PAS besoin d'être créée manuellement et n'a généralement pas besoin d'être configurée (à l'exception de la configuration multidiffusion lorsque la multidiffusion sous-jacente est utilisée).

<#root>

```
FE2068#
show vrf Fabric_VN_1

  Name                              Default RD            Protocols   Interfaces

Fabric_VN_1

                                                          ipv4,ipv6
```

LI0.4099

Vl150

Vl151

Contrairement aux trames Ethernet où toutes les adresses MAC d'un VLAN sont utilisées pour l'IP, il est nécessaire que les adresses IP se trouvent dans une plage d'EID dynamique pour être apprises.

Afficher une instance 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

Les adresses IP qui se trouvent en dehors de ces plages définies sont considérées comme inéligibles pour le fabric et ne sont pas placées dans les bases de données LISP et ne sont pas enregistrées auprès des noeuds du plan de contrôle.

<#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
```

Le résultat affiche toutes les informations d'adresse IP connue localement.

- Pour les hôtes, il s’agit généralement de routes d’hôte (/32 ou /128), mais il peut également s’agir de sous-réseaux s’ils ont été importés dans la base de données LISP basée sur le noeud de périphérie.
- Les adresses IP de l'interface SVI elle-même sont marquées comme « ne pas s'enregistrer » . Cela permet d’éviter que tous les périphériques du fabric n’enregistrent l’adresse IP Anycast auprès du noeud du plan de contrôle.

<#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 Enregistrement de l'EID sur le plan de contrôle

L'enregistrement des terminaux dans un fabric basé sur LISP VXLAN est effectué via l'enregistrement fiable LISP. Cela signifie que tous les enregistrements sont effectués via une session TCP établie, la session LISP. À partir de chaque périphérique de fabric, une session LISP est établie avec chacun des noeuds du plan de contrôle dans le fabric.Grâce à cette session LISP, toutes les inscriptions ont lieu. Si plusieurs noeuds du plan de contrôle sont présents dans un fabric, ils doivent tous être utilisés pour enregistrer les EID.

L'état est Down lorsqu'il n'y a rien à enregistrer sur le périphérique de fabric, ce qui n'est généralement le cas qu'aux frontières externes
qui n'enregistrent aucune plage IP avec le noeud Plan de contrôle ou sur les périphériques Edge sans point d'extrémité

L'enregistrement de l'EID se fait via les messages LISP Registration
qui sont envoyées à tous les noeuds du plan de contrôle configurés.

Pour afficher la session LISP sur un périphérique de fabric, vous pouvez utiliser la commande show lisp session.
Il indique l'état de la session et l'heure à laquelle elle a été active.

<#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 session LISP affichée comme étant inactive peut se produire sur les périphériques qui ne disposent d'aucun EID à enregistrer auprès du noeud Plan de contrôle.
En général, il s'agit de noeuds périphériques qui n'importent pas de routes dans le fabric ou les périphériques Edge sans aucun point d'extrémité connecté.

Affichez des informations plus détaillées sur une session LISP à l'aide de la commande « 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
```

Cette sortie détaillée de la session montre quelles instances sont actives avec EID qui sont enregistrées avec les noeuds du plan de contrôle.

<#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
```

Lorsque l’on regarde le nombre de sessions sur un noeud du plan de contrôle, on voit généralement plus de sessions qui sont actives.

- S'il s'agit d'un noeud Border/CP colocalisé, une session LISP est également établie vers lui-même.
- Dans ce cas, il y a une session de 172.30.250.19:4342 à 172.30.250.19:49270.
- Au cours de cette session, le composant Border enregistre son EID auprès du noeud Plan de contrôle.

1.4 Informations sur le plan de contrôle

Grâce aux informations fournies par les périphériques du fabric via l'enregistrement, le noeud du plan de contrôle peut créer une vue complète du fabric. Par ID d'instance, il tient à jour une table avec les EID acquis et les localisateurs de routage associés.

Affichez ceci pour les instances de couche 3 avec la commande 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
```

Cette commande affiche tous les EID enregistrés et le dernier qui les a enregistrés. Il est important de noter qu'il s'agit généralement du RLOC utilisé, mais cela peut être différent. Les EID peuvent également être enregistrés avec plusieurs RLOC .

