Catalyst 9000 Series 스위치의 LISP VXLAN Fabric 문제 해결

목차

소개

이 문서에서는 LISP VXLAN 기반 패브릭의 기본 구성 요소 및 작동 확인 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Cisco IOS XE 17.9.3 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

LISP VXLAN 기반 패브릭

LISP VXLAN 네트워크를 구축하는 목적은 여러 오버레이 네트워크(Virtual Networks라고도 함)가 언더레이 네트워크 위에 정의되는 아키텍처를 만드는 것입니다.

- 이러한 토폴로지의 언더레이 네트워크는 주로 전송 레이어로 작동하며, 이를 통해 실행되는 오버레이 토폴로지를 인식하지 못합니다.
- 오버레이 네트워크는 언더레이 네트워크에 영향을 주지 않고 추가 및 제거할 수 있습니다.
- 오버레이 네트워크를 사용하면 사용자를 언더레이 네트워크와 효과적으로 분리할 수 있습니다.

LISP VXLAN 패브릭 구축에 사용되는 기술

LISP(Locator Identity Separation Protocol)

- LISP 프로토콜은 패브릭 내에서 사용되는 컨트롤 플레인 프로토콜입니다. 모든 패브릭 디바이스에서 실행되어 패브릭을 구축하고 패브릭을 통해 트래픽이 전송되는 방식을 제어합니다.
- LISP는 2개의 주소 공간을 만듭니다. 하나는 연결성을 광고하는 데 사용되는 RLOC(Routing Locator)용입니다. 다른 주소 공간은 엔드포인트 식별자(EID)이며, 엔드포인트가 상주하는 위치이며 오버레이에 사용됩니다.
- LISP 내에서 EID는 광고된 RLOC로 광고됩니다. EID가 모든 작업을 수행해야 하는 경우 연관된 Routing Locator를 업데이트합니다.
- EID로 향하는 LISP 트래픽이 있는 엔드포인트에 도달하려면 캡슐화하고 이를 캡슐화하여 엔드포인트로 전달하는 RLOC로 터널링해야 합니다.

그룹 기반 정책

- 패브릭 그룹 기반 정책 내에서 세그멘테이션을 허용할 수 있도록 하는 것이 사용됩니다.
- 그룹 기반 정책이 구축된 경우 트래픽은 소스/목적지 IP를 기준으로 하는 대신 보안 그룹으로 분류됩니다.
- 이렇게 하면 복잡한 액세스 제어 목록의 복잡성이 줄어듭니다. 유지 관리해야 하는 IP 주소의 목록 대신 IP 주소/서브넷이 보안 그룹 태그에 할당됩니다.
- 트래픽이 패브릭에서 나갈 때 패브릭으로의 인그레스(ingress)에 SGT가 태그됩니다. 프레임의 목적지는 SGT를 찾습니다.
- 매트릭스를 사용하면 소스 및 대상 SGT가 일치하고 보안 그룹 ACL이 적용되어 패브릭을 떠날 때 트래픽을 적용합니다.

VXLAN 캡슐화

- 패브릭 VXLAN 내부는 모든 트래픽을 캡슐화하는 데 사용됩니다
- 기존 LISP 캡슐화에서 VXLAN을 사용하면 레이어 3 프레임뿐만 아니라 전체 레이어 2 프레임을 캡슐화할 수 있다는 이점이 있습니다. 전체 프레임이 캡슐화됨에 따라 오버레이가 레이어 2와 레이어 3 모두 될 수 있습니다.
- VXLAN은 대상 포트 4789의 UDP를 사용합니다. 따라서 오버레이 토폴로지를 인식하지 못하는 디바이스를 통해 LISP VXLAN 프레임을 전송할 수 있습니다.
- VXLAN은 전체 프레임을 캡슐화하므로 RTU를 늘려 RLOC 간에 트래픽을 전송할 때 단편화가 필요하지 않도록 해야 합니다. 중간 디바이스는 캡슐화된 프레임을 전송하기 위해 더 큰 MTU를 지원해야 합니다.

인증

- 엔드 포인트를 각각의 리소스에 할당 할 수 있는 인증을 사용 할 수 있습니다.
- 802.1x와 같은 프로토콜에서는 MAB 및 Webauth 엔드포인트를 Radius 서버에 대해 인증 및/또는 프로파일링할 수 있으며, 인증 프로파일에 따라 네트워크에 대한 액세스 권한을 부여할 수 있습니다.
- 엔드 포인트/사용자 네트워크 액세스를 제공 하기 위해 엔드 포인트는 각각의 Radius 특성을 사용 하여 엔드 포인트를 각각의 VLAN, SGT 및 기타 특성에 할당 할 수 있습니다.

LISP VXLAN 패브릭의 주요 구성 요소

컨트롤 플레인 노드

- lisp 맵 서버 및 맵 확인자 기능을 보유하고 있습니다.
- 다른 모든 패브릭 디바이스는 컨트롤 플레인 노드에서 EID의 위치를 쿼리하고 해당 EID에 대한 등록을 컨트롤 플레인 노드로 전송합니다.
- 그러면 컨트롤 플레인 노드에서 다양한 EID의 RLOC 이면에 대한 패브릭의 전체 보기를 제공합니다.

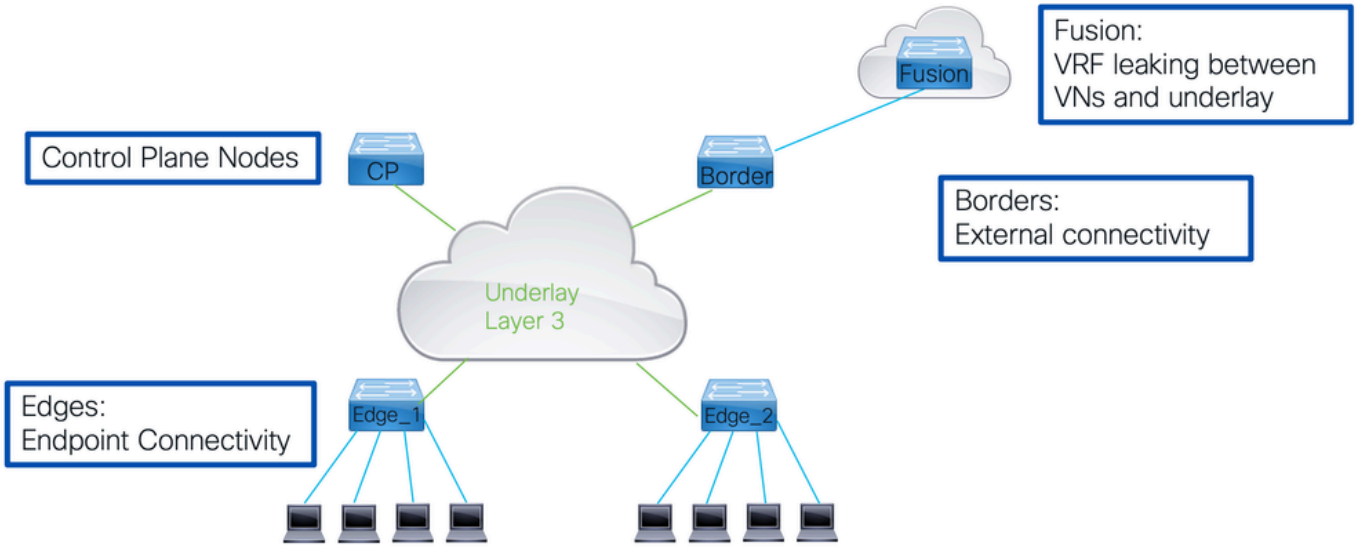
보더 노드

- 패브릭 외부의 다른 패브릭이나 외부 세계와의 연결을 제공합니다.
- 내부 경계는 경로를 패브릭으로 가져와 컨트롤 플레인 노드에 등록합니다.
- 외부 경계는 외부 세계에 연결되며 패브릭 외부에서 알 수 없는 IP 대상에 대한 기본 경로를

제공합니다.

