

Catalyst 9000系列交換機上的LISP VXLAN交換矩陣故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[LISP VXLAN型光纖](#)

[用於構建LISP VXLAN交換矩陣的技術](#)

[LISP VXLAN交換矩陣中的關鍵元件](#)

[終端註冊](#)

[重要資訊](#)

[註冊步驟](#)

[驗證](#)

[1.1 MAC地址學習](#)

[1.2 動態IP地址學習](#)

[1.3 EID與控制平面的配準](#)

[1.4 控制平面資訊](#)

[解析遠端目標](#)

[2.1 乙太網對映快取](#)

[2.2 IP對映快取](#)

[通過交換矩陣的流量轉發](#)

[3.1 第2層或第3層轉發](#)

[3.2 第2層轉發](#)

[3.3 第3層轉發資訊](#)

[3.4 資料包格式](#)

[驗證和安全實施](#)

[4.1 交換機埠身份驗證](#)

[4.2 流量策略和基於組的策略\(CTS\)](#)

[4.3 CTS環境](#)

[相關資訊](#)

簡介

本檔案介紹基於LISP VXLAN的網狀架構的基本元件以及如何驗證其操作。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Cisco IOS XE 17.9.3或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

LISP VXLAN型光纖

部署LISP VXLAN網路的用途是能夠建立一個架構，其中多個重疊網路（也稱為虛擬網路）定義在底層網路之上。

- 這種拓撲中的底層網路主要充當傳輸層，並不知道在其上運行的重疊拓撲。
- 可以新增和刪除重疊網路，而不會影響底層網路。
- 重疊網路的使用有效地將使用者與底層網路分離。

用於構建LISP VXLAN交換矩陣的技術

定位器身分分離通訊協定(LISP)

- LISP協定是交換矩陣內部使用的控制平面協定。它在所有交換矩陣裝置上運行，以構建交換矩陣和控制流量通過交換矩陣的傳送方式。
- LISP建立2個地址空間。一個是路由定位器(RLOC)，用於通告可達性。另一個地址空間用於終端識別符號(EID)，即終端駐留並用於重疊的終端識別符號。
- 在LISP中，使用通告的RLOC通告EID。如果EID移動了需要執行的所有操作，則將更新與其關聯的工藝路線貨位。
- 要到達具有指向EID的LISP流量的端點，需要將其封裝並隧道連線到RLOC，後者將解封裝它並將其轉發到端點。

基於組的策略

- 為了能夠允許在基於交換矩陣組的策略內進行分段，
- 部署基於組的策略時，流量使用安全組分類，而不是基於源/目標IP。
- 這降低了複雜的訪問控制清單的複雜性。需要維護的IP地址清單不同，IP地址/子網被分配到

安全組標籤。

- 當流量從交換矩陣流出時，進入交換矩陣的入口會使用SGT進行標籤，因此會查詢該幀的目標以查詢其SGT。
- 通過使用矩陣，源和目標SGT匹配，並且應用安全組ACL在流量離開交換矩陣時實施流量。

VXLAN封裝

- 交換矩陣內部VXLAN用於封裝所有流量
- 在傳統LISP封裝上使用VXLAN的優點在於它允許封裝整個第2層幀，而不僅僅是第3層幀。封裝整個幀時，允許重疊為第2層和第3層。
- VXLAN使用目的地連線埠4789的UDP。這允許LISP VXLAN訊框透過不會察覺重疊拓撲的裝置。
- VXLAN封裝整個訊框時，增加MTU非常重要，因此在RLOC之間傳送流量時，不需要分段。任何中間裝置都需要支援更大的MTU來傳輸封裝的幀。

驗證

- 為了能夠將端點分配到其各自的資源，可以使用身份驗證。
- 透過通訊協定802.1x，MAB和Webauth端點可以對Radius伺服器進行驗證和/或分析，並可根據其授權設定檔獲得網路存取許可權。
- 藉助各自的Radius屬性，可將終端分配到各自的VLAN、SGT和任何其他屬性，以提供終端/使用者網路訪問。

LISP VXLAN交換矩陣中的關鍵元件

控制平面節點

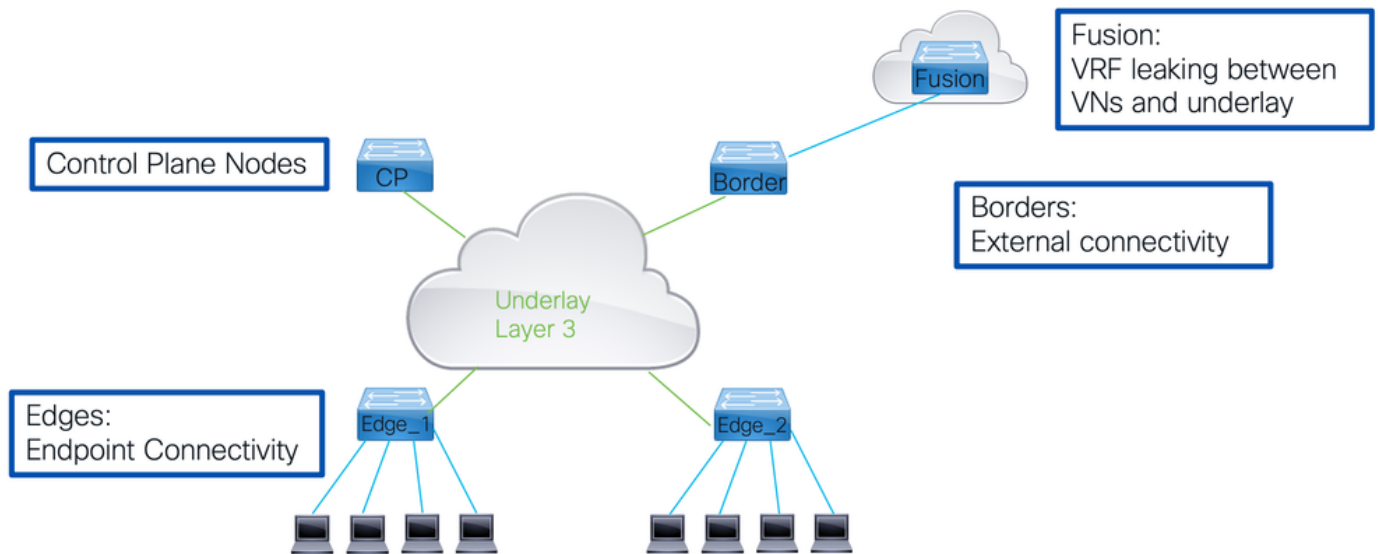
- 具有LISP對映伺服器和對映解析器功能。
- 所有其他交換矩陣裝置查詢控制平面節點的EID位置，並將其EID的註冊傳送到控制平面節點。
- 這會為控制平面節點提供有關各種EID後面的RLOC的交換矩陣的完整檢視。