Pour afficher tous les détails, la commande inclut l'EID et l'instance

<#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
```

Remarque : Dans le résultat détaillé, il est important de prendre en compte les points suivants :

- Proxy : avec ce paramètre, le noeud Plan de contrôle répond directement à une requête Map. Dans le protocole LISP traditionnel, une requête de mappage est transmise au XTR qui a enregistré l'EID, mais avec le proxy défini, le noeud du plan de contrôle répond directement
- TTL, il s'agit de la durée de vie de l'enregistrement EID. Par défaut, il s'agit de 24 heures
- Les informations ETR concernent le périphérique de fabric qui a envoyé

---

l'enregistrement EID

- Informations RLOC, il s'agit du RLOC à utiliser pour atteindre l'EID. Il contient également des informations d'état telles que up/down. si le RLOC est désactivé, il ne doit pas être utilisé. Il contient également une pondération et une priorité qui peuvent être utilisées lorsque plusieurs RLOC existent pour qu'un EID donne la préférence à l'un d'entre eux.

Pour afficher l'historique d'inscription sur le noeud Plan de contrôle, vous pouvez utiliser la commande show lisp server registration history.

- Il donne un aperçu des EID qui ont été enregistrés et désenregistrés.

Afficher l'historique des inscriptions

<#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
```

Affichez l'EID enregistré pour Ethernet et la commande show lisp instance-id <instance> ethernet server (Cela donne un résultat similaire à celui de la couche 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

Ajoutez l'adresse MAC pour obtenir des informations plus détaillées sur un enregistrement

<#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
```

Ajoutez « registration history » pour afficher l'historique d'enregistrement de l'EID Ethernet

---

Remarque : Cette commande est très utile lorsque des périphériques se déplacent dans le fabric pour voir où et quand l'adresse MAC a été enregistrée

---

<#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
```

Pour afficher les informations de résolution d'adresse enregistrées sur le noeud Plan de contrôle, la commande est ajoutée avec address-resolution.

- Cette option affiche uniquement les mappages entre l'adresse MAC et leurs informations de couche 3. Elle doit être utilisée principalement pour les périphéries du fabric afin de réécrire les adresses MAC de destination de couche 2 de la diffusion/multidiffusion à la monodiffusion.
- Le RLOC qui correspond à cette adresse MAC de couche 2 serait résolu séparément .

Ajoutez « address-resolution » pour afficher les informations de résolution d'adresse enregistrées sur le noeud Plan de contrôle

<#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
```

Remarque : Même si les adresses IPv6 locales de liaison ne correspondent pas à l'EID

dynamique IPv6, elles doivent être apprises pour la résolution d'adresse et cela s'afficherait-il sur le noeud Plan de contrôle ? Ils ne seraient pas enregistrés eux-mêmes sous l'ID d'instance de couche 3, mais ils sont disponibles pour la résolution d'adresse.

Résoudre les destinations distantes

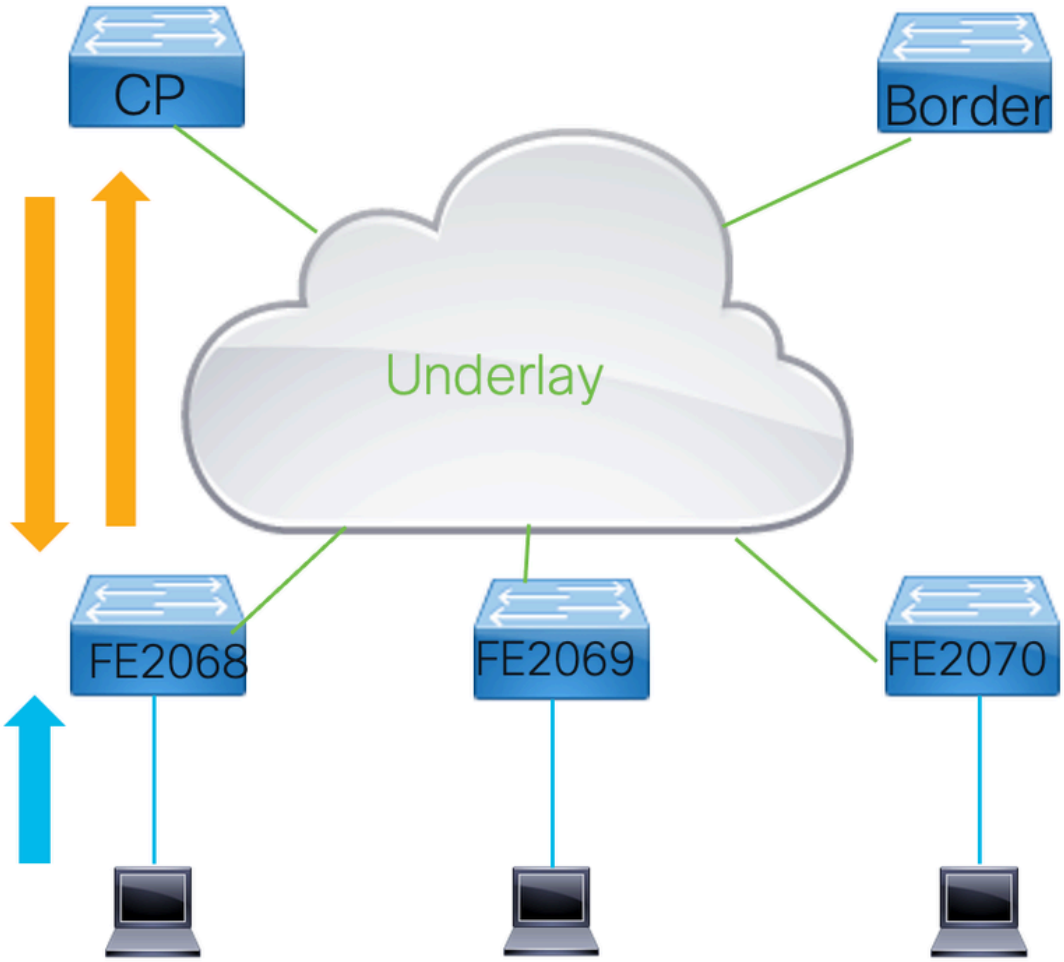
Pour que le trafic soit acheminé via un fabric VXLAN LISP, le RLOC d’une destination doit être résolu. Dans un fabric VXLAN LISP, cette opération est effectuée à l'aide d'un cache de mappage à partir duquel les informations sont placées dans la base d'informations de transfert (FIB) du périphérique de fabric.

Avec les fabrics LISP VXLAN, les caches de mappage doivent être déclenchés en raison des signaux de données.

- Cela signifie que le trafic est transféré au processeur et que le processeur crée une requête de mappage vers le noeud Plan de contrôle pour demander les informations RLOC auxquelles les trames vers cet EID devraient être envoyées.
- Le plan de contrôle, lorsqu'il reçoit une requête de mappage, fournit les informations de l'emplacement de routage associées à cet EID ou renvoie une réponse de mappage négative.
- Quand il envoie une carte-réponse négative, le noeud du plan de contrôle n'indique pas seulement que l'EID demandé n'est pas connu, il offre le bloc entier d'EID auquel cet EID appartiendrait et pour lequel il n'aurait aucun enregistrement.

Avec les informations contenues dans la carte-réponse du noeud du plan de contrôle, la carte-cache est mise à jour.

- La durée de vie des réponses de mappage est généralement de 24 heures. (Pour les réponses de mappage négatives, il ne faut généralement que 15 minutes).
- Pour l'EID Ethernet, les réponses de mappage négatives ne sont pas placées dans le cache de mappage. (Cette opération n'est effectuée que pour les instances de couche 3).



2.1 Cache de mappage Ethernet

Affichez le map-cache Ethernet avec la commande 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        -
```

