Catalyst 9000系列交换机上的LISP VXLAN交换矩阵故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 基于LISP VXLAN的交换矩阵
  - 用于构建LISP VXLAN交换矩阵的技术
  - LISP VXLAN交换矩阵中的关键组件
- 终端注册
  - 重要信息
  - 注册步骤

验证

- 1.1 MAC地址学习
- 1.2动态IP地址学习
- 1.3 EID与控制平面的配准
- 1.4控制平面信息

解析远程目标

- 2.1以太网映射缓存
- 2.2 IP映射缓存

通过交换矩阵的流量转发

- 3.1第2层或第3层转发
- 3.2第2层转发
- 3.3第3层转发信息
- 3.4数据包格式

身份验证和安全实施

- 4.1交换机端口身份验证
- 4.2流量策略和基于组的策略(CTS)
- 4.3 CTS环境

相关信息

简介

本文档介绍基于LISP VXLAN的交换矩阵的基本组件以及如何验证其操作。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

基于LISP VXLAN的交换矩阵

部署LISP VXLAN网络的目的是能够创建一个架构，在该架构中，多个重叠网络（也称为虚拟网络）在底层网络之上定义。

- 此类拓扑中的底层网络主要充当传输层，并不知道其上运行的重叠拓扑。
- 可以添加和删除重叠网络，而不会影响底层网络。
- 重叠网络的使用有效地将用户与底层网络隔离开来。

用于构建LISP VXLAN交换矩阵的技术

定位器身份分离协议(LISP)

- LISP协议是交换矩阵内使用的控制平面协议。它在所有交换矩阵设备上运行，以构建交换矩阵和控制流量通过交换矩阵的发送方式。
- LISP创建2个地址空间。一个用于路由定位器(RLOC)，用于通告可达性。另一个地址空间用于终端标识符(EID)，即终端驻留并用于重叠的终端标识符。
- 在LISP中，使用通告的RLOC通告EID。 如果EID移动了需要执行的所有操作，则更新与其关联的工艺路线货位。
- 要到达具有指向EID的LISP流量的终端，需要封装该终端并通过tunneled指向RLOC，RLOC会解封该终端并将其转发到终端。

基于组的策略

- 为了能够在基于交换矩阵组的策略内实现分段，我们使用了策略。
- 部署基于组的策略时，流量使用安全组进行分类，而不是根据源/目标IP进行分类。
- 这降低了复杂的访问控制列表的复杂性。IP地址/子网被分配给安全组标记，而不是需要维护

的IP地址列表。
- 当流量从交换矩阵流出时，进入交换矩阵的入口会被标记为SGT，帧的目标会被查找其SGT。
- 通过使用矩阵，源和目标SGT匹配，并且应用安全组ACL在流量离开交换矩阵时实施流量。

VXLAN封装

- 交换矩阵内部VXLAN用于封装所有流量
- 在传统LISP封装上使用VXLAN的优点是它允许封装整个第2层帧，而不仅仅是第3层帧。当封装整个帧时，它允许重叠为第2层和第3层。
- VXLAN使用目标端口4789的UDP。这允许LISP VXLAN帧通过不会察觉重叠拓扑的设备进行传输。
- 当VXLAN封装整个帧时，增加MTU非常重要，因此在RLOC之间发送流量时不需要分段。任何中间设备都需要支持更大的MTU来传输封装的帧。

身份验证

- 为了能够将端点分配到其各自的资源，可以使用身份验证。
- 使用作为802.1x的协议，可以对Radius服务器对MAB和Webauth终端进行身份验证和/或分析，并根据其授权配置文件授予网络访问权限。
- 通过各自的Radius属性，可将终端分配到各自的VLAN、SGT和任何其他属性，以提供终端/用户网络访问。

LISP VXLAN交换矩阵中的关键组件

控制平面节点

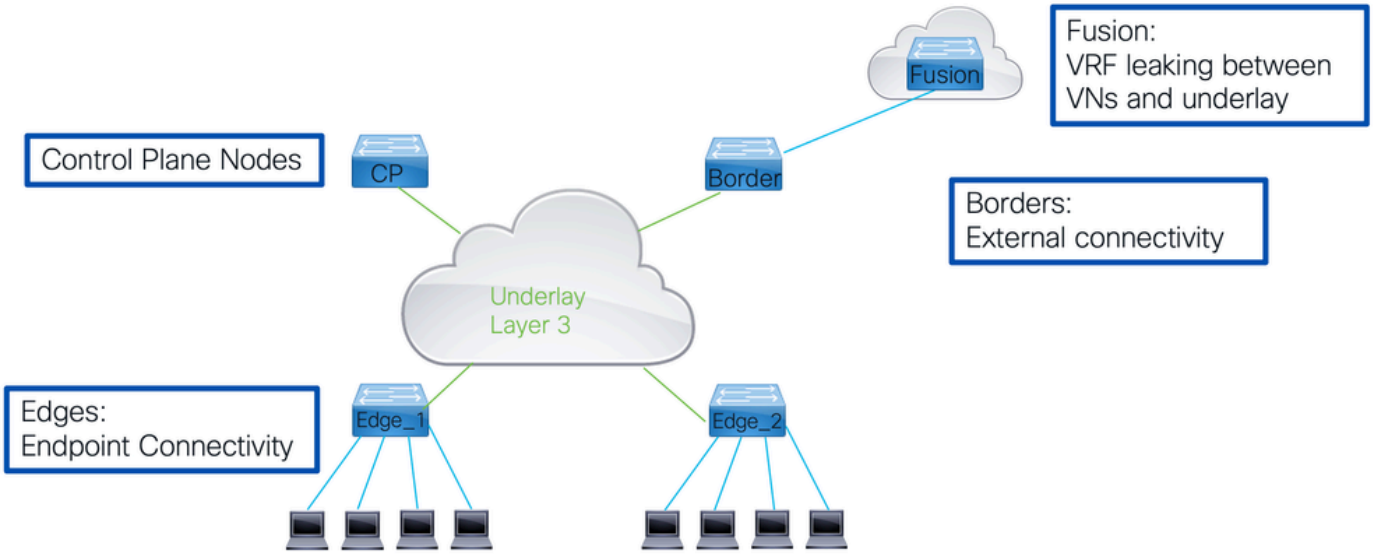
- 具有LISP映射服务器和映射解析器功能。
- 所有其他交换矩阵设备在控制平面节点查询EID的位置，并将其EID注册发送到控制平面节点。
- 这样，控制平面节点就能够完整地了解各种EID位于哪个RLOC后面的交换矩阵。