邊界節點

- 在交換矩陣外部提供到其他交換矩陣或外部世界的連線。
- 內部邊界將路由匯入交換矩陣並向控制平面節點註冊。
- 外部邊界連線到外部世界，並為未知IP目標提供交換矩陣外部的預設路徑。

邊緣節點

- 這些節點提供到交換矩陣內端點的連線。
- 在LISP的定義中，這些是XTR，因為它們將同時執行輸入通道路由器(ITR)和輸出通道路由器(ETR)的功能。



節點不限於只執行一項任務。

- 它們可以在交換矩陣內執行組合甚至所有功能。
- 當邊界節點和控制平面節點駐留在它們稱為並置的裝置上時。
- 如果該節點還提供邊緣功能，則將其稱為機箱中的交換矩陣(FIAB)。

邊界使用VRF lite向網路的其餘部分提供切換。

- 每個重疊或虛擬網路與邊界節點上的VRF例項相關聯。
- 為了將這些不同的VRF連線在一起，使用的是Fusion路由器。該融合路由器不是交換矩陣本身的一部分，但對於將重疊網路連線到交換矩陣的操作至關重要。

LISP VXLAN交換矩陣中的另一個重要概念是使用IP任播的概念。

- 這表示在所有邊緣裝置上都會複製交換虛擬介面(SVI)的IP地址及其MAC地址。
- 在SVI上，每個邊緣的IPv4、IPv6和MAC地址配置相同。
- 對此進行故障排除會帶來一些挑戰。
 - 使用ping測試可達性適用於本地連線的裝置。
 - 要通過LISP VXLAN交換矩陣到達遠端目標，不會返回響應，因為傳送響應的裝置也會將此響應傳送到任意播IP地址，該地址會被傳送到本地交換矩陣裝置，而本地交換矩陣裝置不知道其他交換矩陣節點已傳送原始ping。

終端註冊

要使LISP VXLAN交換矩陣正常工作，控制平面節點必須瞭解所有終端如何通過交換矩陣到達。

- 對於控制平面來說，要瞭解網路中的所有EID，它依賴所有其他交換矩陣裝置將其瞭解的所有EID註冊到控制平面。
- 交換矩陣節點向控制平面節點傳送LISP對映暫存器消息。在隨對映暫存器消息通告的資訊中。

重要資訊

LISP例項識別符號：

- 此識別符號通過交換矩陣傳輸，指示要使用的虛擬網路。
- 在每第3層重疊的LISP VXLAN交換矩陣中，交換矩陣中每個已使用的VLAN使用一個例項，同時也存在第2層例項。

已標識端點(EID):

- 如果這是第2層或第3層例項，則這是MAC地址、IP主機路由 (/32或/128) 或已註冊的IP子網

工藝路線貨位(RLOC):

- 這樣，交換矩陣節點擁有用於通告可達性的IP地址，其他交換矩陣裝置將傳送需要到達EID的封裝流量。

代理標誌：

- 設定此標誌後，它允許控制平面節點直接響應來自其他交換矩陣節點的對映請求，而不使用代理標誌設定所有要轉發到註冊EID的交換矩陣節點的請求。

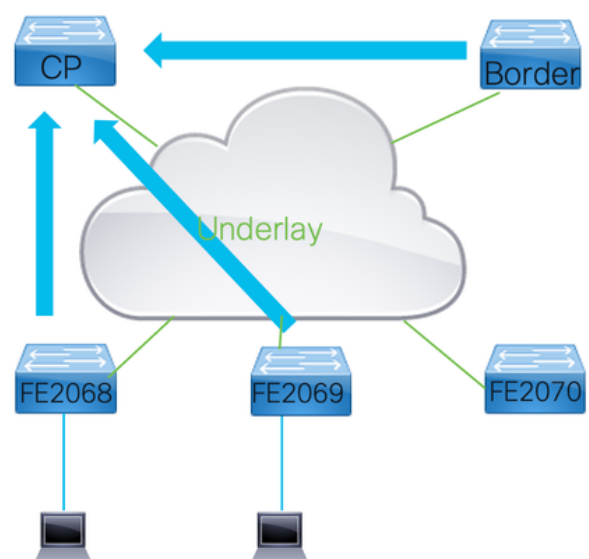
註冊步驟

步驟 1:交換矩陣裝置瞭解終端識別符號。這可以通過配置、路由協定或在交換矩陣裝置上學習而實現。

第2步：交換矩陣裝置向交換矩陣內的每個已知和可達控制平面節點註冊所瞭解的終端。

步驟 3:控制平面節點維護一個註冊的EID表，該EID具有相關的例項ID、RLOC和學習的EID

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



驗證

1.1 MAC地址學習

對於第2層例項，使用的EID是在關聯VLAN內獲取的MAC地址。交換矩陣邊緣通過交換機上的標準方法學習第2層地址。

找到與特定第2層例項ID相關聯的VLAN，您可以檢視配置或命令

使用「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
```

如輸出所示，例項ID 8191與VLAN 150相關聯。這會導致VLAN內的所有MAC地址都向LISP註冊，並成為LISP VXLAN交換矩陣的一部分。

