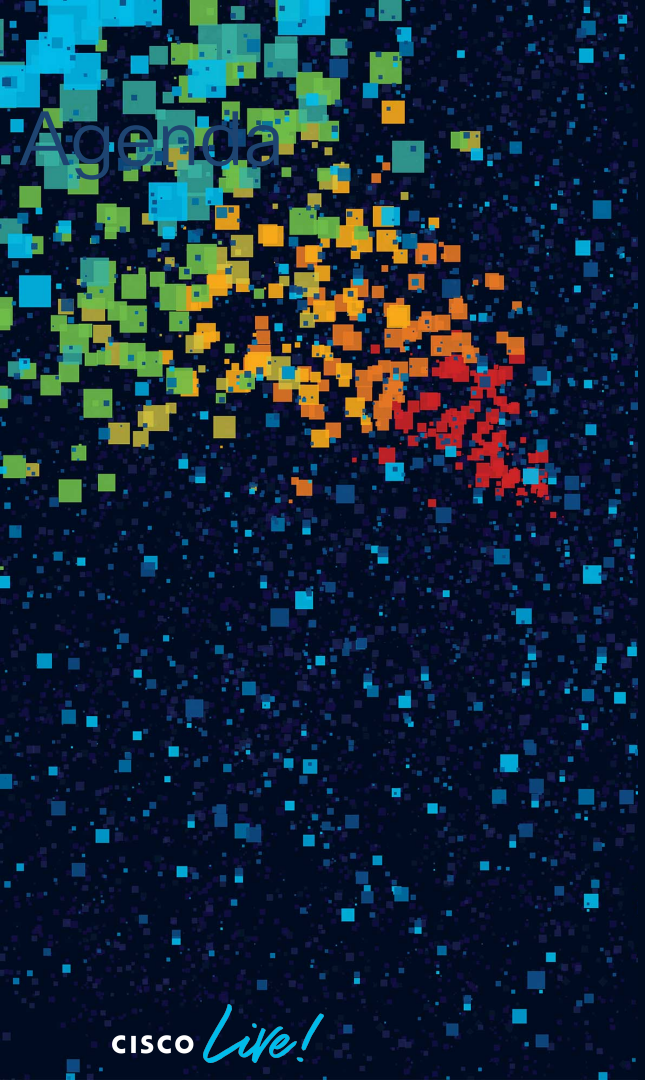
Possibilities

#CiscoLive

SD Access: Troubleshooting the fabric

Jon Balewicz, Technical Leader Engineering
Michel Peters, Technical Leader Engineering

DGTL-BRKARC-2020



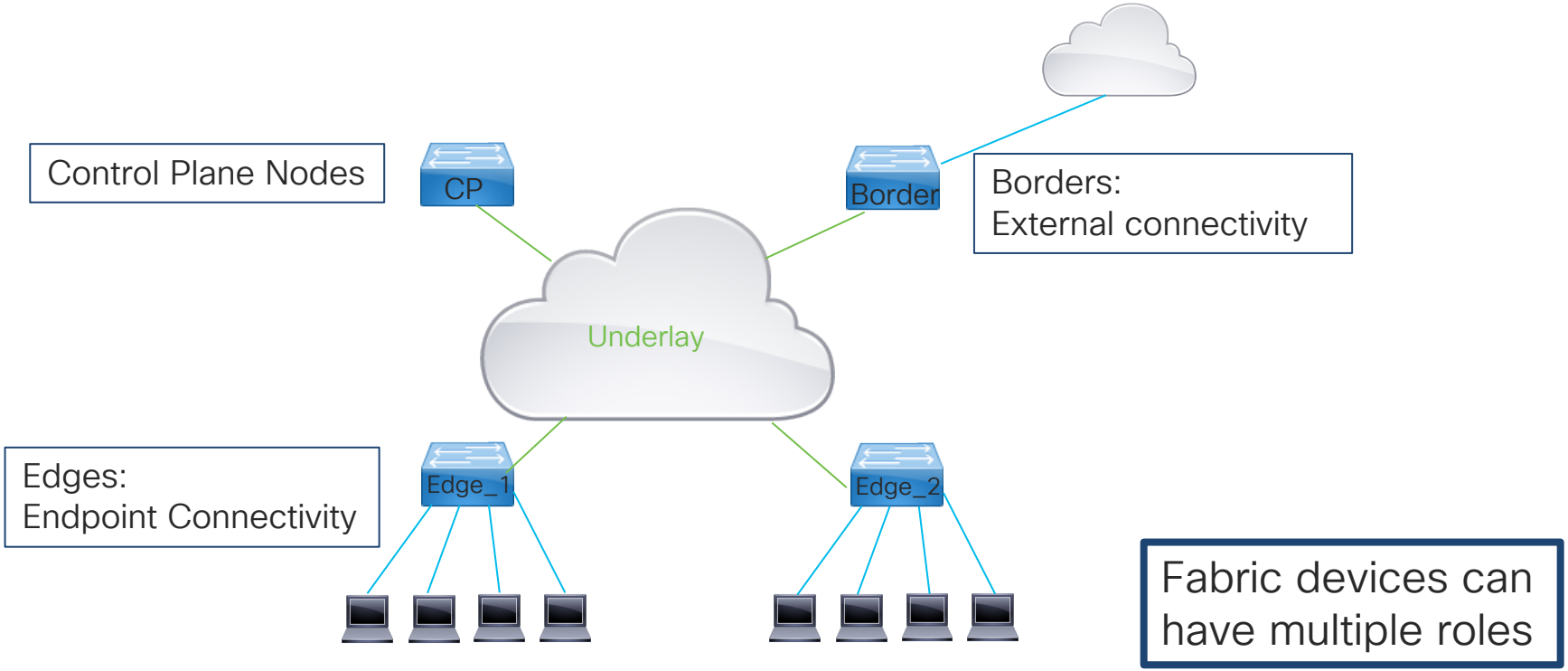
Agenda

- Fabric
- Layer 3 forwarding
- Layer 2 forwarding
- Multicast Forwarding
- Security in the Fabric