Cette commande affiche l'entrée d'adresse MAC distante qui aurait été résolue.

- Pour déclencher une entrée de cache de mappage pour une instance Ethernet, le trafic doit être envoyé vers une destination inconnue.
- Le périphérique de fabric peut alors essayer de le résoudre via le protocole LISP.
- Une fois qu'elle est apprise via une carte-réponse, elle est placée dans le cache de carte et les trames suivantes vers cette destination de couche 2 sont envoyées directement au localisateur de routage appris.

En option, dans les instances de couche 2, l'utilisation d'un flux de trafic BUM .

- LISP/VXLAN n'inonde pas le trafic par défaut car il utilise une technologie de superposition, mais un groupe de multidiffusion IP peut être configuré dans le réseau sous-jacent (GRT) par lequel les trames de couche 2 peuvent être inondées.

Afficher l'adresse du groupe sous-jacent de diffusion

<#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 de mappage IP

Pour les instances de couche 3, les informations de cache de mappage sont similaires à ethernet généré par le trafic envoyé au processeur pour signaler qu'une requête de mappage est envoyée.

- Cependant, pour la couche 3, les paquets ne sont envoyés au processeur que pour signaler le moment où ils doivent être configurés. Pour ce faire, utilisez la commande map-cache configurée. Pour IPv4, il s'agit de 0.0.0.0/0 et de ::0/0 pour IPv6.
- La configuration de cette entrée de cache de mappage sur les noeuds périphériques doit être effectuée avec précaution. Si un noeud de périphérie est configuré avec cette entrée

map-cache 0.0.0.0/0 ou ::0/0 map-cache, il tente de résoudre les destinations inconnues via le fabric au lieu de le router en dehors du fabric.

