Risoluzione dei problemi di LISP VXLAN Fabric sugli switch Catalyst serie 9000

Sommario

Introduzione

Questo documento descrive i componenti di base di un fabric LISP basato su VXLAN e come verificarne il funzionamento.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Cisco IOS XE 17.9.3 o versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

LISP VXLAN based fabric

Lo scopo di una rete VXLAN LISP è di essere in grado di creare un'architettura in cui più reti Overlay, note anche come reti virtuali, vengono definite su una rete Underlay.

- La rete Underlay in tale topologia agirebbe principalmente come un livello di trasporto e non sarebbe a conoscenza delle topologie di sovrapposizione che vi vengono sottoposte.
- Le reti sovrapposte possono essere aggiunte e rimosse senza alcun impatto sulla rete sottostante.
- L'utilizzo di reti sovrapposte separa efficacemente gli utenti dalla rete sottostante.

Tecnologie utilizzate per creare un fabric VXLAN LISP

Locator Identity Separation Protocol (LISP)

- Il protocollo LISP è il protocollo del control plane utilizzato all'interno della struttura. Viene eseguito su tutti i dispositivi fabric per creare l'infrastruttura e controllare la modalità di invio del traffico nell'infrastruttura.
- LISP crea 2 spazi di indirizzo. Uno è per i RLOC (Routing Locator) utilizzati per pubblicizzare la raggiungibilità. L'altro spazio di indirizzi è per gli identificatori di endpoint (EID), dove risiedono gli endpoint ed è utilizzato per la sovrapposizione.
- All'interno di LISP gli EID vengono pubblicizzati con un RLOC pubblicizzato. Se un EID viene spostato, è sufficiente aggiornare la collocazione del ciclo associata.

- Per raggiungere un endpoint con traffico LISP verso un EID, occorre incapsulare il router e collegarlo tramite tunneling alla RLOC, che lo decapsula e lo inoltra all'endpoint.

Criteri basati su gruppo

- Viene utilizzato per consentire la segmentazione all'interno di criteri basati su gruppi di fabric.
- Quando vengono implementati criteri basati su gruppi, il traffico viene classificato con Secure Group anziché in base all'IP di origine/destinazione.
- In questo modo si riduce la complessità delle complesse liste di controllo degli accessi. Al posto degli elenchi di indirizzi IP che devono essere gestiti, gli indirizzi IP e le subnet vengono assegnati a un tag Secure Group.
- All'ingresso nel fabric viene etichettato con un SGT quando il traffico esce dal fabric, la destinazione del frame viene cercata per il suo SGT .
- Con l'uso di una matrice, il SGT di origine e di destinazione viene abbinato e viene applicato un ACL Secure Group per imporre il traffico quando esce dall'infrastruttura.

Incapsulamento VXLAN

- All'interno della struttura, la VXLAN viene usata per incapsulare tutto il traffico
- Il vantaggio di usare la VXLAN sull'incapsulamento LISP legacy è che permette di incapsulare l'intero frame di layer 2, non solo il frame di layer 3. Quando l'intero fotogramma viene incapsulato, le sovrapposizioni possono essere sia di livello 2 che di livello 3.
- VXLAN utilizza UDP con la porta di destinazione 4789. Ciò consente il trasporto dei frame VXLAN LISP anche attraverso dispositivi che non sarebbero a conoscenza della topologia di sovrimpressione.
- Poiché la VXLAN incapsula l'intero frame, è importante aumentare l'MTU in modo da non richiedere la frammentazione, in quanto il traffico viene inviato tra i RLOC. Tutti i dispositivi intermedi devono supportare una MTU più grande per trasportare i frame incapsulati.

Autenticazione

- Per poter assegnare gli endpoint alle rispettive risorse, è possibile utilizzare l'autenticazione.
- Con i protocolli come 802.1x, gli endpoint MAB e Webauth possono essere autenticati e/o profilati rispetto a un server Radius e possono essere autorizzati ad accedere alla rete in base ai loro profili di autorizzazione.
- Con i rispettivi attributi Radius, gli endpoint possono essere assegnati alle rispettive VLAN, SGT e a qualsiasi altro attributo per fornire un accesso alla rete endpoint/utente.

Componenti principali di LISP VXLAN Fabric

Nodo Control Plane

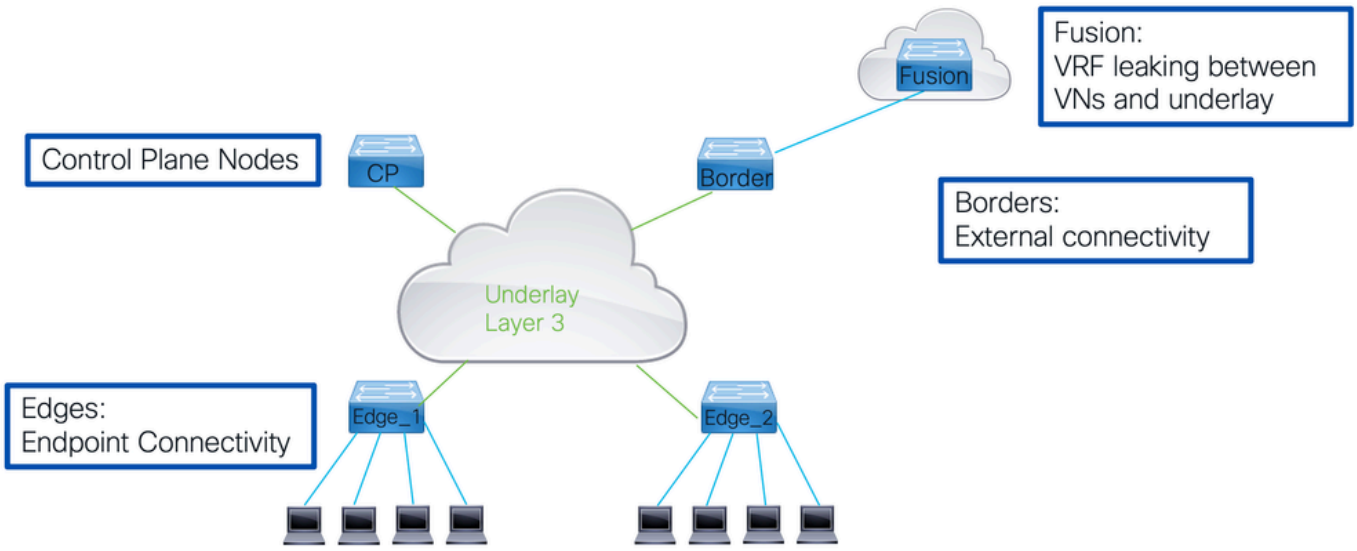
- contiene la funzionalità LISP Map Server e Map Resolver.
- Tutti gli altri dispositivi fabric richiedono al nodo Control Plane la posizione dell'EID e inviano le registrazioni per l'EID ai nodi Control Plane.
- In questo modo i nodi Control Plane hanno una visione completa del fabric per quanto riguarda la RLOC e i vari EID.