에지 노드

- 이러한 노드는 패브릭 내부의 엔드포인트에 대한 연결을 제공합니다.
- LISP의 정의에서는 ITR(Ingress Tunnel Router) 및 ETR(Egress Tunnel Router)의 기능을 모두 수행하는 XTR이 사용됩니다.



노드는 하나의 작업만 수행하는 것으로 제한되지 않습니다.

- 이들은 패브릭 내에서 조합 또는 심지어 모든 기능을 수행할 수 있습니다.
- 경계 노드와 제어 평면 노드가 하나의 디바이스에 상주할 경우 이 노드를 같은 위치라고 합니다.
- 해당 노드가 Edge 기능도 제공하는 경우 FIAB(Fabric In A Box)라고 합니다.

테두리는 VRF lite를 사용하는 네트워크의 나머지 부분에 대한 핸드오프를 제공합니다.

- 각 오버레이 또는 가상 네트워크는 보더 노드의 VRF 인스턴스와 연결됩니다.
- 이러한 다양한 VRF를 함께 연결하려면 Fusion 라우터가 사용됩니다. 이 Fusion Router는 패브릭 자체의 일부가 아니라 오버레이 네트워크를 패브릭에 연결할 수 있는 작업에 매우 중요합니다.

LISP VXLAN 패브릭 내에서 또 다른 중요한 개념은 IP 애니캐스트를 사용하는 개념입니다.

- 즉, 모든 에지 디바이스에서 SVI(Switched Virtual Interface)의 IP 주소 및 MAC 주소가 복제됩니다.
- 모든 Edge는 IPv4, IPv6 및 MAC 주소와 관련하여 SVI에서 동일한 컨피그레이션을 갖습니다.
- 이를 해결하기 위해서는 몇 가지 과제가 따릅니다.
  - Ping으로 연결성을 테스트하는 것은 로컬 연결된 디바이스에서 작동합니다.
  - LISP VXLAN 패브릭을 통해 원격 대상에 도달하려는 경우 응답을 보내는 장치가 이를 anycast IP 주소에도 전송하므로 응답을 반환하지 않습니다. anycast IP 주소는 다른 패

브릭 노드가 원래 ping을 보낸 것을 인식하지 못하는 로컬 패브릭 장치에 적용됩니다.

엔드포인트 등록

LISP VXLAN 패브릭이 작동하려면 Control Plane 노드에서 패브릭을 통해 모든 엔드포인트에 연결할 수 있는 방법을 인식하는 것이 중요합니다.

- 제어 평면이 네트워크의 모든 EID에 대해 알아보려면, 알고 있는 모든 EID를 제어 평면에 등록하기 위해 다른 모든 패브릭 디바이스에 의존합니다.
- 패브릭 노드는 LISP map-register 메시지를 컨트롤 플레인 노드로 전송합니다. map-register 메시지로 광고되는 정보.

중요 정보

LISP 인스턴스 식별자:

- 이 식별자는 패브릭을 통해 전달되며 사용할 가상 네트워크를 나타냅니다.
- 레이어 3 오버레이당 LISP VXLAN 패브릭 내에서 사용된 VLAN당 하나의 인스턴스가 사용되며, 여기에는 레이어 2 인스턴스도 있습니다.

엔드포인트 식별(EID):

- 레이어 2 또는 레이어 3 인스턴스인 경우 MAC 주소, IP 호스트 경로(/32 또는 /128) 또는 등록된 IP 서브넷입니다

라우팅 로케이터(RLOC):

- 이 패브릭 노드는 다른 패브릭 디바이스가 EID에 도달해야 하는 캡슐화된 트래픽을 전송하는 연결 가능성을 광고하는 IP 주소를 소유합니다.

프록시 플래그:

- 이 플래그를 설정하면 컨트롤 플레인 노드가 다른 패브릭 노드의 맵 요청에 직접 응답할 수 있습니다. 프록시 플래그는 모든 요청을 EID를 등록한 패브릭 노드로 전달하도록 설정합니다.

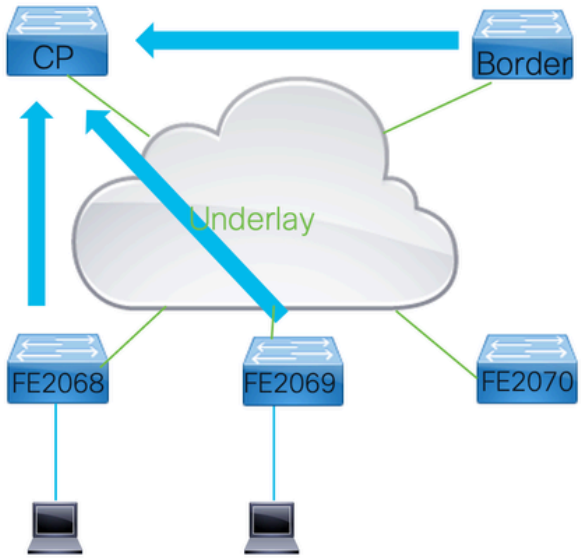
등록 단계

1단계: 패브릭 디바이스는 엔드포인트 식별자에 대해 학습합니다. 이는 컨피그레이션, 라우팅 프로토콜 또는 패브릭 디바이스에서 학습한 경우에 가능합니다.

2단계: 패브릭 디바이스는 파악된 엔드포인트를 패브릭 내의 각 알려진 연결 가능한 제어 평면 노드에 등록합니다.

3단계: 제어 평면 노드는 관련 인스턴스 ID, RLOC 및 학습된 EID를 사용하여 등록된 EID의 테이블을 유지 관리합니다

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



다음을 확인합니다.

1.1 MAC 주소 학습

레이어 2 인스턴스의 경우 사용되는 EID는 연결된 VLAN 내에서 학습되는 MAC 주소입니다. 패브릭 엣지는 스위치의 표준 방법을 통해 레이어 2 주소를 학습합니다.

컨피그레이션을 검토할 수 있는 특정 레이어 2 인스턴스 ID와 연결된 VLAN 또는 명령을 찾습니다

"show lisp instance-id <instance> ethernet"을 사용합니다.

<#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
```

출력에 표시된 대로 instance-id 8191은 VLAN 150과 연결됩니다. 그러면 VLAN 내의 모든 MAC 주소가 LISP에 등록되고 LISP VXLAN 패브릭의 일부가 됩니다.

```
<#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
```

인터페이스 Vl150의 고정 항목은 스위치 가상 인터페이스(인터페이스 vlan 150)의 MAC 주소입니다.

- 이러한 MAC 주소는 모든 에지 디바이스에서 동일하므로 컨트롤 플레인 노드에 등록되지 않습니다.
- 표시되는 CP_LEARN 항목은 패브릭을 통해 학습된 항목입니다. 다른 모든 항목의 경우 동적 또는 정적 항목일 경우 컨트롤 플레인 노드에 등록해야 합니다.

각 방법을 통해 학습된 항목이 lisp 데이터베이스 출력에 나타나면 이 출력에는 이 패브릭 디바이스의 모든 로컬 항목이 포함됩니다.