Affichez la configuration 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
```

Les map-cache 0.0.0.0/0 et ::/0 map-request entraînent la configuration d'une entrée map-cache dans le map-cache avec les actions « send-map-request ». Le trafic qui atteint ce point déclenche des requêtes de mappage. Comme les entrées de cache de mappage doivent être placées dans la FIB qui fonctionne en fonction de la correspondance la plus longue, ceci est appliqué à tout le trafic IP routé qui n'atteint aucune des entrées plus spécifiques.

- Sur les plates-formes prises en charge pour éviter le premier paquet à abandonner, l'action affichée est send-map-request + encapsulate to proxy ETR.
  Ceci a pour résultat que le premier paquet vers une destination inconnue déclenche une requête de mappage et que le paquet est transféré à l'entrée proxy si présent.

<#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,

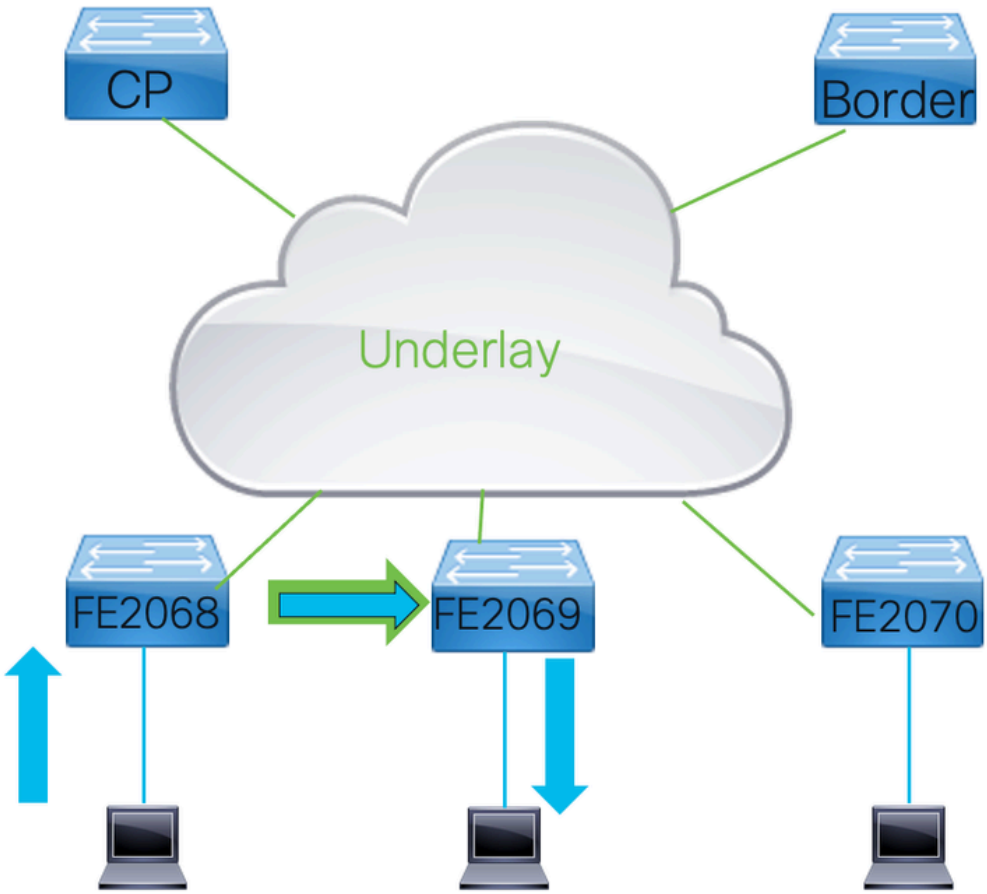
uptime: 22:28:22, expires: 00:13:39, via map-reply, unknown-eid-forward

PETR	Uptime	State	Pri/Wgt	Encap-IID	Metric
172.30.250.19					
	22:28:19	up	10/10	-	0

Dans ce résultat, quelques entrées sont affichées.

- 10.48.13.0/24 et 172.24.2.2/32 dans ce résultat est appris via la carte-réponse et sont terminés. Le trafic vers ces destinations doit être encapsulé et transféré vers les localisateurs respectifs.
- 172.28.0.0/14 est un exemple de réponse de mappage négative reçue et de bloc d'adresses IP renvoyé. Le trafic vers ce sous-réseau ne déclenche pas de requête de mappage tant que cette entrée se trouve dans le cache de mappage.

Transfert du trafic via le fabric



3.1 Transfert de couche 2 ou 3

Le trafic dans un fabric LISP/VXLAN peut être transféré via des instances de couche 2 ou de couche 2.

- La détermination de l'instance utilisée dépend de l'adresse MAC de destination des trames.
- Les trames qui sont envoyées à une adresse MAC autre que celle qui est enregistrée auprès du commutateur. La trame à transférer doit utiliser la couche 2. Si la destination du paquet est le commutateur, elle est transférée via la couche 3.

- Il s'agit de la même logique que celle qui s'appliquerait au transfert normal via un commutateur de la gamme Catalyst 9000.

3.2 Transfert de couche 2

Le transfert de couche 2 via un fabric VXLAN LISP est effectué en fonction de l’adresse MAC de destination de couche 2. Les destinations distantes sont insérées dans la table d’adresses MAC avec l’interface de sortie L2LI0.

Affichage des interfaces de couche 2 locale et distante

<#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
```

Pour les destinations inconnues, s'il est configuré, le trafic est envoyé via le groupe de multidiffusion IP configuré dans le sous-réseau.