Nodi bordo

- Fornisce connettività al di fuori del fabric ad altri fabric o al mondo esterno.
- Le frontiere interne importano i percorsi nel fabric e li registrano con i nodi del Control Plane.
- I confini esterni si connettono al mondo esterno e forniscono un percorso predefinito all'esterno della struttura per le destinazioni IP sconosciute.

Nodi Edge

- Questi nodi forniscono connettività agli endpoint all'interno della struttura.
- Nella definizione del LISP, questi sarebbero XTR poiché svolgerebbero sia la funzione di router del tunnel in entrata (ITR) che la funzione di router del tunnel in uscita (ETR).



I nodi non sono limitati all'esecuzione di una sola operazione.

- Possono eseguire una combinazione o anche tutte le funzioni all'interno del fabric.
- Quando un nodo di bordo e un nodo di piano di controllo risiedono su un dispositivo, vengono definiti "collocati".
- Se tale nodo fornisce anche la funzionalità Edge, deve essere indicato come Fabric In A Box (FIAB).

I bordi permettono di passare il traffico al resto della rete usando VRF lite.

- Ogni overlay o rete virtuale è associata a un'istanza VRF sul nodo di bordo.
- Per collegare i vari VRF viene utilizzato un router Fusion. Il router di fusione non fa parte del fabric stesso, ma è cruciale per le operazioni in modo da poter connettere le reti di overlay al fabric.

Un altro concetto importante nel fabric VXLAN LISP è l'uso di un Anycast IP.

- Ciò significa che su tutti i dispositivi Edge vengono replicati l'indirizzo IP e i relativi indirizzi

MAC delle interfacce virtuali commutate (SVI).
- Ogni perimetro ha la stessa configurazione sulla SVI per quanto riguarda gli indirizzi IPv4, IPv6 e MAC.
- La risoluzione di questo problema implica alcune sfide.
    - Per verificare la raggiungibilità con il comando ping, il sistema funziona con i dispositivi collegati in locale.
    - Per raggiungere le destinazioni remote tramite l'infrastruttura VXLAN LISP, la risposta non viene restituita in quanto il dispositivo che invia la risposta la invia anche all'indirizzo IP anycast che viene puntato al dispositivo fabric locale che non è a conoscenza di quale altro nodo fabric abbia inviato il ping originale.

Registrazione degli endpoint

Affinché un fabric VXLAN LISP funzioni, è fondamentale che il nodo Control Plane sia consapevole di come tutti gli endpoint sono raggiungibili tramite il fabric.

- Affinché il control plane possa conoscere tutti gli EID presenti nella rete, è necessario che tutti gli altri dispositivi fabric registrino tutti gli EID che conosce con il control plane.
- Un nodo fabric invia messaggi LISP di registrazione mappe al nodo del control plane. Tra le informazioni pubblicizzate con il messaggio di registro delle mappe.

Informazioni importanti

Identificatore istanza LISP:

- Questo identificatore viene trasferito nell'infrastruttura e indica la rete virtuale da utilizzare.
- All'interno di un fabric VXLAN LISP per overlay di layer 3, viene utilizzata un'istanza per ogni VLAN usata nel fabric e un'istanza di layer 2.

EID (Endpoint Identified):

- Se si tratta di un'istanza di livello 2 o 3, si tratta dell'indirizzo MAC, della route di host IP (/32 o /128) o di una subnet IP registrata

RLOC (Routing Locator):

- Il nodo fabric possiede un indirizzo IP con il quale annuncia la raggiungibilità dove altri dispositivi fabric inviano traffico incapsulato che dovrebbe raggiungere l'EID.

Flag proxy:

- Quando questo flag è impostato, consente al nodo Control Plane di rispondere direttamente alle richieste di mappatura da altri nodi dell'infrastruttura, senza che il flag proxy imposti tutte le richieste da inoltrare al nodo dell'infrastruttura che ha registrato l'EID.

Procedura di registrazione

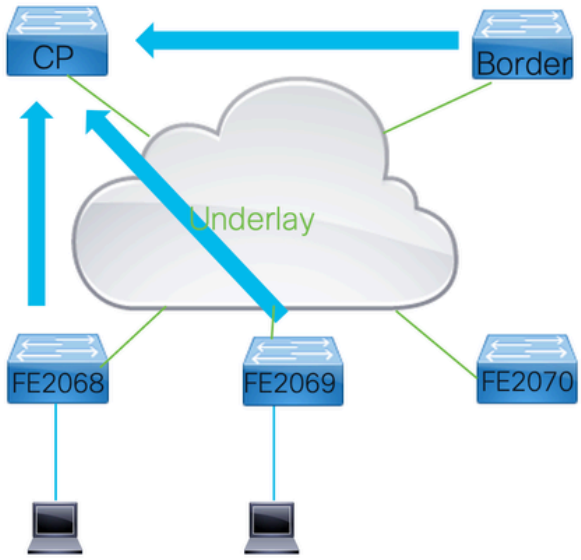
Passaggio 1: I dispositivi Fabric forniscono informazioni sugli identificatori degli endpoint. Questo

può avvenire tramite la configurazione, i protocolli di routing o quando viene appreso dai dispositivi fabric.

Passaggio 2: i dispositivi fabric registrano gli endpoint appresi con ogni nodo Control Plane noto e raggiungibile all'interno della struttura.

Passaggio 3: I nodi Control Plane gestiscono una tabella di EID registrati con il relativo Instance ID, il RLOC e l'EID appreso

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



Verifica

1.1 Apprendimento dell'indirizzo MAC

Per le istanze di layer 2, gli EID utilizzati sono gli indirizzi MAC appresi nella VLAN associata. Fabric Edges apprende gli indirizzi di layer 2 tramite i metodi standard sugli switch.

Individuare la VLAN associata a un ID istanza di layer 2 specifico. È possibile rivedere la configurazione o usare il comando

Utilizzare "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
```

Come mostrato nell'output, l'id istanza 8191 è associato alla VLAN 150. Di conseguenza, tutti gli indirizzi MAC all'interno della vlan devono essere registrati con il protocollo LISP e diventare parte della struttura della 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
```

Le voci statiche con interfaccia Vl150 sono gli indirizzi MAC dell'interfaccia virtuale dello switch (interfaccia vlan 150).

- Questi indirizzi MAC non vengono registrati con il nodo del control plane, in quanto sarebbero gli stessi su tutti i dispositivi edge.
- La voce CP_LEARN visualizzata è quella appresa attraverso la struttura. Per tutte le altre voci, se dinamiche o statiche, devono essere registrate con il nodo del piano di controllo.

Una volta appresi tramite i rispettivi mezzi, questi vengono visualizzati negli output del database lisp, questo output contiene tutte le voci locali su questo dispositivo 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

Per tutti gli indirizzi MAC locali noti visualizzati nel database, viene visualizzato il Localizzatore.

- Localizzatore da utilizzare per registrare questa voce con il nodo del control plane.
- Indica anche lo stato del Locator.Vengono mostrati anche i due indirizzi MAC che appartenevano agli switch SVI, ma sono contrassegnati con il flag "do not register", che impedisce la loro registrazione.
- La voce remota visualizzata nel comando show mac address table non è un indirizzo MAC locale e pertanto non viene visualizzata nel database lisp.

