

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a radial pattern of lines emanating from a bright white point on the right side, creating a sense of motion and energy.

CISCO *Live!*

Let's go



The bridge to possible

SD Access: Troubleshooting the Fabric

Michel Peters, Technical Leader Engineering

CISCO *Live!*

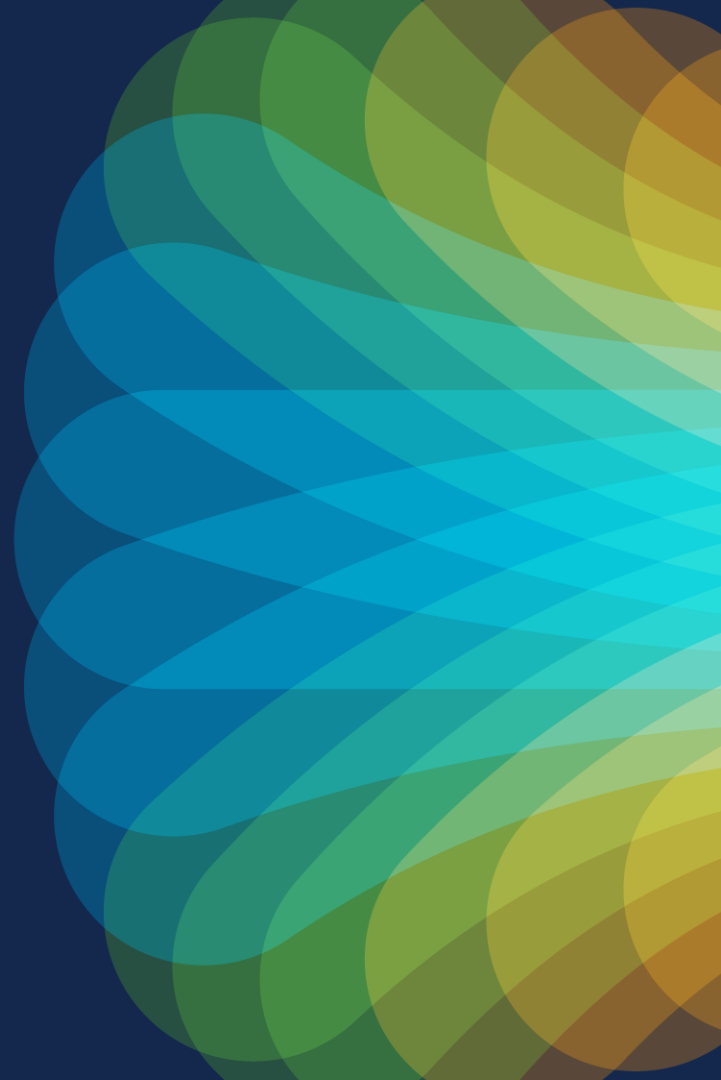
BRKTRS-3820

Agenda

- The Fabric
- Endpoint Registration
- Reaching Remote Endpoints
- Secure Fabric



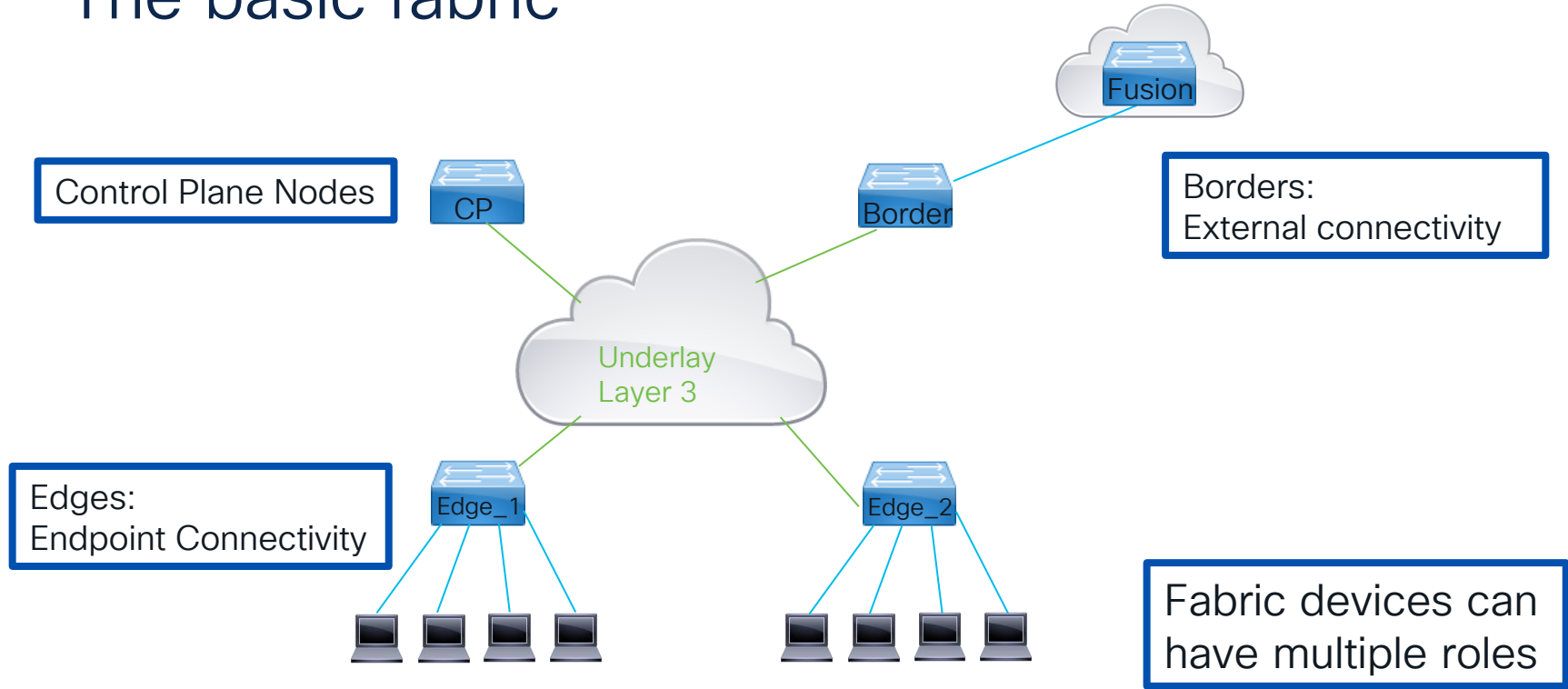
The Fabric



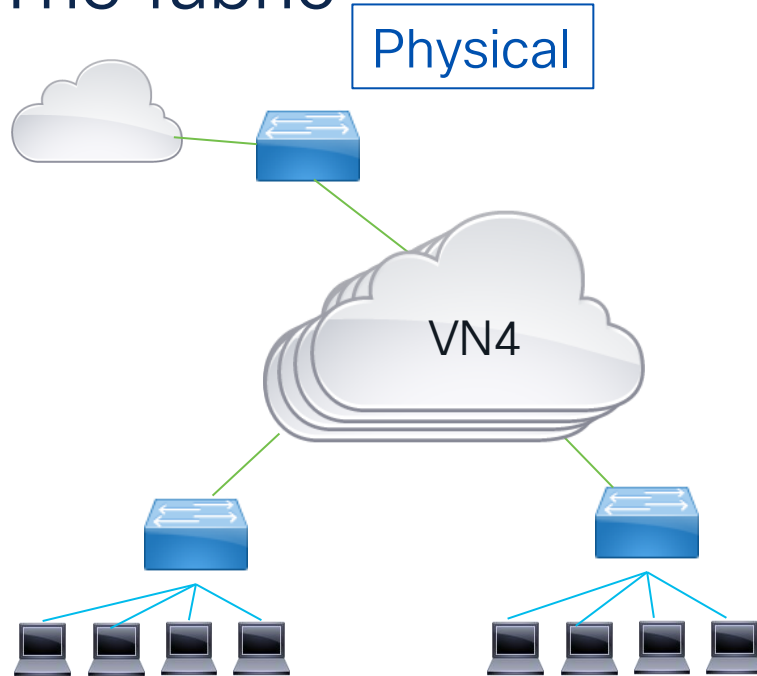
SD Access Fabric Key Technologies

- Locator/ID Separation Protocol,
Control plane protocol inside the fabric
- Cisco TrustSec,
Segmentation, security inside the fabric
- Authentication,
Assignment of endpoints and resources inside the fabric
- VXLAN,
Data plane encapsulation, forwarding traffic between fabric devices