```
<#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

介面VI150的靜態條目是交換機虛擬介面（介面VLAN 150）的MAC地址。

- 這些MAC地址不會註冊到控制平面節點，因為所有邊緣裝置上的這些MAC地址都是相同的。
- 顯示的CP_LEARN條目是通過交換矩陣獲知的條目。對於所有其他動態或靜態條目，它們將註冊到控制平面節點。

一旦通過各自的手段獲知，它們就會出現在lisp資料庫輸出中，此輸出將包含此交換矩陣裝置上的所有本地條目。

<#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
```

對於資料庫中顯示的所有已知本地MAC地址，將顯示定位器。

- 這是用於向控制平面節點註冊此條目的定位器。
- 它還指示了定位器的狀態。還顯示了屬於交換機SVI的2個MAC地址，但顯示時帶有「不註冊」標誌，該標誌阻止這些地址進行註冊。
- 在show mac address table命令中看到的遠端條目不是本地MAC地址，因此不會顯示在lisp資料庫下。

對於第2層例項，不僅要將第2層MAC地址學習為EID，還需要從ARP和ND幀學習地址解析資訊。

- 這樣，LISP VXLAN交換矩陣就能夠轉發這些幀，因為這些幀通常在VLAN中泛洪。
- 由於第2層例項ID並不總是能夠泛洪到另一個機制，該機制允許端點解析同一例項中其他端點的地址解析資訊。為此，交換矩陣裝置學習並註冊通過裝置跟蹤本地獲取的資訊。
- 然後，這也會在控制平面節點中註冊。由於ND或ARP監聽，這些資料包會被傳送到CPU，以觸發對控制平面節點的請求，檢視是否有任何已知MAC地址關聯。
- 如果收到肯定響應，則重新寫入ARP/ND資料包，以便將目的mac地址從廣播或組播更改為單播mac地址。
- 然後，這個重新寫入的資料包可以作為單播幀通過LISP VXLAN交換矩陣轉發。

要檢視交換機上已知的地址解析資訊，可使用命令show device-tracking database。

- 這顯示裝置跟蹤已知的所有對映。
- 交換機自己的IP地址標籤為L(Local)，需要出現在裝置跟蹤資料庫中。

遠端條目也會顯示在此輸出中。

- 在監聽ND或ARP請求後解決這些請求時，它們會被放入鏈路層地址為0000.0000.00fd的裝置跟蹤資料庫中。
- 解析後，資訊會變為解析的mac地址，埠會更改為Tu0。

顯示裝置跟蹤資料庫

<#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 DHCP
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 V1150 150 0100 10
L 2001:DB8::1 0000.0c9f.f18e V1150 150 0100 10
L FE80::200:CFF:FE9F:F18E 0000.0c9f.f18e V1150 150 0100 10

使用「show lisp instance-id <instance> ethernet database address-resolution」命令顯示本地註冊的對映

<#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動態IP地址學習

在IP層上的交換矩陣裝置上，虛擬網路通過將LISP例項ID與VRF相關聯而形成。

- 此VRF接著在各種交換器虛擬介面(SVI)下設定，且成為第3層重疊網路的一部分
- 在大多數情況下，這些SVI也屬於在各自的第2層例項中註冊的VLAN。

使用命令「show lisp instance-id <instance> ipv4」查找VRF和LISP實例ID之間的對映

<#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



附註：此命令還可用於驗證可為此例項啟用的各種功能，以及顯示LISP VXLAN交換矩陣內

使用的控制平面節點

第3層例項建立並連結到VRF後，將建立一個LISP 0 <instance-id>介面，該介面在運行配置中和show vrf下可見。

- 此介面不需要手動建立，通常不需要配置（使用底層組播時組播配置除外）。

```
<#root>
```

```
FE2068#
```

```
show vrf Fabric_VN_1
```

Name	Default RD	Protocols	Interfaces
Fabric_VN_1			

ipv4,ipv6

```
LI0.4099
```

Vl150

Vl151

與乙太網幀不同，VLAN中的所有MAC地址都用於IP，因此需要將IP地址置於要獲知的動態EID範圍內。

顯示LISP例項

```
<#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

在這些定義的範圍之外的IP地址被視為不適合交換矩陣，並且不會放入LISP資料庫並且不會向控制平面節點註冊。

<#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

輸出會顯示所有本地已知IP地址資訊。

- 對於主機來說，這些路由通常是主機路由（/32或/128），但如果這些路由已匯入到基於邊界節點的LISP資料庫中，則它們也可以是子網。
- SVI自身的IP地址標籤為「不註冊」。這樣可以避免所有交換矩陣裝置向控制平面節點註冊任播IP地址。

<#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 EID與控制平面的配準

基於LISP VXLAN的交換矩陣中的終端註冊通過LISP可靠註冊。這意味著所有註冊都通過已建立的TCP會話（即LISP會話）完成。從每個交換矩陣裝置，與交換矩陣中的每個控制平面節點建立LISP會話。通過此LISP會話，所有註冊都會發生。如果交換矩陣中存在多個控制平面節點，則所有節點都將用於註冊EID。

在交換矩陣裝置上沒有任何要註冊的內容時，狀態為關閉，這通常僅在外部邊界上發生不向控制平面節點或在無任何端點的邊緣裝置上註冊任何IP範圍的

EID的註冊通過LISP註冊消息進行傳送到所有已配置的控制平面節點。

要檢視交換矩陣裝置上的LISP會話，可使用命令show lisp session。它會顯示會話的狀態和啟動時間。

```
<#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

顯示為Down的LISP會話可能發生在沒有任何EID以向控制平面節點註冊的裝置上。通常是指邊界節點，這些節點不會將路由匯入交換矩陣或邊緣裝置，並且沒有任何端點連線。

使用「show lisp session vrf default <ip address>」命令顯示有關LISP會話的更多詳細資訊