```
<#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
```

데이터베이스에 표시된 모든 알려진 로컬 MAC 주소에 대해 로케이터가 표시됩니다.

- 이 엔트리를 제어 평면 노드에 등록하는 데 사용할 로케이터입니다.
- 또한 로케이터의 상태를 나타냅니다.스위치 SVI에 속한 2개의 MAC 주소도 표시되지만 등록되지 않도록 하는 "등록하지 않음" 플래그와 함께 표시됩니다.
- show mac address table 명령에 표시된 원격 항목은 로컬 MAC 주소가 아니므로 lisp 데이터베이스 아래에 표시되지 않습니다.

레이어 2 인스턴스의 경우 레이어 2 MAC 주소가 EID로 학습될 뿐만 아니라 ARP 및 ND 프레임에서 주소 해상도 정보를 학습해야 합니다.

- 이는 LISP VXLAN 패브릭이 일반적으로 VLAN 내부에서 플러딩되는 프레임을 전달할 수 있도록 하기 위한 것입니다.

- 레이어 2 인스턴스 ID는 엔드포인트가 동일한 인스턴스의 다른 엔드포인트에 대한 주소 확인 정보를 확인할 수 있도록 하는 다른 메커니즘을 플러딩할 수 있는 기능이 항상 있는 것은 아닙니다. 이를 위해 패브릭 디바이스는 Device-Tracking에서 로컬로 학습된 이 정보를 학습하고 등록합니다.
- 그런 다음 제어 평면 노드에도 등록됩니다. ND 또는 ARP 스누핑으로 인해 이러한 패킷은 CPU로 전송되어 제어 평면 노드에 대한 요청을 트리거하여 연결된 알려진 MAC 주소가 있는지 확인합니다.
- 양성 응답이 다시 오면 대상 mac 주소가 브로드캐스트 또는 멀티캐스트에서 유니캐스트 mac 주소로 변경되도록 ARP/ND 패킷이 재작성됩니다.
- 이렇게 다시 작성된 패킷은 LISP VXLAN 패브릭을 통해 유니캐스트 프레임으로 전달될 수 있습니다.

스위치에 알려진 주소 확인 정보를 보려면 show device-tracking database 명령을 사용할 수 있습니다.

- 디바이스 추적에서 알려진 모든 매핑이 표시됩니다.
- 스위치 소유 IP 주소는 L(Local)로 표시되어 있으며 디바이스 추적 데이터베이스에 있어야 합니다.

원격 항목도 이 출력에 표시됩니다.

- ND 또는 ARP 요청을 스누핑한 후 해결되면 링크 계층 주소 0000.0000.00fd의 디바이스 추적 데이터베이스에 저장됩니다.
- 문제가 해결되면 정보는 확인된 mac 주소로 변경되고 포트는 Tu0으로 변경됩니다.

장치 추적 데이터베이스 표시

<#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
```

'show lisp instance-id <instance> ethernet database address-resolution' 명령을 사용하여 로컬에 등록된 매핑을 표시합니다.

```
<#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 동적 IP 주소 학습

IP 계층의 패브릭 디바이스에서는 LISP Instance-id를 VRF와 연결하여 가상 네트워크를 구성합니다.

- 이 VRF는 다양한 SVI(Switch Virtual Interface)에서 구성되며 레이어 3 오버레이 네트워크의

일부가 됩니다
- 대부분의 경우 이러한 SVI는 해당 레이어 2 인스턴스에 등록된 VLAN에도 속합니다.

'show lisp instance-id <instance>ipv4' 명령을 사용하여 VRF와 LISP 인스턴스 ID 간의 매핑을 찾습니다.

<#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**

참고: 이 명령은 또한 이 인스턴스에 대해 활성화할 수 있는 다양한 기능을 확인하는 데 사용할 수 있으며, LISP VXLAN 패브릭 내에서 사용된 컨트롤 플레인 노드를 표시합니다

레이어 3 인스턴스가 생성되어 VRF에 연결되면 LISP 0 <instance-id> 인터페이스가 생성되고 실행 중인 컨피그레이션에서 show vrf에 표시됩니다.

- 이 인터페이스는 수동으로 생성할 필요가 없으며 일반적으로 언더레이 멀티캐스트를 사용할 경우 멀티캐스트 컨피그레이션과 별도로 컨피그레이션이 필요하지 않습니다.

<#root>

FE2068#

show vrf Fabric_VN_1

Name Default RD Protocols Interfaces

Fabric_VN_1

ipv4,ipv6

LI0.4099

Vl150

Vl151

VLAN의 모든 MAC 주소가 IP에 사용되는 이더넷 프레임과 달리 IP 주소가 Dynamic EID 범위 내에 있어야 학습할 수 있습니다.

LISP 인스턴스 표시

<#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

이러한 정의된 범위를 벗어나는 IP 주소는 패브릭에 적합하지 않은 것으로 간주되며 LISP 데이터베이스에 추가되지 않고 컨트롤 플레인 노드에 등록되지 않습니다.

<#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
```

출력에는 로컬로 알려진 모든 IP 주소 정보가 표시됩니다.

- 호스트의 경우 이러한 경로는 일반적으로 호스트 경로(/32 또는 /128)이지만, 보더 노드를 기반으로 LISP 데이터베이스로 가져온 경우 서브넷일 수도 있습니다.
- SVI 자체의 IP 주소는 "등록 안 함"으로 플래그가 지정됩니다. 이는 모든 패브릭 디바이스가 Anycast IP 주소를 컨트롤 플레인 노드에 등록하는 것을 방지하기 위한 것입니다.

<#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 컨트롤 플레인에 EID 등록

LISP VXLAN 기반 패브릭에서 엔드포인트 등록은 LISP 안정적인 등록을 통해 이루어집니다. 즉, 모든 등록은 설정된 TCP 세션인 LISP 세션을 통해 수행됩니다. 모든 패브릭 디바이스에서 패브릭의 각 컨트롤 플레인 노드와 함께 LISP 세션이 설정됩니다.이 LISP 세션을 통해 모든 등록이 수행됩니다. 패브릭 내에 컨트롤 플레인 노드가 여러 개 있는 경우 모두 EID를 등록하는 데 사용됩니다.

패브릭 디바이스에 등록할 항목이 없는 경우 상태는 Down이며, 이는 일반적으로 External border에서만 발생합니다
엔드포인트가 없는 Edge 디바이스나 Control Plane 노드에 IP 범위를 등록하지 않음

EID의 등록은 LISP 등록 메시지를 통해 이루어집니다
모든 구성된 컨트롤 플레인 노드로 전송해야 합니다.

패브릭 디바이스에서 LISP 세션을 보려면 show lisp session 명령을 사용할 수 있습니다.
세션의 상태와 작동 시간이 표시됩니다.