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

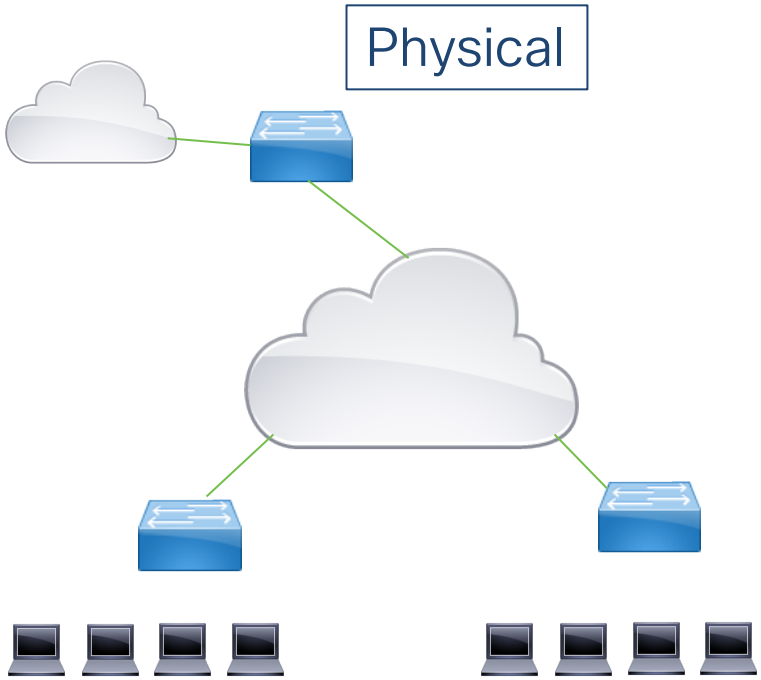
Fabric

The basic fabric

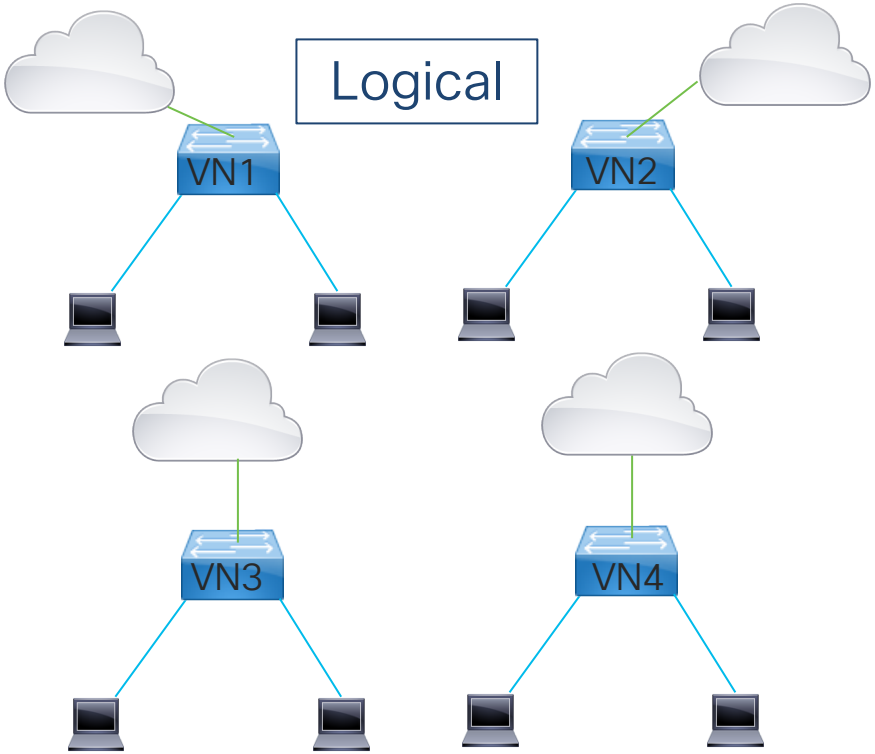


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The fabric



One Underlay



Many Overlays

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD Access Fabric Key Technologies

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LISP Basic operation

- LISP is a routing architecture.
- 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.

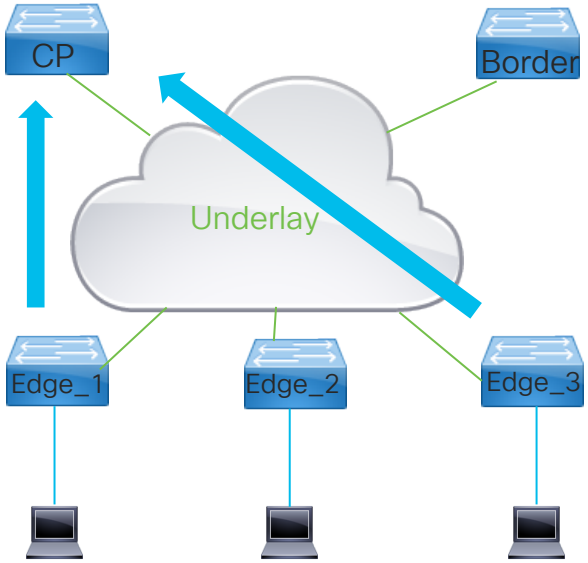
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

LISP basic operation, registering with Map Server

RLOC	EID (mac address)
Edge_1	0050.5692.6d39
Edge_2	0050.5692.9735
Edge_3	70e4.22e5.c4f7

RLOC	EID (IPv4)
Edge_1	192.168.1.100
Edge_2	192.168.2.100
Edge_3	192.168.1.101



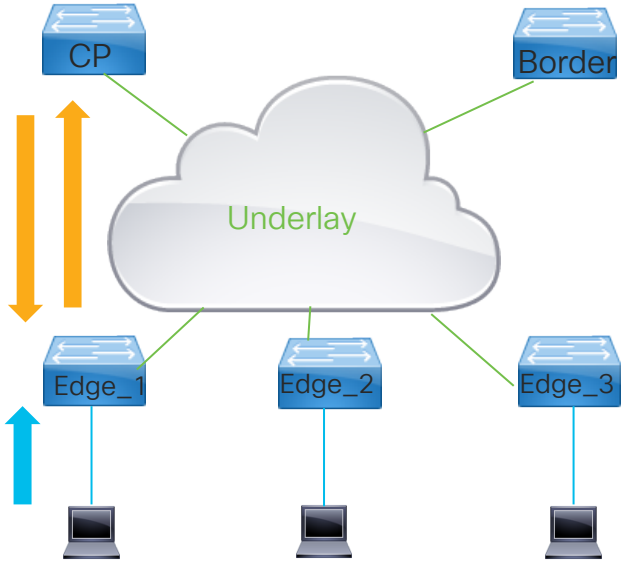
- Fabric devices learn the IPv4, IPv6 and MAC addresses of attached devices
- Fabric device register those with Map Server if they are in the defined EID Space
- Control Plane node keeps central database mapping all the EID to RLOC

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LISP basic operation, resolving

RLOC	EID (mac address)
Edge_1	0050.5692.6d39
Edge_2	0050.5692.9735
Edge_3	70e4.22e5.c4f7

RLOC	EID (IPv4)
Edge_1	192.168.1.100
Edge_2	192.168.2.100
Edge_3	192.168.1.101



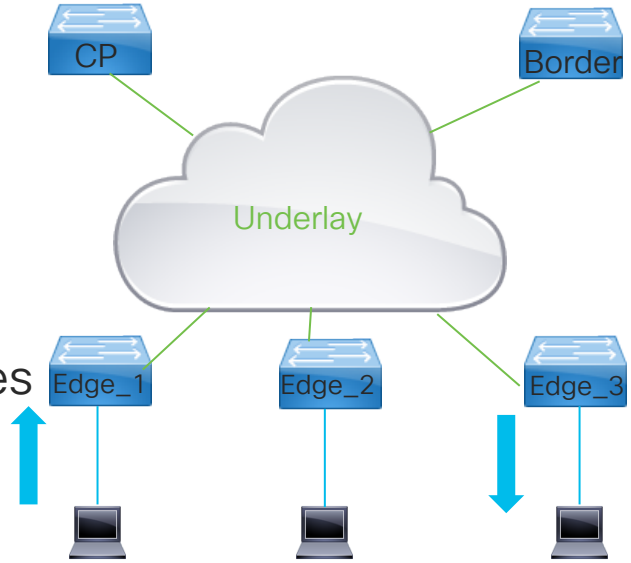
- Endpoint 1 sends packet towards Endpoint 2
- Edge_1 initiates map request to CP node for either Layer 2 or Layer 3 information
- CP responds to Edge_2 with map-response containing RLOC information
- RLOC information added to map-cache to allow traffic forwarding to Endpoint 2

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LISP basic operation, packet forwarding

RLOC	EID (mac address)
Edge_1	0050.5692.6d39
Edge_2	0050.5692.9735
Edge_3	70e4.22e5.c4f7

RLOC	EID (IPv4)
Edge_1	192.168.1.100
Edge_2	192.168.2.100
Edge_3	192.168.1.101

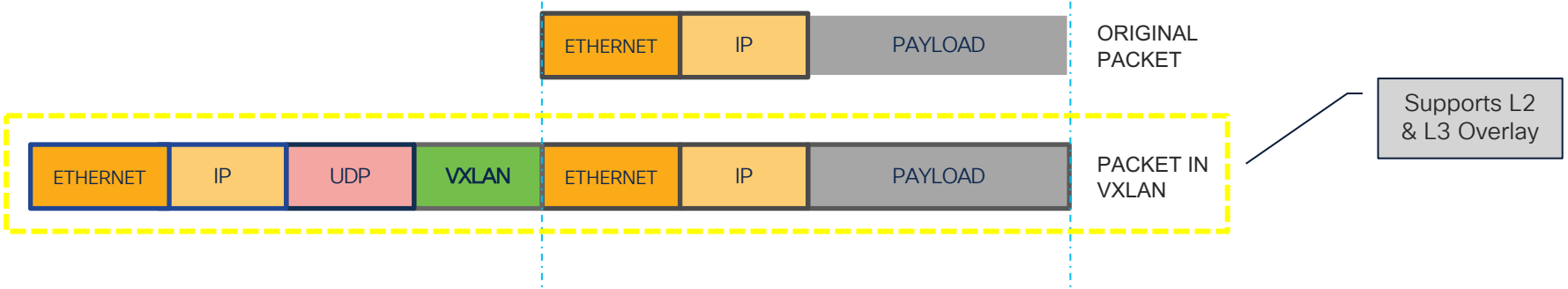


- Overlay traffic in SD Access is encapsulated in VXLAN and send between RLOC addresses
- Loopback0 is typically used for RLOC
- Underlay Routing table provides reachability for RLOC's
- If reachability does not exist to RLOC traffic does not get forwarded