```
<#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 1isp 0 IID 4099 AFI IPv4 2/1    Established
Pubsub subscriber 1isp 0 IID 4099 AFI IPv6 1/0    Idle
Pubsub subscriber 1isp 0 IID 8191 AFI MAC 2/0    Idle
Pubsub subscriber 1isp 0 IID 8192 AFI MAC 0/0    Idle

```

ETR Reliable Registration 1isp 0 IID 4099 AFI IPv4

6/5 TCP

ETR Reliable Registration 1isp 0 IID 4099 AFI IPv6

1/3 TCP

ETR Reliable Registration 1isp 0 IID 8191 AFI MAC

9769/6517 TCP

ETR Reliable Registration 1isp 0 IID 8192 AFI MAC

2/6 TCP

```

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

```

會話的此詳細輸出顯示哪些例項處於活動狀態且具有EID，這些例項已在控制平面節點中註冊。

<#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	

當您檢視「控制平面」節點上的會話數時，通常會顯示更多處於Up狀態的會話。

- 如果這是並置的Border/CP節點，則也會針對自身建立LISP會話。
- 在本例中，存在從172.30.250.19:4342到172.30.250.19:10的會49270。
- 通過此會話，邊界元件向控制平面節點註冊其EID。

1.4控制平面資訊

利用交換矩陣裝置通過註冊提供的資訊，控制平面節點能夠構建交換矩陣的完整檢視。每個Instance-id維護一個包含已獲取的EID及其關聯路由定位器的表。

使用show lisp site命令為第3層例項顯示

```
<#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 Register	Up	Who Last Registered	Inst ID	EID Prefix
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

```
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
```

此命令顯示所有註冊的EID和最後註冊EID的EID。必須注意是，這通常也是正在使用的RLOC，但是這可能不同。此外，EID還可以註冊到多個RLOC。

要顯示完整詳細資訊，命令包括EID和例項

```
<#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



附註：在詳細輸出中，需要注意以下幾點：

- Proxy，使用此設定，控制平面節點將直接響應對映請求。在傳統LISP中，對映請求

被轉發到註冊EID但使用Proxy設定的XTR，控制平面節點會直接響應

- TTL，這是EID註冊的生存時間。預設情況下為24小時
- ETR資訊，與已傳送EID註冊的交換矩陣裝置相關
- RLOC資訊，這是用於到達EID的RLOC。這也包含狀態資訊，如開啟/關閉。如果RLOC關閉，則不會使用它。它還包含權重和優先順序，當存在多個RLOC時，可以使用這些RLOC來使EID優先使用其中一個。

若要檢視「控制平面」節點上的註冊歷史記錄，可以使用show lisp server registration history命令。

- 其中概述了已註冊和取消註冊的EID。

顯示註冊歷史記錄

<#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

顯示已註冊的乙太網EID，命令為show lisp instance-id <instance> ethernet server (此命令提供類似第3層的輸出)

<#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 Register	Up	Who Last Registered	Inst ID	EID Prefix
site_uci	never	no	--	8191	any-mac

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

附加MAC地址以獲取有關註冊的更多詳細資訊

<#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
----	-------	------	------

附加「註冊歷史記錄」以檢視乙太網EID的註冊歷史記錄



附註：當裝置在交換矩陣中漫遊以檢視MAC地址註冊的位置和時間時，此命令非常有用

<#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

```

要檢視控制平面節點上已註冊的地址解析資訊，該命令附加了地址解析。

- 這僅顯示MAC地址與其第3層資訊之間的對映，主要用於交換矩陣邊緣將第2層目標MAC地址從廣播/組播重寫為單播。
- 對應於該第2層MAC地址的RLOC將單獨解析。

附加「address-resolution」以檢視控制平面節點上的註冊地址解析資訊

```
<#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

```



附註：即使鏈路本地IPv6地址與IPv6動態EID不匹配，也要學習它們進行地址解析，並且會顯示在控制平面節點上。這些裝置本身不會在第3層例項ID下註冊，但可用於地址解析。

解析遠端目標

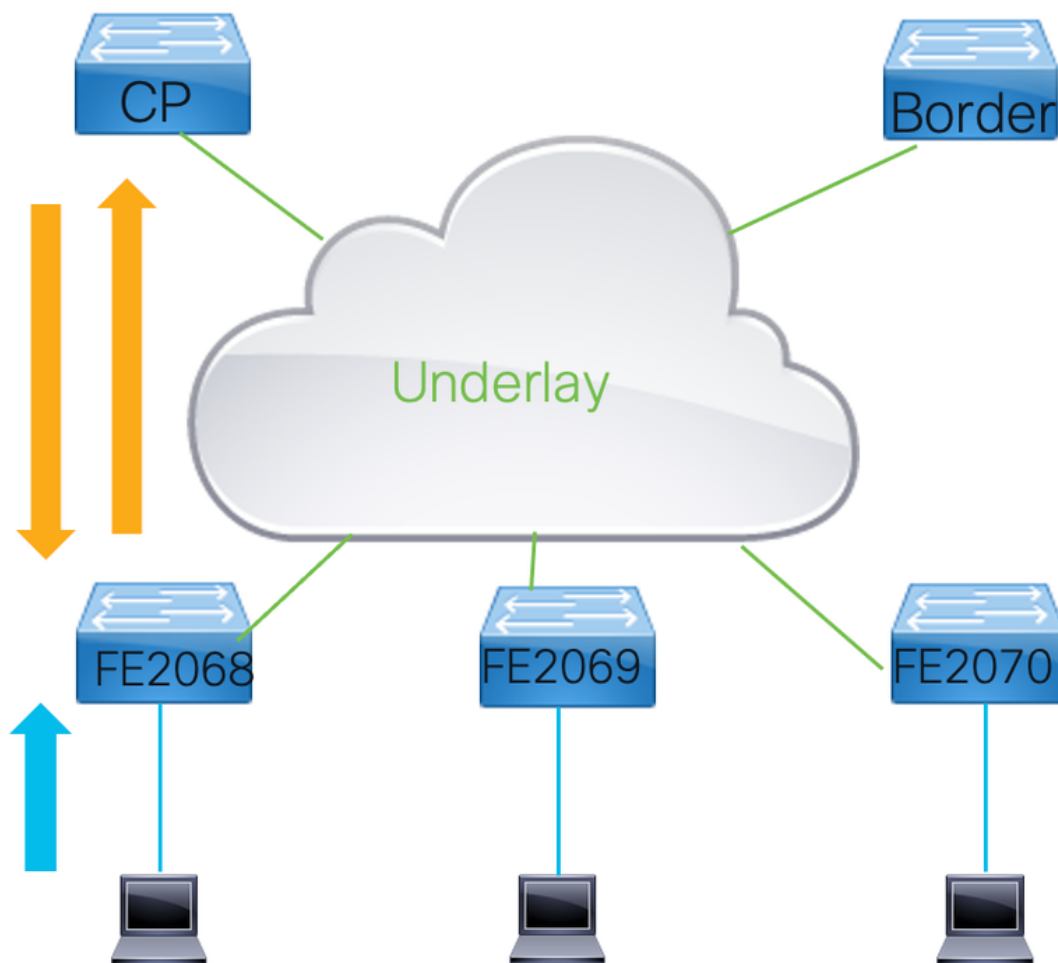
對於要通過LISP VXLAN交換矩陣轉發的流量，需要解析目的地的RLOC。在LISP VXLAN交換矩陣內，這通過使用對映快取來完成，資訊從對映快取被放入交換矩陣裝置的轉發資訊庫(FIB)。

