cisco Live!

ALL IN

#CiscoLive

The bridge to possible

SD Access: Advanced Fabric Troubleshooting

Michel Peters
Technical Leader Engineering
BRKTRS-3010

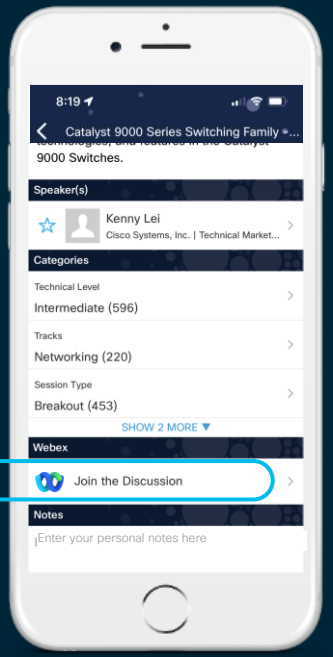
Cisco Webex App

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/#BRKTRS-3010

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

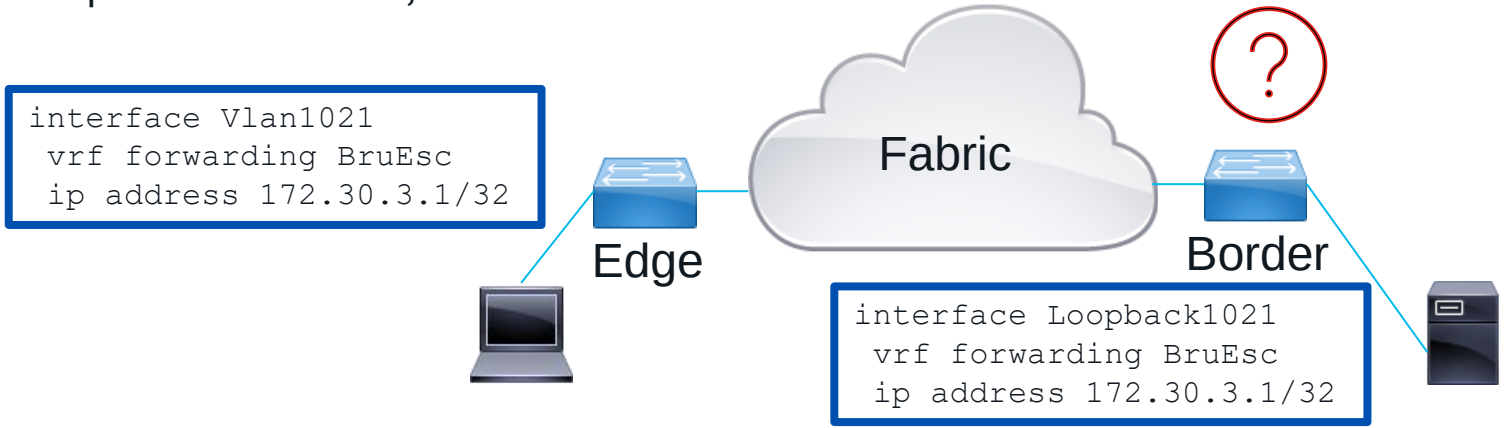
Agenda

- Introduction
- DHCP in the fabric
- SDA Multisite w/SD Access Transit
- Secure Fabric

DHCP in the fabric

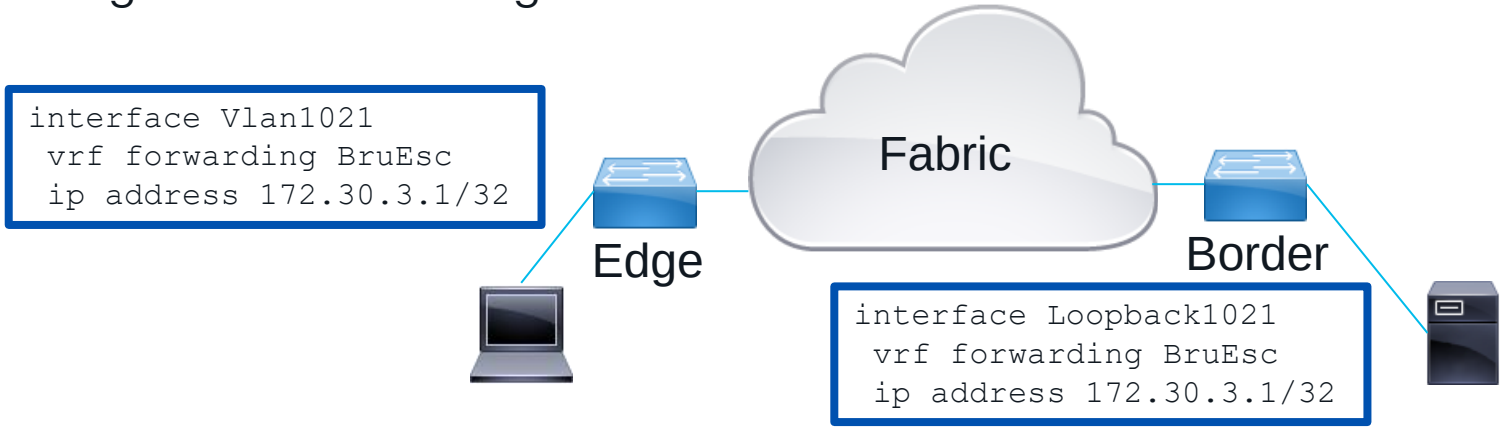
DHCP in the fabric. The problem

- Host sends DHCP Discover
- Edge snoops packet and relays it to the IP helper address
  Setting the gateway IP Address to Switches SVI (anycast IP)
  All edges and the border have this IP addres
- Border de-encapsulates the packet, sends to DHCP server
- DHCP Offer send by DHCP server send back to Anycast IP.
- Border punts packet to CPU, unable to determine where to send now



DHCP in the fabric. The solution

- Host sends DHCP Discover
- DHCP Snooping inserts lisp 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 punts packet to CPU and extracts the option 82 and forwards through fabric to the Edge who forwards it to client