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Plane

- In SD Access the entire Layer 2 packet is encapsulated
- VXLAN encapsulation used for encapsulation
- Outer IP Address are Loopback Addresses of Devices
- VXLAN Network Identifier used for LISP instance ID
- Group Policy ID field inside VXLAN header used for SGT label



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Encapsulation

5	0.863252	192.168.0.1	192.168.0.12	ICMP	148	Echo (ping) request id=0x0b50, seq=1/256, ttl=63 (reply in 9)
6	0.870066	192.168.0.1	192.168.0.12	ICMP	148	Echo (ping) request id=0x0b50, seq=2/512, ttl=63 (reply in 10)
7	1.139082	10.255.1.14	10.254.255.50	LISP	82	Map-Request (RLOC-probe) for [4097] 192.168.0.1/32
8	1.140831	10.255.1.22	10.254.255.52	LISP	94	Map-Reply (RLOC-probe reply) for [4097] 192.168.0.1/32
9	1.864089	192.168.0.12	192.168.0.1	ICMP	148	Echo (ping) reply id=0x0b50, seq=1/256, ttl=63 (request in 5)
10	1.864135	192.168.0.12	192.168.0.1	ICMP	148	Echo (ping) reply id=0x0b50, seq=2/512, ttl=63 (request in 6)
11	1.869295	192.168.0.1	192.168.0.12	ICMP	148	Echo (ping) request id=0x0b50, seq=3/768, ttl=63 (reply in 12)
12	1.869346	192.168.0.12	192.168.0.1	ICMP	148	Echo (ping) reply id=0x0b50, seq=3/768, ttl=63 (request in 11)
13	2.868296	192.168.0.1	192.168.0.12	ICMP	148	Echo (ping) request id=0x0b50, seq=4/1024, ttl=63 (reply in 14)
14	2.868352	192.168.0.12	192.168.0.1	ICMP	148	Echo (ping) reply id=0x0b50, seq=4/1024, ttl=63 (request in 13)

```
> Frame 5: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
> Ethernet II, Src: Cisco_9f:1d:40 (00:00:0c:9f:1d:40), Dst: Cisco_e9:4c:7f (fc:99:47:e9:4c:7f)
> Internet Protocol Version 4, Src: 10.255.1.22, Dst: 10.254.255.52
> User Datagram Protocol, Src Port: 65359, Dst Port: 4789
v Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 13
    VXLAN Network Identifier (VNI): 4097
    Reserved: 0
> Ethernet II, Src: Cisco_9f:00:00 (00:00:0c:9f:00:00), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.12
> Internet Control Message Protocol
```

New Header

VXLAN Header

SGT

LISP Instance ID

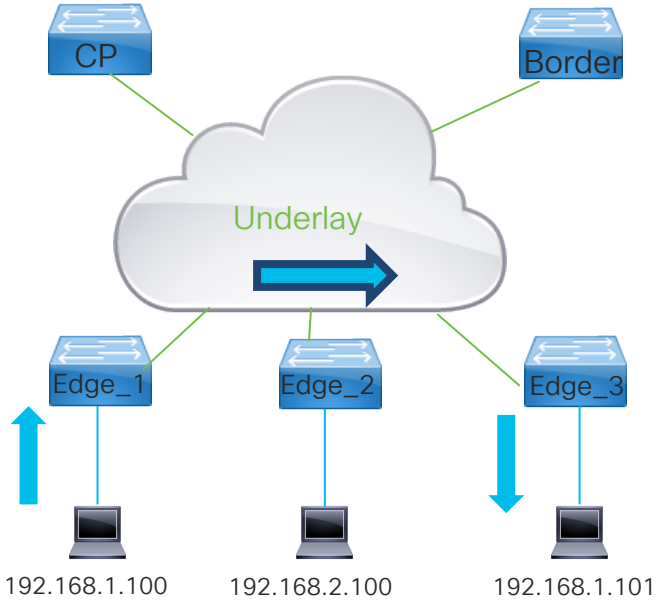
Encapsulated packet

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 3 Forwarding

Layer 3 in the Fabric

RLOC	EID
Edge_1	192.168.1.100
Edge_2	192.168.2.100
Edge_3	192.168.1.101
Border	10.48.91.128/25



- Layer 3 LISP Instance ID's are in 4000 range
- Traffic forwarding
  -> Outside Pool(other subnet):
  "Routed", Client sends to Anycast IP MAC
  Forwarding done based upon destination IP
  -> Inside Pool (same subnet):
  "Bridged", Client sends to MAC of Endpoint
  Forwarding done based upon MAC Address
- All Edges use same IP for SVI (Anycast)

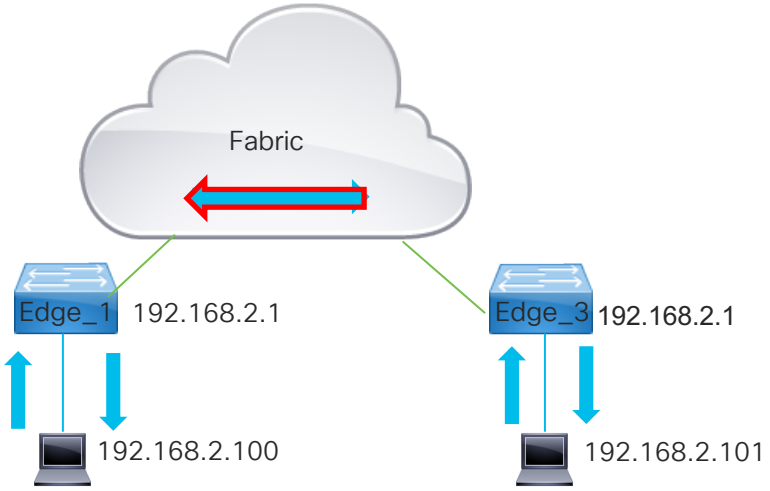
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IP Anycast

- Every Edge Devices uses same VLAN , same IP address and same MAC Address
- Endpoints in the IP Pool(subnet) can be spread through the fabric.
- Default Gateway for Endpoint is set to Anycast IP

```
Edge_1#sh run int vlan 1024
interface Vlan1024
 mac-address 0000.0c9f.f4
 vrf forwarding CiscoLive
 ip address 192.168.2.1 25
 ip helper-address 10.48.91.
 no ip redirects
 ip pim sparse-mode
 ip route-cache same-interfa
 ip igmp version 3
 ip igmp explicit-tracking
 no lisp mobility liveness tes
 lisp mobility 192_168_2_0-
end
```

```
Edge_3#sh run int vlan 1024
interface Vlan1024
 mac-address 0000.0c9f.f45f
 vrf forwarding CiscoLive
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 10.48.91.148
 no ip redirects
 ip pim sparse-mode
 ip route-cache same-interface
 ip igmp version 3
 ip igmp explicit-tracking
 no lisp mobility liveness test
 lisp mobility 192_168_2_0-CiscoLive-IPV4
end
```



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Locally Registered Endpoints

- VN's in SDA correlate to a VRF named as the VN
- Interface LISP 0.<instance-id> part of VRF
- Only endpoints belonging to EID space are added to the LISP database and registered with CP

```
Edge_1#show ip vrf CiscoLive
  Name                    Interfaces
  CiscoLive               Lo4100
                          Vl1022
                          LI0.4100
                          Tu2
                          Vl1024
```

```
Edge_1#show run | section instance-id 4100
 instance-id 4100
  dynamic-eid 192_168_1_0-CiscoLive-IPV4
   database-mapping 192.168.1.0/24 locator-set rloc_ab36f833-b546-4869-930f-578ba1cdf413
     !
  dynamic-eid 192_168_2_0-CiscoLive-IPV4
   database-mapping 192.168.2.0/24 locator-set rloc_ab36f833-b546-4869-930f-578ba1cdf413
     !
  service ipv4
   eid-table vrf CiscoLive
   database-mapping 192.168.200.4/32 locator-set rloc_ab36f833-b546-4869-930f-578ba1cdf413
   map-cache 0.0.0.0/0 map-request
```