<#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
```

Down으로 표시된 LISP 세션은 제어 평면 노드에 등록할 EID가 없는 디바이스에서 발생할 수 있습니다.
일반적으로 이는 연결된 엔드포인트가 없는 패브릭 또는 에지 디바이스로 경로를 가져오지 않는 경계 노드입니다.

'show lisp session vrf default <ip address>' 명령을 사용하여 LISP 세션에 대한 자세한 정보를 표시합니다.

<#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
```

이 자세한 세션 출력은 제어 평면 노드에 등록된 EID로 어떤 인스턴스가 활성화되었는지 보여줍니다.

```
<#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
```

컨트롤 플레인 노드에서 세션 수를 보면 일반적으로 작동 중인 세션이 더 많습니다.

- 이 노드가 함께 배치된 Border/CP 노드인 경우 자신을 향한 LISP 세션도 설정됩니다.
- 이 경우 172.30.250.19:4342에서 172.30.250.19:49270까지의 세션이 있습니다.
- 이 세션을 통해 Border 구성 요소는 컨트롤 플레인 노드에 EID를 등록합니다.

1.4 컨트롤 플레인 정보

등록을 통해 패브릭 디바이스에서 제공하는 정보를 통해 컨트롤 플레인 노드는 패브릭의 전체 보기를 작성할 수 있습니다. Instance-id에 따라 학습된 EID 및 연결된 라우팅 로케이터가 있는 테이블을 유지 관리합니다.

명령이 show lisp site를 사용하여 레이어 3 인스턴스에 대해 이 정보를 표시합니다

<#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
```

이 명령은 등록된 모든 EID와 마지막으로 EID를 등록한 사람을 표시합니다. 일반적으로 이것이 사용 중인 RLOC이기도 하지만, 이는 다를 수 있습니다. 또한 EID는 여러 RLOC에 등록할 수 있습니다.

전체 세부사항을 표시하려면 EID와 인스턴스를 명령어로 포함합니다

<#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
```

참고: 세부적인 결과에서 몇 가지 유의해야 할 사항은 다음과 같습니다.

- 프록시는 이 설정으로 제어 평면 노드가 맵 요청에 직접 응답합니다. 기존 LISP에서는 맵 요청이 EID를 등록한 XTR에 전달되지만 프록시 설정에서는 컨트롤 플레인 노드가 직접 응답합니다
- TTL - EID 등록의 TTL(Time To Live)입니다. 기본적으로 24시간입니다.
- ETR 정보, 이는 EID 등록을 전송한 패브릭 디바이스와 관련이 있습니다
- RLOC 정보, EID에 도달하기 위해 사용되는 RLOC입니다. 여기에는 up/down과 같은 상태 정보도 포함됩니다. rloc가 다운된 경우 사용되지 않습니다. 또한 EID에 대한 여러 RLOC가 있을 때 사용할 수 있는 가중치와 우선순위를 포함하여 둘 중 하나에 우선순위를 부여합니다.

컨트롤 플레인 노드의 등록 기록을 보려면 명령 show lisp server registration history를 사용할 수 있습니다.

- 등록 및 등록 취소된 EID의 개요를 제공합니다.

등록 기록 표시

<#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
```

이더넷에 대해 등록된 EID를 표시합니다. 명령은 show lisp instance-id <instance> ethernet server입니다(레이어 3과 유사한 출력을 제공합니다.)

<#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
```

등록에 대한 자세한 정보를 보려면 MAC 주소를 추가합니다.

```
<#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
```

'등록 기록'을 추가하여 이더넷 EID에 대한 등록 기록을 확인합니다.

참고: 이 명령은 디바이스가 패브릭에서 로밍하여 MAC 주소가 등록된 위치와 시간을 확인할 때 매우 유용합니다

<#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
```

컨트롤 플레인 노드에서 등록된 주소 확인 정보를 보려면 명령에 주소 확인이 추가됩니다.

- 이는 MAC 주소와 해당 레이어 3 정보 간의 매핑만 보여주며, 주로 패브릭 에지에서 레이어 2 목적지 MAC 주소를 브로드캐스트/멀티캐스트에서 유니캐스트로 재작성하는 데 사용됩니다.
- 해당 레이어 2 MAC 주소에 해당하는 RLOC는 별도로 확인됩니다.

'address-resolution'을 추가하여 컨트롤 플레인 노드에서 등록된 주소 확인 정보 보기

<#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

참고: 링크 로컬 IPv6 주소가 IPv6 동적 EID와 일치하지 않더라도 주소 확인을 위해 학습해야 하며, 이는 컨트롤 플레인 노드에 표시됩니다. 이 ID는 레이어 3 인스턴스 ID에 등록되지 않지만 주소 확인에 사용할 수 있습니다.

원격 대상 확인

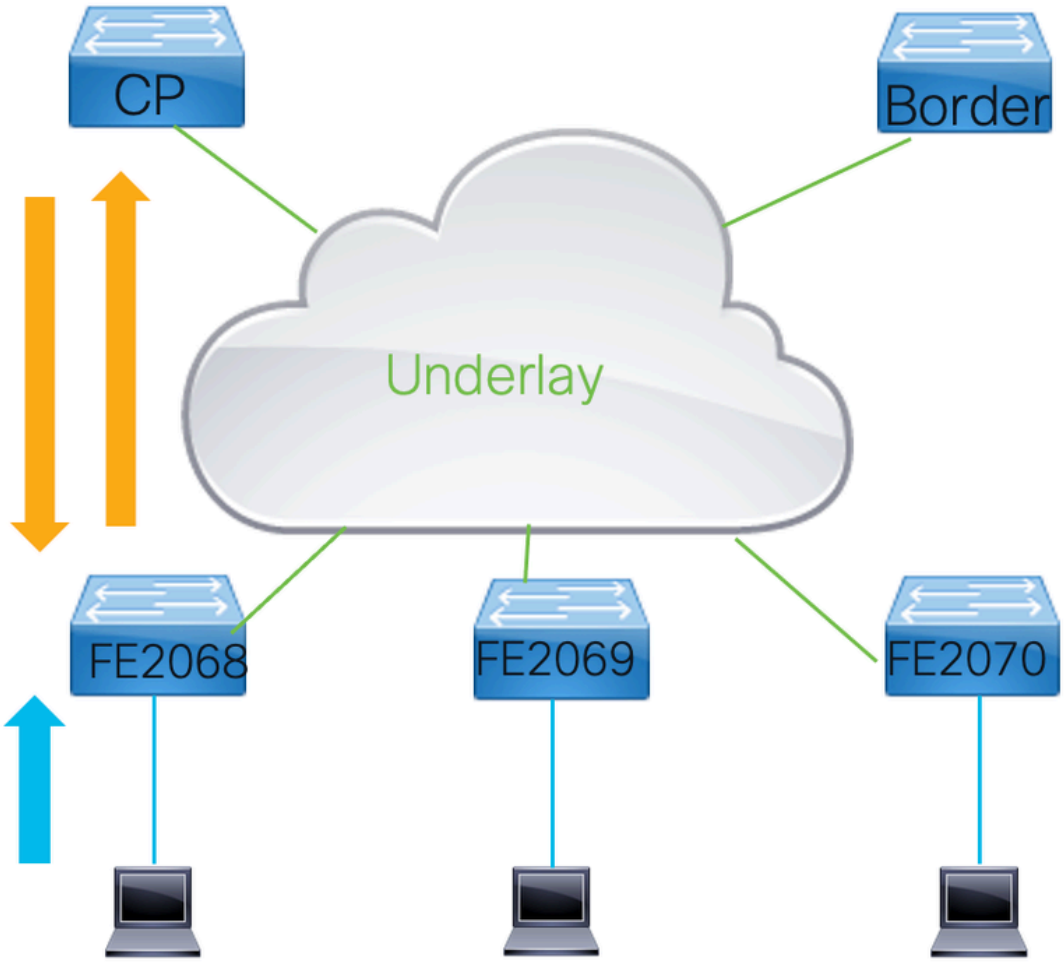
LISP VXLAN 패브릭을 통해 트래픽을 전달하려면 대상의 RLOC를 확인해야 합니다. LISP VXLAN 패브릭 내에서 이 작업은 맵 캐시를 사용하여 수행되며, 이 맵 캐시에서 패브릭 디바이스의 FIB(Forwarding Information Base)에 정보를 입력합니다.

LISP VXLAN 패브릭에서는 데이터 신호로 인해 맵 캐시가 트리거됩니다.

- 이는 트래픽이 CPU로 전달되고 CPU가 컨트롤 플레인 노드에 대한 맵 요청을 생성하여 해당 EID에 대한 프레임을 전송해야 하는 RLOC 정보를 쿼리한다는 것을 의미합니다.
- 맵 요청을 받은 제어 계획은 이 EID와 연결된 라우팅 로케이터 정보를 제공하거나 부정적인 맵 응답을 다시 보냅니다.
- 부정적인 맵 응답을 보낼 때 제어 평면 노드는 요청된 EID가 알려지지 않았음을 나타내는 것만이 아니라 이 EID가 속하는 EID의 전체 블록을 제공하므로 등록이 필요하지 않습니다.

컨트롤 플레인 노드의 map-reply 내부 정보를 사용하여 map-cache가 업데이트됩니다.

- 맵 응답의 TTL은 일반적으로 24시간입니다. (부정적인 맵의 경우 - 일반적으로 15분).
- Ethernet EID의 경우, negative map-replies는 map-cache에 배치되지 않습니다. 이 작업은 레이어 3 인스턴스에만 수행됩니다.



2.1 이더넷 맵 캐시

show lisp instance-id <instance> map-cache 명령을 사용하여 이더넷 map-cache 표시