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 001003 01 0A305B01

03 Sub option lisp
08 Length of option
001003 = 4099 in decimals ->LISP Instance ID 4099
01= IPV4 locator
AC.1E.E9.01 = 172.30.233.1 Source locator (Loopback 0 of xTR)

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
- Show platform dhcpsnooping

DHCP steps on Edge

1. Fabric Edge snoops DHCP packet and punts to DHCP snooping process
2. DHCP snooping process inserts Option 82 information
3. DHCP snooping process punts modified DHCP packet to DHCP relay process
4. DHCP relay process sets GI address to SVI IP Addres
5. Fabric Edge encapsulates packet in VXLAN and sends to Border
6. Response packet gets de-encapsulated and punted to CPU
7. DHCP relay process forwards packet to DHCP snooping process
8. Option 82 removed from DHCP packet
9. Packet forwarded to egress port after looking up mac-address

DHCP Debug – DHCP Snooping

```
1042852: Jun 15 02:32:39.780: DHCP_SNOOPING: received new DHCP packet from input interface
(TenGigabitEthernet1/0/11)
1042853: Jun 15 02:32:39.781: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPREQUEST, input interface: Te1/0/11, MAC da: ffff.ffff.ffff, MAC sa: 10f9.206d.e5b6, 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: 10f9.206d.e5b6, efp_id: 0, vlan_id: 1021,
bootpflag:0x0(Unicast)
1042854: Jun 15 02:32:39.781: DHCP_SNOOPING: add relay information option.
1042855: Jun 15 02:32:39.781: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
1042856: Jun 15 02:32:39.781: :VLAN case : VLAN ID 1021
1042858: Jun 15 02:32:39.781: LISP ID is valid, encoding RID in srloc format
1042859: Jun 15 02:32:39.781: DHCP_SNOOPING: binary dump of relay info option, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0x3 0xFD 0x1 0xB 0x2 0xA 0x3 0x8 0x0 0x10 0x3 0x1 0xAC 0x1E 0xE9 0x1
1042860: Jun 15 02:32:39.782: DHCP_SNOOPING: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (1021)
1042861: Jun 15 02:32:39.782: DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan1021.
```

Packet snooped , option 82 inserted and punted to DHCP relay process

DHCP Debug –DHCP Relay

DHCP Relay functionality sets GI address in DHCP packet and forwards to DHCP server

```
Jun 15 02:32:39.783: DHCPD: Finding a relay for client 10f9.206d.e5b6 on interface
Vlan1021.
Jun 15 02:32:39.783: DHCPD: Looking up binding using address 172.30.3.1
Jun 15 02:32:39.783: DHCPD: setting giaddr to 172.30.3.1.
Jun 15 02:32:39.783: DHCPD: BOOTREQUEST from 10f9.206d.e5b6 forwarded to 10.48.91.148.
```

Reply packet from DHCP server received by relay and forwarded

```
Jun 15 02:32:43.407: DHCPD: forwarding BOOTREPLY to client 10f9.206d.e5b6.
Jun 15 02:32:43.407: DHCPD: creating ARP entry (172.30.3.2, 10f9.206d.e5b6, vrf BruEsc).
Jun 15 02:32:43.407: DHCPD: Address 172.30.3.2 is not local and is in configured LISP EID
space
Jun 15 02:32:43.408: DHCPD: egress Interfce Vlan1021
Jun 15 02:32:43.408: DHCPD: unicasting BOOTREPLY to client 10f9.206d.e5b6 (172.30.3.2).
Jun 15 02:32:43.408: DHCPD: Address 172.30.3.2 is not local and is in configured LISP EID
space
Jun 15 02:32:43.408: DHCPD: egress Interface Vlan1021, called by server 0, reply to relay
0, Interface index 58, subindex 0, Vrf id 2, inner vlan 4096, outer vlan 0
```

DHCP Debug -Snooping

```
Jun 15 02:32:43.408: DHCP_SNOOPING: received new DHCP packet from input interface (Vlan1021)
Jun 15 02:32:43.408: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input
interface: Vl1021, MAC da: 10f9.206d.e5b6, MAC sa: 0000.0c9f.f377, IP da: 172.30.3.2, IP sa:
172.30.3.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 172.30.3.2, DHCP siaddr: 0.0.0.0, DHCP giaddr:
172.30.3.1, DHCP chaddr: 10f9.206d.e5b6, efp_id: 0, vlan_id: 1021, bootpflag:0x0(Unicast)
Jun 15 02:32:43.408: DHCP_SNOOPING: binary dump of option 82, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0x3 0xFD 0x1 0xB 0x2 0xA 0x3 0x8 0x0 0x10 0x3 0x1 0xAC 0x1E 0xE9 0x1
Jun 15 02:32:43.409: DHCP_SNOOPING: binary dump of extracted circuit id, length: 8 data:
0x1 0x6 0x0 0x4 0x3 0xFD 0x1 0xB
Jun 15 02:32:43.409: DHCP_SNOOPING: binary dump of extracted remote id, length: 12 data:
0x2 0xA 0x3 0x8 0x0 0x10 0x3 0x1 0xAC 0x1E 0xE9 0x1
Jun 15 02:32:43.409: DHCP_SNOOPING: opt82 data indicates local packet
Jun 15 02:32:43.409: DHCP_SNOOPING: direct forward dhcp replyto output port:
TenGigabitEthernet1/0/11.
```

- DHCP Snooping receives packet from DHCP relay
- Option 82 checked and removed
- Packet bridged to egress port

Show platform dhcpsnoop - Edge

- Show platform dhcpsnooping client command shows detailed view of DHCP operation
- Works on both Edges and Borders

