The bridge to possible

SD Access: Troubleshooting the Fabric

Michel Peters, Technical Leader Engineering
SDA Solution Escalation Team

BRKTRS-3820

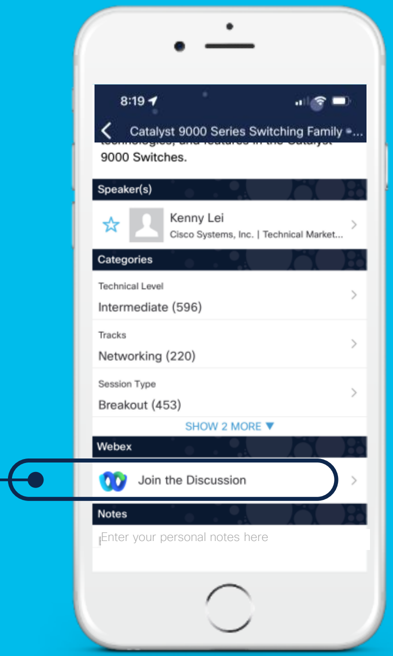
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

**Webex spaces will be moderated
until February 24, 2023.**

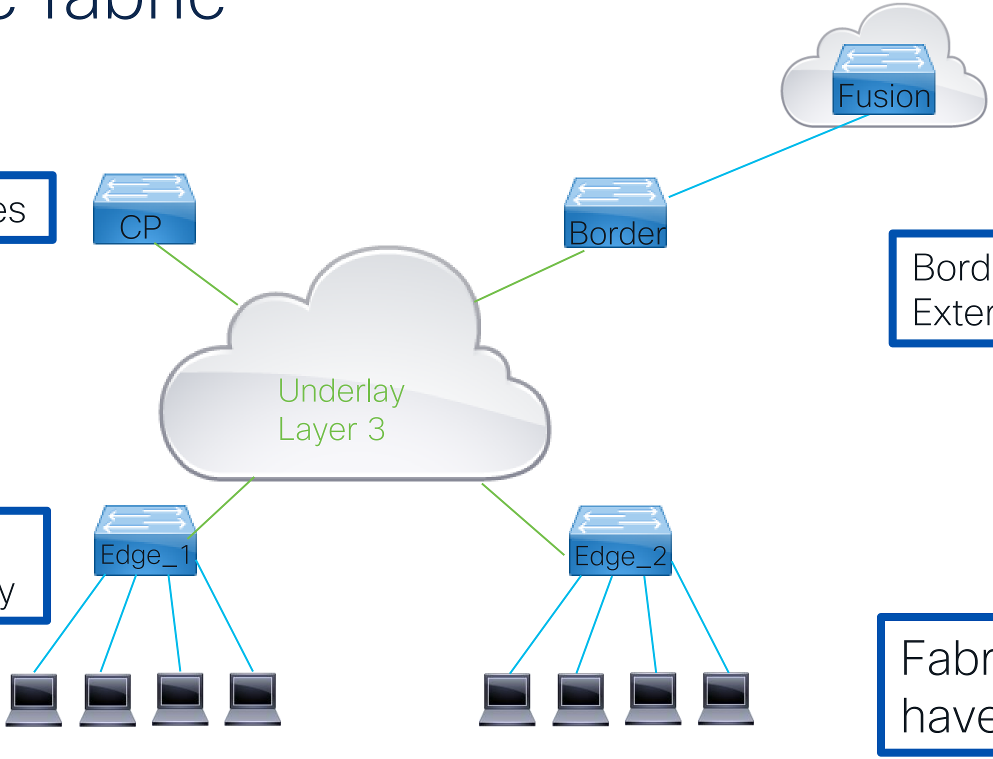
CISCO Live!

Agenda

- The Fabric
- Endpoint Registration
- Reaching Remote Endpoints
- Traffic Forwarding
- Secure Fabric
- Multicast

The Fabric

The basic fabric



Control Plane Nodes

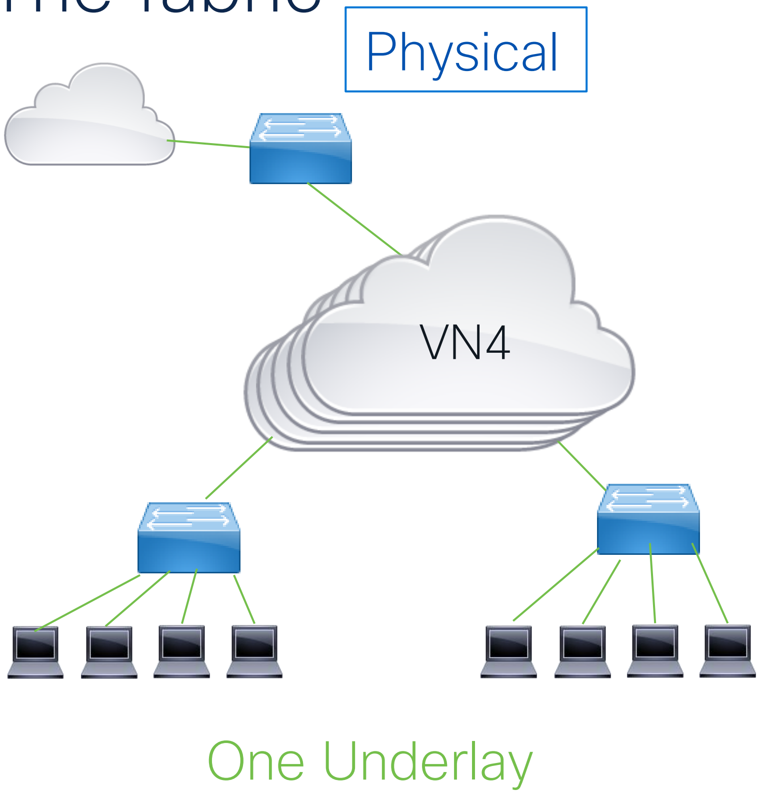
Fusion:
VRF leaking between VNs and underlay

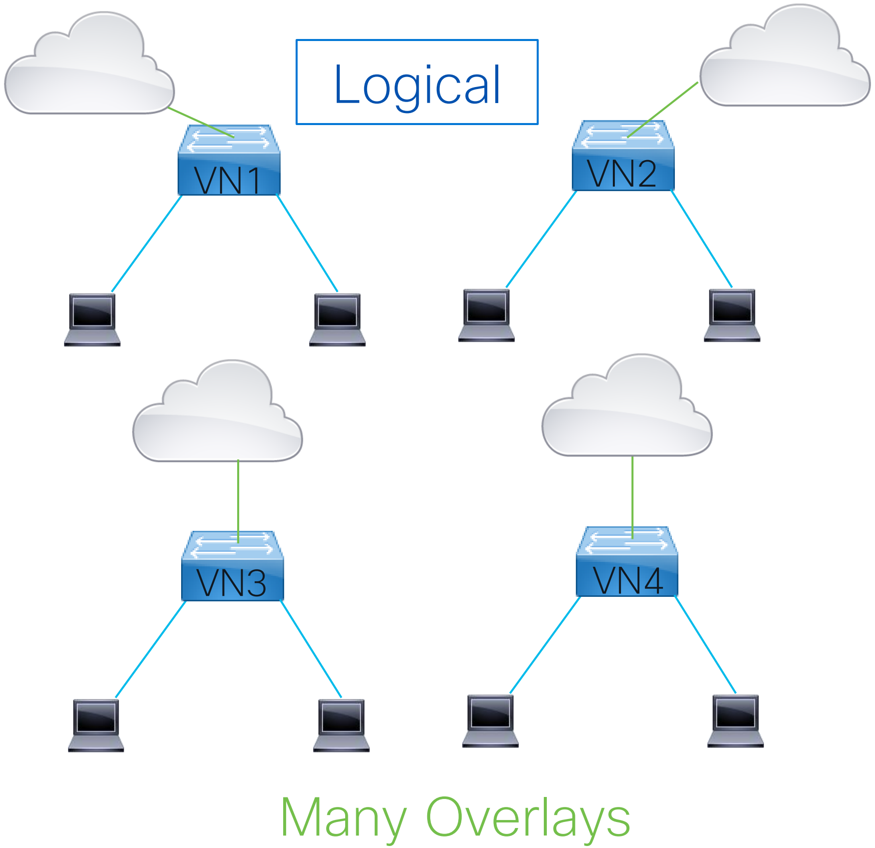
Borders:
External connectivity

Edges:
Endpoint Connectivity

Fabric devices can have multiple roles

The fabric


Physical
VN4
One Underlay


Logical
VN1
VN2
VN3
VN4
Many Overlays

SD Access Fabric Key Technologies

- Locator/ID Separation Protocol,
  Control plane protocol inside the fabric
- Cisco TrustSec,
  Segmentation, security inside the fabric
- Authentication,
  Assignment of endpoints and resources inside the fabric
- VXLAN,
  Dataplane encapsulation, used to tunnel traffic between Fabric Devices

LISP Overview

- LISP is a routing architecture, not just a routing protocol
- LISP creates a level of indirection by using two address spaces: “locators” (RLOC) and “endpoints” (EID)
- Advertise “locators” only in core routing. Removes endpoint subnets from routing tables in Global Routing Table.
- To get path information to end hosts, routers query Control Plane nodes for location information:

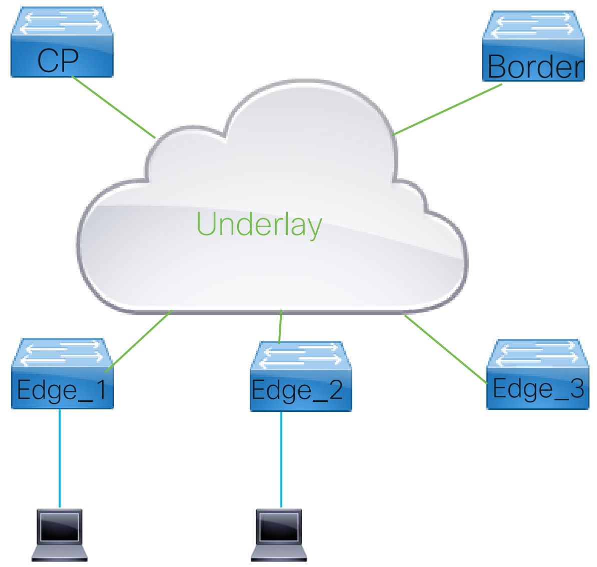
  DNS: who is www.cisco.com -> www.cisco.com is ip address …..
  LISP: where is 192.168.1.1 -> 192.168.1.0/24 is behind 10.1.1.1
- Traffic encapsulated to reach Remote, then de-encapsulated and send

LISP Device	SD Access	Function
ETR (Egress Tunnel Router)& PETR (Proxy ETR)	Edge Device & Border node	Connects a LISP site to a LISP capable core network. Registers EID prefixes with Map Server (MS). Decapsulates LISP packets received from LISP core. PETR works on behalf of non-LISP domain and provides LISP-non-LISP connectivity.
ITR (Ingress Tunnel Router) & PITR (Proxy Ingress Tunnel Router)	Edge Device and Border node	Responsible for forwarding local traffic to external destinations. Resolves RLOC for a given destination by sending Map-request to Map Resolver. Encapsulates traffic and send to fabric. Typically, this is a Access Layer Switch. PITR works on behalf of non-LISP domain and provides LISP-non-LISP connectivity.
XTR (X Tunnel Router)	Edge Device	When both ITR and ETR functions are handled by one router, it is called XTR. This is typical in practice.
MR (Map Resolver)	Control Plane Node	Responds to Map-requests from ITR. Map-requests will be replied with a (Negative) Map-reply or forwarded to appropriate ETR
MS (Map Server)	Control Plane Node	Registers EID space upon receiving Map-register messages from ETR. Updates Map Resolver with EID and RLOC data.
MSMR (Map Server Map Resolver)	Control Plane Node	When a device acts as both Map Server and Map Resolver, it is called MS MR. This is typical in practice.
EID (Endpoint ID)	IP pools/End Points	Endpoint Identifier. IP addresses. Hidden from core network routing table. RLOC acts next-hop to reach EID space.
RLOC (Routing Locator)	Fabric Devices	Routing Locator. Exists in global routing tables. Authoritative to reach EID space.

Endpoints Registrations

LISP operation, registering with Map Server

Instance	RLOC	EID (mac address)
8189	Edge_1	10f9.206d.e5b7
8189	Edge_2	10f9.206d.e5b6
4099	Edge_1	172.30.3.3/32
4099	Edge_2	172.30.3.2/32
4099	Border	10.48.91.128/25

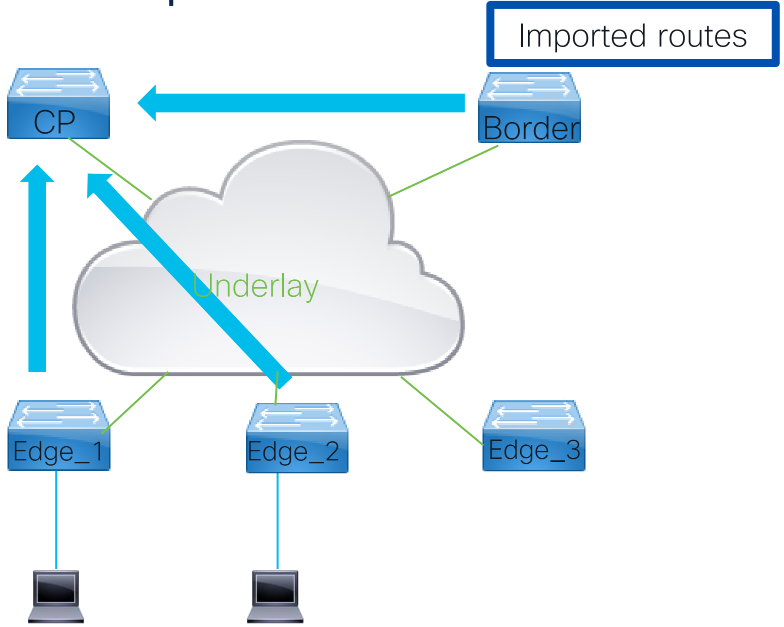


- Fabric devices dynamically learn IP and Mac addresses of attached devices to register with control plane node using map-register messages.
- 2 Instances in use:
  - Layer 2, one instance per Vlan/SVI
  - Layer 3, one instance per Virtual Network
- Control Plane nodes maintain central database mapping
- Wireless endpoints get signaled by WLC when using Fabric Enabled Wireless

LISP operation, registering with Map Server

Instance	RLOC	EID (mac address)
8189	Edge_1	10f9.206d.e5b7
8189	Edge_2	10f9.206d.e5b6
4099	Edge_1	172.30.3.3/32
4099	Edge_2	172.30.3.2/32
4099	Border	10.48.91.128/25

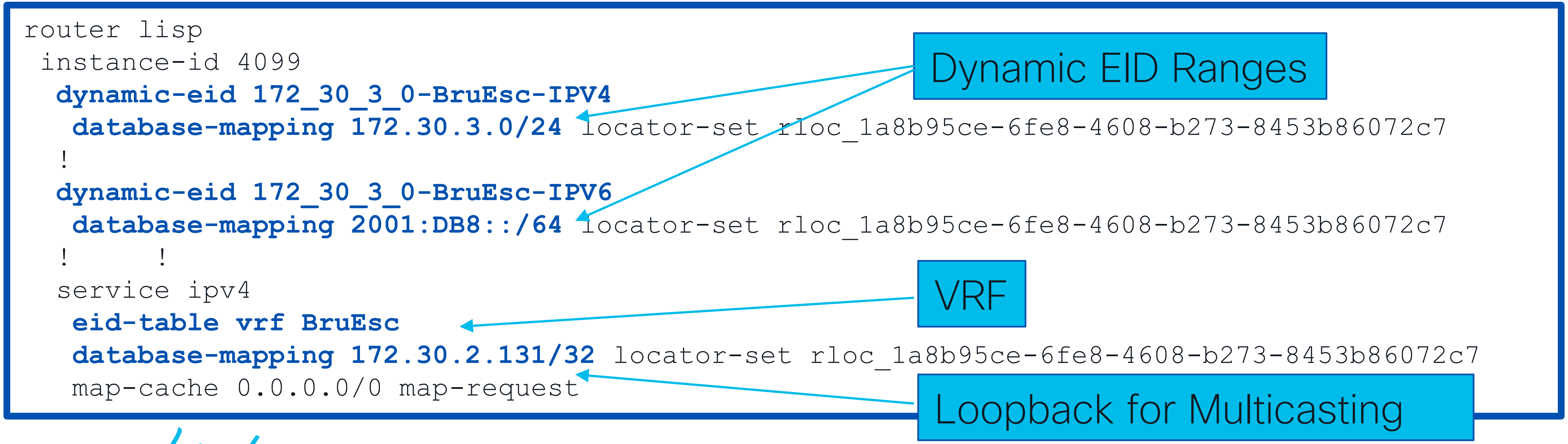
- Internal borders learn external routes and register with CP
- Edge devices learn IP and Mac address information
- Learned Endpoint Information gets registered with CP
- Control Plane maintains Database of all Endpoint Registration.
- Control Plane maintains TTL for registered entries
- Edge Devices will de-register if Endpoint disconnects
- Proxy ETR configuration pushed to Edge devices to allow default routing



Virtual Networks and LISP instances

- VRF's & LISP Instance ID form Virtual Networks
- Dynamic EID range dictate what Endpoints to learn
- Loopbacks for Multicasting purpose added directly into database for registering with Control Plane

```
Edge_1#sh ip vrf BruEsc
  Name                  Interfaces
  BruEsc                Lo4099
                        Vl1021
                        LI0.4099
                        Tu2
                        Vl1022
```



```
router lisp
 instance-id 4099
  dynamic-eid 172_30_3_0-BruEsc-IPV4
   database-mapping 172.30.3.0/24 locator-set rloc_1a8b95ce-6fe8-4608-b273-8453b86072c7
  !
  dynamic-eid 172_30_3_0-BruEsc-IPV6
   database-mapping 2001:DB8::/64 locator-set rloc_1a8b95ce-6fe8-4608-b273-8453b86072c7
  !     !
  service ipv4
   eid-table vrf BruEsc
   database-mapping 172.30.2.131/32 locator-set rloc_1a8b95ce-6fe8-4608-b273-8453b86072c7
   map-cache 0.0.0.0/0 map-request
```

Edge Configuration: SVI/VLAN Configuration

- Layer 3 Subnets and Layer 2 Pools deployed to all Edges is consistent throughout a fabric site
- SDA uses Anycast IP and Mac. All SVI configurations same on edges
- Connections between edges should be L3 to avoid mac-learning issues

```
Edge_1#sh run int vlan 1021
interface Vlan1021
 mac-address 0000.0c9f.f377
 vrf forwarding BruEsc
 ip address 172.30.3.1 255.255.255.0
 ip helper-address 10.48.91.148
 no lisp mobility liveness test
 lisp mobility 172_30_3_0-BruEsc-IPV4
```

```
Edge_2#sh run int vlan 1021
interface Vlan1021
 mac-address 0000.0c9f.f377
 vrf forwarding BruEsc
 ip address 172.30.3.1 255.255.255.0
 ip helper-address 10.48.91.148
 no lisp mobility liveness test
 lisp mobility 172_30_3_0-BruEsc-IPV4
```