Per un'istanza di layer 2, non solo gli indirizzi MAC di layer 2 vengono appresi come EID, ma è anche necessario apprendere le informazioni sulla risoluzione degli indirizzi dai frame ARP e ND.

- In questo modo, il fabric VXLAN dell'interfaccia LISP è in grado di inoltrare quei frame che normalmente vengono trasmessi all'interno della VLAN.
- Poiché l'ID istanza di layer 2 non sempre è in grado di passare a un altro meccanismo che consentirebbe agli endpoint di risolvere le informazioni sulla risoluzione degli indirizzi per altri endpoint nella stessa istanza. Per questo motivo, i dispositivi fabric apprendono e registrano queste informazioni che vengono apprese localmente mediante il rilevamento dei dispositivi.
- che viene quindi registrato anche con i nodi del Control Plane. A causa dello snooping ND o ARP, questi pacchetti vengono puntati alla CPU per attivare una richiesta ai nodi del Control Plane per vedere se c'è qualche indirizzo MAC noto associato.
- In caso di risposta positiva, i pacchetti ARP/ND vengono riscritti in modo che l'indirizzo mac di destinazione venga modificato da broadcast o multicast all'indirizzo mac unicast.
- Questo pacchetto riscritto può quindi essere inoltrato attraverso il fabric VXLAN LISP come frame unicast.

Per visualizzare le informazioni sulla risoluzione degli indirizzi note sullo switch, è possibile usare il comando show device-tracking database.

- Vengono mostrati tutti i mapping noti mediante il rilevamento dei dispositivi.
- Gli indirizzi IP degli switch sono contrassegnati con L(Local) e devono essere presenti nel database di rilevamento dei dispositivi.

In questo output vengono visualizzate anche voci remote.

- Quando vengono risolti dopo lo snooping della richiesta ND o ARP, vengono inseriti nel database di rilevamento dispositivi con un indirizzo di livello di collegamento 0000.0000.00fd.
- Nel momento in cui vengono risolti, le informazioni vengono modificate in direzione dell'indirizzo MAC risolto e la porta viene modificata in Tu0.

Visualizzare il database di rilevamento dispositivi

<#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
```

Visualizzare i mapping registrati localmente con il 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 Apprendimento degli indirizzi IP dinamici

Sui dispositivi fabric su un layer IP, una rete virtuale viene formata associando un ID istanza LISP a un VRF.

- Questo VRF viene quindi configurato nelle diverse interfacce virtuali dello switch (SVI) e diventa parte della rete di overlay di layer 3
- Nella maggior parte dei casi queste SVI appartengono anche a VLAN registrate con le rispettive istanze di layer 2.

Trovare il mapping tra VRF e LISP Instance id con il 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: Questo comando può essere utilizzato anche per verificare le varie funzioni che possono essere abilitate per questa istanza e per visualizzare i nodi Control Plane utilizzati all'interno del fabric VXLAN LISP

Una volta creata un'istanza di layer 3 e collegata a un VRF, viene creata un'interfaccia LISP 0 <id-istanza> che è visibile nella configurazione corrente e in show vrf.

- Questa interfaccia NON deve essere creata manualmente e in genere non richiede alcuna configurazione (ad eccezione della configurazione multicast quando si utilizza il multicast inferiore).

<#root>

FE2068#

show vrf Fabric_VN_1

  Name   Default RD   Protocols   Interfaces

Fabric_VN_1

                  ipv4,ipv6

LI0.4099

Vl150

Vl151

A differenza dei frame Ethernet, in cui tutti gli indirizzi MAC di una VLAN vengono utilizzati per l'IP, è necessario che gli indirizzi IP si trovino in un intervallo EID dinamico.

Visualizzare un'istanza 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
```

Gli indirizzi IP che non rientrano in questi intervalli definiti vengono considerati non idonei per la

struttura e non vengono inseriti nei database LISP e non registrati nei nodi del control plane.

<#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

L'output mostra tutte le informazioni sull'indirizzo IP conosciute localmente.

- Per gli host, si tratta in genere di route host (/32 o /128), ma possono anche essere subnet se importate nel database LISP sul nodo di bordo.
- Gli indirizzi IP dell'SVI sono contrassegnati come "do not register" (non registrare). In questo modo, si evita che tutti i dispositivi fabric registrino l'indirizzo IP Anycast sul control plane node.

<#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 Registrazione dell'EID sul Control Plane

La registrazione degli endpoint in una struttura basata su VXLAN LISP avviene tramite una registrazione affidabile LISP. Ciò significa che tutte le registrazioni vengono effettuate tramite una sessione TCP stabilita, la sessione LISP. Da ogni dispositivo fabric viene stabilita una sessione LISP con ciascuno dei nodi del control plane nella struttura. Attraverso questa sessione LISP si

verificano tutte le registrazioni. Se all'interno di una struttura sono presenti più nodi del Control Plane, tutti devono essere utilizzati per registrare gli EID con.

Lo stato è Inattivo quando non c'è nulla da registrare sul dispositivo fabric, il che in genere si verifica solo alle frontiere esterne
che non registrano intervalli IP con il nodo Control Plane o su dispositivi Edge senza endpoint

La registrazione dell'EID avviene tramite i messaggi di registrazione LISP
che vengono inviati a tutti i nodi del control plane configurati.

Per visualizzare la sessione LISP su un dispositivo fabric, è possibile utilizzare il comando show lisp session.
Viene visualizzato lo stato della sessione e l'ora in cui è stata attivata.

<#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 sessione LISP mostrata come Inattiva può essere eseguita su dispositivi che non dispongono di EID da registrare con il nodo Control Plane.
Si tratta in genere di nodi di bordo che non importano route nei dispositivi fabric o Edge senza alcun endpoint connesso.

Visualizzare informazioni più dettagliate su una sessione LISP con il comando 'show lisp session vrf default <indirizzo ip>'

<#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
```

Questo output dettagliato della sessione mostra quali istanze sono attive con EID registrate con i nodi del control plane.

<#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
```

Se si osserva il numero di sessioni in un nodo di Control Plane, in genere vengono visualizzate più sessioni attive.

- Se si tratta di un nodo Border/CP con posizione condivisa, viene stabilita anche una sessione LISP verso se stessa.
- In questo caso c'è una sessione da 172.30.250.19:4342 a 172.30.250.19:49270.
- Durante questa sessione, il componente Border registra il proprio EID con il Control Plane Node.

1.4 Informazioni sul Control Plane

Con le informazioni fornite dai dispositivi fabric tramite registrazione, il nodo del control plane è in grado di creare una vista completa del fabric. Per Instance-id gestisce una tabella con gli EID appresi e le relative collocazioni di instradamento associate.