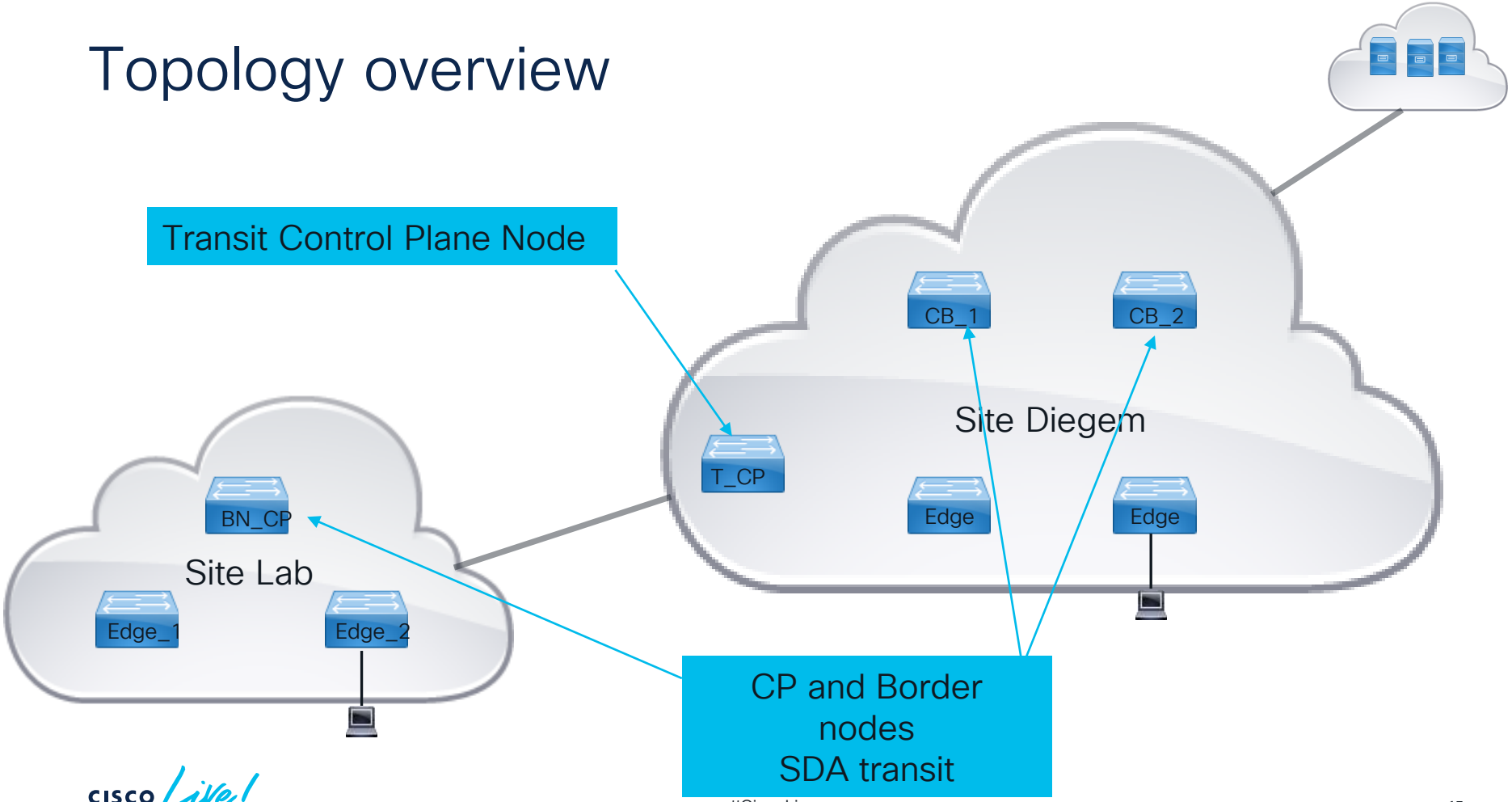
```
Border_CP_1#show platform dhcpsnooping client stats 10f9.206d.e5b6
DHCPSN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
Packet Trace for client MAC 10F9.206D.E5B6:
Timestamp                Destination MAC  Destination Ip  VLAN  Message      Handler:Action
------------------------ ---------------- --------------- ----  ------------ ---------------
2022/06/15 02:32:43.409  FFFF.FFFF.FFFF   172.30.3.1      1     DHCPACK(U)     PUNT:RECEIVED
2022/06/15 02:32:43.409  FFFF.FFFF.FFFF   172.30.3.1      0     DHCPACK(U)     LISP:GLEAN
```

Show platform dhcpsnoop - Edge

```
Edge_2#sh platform dhcpsnooping client stats 10f9.206d.e5b6
DHCPSN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
Packet Trace for client MAC 10F9.206D.E5B6:
Timestamp                Destination MAC  Destination Ip  VLAN  Message      Handler:Action
------------------------ ---------------- --------------- ----  ------------ ----------------
2022/06/15 02:32:43.403  FFFF.FFFF.FFFF   255.255.255.255 1021  DHCPREQUEST(U)  PUNT:RECEIVED
2022/06/15 02:32:43.403  FFFF.FFFF.FFFF   255.255.255.255 1021  DHCPREQUEST(U)  PUNT:TO_DHCPSN
2022/06/15 02:32:43.404  FFFF.FFFF.FFFF   255.255.255.255 1021  DHCPREQUEST(U)  BRIDGE:RECEIVED
2022/06/15 02:32:43.404  FFFF.FFFF.FFFF   255.255.255.255 1021  DHCPREQUEST(U)  BRIDGE:TO_DHCPD
2022/06/15 02:32:43.404  FFFF.FFFF.FFFF   255.255.255.255 1021  DHCPREQUEST(U)  BRIDGE:TO_INJECT
2022/06/15 02:32:43.404  FFFF.FFFF.FFFF   255.255.255.255 1021  DHCPREQUEST(U)  L2INJECT:TO_FWD
2022/06/15 02:32:43.404  0000.0000.003C   10.48.91.148    0     DHCPREQUEST(U)  INJECT:RECEIVED
2022/06/15 02:32:43.404  0000.0000.003C   10.48.91.148    0     DHCPREQUEST(U)  INJECT:TO_L2FWD
2022/06/15 02:32:43.406  FFFF.FFFF.FFFF   172.30.3.1      1021  DHCPACK(U)      PUNT:RECEIVED
2022/06/15 02:32:43.407  FFFF.FFFF.FFFF   172.30.3.2      0     DHCPACK(U)      INJECT:RECEIVED
2022/06/15 02:32:43.407  10F9.206D.E5B6   172.30.3.2      0     DHCPACK(U)      INTERCEPT:RECEIVED
2022/06/15 02:32:43.407  10F9.206D.E5B6   172.30.3.2      1021  DHCPACK(U)      INTERCEPT:TO_DHCPSN
```