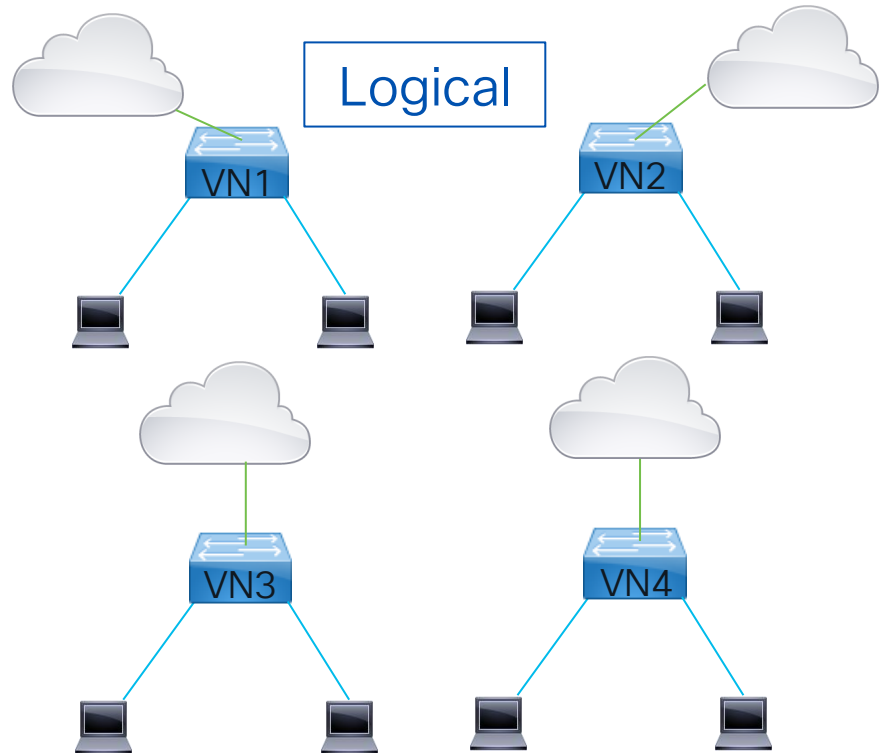
The basic fabric



The fabric



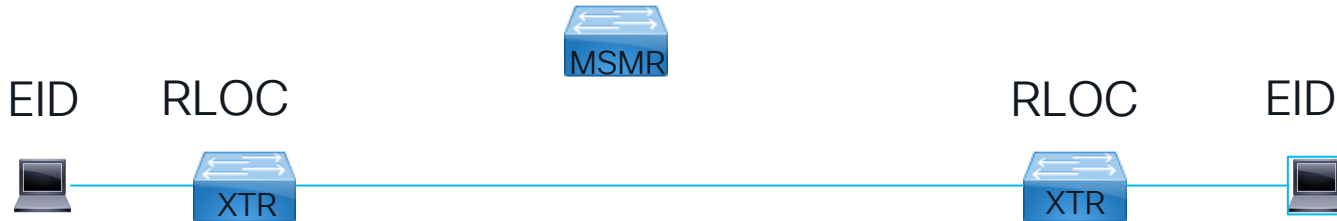
One Underlay



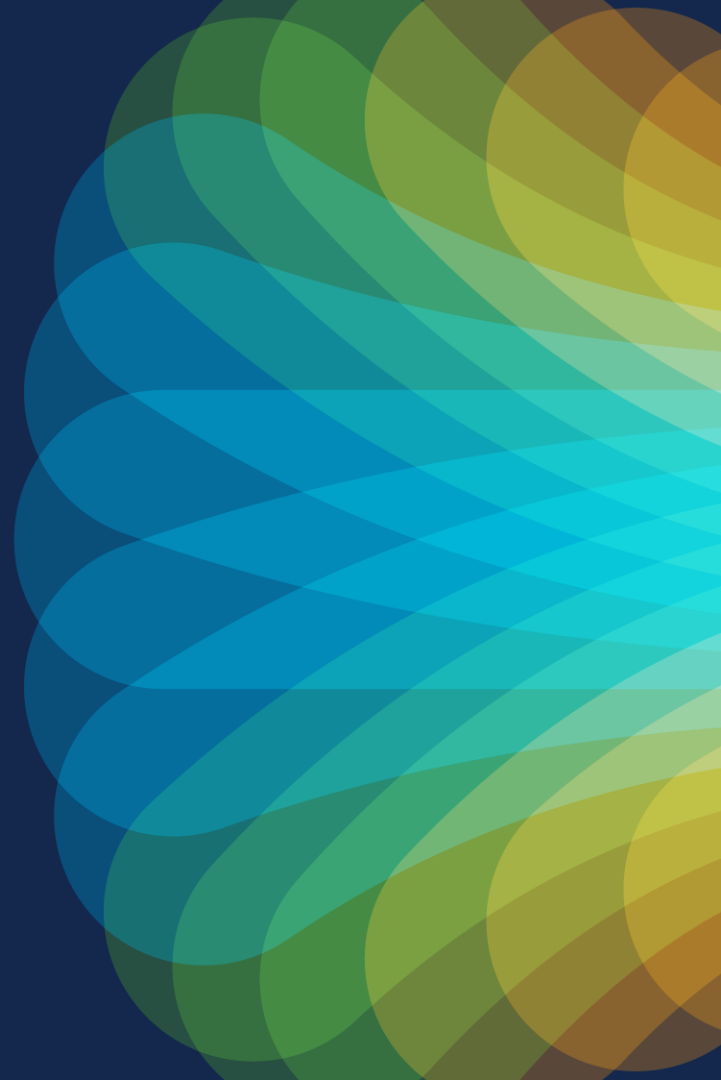
Many Overlays

LISP Basics

- LISP creates a level of indirection between endpoints and location
- Two address spaces, Endpoint Identifiers (EID) and Routing Locators(RLOC)
- XTR (Ingress Tunnel Router + Egress Tunnel routers) responsible for getting traffic through the network and registering/resolving EID
- Reachability established by querying Map Server/Map Resolver nodes
 - Q : Where is EID X
 - A : X is behind RLOC B
- Traffic send from fabric device to fabric device based on RLOC
- Control Plane node hosts Map Server/Map Resolver functionality(MSMR)



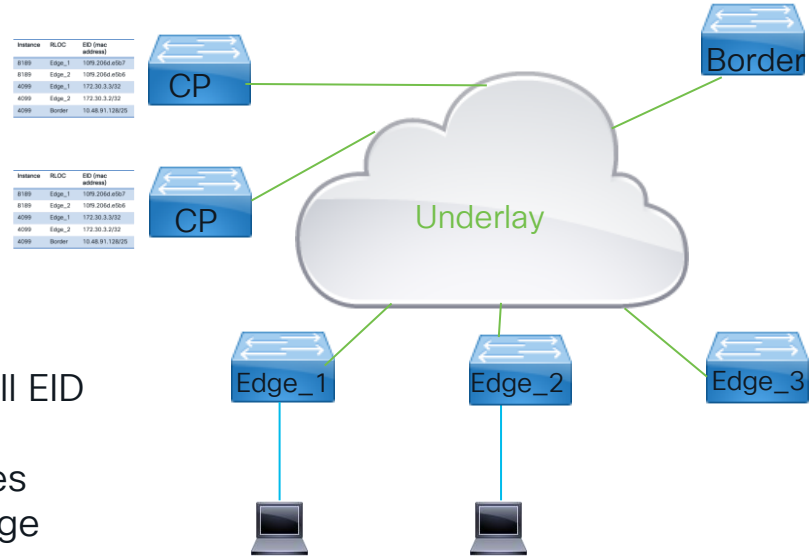
Endpoints Registrations



Control Plane Nodes, Central Database

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	10.48.13.0/24

- Control Plane node contains a database of all EID to RLOC mappings inside the fabric.
- Fabrics can have multiple control plane nodes
- One Layer 3 instance per VRF/VN, 4000 range
- One Layer 2 Instance per VLAN, 8000 range
- Control plane node VLAN and VRF unaware.
Based purely on LISP Instance ID



