cisco Live!

# ALL IN

#CiscoLive

The bridge to possible

# SD Access: Troubleshooting the Fabric

Michel Peters
Technical Leader Engineering
BRKENT-3820

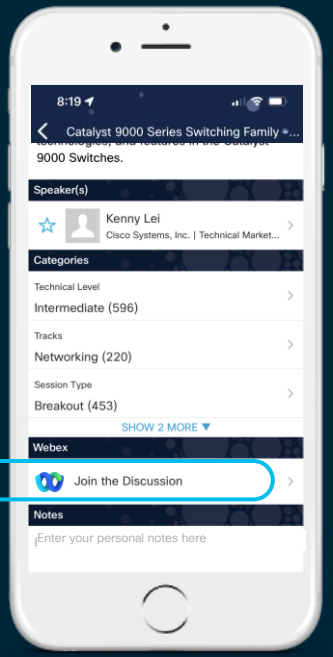
# Cisco Webex App

## 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




https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-3820

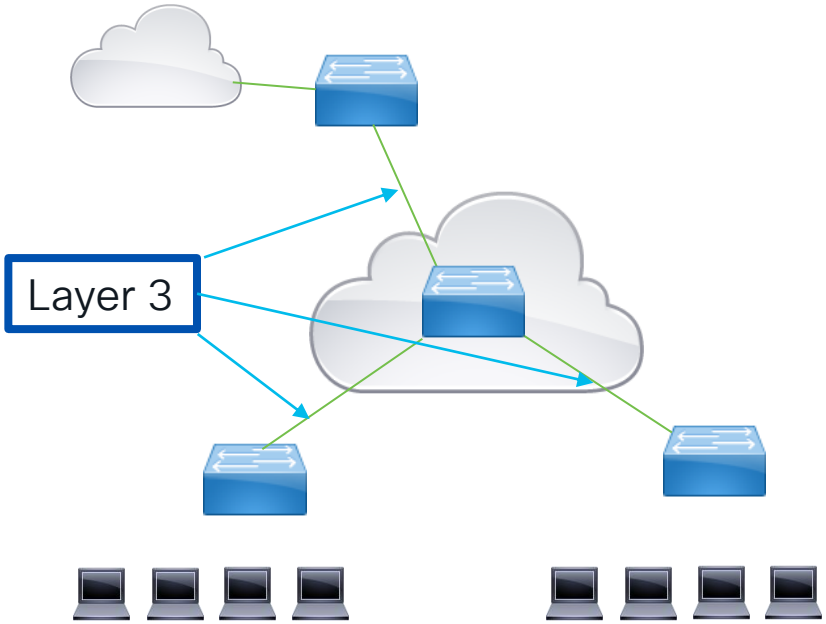
## Webex spaces will be moderated by the speaker until June 17, 2022.

# Agenda

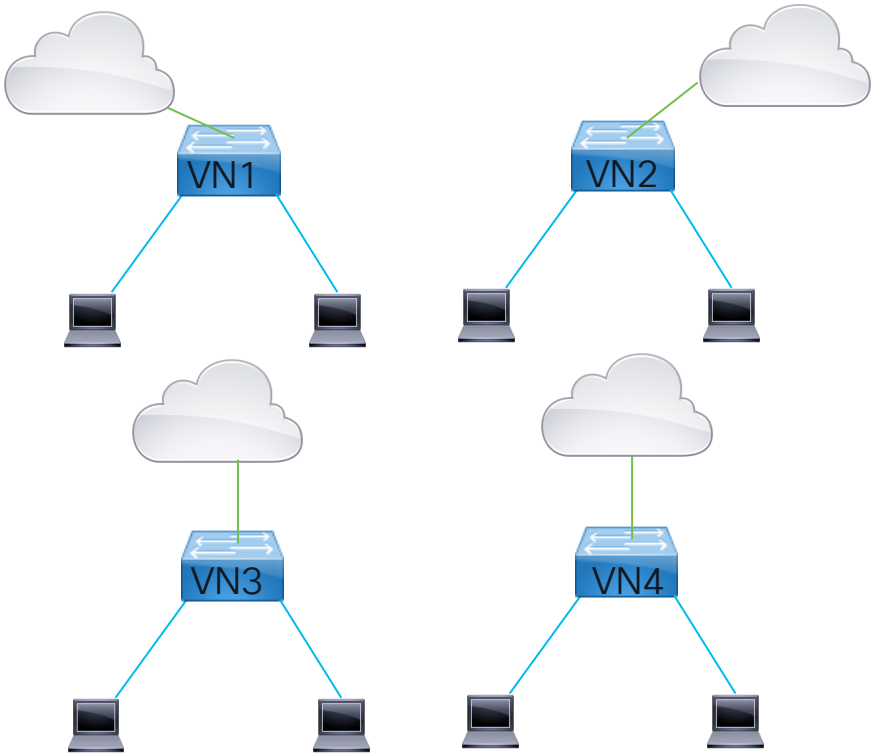
- Fabric overview
- Endpoints Registrations
- Reaching Remote Endpoints