使用LISP VXLAN交換矩陣時，對映快取將由於資料訊號而被觸發。

- 這意味著將流量轉發到CPU，並且CPU建立指向控制平面節點的對映請求，以查詢需要向該EID傳送哪些幀的RLOC資訊。
- 當控制計畫收到對映請求時，它將提供與此EID關聯的路由定位器資訊，或者傳送回負對映回覆。
- 當它傳送一個否定對映回覆時，控制平面節點不僅會指示所請求的EID未知，還會提供該EID將屬於的整個EID塊（它將沒有任何註冊）。

使用來自控制平面節點的map-reply內的資訊更新對映快取。

- 對映回覆的TTL通常為24小時。（對於負對映回覆，通常只有15分鐘）。
- 對於乙太網EID，負對映回覆不會放入對映快取。（這僅適用於第3層例項）。



2.1 乙太網對映快取

使用show lisp instance-id <instance> map-cache命令顯示乙太網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	-	
----------	----	-------	---	--

此命令顯示應已解析的遠端MAC地址條目。

- 要觸發乙太網例項流量的對映快取條目，需要將流量傳送到未知目標。
- 這會導致交換矩陣裝置嘗試通過LISP解析它。
- 一旦通過對映回覆獲知，該路由將被放入對映快取中，隨後發往該第2層目的地的幀將直接傳送到獲知的路由定位器。

在第2層例項中，可選的是BUM流量泛洪的使用。

- 預設情況下，LISP/VXLAN不會泛洪流量，因為它使用重疊技術，但可以在底層網路(GRT)中設定IP多點傳送群組，透過此網路可以泛洪第2層訊框。

顯示廣播底層組地址

```
<#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 IP對映快取

對於第3層例項，對映快取資訊與傳送到CPU的流量生成的乙太網類似，該流量發出訊號會導致傳送對映請求。

- 但是，對於第3層資料包，在設定該資料包時，僅會被傳送到CPU以發出訊號。這通過配置的map-cache命令來完成。對於IPv4，這是0.0.0.0/0，對於IPv6，這是::0/0。
- 在邊界節點上配置此對映快取條目必須小心。如果邊界節點配置了此map-cache 0.0.0.0/0或::0/0對映快取條目，則它會嘗試通過交換矩陣解析未知目標，而不是將其路由到交換矩陣之外。

顯示對映快取配置

```
<#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

```

map-cache 0.0.0.0/0和 : :/0 map-request導致使用「send-map-request」操作在對映快取中配置對映快取條目。命中此的流量會觸發對映請求。由於對映快取條目將被放入基於最長匹配的FIB中，這會應用到所有未命中任何更具體條目的路由IP流量。

- 在支援的平台上，為了避免第一個封包被捨棄，顯示的操作是send-map-request + encapsulate to proxy ETR。
這會導致第一個傳送到未知目的地的資料包觸發對映請求，並且如果存在則將該資料包轉發到 proxy-etr。