Control Plane, displaying learned EID

```
Border_1#show lisp instance-id 4100 ipv4 server 172.20.23.4/32
```

```
LISP Site Registration Information
```

```
Site name: site_uci
```

```
Description: map-server configured from Cisco DNA-Center
```

```
Allowed configured locators: any
```

```
Requested EID-prefix:
```

```
  EID-prefix: 172.20.23.4/32 instance-id 4100
```

```
  First registered: 1w0d
```

```
  Last registered: 1w0d
```

```
Routing table tag: 0
```

```
Origin: Dynamic, more specific of 172.20.23.0/24
```

```
Merge active: No
```

```
Proxy reply: Yes
```

```
Skip Publication: No
```

```
Force Withdraw: No
```

```
TTL: 1d00h
```

```
State: complete
```

```
Extranet IID: Unspecified
```

Output/command same
for IPv6/Ethernet

Registration history

Proxy reply, CP responds
for this EID directly

TTL ,lifetime of entry.

Control Plane, displaying learned EID - continued

```
Border_1#show lisp instance-id 4100 ipv4 server 172.20.23.4/32
```

```
..
```

```
Registration errors:
```

```
Authentication failures: 0
```

```
Allowed locators mismatch: 0
```

```
ETR 172.20.106.12:31833
```

```
last registered 1w0d, proxy-reply, map-notify
```

```
TTL 1d00h, no merge, hash-function sha1
```

```
state complete, no security-capability
```

```
nonce 0x6E1E008E-0xF45E4566
```

```
xTR-ID 0xD98B502D-0x8988F718-0xF5D51AF0-0xE402FBC9
```

```
site-ID unspecified
```

```
Domain-ID 2737483936
```

```
Multihoming-ID unspecified
```

```
sourced by reliable transport
```

Locator	Local	State	Pri/Wgt	Scope	RDP
172.20.106.12	yes	up	10/10	IPv4 none	[-]

ETR that registered EID

RLOC information

Priority and Weight for this Locator.

Multiple Locators for an EID

Show only last
registering ETR

```
Border_1#sh lisp instance-id 4100 ipv4 server | inc 10.48.13.0
Site Name   Last      Up      Who Last      Inst      EID Prefix
            Register  Registered  ID
            1wld     yes#    172.31.255.18:27842  4100      10.48.13.0/24
```

```
Border_1#show lisp instance-id 4100 ipv4 server 10.48.13.0/24
ETR 172.31.255.18:27842
```

```
last registered 1wld, proxy-reply, map-notify
TTL 1d00h, merge, hash-function sha1
```

Locator	Local	State	Pri/Wgt	Scope
172.31.255.18	yes	up	10/10	IPv4 none

```
ETR 172.33.250.1:44153
```

```
last registered 1wld, proxy-reply, map-notify
TTL 1d00h, merge, hash-function sha1
```

Locator	Local	State	Pri/Wgt	Scope
172.33.250.1	yes	up	10/10	IPv4 none

```
Merged locators
```

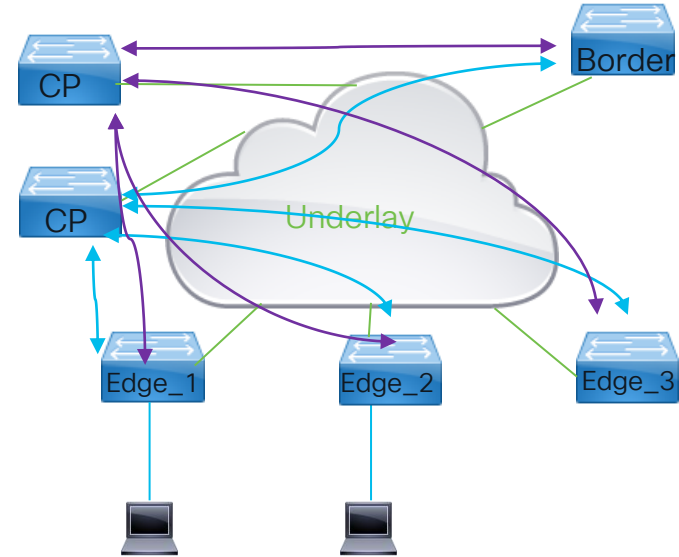
Locator	Local	State	Pri/Wgt	Scope	Registering ETR
172.31.255.18	yes	up	10/10	IPv4 none	172.31.255.18:27842
172.33.250.1	yes	up	10/10	IPv4 none	172.33.250.1:44153

Two ETR's shown to
have registered the EID

Both borders learned
routes and registered
reachability to the EID

Control Plane Nodes, Learning information

- Fabric Devices register EID's towards each Control Plane node
- SDA uses LISP reliable transport
- Borders and Edges have a LISP session towards each CP node
- LISP Session comes up only when there a registration. Often seen on external borders not importing routes
- Same EID's can be registered by multiple Fabric device



LISP sessions

- Every fabric device establishes a LISP session to each CP node.
- CP nodes do not have a session to each other

```
Border_1#sh lisp session
```

```
Sessions for VRF default, total: 14, established: 6
```

Peer	State	Up/Down	In/Out	Users
172.20.106.1:13759	Up	3w2d	60/92	9
172.20.106.7:44599	Up	3w2d	205/224	9
172.31.255.18:4342	Up	3w2d	1051/300	8
172.31.255.18:27842	Up	3w2d	300/1051	8
172.33.250.1:4342	Up	1w0d	807/277	8
172.33.250.1:44153	Up	1w0d	213/840	7

Session from Border to CP on same node.

```
Switch-172-20-106-12#sh lisp session
```

```
Sessions for VRF default, total: 2, established: 2
```

Peer	State	Up/Down	In/Out	Users
172.31.255.18:4342	Up	3w2d	391/381	14
172.33.250.1:4342	Up	1w0d	209/199	14

One session created to each CP node

LISP session, more detail

```
Switch-172-20-106-12#sh lisp vrf Default session 172.33.250.1
```

```
Peer address:      172.33.250.1:4342
```

```
Local address:     172.20.106.12:52814
```

```
Session Type:      Active
```

```
Session State:     Up (1w0d)
```

```
Messages in/out:   209/199
```

```
Bytes in/out:      11365/25244
```

Session should have long
uptime in stable enviroment

Type	ID						State
Pubsub subscriber	lisp 0	IID 4097	AFI IPv4	1/0			Idle
Pubsub subscriber	lisp 0	IID 4100	AFI IPv6	1/0			Idle
ETR Reliable Registration	lisp 0	IID 4100	AFI IPv6	44/43			TCP
ETR Reliable Registration	lisp 0	IID 16777214	AFI IPv4	5/2			TCP
ETR Reliable Registration	lisp 0	IID 4097	AFI IPv4	0/1			TCP
ETR Reliable Registration	lisp 0	IID 4100	AFI IPv4	8/7			TCP
ETR Reliable Registration	lisp 0	IID 8188	AFI MAC	84/140			TCP
ETR Reliable Registration	lisp 0	IID 8189	AFI MAC	0/1			TCP
ETR Reliable Registration	lisp 0	IID 8190	AFI MAC	0/1			TCP
Capability Exchange	N/A						waiting