```
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        -
```

이 명령은 확인되었을 원격 MAC 주소 항목을 표시합니다.

- 이더넷 인스턴스 트래픽에 대한 맵 캐시 항목을 트리거하려면 알 수 없는 대상으로 전송해야 합니다.
- 그러면 패브릭 디바이스에서 LISP를 통해 이를 해결하려고 시도합니다.
- 맵 응답을 통해 학습되면 맵 캐시에 저장되며, 레이어 2 목적지로 향하는 후속 프레임은 학습된 Routing Locator로 직접 전송됩니다.

선택적으로 레이어 2 인스턴스에서는 BUM 트래픽의 플러드를 사용합니다.

- LISP/VXLAN은 오버레이 기술을 사용하므로 기본적으로 트래픽을 플러딩하지 않지만 GRT(Underlay Network)에서 레이어 2 프레임을 플러딩할 수 있는 IP Multicast 그룹을 구성할 수 있습니다.

브로드캐스트 언더레이 그룹 주소 표시

```
<#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 맵 캐시

레이어 3 인스턴스의 경우 맵 캐시 정보는 CPU에 트래픽을 전송하여 신호를 보내는 이더넷 빌드 정보와 유사합니다.

- 그러나 레이어 3 패킷의 경우 CPU에만 적용되어 이 설정이 필요한 시점을 알립니다. 이 작업은 구성된 map-cache 명령에 의해 수행됩니다. IPv4의 경우 0.0.0.0/0, IPv6의 경우 ::0/0입니다.
- 경계 노드에서 이 맵 캐시 항목의 컨피그레이션은 신중하게 수행해야 합니다. border node가 이 map-cache 0.0.0.0/0 또는 ::0/0 map-cache 엔트리로 구성된 경우 패브릭 외부로 라우팅하는 대신 패브릭을 통해 알 수 없는 대상을 확인하려고 시도합니다.

맵 캐시 컨피그레이션 표시

<#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 및 ::/0 map-request를 사용하면 map-cache에서 map-cache 항목이 "send-map-request" 작업과 함께 구성됩니다. 이를 적중하는 트래픽은 map-requests를 트리거합니다. 맵 캐시 엔트리는 최장 일치(longest-match)를 기반으로 작동하는 FIB에 넣기 때문에, 특정 엔트리에

도달하지 않는 모든 라우팅된 IP 트래픽에 적용됩니다.

- 첫 번째 패킷이 삭제되는 것을 방지하기 위해 지원되는 플랫폼에서 표시된 작업은 send-map-request + encapsulate to proxy ETR입니다.
  그러면 알 수 없는 대상에 대한 첫 번째 패킷이 map-request를 트리거할 뿐만 아니라 패킷이 프록시-etr로 전달됩니다(있는 경우).

<#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

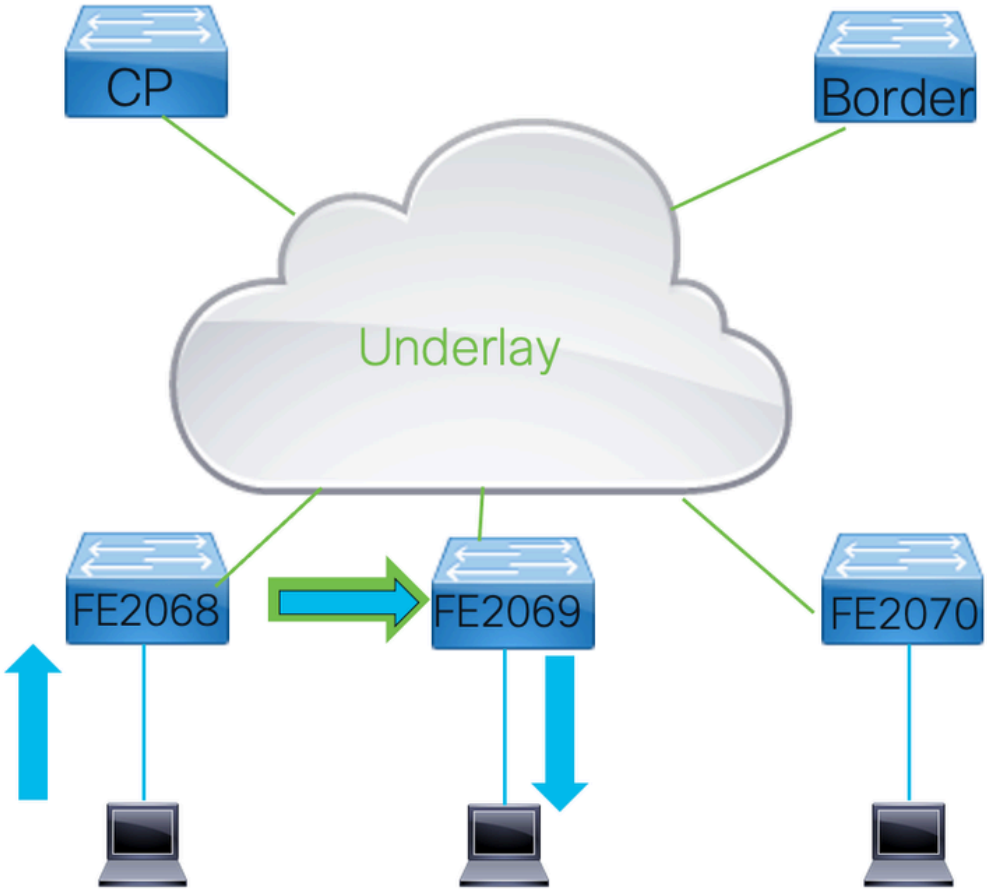
Locator	Uptime	State	Pri/Wgt	Encap-IID
172.30.250.44				

```
  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
```

이 출력에는 몇 개의 항목이 표시됩니다.