LISP Database

```
Edge_1#sh ip arp vrf BruEsc 172.30.3.3
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.30.3.3             171  10f9.206d.e5b7  ARPA   Vlan1021
Edge_1#sh lisp instance-id 4099 ipv4 database 172.30.3.3/32
LISP ETR IPv4 Mapping Database for EID-table vrf BruEsc (IID 4099), LSBs: 0x1
172.30.3.3/32, dynamic-eid 172_30_3_0-BruEsc-IPV4,..
  Uptime: 3d15h, Last-change: 3d15h
  Locator       Pri/Wgt  Source     State
  172.30.233.6   10/10   cfg-intf   site-self, reachable
```

- LISP Database contains Endpoints that are present on the device. Contains dynamic EID, imported routes and configured entries
- Layer Endpoints learned via ARP/DHCP Snooping/Device Tracking
- Locator IP address is typically Loopback0 of Fabric Device in the Underlay network, needs to be reachable inside routing tables of other fabric devices
- Wildcard (*) when used will show all instances with lisp commands

Registration of L3 Endpoints with Map Server (CP)

- LISP Reliable Transport used with SDA. Using TCP in stead of UDP
- LISP Session Down can be due to failed connectivity or in case no EID's are to be registered (border node)
- Registration only authorized when LISP key matches with CP node
- Map register messages send to all CP nodes to register EID's

```
Edge_1#sh lisp session
Peer                          State      Up/Down        In/Out    Users
172.31.255.182:4342           Up         00:00:25       54/22     12
Edge_1#sh tcp brief
TCB            Local Address               Foreign Address              (state)
7EFDC4E8BA90  172.30.233.6.43136         172.31.255.182.4342            ESTAB
Edge_1#sh lisp instance-id 4100 ipv4 statistics  | sec Map-Register
    Map-Register records in/out:                        0/28
    Map-Server AF disabled:                             0
    Authentication failures:                            0
```

Layer 2 Endpoints

- Mac Addresses learned in Vlan registered with Control Plane
- SVI mac address is excluded
- Wireless Mac addresses signalled by WLC using map-notifications

```
Edge_1#sh mac ad vlan 1021
Vlan    Mac Address       Type        Ports
----    -----------       ---------   -----
1021    0000.0c9f.f377    STATIC      Vl1021
1021    10f9.206d.e5b7    STATIC      Te1/0/11
1021    701f.539b.0a75    STATIC      Vl1021
1021    10f9.206d.e5b6    CP_LEARN    L2LI0
Total Mac Addresses installed by LISP: REMOTE: 1
```

```
Edge_1#sh lisp instance-id 8189 ethernet database
LISP ETR MAC Mapping Database for EID-table Vlan 1021 (IID 8189), LSBs: 0x1
0000.0c9f.f377/48, dynamic-eid Auto-L2-group-8189, do not register, inherited from
default locator-set rloc_1a8b95
  Uptime: 3d23h, Last-change: 3d23h
    Locator          Pri/Wgt  Source     State
  172.30.233.6     10/10    cfg-intf   site-self, reachable
10f9.206d.e5b7/48, dynamic-eid Auto-L2-group-8189, inherited from default locator-set
rloc_1a8b95
  Uptime: 3d23h, Last-change: 3d23h
  Locator          Pri/Wgt  Source     State
  172.30.233.6     10/10    cfg-intf   site-self, reachable
```

Control Plane Node (MSMR)

- Control Plane Node acts as both Map Server and Map resolver (MSMR)
- Keeps database of all EID registrations for all AF(Ethernet/IPv4/IPV6)
- No synchronization between Control Plane nodes
- Show lisp site command gives overview of all IPv4/IPv6 registrations

```
Border_CP_1#sh lisp site instance-id 4099
LISP Site Registration Information
Site Name      Last      Up     Who Last                 Inst     EID Prefix
               Register         Registered               ID
site_uci       never     no     --                       4099     0.0.0.0/0
               never     no     --                       4099     172.30.2.128/25
               05:17:04  yes#   172.30.233.6:43136       4099     172.30.2.131/32
               00:00:07  yes#   172.30.233.1:4342        4099     172.30.2.132/32
               never     no     --                       4099     172.30.3.0/24
               00:00:07  yes#   172.30.233.1:4342        4099     172.30.3.2/32
               05:17:04  yes#   172.30.233.6:43136       4099     172.30.3.3/32
               never     no     --                       4099     172.30.4.0/24
```

Control Plane Node (MSMR) details on EID

```
Border_CP_1#sh lisp site 172.30.3.2/32 instance-id 4099
  EID-prefix: 172.30.3.2/32 instance-id 4099
    First registered:      4d23h
    Last registered:       00:00:01
    Origin:                Dynamic, more specific of 172.30.3.0/24
    Proxy reply:           Yes
    TTL:                   1d00h
    State:                 complete
    Extranet IID:          Unspecified
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.30.233.1, last registered 00:00:01, proxy-reply, map-notify
                      TTL 1d00h, no merge, hash-function sha1, nonce 0x7
                      state complete, no security-capability
                      xTR-ID 0x41DCA445-0xF8480845-0x4E7EB2E4-0xFA8E33CF
                      site-ID unspecified
      Locator         Local  State      Pri/Wgt  Scope
      172.30.233.1    yes    up          10/10   IPv4 none
```

Age of EID

Without proxy bit set CP would forward request to registering ETR

ETR Information

RLOC Information

Layer 2 Control Plane

- Registration history for Layer 3 EID usefull for roaming clients

```
Border_CP_1#sh 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
Feb  8 18:52:48.493      8189 TCP   No   No  172.31.254.20      -*172.30.149.5/32
Feb  8 18:52:48.796      4099 TCP   No   No  172.31.254.20      + 172.30.3.102/32
Feb  8 18:52:48.799      4099 TCP   No   No  172.31.254.20      + 172.30.3.151/32
Feb  8 18:52:49.330      8189 TCP   No   No  172.31.254.20      +*172.30.149.1/32
Feb  8 18:53:12.382      8189 TCP   No   No  172.31.254.20      -*172.30.149.1/32
Feb  8 18:53:13.197      8189 TCP   No   No  172.31.254.20      +*172.30.149.5/32
Feb  8 18:53:18.381      8189 TCP   No   No  172.31.254.20      -*172.30.149.5/32
Feb  8 18:53:19.222      8189 TCP   No   No  172.31.254.20      +*172.30.149.1/32
Feb  8 18:53:26.381      8189 TCP   No   No  172.31.254.20      -*172.30.149.1/32
Feb  8 18:53:27.221      8189 TCP   No   No  172.31.254.20      +*172.30.149.5/32
```

Layer 2 Control Plane

- Layer 2 registrations not under lisp site but under ethernet server

```
Border_CP_1#sh lisp instance-id 8189 ethernet server
LISP Site Registration Information
Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   8189     any-mac
               03:57:06  yes#   172.30.233.1:51300   8189     10f9.206d.e5b6/48
               10:12:16  yes#   172.30.233.6:43136   8189     10f9.206d.e5b7/48
```

```
Border_CP_1#sh lisp inst 8189 ethernet server 10f9.206d.e5b6 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
Jun  6 02:51:41.699      8189 TCP   No   No  172.30.233.1    + 10f9.206d.e5b6/48
Jun  6 03:51:49.913      8189 TCP   No   No  172.30.233.1    - 10f9.206d.e5b6/48
Jun  6 03:52:06.392      8189 TCP   No   No  172.30.233.1    + 10f9.206d.e5b6/48
```

Address Resolution Information

- Within Layer 2 Instances Address Resolution also registered with control plane
- Used for ARP rewrite to avoid Layer 2 flooding
- ARP Request snooped by Edge. Device Tracking changes destination mac address to known mac-address of destination

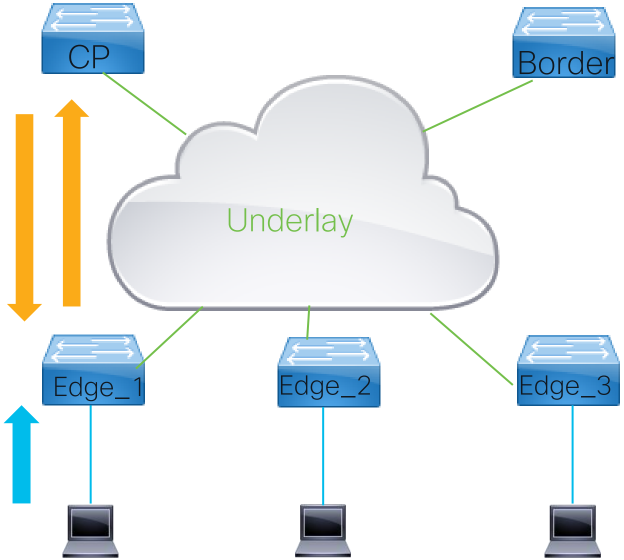
```
Border_CP_1#sh lisp instance-id 8189 ethernet server address-resolution
Address-resolution data for router lisp 0 instance-id 8189
L3 InstID    Host Address                                 Hardware Address
     4099    172.30.3.100/32                              a036.9f91.0937
     4099    172.30.3.101/32                              a036.9f86.e877
     4099    172.30.3.105/32                              548a.ba7c.4a14
     4099    172.30.3.113/32                              a036.9f86.e876
```

Reaching Remote Endpoints

LISP basic operation, resolving

Instance	RLOC	EID (mac address)
8189	Edge_1	10f9.206d.e5b7
8189	Edge_2	10f9.206d.e5b6
4099	Edge_1	172.30.3.3/32
4099	Edge_2	172.30.3.2/32
4099	Border	10.48.91.128/25

- Endpoint 1 sends packet towards Endpoint 2
- Packet send to CPU for signaling.
- Edge_1 initiates map request to CP node
- CP responds to Edge_1 with map-response containing RLOC information on behalf of Edge_2
- Edge_1 creates map-cache entry and is ready to forward traffic directly to Edge_2