Users using the session

Virtual Networks and LISP instances

- VRF's & LISP Instance mapped to Virtual Networks
- Dynamic EID range dictate what Endpoints to learn
- Loopback when in overlay configured into Database to register with Control Plane.

```
Edge_1#sh ip vrf VN_One
Name                               Interfaces
VN_One                             Lo4100
                                     V11021
                                     LI0.4100
                                     Tu2
```

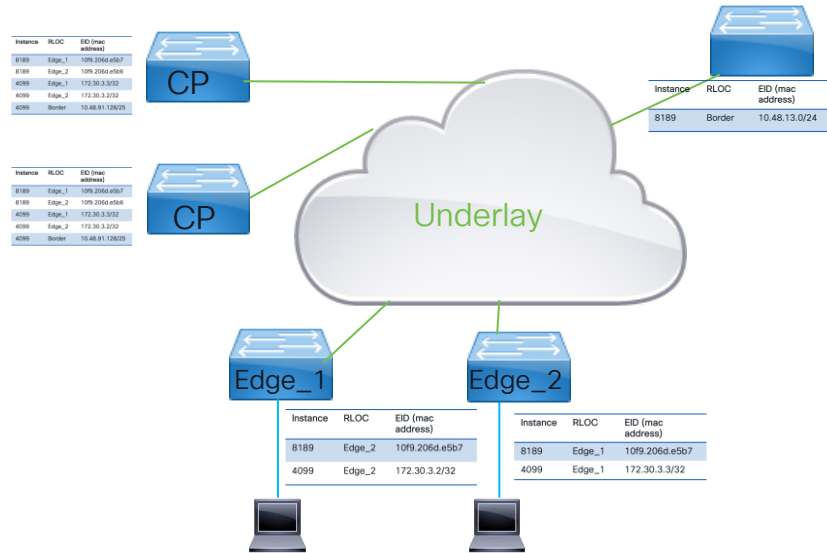
```
router lisp
instance-id 4099
dynamic-eid 172_20_23_0-VN_One-IPV4
  database-mapping 172.20.23.0/24 locator-set rloc_1a8b95ce-6fe8-4608-b273-8453b86072c7
!
dynamic-eid 172_20_23_0-VN_One-IPV6
  database-mapping 2001:DB8::/64 locator-set rloc_1a8b95ce-6fe8-4608-b273-8453b86072c7
!
service ipv4
  eid-table vrf VN_One
  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

Fabric Devices, local LISP database



- Every Fabric Device registers known EID's to create its own local database
- Only local EID are contained in local database
- Database used to register local EID with each Control Plane node
- EID can be Dynamically learned , configured or imported

LISP Database, looking at entries

```
Border_1#sh lisp instance-id 4100 ipv4 database 10.48.13.0/24
```

```
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf VN_One (IID 4100), LSBs: 0x3  
Entries total 1, no-route 1, inactive 0, do-not-register 0
```

```
10.48.13.0/24, route-import, default locator-set rloc_ld, auto-discover-rlocs
```

```
Uptime: 1w5d, Last-change: 1w5d
```

```
Domain-ID: local, tag: 733777
```

```
Service-Insertion: N/A
```

Locator	Pri/Wgt	Source	State
172.31.255.18	10/10	cfg-intf	site-self, reachable
172.33.250.1	10/10	auto-disc	site-other, report-reachable
Map-server	Uptime	ACK	Domain-ID
172.31.255.18	1w5d	Yes	2737483936
172.33.250.1	1w5d	Yes	2737483936

- Behind the EID it indicates where the EID is learned from.
- Route import means its an imported routed, learned via BGP on border node in this example

LISP Database, looking at local entries

```
Switch-172-20-106-1#sh lisp instance-id 4100 ipv4 database 172.20.23.8/32
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf VN_One (IID 4100), LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 1
172.20.23.8/32, dynamic-eid 172_20_23_0-VN_One-IPV4, inherited from default locator-set
rloc_b92acdbc-a469-4b78-882d-c9b12852658a
  Uptime: 04:27:07, Last-change: 04:27:07
  Domain-ID: local
  Service-Insertion: N/A
  Locator      Pri/Wgt  Source      State
  172.20.106.1  10/10    cfg-intf    site-self, reachable
    Affinity-id: 4294967295 , 4294967295
  Map-server    Uptime      ACK  Domain-ID
  172.31.255.18 04:27:07    Yes  0
  172.33.250.1  04:27:07    Yes  0
```

- Only EIDs that are part of Dynamic EID are learned and registered with CP
- Map-Server (CP) sends Ack when an entry is registered.
- Learning happens through ARP/DHCP/ND/RA and Mac Learning

LISP Database, looking at entries

```
Switch-172-20-106-1#show run int vlan 1021 | inc ip address
ip address 172.20.23.1 255.255.255.0
Switch-172-20-106-1#sh lisp instance-id 4100 ipv4 database 172.20.23.1/32
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf VN_One (IID 4100), LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 1
172.20.23.1/32, dynamic-eid 172_20_23_0-VN_One-IPV4, do not register, inherited from
default locator-set rloc_b92acdbc-a469-4b78-882d-c9b12852658a
Uptime: 1w5d, Last-change: 1w5d
Domain-ID: local
Service-Insertion: N/A
Locator      Pri/Wgt  Source      State
172.20.106.1 10/10    cfg-intf    site-self, reachable
Affinity-id: 4294967295 , 4294967295
```

- IP addresses and mac addresses belonging to the Anycast IP are not registered with control plane nodes
- To avoid registration they are put into the database with the “do not register” flag set

Edge Configuration: SVI/VLAN Configuration

- Layer 3 Subnets and Layer 2 Pool configuration on Edges is consistent throughout a fabric site
- SDA uses Anycast IP and Mac. All SVI configurations same on edges
Uses same IP address and Same mac on all Edges
- Connections between edges should be Layer 3, avoid mac-learning issues

```
Switch-172-20-106-7#sh run int vlan 1021
interface Vlan1021
  mac-address 0000.0c9f.f377
  vrf forwarding VN_One
  ip address 172.20.23.1 255.255.255.0
  ip helper-address 10.48.91.148
  no lisp mobility liveness test
  lisp mobility 172_20_23_0-VN_One-IPv4
```

```
Switch-172-20-106-7#sh run int vlan 1021
interface Vlan1021
  mac-address 0000.0c9f.f377
  vrf forwarding VN_One
  ip address 172.20.23.1 255.255.255.0
  ip helper-address 10.48.91.148
  no lisp mobility liveness test
  lisp mobility 172_20_23_0-VN_One-IPv4
```

Analyzing EID registration history

- Registration history for EID gives a good insight into dynamic nature of clients.