```
<#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

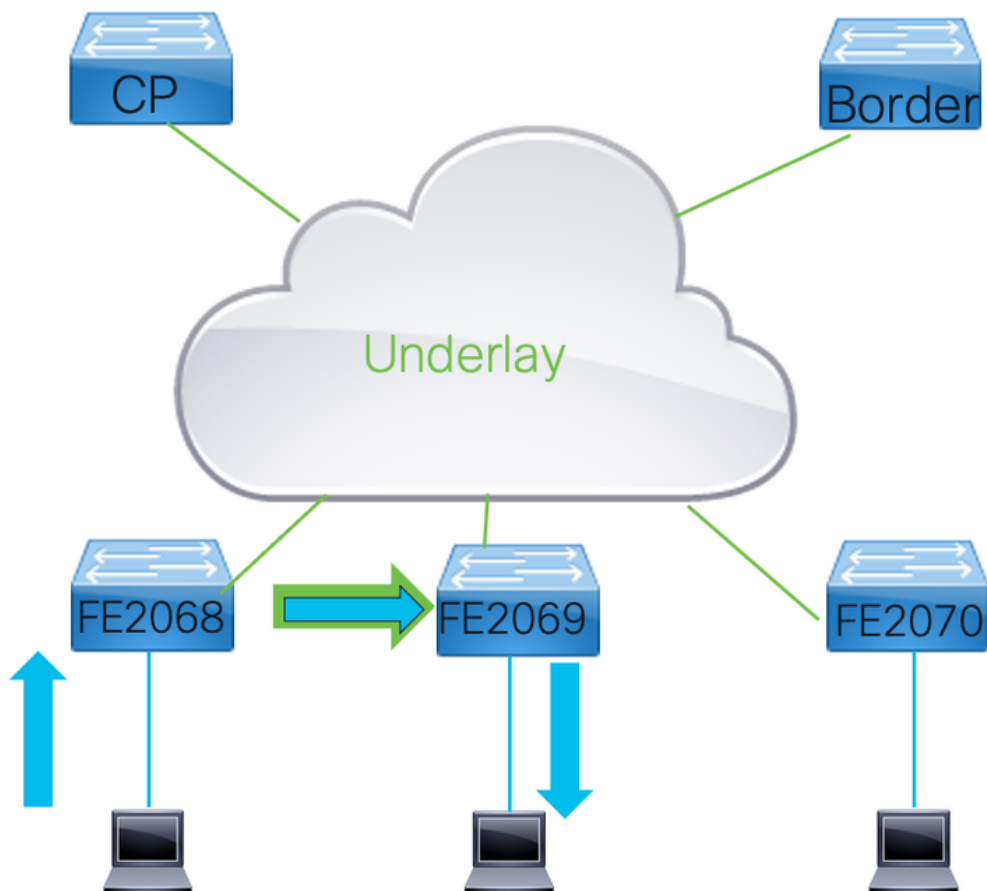
172.30.250.19

22:28:19 up 10/10 - 0

在此輸出中顯示了幾個條目。

- 此輸出中的10.48.13.0/24和172.24.2.2/32通過對映應答獲知並完成。到達這些目的地的流量將被封裝並轉發到各自的定位器。
- 172.28.0.0/14是已收到負對映回覆和已返回IP地址塊的示例。只要此條目位於對映快取中，流向此子網的流量就不會觸發對映請求。

通過交換矩陣的流量轉發



3.1第2層或第3層轉發

LISP/VXLAN交換矩陣中的流量可通過第2層或第2層例項轉發。

- 確定使用哪個例項取決於幀的目的MAC地址。
- 傳送到除在交換機上註冊的MAC地址以外的任何MAC地址的幀將使用第2層。如果資料包的目的地是交換機，則通過第3層轉發該幀。
- 此邏輯與通過Catalyst 9000系列交換器的正常轉送相同。

3.2第2層轉發

通過LISP VXLAN交換矩陣的第2層轉發基於第2層目標MAC地址完成。遠端目標將插入具有輸出介面L2LI0的MAC地址表中。

顯示本地和遠端第2層介面

```
<#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
```

對於未知目的地（如果已設定），流量會透過底層中設定的IP多點傳送群組傳送。

- 為了確保廣播、未知單播和組播（僅限選擇性組播泛洪）流量的正確泛洪，需要在底層中有一個正確運行的組播環境。
- 透過此多點傳送底層群組傳送的流量將封裝在VXLAN中。
- 所有其他邊緣必須加入組播組，接收流量並解除封裝已知第2層例項的流量。

顯示底層IP組播組

```
<#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:

此輸出顯示交換矩陣中配置客戶端傳送泛洪流量的所有其他Edge的S、G條目。它還顯示一個S、G條目，其中此邊緣裝置的Loopback0作為源。

對於通過底層組播組的流量的接收端，show ip mroute命令還會顯示L2LISP0。<instance>這將指示此邊緣裝置將對哪些第2層例項解除封裝泛洪流量並將其轉發到相關介面。

3.3第3層轉發資訊

要確定在部署LISP VXLAN交換矩陣時如何轉發流量，請務必驗證CEF。

- LISP不同於傳統路由協定，它不會在路由表中插入路由方向，而是直接與CEF互動以更新FIB。

對於給定的遠端目標，對映快取資訊包含要使用的定位器資訊。

顯示貨位資訊

```
<#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)
```

從對映快取中，用於此EID的定位符為172.30.250.44。因此，將封裝流向此目標的流量，並且外部IP報頭的IP目標地址為172.30.250.44。

在用於此例項的VRF的路由表中，不顯示此條目。

```
<#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 2
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
```

CEF輸出提供了有關通過LISP VXLAN交換矩陣的轉發的詳細資訊。

- 當新增show ip cef命令的detail關鍵字時，它並不只是為要傳送的封裝幀指定目標。
- 具有此輸出的輸出介面是LISP 0。<instance>表示流量已傳送並封裝。

<#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

由於流量將封裝到下一躍點，因此下一步是運行show ip cef <next hop>來檢視資料包也將路由到的輸出介面。

運行以檢視輸出介面

```
<#root>
```

```
FE2067#
```

```
sh ip cef 172.30.250.44
```

```
172.30.250.44/32
```

```
nexthop 172.30.250.38 GigabitEthernet1/0/23
```



附註：可以有2個不同級別的等價多路徑(ECMP)路由。

- 如果存在2個通告的RLOC，流量可以在重疊中進行負載均衡；如果存在到達RLOC IP地址的冗餘路徑，則可以在底層網路中實現負載均衡。
- 由於UDP目的地埠固定為4789，且兩個交換矩陣裝置之間所有流的源和目標IP地址相同，因此需要採用某種形式的抗極化機制，以避免所有資料包通過同一路徑路由。
- 使用LISP VXLAN時，這是外部報頭中的UDP源埠，對於溢位網路中的不同流來說，該埠是不同的。

3.4資料包格式

- 在LISP VXLAN網狀架構中，所有流量均完全封裝在VXLAN中。這包括整個第2層幀，以便同時支援第2層和第3層重疊。

對於第2層幀，將封裝原始報頭。對於通過第3層例項傳送的幀，使用虛擬第2層報頭。