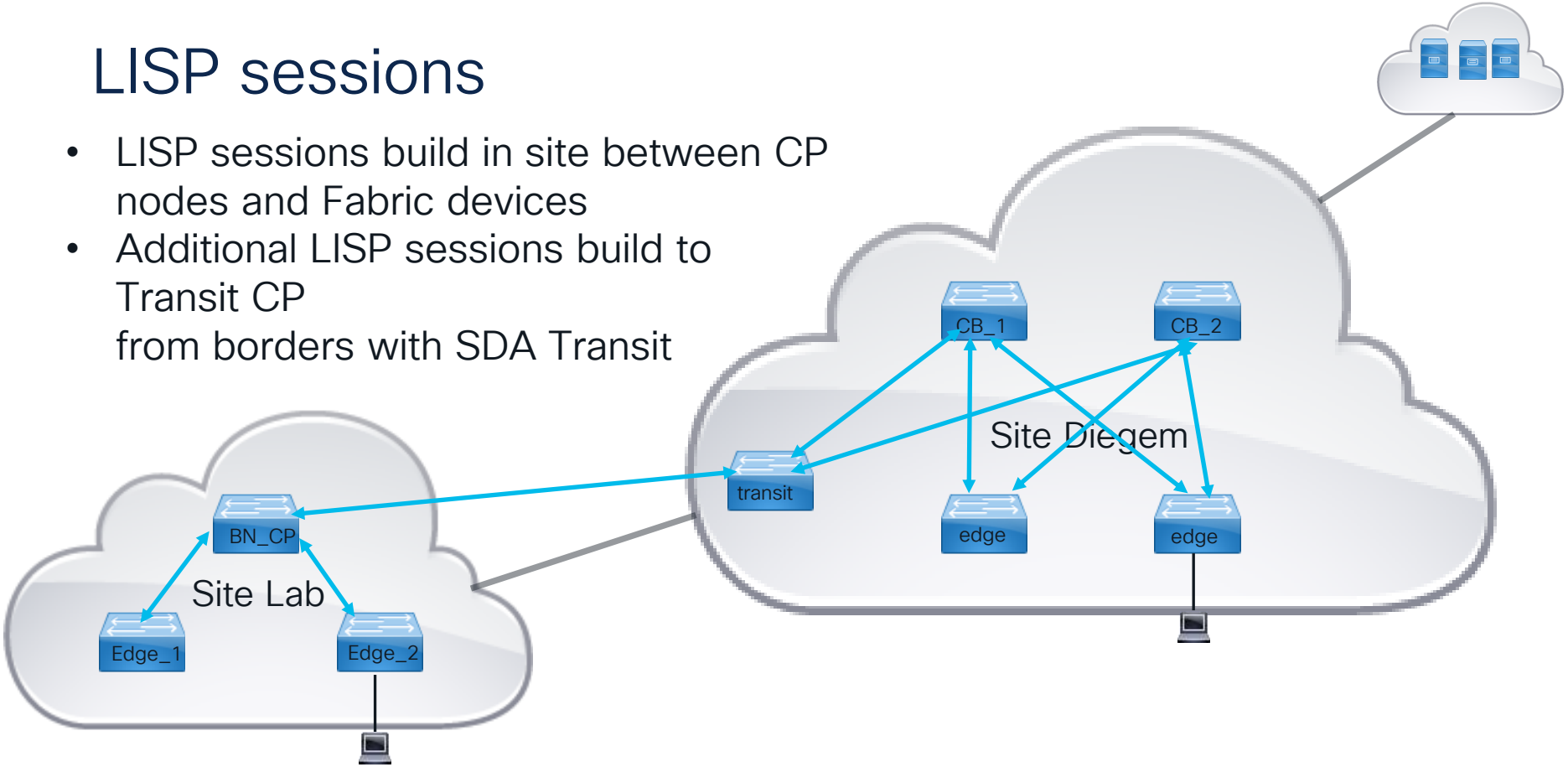
SDA Multisite

Topology overview



LISP sessions

- LISP sessions build in site between CP nodes and Fabric devices
- Additional LISP sessions build to Transit CP
  from borders with SDA Transit



Transit Control Plane LISP sessions

- Borders with SDA transit establish LISP Sessions with Transit Control Plane Node to register EID's for their respective sites

```
T_CP#show lisp session
Sessions for VRF default, total: 6, established: 3
Peer                          State      Up/Down        In/Out    Users
172.30.250.6:51249            Up         1w2d       3912668/4693161 5
172.30.250.7:14459            Up         1w2d       3908138/4365316 5
172.31.255.182:39074          Up         1w2d        47657/980461   5
```

- Site border has LISP session with fabric devices and with Transit CP

```
BN_CP_1#sh lisp session
Sessions for VRF default, total: 5, established: 3
Peer                          State      Up/Down        In/Out    Users
172.30.233.1:51300            Up         1w1d           35/65     10
172.30.233.6:43136            Up         1w1d           76/107    10
172.31.254.18:4342            Up         1w6d       980461/47657  6
```