```
Border_1#sh lisp instance-id 4100 ipv4 server registration-history last 10
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event
```

Timestamp (UTC)	Instance	Proto	Roam	WLC	Source	EID prefix
Feb 8 18:52:48.493	8189	TCP	No	No	172.31.254.20	-*172.30.149.5/32
Feb 8 18:52:48.796	4099	TCP	No	No	172.31.254.20	+ 172.30.3.102/32
Feb 8 18:52:48.799	4099	TCP	No	No	172.31.254.20	+ 172.30.3.151/32
Feb 8 18:52:49.330	8189	TCP	No	No	172.31.254.20	+*172.30.149.1/32
Feb 8 18:53:12.382	8189	TCP	No	No	172.31.254.20	-*172.30.149.1/32
Feb 8 18:53:13.197	8189	TCP	No	No	172.31.254.20	+*172.30.149.5/32

Address Resolution Information

- By default there no flooding capability in fabric. ARP/ND needs flooding
- Address Resolution information learned on edges is registered with the Control Plane nodes
- Device-Tracking process on Fabric Devices responsible for snooping ARP/ND packets and rewriting Destination Address to Unicast Address based learned from LISP

```
Border_1#sh lisp instance-id 8189 ethernet server address-resolution
Address-resolution data for router lisp 0 instance-id 8188
L3 InstID      Host Address                               Hardware Address
  4100         172.20.23.2/32                     58ac.78f8.9422
  4100         172.20.23.3/32                     1cd1.e00e.838c
  4100         2001:DB8:0:1:250:56FF:FE85:9814/128 0050.5685.9814
  4100         FE80::250:56FF:FE85:9814/128         0050.5685.9814
```

Address Resolution Information, local

- Device-tracking learns and tracks IP endpoints
- Address Resolution information stored in local database to register with control plane
- Registrations only for Address Resolution purposes and are under Layer 2 Instance

```
Switch-172-20-106-7#sh device-tracking database | inc 0050.5685.9814
ARP 172.20.100.100                0050.5685.9814      Gi1/0/1      1021
ND FE80::250:56FF:FE85:9814      0050.5685.9814      Gi1/0/1      1021
ND 2001:DB8:0:1:250:56FF:FE85:9814 0050.5685.9814      Gi1/0/1      1021
Switch-172-20-106-7#sh lisp instance-id 8188 ethernet database address-resolution
LISP ETR Address Resolution for LISP 0 EID-table Vlan 1021 (IID 8188)
Hardware Address      L3 InstID Host Address
0050.5685.9814        4100 FE80::250:56FF:FE85:9814/128
                      4100 172.20.100.100/32
                      4100 2001:DB8:0:1:250:56FF:FE85:9814/128
```

Address Resolution information

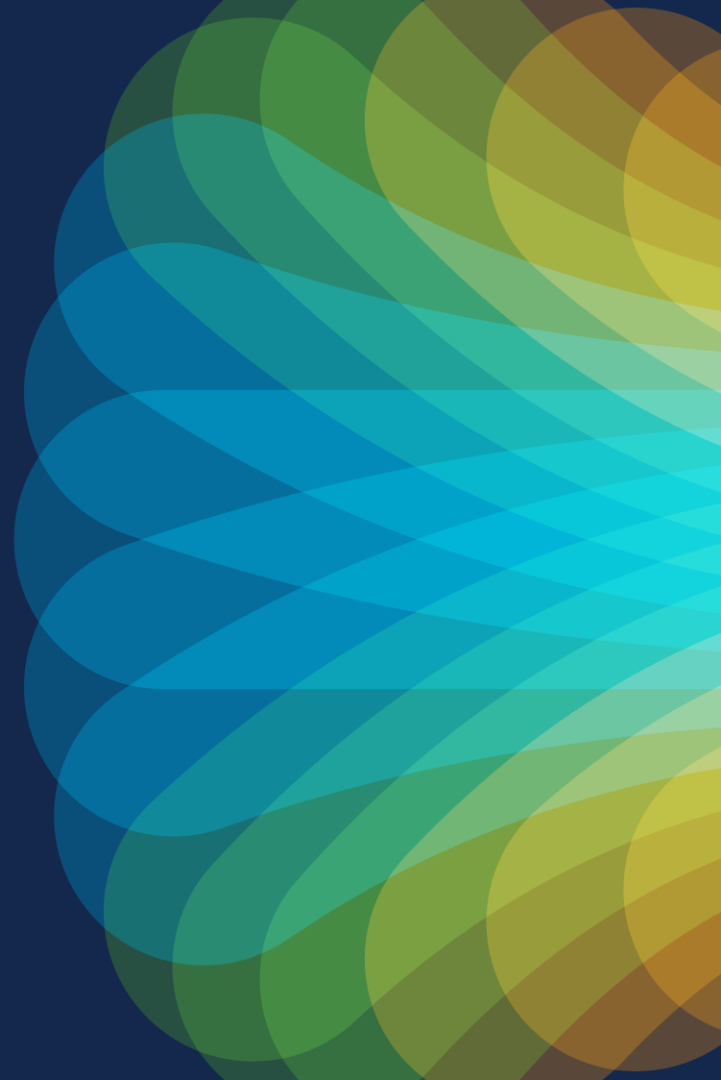
- Device-tracking shows 0000.0000.00fd when an IP address is in the process of being resolved. Interface shows where packet that originated the request is located
- For resolved entries it shows them as RMT entries.
- Entries have short live time to show inside device-tracking
- Only in used when flood arp-nd is not enabled

```
Switch-172-20-106-1#show device-tracking database
```

```
Binding Table has 9 entries, 3 dynamic (limit 200000)
```

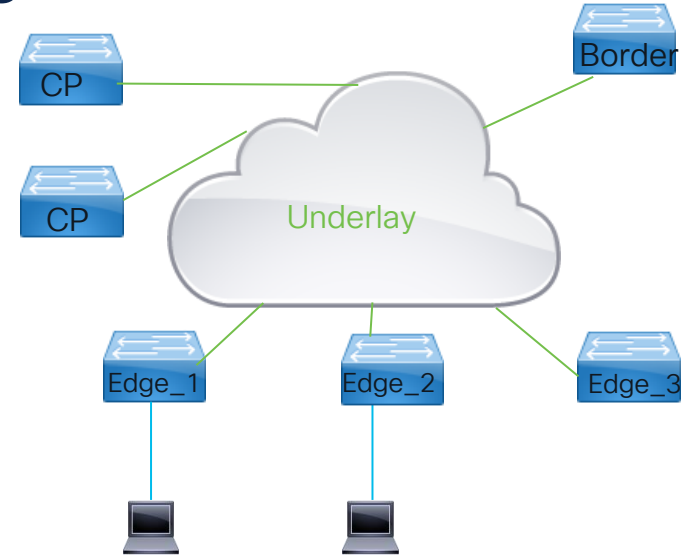
	Network Layer Address	Link Layer Address	Interface	vlan
API	172.20.23.100	0000.0000.00fd	Gi1/0/15	1021 <- in process
DH4	172.20.23.9	0015.f9db.da68	Gi1/0/15	1021 <- local host
RMT	172.20.23.2	58ac.78f8.9422	L2LI0	1021 <- remote host
L	172.20.23.1	0000.0c9f.ff95	Vl1021	1021 <- SVI IP

Reaching Remote Endpoints



Traffic Forwarding, Map Caches

- Traffic forwarding to non-local destinations is done based upon the map-cache
- Map-Cache entries have different actions:
 - send-map-request, triggers the sending of map-request to the Control Plane Node
 - Encapsulate, forward traffic based on learned Destination Routing Locator
 - Forward Native, previous map-reply was unsuccessful, attempt normal forwarding.
- Map-caches are longest match lookup.
- Edges/Borders send LISP Encapsulated Map Request messages to Control Plane node
- For EID with Proxy set CP responds direct, otherwise forwards to registering device to respond



Looking at the Map Cache

Map-caches are displayed with the command :

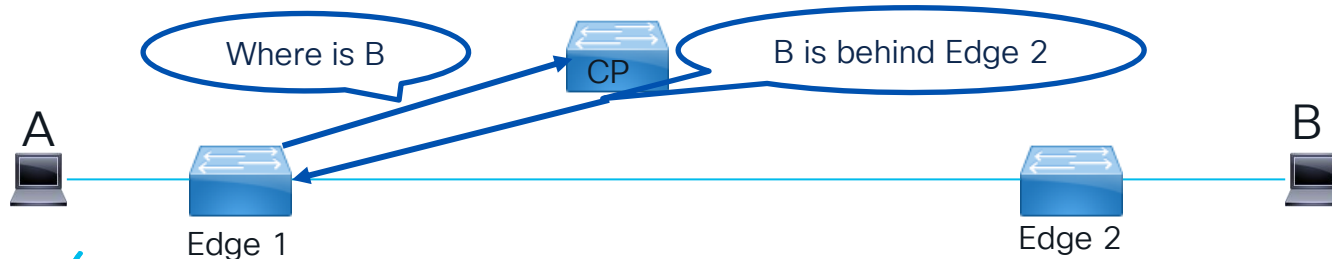
“Show lisp instance-id <instance-id> <AF> map-cache”