边界节点

- 提供交换矩阵外部到其他交换矩阵或外部世界的连接。
- 内部边界将路由导入交换矩阵并向控制平面节点注册路由。
- 外部边界连接到外部世界，并为未知IP目标提供交换矩阵外部的默认路径。

边缘节点

- 这些节点提供到交换矩阵内部端点的连接。
- 在LISP的定义中，这些是XTR，因为它们将同时执行入口隧道路由器(ITR)和出口隧道路由器(ETR)的功能。



节点不仅限于执行一项任务。

- 它们可以在交换矩阵内执行组合或甚至所有功能。
- 当边界节点和控制平面节点驻留在它们称为共置的一台设备上时。
- 如果该节点还提供边缘功能，则将其称为一体化交换矩阵(FIAB)。

边界使用VRF lite向网络的其余部分提供切换。

- 每个重叠或虚拟网络与边界节点上的VRF实例相关联。
- 要将各种VRF连接在一起，需要使用Fusion路由器。该融合路由器不是交换矩阵本身的一部分，但对于将重叠网络连接到交换矩阵的操作至关重要。

LISP VXLAN交换矩阵中的另一个重要概念是使用IP任播的概念。

- 这意味着在所有边缘设备上复制交换虚拟接口(SVI)的IP地址及其MAC地址。
- 在SVI上，每个边缘对于IPv4、IPv6和MAC地址具有相同的配置。
- 对此进行故障排除会带来一些挑战。
    - 使用ping测试可达性适用于本地连接的设备。
    - 要通过LISP VXLAN交换矩阵到达远程目标，不会返回响应，因为发送响应的设备也会将此响应发送到任意播IP地址，该地址会被传送给本地交换矩阵设备，而本地交换矩阵设备不知道其他交换矩阵节点已发送原始ping。

终端注册

要使LISP VXLAN交换矩阵正常工作，控制平面节点必须知道如何通过交换矩阵到达所有终端。

- 对于要了解网络中所有EID的控制平面，它依赖所有其他交换矩阵设备将其了解的所有EID注册到控制平面。
- 交换矩阵节点将LISP映射注册消息发送到控制平面节点。在映射寄存器消息通告的信息中。

重要信息

LISP实例标识符：

- 此标识符通过交换矩阵传输，并指示要使用的虚拟网络。
- 在第3层重叠的LISP VXLAN交换矩阵中，交换矩阵中每个已使用的VLAN使用一个实例，同时还有第2层实例。

已识别终端(EID):

- 如果这是第2层或第3层实例，则这是MAC地址、IP主机路由（/32或/128）或已注册的IP子网

工艺路线货位(RLOC):

- 交换矩阵节点拥有的IP地址用于通告可达性，其他交换矩阵设备将发送需要到达EID的封装流量。

代理标志：

- 设置此标志后，它允许控制平面节点直接响应来自其他交换矩阵节点的映射请求，而不使用代理标志设置要转发到注册EID的交换矩阵节点的所有请求。

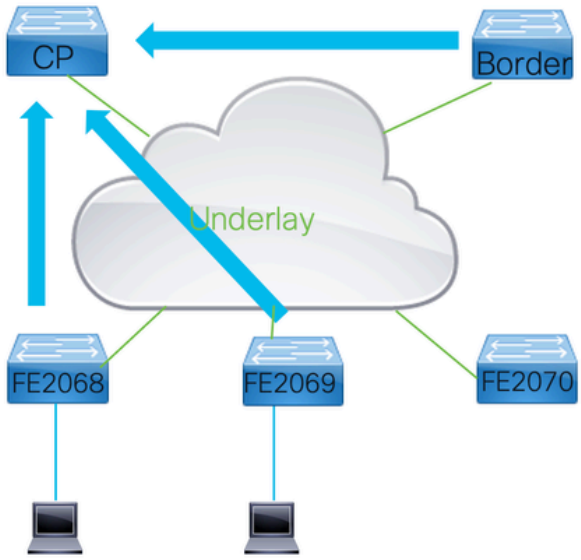
注册步骤

步骤 1：交换矩阵设备了解终端标识符。这可以通过配置、路由协议或在交换矩阵设备上学习实现。

第2步：交换矩阵设备向交换矩阵内的每个已知和可到达的控制平面节点注册所了解的终端。

步骤 3：控制平面节点维护一个注册的EID表，该EID具有相关的实例ID、RLOC和学习到的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