Layer 3 Map Cache

- Map-requests triggered by hitting an Entry with send-map-request action

  map-cache 0.0.0.0/0 map-request

- External borders Providing Internet access do not have map-cache 0.0.0.0/0
- Responses from Control Plane Nodes are cached on fabric devices to build the map cache.
- Successful map-requests are cached with a default TTL of 1 day
  Time to Live can be changed with “etr map-cache-ttl” on edges/borders
- Negative map-requests have TTL of 15 minutes.
  Traffic forwarded to proxy-etr if configured (use-petr configuration)
- Control plane node returns largest possible block containing requested EID when sending Negative Map Reply. Action will be either send to Proxy ETR or forward native (eg, try normal routing)

Resolving Remote L3 Destinations

```
Edge_1#sh lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 7 entrie
0.0.0.0/0, uptime: 5d05h, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
0.0.0.0/1, uptime: 11:28:43, expires: 00:10:14, via map-reply, forward-native
  Encapsulating to proxy ETR
172.30.2.129/32, uptime: 11:30:36, expires: 00:29:39, via map-reply, complete
  Locator         Uptime    State  Pri/Wgt     Encap-IID
  172.31.255.182  11:30:36  up      10/10        -
172.30.3.0/24, uptime: 5d05h, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
172.30.3.2/32, uptime: 00:16:31, expires: 23:43:28, via map-reply, complete
  Locator       Uptime    State  Pri/Wgt     Encap-IID
  172.30.233.1  00:16:31  up      10/10        -
172.30.4.0/24, uptime: 5d05h, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
```

Triggers map-request and forwards to petr

NMR, send to petr

Encapsulate to RLOC

Map Cache shows EID range, source of cache entry and action to be taken.

Resolving Layer 2 Mac Addresses

- If traffic received with destination mac address not the SVI Mac Addres traffic will be Layer 2 switches
- Map request triggered by sending traffic to mac address not in mac table
- Layer 2 Flooding optional for BUM traffic using Multicast in Underlay

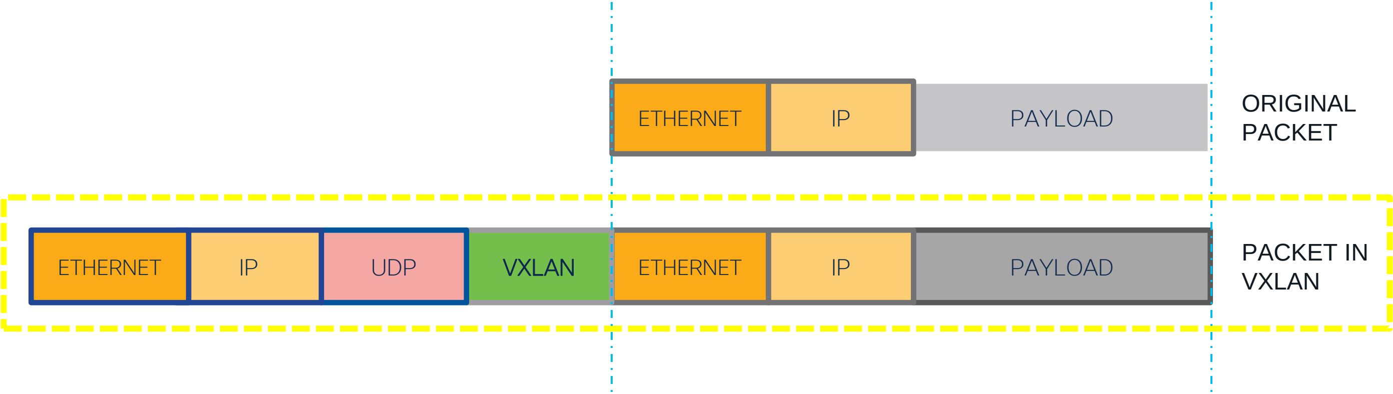
```
9300_1#sh mac add dynamic vlan 1021
Vlan    Mac Address       Type        Ports
----    -----------       ---------   -----
1021    10f9.206d.e5b6    CP_LEARN    L2LI0
Total Mac Addresses installed by LISP: REMOTE: 1
9300_1#sh lisp instance-id 8189 ethernet map-cache
LISP MAC Mapping Cache for EID-table Vlan 1021 (IID 8189), 1 entries
10f9.206d.e5b6/48, uptime: 1w4d, expires: 02:06:25, via map-reply, complete
  Locator        Uptime    State  Pri/Wgt     Encap-IID
  172.30.233.1   1w4d      up      10/10         -
```

CP_LEARN points to mac addresses from map-cache

Traffic Forwarding

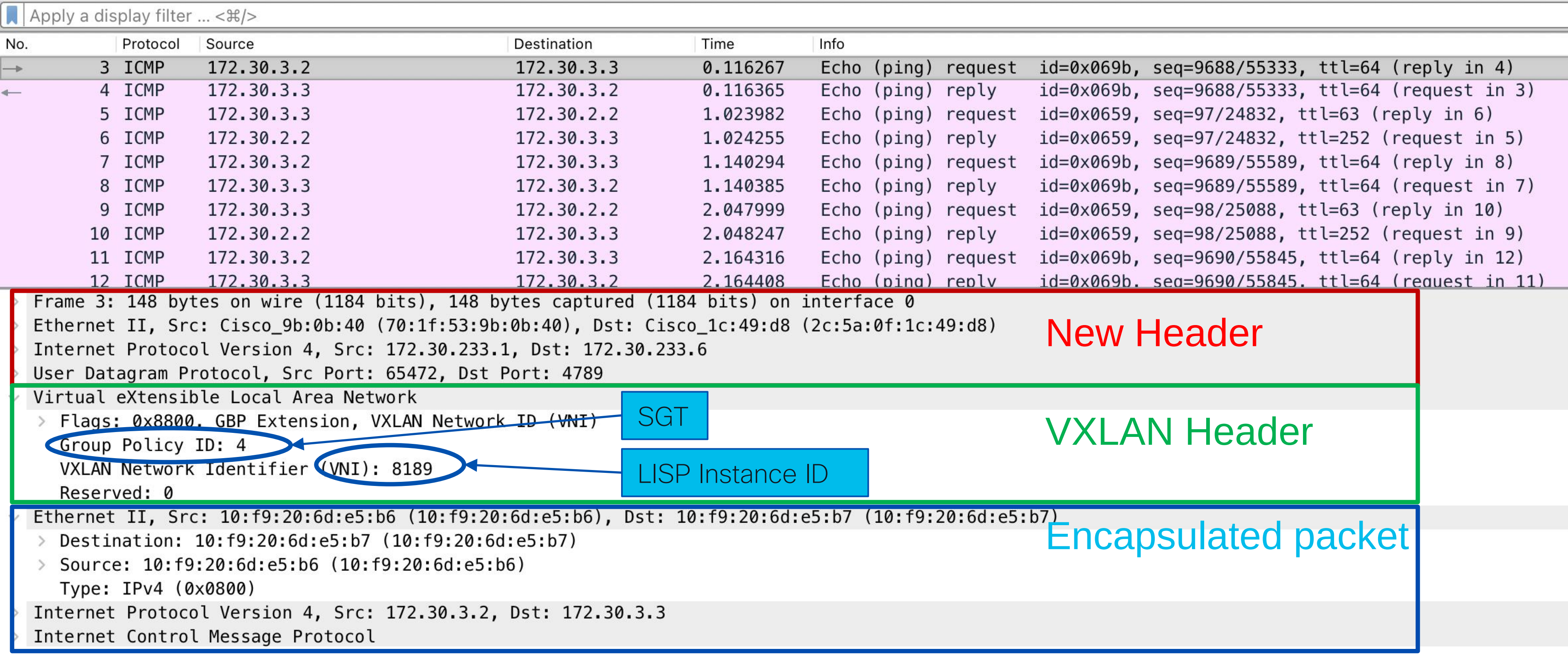
Data Plane

- In SD Access the entire packet is encapsulated
- VXLAN encapsulation used. Outer IP is RLOC
- VXLAN Network Identifier used for LISP instance ID
- Group Policy ID set to SGT



Supports L2 & L3 Overlay

Packet Encapsulation



```
Apply a display filter ... <⌘/>

No.       Protocol  Source              Destination         Time        Info
→    3    ICMP      172.30.3.2          172.30.3.3          0.116267    Echo (ping) request  id=0x069b, seq=9688/55333, ttl=64 (reply in 4)
←    4    ICMP      172.30.3.3          172.30.3.2          0.116365    Echo (ping) reply    id=0x069b, seq=9688/55333, ttl=64 (request in 3)
     5    ICMP      172.30.3.3          172.30.2.2          1.023982    Echo (ping) request  id=0x0659, seq=97/24832, ttl=63 (reply in 6)
     6    ICMP      172.30.2.2          172.30.3.3          1.024255    Echo (ping) reply    id=0x0659, seq=97/24832, ttl=252 (request in 5)
     7    ICMP      172.30.3.2          172.30.3.3          1.140294    Echo (ping) request  id=0x069b, seq=9689/55589, ttl=64 (reply in 8)
     8    ICMP      172.30.3.3          172.30.3.2          1.140385    Echo (ping) reply    id=0x069b, seq=9689/55589, ttl=64 (request in 7)
     9    ICMP      172.30.3.3          172.30.2.2          2.047999    Echo (ping) request  id=0x0659, seq=98/25088, ttl=63 (reply in 10)
    10    ICMP      172.30.2.2          172.30.3.3          2.048247    Echo (ping) reply    id=0x0659, seq=98/25088, ttl=252 (request in 9)
    11    ICMP      172.30.3.2          172.30.3.3          2.164316    Echo (ping) request  id=0x069b, seq=9690/55845, ttl=64 (reply in 12)
    12    ICMP      172.30.3.3          172.30.3.2          2.164408    Echo (ping) reply    id=0x069b, seq=9690/55845, ttl=64 (request in 11)

> Frame 3: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
> Ethernet II, Src: Cisco_9b:0b:40 (70:1f:53:9b:0b:40), Dst: Cisco_1c:49:d8 (2c:5a:0f:1c:49:d8)
> Internet Protocol Version 4, Src: 172.30.233.1, Dst: 172.30.233.6
> User Datagram Protocol, Src Port: 65472, Dst Port: 4789
v Virtual eXtensible Local Area Network
    > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
      Group Policy ID: 4
      VXLAN Network Identifier (VNI): 8189
      Reserved: 0
v Ethernet II, Src: 10:f9:20:6d:e5:b6 (10:f9:20:6d:e5:b6), Dst: 10:f9:20:6d:e5:b7 (10:f9:20:6d:e5:b7)
    > Destination: 10:f9:20:6d:e5:b7 (10:f9:20:6d:e5:b7)
    > Source: 10:f9:20:6d:e5:b6 (10:f9:20:6d:e5:b6)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.30.3.2, Dst: 172.30.3.3
> Internet Control Message Protocol
```