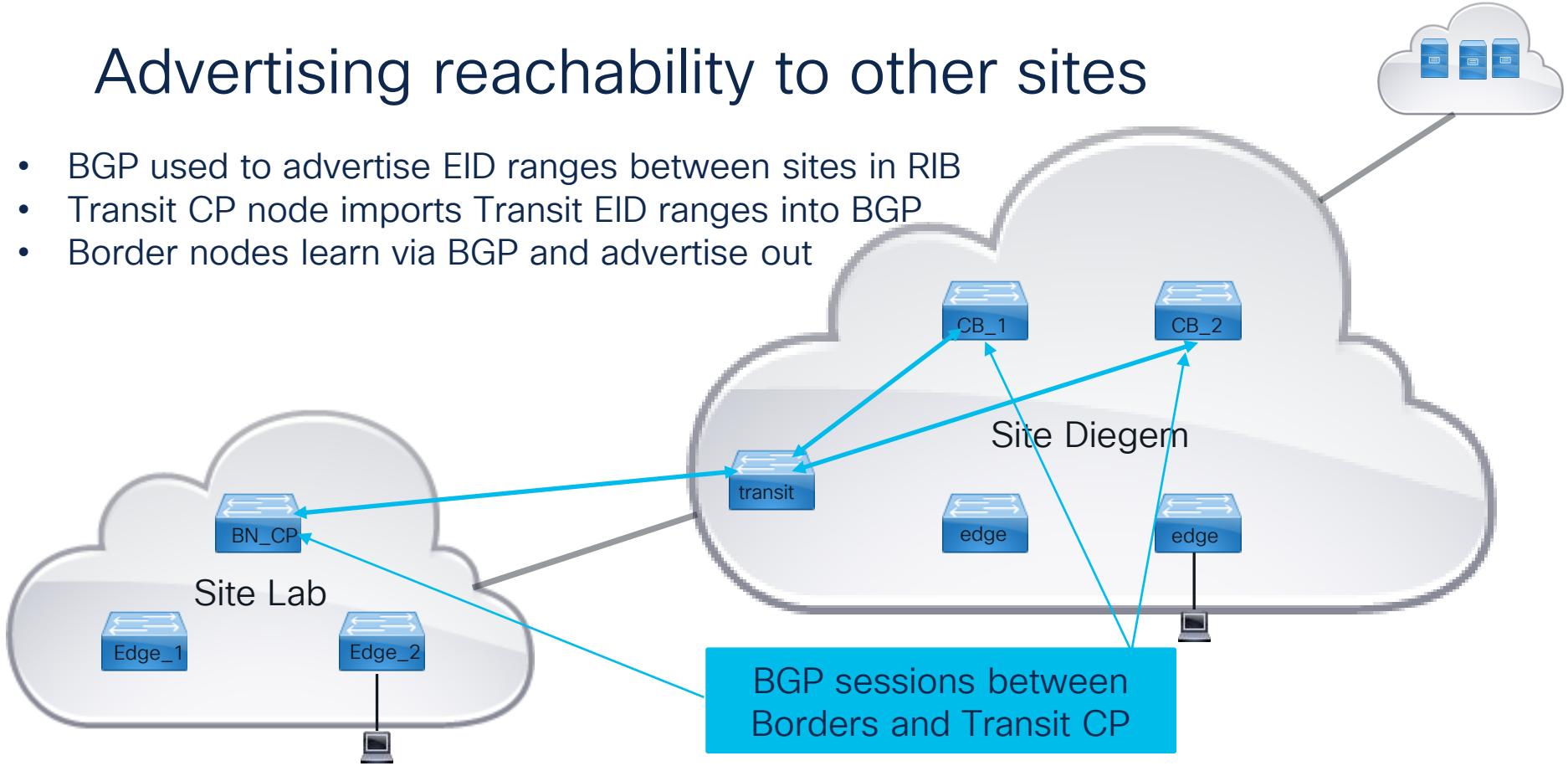
LISP session details

```
T_CP#sh lisp vrf default session  172.30.250.6
Peer address:      172.30.250.6:51249
Local address:     172.31.254.18:4342
Session Type:      Passive
Session State:     Up (1w2d)
Messages in/out:   3912670/4693164
Bytes in/out:      522556968/264531304
Users:             5
  Type                      ID                                    In/Out     State
  Capability Exchange       N/A                                    1/1       waiting
  Policy publisher          lisp 0 IID 4099 AFI IPv4               1/13      working
  MS Reliable Registration  lisp 0 IID 4099 AFI IPv4            3912664/4693138 waiting
    WLC subscription received
  MS Reliable Registration  lisp 0 IID 4097 AFI IPv4               1/0       idle
    WLC subscription received
  MS Reliable Registration  lisp 0 IID 16777214 AFI IPv4           3/3       waiting
    WLC subscription received
```

User count indicates number of Instances having registered

Advertising reachability to other sites

- BGP used to advertise EID ranges between sites in RIB
- Transit CP node imports Transit EID ranges into BGP
- Border nodes learn via BGP and advertise out



Packet Forwarding – Advertising routes to the outside

- Route-maps in place on transit CP to prevent routing loops
- Imports Transit EID's from lisp and advertised to border nodes

```
router bgp 65540
!
 address-family ipv4
  redistribute lisp metric 10
  neighbor 172.30.250.6 activate
  neighbor 172.30.250.6 send-community both
  neighbor 172.30.250.6 route-map deny-all in
  neighbor 172.30.250.6 route-map tag_transit_eids out
!
 address-family ipv4 vrf BruEsc
  redistribute lisp metric 10
```

Advertising routes to the outside

- Border nodes show route learned via BGP from Transit Control Plane
- Border nodes import routes into lisp's map-cache with action send-map-request

```
CB_1#sh ip route vrf BruEsc 172.30.3.0
Routing Table: BruEsc
Routing entry for 172.30.3.0/24
  Known via "bgp 65200", distance 20, metric 10
  Tag 65540, type external
  Redistributing via lisp
  Last update from 172.31.254.18 1w6d ago
  Routing Descriptor Blocks:
  * 172.31.254.18 (default), from 172.31.254.18, 1w6d ago
      opaque_ptr 0x7F36CBE82778
      Route metric is 10, traffic share count is 1
```

Map-Cache, before map-request

```
BN_CP_1#sh ip bgp vpnv4 vrf BruEsc
BGP table version is 1991, local router ID is 172.31.255.182
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf BruEsc)
 *>   10.48.91.128/25  172.31.254.18           10             0 65540 ?
 *>   172.30.0.0/24    172.31.254.18           10             0 65540 ?
```

- Map-cache populated via route-import with action send map-request
- Traffic send to remote sites will trigger map-request and create complete map-cache entry.