EID Space

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Locally Registered Endpoints

```
Edge_1#show ip arp vrf CiscoLive 192.168.1.100
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.100          3   0050.5692.6d39  ARPA   Vlan1022
Edge_1#show lisp instance-id 4100 ipv4 database 192.168.1.100/32
LISP ETR IPv4 Mapping Database for EID-table vrf CiscoLive (IID 4100), LSBs: 0x1
Entries total 2, no-route 0, inactive 0
192.168.1.100/32, dynamic-eid 192_168_1_0-CiscoLive-IPV4, inherited from default
locator-set rloc_ab36f833-b546-4869-930f-578ba1cdf413
  Locator         Pri/Wgt  Source     State
  172.31.255.109   10/10   cfg-intf   site-self, reachable
```

- LISP Database registers only Learned Endpoints that are inside the EID Space
- Endpoints can be learned via ARP or DHCP Snooping
- Locator RLOC as advertised by Fabric Device registering the entry. RLOC IP address should be advertised in Underlay network as host route

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Registration of Endpoints with Map Server (CP)

- IPv4/IPv6 Endpoints can be reached when learned by Edge and registered with CP
- Dynamic Endpoints learned via ARP and Device Tracking (DHCP/ARP)
- Once learned by Fabric Device it registered using LISP Reliable Transport with CP

```
Edge_1#show lisp session
Sessions for VRF default, total: 2, established: 2
Peer                          State      Up/Down        In/Out    Users
172.31.255.28:4342            Up         07:14:14      111/46     6
172.31.255.29:4342            Up         07:14:14      111/46     6

Edge_1#show lisp instance-id 4100 ipv4 statistics  | sec Map-Register
  Map-Register records in/out:                      0/28
    Map-Server AF disabled:                         0
    Authentication failures:                        0
Edge_1#show lisp instance-id 4100 ipv4 statistics  | sec Map-Requests
  Map-Requests in/out:                              9/12
    Encapsulated Map-Requests in/out:               0/8
    RLOC-probe Map-Requests in/out:                 9/4
    SMR-based Map-Requests in/out:                  4/0
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Node (MSMR)

- Control Plane Node maintains table with all EID registrations
- Redundant Control Plane node do not synchronize each other.

```
CP_1#show lisp site instance-id 4100
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      --                    4100      0.0.0.0/0
                07:32:40   yes#    172.31.255.29:12616   4100      10.48.91.128/25
                never      no      --                    4100      192.168.1.0/24
                00:03:39   yes#    172.31.255.109:13974  4100      192.168.1.100/32
                07:32:40   yes#    172.31.255.111:43564  4100      192.168.1.101/32
                never      no      --                    4100      192.168.2.0/24
                06:14:53   yes#    172.31.255.110:43692  4100      192.168.2.100/32
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Node (MSMR) details on EID

```
CP_1#show lisp site 192.168.1.100/32 instance-id 4100
Requested EID-prefix:
  EID-prefix: 192.168.1.100/32 instance-id 4100
    First registered:     00:15:25
    Last registered:      00:15:25
    Routing table tag:    0
    Origin:               Dynamic, more specific of 192.168.1.0/24
    Merge active:         No
    Proxy reply:          Yes
    TTL:                  1d00h
    State:                complete
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.31.255.109:13974, last registered 00:15:25, proxy-reply, map-notify
                              state complete, no security-capability
                              sourced by reliable transport
      Locator          Local  State      Pri/Wgt  Scope
      172.31.255.109   yes    up          10/10   IPv4 none
```

When registered on CP

Proxy Reply -> CP will respond on behalf of registering

ETR Information

RLOC Information

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Inactive clients

- Device Tracking sending regular ARP probes to ensure device reachability
- Endpoints become inactive when no longer active on the network or roamed away to another fabric device

```
Edge_1#show lisp instance-id 4100 ipv4 database  192.168.1.100/32
LISP ETR IPv4 Mapping Database for EID-table vrf CiscoLive (IID 4100), LSBs: 0x1
Entries total 2, no-route 0, inactive 1
192.168.1.100/32, Inactive, expires: 23:58:48
Edge_1#show lisp instance-id 4100 ipv4 smr
LISP SMR Table for router lisp 0 (CiscoLive) IID 4100
Prefix                                   Producer
192.168.1.100/32                         away table
192.168.200.4/32                         local EID
Edge_1#show lisp instance-id 4100 ipv4 away
LISP Away Table for router lisp 0 (CiscoLive) IID 4100
Prefix                                   Producer
192.168.1.100/32                         local EID
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resolving Remote Destinations

- Map Cache checked for Destination IP match.

  → Hit: traffic forwarded using cached information
  → No Hit: Map request is sent to the CP node(s)

- Responses from Control Plane Nodes are cached on fabric devices to build the map cache.
- Successful map-requests are cached with a TLL of 1 day
- Control plane node returns largest possible block containing requested EID when sending NMR.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resolving Remote Destinations

```
Edge_2#show lisp instance-id 4100 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf CiscoLive (IID 4100), 8 entries
0.0.0.0/0, uptime: 1d03h, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
8.0.0.0/7, uptime: 00:00:04, expires: 23:59:55, via map-reply, forward-native
  Encapsulating to proxy ETR
10.48.91.128/25, uptime: 00:00:16, expires: 23:59:44, via map-reply, complete
  Locator          Uptime    State      Pri/Wgt     Encap-IID
  172.31.255.29    00:00:16  up          10/10        -
192.168.1.0/24, uptime: 1d03h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
192.168.1.100/32, uptime: 1d02h, expires: 03:39:23, via map-reply, complete
  Locator           Uptime    State      Pri/Wgt     Encap-IID
  172.31.255.109    20:20:36  up          10/10        -
192.168.2.0/24, uptime: 1d03h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
```

Negative map-reply

External Subnet

EID Subnet

Resolved Remote Destination

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LISP Remote forwarding on edge, more detail

- Routing table for VRF on edges show no Default Gateway or remote routes
- Entries in Database are inserted into routing table
- Remote entries in map-cache are not displayed or as Null routes

```
Edge_2#show ip route vrf CiscoLive
Routing Table: CiscoLive
Gateway of last resort is not set
      192.168.2.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Vlan1024
L        192.168.2.1/32 is directly connected, Vlan1024
l        192.168.2.100/32 [10/1] via 192.168.2.100, 2d18h, Vlan1024
      192.168.200.0/32 is subnetted, 1 subnets
C        192.168.200.9 is directly connected, Loopback4100
CP_2#show ip route vrf CiscoLive
Routing Table: CiscoLive
B        192.168.1.0/24 [200/0], 3d20h, Null0
C        192.168.1.1/32 is directly connected, Loopback1022
l        192.168.1.100/32 [250/1], 2d14h, Null0
l        192.168.1.101/32 [250/1], 2d22h, Null0
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LISP Remote forwarding, more detail

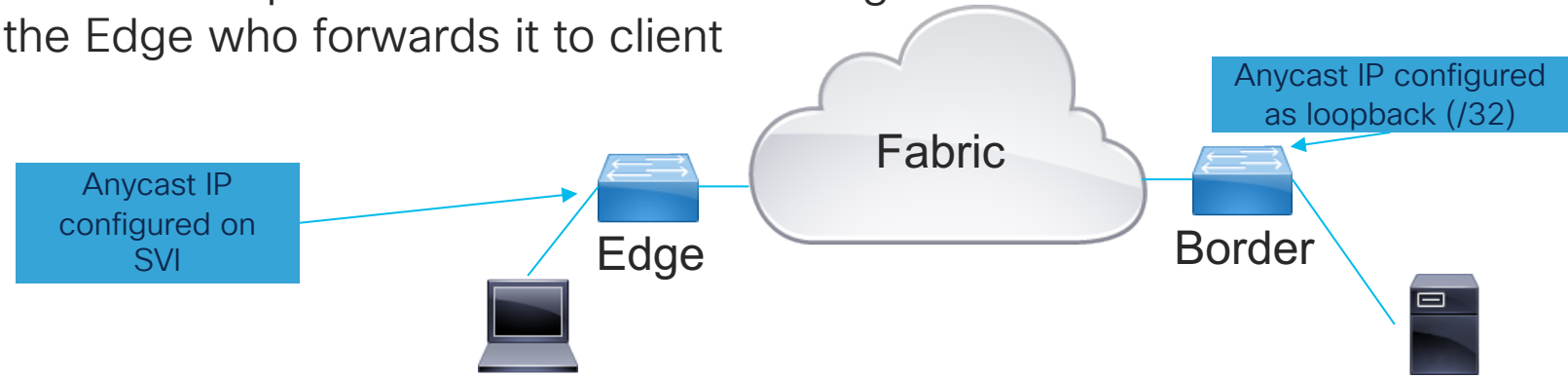
```
Edge_2#show ip cef vrf CiscoLive 192.168.1.100/32 detail
192.168.1.100/32, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 2 packets 1152 bytes fwd action encap, cfg as EID space, dynamic
EID need encap
  SC inherited: LISP cfg dyn-EID - LISP configured dynamic-EID
  LISP EID attributes: localEID No, c-dynEID Yes, d-dynEID No
  LISP source path list
    nexthop 172.31.255.109 LISP0.4100
  2 IPL sources [no flags]
  nexthop 172.31.255.109 LISP0.4100
```