New Header

VXLAN Header

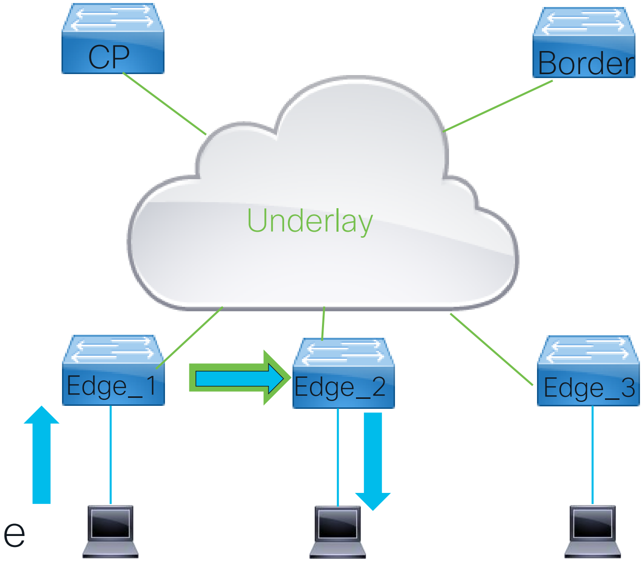
SGT

LISP Instance ID

Encapsulated packet

LISP basic operation, packet forwarding

Instance	RLOC	EID (mac address)
8189	Edge_1	10f9.206d.e5b7
8189	Edge_2	10f9.206d.e5b6
4099	Edge_1	172.30.3.3/32
4099	Edge_2	172.30.3.2/32
4099	Border	10.48.91.128/25



- Overlay traffic in SD Access is encapsulated in VXLAN and send between RLOC addresses
- Underlay network unaware of overlay topology
- Reachability to RLOC should exist in Route table
  - ipv4 locator reachability minimum-mask-length 32
  - ipv4 locator reachability exclude-default

Layer 2 or Layer 3 forwarding

- SDA supports both layer 2 and Layer 3 forwarding through fabric
- Traffic inside IP pool (vlan) will be encapsulated using Layer 2 instance
- Traffic destined outside IP pool send using Layer 3 instance id
- Layer 2 forwards traffic based on Destination Mac Address and L2 Map-cache
- Layer 3 forwarding decision based on Destination IP address
- Borders can have Layer 2 and Layer 3 handoffs.

LISP Remote forwarding

- Show ip route does not show full detail on forwarding
- Default route and remote entries would not show on edge with show ip route, only on border

```
Edge_1#sh ip route vrf BruEsc
..
Gateway of last resort is not set
      172.30.0.0/16 is variably subnetted, 7 subnets, 2 masks
C        172.30.2.131/32 is directly connected, Loopback4099
C        172.30.3.0/24 is directly connected, Vlan1021
L        172.30.3.1/32 is directly connected, Vlan1021
l        172.30.3.3/32 [10/1] via 172.30.3.3, 4d07h, Vlan1021
```

```
Border_CP_1#sh ip route vrf BruEsc
Gateway of last resort is not set
       172.30.3.0/24 [200/0], 6w4d, Null0
C        172.30.3.1/32 is directly connected, Loopback1021
l        172.30.3.2/32 [250/1], 07:20:46, Null0
l        172.30.3.3/32 [250/1], 13:35:56, Null0
```

Null routes on Border

LISP Remote forwarding, more detail

```
Edge_1#sh ip cef vrf BruEsc 172.30.3.2 detail
172.30.3.2/32, 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
  SC inherited: LISP generalised SMR - [enabled, inheriting, 0x7EFDC4E7A0A8 locks: 4]
  LISP source path list
    nexthop 172.30.233.1 LISP0.4099
  2 IPL sources [no flags]
  nexthop 172.30.233.1 LISP0.4099
```

- CEF gives accurate view of forwarding inside fabric device
- LISP subinterface is Instance-id , nexthop IP Address is RLOC of destination
- Show ip cef <nexthop> gives egress interface information in underlay for next hop.

LISP Remote forwarding, Layer 2

- Switches MATM table showing RLOC information for remote entries used for forwarding

```
9300_1#sh platform software fed switch active matm macTable vlan 1021
VLAN    MAC                     Type  Seq#    EC_Bi  Flags  *a_time  *e_time  ports
------------------------------------------------------------------------------------------------
1021    0000.0c9f.f377      0x8002         0  78007      64  0          0  Vlan1021
1021    10f9.206d.e5b6  0x1000001         0      0      64  0          0  RLOC 172.30.233.1 adj_id 220
1021    a036.9f91.0937     0x44202     9260      0      64  0          0  TenGigabitEthernet1/0/10
Total Mac number of addresses:: 3
*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR              0x1  MAT_STATIC_ADDR              0x2  MAT_CPU_ADDR                 0x4  MAT_DISCARD_ADDR             0x8
MAT_ALL_VLANS                0x10  MAT_NO_FORWARD              0x20  MAT_IPMULT_ADDR             0x40  MAT_RESYNC                  0x80
MAT_DO_NOT_AGE              0x100  MAT_SECURE_ADDR            0x200  MAT_NO_PORT                0x400  MAT_DROP_ADDR              0x800
MAT_DUP_ADDR               0x1000  MAT_NULL_DESTINATION      0x2000  MAT_DOT1X_ADDR            0x4000  MAT_ROUTER_ADDR           0x8000
MAT_WIRELESS_ADDR         0x10000  MAT_SECURE_CFG_ADDR      0x20000  MAT_OPQ_DATA_PRESENT     0x40000  MAT_WIRED_TUNNEL_ADDR   0x80000
MAT_DLR_ADDR             0x100000  MAT_MRP_ADDR            0x200000  MAT_MSRP_ADDR           0x400000  MAT_LISP_LOCAL_ADDR    0x800000
MAT_LISP_REMOTE_ADDR 0x1000000  MAT_VPLS_ADDR          0x2000000  MAT_LISP_GW_ADDR       0x4000000
```

LISP Remote forwarding, Layer 2 Flooding

- Layer 2 flooding relies on Underlay Multicast routing configuration
- Multicast configuration needs to be pushed through Lan Automation or manual configuration
- Multicast failures in Underlay may lead to issues with BUM traffic

```
9300_1#sh run | sec instance-id 8189
 instance-id 8189
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1021
   broadcast-underlay 239.0.17.3
   flood arp-nd
   flood unknown-unicast
   database-mapping mac locator-set rloc_1a8b95ce-6fe8-4608-b273-8453b86072c7
   exit-service-ethernet
  !
  exit-instance-id
```

LISP Remote forwarding, Layer 2 Flooding

- Every edge sending BUM traffic will be a source on the group

```
9300_1#sh ip mroute 239.0.17.3 172.30.233.6
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(172.30.233.6, 239.0.17.3), 1w5d/00:03:11, flags: FT
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet1/0/24, Forward/Sparse, 1w5d/00:03:04
9300_1#sh ip mroute 239.0.17.3 172.30.233.1
IP Multicast Routing Table
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(172.30.233.1, 239.0.17.3), 1w5d/00:02:06, flags: JT
  Incoming interface: TenGigabitEthernet1/0/24, RPF nbr 172.30.233.4
  Outgoing interface list:
    L2LISP0.8189, Forward/Sparse-Dense, 00:16:19/00:01:40
    L2LISP0.8190, Forward/Sparse-Dense, 1d00h/00:01:00
```

Entry used to encapsulate

De-encapsulating traffic towards L2 Instances

Secure Fabric

Secure Fabric

- Authentication provides the ability to authorize endpoints/devices and supply them with the required network access profiles
- Radius attributes in Access Accept can set :
  - Voice Domain authorization
  - Vlan Assignment
  - SGT Assignment
  - DACL
  - Templates
  - etc
- On Catalyst 9000 switches the Authentication is performed by Session Manager process(SMD). Traditional debugs wont show expected debugs for Authentication
- To enable traces: set platform software trace smd switch active R0 <facility> <level>
- To gather traces : show logging process smd

AAA server status

- Session Manager Process takes care of Authentication of endpoints (dot1x/mab)
- IOSd runs rest of AAA used on switches
- Cisco DNA Center pushes config for AAA to device and to ISE (if in use).
- Both IOS and Session Manager process send/receive traffic to Radius Server
- Ensure both SMD and IOSd report the server to be in Up state

```
Edge_2#show aaa server
RADIUS: id 1, priority 1, host 10.48.91.222, auth-port 1812, acct-port 1813, hostname dnac-radius_10.48.91.222
     State: current UP, duration 135026s, previous duration 12s
     Dead: total time 41s, count 3
     Platform State from SMD: current UP, duration 135054s, previous duration 29s
     SMD Platform Dead: total time 29s, count 2
```