Visualizzare questo comando per le istanze di layer 3 con il 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
```

Questo comando visualizza tutti gli EID registrati e l'ultimo che ha registrato l'EID. È importante notare che in genere questo sarebbe anche il RLOC in uso, ma questo può essere diverso. Anche gli EID possono essere registrati con più RLOC.

Per visualizzare i dettagli completi, includere l'EID e l'istanza

<#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: Nell'output dettagliato è importante tenere presente quanto segue:

- Proxy, con questo set il nodo Control Plane risponde direttamente a una richiesta Map. Nel LISP tradizionale una richiesta di mappa viene inoltrata al XTR che ha registrato l'EID ma con l'impostazione Proxy il nodo del control plane risponde direttamente
- TTL, questa è la durata della registrazione dell'EID. Per impostazione predefinita è di 24 ore
- Informazioni ETR, relative al dispositivo fabric che ha inviato la registrazione EID
- Informazioni RLOC, si tratta dell'RLOC da utilizzare per raggiungere l'EID. Contiene inoltre informazioni sullo stato, ad esempio quelle relative all'attivazione e alla disattivazione. se l'RLOC non è attivo, non viene utilizzato. Contiene inoltre un peso e una priorità che possono essere utilizzati quando esistono più RLOC per un EID per dare la preferenza a uno di essi.

Per visualizzare la cronologia delle registrazioni sul nodo Control Plane, è possibile utilizzare il comando show lisp server registration history.

- Fornisce una panoramica dell'EID che è stato registrato e cancellato.

Visualizza cronologia registrazioni

<#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
```

Visualizzare l'EID registrato per Ethernet. Il comando è show lisp instance-id <instance> ethernet server (restituisce un output simile a quello del layer 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

Aggiungere l'indirizzo MAC per ottenere informazioni più dettagliate su una registrazione

<#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
```

Aggiungi 'cronologia registrazioni' per visualizzare la cronologia delle registrazioni per EID Ethernet

---

Nota: Questo comando è molto utile quando i dispositivi girano nella struttura per vedere dove e quando l'indirizzo MAC è stato registrato

---

<#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
```

Per visualizzare le informazioni registrate sulla risoluzione degli indirizzi nel nodo Control Plane, il comando viene aggiunto alla risoluzione degli indirizzi.

- Mostra solo le mappature tra l'indirizzo MAC e le relative informazioni di layer 3 e deve essere utilizzato principalmente per i bordi dell'infrastruttura per riscrivere gli indirizzi MAC di destinazione di layer 2 da broadcast/multicast a unicast.
- L'RLOC corrispondente all'indirizzo MAC di layer 2 verrà risolto separatamente.

Aggiungere 'address-resolution' per visualizzare le informazioni registrate sulla risoluzione degli indirizzi nel nodo Control Plane

<#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: Anche se gli indirizzi IPv6 locali del collegamento non corrispondono all'EID dinamico IPv6, devono essere appresi per la risoluzione degli indirizzi e verrebbero visualizzati nel nodo Control Plane. Questi non verrebbero registrati sotto l'ID istanza di layer 3, ma sono disponibili per la risoluzione degli indirizzi.

Risolvi destinazioni remote

Per inoltrare il traffico tramite un fabric VXLAN LISP, è necessario risolvere il RLOC di una destinazione. All'interno di un fabric VXLAN LISP, questa operazione viene effettuata con l'uso di una map-cache dalla quale le informazioni vengono inserite nella Forwarding Information Base (FIB) del dispositivo Fabric.

Con LISP VXLAN fabric le cache delle mappe devono essere attivate a causa dei segnali dei dati.

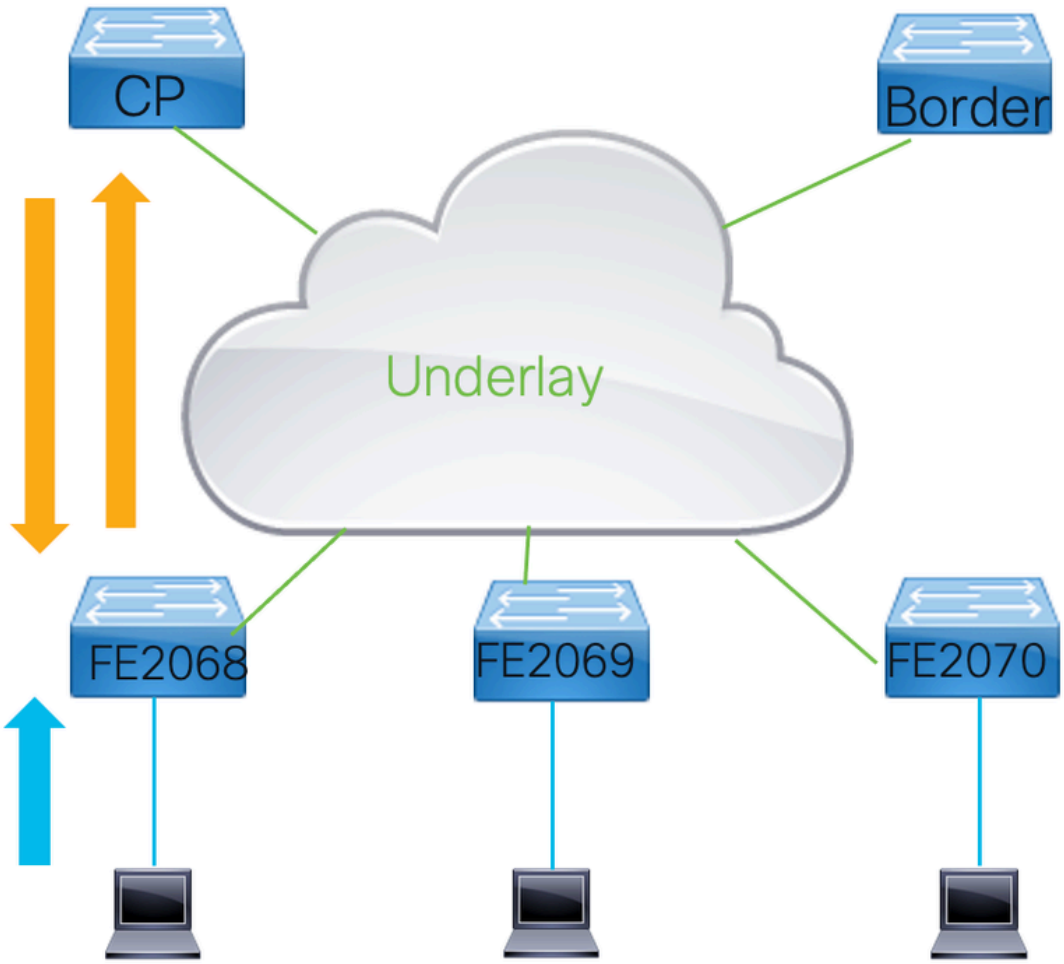
- Questo significa che il traffico viene inoltrato alla CPU e la CPU crea una richiesta di mappa verso il nodo Control Plane per cercare le informazioni RLOC a cui i frame verso l'EID dovrebbero essere inviati.
- Quando riceve una richiesta di mapping, il piano di controllo fornisce le informazioni sulla collocazione del ciclo associate all'EID oppure restituisce una risposta di mapping negativa.
- Quando invia una risposta negativa alla mappa, il nodo del control plane non indica semplicemente che l'EID richiesto non è noto, ma offre l'intero blocco di EID a cui l'EID appartiene e per il quale non ha alcuna registrazione.