- Pour garantir un flux correct de diffusion, un trafic de monodiffusion et de multidiffusion inconnue (diffusion multidiffusion sélective uniquement), un environnement de multidiffusion correctement opérationnel dans le sous-réseau est nécessaire.
- Le trafic qui serait envoyé via ce groupe multicast-underlay doit être encapsulé dans VXLAN.
- Toutes les autres arêtes doivent rejoindre le groupe de multidiffusion et recevoir le trafic et le désencapsuler pour les instances de couche 2 connues.

Affichez le groupe de multidiffusion IP sous-jacent

<#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:
```

Cette sortie montre une entrée S, G pour tous les autres périphériques du fabric où les clients sont configurés pour envoyer le trafic inondé. Il affiche également une entrée S, G avec le Loopback0 de ce périphérique Edge comme source.

Pour le côté récepteur du trafic via le groupe de multidiffusion sous-jacent, la commande show ip mroute affiche également L2LISP0.<instance>
cela indique pour quelles instances de couche 2 ce périphérique de périphérie désencapsule le trafic diffusé et le transfère à son
les interfaces pertinentes.

3.3 Transmission des informations de couche 3

Pour déterminer comment le trafic est transféré lorsqu'un fabric VXLAN LISP est déployé, il est important de vérifier CEF.

- Contrairement aux protocoles de routage traditionnels, LISP insère la direction de routage non pas dans la table de routage, mais interagit directement avec CEF pour mettre à jour la FIB.

Pour une destination distante donnée, les informations de cache de mappage contiennent les informations de localisateur à utiliser.

Afficher les informations de localisation

<#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)
```

À partir du cache de mappage, le localisateur à utiliser pour cet EID est 172.30.250.44. Ainsi, le trafic vers cette destination doit être encapsulé et l'en-tête IP externe a une adresse IP de destination de 172.30.250.44.

Dans la table de routage du VRF utilisé pour cette instance, cette entrée n'est pas affichée.

<#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
```

Les sorties CEF fournissent plus d'informations sur le transfert via le fabric VXLAN LISP.

- Lorsque le mot clé detail est ajouté à la commande show ip cef, il ne fournit pas uniquement la destination de la trame encapsulée à envoyer.
- L’interface de sortie avec ce résultat est LISP 0.<instance> indique que le trafic est envoyé encapsulé.

<#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
```

Comme le trafic serait envoyé encapsulé vers le saut suivant, l'étape suivante consiste à exécuter une commande show ip cef <next hop> pour voir l'interface de sortie où le paquet serait également routé.

Exécutez pour afficher l'interface de sortie

<#root>

```
FE2067#

sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23
```

Remarque : Il existe deux niveaux différents de routage ECMP (equal cost multiple path) possibles.

- Le trafic peut être équilibré en charge dans la superposition s'il y a 2 RLOC annoncés et peut être équilibré en charge dans le réseau sous-jacent s'il existe des chemins redondants pour atteindre une adresse IP RLOC.
- Étant donné que le port de destination UDP est fixé à 4789 et que les adresses IP source et de destination de tous les flux entre deux périphériques de fabric sont identiques, une forme de mécanisme anti-polarisation doit être mise en place pour éviter que tous les paquets soient routés sur le même chemin.
- Avec LISP VXLAN, il s'agit du port source UDP dans l'en-tête externe qui serait différent pour différents flux dans le réseau de débordement.

3.4 Format des paquets

- Dans les fabrics VXLAN LISP, tout le trafic est entièrement encapsulé dans VXLAN. Cela inclut l’intégralité de la trame de couche 2 pour pouvoir prendre en charge les superpositions de couche 2 et de couche 3.
  Pour les trames de couche 2, l’en-tête d’origine est encapsulé. Pour les trames envoyées via une instance de couche 3, un en-tête de couche 2 factice est utilisé.