- 이 출력의 10.48.13.0/24 및 172.24.2.2/32은 map-reply를 통해 학습되고 완성됩니다. 이러한 대상에 대한 트래픽은 캡슐화되어 각 로케이터로 전달됩니다.
- 172.28.0.0/14은 수신된 음성 맵 응답과 반환된 IP 주소 블록의 예입니다. 이 서브넷에 대한 트래픽은 이 항목이 맵 캐시에 있는 한 맵 요청을 트리거하지 않습니다.

패브릭을 통한 트래픽 포워딩



3.1 레이어 2 또는 레이어 3 포워딩

LISP/VXLAN 패브릭의 트래픽은 레이어 2 또는 레이어 인스턴스를 통해 전달될 수 있습니다.

- 사용되는 인스턴스는 프레임의 대상 MAC 주소에 따라 결정됩니다.
- 어떤 MAC 주소로든 전송되는 프레임(스위치에 등록된 프레임 이외의 주소)은 레이어 2를 사용합니다. 패킷의 대상이 스위치인 경우 레이어 3을 통해 전달됩니다.
- 이는 Catalyst 9000 Series 스위치를 통한 일반 포워딩에 적용되는 로직과 동일합니다.

3.2 레이어 2 포워딩

LISP VXLAN 패브릭을 통한 레이어 2 전달은 레이어 2 대상 MAC 주소를 기반으로 수행됩니다. 원격 대상은 이그레스 인터페이스 L2LI0을 사용하여 MAC 주소 테이블에 삽입됩니다.

로컬 및 원격 레이어 2 인터페이스 표시

```
<#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
```

알 수 없는 대상의 경우 구성된 경우 언더레이에서 구성된 IP 멀티캐스트 그룹을 통해 트래픽이 전송됩니다.

- 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트(선택적 멀티캐스트 플러드만 해당) 트래픽의 올바른 플러드를 보장하려면 언더레이에서 올바르게 작동하는 멀티캐스트 환경이 필요합니다.
- 이 멀티캐스트 언더레이 그룹을 통해 전송되는 트래픽은 VXLAN에서 캡슐화되어야 합니다.
- 다른 모든 에지는 멀티캐스트 그룹에 조인하고 트래픽을 수신하고 알려진 레이어 2 인스턴스에 대해 트래픽을 캡슐화 해제해야 합니다.

언더레이 IP 멀티캐스트 그룹 표시

<#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:
```

이 출력은 플러딩된 트래픽을 전송하도록 클라이언트가 구성된 패브릭의 다른 모든 에지에 대한

S,G 항목을 보여줍니다. 또한 이 Edge 디바이스의 Loopback0이 소스로 포함된 S,G 엔트리 하나가 표시됩니다.

언더레이 멀티캐스트 그룹을 통과하는 트래픽의 수신자 측에 대해 show ip mroute 명령은 L2LISP0.<instance>도 표시합니다.
이는 이 에지 디바이스가 플러딩된 트래픽의 캡슐화를 해제하고 해당 디바이스로 포워딩할 레이어 2 인스턴스를 나타냅니다
관련 인터페이스.

3.3 레이어 3 포워딩 정보

LISP VXLAN 패브릭을 구축할 때 트래픽이 전달되는 방식을 확인하려면 CEF를 확인하는 것이 중요합니다.

- LISP는 기존 라우팅 프로토콜과 달리 라우팅 테이블에 라우팅 방향을 삽입하지만 CEF와 직접 상호 작용하여 FIB를 업데이트합니다.

지정된 원격 대상의 경우 맵 캐시 정보에는 사용할 로케이터 정보가 포함됩니다.

로케이터 정보 표시

```
<#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)
```

맵 캐시에서 이 EID에 사용할 로케이터는 172.30.250.44입니다. 따라서 이 대상에 대한 트래픽은 캡슐화되어야 하며 외부 IP 헤더의 IP 대상 주소는 172.30.250.44입니다.

이 인스턴스에 사용된 VRF의 라우팅 테이블에서는 이 항목이 표시되지 않습니다.

<#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 출력은 LISP VXLAN 패브릭을 통한 전달에 대한 자세한 정보를 제공합니다.

- show ip cef 명령에 detail 키워드가 추가되면 캡슐화된 프레임을 전송할 목적지만 지정하지 않습니다.
- 이 출력의 이그레스 인터페이스는 LISP 0입니다.<instance>는 트래픽이 캡슐화되어 전송됨을 나타냅니다.

<#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
```

다음 홉으로 트래픽을 캡슐화하여 전송하므로, 다음 단계는 show ip cef <next hop>을 실행하여 패킷이 라우팅되는 이그레스 인터페이스를 확인하는 것입니다.

이그레스 인터페이스를 보려면 실행

<#root>

```
FE2067#

sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23
```

참고: ECMP(Equal Cost Multiple Path) 라우팅은 2가지 레벨로 가능합니다.

- 보급된 RLOC가 2개인 경우 오버레이에서 트래픽의 로드 밸런싱을 수행할 수 있으며, RLOC IP 주소에 도달하기 위한 중복 경로가 있는 경우 언더레이 네트워크에서 로드 밸런싱을 수행할 수 있습니다.
- UDP 목적지 포트가 4789로 고정되고 두 패브릭 디바이스 간의 모든 플로우에 대한 소스 및 목적지 IP 주소가 동일하기 때문에, 동일한 경로를 통해 라우팅되는 모든 패킷을 방지하기 위해 일부 유형의 편파 방지 메커니즘이 발생해야 합니다.
- LISP VXLAN의 경우 이는 외부 헤더에 있는 UDP 소스 포트이며 오버플로 네트워크의 다른 플로우에 대해 다릅니다.

3.4 패킷 형식

- LISP VXLAN 패브릭 내에서 모든 트래픽은 VXLAN에서 완전히 캡슐화됩니다. 여기에는 레이어 2 및 레이어 3 오버레이를 모두 지원할 수 있도록 전체 레이어 2 프레임이 포함됩니다. 레이어 2 프레임의 경우 원래 헤더가 캡슐화됩니다. 레이어 3 인스턴스를 통해 전송되는 프레임의 경우 더미 레이어 2 헤더가 사용됩니다.