Debugging/Tracing authentication

- Tracelogs can be quite verbose , redirect to file or filter to get the content needed

```
Edge_2#show logging process smd  | inc RADIUS
[radius] [22001]: (info): RADIUS: Send Access-Request to 10.48.91.222:1812 id 1812/244, len 497
[radius] [22001]: (info): RADIUS:  authenticator c1 72 6b f4 6c 99 09 61 - 4e 46 08 d4 5b 39 3f 2f
[radius] [22001]: (info): RADIUS:   Cisco AVpair       [1]    205  "cts-pac-opaque="
[radius] [22001]: (info): RADIUS:  User-Name           [1]     10  "michelpe"
[radius] [22001]: (info): RADIUS:   Cisco AVpair       [1]     21  "service-type=Framed"
[radius] [22001]: (info): RADIUS:  Framed-MTU          [12]     6  1468
[radius] [22001]: (info): RADIUS:  EAP-Message         [79]    15  ...
[radius] [22001]: (info): RADIUS:  Message-Authenticator[80]    18  ...
[radius] [22001]: (info): RADIUS:  EAP-Key-Name        [102]    2  *
[radius] [22001]: (info): RADIUS:   Cisco AVpair       [1]     43  "audit-session-id=84021EAC00001179"
[radius] [22001]: (info): RADIUS:   Cisco AVpair       [1]     14  "method=dot1x"
[radius] [22001]: (info): RADIUS:   Cisco AVpair       [1]     25  "client-iif-id=407463561"
[radius] [22001]: (info): RADIUS:  NAS-IP-Address      [4]      6  172.30.233.1
[radius] [22001]: (info): RADIUS:  NAS-Port-Id         [87]    26  "TenGigabitEthernet1/0/11"
[radius] [22001]: (info): RADIUS:  NAS-Port-Type       [61]     6  Ethernet                  [15]
[radius] [22001]: (info): RADIUS:  NAS-Port            [5]      6  50111
[radius] [22001]: (info): RADIUS:  Calling-Station-Id  [31]    19  "10-F9-20-6D-E5-B6"
[radius] [22001]: (info): RADIUS:  Called-Station-Id   [30]    19  "70-1F-53-9B-0B-0B"
```

Debugging/Tracing authentication -2

- Access-Accept received by Session Manager show the attributes to be applied to the end point authentication session
- Vlan send by using VLAN name

```
[radius] [22001]: (info): RADIUS: Received from id 1812/254 10.48.91.222:0, Access-Accept, len 450
[radius] [22001]: (info): RADIUS:  authenticator 23 fb 53 b0 bd f2 79 dc - 4a 79 5a e0 b2 07 ae fd
[radius] [22001]: (info): RADIUS:  User-Name            [1]     10  "michelpe"
[radius] [22001]: (info): RADIUS:  Class                [25]    54  ...
[radius] [22001]: (info): RADIUS:  Tunnel-Type          [64]     6  VLAN                      [13]
[radius] [22001]: (info): RADIUS:  Tunnel-Medium-Type   [65]     6  ALL_802                   [6]
[radius] [22001]: (info): RADIUS:  EAP-Message          [79]     6  ...
[radius] [22001]: (info): RADIUS:  Message-Authenticator[80]    18  ...
[radius] [22001]: (info): RADIUS:  Tunnel-Private-Group-Id[81]    20  "172_30_3_0-BruEsc"
[radius] [22001]: (info): RADIUS:  EAP-Key-Name         [102]   67  *
[radius] [22001]: (info): RADIUS:   Cisco AVpair        [1]     32  "cts:security-group-tag=00C8-01"
[radius] [22001]: (info): RADIUS:   Cisco AVpair        [1]     26  "cts:sgt-name=CL_Client_1"
[radius] [22001]: (info): RADIUS:   Cisco AVpair        [1]     15  "cts:vn=BruEsc"
```

Authentication Results

```
Edge_2#sh access-session interface te 1/0/11 details
            Interface:  TenGigabitEthernet1/0/11
               IIF-ID:  0x18496689
          MAC Address:  10f9.206d.e5b6
         IPv6 Address:  2001:db8::e078:8fae:fd0b:3def
         IPv4 Address:  172.30.3.116
            User-Name:  michelpe
          Device-type:  Microsoft-Workstation
          Device-name:  MSFT 5.0
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
       Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
```

IP information learned via Device Tracking

Authorization status

Voice(tagged),
Data (untagged)
Unknown(not authenticated

```
Server Policies:
             VN Value:  BruEsc
           Vlan Group:  Vlan: 1021
            SGT Value:  200
Method status list:
       Method           State
        dot1x           Authc Success
```

Policies send via Radius

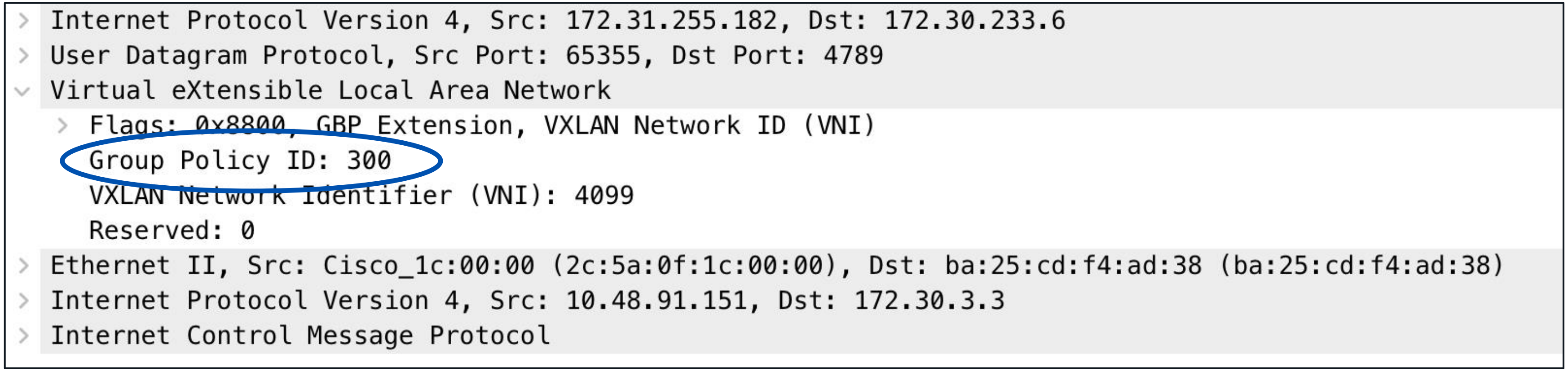
Method state success does not indicate auth state of client

Cisco TrustSec

- Every endpoint in the fabric gets assigned a Secure Group Tag
- Secure Group Tag transmitted in Policy Field in VXLAN header of encapsulated frames
- Fabric devices download CTS environment data from ISE server
- Fabric devices request policies for all known SGT's on that device
- Traffic being allowed/denied based upon SGT -> DGT mapping
- Traffic policy can contain optional SGACL or just deny/permit all
- Default action applied to all cells not populated.

Ingress Tagging

- Ingress Fabric Device tagging every frame with SGT Tag
- SGT tag carried through fabric inside Group Policy ID field in VXLAN header
- Mapping from IP to SGT occurs through authentication result, static config or SXP session.
- SGT tag set on ingress, carried through fabric, enforced when tag removed



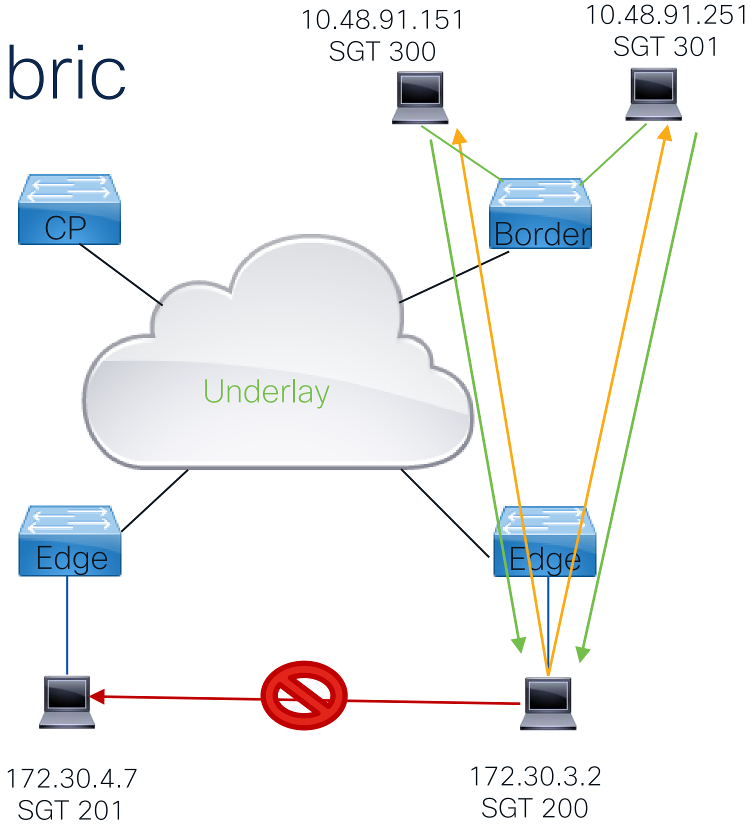
```
> Internet Protocol Version 4, Src: 172.31.255.182, Dst: 172.30.233.6
> User Datagram Protocol, Src Port: 65355, Dst Port: 4789
v Virtual eXtensible Local Area Network
    > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
      Group Policy ID: 300
      VXLAN Network Identifier (VNI): 4099
      Reserved: 0
> Ethernet II, Src: Cisco_1c:00:00 (2c:5a:0f:1c:00:00), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
> Internet Protocol Version 4, Src: 10.48.91.151, Dst: 172.30.3.3
> Internet Control Message Protocol
```