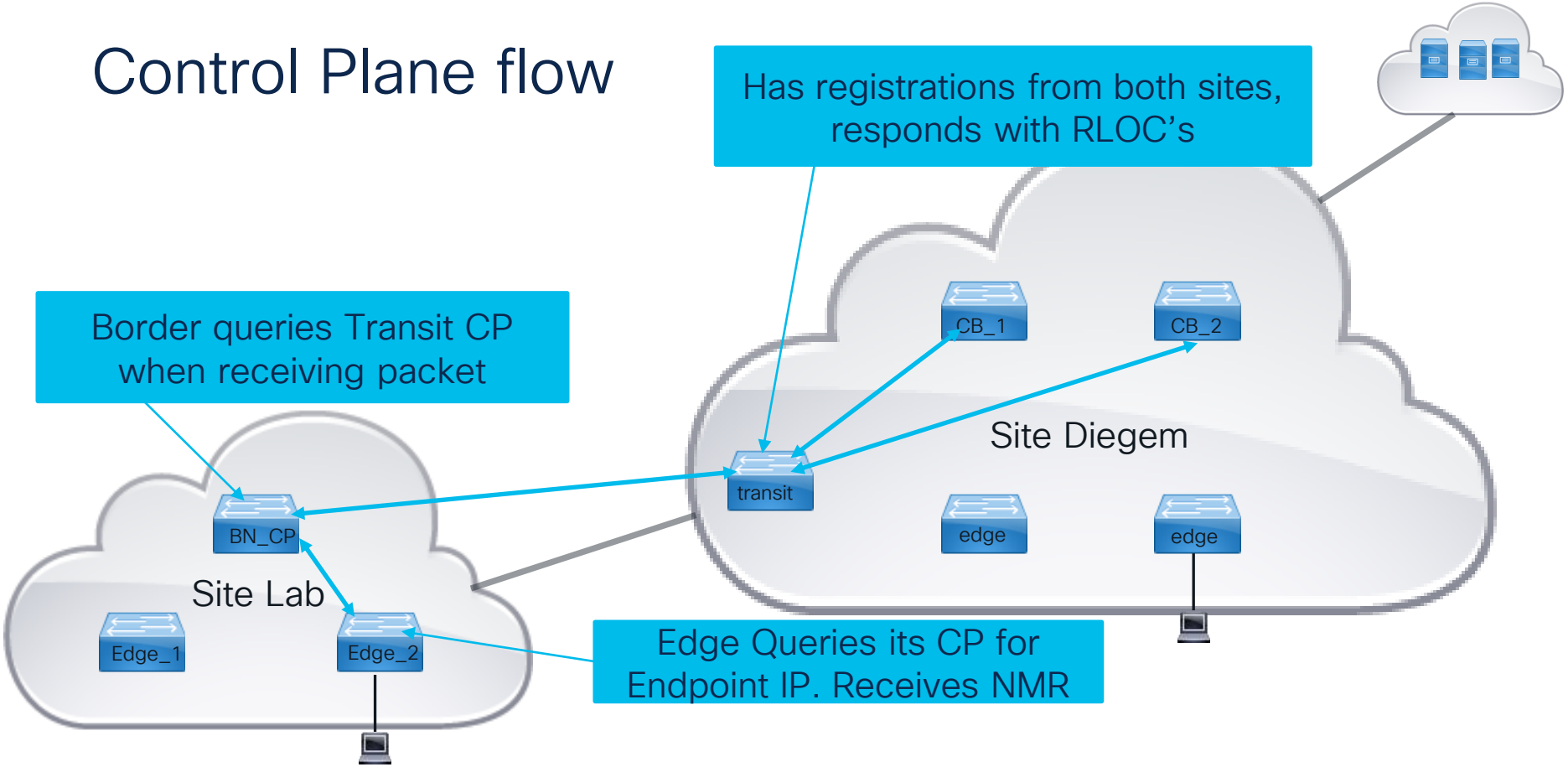
```
BN_CP_1#sh lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 33 entries
10.48.91.128/25, uptime: 1w6d, expires: never, via route-import, send-map-request
  Encapsulating to proxy ETR
172.30.0.0/24, uptime: 1w6d, expires: never, via route-import, send-map-request
  Encapsulating to proxy ETR
```

Routes Advertised to Fusion

- Border nodes with IP transit will advertise out local EID ranges and transit EID ranges.
- Next Hop for transit EID's set to Transit CP IP address in RIB Traffic not forwarded through Transit, FIB will point to LISP

```
CB_2#sh ip bgp vpnv4 all neighbors 172.30.247.14 advertised-routes
     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf BruEsc)
 *>   172.30.0.0/24    0.0.0.0                                32768 i
 *>   172.30.1.0/24    0.0.0.0                                32768 i
 *>   172.30.2.0/25    0.0.0.0                                32768 i
 *>   172.30.2.128/25  172.31.254.18           10                 0 65540 ?
 *>   172.30.2.129/32  172.31.254.18           10                 0 65540 ?
 *>   172.30.3.0/24    172.31.254.18           10                 0 65540 ?
 *>   172.30.4.0/24    172.31.254.18           10                 0 65540 ?
```

Control Plane flow



Local EID registrations

- Local EID ranges on Border nodes get registered with Control Plane node
- Map server ACK confirms registration with Transit Control Plane node.

```
CB_2#sh lisp instance-id 4099 ipv4 database 172.30.0.0/24
LISP ETR IPv4 Mapping Database for EID-table vrf BruEsc (IID 4099), LSBs: 0x3
172.30.0.0/24, locator-set rloc_b3d47f9a-5fe2-4fe1-b23e-ad4b736fd0d6, auto-discover-
rlocs, proxy
  Uptime: 12w6d, Last-change: 2w0d
  Domain-ID: unset
  Service-Insertion: N/A (0)
  Locator        Pri/Wgt  Source     State
  172.30.250.6    10/10   auto-disc  site-other, report-reachable
  172.30.250.7    10/10   cfg-intf   site-self, reachable
  Map-server        Uptime         ACK  Domain-ID
  172.31.254.18     2w0d           Yes  0
```