# Fabric overview

# Overlay Technology



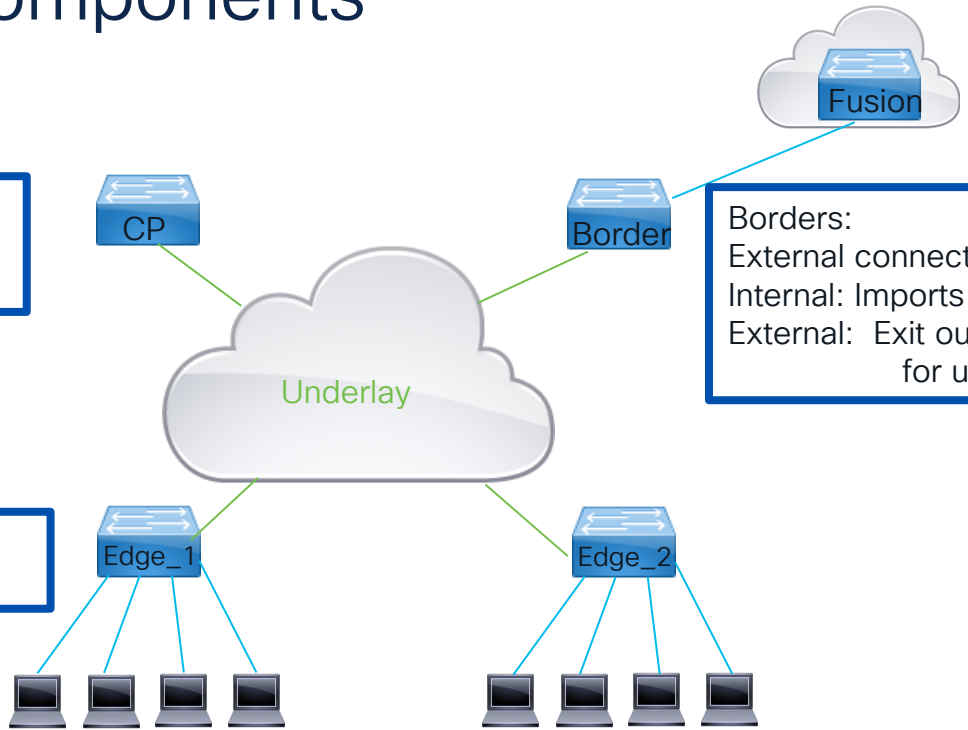

One Underlay
Layer 3 links




Multiple Virtual
Networks as Overlays

# Fabric Components

Control Plane Nodes:
Controls forwarding through the fabric




Borders:
External connectivity:
Internal: Imports routes into the fabric
External: Exit out of fabric
for unknown destinations

Edges:
Endpoint Connectivity

Fabric devices can have multiple roles

# SD Access Fabric Key Technologies

- Locator/ID Separation Protocol,
  Control plane protocol used inside the fabric for the Overlay networks
- VXLAN,
  Used for encapsulating all Dataplane traffic trough the underlay to form the overlay networks
- Cisco TrustSec,
  Assigning of a Policy label to all packets and enforcing security policies
- Authentication,
  Assigns endpoints using Dot1x/MAB with their respective authorization profiles and associated pools