```
<#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
```

從通過LISP VXLAN交換矩陣傳輸的幀捕獲示例中可看出，vxlan資料包中有完全封裝的幀。作為第3層幀，乙太網報頭是一個虛擬報頭。

在VXLAN報頭中，「VLAN網路識別符號」(VLAN Network Identifier)欄位包含幀所屬的LISP例項ID。

- 通過Group Policy ID欄位攜帶幀SGT標籤。
- 在交換矩陣中的入口上設定該值，並將其傳遞到交換矩陣，直到完成基於組的策略實施。

驗證和安全實施

4.1 交換機埠身份驗證

要將終端動態分配到各自的VLAN並為其分配SGT標籤身份驗證，可使用。

- Dot1x/MAB/central webauth等驗證通訊協定可以部署在Radius伺服器上，用於驗證和授權使用者與端點，該伺服器會將屬性傳回交換器，以便允許網路存取正確池中的使用者端/端點，並使用正確網路存取授權。

對於LISP VXLAN交換矩陣，有幾種常見的radius屬性：

- Vlan分配：從radius伺服器到交換機（終端可分配給特定第2層/第3層LISP例項）的此屬性設定為VLAN ID或名稱。
- SGT值：此屬性設定SGT向此SGT分配端點。這將用於針對此終端的基於組的策略，並向通過此終端發起的結構傳送的所有幀分配SGT值。
- 語音授權：語音裝置在語音vlan上運行。此設定允許終端在埠上配置的語音vlan中傳送和接收流量的語音授權。這樣可分隔各自VLAN中的語音和資料流量
- 會話超時：各個端點具有各自的作業階段逾時。可以從radius伺服器傳送逾時，以表示使用者端需要重新驗證身份的頻率
- 模板：對於某些端點，需要在埠上應用不同的模板才能正常運行。 可以從Radius伺服器傳送模板名稱，該模板名稱指示需要應用於埠的內容

使用show access-session命令檢查埠上的身份驗證結果

```
<#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

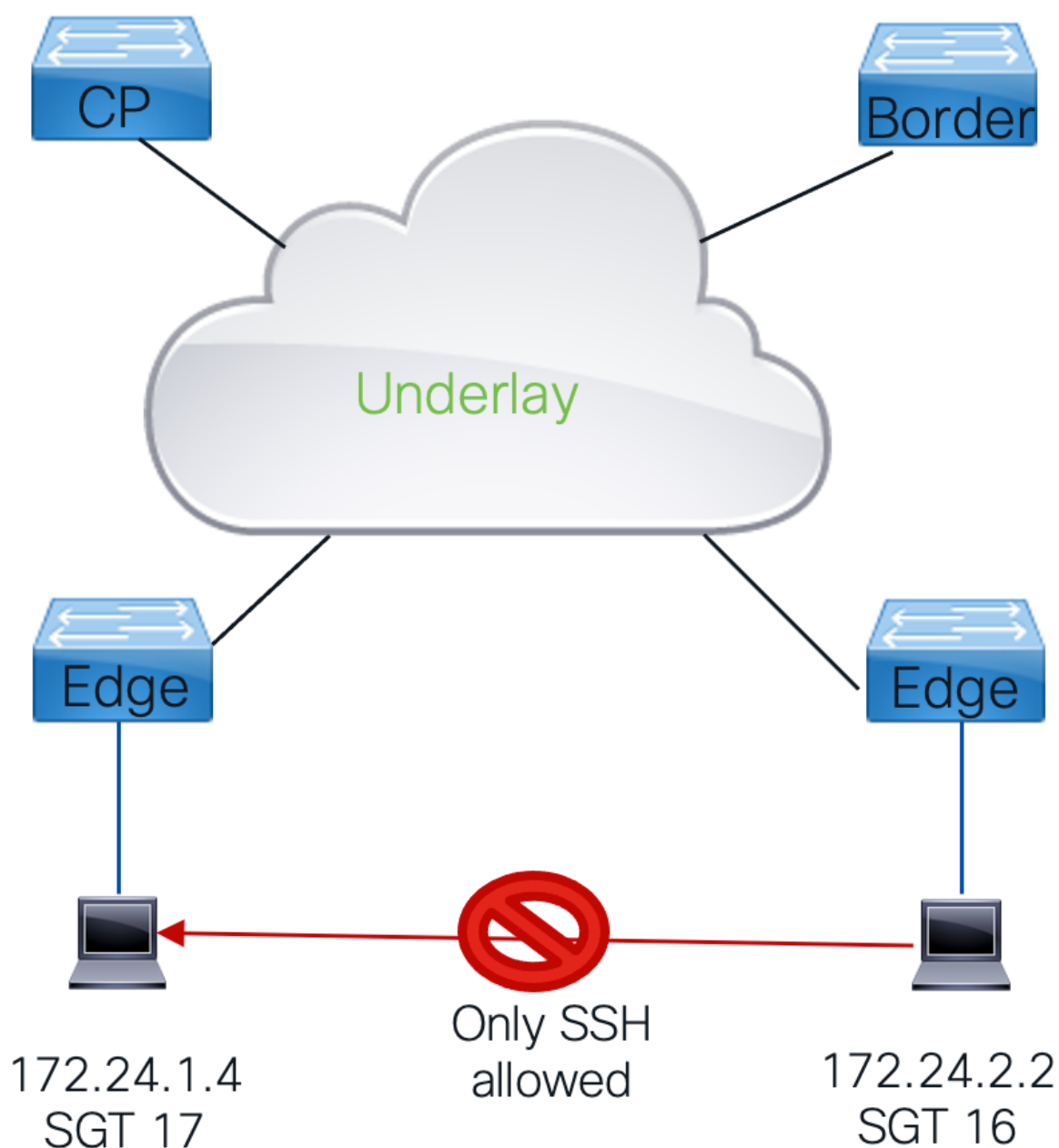
Success

請注意以下關鍵欄位：

- IPv4和IPv6地址：通常通過裝置跟蹤學習。
- 使用者名稱:這是用於身份驗證的使用者名稱。
 - 對於Dot1x，這通常是進行身份驗證的使用者。
 - 使用MAB時，這是將傳送到Radius作為使用者名稱和密碼以進行驗證的工作站的MAC位址。
- 狀態:這表示身份驗證的狀態和身份驗證結果。
- 域：對於正常端點，此域將是Data域，因此流量將在埠上無標籤傳送/接收。（對於語音裝置，可將其設定為「語音」）