- CEF gives an accurate view of forwarding
- Next Hop egressing out of LISP interface is in Underlay network
- Using “internal” keyword provides even more detail
- Show ip cef <nexthop> gives egress interface information in underlay

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP in the fabric. Quick overview

- Host sends DHCP Discover
- DHCP Snooping inserts remote agent in option 82
- DHCP Relay forwards to DHCP server through fabric, setting giaddress to IP Anycast address
- DHCP Offer send by DHCP server to Anycast IP address.
- Border extracts the option 82 and forwards through fabric to the Edge who forwards it to client



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Option 82 Agent Remote ID Decoding

AA BB CC CC CC DD EE EE EE EE

AA = Sub option, 03 = LISP (01 = mac address, 02 = string)
BB = length of option
CCCCCCC = LISP Instance ID
DD = Address Family IPv4 = 01 IPv6 -02
EEEEEEEE =Source locator

03 08 001002 01 c0a80106

03 Sub option lisp
08 Length of option
001002 = 4098 in decimals ->LISP Instance ID 4098
01= IPV4 locator
c0.a8.01.06 = 192.168.1.6 Source locator (Loopback 0 of xTR)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP related debugs

- `debug ip dhcp snooping`
  Enables showing detail with regards to DHCP snooping and the insertion of option 82 remote circuit
- `debug ip dhcp server`
  Enables debug with regards to the relay function , insertion giaddress and relay functionality to the Server
- `debug dhcp detail`
  Adds additional detail with regards to LISP in DHCP debugs

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Debug – DHCP Snooping

```
Jan 27 18:23:14.889: DHCP_SNOOPING: received new DHCP packet from input interface
(GigabitEthernet1/0/1)
Jan 27 18:23:14.890: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST,
input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC sa: 0050.5692.6d39, IP da:
255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP
siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.5692.6d39, efp_id: 0, vlan_id:
1022
Jan 27 18:23:14.891: DHCP_SNOOPING: add relay information option.
Jan 27 18:23:14.891: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
Jan 27 18:23:14.891: :VLAN case : VLAN ID 1022
Jan 27 18:23:14.891:  VRF id is valid
Jan 27 18:23:14.891: LISP ID is valid, encoding RID in srloc format
Jan 27 18:23:14.892: DHCP_SNOOPING: binary dump of relay info option, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0x3 0xFE 0x1 0x1 0x2 0xA 0x3 0x8 0x0 0x10 0x4 0x1 0xAC 0x1F
0xFF 0x6D
Jan 27 18:23:14.893: DHCP_SNOOPING: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (1022)
Jan 27 18:23:14.893: DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan1022.
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Debug –DHCP Relay

DHCP Relay functionality sets GI address in DHCP packet and forwards

```
Jan 27 18:23:14.896: DHCPD: Finding a relay for client 0050.5692.6d39 on interface
Vlan1022.
Jan 27 18:23:14.896: DHCPD : Locating relay for Subnet 192.168.1.1
Jan 27 18:23:14.896: DHCPD: there is no pool for 192.168.1.1.
Jan 27 18:23:14.896: DHCPD: Looking up binding using address 192.168.1.1
Jan 27 18:23:14.897: DHCPD: setting giaddr to 192.168.1.1.
Jan 27 18:23:14.897: DHCPD: BOOTREQUEST from 0050.5692.6d39 forwarded to 10.48.91.148.
```

Reply packet from DHCP server received by relay and forwarded

```
Jan 27 18:23:14.901: DHCPD: forwarding BOOTREPLY to client 0050.5692.6d39.
Jan 27 18:23:14.901: DHCPD: Option 125 not present in the msg.
Jan 27 18:23:14.902: DHCPD: src nbma addr as zero
Jan 27 18:23:14.902: DHCPD: ARP entry exists (192.168.1.100, 0050.5692.6d39).
Jan 27 18:23:14.902: DHCPD: egress Interface Vlan1022
Jan 27 18:23:14.902: DHCPD: unicasting BOOTREPLY to client 0050.5692.6d39 (192.168.1.100).
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Debug -Snooping

```
Jan 27 18:23:14.903: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input
interface: Vl1022, MAC da: 0050.5692.6d39, MAC sa: 0000.0c9f.f45d, IP da: 192.168.1.100, IP sa:
192.168.1.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.1.100, DHCP siaddr: 0.0.0.0, DHCP
giaddr: 192.168.1.1, DHCP chaddr: 0050.5692.6d39, efp_id: 0, vlan_id: 1022
Jan 27 18:23:14.904: DHCP_SNOOPING: binary dump of option 82, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0x3 0xFE 0x1 0x1 0x2 0xA 0x3 0x8 0x0 0x10 0x4 0x1 0xAC 0x1F 0xFF 0x6D
Jan 27 18:23:14.906: DHCP_SNOOPING: binary dump of extracted circuit id, length: 8 data:
0x1 0x6 0x0 0x4 0x3 0xFE 0x1 0x1
Jan 27 18:23:14.907: DHCP_SNOOPING: binary dump of extracted remote id, length: 12 data:
0x2 0xA 0x3 0x8 0x0 0x10 0x4 0x1 0xAC 0x1F 0xFF 0x6D
Jan 27 18:23:14.909: No entry found for mac(0050.5692.6d39) vlan(1022) GigabitEthernet1/0/1
Jan 27 18:23:14.909: host tracking not found for update add dynamic (192.168.1.100, 0.0.0.0,
0050.5692.6d39) vlan(1022)
Jan 27 18:23:14.909: DHCP_SNOOPING: remove relay information option.
Jan 27 18:23:14.909: platform lookup dest vlan for input_if: Vlan1022, is NOT tunnel,
if_output: Vlan1022, if_output->vlan_id: 1022, pak->vlan_id: 1022
Jan 27 18:23:14.910: DHCP_SNOOPING: direct forward dhcp replyto output port:
GigabitEthernet1/0/1.
```

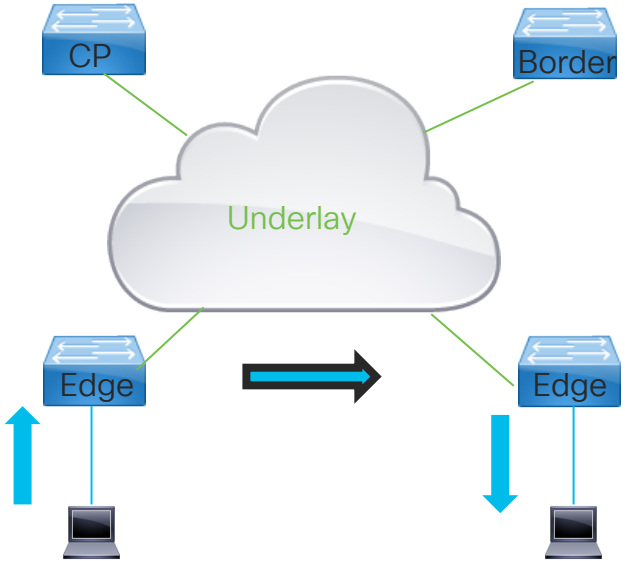
DHCP Snooping forwarding packet to Egress Interface

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Forwarding

Layer 2 in the Fabric

EID (mac address)
0050.5692.6d39
0050.5692.9735
70e4.22e5.c4f7



- Forwarding occurs inside an IP pool, based on Layer 2 MAC Addressing
- Complete Ethernet frame gets encapsulated in VXLAN and transported through fabric
- All traffic inside an IP pool gets send via Layer 2 instances (8000 range)
- MAC Addresses are registered with CP node
- Edge Nodes resolve and cache remote MAC addresses similar as done with Layer 3.
- Layer 2 Instances are associated with the VLAN corresponding to the SVI