<#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
```

Comme le montre l’exemple de capture d’une trame transportée par un fabric VXLAN LISP, la trame entièrement encapsulée se trouve à l’intérieur du paquet vxlan. En tant que trame de couche 3, l’en-tête Ethernet est un en-tête factice.

Dans l’en-tête VXLAN, le champ VLAN Network Identifier porte l’ID d’instance LISP auquel la trame appartient.

- Le champ ID de stratégie de groupe transporte la balise SGT des trames.
- Cette action est définie en entrée dans le fabric et est exécutée jusqu'à ce que l'application de la stratégie basée sur le groupe soit effectuée.

Authentification et application de la sécurité

4.1 Authentification des ports de commutation

Pour attribuer dynamiquement des terminaux à leurs VLAN respectifs et leur attribuer une authentification de balise SGT, vous pouvez utiliser.

- Les protocoles d'authentification tels que Dot1x/MAB/central webauth peuvent être déployés pour authentifier et autoriser les utilisateurs et les terminaux sur un serveur Radius qui renvoie les attributs au commutateur pour permettre l'accès réseau au client/terminal dans le pool correct et avec l'autorisation d'accès réseau correcte.

Pour le fabric VXLAN LISP, il existe peu d’attributs de rayon communs :

- Affectation De Vlan : Cet attribut est défini sur l'ID de VLAN ou le nom du serveur RADIUS

vers les commutateurs. Un point d'extrémité peut être attribué à une instance LISP spécifique de couche 2/couche 3.
- Valeur SGT : Cet attribut définit une SGT et attribue un point de terminaison à cette SGT. Il est utilisé pour les politiques basées sur les groupes vers ce point d'extrémité et attribue une valeur SGT à toutes les trames envoyées via le fabric et provenant de ce point d'extrémité.
- Autorisation vocale : Les périphériques vocaux fonctionnent sur le VLAN voix. Ceci définit l'autorisation vocale du point d'extrémité qui serait autorisé à envoyer et recevoir du trafic dans le VLAN voix configuré sur un port. Cela permet de séparer le trafic voix et données dans leurs VLAN respectifs
- Expiration de session : Les différents points d'extrémité ont leurs propres délais d'attente pour les sessions. Un délai d'attente peut être envoyé à partir du serveur RADIUS pour indiquer la fréquence à laquelle un client doit s'authentifier à nouveau
- Modèle : Pour certains terminaux, un modèle différent doit être appliqué sur un port pour fonctionner correctement. Un nom de modèle pourrait être envoyé à partir du serveur Radius qui indiquerait ce qui doit être appliqué au port

Vérifiez le résultat de l'authentification sur un port en utilisant la commande 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

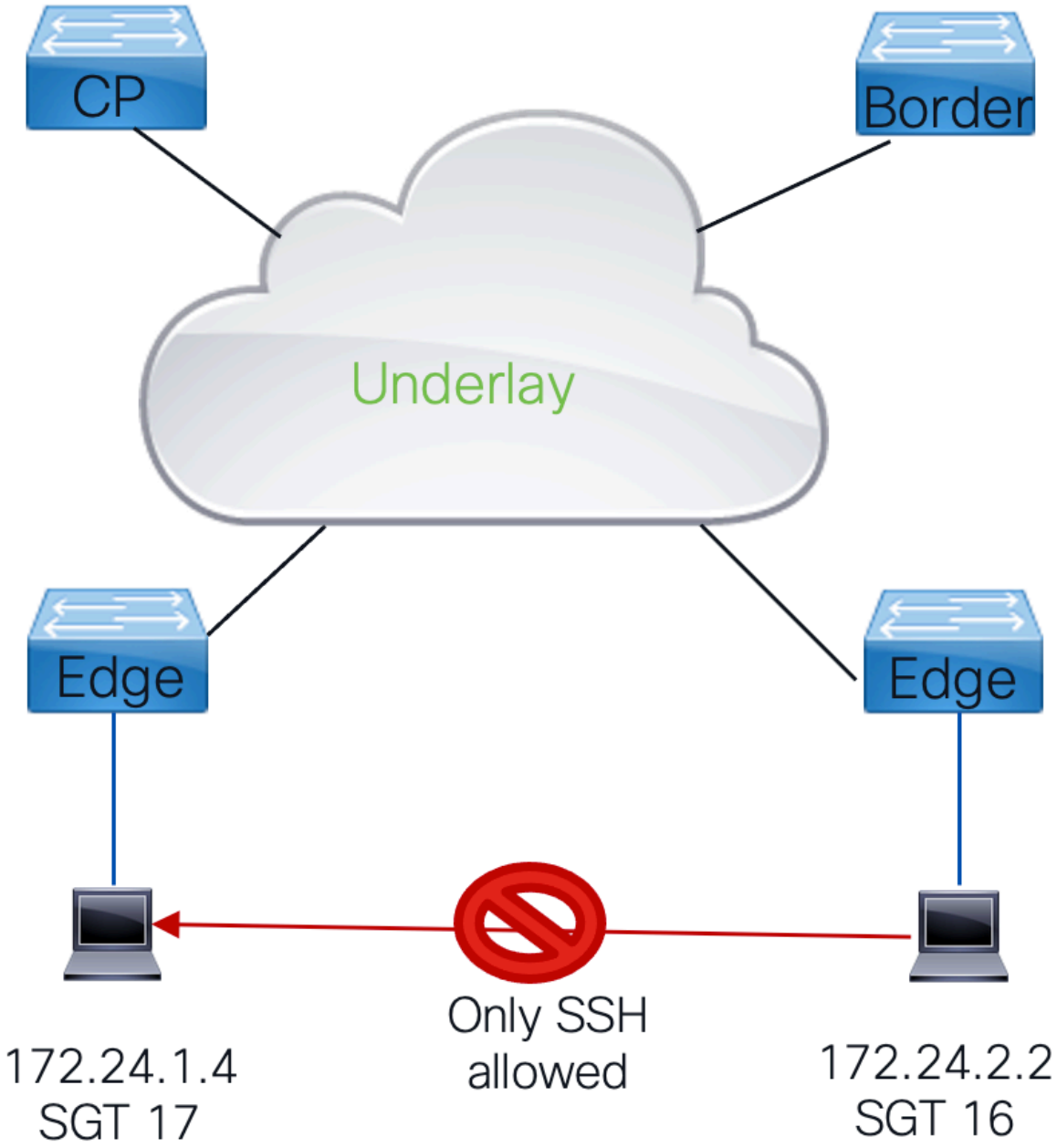