Con le informazioni contenute nella mappa-risposta dal nodo del control plane, la mappa-cache viene aggiornata.

- Il valore TTL per le risposte delle mappe è in genere di 24 ore. (Per le risposte di mappa

negative, in genere solo 15 minuti).

- Per l'EID Ethernet, le risposte negative delle mappe non vengono inserite nella cache delle mappe. Questa operazione viene eseguita solo per le istanze di layer 3.



2.1 Ethernet map-cache

Visualizzare Ethernet map-cache con il 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        -
```

Questo comando mostra la voce dell'indirizzo MAC remoto che sarebbe stata risolta.

- Per attivare una voce map-cache per un'istanza Ethernet, il traffico deve essere inviato a una destinazione sconosciuta.
- In questo modo il dispositivo fabric proverebbe a risolverlo tramite LISP.
- Una volta appreso tramite una risposta mappa, verrà inserito nella cache delle mappe e i fotogrammi successivi verso la destinazione di layer 2 verranno inviati direttamente al localizzatore di routing appreso.

Facoltativamente, nelle istanze di layer 2 viene utilizzato il flusso del traffico BUM.

- LISP/VXLAN non inonda il traffico per impostazione predefinita in quanto utilizza una tecnologia di sovrimpressione, ma è possibile configurare un gruppo IP Multicast nella rete sottostante (GRT) attraverso il quale i frame di layer 2 potrebbero essere inondati.

Visualizza l'indirizzo del gruppo sottostante di trasmissione

<#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 mappa IP

Per le istanze di layer 3, le informazioni della map-cache sono simili a quelle della build ethernet generata dal traffico inviato alla CPU per segnalare l'invio di una map-request.

- Tuttavia, per i pacchetti di layer 3, solo la CPU viene puntata per segnalare quando deve essere configurato. Questa operazione viene eseguita dal comando map-cache configurato.

Per IPv4 questo valore è 0.0.0.0/0 e ::0/0 per IPv6.

- La configurazione di questa voce della cache delle mappe sui nodi di confine deve essere eseguita con cautela. Se un nodo di bordo è configurato con questa voce map-cache 0.0.0.0/0 o ::0/0, tenta di risolvere le destinazioni sconosciute tramite l'infrastruttura anziché instradarla all'esterno dell'infrastruttura.

Visualizza la configurazione della cache delle mappe

<#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
```

Il comando map-cache 0.0.0.0/0 e ::/0 map-request determinano la configurazione di una voce map-cache nella map-cache con le azioni "send-map-request". Il traffico che raggiunge questo innesca le richieste di mapping. Poiché le voci map-cache devono essere inserite nel FIB che funziona in base alla corrispondenza più lunga, questa viene applicata a tutto il traffico IP indirizzato che non colpisce nessuna delle voci più specifiche.

- Sulle piattaforme supportate, per evitare che il primo pacchetto venga scartato, l'azione mostrata è send-map-request + encapsulate to proxy ETR.
  Il risultato è che il primo pacchetto verso una destinazione sconosciuta attiva una richiesta map e, se presente, il pacchetto viene inoltrato al router proxy.

<#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

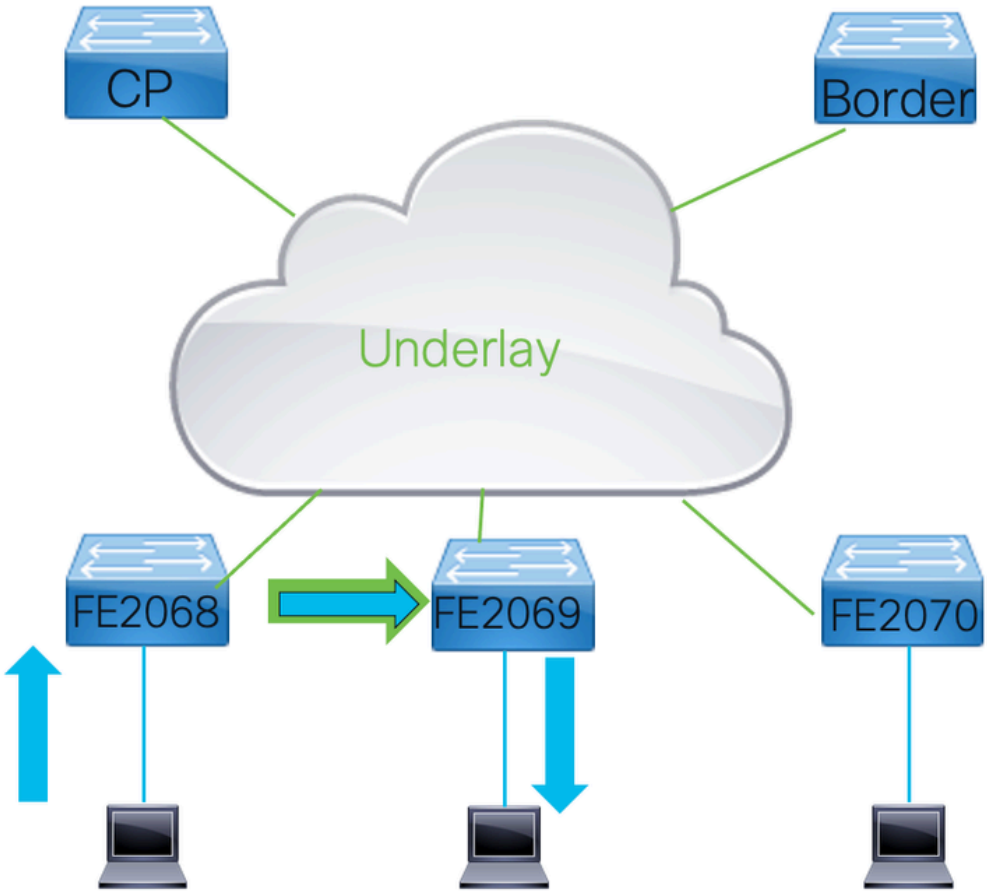
PETR	Uptime	State	Pri/Wgt	Encap-IID	Metric
172.30.250.19					

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

In questo output vengono mostrate alcune voci.

- 10.48.13.0/24 e 172.24.2.2/32 in questo output viene appreso tramite corrispondenza-risposta e viene completato. Il traffico verso queste destinazioni deve essere incapsulato e inoltrato ai rispettivi localizzatori.
- 172.28.0.0/14 è un esempio di risposta di mapping negativa ricevuta e di un blocco di indirizzi IP restituito. Il traffico verso questa subnet non attiva una richiesta di mapping finché la voce è nella cache delle mappe.

Inoltro del traffico attraverso l'infrastruttura



3.1 Inoltro di livello 2 o 3

Il traffico in un'infrastruttura LISP/VXLAN può essere inoltrato tramite istanze di layer 2 o layer 2.