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Modes

- Initial implementation with DNA Center 1.1 utilized layer 2 proxy ARP
- Default behavior changed to Layer 2 Extension mode on Cisco DNA Center adds Layer 2 transport through Fabric (Transports Known Unicast traffic) through Fabric
- Layer 2 Flooding mode allows flooding of selected traffic through the use of an underlay Mcast Group (broadcast-underlay) config present in config
- Traffic on the same subnet is sent via Layer 2, Traffic outside the subnet send via Layer 3

```
Edge_3#show run | section instance-id 8190
 instance-id 8190
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1022
   broadcast-underlay 239.0.0.3
   database-mapping mac locator-set rloc_88
   exit-service-ethernet
```

```
Edge_3#show run interface vlan 1022
interface Vlan1022
 mac-address 0000.0c9f.f45d
 vrf forwarding CiscoLive
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 10.48.91.148
  no lisp mobility liveness test
 lisp mobility 192_168_1_0-CiscoLive-IPV4
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 MAC Address Tables

- Local clients show as Dynamic or Static for Authenticated endpoints
- Remote MAC Addresses ->CP_LEARN and port Tu0
- Anycast IP with associated MAC learned on both clients
- ARP tables on clients hold mac address of remote, traffic from client to client is send to mac address of client

```
Edge_3#show mac add | inc 1022|--|Type
-------------------------------------------
VLAN    MAC Address        Type        Ports
----    -----------        --------    -----
1022    0000.0c9f.f45d     STATIC      Vl1022
1022    58bf.eab6.4b75     STATIC      Vl1022
1022    70e4.22e5.c4f7     STATIC      Gi1/0/1
1022    0050.5692.6d39     CP_LEARN    Tu0
```

Local

```
guest@Client_3:~$ ip neig
192.168.1.100 dev eth0 lladdr 00:50:56:92:6d:39
192.168.1.1 dev eth0 lladdr 00:00:0c:9f:f4:5d
```

Remote

```
guest@Client_1:~$ ip neig
192.168.1.1 dev eth0 lladdr 00:00:0c:9f:f4:5d
192.168.1.101 dev eth0 lladdr 70:e4:22:e5:c4:f7
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LISP Local registered mac addresses

- Layer 2 LISP uses show lisp instance-id <instance> ethernet commands
- Similar to L3 LISP, L2 maintains local entries in a database.
- All MAC addresses part of Layer 2 EID space, all MAC addresses can be learned and registered

```
Edge_3#show lisp instance-id 8190 ethernet database
LISP ETR MAC Mapping Database for EID-table VLAN 1022 (IID 8190), LSBs: 0x1
Entries total 1, no-route 0, inactive 0

70e4.22e5.c4f7/48, dynamic-eid Auto-L2-group-8190, inherited from default locator-
set rloc_88efd7b1-bb88-42d7-8a3f-68e1bfe94085
  Locator          Pri/Wgt  Source     State
  172.31.255.111    10/10   cfg-intf   site-self, reachable
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Node

- All MAC Addresses registered in Fabric on CP node as EID Prefix
- Show LISP instance-id <id> ethernet server uses Layer 2 instance-id or *

```
CP_1#show lisp instance-id 8190 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     --                    8190     any-mac
                3d04h      yes#   172.31.255.19:2470    8190     0000.0c9f.f45d/48
                2d22h      yes#   172.31.255.109:13974  8190     0050.5692.6d39/48
                03:36:25   yes#   172.31.255.111:43564  8190     70e4.22e5.c4f7/48
                3d04h      yes#   172.31.255.19:2470    8190     fc99.47e9.4c7f/48
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CP Node, Ethernet EID more detailed information

```
CP_1#show lisp instance-id 8190 ethernet server 0050.5692.6d39
Requested EID-prefix:
  EID-prefix: 0050.5692.6d39/48 instance-id 8190
    First registered:     2d22h
    Last registered:      2d22h
    Routing table tag:    0
    Origin:               Dynamic, more specific of any-mac
    Merge active:         No
    Proxy reply:          Yes
    TTL:                  1d00h
    State:                complete
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.31.255.109:13974, last registered 2d22h, proxy-reply, map-notify
                              TTL 1d00h, sourced by reliable tra
      Locator          Local  State      Pri/Wgt  Scope
      172.31.255.109   yes    up          10/10   IPv4 none
```

Registration info

CP responds to map-reply

RLOC info

- Control Plane node detailed information on registered MAC address

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Map-Cache

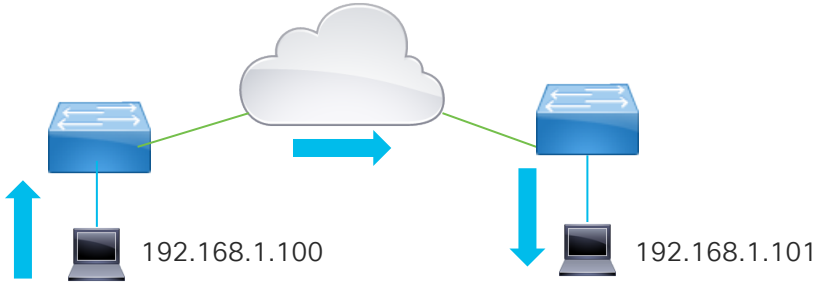
```
Edge_1#show lisp instance-id 8190 ethernet map-cache detail
LISP MAC Mapping Cache for EID-table VLAN 1022 (IID 8190), 1 entries
70e4.22e5.c4f7/48, uptime: 04:09:04, expires: 19:50:55, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 04:09:04, map-source: 172.31.255.111
  Idle, Packets out: 0(0 bytes)
  Encapsulating dynamic-EID traffic
  Locator          Uptime    State      Pri/Wgt     Encap-IID
  172.31.255.111   04:09:04  up          10/10        -
    Last up-down state change:         04:09:04, state change count: 1
    Last route reachability change:    04:09:04, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            04:09:04 (rtt 3ms)
```

- Fabric Devices resolve RLOC when traffic send to unknown Destination MAC addresses using map-request.
- Similar to Layer 3 a map-cache is build for Layer 2 entries with result

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ARP in the Fabric

- ARP protocol relies on Layer 2 Broadcasts to resolve IP to MAC Address
- Layer 2 Broadcast domain (without Layer 2 flooding) constrained to just Fabric Edge
- Device Tracking enables ARP snooping , allowing rewriting of Destination MAC
- Fabric Edge register learned Address Resolution info with Control Plane node
- Fabric Edge's query Control Plane node for Address Resolution info to rewrite broadcast to Unicast MAC Address and send it through fabric as Unicast



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ARP Captures

No.	Time	Source	Destination	Protocol	Length	Info
45	8.727061800	192.168.100.14	192.168.100.14	LISP	114	Encapsulated Map-Request for Unknown LCAF Type (53)/32
46	8.727552924	10.254.255.3	10.254.255.151	LISP	96	Map-Reply for Unknown LCAF Type (53)/32
47	8.728329839	Vmware_92:7f:e4	Vmware_92:e6:73	ARP	110	[Malformed Packet]
48	9.594282474	Vmware_92:7f:e4	Vmware_92:e6:73	ARP	110	Who has 192.168.100.14? Tell 192.168.100.19

```
▶ Frame 48: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▼ Ethernet II, Src: Cisco_9f:37:e7 (00:00:0c:9f:37:e7), Dst: Cisco_84:bb:76 (70:d3:79:84:bb:76)
  ▶ Destination: Cisco_84:bb:76 (70:d3:79:84:bb:76)
  ▶ Source: Cisco_9f:37:e7 (00:00:0c:9f:37:e7)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.254.255.151, Dst: 10.254.255.152
▶ User Datagram Protocol, Src Port: 65480, Dst Port: 4789
▼ Virtual eXtensible Local Area Network
  ▶ Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 8191
    Reserved: 0
▼ Ethernet II, Src: Vmware_92:7f:e4 (00:50:56:92:7f:e4), Dst: Vmware_92:e6:73 (00:50:56:92:e6:73)
  ▶ Destination: Vmware_92:e6:73 (00:50:56:92:e6:73)
  ▶ Source: Vmware_92:7f:e4 (00:50:56:92:7f:e4)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Vmware_92:7f:e4 (00:50:56:92:7f:e4)
    Sender IP address: 192.168.100.19
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.100.14
```