- 伺服器策略：這是來自Radius伺服器的資訊（例如Vlan分配和SGT分配）的位置
- 方法狀態清單：此處顯示運行的方法的概述。
 - 標準dot1x在MAB之前運行。
 - 如果端點不響應EAPOL幀，該方法將故障轉移至mab。
 - 這將顯示dot1x已失敗。
 - MAB顯示authc success表示它已成功進行身份驗證，它並不反映身份驗證結果是訪問接受還是拒絕。

4.2流量策略和基於組的策略(CTS)



在LISP VXLAN交換矩陣內，CTS用於實施流量策略：

- 基於組的策略架構基於安全組標籤。
- 交換矩陣內的所有流量都分配在入口和SGT標籤上，該標籤在每個幀中通過交換矩陣傳輸。
- 當此流量離開交換矩陣時，將強制實施流量策略。
- 此操作在基於組的策略中完成，該策略根據由源 — 目標SGT組成的矩陣檢查資料包的源和目標組標籤，其中結果是一個定義允許或不允許哪些流量的SGACL。
- 當矩陣內沒有源 — 目標SGT的特定匹配項時，將應用定義的預設操作。

4.3 CTS環境

要使用基於組的策略運行，交換矩陣裝置首先需要獲取CTS封裝。

- 此PAC將用於RADIUS幀內部，以授權思科ISE上的RADIUS幀。這用於設定Radius幀中的cts-pac-opaque欄位。

顯示CTS pac資訊

```
<#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
```

確保CTS pac已配置且有效很重要。Fabric裝置會自動刷新該值。



附註：要手動觸發刷新，可以發出命令「cts refresh pac」。

要運行基於組的策略，請下載環境資料並下載所需的策略資訊。

- 此環境資料包含交換機本身使用的CTS標籤，以及下載Radius伺服器上已知的所有基於組的策略組的表。

顯示cts環境資料

<#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
```

使用基於組的策略時，僅下載的策略是裝置具有需要強制使用的本地終端的CTS標籤。

- 為了能夠檢查從IP地址（或子網）到基於組的策略組的對映，可以使用命令「show cts role-based sgt-map vrf <vrf> all」。

顯示VRF的所有已知IP到SGT資訊

```
<#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
```

此輸出顯示了給定VRF的所有已知IP地址（和子網）及其基於組的策略關聯。

- 可以看到，一個端點的一個IP地址被分配了基於組的策略組17並且來源為本地。
- 這是發生在埠上的身份驗證結果，其中結果表明標籤與該端點關聯。
- 還重點介紹交換機自己的IP地址，這些地址分配有device-sgt tag作為內部源標籤。
- 也可以通過配置或通過SXP會話向ISE分配基於組的策略標籤。

當裝置得知SGT標籤時，它會嘗試從ISE伺服器下載與其關聯的策略。

- show cts authorization entications命令概述了嘗試下載這些項的時間以及它們是否已連續下載。



附註：如果策略發生任何更改，將定期刷新策略。ISE還可以推送CoA命令以觸發交換機，以便在更改時下載新策略。要手動刷新策略，請發出命令「cts refresh policy」。

顯示嘗試下載的策略的概述，以及是否已連續下載

<#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 =

SUCCEDED

AAA Unique-ID = 4031

如果下載了任何策略，則可以使用命令「show cts rolebased policies」顯示這些策略。

<#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

此命令顯示裝置已學習的所有策略。在ISE伺服器上，可能有更多策略用於不同的組，但裝置只嘗試下載它知道終端使用的策略。這節省了寶貴的硬體資源。

此命令還顯示要應用於沒有特定條目已知的流量的預設操作。在本例中是Permit IP，因此所有與表中特定條目不匹配的流量都允許通過。

執行show cts rbac <name>，以取得已下載RBACL的確切內容的詳細資訊

```
<#root>
```

```
FE2067#
```

```
sh cts rbac1 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
```

在此案例中，唯一允許傳送至應用了此RBACL的終結點的流量是面向22(SSH)和23(Telnet)的tcp資料包。



附註：RBACL只能在一個方向上運行。除非返回流量中有策略，否則將使用預設策略強制執行該策略。進入交換矩陣的流量未強制執行，它通過交換矩陣傳送輸入節點上已知的SGT標籤。僅當它離開交換矩陣並且要在該裝置上存在的策略上實施時，才會實施該策略。通常，這些策略是相同的，但可以擴展CTS域，例如，使用防火牆，在該防火牆中可以定義其他策略，具體取決於部署的安全策略。

運行show cts role-based counters以驗證幀是否已丟棄

- 此命令顯示整個交換機的累積計數器。每個介面沒有對應的命令。

```
<#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						

此概述顯示了此案例中交換機知道的所有已知條目，這些條目能夠匹配從17到16以及從16到17的流量。

- 任何屬於* *範圍的其他匹配項都會應用預設操作，因此，如果任何流量（例如18到16）與交換機上的已知矩陣不匹配，則應用預設操作。

即使計數器是累積的，它們也會給出流量是否被丟棄的正確指示。

- 要確定哪個流量會命中條目，可以在ISE伺服器上將log關鍵字新增到各自的策略中，這會導致交換機在命中該條目時提供日誌消息。
- 可以對預設操作(* *)或矩陣中某個更具體的條目執行此操作。

相關資訊

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。