Security Policies inside the Fabric

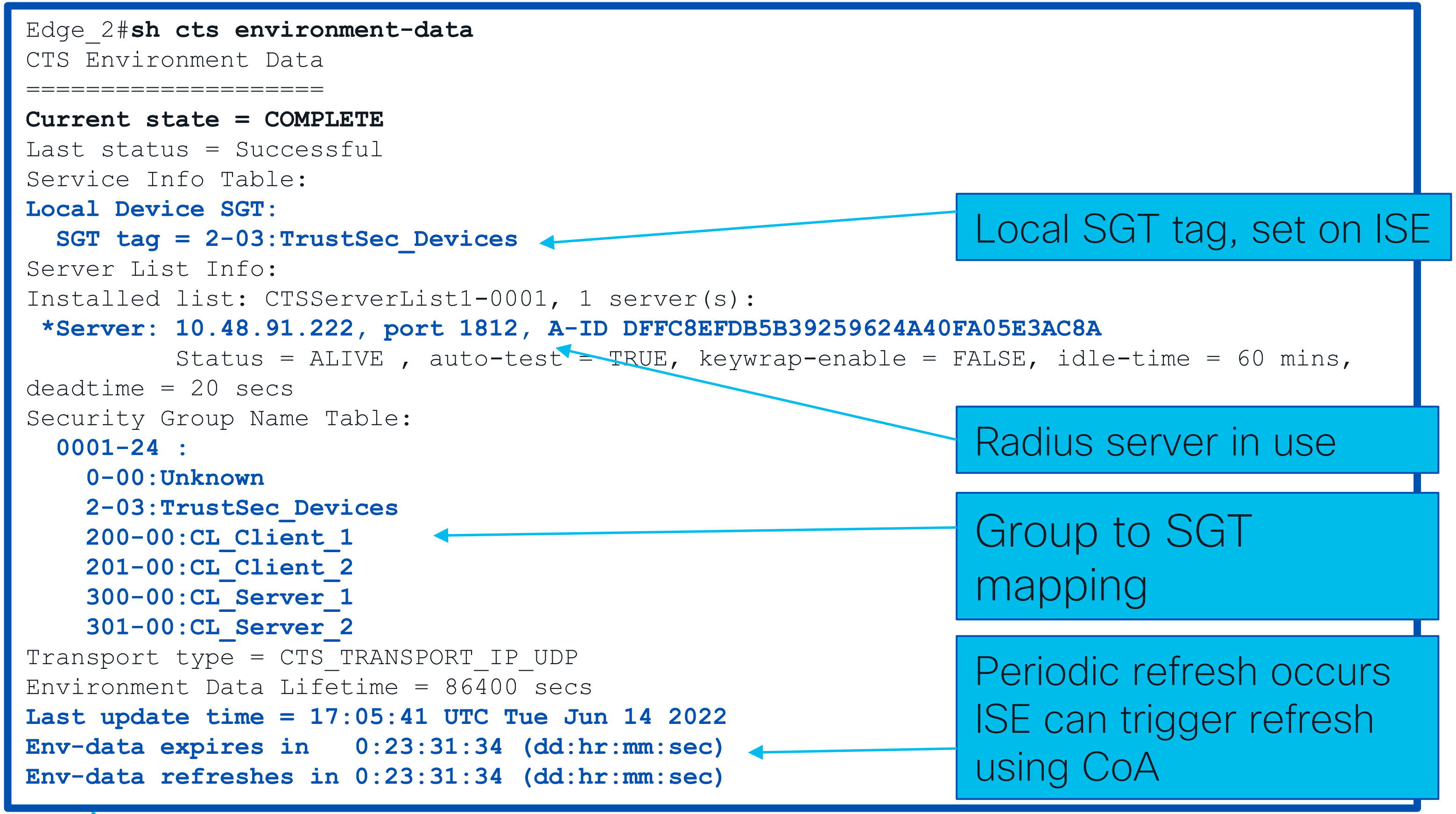
SGT	Endpoint
200	172.30.3.2
201	172.30.4.7
300	10.48.91.151
301	10.48.91.251

SRC	DST	Action
200	301	Permit ssh Deny any
200	300	Permit http(s) Deny any
200	201	Deny all
*	*	Permit All

- Policies are uni-directional, not bi-directional
- Border node enforces policies if tag stripped
- Use SXP or Static mappings on border to enforce policies and ensure tagging occurs towards fabric
- Policies enforced for routed and non-routed frames



CTS environment data



```
Edge_2#sh cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-03:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.91.222, port 1812, A-ID DFFC8EFDB5B39259624A40FA05E3AC8A
          Status = ALIVE , auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Security Group Name Table:
  0001-24 :
    0-00:Unknown
    2-03:TrustSec_Devices
    200-00:CL_Client_1
    201-00:CL_Client_2
    300-00:CL_Server_1
    301-00:CL_Server_2
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 17:05:41 UTC Tue Jun 14 2022
Env-data expires in   0:23:31:34 (dd:hr:mm:sec)
Env-data refreshes in 0:23:31:34 (dd:hr:mm:sec)
```

Local SGT tag, set on ISE

Radius server in use

Group to SGT mapping

Periodic refresh occurs ISE can trigger refresh using CoA

Problems downloading CTS enviroment?

- Check PAC on device and ISE
- Check ISE live logs for errors
- Re-set CTS credentials with cts credentials id
- Refresh pac with *cts refresh pac* confirm lifetime changed on both
- Refresh enviroment data with cts refresh enviroment-data
- Entire cts table only downloaded when new version available.

```
Edge_1#show cts pacs
AID: DFFC8EFDB5B39259624A40FA05E3AC8A
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: DFFC8EFDB5B39259624A40FA05E3AC8A
  I-ID: FCW2135G0AL
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 11:54:17 UTC Wed Jun 22 2022
PAC-Opaque:
000200B80003000100040010DFFC8EFDB5B39259624A40FA05E3
AC8A0006009C00030100B74B07EC9F302303F7DA9AEE1E7EBB24
00000136239AE5100093A8063C0997BC0371AAC105A77C6D0FD
415E9C5B31ED952C3ACDE42CBA076C57B20634171 3D49E7AB92D
B50DFD08B44D5ABBE7ABFD89068C7C510AFBB600CFE96FE28D0A
0EA2D7082748EF30AC4953B7EFC73B80D9E61B21F4608DDD4450
01E1003329DB16E10597922345DC2966691003C796A5635090B3
C5A459501825
Refresh timer is set for 5d19h
```

CTS IP to SGT Mapping

- All endpoints not assigned an SGT tag via Authentication or static configuration will belong to SGT 0 (unknown)
- SGT can be learned Locally on switch or via SXP sessions
- If mappings are not present in sgt-map table policies will not be downloaded

```
Edge_1#sh cts role-based sgt-map vrf BruEsc all
IP Address                      SGT     Source
============================================
172.30.3.2                      200     LOCAL
BN_1#sh cts role-based sgt-map vrf BruEsc all
IP Address                      SGT     Source
============================================
10.48.91.151                    300     CLI
10.48.91.251                    301     CLI
```

Endpoint IP assigned SGT 200 via 802.1x

Border learns entries via SXP or CLI

CTS Authorization Entries

```
Edge_1#show cts authorization entries
Authorization Entries Info
==========================
Peer name                 = Unknown-200
Peer SGT                  =  200-01:CL_Client_1
Entry State               = COMPLETE
Entry last refresh        = 18:43:51 UTC Wed Jun 8 2022
SGT  policy last refresh = 18:43:51 UTC Wed Jun 8 2022
SGT policy refresh time   = 86400
Policy expires in    0:21:41:21 (dd:hr:mm:sec)
Policy refreshes in 0:21:41:21 (dd:hr:mm:sec)
Retry_timer                   = not running
Cache data applied            = NONE
Entry status                  = SUCCEEDED
AAA Unique-ID                 = 7531
```

- For every known SGT mapping on Fabric device an Authorization entry is there regardless if there is or is not a policy associated with it
- Entries can be refreshed with cts refresh policy
- SGT groups should be present on ISE to succeed. Undefined SGTs will show failed

CTS Policies

- Policies downloaded for SGTs with local presence
- Enforcement occurs on Egress mapping SGT inside VXLAN packet to Destination SGT
- All other traffic will hit a * * policy
- RBACL names are appended with a version,
  Ex: AllowWev-00 is version 00 of RBACL name NoTelnet

```
BN_1#sh cts role-based permissions to 300
IPv4 Role-based permissions from group 200 to group 300:CL_Server_1:
AllowWeb-00
IPv4 Role-based permissions from group 201 to group 300:CL_Server_1:
AllowWeb-00
BN_1#sh cts rbacl AllowWeb
CTS RBACL Policy
  name    = AllowWeb-00
  RBACL ACEs:
    permit tcp dst eq 80
    permit tcp dst eq 443
    permit udp dst eq 443
    deny ip
```

Monitoring SGT traffic

- Counters are accumulative per device, not per port
- Traffic not hitting a more specific entry will hit * *
- Different Column for Software and Hardware enforcement

```
BN_1#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
*       *       0          0          4965       312090     0          0
200     300     0          0          0          0          0          0
201     300     0          15         0          146        0          0
200     301     0          0          0          0          0          0
201     301     0          0          0          195        0          0
Edge_1#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
*       *       0          0          13296      21927      0          0
200     201     0          13         0          0          0          0
```