<#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
```

LISP VXLAN 패브릭을 통해 전달된 프레임의 샘플 캡처에서 알 수 있듯이 vxlan 패킷 내부에는 완전히 캡슐화된 프레임이 있습니다. 레이어 3 프레임인 이더넷 헤더는 더미 헤더입니다.

VXLAN 헤더에서 VLAN Network Identifier(VLAN 네트워크 식별자) 필드는 프레임이 속하는 LISP 인스턴스 ID를 전달합니다.

- Group Policy ID(그룹 정책 ID) 필드를 통해 프레임 SGT 태그가 전달됩니다.
- 이는 패브릭의 인그레스(ingress)에 설정되며, 그룹 기반 정책 시행이 수행될 때까지 패브릭을 향해 전달됩니다.

인증 및 보안 적용

4.1 스위치 포트 인증

각 VLAN에 엔드포인트를 동적으로 할당하고 SGT 태그 인증을 할당할 수 있습니다.

- Dot1x/MAB/central webauth와 같은 인증 프로토콜을 구축할 수 있으며, 스위치에 특성을 다시 보내는 Radius 서버의 사용자 및 엔드포인트를 인증하고 권한을 부여하여 올바른 풀의 클라이언트/엔드포인트에 대한 네트워크 액세스와 올바른 네트워크 액세스 권한 부여를 허용합니다.

LISP VXLAN 패브릭에는 몇 가지 일반적인 radius 특성이 있습니다.

- Vlan 할당: 이 특성은 VLAN ID 또는 RADIUS 서버에서 스위치로의 이름으로 설정되며 엔드포인트는 특정 Layer 2/Layer 3 LISP 인스턴스에 할당할 수 있습니다.
- SGT 값: 이 특성은 SGT를 설정하고 이 SGT에 엔드포인트를 할당합니다. 이는 이 엔드포인트에 대한 그룹 기반 정책에 사용될 뿐만 아니라 이 엔드포인트에서 시작된 패브릭을 통해 전송되는 모든 프레임에 SGT 값을 할당합니다.
- 음성 권한 부여: 음성 디바이스는 음성 VLAN에서 작동합니다. 이렇게 하면 엔드포인트가 포

트에 구성된 음성 VLAN에서 트래픽을 보내고 받을 수 있는 음성 권한 부여가 설정됩니다. 이는 음성 및 데이터 트래픽을 각 VLAN에서 분리하기 위한 것입니다

- 세션 시간 초과: 다양한 엔드포인트에 세션에 대한 고유한 시간 제한이 있습니다. 클라이언트가 재인증해야 하는 빈도를 나타내기 위해 RADIUS 서버에서 시간 초과를 보낼 수 있습니다
- 템플릿: 일부 엔드포인트의 경우 올바르게 작동하려면 포트에 다른 템플릿을 적용해야 합니다. 포트에 적용해야 할 항목을 나타내는 템플릿 이름을 Radius 서버에서 보낼 수 있습니다

포트에 대한 인증 결과 확인 show access-session 명령을 사용합니다

<#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

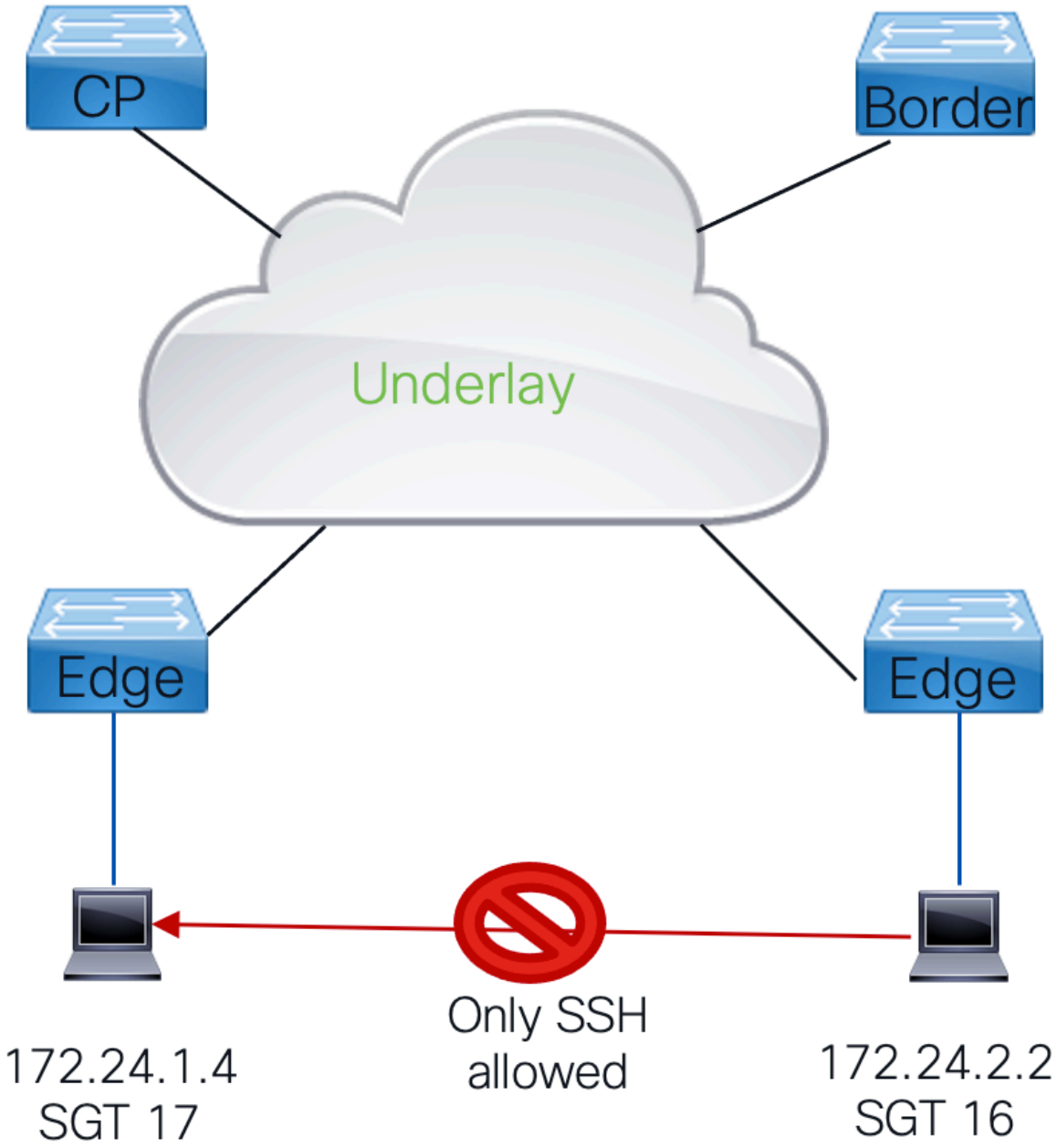
```
mab Authc
```

Success

다음 주요 필드에 유의하십시오.

- IPv4 및 IPv6 주소: 일반적으로 디바이스 추적을 통해 학습됩니다.
- 사용자 이름: 인증에 사용되는 사용자 이름입니다.
    - Dot1x의 경우 일반적으로 인증을 수행하는 사용자입니다.
    - MAB를 사용 할 때 이는 인증을 위해 사용자 이름 및 암호로 Radius에 전송 된 스테이션의 MAC 주소 입니다.
- 상태: 인증 및 인증 결과의 상태를 나타냅니다.
- 도메인: 일반 엔드포인트의 경우 Data 도메인이 되므로 트래픽은 포트에서 태그가 지정되지 않은 상태로 송수신됩니다. (음성 장치의 경우 이 설정을 음성으로 설정할 수 있음)
- 서버 정책: Vlan 할당 및 SGT 할당과 같은 Radius 서버의 정보가 표시되는 위치입니다
- 메서드 상태 목록: 다음은 실행된 메서드의 개요를 보여 줍니다.
    - 표준 dot1x는 MAB 전에 실행됩니다.
    - 엔드포인트가 EAPOL 프레임에 응답하지 않을 경우 방법은 mab로 장애 조치됩니다.
    - 그러면 dot1x가 실패한 것으로 표시됩니다.
    - MAB는 인증 성공 이 인증 할 수 있도록 관리 되었음을 나타냅니다. 인증 결과가 액세스 수락 또는 거부 인지 여부를 반영 하지 않습니다.

4.2 트래픽 정책 및 CTS(그룹 기반 정책)



LISP VXLAN 패브릭 내에서 CTS를 사용하여 트래픽 정책을 적용합니다.

- Group Based Policy 아키텍처는 Secure Group Tag를 기반으로 합니다.
- 패브릭 내부의 모든 트래픽은 모든 프레임에서 패브릭을 통해 전달되는 인그레스 및 SGT 태그에 할당됩니다.
- 이 트래픽이 패브릭을 벗어날 경우 트래픽 정책이 적용됩니다.
- 이 작업은 Group Based Policies(그룹 기반 정책)에서 수행되며, 이 정책은 패킷의 소스 및 목적지 그룹 태그를 Source-Destination SGT로 구성된 매트릭스에 대해 검사합니다. 여기서 결과는 어떤 트래픽이 허용되거나 허용되지 않을 것인지를 정의하는 SGACL입니다.
- Source-Destination SGT에 대한 매트릭스 내에 특정 일치가 없는 경우 정의된 기본 작업이 적용됩니다.

4.3 CTS 환경

그룹 기반 정책을 사용하여 운영하려면 패브릭 디바이스에 필요한 첫 번째 사항은 CTS pac를 가져오는 것입니다.

- 이 pac는 Cisco ISE의 RADIUS 프레임을 인증 하기 위해 반경 프레임 내에서 사용 됩니다. 이는 Radius 프레임 내에서 cts-pac-opaque 필드를 설정하는 데 사용됩니다.

CTS pac 정보 표시