验证

1.1 MAC地址学习

对于第2层实例，使用的EID是在关联VLAN内获取的MAC地址。交换矩阵边缘通过交换机上的标准方法学习第2层地址。

找到与特定第2层实例ID相关联的VLAN，您可以查看配置或命令

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
```

如输出所示，实例ID 8191与VLAN 150关联。这会导致VLAN内的所有MAC地址都向LISP注册，并成为LISP VXLAN交换矩阵的一部分。

<#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
```

接口Vl150的静态条目是交换机虚拟接口（接口vlan 150）的MAC地址。

- 这些MAC地址不会注册到控制平面节点，因为所有边缘设备上的这些MAC地址都相同。
- 显示的CP_LEARN条目是通过交换矩阵获知的条目。对于所有其他动态或静态条目，它们将注册到控制平面节点。

一旦通过各自的手段获知，它们就会出现在lisp数据库输出中，此输出将包含此交换矩阵设备上的所有本地条目。

```
<#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
```

对于数据库中显示的所有已知本地MAC地址，将显示定位器。

- 这是用于向控制平面节点注册此条目的定位器。
- 它还指示了定位器的状态。也会显示属于交换机SVI的2个MAC地址，但会显示“不注册”标记，以防止它们被注册。
- 在show mac address table命令中看到的远程条目不是本地MAC地址，因此不会显示在lisp数据库下。

对于第2层实例，不仅需要将第2层MAC地址学习为EID，还需要从ARP和ND帧学习地址解析信息。

- 这样LISP VXLAN交换矩阵才能转发这些帧，因为它们通常在VLAN内泛洪。
- 由于第2层实例ID并不总是能够泛洪到另一个机制，该机制允许终端解析同一实例中其他终端的地址解析信息。为此，交换矩阵设备将学习并注册通过设备跟踪本地获取的信息。
- 然后，这也会向控制平面节点注册。由于ND或ARP监听，这些数据包被传送到CPU，以触发对控制平面节点的请求，查看是否有任何已知MAC地址关联。
- 如果收到肯定响应，则会重写ARP/ND数据包，以便将目的mac地址从广播或组播更改为单播mac地址。
- 然后，此重写的数据包可以作为单播帧通过LISP VXLAN交换矩阵转发。

要查看交换机上已知的地址解析信息，可使用命令show device-tracking database。

- 这确实显示设备跟踪已知的所有映射。
- 交换机自己的IP地址标记为L（本地），需要存在于设备跟踪数据库中。

远程条目也会显示在此输出中。

- 在监听ND或ARP请求后解决这些问题后，它们会被放入链路层地址为0000.0000.00fd的设备跟踪数据库中。
- 解析后，信息会更改为解析的mac地址，端口会更改为Tu0。

显示设备跟踪数据库

<#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
```

使用命令“show lisp instance-id <instance> ethernet database address-resolution”显示本地注册的映射

<#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动态IP地址学习

在IP层上的交换矩阵设备上，通过将LISP实例ID与VRF关联来形成虚拟网络。

- 此VRF随后在各种交换机虚拟接口(SVI)下配置，它们成为第3层重叠网络的一部分
- 在大多数情况下，这些SVI也属于向其各自的第2层实例注册的VLAN。

使用命令“show lisp instance-id <instance> ipv4”查找VRF与LISP实例ID之间的映射

<#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
```

注意：此命令还可用于验证可为此实例启用的各种功能，以及显示LISP VXLAN交换矩阵内

使用的控制平面节点

创建第3层实例并将其链接到VRF后，将创建一个LISP 0 <instance-id>接口，该接口在运行配置中和show vrf下可见。

- 此接口不需要手动创建，通常不需要配置（使用底层组播时组播配置除外）。

<#root>

FE2068#

show vrf Fabric_VN_1

  Name   Default RD   Protocols   Interfaces

Fabric_VN_1

                                                          ipv4,ipv6

LI0.4099

Vl150

Vl151

与将VLAN中的所有MAC地址用于IP的以太网帧不同，需要获取IP地址在动态EID范围内。

显示LISP实例

<#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
```

在这些定义的范围之外的IP地址被视为不符合交换矩阵的条件，并且不会放入LISP数据库且不会向

控制平面节点注册。

<#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

输出显示所有本地已知IP地址信息。

- 对于主机，这些路由通常是主机路由（/32或/128），但如果这些路由已导入到基于边界节点的LISP数据库中，则它们也可以是子网。
- 来自SVI自身的IP地址标记为“不注册”。 这样可以避免所有交换矩阵设备向控制平面节点注册任播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与控制平面的配准

基于LISP VXLAN的交换矩阵中的终端注册通过LISP可靠注册。这意味着所有注册均通过已建立的TCP会话（即LISP会话）完成。从每个交换矩阵设备与交换矩阵中的每个控制平面节点建立LISP会话。通过此LISP会话，所有注册都会发生。如果交换矩阵中存在多个控制平面节点，则所有控制平面节点都将用于注册EID。

当交换矩阵设备上没有任何要注册的内容时（通常仅在外部边界上发生），状态为Down
不会向控制平面节点或在无任何端点的边缘设备上注册任何IP范围的设备

EID的注册通过LISP注册消息进行
发送到所有已配置的控制平面节点。

要查看交换矩阵设备上的LISP会话，可使用命令show lisp session。
它确实显示会话的状态和启动时间。

<#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

显示为Down的LISP会话可能发生在没有任何EID注册到控制平面节点的设备上。
通常是指没有连接任何端点的边界节点，这些节点不会将路由导入到交换矩阵或边缘设备中。

使用命令“show lisp session vrf default <ip address>”显示有关LISP会话的更多详细信息

<#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
```