Transit Control Plane information

- Transit Control Plane shows EID ranges registered from all sites
- SDA transit only supported on External Borders
- Multiple Borders can register EID. Last Registered isnt only Registered

```
T_CP#show lisp site
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
                3d10h      yes#    172.30.250.7:15644    4099      10.48.91.128/25
                1w6d       yes#    172.30.250.6:51249    4099      172.30.0.0/24
                1w6d       yes#    172.31.255.182:39074  4099      172.30.3.0/24
                1w6d       yes#    172.31.255.182:39074  4099      172.30.4.0/24
```

Transit Control Plane EID detail

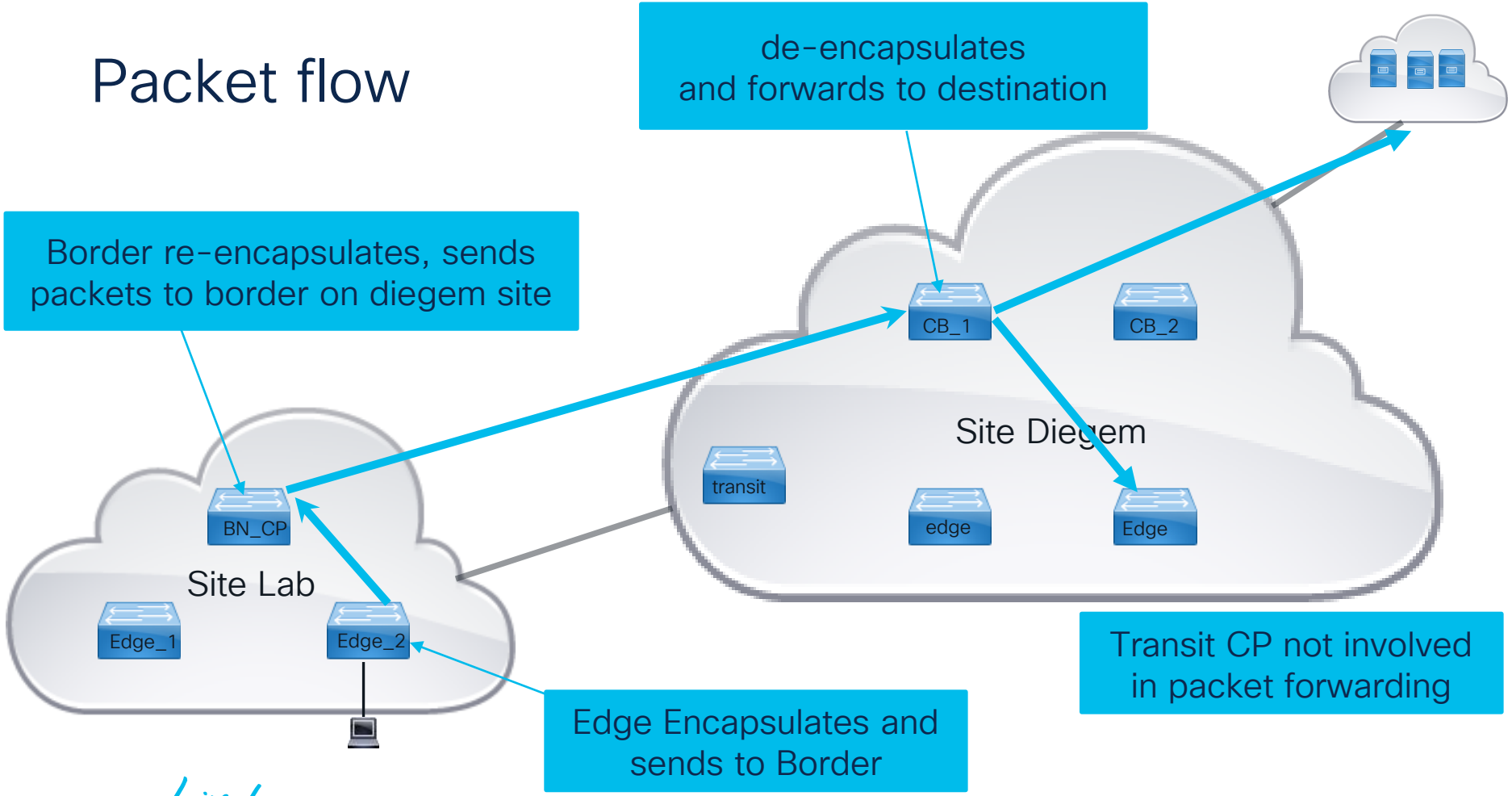
```
T_CP#sh lisp site 172.30.0.0/24 instance-id 4099
LISP Site Registration Information
  EID-prefix: 172.30.0.0/24 instance-id 4099
    First registered:     2w0d
    Last registered:      2w0d
    Routing table tag:    0
    Origin:               Dynamic, more specific of 0.0.0.0/0
    Merge active:         Yes
    Proxy reply:          Yes
    Skip Publication:     No
    Force Withdraw:       No
    TTL:                  1d00h
    State:                complete
    Extranet IID:         Unspecified
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
```

Transit CP EID detail (2)

```
ETR 172.30.250.7:15644, last registered 4d05h, proxy-reply, map-notify
                        TTL 1d00h, merge, hash-function sha1, nonce 0xADABAB12-0xF
                        state complete, routing table tag 65013
                        sourced by reliable transport
  Locator       Local  State      Pri/Wgt  Scope
  172.30.250.7  yes    up          10/10   IPv4 none
ETR 172.30.250.6:27811, last registered 4d05h, proxy-reply, map-notify
                        TTL 1d00h, merge, hash-function sha1, nonce 0x5749E3FA-0x4
                        state complete, routing table tag 65013
                        sourced by reliable transport
  Locator       Local  State      Pri/Wgt  Scope
  172.30.250.6  yes    up          10/10   IPv4 none
Merged locators
  Locator       Local  State      Pri/Wgt  Scope        Registering ETR
  172.30.250.6  yes    up          10/10   IPv4 none    172.30.250.6:27811
  172.30.250.7  yes    up          10/10   IPv4 none    172.30.250.7:15644
```