```
<#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
```

CTS pac가 구성되고 유효한지 확인해야 합니다. 이 기능은 패브릭 디바이스에서 자동으로 새로 고쳐집니다.

참고: 수동으로 새로 고침을 트리거하려면 "cts refresh pac" 명령을 실행할 수 있습니다.

그룹 기반 정책이 작동하려면 환경 데이터를 다운로드하고 필요한 정책 정보를 다운로드합니다.

- 이 환경 데이터에는 스위치 자체에서 사용하는 CTS 태그와 Radius 서버에 알려진 모든 그룹 기반 정책 그룹의 테이블이 모두 포함되어 있습니다.

cts 환경 데이터 표시

```
<#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

그룹 기반 정책이 사용되는 경우 다운로드되는 정책은 디바이스에 적용해야 하는 로컬 엔드포인트가 있는 CTS 태그뿐입니다.

- IP 주소(또는 서브넷)에서 그룹 기반 정책 그룹으로의 매핑을 확인하려면 "show cts role-based sgt-map vrf <vrf> all" 명령을 사용할 수 있습니다.

VRF에 대해 알려진 모든 IP-SGT 정보 표시

<#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
```

이 출력은 지정된 VRF 및 그룹 기반 정책 연결에 대한 알려진 모든 IP 주소(및 서브넷)를 표시합니다.

- 볼 수 있듯이 그룹 기반 정책 그룹 17에 할당되고 로컬에서 소싱된 엔드포인트의 IP 주소 하나가 있습니다.

- 이는 포트에서 발생하는 인증의 결과이며, 결과에 해당 엔드포인트와 연결된 태그가 표시됩니다.
- 또한 스위치 자체 IP 주소를 강조 표시하며, 이는 디바이스 sgt 태그가 내부 소스로 할당됩니다.
- 그룹 기반 정책 태그는 컨피그레이션을 통해 또는 ISE에 대한 SXP 세션을 통해 할당할 수도 있습니다.

디바이스가 SGT 태그를 알게 되면 ISE 서버에서 연결된 정책을 다운로드하려고 시도합니다.

- show cts authorization entries 명령은 해당 항목이 다운로드되려고 시도되었을 때 그리고 연속으로 다운로드되었거나 다운로드되지 않은 경우 개요를 제공합니다.

참고: 정책이 변경될 경우 주기적으로 정책을 새로 고쳐야 합니다. ISE는 또한 변경 사항이 있을 때 새 정책을 다운로드하기 위해 스위치가 트리거되도록 CoA 명령을 푸시할 수 있습니다. 정책을 수동으로 새로 고치려면 "cts refresh policy" 명령을 실행합니다.

다운로드를 시도한 정책 개요 및 정책이 연속으로 다운로드되었거나 다운로드되지 않은 경우 표시

<#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

다운로드한 정책이 있는 경우 "show cts rolebased policies(cts 역할 기반 정책 표시)" 명령과 함께 표시할 수 있습니다.

<#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

이 명령은 디바이스에서 학습한 모든 정책을 표시합니다. ISE 서버에는 다른 그룹에 대해 더 많은 정책이 있을 수 있지만 디바이스는 엔드포인트를 알고 있는 정책만 다운로드하려고 시도합니다. 이는 귀중한 하드웨어 리소스를 절약합니다.

이 명령은 더 이상 특정 항목을 알 수 없는 트래픽에 적용될 기본 작업도 표시합니다. 이 경우

Permit IP이므로 테이블의 특정 엔트리와 일치하지 않는 모든 트래픽은 통과를 허용해야 합니다.

show cts rbacl <name>을 실행하여 다운로드된 RBACL의 정확한 내용에 대한 자세한 내용을 확인합니다

<#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

이 경우 이 RBACL이 적용된 엔드포인트로 보낼 수 있는 트래픽은 22(SSH) 및 23(텔넷)을 향하는 tcp 패킷뿐입니다.

참고: RBACL은 한 방향으로만 작동합니다. 반환 트래픽에 정책이 없는 경우 기본 정책으로 시행됩니다. 패브릭을 인그레스(ingress)하는 트래픽은 시행되지 않으며 인그레스 노드에 알려진 SGT 태그와 함께 패브릭을 통해 전송됩니다. 패브릭을 떠날 때만 시행되며 해당 장치에 있는 정책에 시행됩니다. 일반적으로 이러한 정책은 동일하지만, 예를 들어 배포된 보안 정책에 따라 다른 정책을 정의할 수 있는 방화벽을 사용하여 CTS 도메인을 확장할 수 있습니다.

'cts 역할 기반 카운터 표시'를 실행하여 프레임이 삭제되었는지 여부를 확인합니다.

- 이 명령은 전체 스위치에 대한 누적 카운터를 표시합니다. 인터페이스당 equivelant 명령은 없

습니다.

<#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

이 개요에서는 스위치에서 이 경우 17에서 16으로, 16에서 17로 트래픽을 매칭할 수 있도록 알고 있는 모든 알려진 엔트리를 보여줍니다.

- **에 해당하는 다른 일치 항목에는 기본 작업이 적용되므로 예를 들어 18~16과 같은 트래픽이 발생할 경우 스위치에서 알려진 매트릭스와 일치하지 않고 기본 작업이 적용됩니다.

카운터는 누적되지만 트래픽이 삭제되면 좋은 표시를 제공합니다.

- 어떤 트래픽이 어떤 항목에 도달하는지 확인하기 위해 log 키워드를 ISE 서버에서 각 정책에 추가할 수 있습니다. 그러면 스위치가 이 항목에 도달하면 로그 메시지를 제공합니다.
- 이 작업은 기본 작업(* *) 또는 매트릭스의 특정 항목 중 하나에 대해 수행할 수 있습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.