- La determinazione dell'istanza utilizzata dipende dall'indirizzo MAC di destinazione v dei frame.

- I frame che vengono inviati a qualsiasi indirizzo MAC diverso da quello registrato con lo switch in cui devono essere inoltrati i frame utilizzano il layer 2. Se la destinazione del pacchetto è lo switch, il pacchetto viene inoltrato attraverso il layer 3.
- Questa logica si applica anche all'inoltro normale tramite uno switch Catalyst serie 9000.

3.2 Inoltro di livello 2

L'inoltro di layer 2 tramite infrastruttura VXLAN LISP viene eseguito in base all'indirizzo MAC di destinazione di layer 2. La destinazione remota viene inserita nella tabella degli indirizzi MAC con l'interfaccia in uscita L2LI0.

Visualizzare le interfacce di layer 2 locali e remote

<#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
```

Per destinazioni sconosciute, se configurate, il traffico viene inviato tramite il gruppo multicast IP configurato nell'alloggiamento sottostante.

- Per garantire la corretta trasmissione del traffico Broadcast, Unicast sconosciuto e Multicast (solo Flood multicast selettivo), è necessario un ambiente multicast correttamente operativo nell'alloggiamento sottostante.
- Il traffico che verrebbe inviato tramite questo gruppo di underlay multicast deve essere incapsulato nella VXLAN.
- Tutti gli altri bordi devono unirsi al gruppo multicast e ricevere il traffico e decapsulare il traffico per le istanze di layer 2 conosciute.

Visualizzare il gruppo multicast IP sottostante

<#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:
```

Questo output mostra una voce S,G per tutti gli altri spigoli nella struttura in cui sono configurati i

client che invierebbero il traffico esteso. Mostra anche una voce S,G con il loopback0 di questo dispositivo Edge come origine.

Per il lato ricevente del traffico che attraversa il gruppo multicast sottostante, il comando show ip route visualizza anche L2LISP0.<instance>
questo comando indica per quali istanze di layer 2 il dispositivo edge deve decapsulare il traffico flooded e inoltrarlo al relativo
interfacce rilevanti.

3.3 Inoltro di informazioni sul layer 3

Per determinare la modalità di inoltro del traffico quando viene distribuita una struttura LISP VXLAN, è importante verificare il CEF.

- A differenza dei protocolli di routing tradizionali, LISP inserisce la direzione di routing non nella tabella di routing ma interagisce direttamente con il CEF per aggiornare il FIB.

Per una determinata destinazione remota le informazioni della cache delle mappe contengono le informazioni dell'indicatore di percorso da utilizzare.

Visualizzare le informazioni sull'indicatore di posizione

<#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)
```

Dalla map-cache, il Locator da usare per l'EID è 172.30.250.44. Il traffico verso questa

destinazione deve essere incapsulato e l'intestazione IP esterna ha un indirizzo di destinazione IP di 172.30.250.44.

Questa voce non viene visualizzata nella tabella di routing per il VRF utilizzato per questa istanza.

<#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
```

Gli output CEF forniscono ulteriori informazioni sull'inoltro attraverso il fabric VXLAN LISP.

- quando si aggiunge la parola chiave detail al comando show ip cef, non viene fornita solo la destinazione del fotogramma incapsulato da inviare.
- L'interfaccia in uscita con questo output è LISP 0.<instance> indica che il traffico viene inviato incapsulato.

<#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
```

Poiché il traffico verrebbe inviato incapsulato verso l'hop successivo, il passaggio successivo è eseguire un show ip cef <hop successivo> per visualizzare l'interfaccia in uscita contenente il pacchetto.

Esegui per visualizzare l'interfaccia di uscita

<#root>

```
FE2067#

sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23
```

Nota: Sono possibili 2 diversi livelli di routing ECMP (Multiple Path) a costo uguale.

- È possibile bilanciare il carico del traffico nella sovrimpressione nel caso in cui vi siano 2 RLOC annunciati e può essere bilanciato il carico nella rete sottostante se esistono percorsi ridondanti per raggiungere un indirizzo IP RLOC.
- Poiché la porta di destinazione UDP è fissata a 4789 e gli indirizzi IP di origine e destinazione per tutti i flussi tra due dispositivi fabric sono gli stessi, è necessario che si verifichi una forma di meccanismo anti-polarizzazione per evitare che tutti i pacchetti vengano instradati sullo stesso percorso.
- Con LISP VXLAN, questa è la porta di origine UDP nell'intestazione esterna che sarebbe diversa per i diversi flussi nella rete di overflow.

3.4 Formato pacchetto

- All'interno dei fabric LISP VXLAN tutto il traffico è completamente incapsulato nella VXLAN. Questo include l'intero frame di layer 2 per supportare sia le sovrapposizioni di layer 2 che di layer 3.

Per i frame di layer 2 l'intestazione originale è incapsulata. Per i frame inviati tramite un'istanza di livello 3 viene utilizzata un'intestazione di livello 2 fittizia.

<#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
```

Come mostrato dall'acquisizione di esempio di un frame trasportato attraverso un fabric VXLAN LISP, il frame completamente incapsulato all'interno del pacchetto vxlan. Come un frame di layer 3, l'intestazione ethernet è un'intestazione fittizia.

Nell'intestazione VXLAN, il campo VLAN Network Identifier contiene l'ID istanza LISP a cui appartiene il frame.

- Tramite il campo ID Criteri di gruppo viene inserito il tag SGT dei frame.
- Questo viene impostato sull'entrata nel fabric e viene trasportato verso il fabric fino a quando non viene applicata la policy basata su gruppo.

Autenticazione e applicazione della sicurezza

4.1 Autenticazione porta switch

Per assegnare dinamicamente gli endpoint alle rispettive VLAN e assegnare loro un tag SGT, è possibile utilizzare l'autenticazione.

- I protocolli di autenticazione come Dot1x/MAB/central webauth possono essere implementati per autenticare e autorizzare utenti ed endpoint su un server Radius che invia attributi allo switch per consentire l'accesso di rete al client/endpoint nel pool corretto e con l'autorizzazione di accesso alla rete corretta.