As both borders advertise the EID range traffic will be loadbalanced

Packet flow



Packet Flow – Edge

```
Edge_2#sh lisp instance-id 4099 ipv4 map-cache 10.48.91.251
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 7 entries
0.0.0.0/1, uptime: 1d00h, expires: 00:07:55, via map-reply, forward-native
  Sources: map-reply
  State: forward-native, last modified: 1d00h, map-source: 172.31.255.182
  Active, Packets out: 11757(3928172 bytes), counters are not accurate (~ 00:02:30 ago)
  Encapsulating to proxy ETR
```

- Edge Device uses Proxy-ETR to send traffic to border with SDA Transit

```
Edge_2#sh ip cef vrf BruEsc 10.48.91.251 detail
0.0.0.0/1, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000000
  LISP remote EID: 11757 packets 3928172 bytes fwd action encap
  LISP source path list
    nexthop 172.31.255.182 LISP0.4099
  2 IPL sources [no flags]
  nexthop 172.31.255.182 LISP0.4099
```

Packet Flow – Border

Map-source showing IP address of Transit CP

```
BN_CP_1#sh lisp instance-id 4099 ipv4 map-cache 10.48.91.128/25
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 32 entries
10.48.91.128/25, uptime: 3d14h, expires: 09:19:13, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 3d14h, map-source: 172.31.254.18
  Exempt, Packets out: 16867(9714520 bytes), counters are not accurate (~ 00:00:36 ago)
  Configured as EID address space
  Locator       Uptime    State  Pri/Wgt     Encap-IID
  172.30.250.6  3d14h     up      10/10        -
    Last up-down state change:         3d14h, state change count: 1
    Last route reachability change:    3d14h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            3d14h (rtt 2ms)
  172.30.250.7  3d14h     up      10/10        -
    Last up-down state change:         3d14h, state change count: 1
    Last route reachability change:    3d14h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            3d14h (rtt 1ms)
```

Packet Flow – Border

- Border on site Lab forwarding packets to both borders on site Diegem
- Packet will be forwarded encapsulated in VXLAN
- ECMP will be used to loadbalance traffic between 2 next hops in overlay

```
BN_CP_1#show ip cef vrf BruEsc 10.48.91.128/25 detail
10.48.91.128/25, epoch 0, flags [subtree context, rib defined all
labels, check lisp eligibility], per-destination sharing
  SC owned,sourced: LISP remote EID - locator status bits 0x00000003
  LISP remote EID: 16867 packets 9714520 bytes fwd action encap, cfg as
EID space
  LISP source path list
    nexthop 172.30.250.6 LISP0.4099
    nexthop 172.30.250.7 LISP0.4099
```

CTS

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 when ingressing fabric, carried through fabric

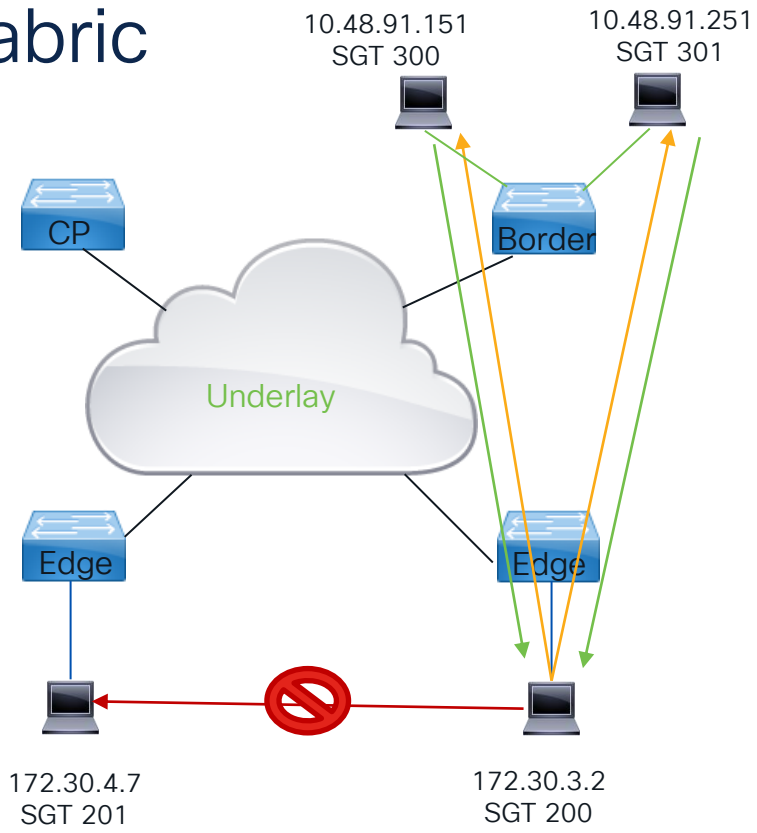
```
> Internet Protocol Version 4, Src: 172.31.255.182, Dst: 172.30.233.6
> User Datagram Protocol, Src Port: 65355, Dst Port: 4789
v Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 300
    VXLAN Network Identifier (VNI): 4099
    Reserved: 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 when leaving fabric
- Use SXP or Static mappings on border to enforce policies and ensure tagging occurs towards fabric



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-date
- 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
000000136239AE5100093A8063C0997BC0371AAC105A77C6D0FD
415E9C5B31ED952C3ACDE42CBA076C57B206341713D49E7AB92D
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 knows 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
```

Border learned 2 mappings via SXP to ISE Server

- 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
```

Usefull 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

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

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

Thank you

cisco Live!

ALL IN

#CiscoLive