会话的此详细输出显示哪些实例具有向控制平面节点注册的EID处于活动状态。

```
<#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
```

查看控制平面节点上的会话数时，通常会显示更多处于启用状态的会话。

- 如果这是并置的Border/CP节点，则还会建立面向自身的LISP会话。
- 在本例中，存在从172.30.250.19:4342到172.30.250.19:49270的会话。
- 通过此会话，边界组件向控制平面节点注册其EID。

1.4控制平面信息

利用交换矩阵设备通过注册提供的信息，控制平面节点能够构建交换矩阵的完整视图。根据实例ID，维护一个包含已获取的EID及其关联路由定位器的表。

使用show lisp site命令为第3层实例显示此

```
<#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
```

此命令显示所有注册的EID和最后注册EID的EID。需要注意的是，这通常也是正在使用的RLOC，但这可能不同。此外，EID还可以注册到多个RLOC(RLOCs)。

要显示完整的详细信息，命令包括EID和实例

```
<#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
```

注意：在详细输出中，需要注意以下几点：

- 代理，使用此设置，控制平面节点会直接响应映射请求。在传统LISP中，映射请求被

转发到注册EID但通过代理设置控制平面节点直接响应的XTR
- TTL，这是EID注册的生存时间。默认情况下为24小时
- ETR信息，这与已发送EID注册的交换矩阵设备有关
- RLOC信息，这是用于到达EID的RLOC。这也包含状态信息，如在up/down中。如果RLOC关闭，则不会使用它。它还包含权重和优先级，当存在多个RLOC时，可以使用这些RLOC来为EID赋予其中一个优先级。

要查看控制平面节点上的注册历史记录，可以使用命令show lisp server registration history。

- 它概述了已注册和取消注册的EID。

显示注册历史记录

<#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
```

显示已注册的以太网EID，命令为show lisp instance-id <instance> ethernet server（此命令提供类似第3层的输出）

<#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      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

附加MAC地址以获取有关注册的更多详细信息

<#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“registration history”以查看以太网EID的注册历史记录

注意：当设备在交换矩阵中漫游以查看MAC地址注册的位置和时间时，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
```

要查看控制平面节点上已注册的地址解析信息，命令后面会附加address-resolution。

- 这仅显示MAC地址与其第3层信息之间的映射，主要用于交换矩阵边缘将第2层目标MAC地址从广播/组播重写为单播。
- 对应于该第2层MAC地址的RLOC将单独解析。

附加“address-resolution”以查看控制平面节点上的注册地址解析信息

<#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
```

注意：即使链路本地IPv6地址与IPv6动态EID不匹配，也要学习地址解析，这会显示在控制平面节点上。这些设备本身不会在第3层实例ID下注册，但可用于地址解析。

解析远程目标

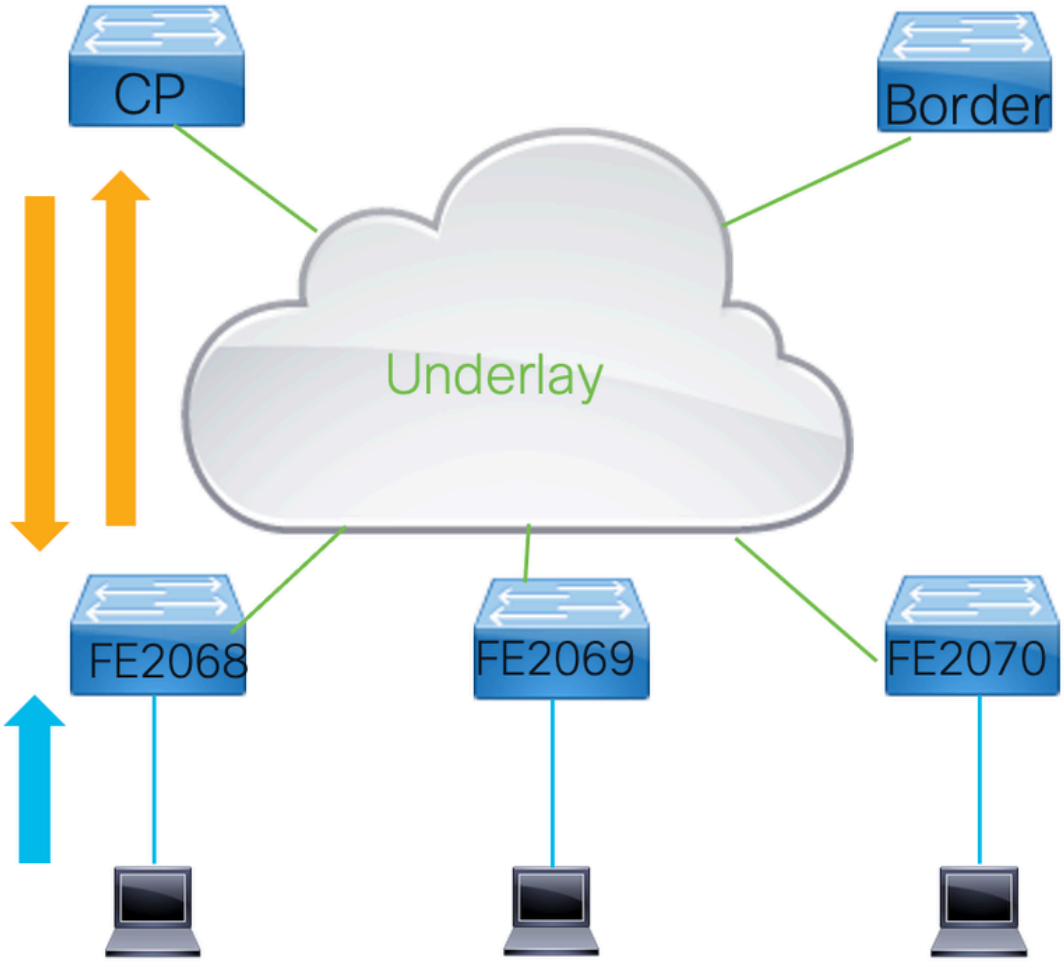
对于通过LISP VXLAN交换矩阵转发的流量，需要解析目标的RLOC。在LISP VXLAN交换矩阵中，这通过使用映射缓存来完成，信息将从映射缓存放入交换矩阵设备的转发信息库(FIB)。

使用LISP VXLAN交换矩阵时，会由于数据信号触发映射缓存。

- 这意味着流量被转发到CPU，并且CPU创建指向控制平面节点的映射请求，以查询RLOC信息，需要将指向该EID的帧发送到哪个RLOC。
- 当控制计划收到映射请求时，它会提供与此EID关联的路由定位器信息，或者发回否定映射应答。
- 当它发送负映射应答时，控制平面节点不仅会指示所请求的EID未知，还会提供该EID所属的整个EID块，而该EID将不具有任何注册。

使用来自控制平面节点的map-reply内的信息更新映射缓存。

- 映射应答的TTL通常为24小时。（对于负映射回复，通常只有15分钟）。
- 对于以太网EID，负映射回复不会放入映射缓存。（这仅适用于第3层实例）。



2.1以太网映射缓存

使用show lisp instance-id <instance> map-cache命令显示以太网映射缓存

<#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        -
```