Per il fabric VXLAN LISP, gli attributi del raggio comuni sono pochi:

- Assegnazione VLAN: Questo attributo è impostato sull'ID o sul nome della VLAN tra il server radius e gli switch che un endpoint può essere assegnato a una specifica istanza LISP di layer 2/3.
- Valore SGT: Questo attributo imposta un SGT e assegna un endpoint a questo SGT. Questa opzione viene utilizzata per i criteri basati su gruppo per l'endpoint e per l'assegnazione di un valore SGT a tutti i frame inviati tramite l'infrastruttura originati dall'endpoint.
- Autorizzazione vocale: I dispositivi voce funzionano sulla vlan vocale. Questa opzione consente di impostare l'autorizzazione vocale in modo che l'endpoint possa inviare e ricevere il traffico nella vlan vocale configurata su una porta. In questo modo, il traffico voce e dati viene separato nelle rispettive VLAN
- Timeout sessione: Vari endpoint dispongono di timeout specifici per le sessioni. È possibile inviare un timeout dal server RADIUS per indicare la frequenza con cui un client deve ripetere l'autenticazione
- Modello: Per il corretto funzionamento di alcuni endpoint, è necessario applicare un modello diverso a una porta. È possibile inviare un nome di modello dal server Radius che indichi cosa deve essere applicato alla porta

Per verificare il risultato dell'autenticazione su una porta, usare il comando show access-session

<#root>

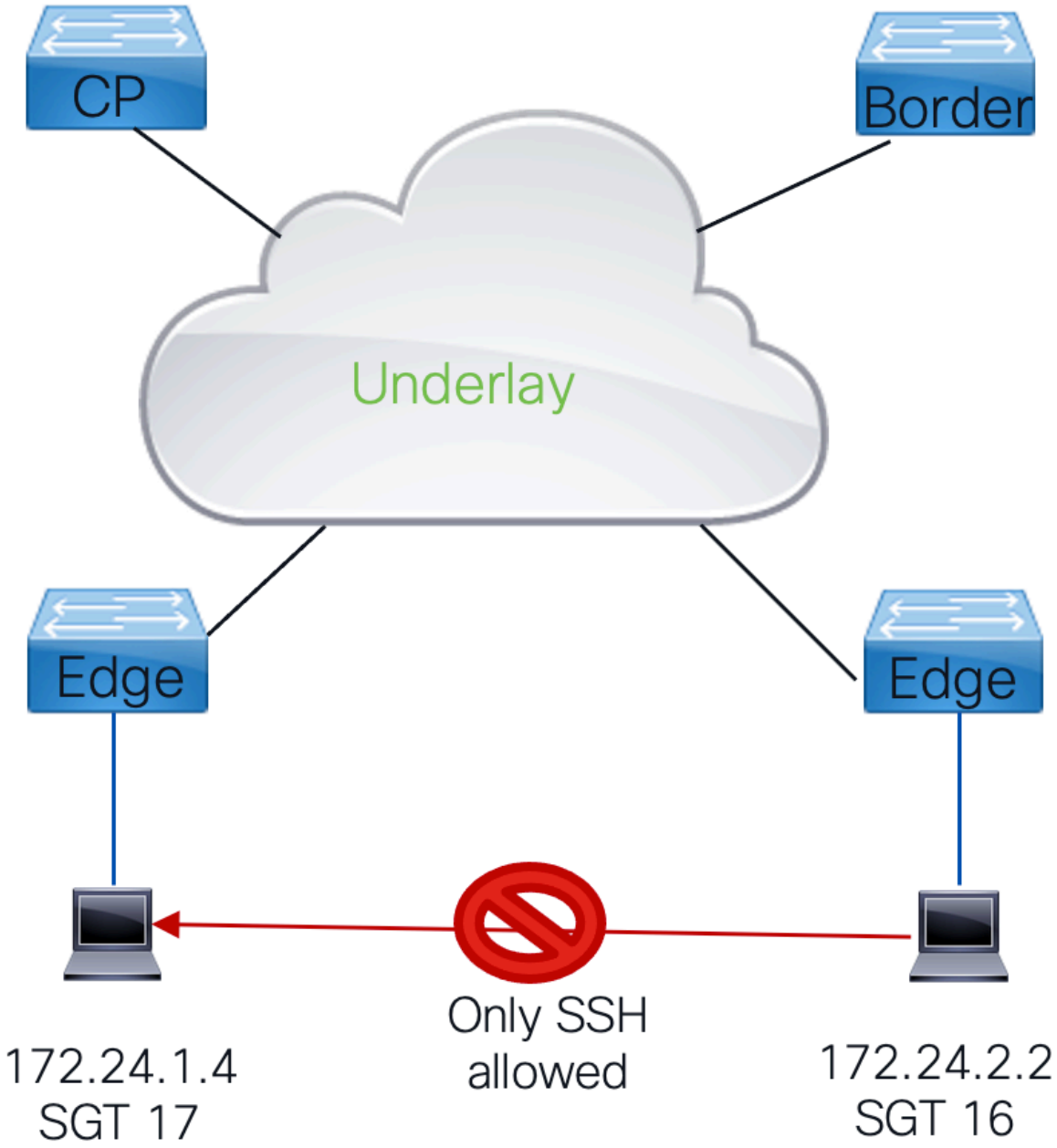
```
FE2067#

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
```

Tenere presente quanto riportato di seguito.

- Indirizzi IPv4 e IPv6: In genere appreso tramite il controllo dei dispositivi.
- Username: Nome utente utilizzato per l'autenticazione.
    - Per Dot1x si tratta in genere dell'utente che esegue l'autenticazione.
    - Quando si usa MAB, questo è l'indirizzo MAC della stazione che viene inviata a Radius come nome utente e password per l'autenticazione.
- Stato: Indica lo stato dell'autenticazione e il risultato dell'autenticazione.
- Dominio: Per gli endpoint normali, questo sarebbe il dominio dati, quindi il traffico verrebbe inviato/ricevuto senza tag sulla porta. (per i dispositivi voce può essere impostato su Voce)
- Criteri server: In questa posizione vengono memorizzate le informazioni provenienti dal server Radius, ad esempio l'assegnazione della VLAN e l'assegnazione SGT
- Elenco stato metodo: In questa pagina viene illustrata una panoramica dei metodi eseguiti.
    - Il punto 1x standard viene eseguito prima del MAB.
    - Se un endpoint non risponde ai frame EAPOL, il metodo esegue il failover su mab.
    - In questo modo il dot1x risulterebbe non riuscito.
    - Il MAB indica che l'autenticazione è riuscita indica che è riuscita ad eseguire l'autenticazione e non indica se il risultato dell'autenticazione sarebbe un'operazione di accettazione o rifiuto dell'accesso.

4.2 Politiche del traffico e Criteri basati sul gruppo (CTS)



All'interno di una struttura LISP VXLAN, il protocollo CTS viene utilizzato per applicare i criteri del traffico:

- L'architettura dei criteri basati su gruppi è basata su tag di gruppo sicuri.
- Tutto il traffico all'interno della struttura viene assegnato in entrata e con un tag SGT che viene trasportato attraverso la struttura in ogni struttura.
- Quando il traffico esce dalla rete, vengono applicate le policy sul traffico.
- Questa operazione viene eseguita in Criteri basati su gruppo, che controlla i tag del gruppo di origine e di destinazione del pacchetto rispetto alla matrice costituita da SGT origine-destinazione in cui il risultato è un SGACL che definisce il traffico che sarebbe o non sarebbe consentito.
- Quando nella matrice non è presente alcuna corrispondenza specifica per il SGT origine-

destinazione, deve essere applicata l'azione predefinita definita.

4.3 Ambiente CTS

Per utilizzare le policy di gruppo, la prima cosa necessaria per i dispositivi Fabric è ottenere un pacchetto CTS.