MAP request/reply from Fabric Edge for Mapping

VXLAN header

Unicast Destination MAC

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device tracking

- Device tracking facilitates learning of End Points for Layer 2 Operation
- Learning happens for IPv4 and IPv6
- Probes used to verify/maintain reachability
- Remote entries shown via Interface Tunnel 0, shorter aging time, no probing

```
Edge_1#show device-tracking database vlanid 1022
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - [illegible] flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:[illegible]
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  age   sta[illegible]
ARP 192.168.1.101              70e4.22e5.c4f7  Tu0            1022  0005   10s  REA[illegible]
ND  FE80::250:56FF:FE92:6D39   0050.5692.6d39  Gi1/0/1        1022  0005    4mn REACHABLE  16 s try 0
DH4 192.168.1.100              0050.5692.6d39  Gi1/0/1        1022  0025    20s REACHABLE  289 s try 0
L   192.168.1.1                0000.0c9f.f45d  Vl1022         1022  0100 5109mn REACHABLE
```

Remote Entry

Local Client

Anycast SVI

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Local Mappings

- LISP maintains local database for Address Resolution
- Address Resolution is part of the Layer 2 Instance.
- Both IPv4 and IPv6 Address are registered with Control Plane Node

```
Edge_1#show lisp instance-id 8190 ethernet database address-resolution
LISP ETR Address Resolution for EID-table VLAN 1022 (IID 8190)
(*) -> entry being deleted
Hardware Address        Host Address          L3 InstID
0050.5692.6d39          FE80::250:56FF:FE92:      4100
                        192.168.1.100/32          4100
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CP Address Resolution Mapping Info

- Control Plane Node maintains Address Resolution table for Layer 2 Instances
- Other Fabric Edges send mapping request to CP node when ARP entry is being received.
- CP Node responds to mapping queries from Fabric Edges

```
CP_2#show lisp instance-id 8190 ethernet server address-resolution
Address-resolution data for router lisp 0 instance-id 8190
L3 InstID    Host Address                                Hardware Address
     4100    192.168.1.100/32                            0050.5692.6d39
     4100    192.168.1.101/32                            70e4.22e5.c4f7
     4100    FE80::250:56FF:FE92:6D39/128                0050.5692.6d39
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

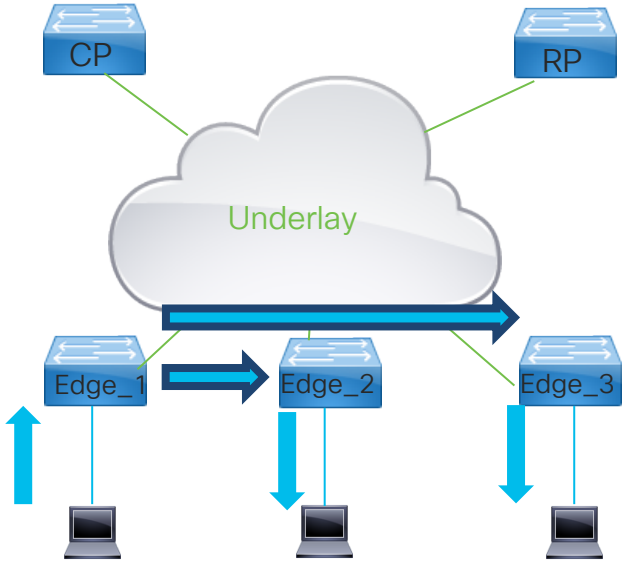
Multicast in the Fabric

Multicasting in the Fabric

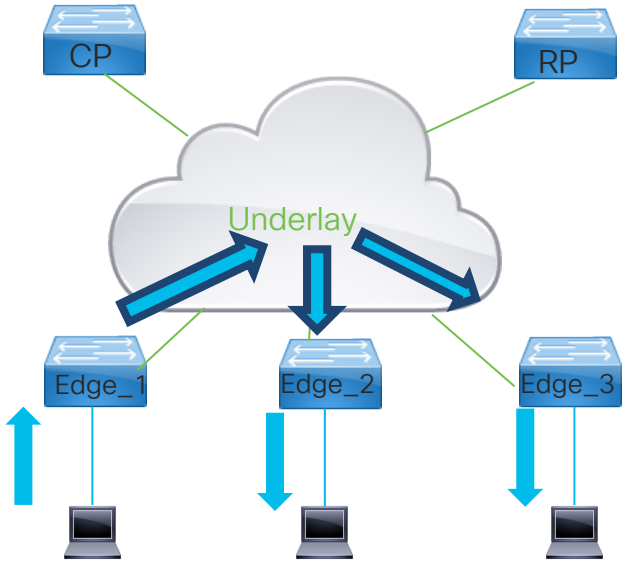
- Multicasting in the overlay for SD Access modes:
  - Head End Replication mode, multicast packets are replicated using unicast encapsulation to all fabric devices (that joined the group.)
  - Native Multicast relies on underlay multicast topology using SSM groups Overlay Multicast groups are hashes to a range of groups in underlay network. Hashing collisions can occur but should not present unwanted traffic flooded to clients
- Head End Replication can be enabled regardless of underlay multicast capable
- Native Multicast prevents Packet Duplication

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multicast Overview



Head End Replication
One destination one packet



Native Multicast
One packet to all destinations

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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)
  Doing 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 ()
  Doing 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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Native Multicast – First Hop Router

```
Edge_1#show ip mroute vrf CiscoLive 239.100.100.100 verbose
IP Multicast Routing Table
(*, 239.100.100.100), 23:32:06/stopped, RP 192.168.200.1, flags: SPF
  Incoming interface: LISP0.4100, RPF nbr 172.31.255.28, LISP:
[172.31.255.28, 232.0.3.1]
  Outgoing interface list: Null
(192.168.1.100, 239.100.100.100), 23:32:06/00:02:53, flags: FTp
  Incoming interface: Vlan1022, RPF nbr 0.0.0.0
  Outgoing interface list:
    LISP0.4100, (172.31.255.109, 232.0.3.1), Forward/Sparse,
17:09:05/stopped, p
      172.31.255.111, 17:09:04/00:03:07
      172.31.255.110, 17:09:05/00:02:41
```

Underlay Group

Subscribers

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Native Multicast – First Hop Router

```
Edge_1#show ip mfib 172.31.255.109 232.0.3.1
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
second
Other counts:       Total/RPF failed/Other drops
I/O Item Counts:    FS Pkt Count/PS Pkt Count
Default
 (172.31.255.109,232.0.3.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 1/1/0
   HW Forwarding:   61913/1/102/0, Other: 0/0/0
   GigabitEthernet1/0/24 Flags: F NS
     Pkts: 0/0
```

SSM group overlay uses

Egress port

- In underlay network, the Overlay traffic is sent encapsulated in VXLAN
- Traffic is sent as a multicast with source the RLOC of this fabric device

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Native Multicast – Egress Router

```
Edge_2#show ip mroute 232.0.3.1
IP Multicast Routing Table
(172.31.255.28, 232.0.3.1), 17:38:29/00:00:30, flags: sT
  Incoming interface: GigabitEthernet2/0/47, RPF nbr 172.31.250.64
  Outgoing interface list:
    Null0, Forward/Dense, 17:38:29/stopped
(172.31.255.109, 232.0.3.1), 17:38:29/00:00:30, flags: sT
  Incoming interface: GigabitEthernet2/0/47, RPF nbr 172.31.250.64
  Outgoing interface list:
    Null0, Forward/Dense, 17:38:29/stopped
```

*,G , sourced at RP

S,G , sourced at FHR

- Egress Interface showing Null. Traffic is being De-encapsulated
- RPF neighbor for Underlay Multicast group is upstream router

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Native Multicast, Egress Router

- At the Egress Fabric Device traffic is de-encapsulated and sent out
- RPF neighbor in Overlay is the RLOC of encapsulating device