此命令显示应已解析的远程MAC地址条目。

- 要触发以太网实例流量的映射缓存条目，需要将流量发送到未知目标。
- 这会导致交换矩阵设备尝试通过LISP解决此问题。
- 一旦通过映射应答获知，它将被放入映射缓存中，随后发往第2层目的地的帧将直接发送到获知的路由定位器。

在第2层实例中，可选的是BUM流量泛洪。

- 默认情况下，LISP/VXLAN不会泛洪流量，因为它使用重叠技术，但是可以在底层网络(GRT)中配置IP组播组，通过该组可以泛洪第2层帧。

显示广播底层组地址

<#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映射缓存

对于第3层实例，映射缓存信息类似于通过发送到CPU的流量构建的以太网，以发出导致发送映射请求的信号。

- 但是，对于第3层数据包，在设置此数据包时，只传送到CPU发出信号。这通过配置的map-cache命令来完成。对于IPv4，该地址为0.0.0.0/0，对于IPv6，该地址为：:0/0。
- 边界节点上的此映射缓存条目的配置必须小心。如果边界节点配置有此map-cache 0.0.0.0/0或：:0/0映射缓存条目，它会尝试通过交换矩阵解析未知目标，而不是将其路由到交换矩阵外部。

显示映射缓存配置

<#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导致映射缓存条目通过“send-map-request”操作在映射缓存中配置。达到此值的流量会触发映射请求。由于映射缓存条目将放入基于最长匹配的FIB，因此它适用于未命中任何更具体条目的所有路由IP流量。

- 在支持的平台上，为避免丢弃第一个数据包，显示的操作是send-map-request + encapsulate to proxy ETR。
  这会导致发往未知目标的第一个数据包触发映射请求，并且数据包被转发到代理etr（如果存在）。

<#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

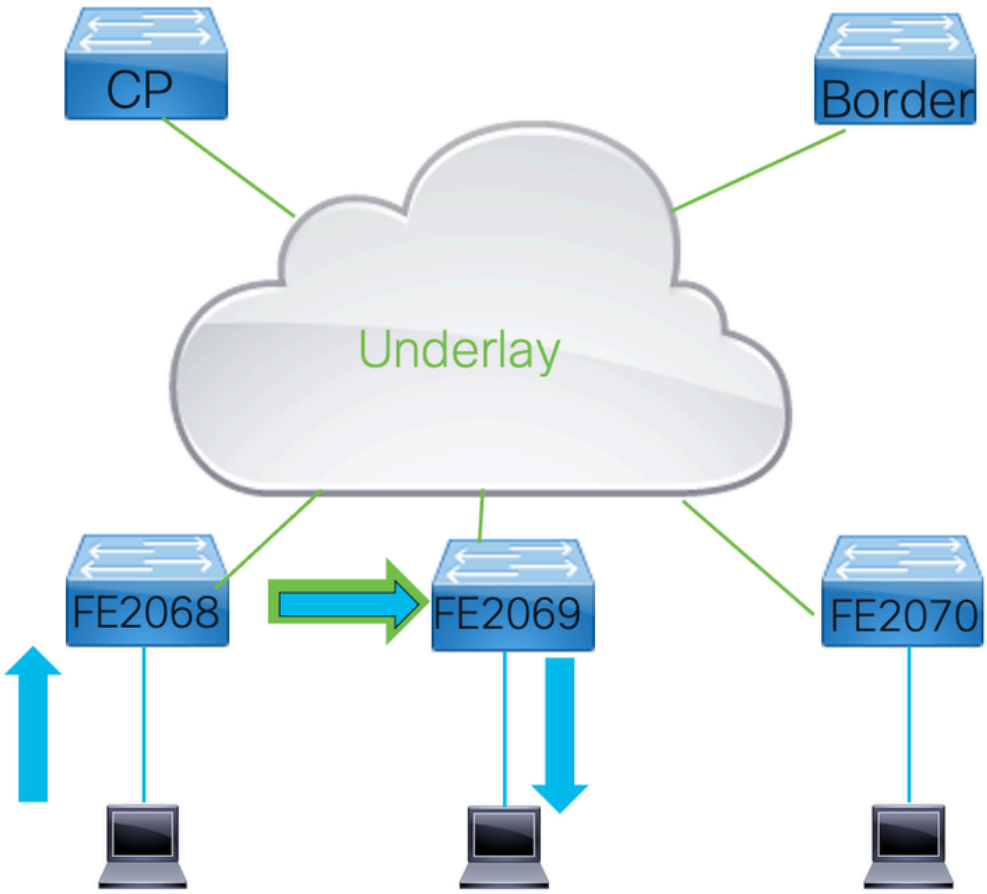
Locator	Uptime	State	Pri/Wgt	Encap-IID

```
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
```