```
Switch-172-20-106-7#sh lisp instance-id 4100 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN_One (IID 4100), 5 entries
0.0.0.0/0, uptime: 00:00:35, expires: 00:00:24, via static-send-map-request
  Negative cache entry, action: send-map-request
8.0.0.0/7, uptime: 00:00:03, expires: 00:14:56, via map-reply, forward-native
  Negative cache entry, action: forward-native
10.48.13.0/24, uptime: 06:11:42, expires: 17:48:17, via map-reply, complete
  Locator      Uptime      State  Pri/Wgt      Encap-IID
  172.31.255.18 06:11:42   up     10/10        -
  172.33.250.1  06:11:42   up     10/10        -
172.20.23.0/24, uptime: 4w1d, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
```

Looking at the Map Cache , send map request

```
Switch-172-20-106-7#sh lisp instance-id 4100 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN_One (IID 4100), 5 entries
0.0.0.0/0, uptime: 00:00:35, expires: 00:00:24, via static-send-map-request
Negative cache entry, action: send-map-request
..
172.20.23.0/24, uptime: 4w1d, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
```

- Edges and internal borders are configured with:
map-cache 0.0.0.0/0 map-request to trigger map-request to CP
- Map Reply from Control Plane node used to further build map-cache



Looking at the Map Cache , Negative Map Reply

```
Switch-172-20-106-7#sh lisp instance-id 4100 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN_One (IID 4100), 5 entries
..
8.0.0.0/7, uptime: 00:00:03, expires: 00:14:56, via map-reply, forward-native
    Negative cache entry, action: forward-native
..
```

- Control Plane node returns Negative Map Reply when EID not known
- Default NMR TTL is 15 minutes
- Negative Map Reply contains biggest possible range of EID's not known Control Plane. Ex, 8.0.0.0/7 as response to Map Request to 8.8.8.8/32
- Traffic will be forwarded to Anycast Border (if reachable) or forwarded native
- For Ethernet traffic will be flooded (if enabled)

```
8.0.0.0/7, uptime: 00:00:03, expires: 00:14:56, via map-reply, forward-native
    Encapsulating to proxy ETR ←use-petr configured on Edge
```

Looking at the Map Cache , encapsulate

```
Switch-172-20-106-7#sh lisp instance-id 4100 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN_One (IID 4100), 5 entries
..
10.48.13.0/24, uptime: 06:11:42, expires: 17:48:17, via map-reply, complete
  Locator      Uptime      State  Pri/Wgt  Encap-IID
  172.31.255.18 06:11:42   up     10/10    -
  172.33.250.1  06:11:42   up     10/10    -
```

- Completed entries allow the fabric device to encapsulate and send the traffic
- Multiple RLOC's might be returned. Traffic will be load balanced between locations (flow based) in overlay
- Load balancing might also occur in Underlay for reaching the RLOC
- RLOC needs to be reachable

Forwarding of IP traffic through the fabric

```
Switch-172-20-106-7#show ip route vrf VN_One
Routing Table: VN_One
C       172.20.23.0/24 is directly connected, Vlan1021
L       172.20.23.1/32 is directly connected, Vlan1021
l       172.20.23.2/32 [10/1] via 172.20.23.2, 2w0d, Vlan1021
Switch-172-20-106-7#sh ip cef vrf VN_One 10.48.13.0/24 detail
10.48.13.0/24, epoch 0, flags [subtree context, check lisp eligibility
  SC owned,sourced: LISP remote EID - locator status bits 0x00000003
  LISP remote EID: 2 packets 628 bytes fwd action encap
  LISP source path list
    nexthop 172.31.255.18 LISP0.4100
    nexthop 172.33.250.1 LISP0.4100
  2 IPL sources [no flags]
  nexthop 172.31.255.18 LISP0.4100
  nexthop 172.33.250.1 LISP0.4100
```

Use show ip cef <nexthop>
for egress interface

- Routing Table does not show forwarding information.
- CEF command displays forwarding done through the fabric.

Layer 2 forwarding through the fabric

- Layer 2 forwarding happens when Destination Mac Address does not match mac address of SVI
- Map cache triggered by sending traffic to unknown mac address
- Layer 2 Flooding optional for BUM traffic using Multicast in Underlay

```
Switch-172-20-106-7#sh mac add dynamic vlan 1021
```

Vlan	Mac Address	Type	Ports
------	-------------	------	-------

1021	10f9.206d.e5b6	CP_LEARN	L2L10
------	----------------	----------	-------

```
Total Mac Addresses installed by LISP: REMOTE: 1
```

```
Switch-172-20-106-7#sh lisp instance-id 8189 ethernet map-c
```

```
LISP MAC Mapping Cache for EID-table Vlan 1021 (IID 8189), 1 entries
```

```
10f9.206d.e5b6/48, uptime: 1w4d, expires: 02:06:25, via map-reply, complete
```

Locator	Uptime	State	Pri/Wgt	Encap-IID
172.30.233.1	1w4d	up	10/10	-

CP_LEARN points to mac addresses from map-cache

LISP Remote forwarding, Layer 2 Flooding

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

```
Switch-172-20-106-7#sh run | sec instance-id 8189
instance-id 8189
  remote-rloc-probe on-route-change
  service ethernet
    eid-table vlan 1021
    broadcast-underlay 239.0.17.3    ← Mcast group used for flooding
    flood arp-nd                    ← Floor ARP en ND packets
    flood unknown-unicast.          ← Flood Unknown Unicast packets
    database-mapping mac locator-set rloc_1a8b95ce-6fe8-4608-b273-8453b86072c7
  exit-service-ethernet
  !
exit-instance-id
```

LISP Remote forwarding, Layer 2 Flooding

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

```
Switch-172-20-106-7#sh ip mroute 239.0.17.3 172.30.233.6
```

```
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(172.30.233.6, 239.0.17.3), 1w5d/00:03:11, flags: FT
```

```
Incoming interface: Null0, RPF nbr 0.0.0.0
```

```
Outgoing interface list:
```

```
TenGigabitEthernet1/0/24, Forward/Sparse, 1w5d/00:03:04
```

```
Switch-172-20-106-7#sh ip mroute 239.0.17.3 172.30.233.1
```

```
IP Multicast Routing Table
```

```
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(172.30.233.1, 239.0.17.3), 1w5d/00:02:06, flags: JT
```

```
Incoming interface: TenGigabitEthernet1/0/24, RPF nbr 172.30.233.4
```

```
Outgoing interface list:
```

```
L2LISP0.8189, Forward/Sparse-Dense, 00:16:19/00:01:40
```

```
L2LISP0.8190, Forward/Sparse-Dense, 1d00h/00:01:00
```

Entry used to
encapsulate

De-encapsulating traffic
towards L2 Instances

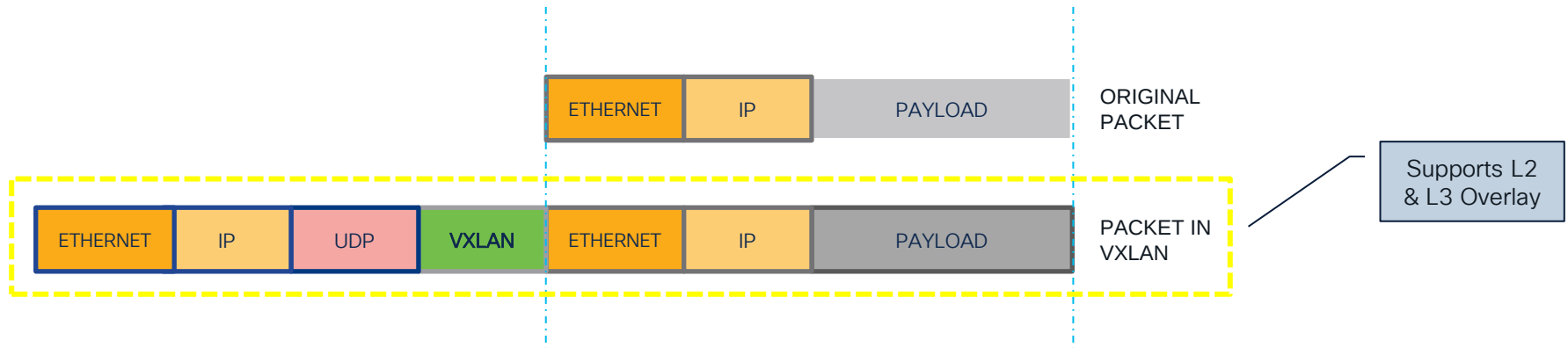
Forwarding Layer 2 traffic through the fabric

- MATM tables in FED shows forwarding from platform perspective
- Type in MATM will indicate it's a LISP Remote Address