Useful debugs

- To diagnose issues with mapping or download from ISE

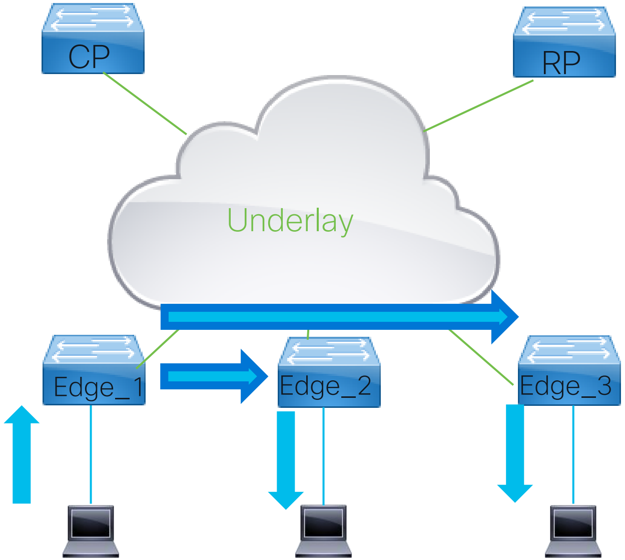
  Debug cts all
  Debug rbm all

- CTS runs on top of IOSd, not part of SMD.
  Radius debugs will show exchanges with ISE

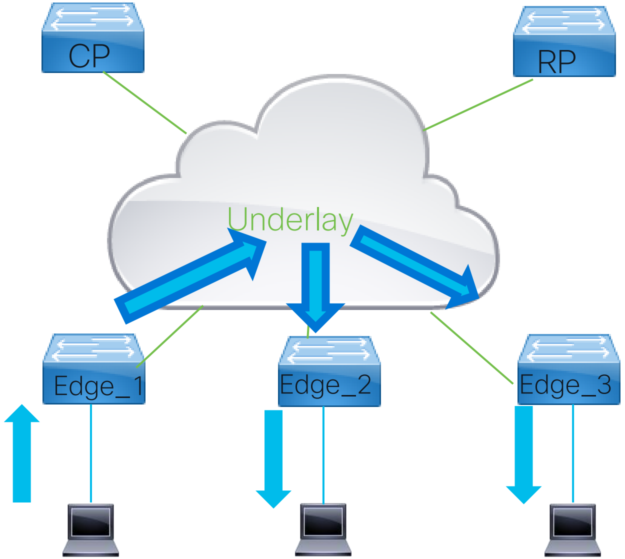
- Hardware mappings of IP to SGT:
  show cts role-based sgt-map platform

Multicasting

Multicast Overview, 2 modes of operation



Head End Replication
One packet per destination



Native Multicast
One packet, multilple destinations

RPF Resolution within SDA

Local

```
Edge_1#show ip rpf vrf CiscoLive 192.168.1.100
RPF information for ? (192.168.1.100)
  RPF interface: Vlan1022
  RPF neighbor:192.168.1.100 directly connected
  RPF route/mask: 192.168.1.100/32
  RPF type: unicast (lisp)
  distance-preferred lookups across tables
  RPF topology: ipv4 multicast base
```

Remote

```
Edge_1#show ip rpf vrf CiscoLive 192.168.1.101
RPF information for ? (192.168.1.101)
  RPF interface: LISP0.4100
  RPF neighbor: ? (172.31.255.111)
  RPF route/mask: 192.168.1.101/32
  RPF type: unicast ()
  distance-preferred lookups across tables
  RPF topology: ipv4 multicast base
```

- In SDA RPF resolution needs interaction with LISP to determine RPF path
- RPF resolution for Sources reachable through the fabric:
  - RPF Interface LISP 0.<instance ID>
  - RPF Neighbor, RLOC IP address of Fabric Device source resides
- If RPF cannot be resolved, multicast traffic will not be forwarded

Head End Replication Mode, FHR

```
Edge_1#show ip mroute vrf CiscoLive 239.100.100.100
IP Multicast Routing Table
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.100.100.100), 02:29:39/stopped, RP 192.168.200.1, flags: SPF
  Incoming interface: LISP0.4100, RPF nbr 172.31.255.28
  Outgoing interface list: Null
(192.168.1.100, 239.100.100.100), 02:29:39/00:02:35, flags: FT
  Incoming interface: Vlan1022, RPF nbr 0.0.0.0
  Outgoing interface list:
    LISP0.4100, 172.31.255.110, Forward/Sparse, 00:10:30/00:02:54
    LISP0.4100, 172.31.255.111, Forward/Sparse, 01:09:35/00:02:46
```

1 copy per receiver

- First Hop Router sending traffic through VXLAN to both RLOCs with receivers
- All edge nodes join the *.G pointing to the RP RLOC IP address
- Traffic from Sender gets encapsulated into VXLAN , similar to Unicast traffic

Head End Replication Mode, Egress Router

- On receiver side the packet is de-encapsulated and sent to the receiver

```
Edge_3#show ip mroute vrf CiscoLive 239.100.100.100
(*, 239.100.100.100), 05:14:22/stopped, RP 192.168.200.1, flags: SJC
  Incoming interface: LISP0.4100, RPF nbr 172.31.255.28
  Outgoing interface list:
    Vlan1022, Forward/Sparse, 01:52:18/00:02:13
(192.168.1.100, 239.100.100.100), 01:29:05/00:02:09, flags: JT
  Incoming interface: LISP0.4100, RPF nbr 172.31.255.109
  Outgoing interface list:
    Vlan1022, Forward/Sparse, 01:29:05/00:02:13
Edge_3#show ip igmp vrf CiscoLive groups
Group Address    Interface                Uptime    Expires   Last
239.100.100.100  Vlan1022                 01:53:01  00:02:26  192.168.1.101
Edge_3#show ip igmp snooping groups
VLAN      Group                    Type        Version      Port List
-----------------------------------------------------------------------
1022      239.100.100.100          igmp        v3           Gi1/0/1
```

RPF of (S,G) is RLOC of FHR

Ingress LISP Egress Vlan1022

IGMP join on Gi 1/0/1 triggered the join.

Native Multicast – First Hop Router - Overlay

- In overlay LISP interface is showing in Outgoing Interface List
- Using verbose keyword, the corresponding Underlay Group is shown
- Underlay group will be used to carry multicast traffic encapsulated in VXLAN
- Group calculated using Hash function, groups might use same underlay group

```
Edge_1#show ip mroute vrf BruEsc 239.100.100.100  172.30.3.100 verbose
IP Multicast Routing Table
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(172.30.3.100, 239.100.100.100), 00:04:54/00:01:58, flags: FTp
  Incoming interface: Vlan1021, RPF nbr 0.0.0.0
  Outgoing interface list:
    LISP0.4099, (172.30.233.6, 232.0.3.1), Forward/Sparse, 00:03:52/stopped, Pkts:0, p
      172.30.233.1, 00:03:52/00:02:33
```

Underlay Group used for distribution

Subscribers

Native Multicast – First Hop Router - Underlay

```
9300_1#sh ip mfib 232.0.3.1 172.30.233.6 verbose
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   HW Pkt Count/FS Pkt Count/PS Pkt Count   Egress Rate in pps
Default
 (172.30.233.6,232.0.3.1) Flags: K HW
   0x110  OIF-IC count: 0, OIF-A count: 1
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   1037/1/168/1, Other: 0/0/0
   Null0 Flags: RA A MA
   TenGigabitEthernet1/0/24 Flags: RF F NS
     CEF: Adjacency with MAC: 01005E000301701F539B0A400800
     Pkts: 0/0/0    Rate: 0 pps
```

Source IP is RLOC of edge

Null0 as ingress

Egress port

- In underlay network, the Overlay traffic is sent encapsulated in VXLAN
- Native Multicast relies on SSM configuration in Underlay being present and operational
- Ingress Interface showing as Null0 , encapsulated traffic originates on device

Native Multicast – Intermediate node- Underlay

```
Border_CP_1#sh ip mfib 232.0.3.1 172.30.233.6 verbose
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   HW Pkt Count/FS Pkt Count/PS Pkt Count   Egress Rate in pps
Default
 (172.30.233.6,232.0.3.1) Flags: K HW
   0xC0  OIF-IC count: 0, OIF-A count: 1
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   175/1/180/1, Other: 0/0/0
   GigabitEthernet5/0/47 Flags: RA A MA
   GigabitEthernet5/0/48 Flags: RF F NS
     CEF: Adjacency with MAC: 01005E0003012C5A0F1C49D80800
     Pkts: 0/0/0    Rate: 0 pps
```

- Intermediate node not joined the Overlay Multicast group
- Normal Multicast routing is occurring
- If node would join Overlay LISP decap would be added to OIL

Native Multicast – Egress Router

```
Edge_2#sh ip mfib 232.0.3.1 172.30.233.6 verbose
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   HW Pkt Count/FS Pkt Count/PS Pkt Count   Egress Rate in pps
Default
 (172.30.233.6,232.0.3.1) Flags: K HW
   0x102  OIF-IC count: 0, OIF-A count: 1
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   1038/1/180/1, Other: 0/0/0
   TenGigabitEthernet1/0/24 Flags: RA A MA
   Null0, LISPv4 Decap Flags: RF F NS
     CEF: OCE (lisp decap)
     Pkts: 0/0/0    Rate: 0 pps
```

- LISPv4 Decap interface showing traffic will be de-encapsulated
- Only groups/instances joined will have its traffic de-encapsulated and forwarded.

Native Multicast, Egress Router

- De-encapsulated traffic forwarded as per mroute table
- RPF neighbor in VRF points to RLOC of encapsulating device
- Flag I set, LISP Decap Refcnt Contributor
- IGMP snooping indicates what Layer 2 ports receive multicast traffic

```
Edge_2#show ip mrout vrf BruEsc  239.100.100.100 172.30.3.100 verbose
IP Multicast Routing Table
(172.30.3.100, 239.100.100.100), 00:03:20/00:02:39, flags: TI
  Incoming interface: LISP0.4099, RPF nbr 172.30.233.6, LISP: [172.30.233.6, 232.0.3.1]
  Outgoing interface list:
    Vlan1021, Forward/Sparse-Dense, 00:03:20/00:02:49, Pkts:0
Edge_2#show ip igmp snooping groups
Vlan      Group                     Type        Version     Port List
--------------------------------------------------------------------
1021      239.100.100.100           igmp        v3          Gi1/0/10
```

Questions

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!

ALL IN