在此输出中显示了一些条目。

- 此输出中的10.48.13.0/24和172.24.2.2/32通过映射应答获知并完成。流向这些目的地的流量将被封装并转发到各自的定位器。
- 172.28.0.0/14是已收到负映射应答和已返回的IP地址块的示例。只要此条目在映射缓存中，流向此子网的流量就不会触发映射请求。

通过交换矩阵的流量转发



3.1第2层或第3层转发

LISP/VXLAN交换矩阵中的流量可通过第2层或第2层实例转发。

- 确定使用哪个实例取决于帧的目的MAC地址。
- 发送到任何MAC地址（而不是向交换机注册的MAC地址）的帧将转发到第2层。如果数据包的目的地是交换机，则会通过第3层转发该帧。
- 此逻辑同样适用于通过Catalyst 9000系列交换机的正常转发。

3.2第2层转发

通过LISP VXLAN交换矩阵的第2层转发基于第2层目标MAC地址完成。远程目标将插入具有出口接口L2LI0的MAC地址表中。

显示本地和远程第2层接口

<#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
```

对于未知目标（如果已配置），流量通过底层中配置的IP组播组发送。

- 为了确保广播、未知单播和组播（仅选择组播泛洪）流量的正确泛洪，需要底层能够正常运行的组播环境。
- 将通过此组播底层组发送的流量将封装在VXLAN中。
- 所有其他边缘必须加入组播组并接收流量，并为已知的第2层实例解封流量。

显示基础IP组播组

<#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:
```

此输出显示交换矩阵中配置有发送泛洪流量的客户端的所有其他Edge的S、G条目。它还显示一个S、G条目，其中此边缘设备的Loopback0作为源。

对于通过底层组播组的流量接收端，show ip mroute命令还显示L2LISP0.<instance>
这将指示此边缘设备将对哪些第2层实例取消封装泛洪流量并将其转发到
相关接口。

3.3第3层转发信息

要确定部署LISP VXLAN交换矩阵时如何转发流量，请务必验证CEF。

- LISP与传统路由协议不同，它不会在路由表中插入路由方向，而是直接与CEF交互以更新FIB。

对于给定的远程目标，映射缓存信息包含要使用的定位器信息。

显示定位器信息

<#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)
```

从映射缓存中，用于此EID的定位器为172.30.250.44。因此，将封装流向此目标的流量，并且外部IP报头的IP目标地址为172.30.250.44。

在用于此实例的VRF的路由表中，不显示此条目。

<#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
       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输出提供有关通过LISP VXLAN交换矩阵的转发的详细信息。

- 当添加了show ip cef命令的detail关键字时，它并不只是为要发送的封装帧指定目标。
- 输出为LISP 0.<instance>的传出接口表示流量已封装发送。

<#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

由于流量将被封装到下一跳中，下一步是运行show ip cef <next hop>以查看数据包也将路由出去的出口接口。

运行以查看出口接口

<#root>

```
FE2067#
sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23
```

注意：有2个不同级别的等价多路径(ECMP)路由是可能的。

- 如果存在2个通告的RLOC，流量可以在重叠中进行负载均衡；如果存在到达RLOC IP地址的冗余路径，流量可以在底层网络中实现负载均衡。
- 由于UDP目的端口固定为4789，并且两个交换矩阵设备之间所有流的源IP地址和目的IP地址相同，因此需要采用某种形式的抗极化机制，以避免所有数据包通过同一路径路由。
- 使用LISP VXLAN时，这是外部报头中的UDP源端口，对于溢出网络中的不同流量来说会有所不同。

3.4数据包格式

- 在LISP VXLAN交换矩阵内，所有流量都完全封装在VXLAN中。这包括整个第2层帧，以便能够支持第2层和第3层重叠。
  对于第2层帧，将封装原始报头。对于通过第3层实例发送的帧，使用虚拟的第2层报头。

<#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
```