- Questo pacchetto deve essere usato all'interno di frame del raggio per autorizzare i frame RADIUS su Cisco ISE. Questa opzione viene utilizzata per impostare il campo ct-pac-opaque all'interno dei fotogrammi del raggio.

Visualizzare le informazioni sul pacchetto 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

È importante verificare che il pacchetto CTS sia configurato e valido. Questo viene aggiornato automaticamente dal dispositivo Fabric.

Nota: Per attivare manualmente un aggiornamento, è possibile emettere il comando "cts refresh pac".

Per le policy basate su gruppo, consente di scaricare i dati dell'ambiente e le informazioni sulle policy necessarie.

- I dati dell'ambiente contengono sia il tag CTS usato dallo switch stesso sia la tabella di tutti i gruppi di criteri basati su gruppo noti sul server Radius.

Visualizzare i dati dell'ambiente CTS

<#root>

FE2067#

sh cts environment-data

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

COMPLETE

Last status =

Successful

Service Info Table:
Local Device SGT:
SGT tag =

2-00:TrustSec_Devices

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

10.48.13.221

, port 1812,

A-ID C7105D0DA108B6AE0FB00499233B9C6A

Status = ALIVE
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
0-00:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:Production_Users
8-00:Developers
9-00:Auditors
10-00:Point_of_Sale_Systems
11-00:Production_Servers
12-00:Development_Servers
13-00:Test_Servers
14-00:PCI_Servers
15-00:BYOD
16-00:Fabric_Client_1
17-00:Fabric_Client_2
255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 11:46:41 UTC Fri Mar 31 2023
Env-data expires in 0:19:17:04 (dd:hr:mm:sec)

```
Env-data refreshes in 0:19:17:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
Retry_timer (60 secs) is not running
```

Quando vengono utilizzati criteri basati su gruppi, gli unici criteri che vengono scaricati sono i tag CTS che il dispositivo ha endpoint locali con cui deve applicare.

- Per verificare il mapping dall'indirizzo IP (o subnet) a un gruppo di criteri basato su gruppo, è possibile utilizzare il comando "show cts role-based sgt-map vrf <vrf> all".

Visualizzare tutte le informazioni da IP a SGT note per 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
```

Questo output mostra tutti gli indirizzi IP (e le subnet) noti per un determinato VRF e le relative associazioni di criteri basate su gruppo.

- Come si può vedere, c'è un indirizzo IP di un endpoint a cui sono assegnati criteri basati sul gruppo 17 e che ha origine locale.
- Questo è il risultato dell'autenticazione che si verifica sulla porta e dove i risultati indicano che il tag associato all'endpoint.
- Vengono inoltre evidenziati gli indirizzi IP degli switch ai quali viene assegnato il tag del segmento di dispositivo come interno di origine.
- Le etichette dei criteri basati sui gruppi possono essere assegnate anche tramite la configurazione o una sessione SXP verso ISE.

Quando un dispositivo viene a conoscenza di un tag SGT, cerca di scaricare le policy associate dal server ISE.

- Il comando show cts authorization fornisce una panoramica dei casi in cui si è tentato di scaricarli e se sono stati o non sono stati scaricati successivamente.

Nota: I criteri devono essere aggiornati periodicamente in caso di modifiche. ISE può anche eseguire un comando CoA per attivare lo switch in modo da scaricare nuove policy quando vengono apportate modifiche. Per aggiornare manualmente i criteri, viene emesso il comando "ct refresh policy".

Visualizza una panoramica dei criteri che si è tentato di scaricare e se sono stati o non sono stati scaricati successivamente

<#root>

```
FE2067#
```

show cts authorization entries

```
Authorization Entries Info
==========================
Peer name = Unknown-0
Peer SGT =
```

0-00:Unknown

```
Entry State =
```

COMPLETE

```
Entry last refresh = 22:14:46 UTC Thu Mar 30 2023
SGT policy last refresh = 22:14:46 UTC Thu Mar 30 2023
SGT policy refresh time = 86400
```

```
Policy expires in 0:05:23:44 (dd:hr:mm:sec)
Policy refreshes in 0:05:23:44 (dd:hr:mm:sec)
Retry_timer = not running
Cache data applied = NONE
Entry status =
```

SUCCEEDED

```
AAA Unique-ID = 11

Peer name = Unknown-17
Peer SGT =
```

17-01:Fabric_Client_2

```
Entry State =
```

COMPLETE

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

SUCCEEDED

```
AAA Unique-ID = 4031
```

Se sono stati scaricati dei criteri, è possibile visualizzarli con il comando "show cts criteri basati sui ruoli".

<#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
```

Con questo comando vengono visualizzati tutti i criteri appresi dal dispositivo. Sul server ISE sono potenzialmente presenti più policy per gruppi diversi, ma il dispositivo cerca solo di scaricare le policy per cui conosce gli endpoint. Ciò consente di risparmiare preziose risorse hardware.

Questo comando mostra anche l'azione predefinita da applicare al traffico per cui non è nota un'immissione più specifica. In questo caso, è necessario autorizzare il passaggio di tutto il traffico che non corrisponde a una voce specifica della tabella.

Eseguire show cts rbacl <nome>per ottenere maggiori dettagli sul contenuto esatto del RBACL scaricato

<#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

In questo caso, l'unico traffico che può essere inviato all'endpoint a cui è applicato questo RBACL è il traffico tcp verso il 22 (SSH) e il 23 (Telnet).

Nota: RBACL funziona solo in una direzione. A meno che nel traffico di ritorno non siano presenti criteri, questi vengono applicati con i criteri predefiniti. Il traffico che entra nella struttura non viene imposto, ma viene inviato attraverso la struttura con il tag SGT noto sul

---

nodo in entrata. Viene applicata solo quando lascia l'infrastruttura e deve essere applicata ai criteri presenti in tale dispositivo. In genere, questi criteri sarebbero gli stessi, ma è possibile estendere il dominio CTS, ad esempio con un firewall in cui potrebbero essere stati definiti altri criteri, a seconda dei criteri di sicurezza distribuiti.

Eseguire il comando 'show cts - contatori basati sul ruolo' per verificare se i frame vengono eliminati o meno

- Con questo comando vengono visualizzati i contatori cumulativi per l'intero switch. Non sono disponibili comandi equivalenti per ciascuna interfaccia.

<#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

In questa panoramica vengono mostrate tutte le voci note conosciute dallo switch in questo caso per poter far corrispondere il traffico tra 17 e 16 e tra 16 e 17.

- Qualsiasi altra corrispondenza che rientra nell'intervallo * e ottiene l'azione predefinita applicata, in modo che se arriva un traffico tra 18 e 16, ad esempio, non corrisponda alla matrice nota sullo switch e venga applicata l'azione predefinita.

Anche se i contatori sono cumulativi, danno una buona indicazione se il traffico viene scartato.

- Per determinare il traffico che interesserebbe una voce, è possibile aggiungere la parola chiave log sul server ISE alle rispettive policy, in modo che lo switch invii messaggi log quando questa voce viene trovata.
- Questa operazione può essere eseguita sia per l'azione predefinita (* *) che per una delle voci più specifiche della matrice.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).