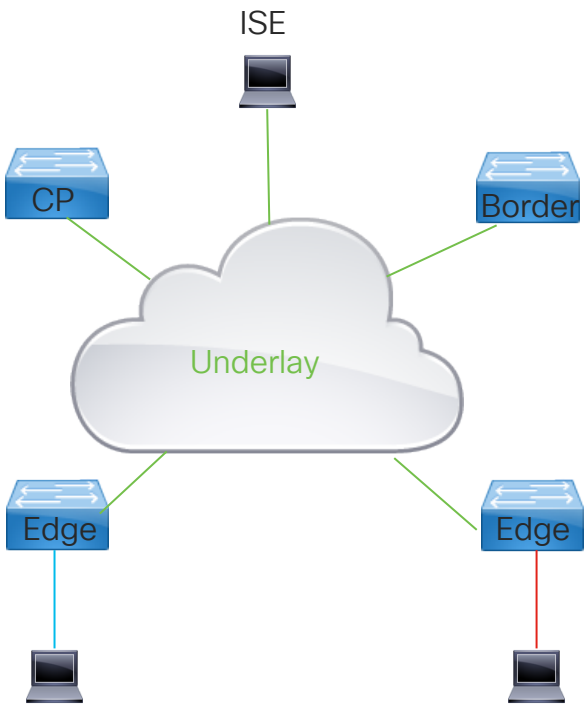
```
Edge_2#show ip mroute vrf CiscoLive 239.100.100.100
(*, 239.100.100.100), 1d00h/stopped, RP 192.168.200.1, flags: SJC
  Incoming interface: LISP0.4100, RPF nbr 172.31.255.28
  Outgoing interface list:
    Vlan1024, Forward/Sparse, 22:02:36/00:02:42
(192.168.1.100, 239.100.100.100), 22:02:35/00:01:21, flags: JT
  Incoming interface: LISP0.4100, RPF nbr 172.31.255.109
  Outgoing interface list:
    Vlan1024, Forward/Sparse, 22:02:35/00:02:42
Edge_2#show ip igmp snooping groups
VLAN      Group                    Type        Version     Port List
------------------------------------------------------------------------
1024      239.100.100.100          igmp        v3          Gi2/0/1
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security in the Fabric

Authentication in the Fabric

- Switch based authentication provides:
  - Access Control to Fabric
  - Assignment to VN/Pool
  - Policy Assignment to Endpoint
- ISE recommended, not mandatory
- Switches use 802.1x and MAC Address Bypass (MAB) to authenticate endpoints
- ISE can use profiling to determine type of endpoint



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Authentication Profiles

- Default Profile per Fabric, applied to all Layer 2 Interfaces
  Can be overridden using host onboarding on Cisco DNA Center
- Order of Authentication methods and timers can be tuned on Cisco DNA Center
- Authentication profiles:
  - Closed Authentication, Most Secure
    Dot1x & MAB using Closed Authentication
  - Open Authentication, Moderately Secure
    Dot1x & MAB using Open authentication
  - Easy Connect, Moderately Secure
    Dot1x & MAB using open authentication and pre-auth ACL
  - No Authentication, Unsecure

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Access Session details

```
Edge_3#show access-session interface gigabitEthernet 1/0/1 details
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x19558A98
          MAC Address:  70e4.22e5.c4f7
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.1.101
            User-Name:  CLtestuser
          Device-type:  Cisco-Device
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC1FFA45000000107B7EA0EB
      Acct Session ID:  0x00000005
               Handle:  0x1d000006
       Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
```

- IPv4/IPv6 info from device tracking
- Username that authenticates
- Device-type from profiling
- Domain: Data or Voice
- Control Direction: in or both
- Policy: Applied policy on interface

- Server Policies, sent from RADIUS
- Method : DOT1x or MAB and its state

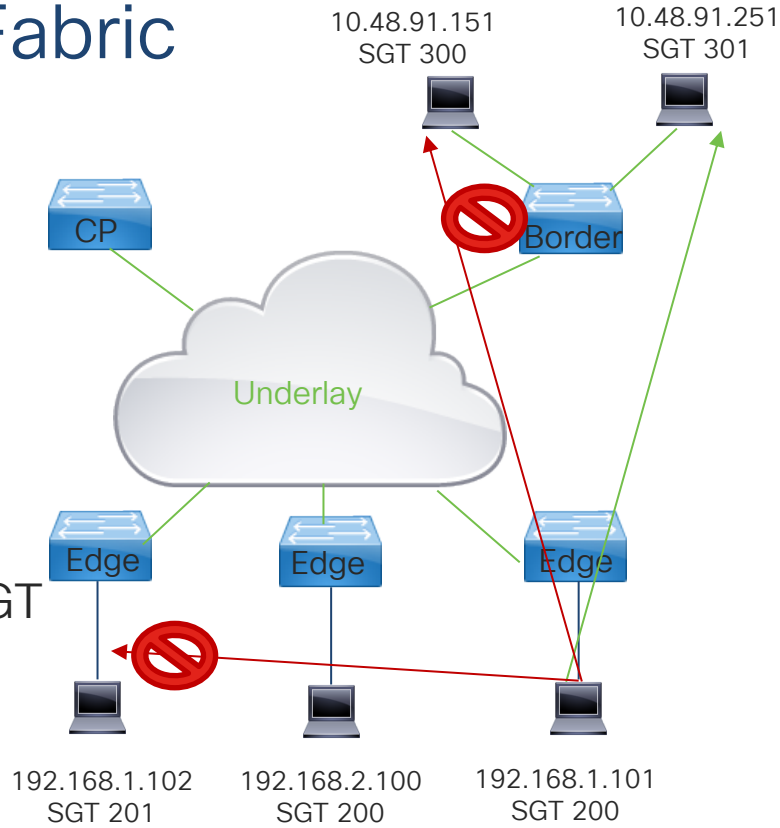
```
Server Policies:
            VLAN Group:  VLAN: 1022
             SGT Value:  200

Method status list:
        Method           State
         dot1x           Authc Success
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Policies inside the Fabric

SGT	Endpoint
200	192.168.1.101
201	192.168.1.102
200	192.168.2.100
300	10.48.91.151
301	10.48.91.251

SRC	DST	Action
200	301	Permit ssh Deny any
200	300	Deny ssh Permit any
200	201	Deny ssh Deny telnet Permit any



- Security based on Cisco TrustSec Solution
- Policy header inside VXLAN header carries SGT
- Every endpoint assigned SGT Traffic policies enforced on egress not ingres
- Policies downloaded from ISE based on groups

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 download permissions for all SGT on switch (Destination mappings only)
- Traffic being allowed/denied based upon SGT -> DGT mapping
- Traffic policy can be deny all, permit all, or SGACL
- Default action applied to all cells not populated.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CTS environment data

```
Edge_1#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-01:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.91.222, port 1812, A-ID 25FCBAE325B2C0E4073058F860957868
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-01:Unknown
   ..
    20-00:Phones
    200-01:CL_Client_1
    201-01:CL_Client_2
   ..
Environment Data Lifetime = 86400 secs
Last update time = 16:26:35 UTC Wed Jan 8 2020
Env-data expires in   0:20:50:45 (dd:hr:mm:sec)
Env-data refreshes in 0:20:50:45 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

CTS environment data from ISE. Crucial for Enforcement to occur

Radius server used

Groups known on ISE

ISE can trigger CoA to update

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CTS Enforcement

- 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

```
Edge_1#show cts role-based sgt-map vrf CiscoLive all
Active IPv4-SGT Bindings Information
IP Address              SGT     Source
============================================
192.168.1.102           201     LOCAL
CP_2#show cts role-based sgt-map vrf CiscoLive all
Active IPv4-SGT Bindings Information
IP Address              SGT     Source
============================================
10.48.91.151            300     SXP
10.48.91.251            301     SXP
```

Endpoint IP assigned SGT 201 via 802.1x

Border learned 2 mappings via SXP to ISE Server

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CTS Policies

- Fabric Devices only Downloaded Policies it needs enforcing (egress enforcement) and is present on ISE
- All other traffic will hit a * * policy
- RBACL names are appended with a version,
  Ex: NoTelnet-00 is version 00 of RBACL name NoTelnet

```
CP_2#show cts role-based permissions to 300
IPv4 Role-based permissions from group 200:CL_Client_1 to group 300:CL_Servers_1:
AllowSSHPING-00
IPv4 Role-based permissions from group 201:CL_Client_2 to group 300:CL_Servers_1:
allowping-00
CP_2#show cts rbacl AllowSSHPING
CTS RBACL Policy
  name    = AllowSSHPING-00
  refcnt = 4
    RBACL ACEs:
    permit tcp dst eq 22
    permit icmp
    deny ip
```

```
CP_2#show cts rbacl allowping
CTS RBACL Policy
  name    = allowping-00
   refcnt = 4
  RBACL ACEs:
    permit icmp
    deny tcp dst eq 22
    permit ip
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring SGT traffic

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

```
CP_2#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           0           0           13          0           0
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

CISCO

Possibilities

#CiscoLive