```
Switch-172-20-106-7#sh platform software fed switch active matm macTable vlan 1021
VLAN      MAC                               Type  Seq#    EC_Bi  Flags  *a_time  *e_time  ports
-----
1021      0000.0c9f.f377                     0x8002      0   78007    64    0         0      Vlan1021
1021      10f9.206d.e5b6  0x1000001      0     0      64    0         0      RLOC 172.30.233.1 adj_id 220
1021      a036.9f91.0937                     0x44202    9260    0      64    0         0      TenGigabitEthernet1/0/10
Total Mac number of addresses:: 3
*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR          0x1  MAT_STATIC_ADDR          0x2  MAT_CPU_ADDR             0x4  MAT_DISCARD_ADDR         0x8
MAT_ALL_VLANS              0x10 MAT_NO_FORWARD            0x20 MAT_IPMUL_T_ADDR          0x40 MAT_RESYNC                 0x80
MAT_DO_NOT_AGE             0x100 MAT_SECURE_ADDR          0x200 MAT_NO_PORT               0x400 MAT_DROP_ADDR              0x800
MAT_DUP_ADDR               0x1000 MAT_NULL_DESTINATION     0x2000 MAT_DOT1X_ADDR            0x4000 MAT_ROUTER_ADDR            0x8000
MAT_WIRELESS_ADDR          0x10000 MAT_SECURE_CFG_ADDR      0x20000 MAT_OPQ_DATA_PRESENT      0x40000 MAT_WIRED_TUNNEL_ADDR      0x80000
MAT_DLR_ADDR               0x100000 MAT_MRP_ADDR              0x200000 MAT_MSRRP_ADDR            0x400000 MAT_LISP_LOCAL_ADDR        0x800000
MAT_LISP_REMOTE_ADDR 0x1000000 MAT_VPLS_ADDR             0x2000000 MAT_LISP_GW_ADDR          0x4000000
```

Data Plane

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



Packet Encapsulation

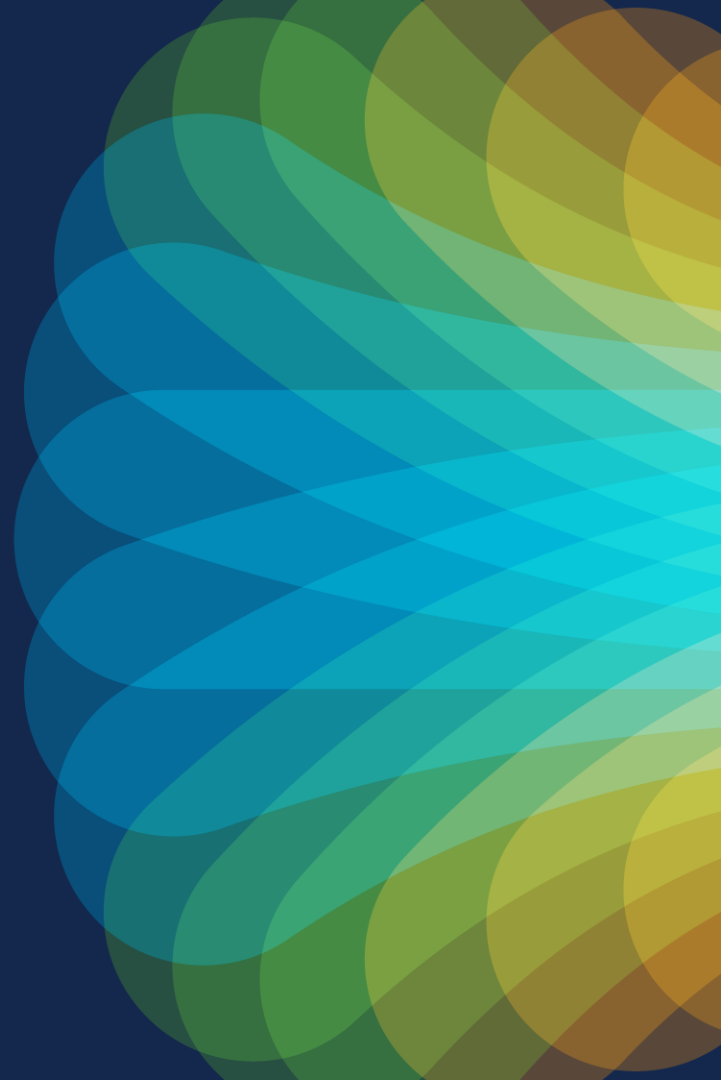
Apply a display filter ... <=>/>					
No.	Protocol	Source	Destination	Time	Info
→ 3	ICMP	172.30.3.2	172.30.3.3	0.116267	Echo (ping) request id=0x069b, seq=9688/55333, ttl=64 (reply in 4)
← 4	ICMP	172.30.3.3	172.30.3.2	0.116365	Echo (ping) reply id=0x069b, seq=9688/55333, ttl=64 (request in 3)
5	ICMP	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					
Virtual eXtensible Local Area Network					
> Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)					
Group Policy ID: 4					
VXLAN Network Identifier (VNI): 8189					
Reserved: 0					
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

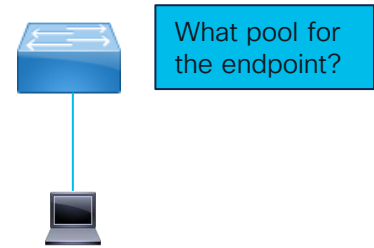
Encapsulated packet

Secure Fabric



Authorizing & Assignment Endpoints

- Radius/ISE can be used to profile, authorize and assign Endpoints by returning selective Radius Attributes in Access-Accepts
- Radius attributes in Access Accept can set :
 - Voice Domain authorization
 - Vlan Assignment
 - SGT Assignment
 - DACL
 - Templates
 - etc
- On Catalyst 9000 switches the Authentication is performed by Session Manager process(SMD). Traditional debugs wont show expected debugs for Authentication
- To enable traces: set platform software trace smd switch active R0 <facility> <level>
- To gather traces : show logging process smd



AAA server status

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

```
Edge_2#show aaa server
```

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

Catalyst 9000 Endpoint Authentication

- On Catalyst 9000 switches the Authentication is performed by Session Manager process(SMD).
- Traditional debugs wont show expected debugs for Authentication
- Normal IOS debugs might not yield expected debugging outputs.
- To enable traces:

```
set platform software trace smd switch active R0 <facility> <level>
```

- To gather traces :

```
show logging process smd
```

Debugging/Tracing authentication

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

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

Debugging/Tracing authentication -2

- Access Accept received by Session managers shows the attributes to be applied to the session within the access-accept send by Radius