```
mab Authc
```

Success

Notez ces champs clés :

- Adresses IPv4 et IPv6 : Généralement apprise par le suivi des périphériques.
- username (nom d'utilisateur) : Nom d'utilisateur utilisé pour l'authentification.
  - Pour Dot1x, il s'agit généralement de l'utilisateur qui s'authentifie.
  - Lorsque MAB est utilisé, il s'agit de l'adresse MAC de la station qui est envoyée à Radius en tant que nom d'utilisateur et mot de passe pour l'authentification.
- État : Indique l'état de l'authentification et le résultat de l'authentification.
- Domaine : Pour les points d'extrémité normaux, il s'agit du domaine de données, de sorte que le trafic est envoyé/reçu non étiqueté sur le port. (Pour les périphériques vocaux, ce paramètre peut être défini sur Voice)
- Stratégies de serveur : Il s'agit de l'emplacement où les informations du serveur Radius comme l'affectation Vlan et l'affectation SGT
- Liste d'état de méthode : Ceci montre une vue d'ensemble des méthodes exécutées.
  - Le dot1x standard s'exécute avant MAB.
  - Si un terminal ne répond pas aux trames EAPOL, la méthode bascule sur mab.
  - Cela montrerait alors dot1x comme ayant échoué.
  - MAB indique que la réussite de l'authentification indique qu'il a réussi à s'authentifier. Il ne reflète pas si le résultat de l'authentification serait un refus ou un acceptation d'accès.

4.2 Politiques de trafic et politiques basées sur les groupes (CTS)



Dans un fabric VXLAN LISP, CTS est utilisé pour appliquer les politiques de trafic :

- L'architecture de la stratégie de groupe repose sur des balises de groupe sécurisées.
- Tout le trafic à l'intérieur du fabric est affecté à l'entrée et à l'étiquette SGT qui est transportée à travers le fabric dans chaque trame.
- Lorsque ce trafic quitte le fabric, les politiques de trafic sont appliquées.
- Cette opération est effectuée dans les politiques basées sur les groupes qui vérifient les balises de groupe source et de destination du paquet par rapport à la matrice constituée des balises SGT source-destination, où le résultat est une liste SGACL qui définit le trafic autorisé ou non.
- En l'absence de correspondance spécifique dans la matrice pour le SGT Source-Destination, l'action par défaut définie doit être appliquée.

4.3 Environnement CTS

Pour fonctionner avec des politiques basées sur des groupes, la première chose à faire pour les périphériques d'un fabric est d'obtenir un paquet CTS.

- Ce paquet doit être utilisé à l'intérieur des trames RADIUS pour autoriser les trames RADIUS sur Cisco ISE. Ceci est utilisé pour définir le champ cts-pac-opaque à l'intérieur des trames Radius.

Affichez les informations de configuration 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
```