从通过LISP VXLAN交换矩阵传输的帧捕获示例可以看出，vxlan数据包中有完全封装的帧。作为第3层帧，以太网报头是一个虚报报头。

在VXLAN报头中，“VLAN网络标识符”(VLAN Network Identifier)字段传输帧所属的LISP实例ID。

- 通过Group Policy ID字段传输帧SGT标记。
- 这会在交换矩阵中的入口设置并传递到交换矩阵，直到完成基于组的策略实施。

身份验证和安全实施

4.1交换机端口身份验证

要动态地将终端分配到其各自的VLAN并为其分配SGT标记身份验证，可以使用SGT标记身份验证。

- 作为Dot1x/MAB/central webauth的身份验证协议可以部署在Radius服务器上对用户和终端进行身份验证和授权，该服务器将属性发送回交换机，以允许网络访问正确池中的客户端/终端并使用正确的网络访问授权。

对于LISP VXLAN交换矩阵，有几种常见的RADIUS属性：

- Vlan分配：从RADIUS服务器到交换机，此属性设置为VLAN ID或名称，终端可分配给特定第2层/第3层LISP实例。
- SGT值：此属性设置SGT向此SGT分配终端。这将用于针对此终端的基于组的策略，并向通过此终端发起的交换矩阵发送的所有帧分配SGT值。
- 语音授权：语音设备在语音vlan上运行。这会设置允许终端在端口上配置的语音vlan中发送和接收流量的语音授权。这样可以分离其各自的VLAN中的语音和数据流量
- 会话超时:各个终端都有自己的会话超时。可以从radius服务器发送超时来指示客户端需要重新身份验证的频率
- 模板：对于某些终端，需要在端口上应用不同的模板才能正常运行。 可以从Radius服务器发送模板名称，该名称将指示需要应用到端口的内容

使用show access-session命令检查端口上的身份验证结果

```
<#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
```

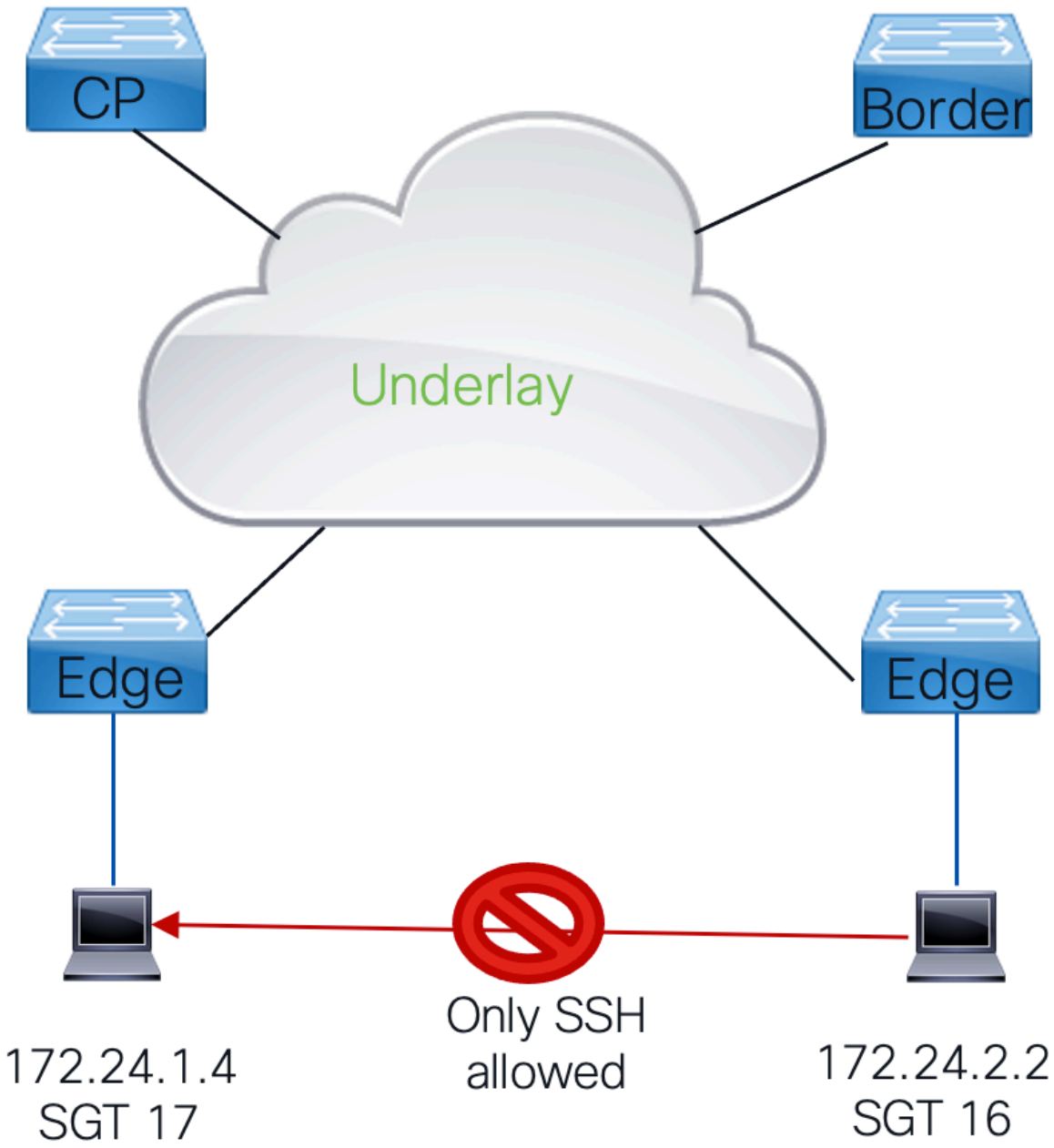
Success

请注意以下关键字段：

- IPv4和IPv6地址：通常通过设备跟踪学习。
- username：这是用于身份验证的用户名。
  - 对于Dot1x，这通常是进行身份验证的用户。
  - 使用MAB时，这是站点的MAC地址，作为用户名和密码发送到Radius进行身份验证。
- 状态:这表示身份验证的状态和身份验证结果。
- 域名：对于普通终端，这是数据域，因此流量将在端口上无标记发送/接收。（对于语音设备，可将其设置为“语音”）