```
[radius] [22001]: (info): RADIUS: Received from id 1812/254 10.48.91.222:0, Access-Accept, len 450
[radius] [22001]: (info): RADIUS: authenticator 23 fb 53 b0 bd f2 79 dc - 4a 79 5a e0 b2 07 ae fd
[radius] [22001]: (info): RADIUS: User-Name [1] 10 "michelpe"
[radius] [22001]: (info): RADIUS: Class [25] 54 ...
[radius] [22001]: (info): RADIUS: Tunnel-Type [64] 6 VLAN [13]
[radius] [22001]: (info): RADIUS: Tunnel-Medium-Type [65] 6 ALL_802 [6]
[radius] [22001]: (info): RADIUS: EAP-Message [79] 6 ...
[radius] [22001]: (info): RADIUS: Message-Authenticator[80] 18 ...
[radius] [22001]: (info): RADIUS: Tunnel-Private-Group-Id[81] 20 "172_30_3_0-BruEsc"
[radius] [22001]: (info): RADIUS: EAP-Key-Name [102] 67 *
[radius] [22001]: (info): RADIUS: Cisco AVpair [1] 30 "linksec-policy=should-secure"
[radius] [22001]: (info): RADIUS: Cisco AVpair [1] 32 "cts:security-group-tag=00C8-01"
[radius] [22001]: (info): RADIUS: Cisco AVpair [1] 26 "cts:sgt-name=CL_Client_1"
[radius] [22001]: (info): RADIUS: Cisco AVpair [1] 15 "cts:vn=BruEsc"
```

Authentication Results

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

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

IP information learned via
Device Tracking

Authorization status

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

Policies send via Radius

Method state success does
not indicate auth state of
client

Cisco TrustSec

- Every endpoint in the fabric gets assigned a Secure Group Tag
- Secure Group Tag transmitted in Policy Field in VXLAN header of encapsulated frames
- Fabric devices download CTS environment data from ISE server
- Fabric devices request policies for all known SGT's on that device
- Traffic being allowed/denied based upon SGT -> DGT mapping
- Traffic policy can contain optional SGACL or just deny/permit all
- Default action applied if no match found

Ingress Tagging

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

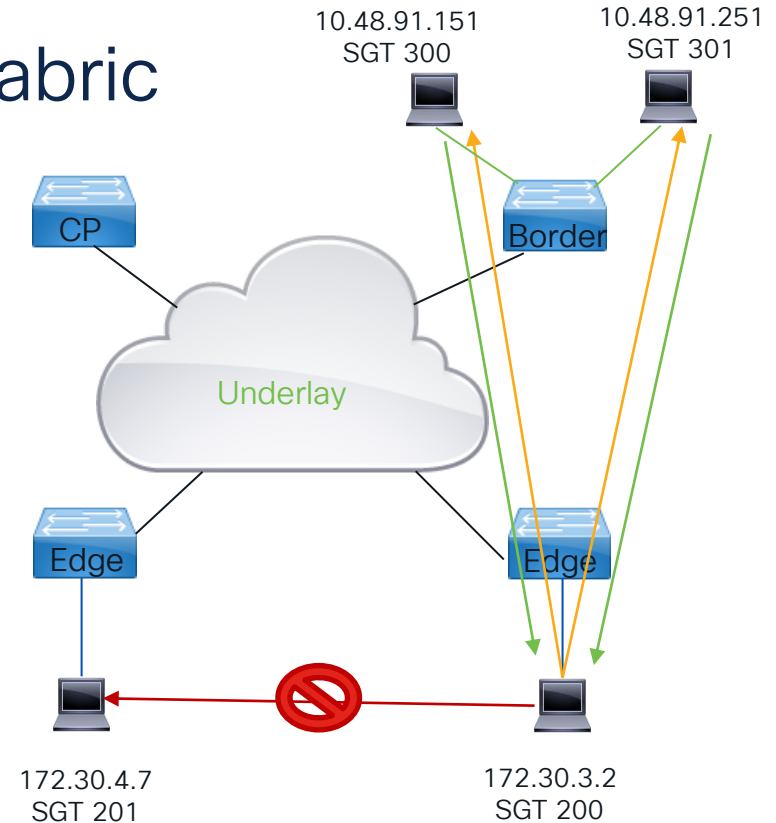
```
> Internet Protocol Version 4, Src: 172.31.255.182, Dst: 172.30.233.6
> User Datagram Protocol, Src Port: 65355, Dst Port: 4789
> Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 300
    VXLAN Network Identifier (VNI): 4099
    Reserved: 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 ip
*	*	Permit ip

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



CTS environment data

```
Edge_2#sh cts environment-data
```

```
CTS Environment Data
```

```
=====
```

```
Current state = COMPLETE
```

```
Last status = Successful
```

```
Service Info Table:
```

```
Local Device SGT:
```

```
SGT tag = 2-03:TrustSec_Devices
```

```
Server List Info:
```

```
Installed list: CTSServerList1-0001, 1 server(s):
```

```
*Server: 10.48.91.222, port 1812, A-ID DFFC8EFDB5B39259624A40FA05E3AC8A
```

```
Status = ALIVE , auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,  
deadtime = 20 secs
```

```
Security Group Name Table:
```

```
0001-24 :
```

```
0-00:Unknown
```

```
2-03:TrustSec_Devices
```

```
200-00:CL_Client_1
```

```
201-00:CL_Client_2
```

```
300-00:CL_Server_1
```

```
301-00:CL_Server_2
```

```
Transport type = CTS_TRANSPORT_IP_UDP
```

```
Environment Data Lifetime = 86400 secs
```

```
Last update time = 17:05:41 UTC Tue Jun 14 2022
```

```
Env-data expires in 0:23:31:34 (dd:hr:mm:sec)
```

```
Env-data refreshes in 0:23:31:34 (dd:hr:mm:sec)
```

Local SGT tag, set on ISE

Radius server in use

Group to SGT mapping

Periodic refresh occurs
ISE can trigger refresh
using CoA

Problems downloading CTS environment?

- 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 environment data with cts refresh environment-data
- Entire cts table only downloaded when new version available.

```
Edge_1#show cts pacs
AID: DFFC8EFDB5B39259624A40FA05E3AC8A
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: DFFC8EFDB5B39259624A40FA05E3AC8A
  I-ID: FCW2135G0AL
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 11:54:17 UTC Wed Jun 22 2022
PAC-Opaque:
000200B80003000100040010DFFC8EFDB5B39259624A40FA05E3
AC8A0006009C00030100B74B07EC9F302303F7DA9AEE1E7EBB24
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 learns entries
via SXP or CLI

CTS Authorization Entries

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

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

CTS Policies

- Policies downloaded for SGTs with local presence
- Enforcement occurs on Egress , not on ingress
- RBACL names are appended with a version,
Ex: AllowWeb-00 is version 00 of RBACL name NoTelnet

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

Monitoring SGT traffic

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

```
BN_1#show cts role-based counters
```

```
Role-based IPv4 counters
```

From	To	SW-Denied	HW-Denied	SW-Permitt	HW-Permitt	SW-Monitor	HW-Monitor
*	*	0	0	4965	312090	0	0
200	300	0	0	0	0	0	0
201	300	0	15	0	146	0	0
200	301	0	0	0	0	0	0
201	301	0	0	0	195	0	0

```
Edge_1#show cts role-based counters
```

```
Role-based IPv4 counters
```

From	To	SW-Denied	HW-Denied	SW-Permitt	HW-Permitt	SW-Monitor	HW-Monitor
*	*	0	0	13296	21927	0	0
200	201	0	13	0	0	0	0

Useful debugs

- To diagnose issues with mapping or download from ISE
 - Debug cts all
 - Debug rbm all
- CTS runs on top of IOSd, not part of SMD.
Radius debugs will show exchanges with ISE
- Hardware mappings of IP to SGT:
show cts role-based sgt-map platform

Before needing to troubleshoot

- Get familiar with the CLI's
- Download this pdf for reference



The bridge to possible

Thank you

CISCO *Live!*

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, including blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go