Il est important de s'assurer que le paquet CTS est configuré et valide. Le périphérique Fabric actualise automatiquement cette fonction.

Remarque : Pour déclencher manuellement une actualisation, la commande "cts refresh pac" peut être exécutée.

Pour que les stratégies de groupe fonctionnent, il télécharge les données d'environnement ainsi que les informations de stratégie requises.

- Ces données d'environnement contiennent à la fois la balise CTS utilisée par le commutateur lui-même et téléchargent la table de tous les groupes de stratégies basés sur des groupes connus sur le serveur Radius.

Afficher les données d'environnement 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
```

Lorsque des stratégies basées sur des groupes sont utilisées, les seules stratégies téléchargées sont les balises CTS que le périphérique a des points d'extrémité locaux avec lesquels il doit appliquer.

- Pour pouvoir vérifier le mappage de l'adresse IP (ou du sous-réseau) à un groupe de stratégies basé sur un groupe, la commande "show cts role-based sgt-map vrf <vrf> all" peut être utilisée.

Afficher toutes les informations IP à SGT connues pour 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
```

Ce résultat montre toutes les adresses IP connues (et les sous-réseaux) pour un VRF donné et leurs associations de politiques basées sur des groupes.

- Comme vous pouvez le voir, une adresse IP d'un terminal est affectée au groupe de stratégies basé sur un groupe 17 et provient de l'adresse locale.
- Il s'agit du résultat de l'authentification qui se produit sur le port et où les résultats indiquent que l'étiquette est associée à ce point d'extrémité.
- Il met également en évidence les adresses IP propres aux commutateurs qui sont affectées à l'étiquette device-sgt comme interne source.
- Les balises de stratégie de groupe peuvent également être attribuées via la configuration ou via une session SXP vers ISE.

Lorsqu'un périphérique apprend l'existence d'une balise SGT, il tente de télécharger les stratégies qui lui sont associées à partir du serveur ISE.

- La commande show cts authorization entries donne une vue d'ensemble quand ils ont été tentés d'être téléchargés et s'ils ont été ou n'ont pas été téléchargés successivement.

Remarque : Les politiques doivent être mises à jour périodiquement en cas de modification des politiques. ISE peut également envoyer une commande CoA pour que le commutateur soit déclenché afin de télécharger de nouvelles stratégies lorsque des modifications sont apportées. Pour actualiser manuellement les stratégies, la commande "cts refresh policy" est exécutée.

Affichez une vue d'ensemble des stratégies que vous avez tenté de télécharger et si elles ont été ou non téléchargées successivement

<#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 des stratégies sont téléchargées, elles peuvent être affichées à l'aide de la commande « 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
```

Cette commande affiche toutes les stratégies que le périphérique a apprises. Sur le serveur ISE, il existe potentiellement plus de stratégies pour différents groupes, mais le périphérique tente uniquement de télécharger les stratégies pour lesquelles il connaît les terminaux. Cela permet d'économiser de précieuses ressources matérielles.

Cette commande affiche également l'action par défaut qui doit être appliquée au trafic pour lequel aucune entrée plus spécifique n'est connue. Dans ce cas, il s'agit de l'autorisation IP, de sorte que tout le trafic qui ne correspond pas à une entrée spécifique dans la table doit être autorisé à passer.

Exécutez la commande show cts rbacl <name>pour obtenir plus de détails sur le contenu exact de la liste de contrôle d'accès au routeur qui a été téléchargée

<#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

Dans ce cas, le seul trafic autorisé à être envoyé au point d'extrémité auquel cette liste RBACL est appliquée est les paquets TCP vers 22 (SSH) et 23 (Telnet).

Remarque : RBACL ne fonctionne que dans une seule direction. À moins qu'il y ait une

---

politique dans le trafic de retour, elle est appliquée avec la politique par défaut. Le trafic qui entre dans le fabric n'est pas appliqué, il est envoyé via le fabric avec la balise SGT connue sur le noeud d'entrée. Elle n'est appliquée que lorsqu'elle quitte le fabric et doit être appliquée aux stratégies présentes sur ce périphérique. En général, ces stratégies sont identiques, mais il est possible d'étendre le domaine CTS, par exemple avec un pare-feu, où d'autres stratégies auraient pu être définies en fonction des stratégies de sécurité déployées.

Exécutez « show cts role-based counters » pour valider si les trames sont abandonnées ou non

- Cette commande affiche les compteurs cumulés pour l'ensemble du commutateur. Il n’existe pas de commande équivalente pour chaque 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

Cette vue d'ensemble montre toutes les entrées connues que le commutateur connaît dans ce cas pour pouvoir faire correspondre le trafic de 17 à 16 et de 16 à 17.

- Toute autre correspondance qui tombe sous le * * et obtient l'action par défaut appliquée de sorte que si un trafic par exemple de 18 à 16 viendrait il ne correspond pas à la matrice connue sur le commutateur et ont l'action par défaut appliquée.

Même si les compteurs sont cumulatifs, ils donnent une bonne indication si le trafic est abandonné.

- Pour déterminer le trafic qui atteindrait une entrée, le mot-clé log peut être ajouté sur le serveur ISE aux stratégies respectives, ce qui a pour conséquence que le commutateur fournit des messages de journal lorsque cette entrée est atteinte.
- Cela peut être fait à la fois pour l'action par défaut (* *) ou pour l'une des entrées plus spécifiques de la matrice.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.