- 服务器策略：这是来自Radius服务器的信息（如Vlan分配和SGT分配）的位置
- 方法状态列表：这显示了运行的方法的概述。
  - 标准dot1x在MAB之前运行。
  - 如果终端不响应EAPOL帧，则此方法将故障转移到mab。
  - 这将显示dot1x已失败。
  - MAB显示authc success表示它经过身份验证，它不反映身份验证结果是access-accept还是reject。

4.2流量策略和基于组的策略(CTS)



在LISP VXLAN交换矩阵CTS中，用于实施流量策略：

- 基于组的策略架构基于安全组标记。
- 交换矩阵内的所有流量都分配到入口和SGT标记上，该标记在每个帧中通过交换矩阵传输。
- 当此流量离开交换矩阵时，将实施流量策略。
- 此操作在基于组的策略中完成，该策略根据由源 — 目标SGT组成的矩阵检查数据包的源和目标组标记，其中结果是定义允许或不允许哪些流量的SGACL。
- 当矩阵内没有源 — 目标SGT的特定匹配项时，将应用定义的默认操作。

4.3 CTS环境

要使用基于组的策略运行，交换矩阵设备首先需要获取CTS建立。

- 此pac将在RADIUS帧内用于授权思科ISE上的RADIUS帧。这用于设置Radius帧中的cts-pac-opaque字段。

显示CTS pac信息

<#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

确保CTS pac已配置且有效非常重要。交换矩阵设备会自动刷新该值。

注意：要手动触发刷新，可发出命令“cts refresh pac”。

要运行基于组的策略，它会下载环境数据并下载所需的策略信息。

- 此环境数据既包含交换机本身使用的CTS标记，也包含Radius服务器上已知的所有基于组的策略组的表。

显示cts环境数据

<#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
```

当使用基于组的策略时，仅下载的策略是设备具有需要强制实施的本地终端的CTS标记。

- 为了能够检查从IP地址（或子网）到基于组的策略组的映射，可以使用命令“show cts role-based sgt-map vrf <vrf> all”。

显示VRF的所有已知IP到SGT信息

<#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
```

此输出显示给定VRF的所有已知IP地址（和子网）及其基于组的策略关联。

- 可以看到，终端有一个IP地址被分配了基于组的策略组17，并且源自本地。
- 这是端口上发生的身份验证的结果，其中结果指示与该终端关联的标记。
- 它还突出显示了交换机自己的IP地址，这些地址分配有device-sgt tag作为sourced internal。
- 也可以通过配置或通过指向ISE的SXP会话分配基于组的策略标记。

当设备获知SGT标记时，它会尝试从ISE服务器下载与其关联的策略。

- 命令show cts authorization entications概述了尝试下载这些项的时间以及它们是否已连续下载。

注意：如果策略发生任何更改，将定期刷新策略。ISE还可以推送CoA命令，使交换机在更改时触发以下载新策略。 要手动刷新策略，请发出命令“cts refresh policy”。

显示尝试下载的策略的概述，以及是否连续下载

<#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
```

如果下载了任何策略，则可以使用命令“show cts rolebased policies”显示这些策略。

```
<#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
```

此命令显示设备了解的所有策略。在ISE服务器上，可能有更多策略用于不同的组，但设备仅尝试下载其知道终端用于的策略。这样可以节约宝贵的硬件资源。

此命令还显示要应用于流量且没有更多特定条目的默认操作。在本例中，它是Permit IP，因此所有与表中特定条目不匹配的流量都将被允许通过。

运行show cts rbacl <name>以获取有关已下载RBACL的确切内容的详细信息

<#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

在这种情况下，允许发送到应用了此RBACL的终端的唯一流量是指向22(SSH)和23(Telnet)的tcp数据包。

注意：RBACL只能在一个方向上运行。除非返回流量中有策略，否则将使用默认策略实施该策略。进入交换矩阵的流量不会被强制实施，它通过交换矩阵发送带有入口节点上已知的SGT标记。仅当它离开交换矩阵且要在设备上存在的策略上实施时，才会实施该策略。通常，这些策略是相同的，但可以扩展CTS域，例如使用防火墙，其中可以定义其他策略，具体取决于部署的安全策略。

运行show cts role-based counters以验证帧是否已丢弃

- 此命令显示整个交换机的累积计数器。每个接口没有对应的命令。

<#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
```

此概述显示了交换机知道的所有已知条目，在本例中这些条目能够匹配从17到16以及从16到17的流量。

- 任何属于* *范围内的其他匹配项都会应用默认操作，因此，如果任何流量（例如18到16）与交换机上的已知矩阵不匹配，则应用默认操作。

即使计数器是累积的，它们也会很好地指示流量是否被丢弃。

- 要确定哪个流量会命中条目，可以在ISE服务器上将log关键字添加到各自的策略，这会导致交换机在命中该条目时提供日志消息。
- 此操作既可以对默认操作(* *)执行，也可以对矩阵中的某个特定条目执行。

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。