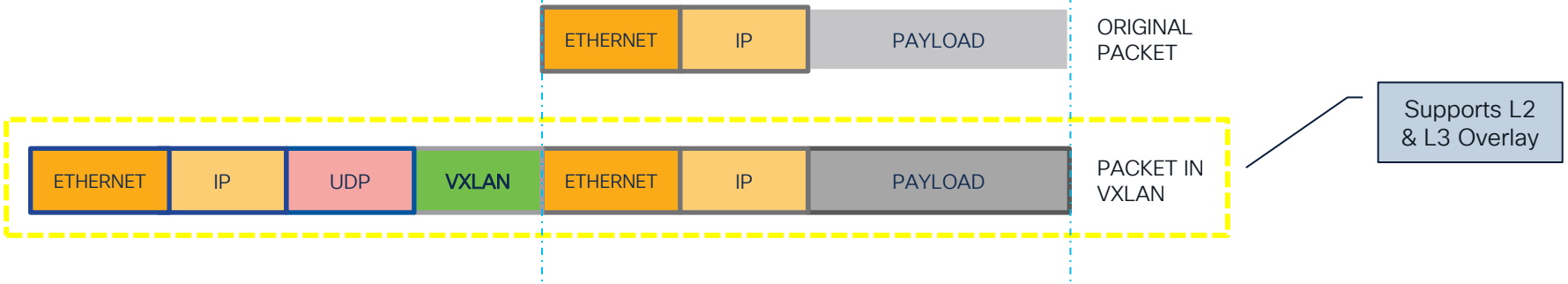
# LISP Basic operation

- LISP is a routing architecture, not just a routing protocol
- LISP creates a level of indirection by using two spaces: “locators” (RLOC) and “endpoints” (EID)
- Advertise “locators” in core routing. Removes “hosts” from routing tables. Host prefixes moved to an alternative system database
- Routers in Underlay only need routing information to RLOC space, simplifies Underlay network
- To get path information to end hosts, routers query locator-end host map servers. Mapping analogous to DNS.
- Routers hold map-cache of locator-hosts.

| LISP Device | SD Access | Function |
|---|---|---|
| RLOC (Routing Locator) | Fabric Devices | Routing Locator. Exists in global routing tables. Authoritative to reach EID space. |
| 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. |
| 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) &<br>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. |

# Data Plane

- In SD Access the entire Layer 2 packet is encapsulated
- VXLAN encapsulation used. IP address in new header set to RLOC
- VXLAN Network Identifier field set to LISP instance ID
- Group Policy ID field in XVLAN set to Ingress SGT and preserved through the fabric. Enforcement occurs on egress



# Endpoints Registrations

# Virtual Networks and LISP instances

- VRF's correlate to Virtual Networks
- Dynamic EID ranges specify which EID are learned
- When Multicast enabled Loopback interfaces are created inside VRF

```
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
```

Dynamic EID Ranges

VRF

Loopback for Multicasting

# Edge Configuration: SVI/VLAN Configuration

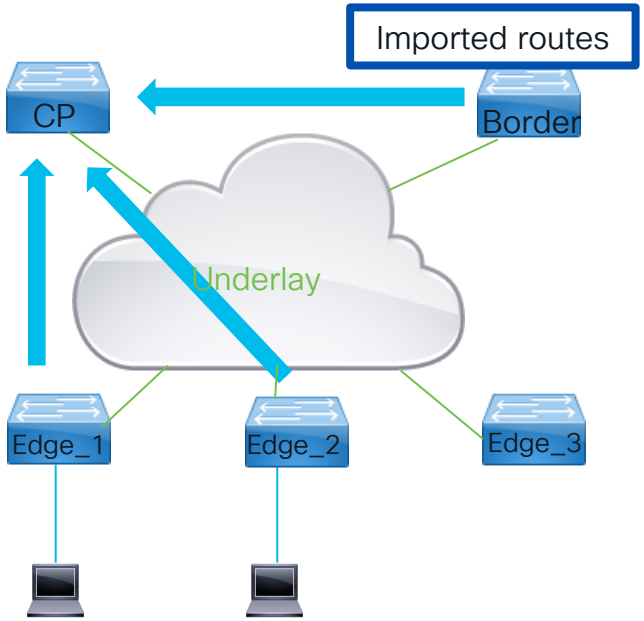
- Layer 3 Subnets and Layer 2 Pools deployed to all Edges is consistent throughout a fabric site
- Same IP address and mac are used on all edges(IP Anycast)
- Connections between edges should be L3 to avoid mac-learning issues

```
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 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 the IP and Mac addresses of attached devices to register with control plane node using map-register messages
- Layer 2 Instances start with 8xxx, 1 instance per Vlan
- 4xxx Instances used for Layer 3 Virtual Networks, 1 per Virtual Network, IPv4 and IPv6 share same instance
- Control Plane nodes maintain central database mapping

# 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 registers Learned Endpoints that are inside the EID ranges
- Endpoints can be 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
- Wildcard (*) when used will show all instances with lisp commands

# Registration of 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 communication or no EID's to be registered
- Registration only succeeds when LISP key matches with CP node
- Map register messages send to CP nodes to register all 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

- Entries with Type CP_LEARN are remote entries
- Only endpoint macaddresses are registered with Control Plane

```
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 0x768..
                      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

With proxy set Control plane responds on behalf of XTR

ETR Information

RLOC Information

# Layer 2 Control Plane

```
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
```

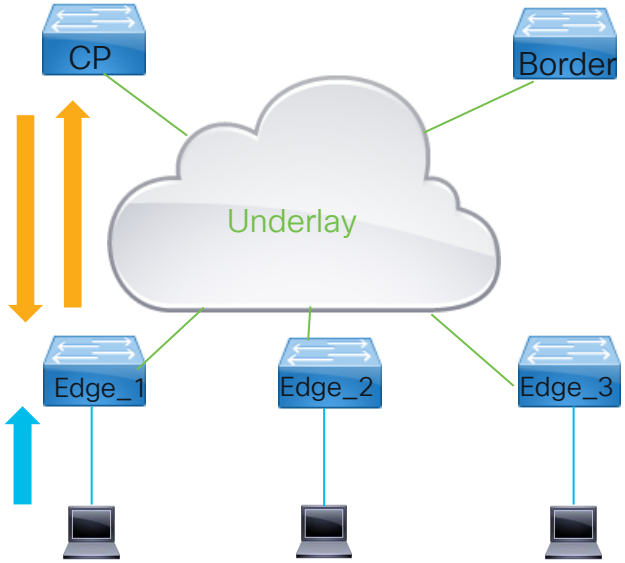
- Mac registrations on CP shown using show lisp instance-id * ethernet server

```
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
```

# 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
- Edge_1 initiates map request to CP node
- CP responds to Edge_2 with map-response containing RLOC information
- Edge_1 creates map-cache entry and is ready to forward traffic

# Map Cache

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

  map-cache 0.0.0.0/0 map-request

- 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 set by registering device with “etr map-cache-ttl”
- Negative map-requests have TTL of 15 minutes
- Control plane node returns largest possible block containing requested EID when sending Negative Map Reply

# Resolving Remote Destinations

```
Edge_1#sh lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 7 entries
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

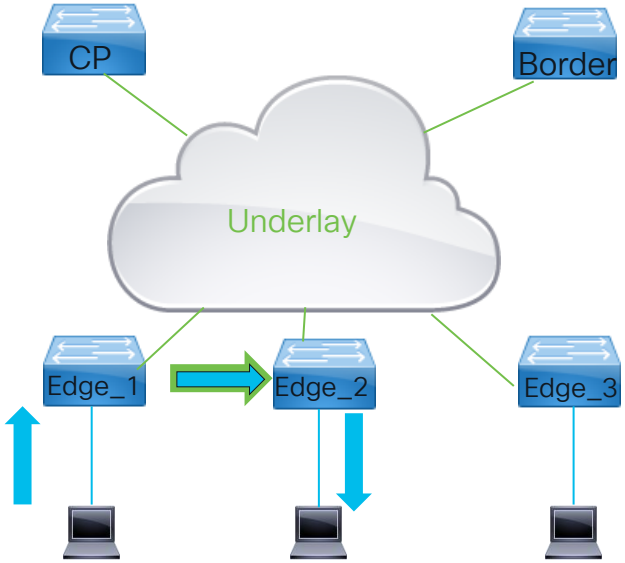
NMR, send to petr

Encapsulate to RLOC

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

# 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 inside fabric
- Traffic inside  IP pool will be encapsulated using Layer 2 instance
- Traffic destined outside IP pool send using Layer 3 instance
- Layer 2 forwards traffic based on Destination Mac Address and L2 Map-cache
- Optional flooding of BUM traffic using Multicast group in underlay
- Traffic outside IP pool will be routed using an Layer 3 LISP Instance

# LISP Remote forwarding

- Show ip route does not show full detail on forwarding
- Default route and remote entries not showing on edges. As Null0 routes 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
```

# 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.

# 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

# Questions?

# Related sessions:

- BRKTRS-3010 : SD Access: Advanced Fabric Troubleshooting
- BRKTRS-3090 : Troubleshooting the Cisco Catalyst 9000 Series Switches
- BRKTRS-2811a & BRKTRS-2811b : Overview of Packet Capturing Tools in Cisco Switches and Routers
- LABTRS-2391 Packet Capturing Tools in Enterprise Switching Environments

# Cisco Networking Bot

https://cnb.cisco.com/

## Empowering Users by Digitizing Cisco Product & Adoption Experiences

EoS/EoL

Product Migration/Adoption

Config / Tshoot Guides

Security Advisories

Release Recommendations

HW-SW Compatibility

Transforming Customer Experience with Cisco AI Chatbots

# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

**Pay for Learning with Cisco Learning Credits**

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

## Learn

**Cisco U.**
IT learning hub that guides teams and learners toward their goals

**Cisco Digital Learning**
Subscription-based product, technology, and certification training

**Cisco Modeling Labs**
Network simulation platform for design, testing, and troubleshooting

**Cisco Learning Network**
Resource community portal for certifications and learning

## Train

**Cisco Training Bootcamps**
Intensive team & individual automation and technology training programs

**Cisco Learning Partner Program**
Authorized training partners supporting Cisco technology and career certifications

**Cisco Instructor-led and Virtual Instructor-led training**
Accelerated curriculum of product, technology, and certification courses

## Certify

**Cisco Certifications and Specialist Certifications**
Award-winning certification program empowers students and IT Professionals to advance their technical careers

**Cisco Guided Study Groups**
180-day certification prep program with learning and support

**Cisco Continuing Education Program**
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

# Thank you

cisco Live!

# ALL IN

#CiscoLive