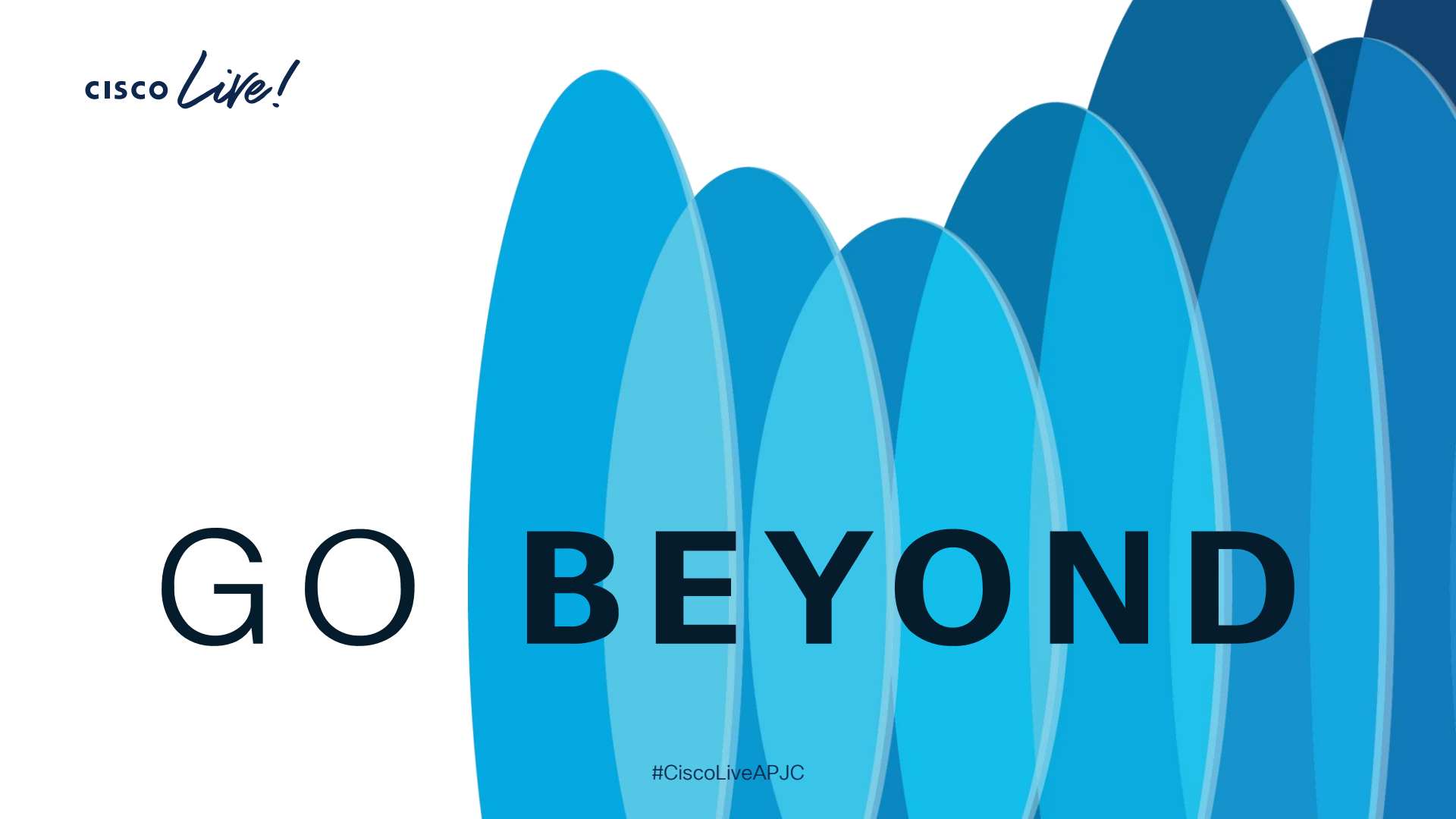

cisco Live!
GO BEYOND
#CiscoLiveAPJC

"Reconciliation"- Dustin Koa Art

Advanced LISP SD-Access Forwarding Architecture

Jerome Dolphin, Technical Marketing Engineer
CCIE#17805 (R&S, SEC), CCDE#2013::3

BRKENS-3555

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-3555

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

Webex spaces will be moderated by the speaker until November 15, 2024.

cisco Live!

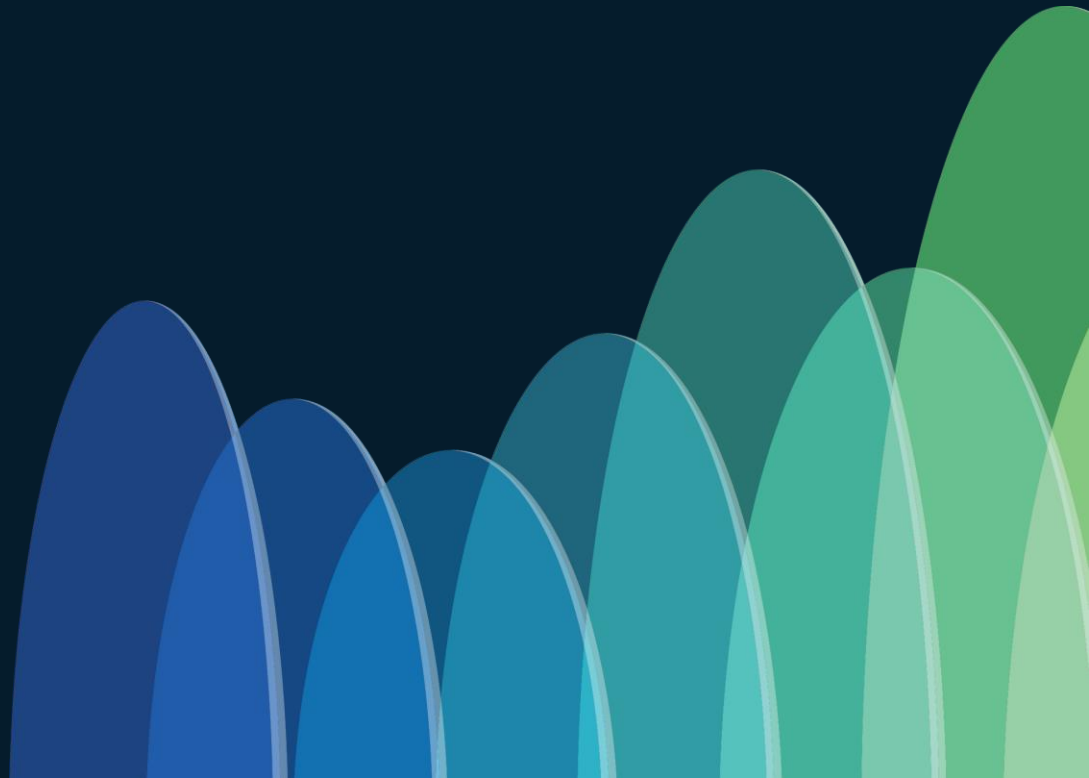
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- LISP Fundamentals
- LISP Virtualisation and Configuration
- Protocol and Packet Walks for Common SD-Access Scenarios
- First Hop Security
- Conclusion

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introduction

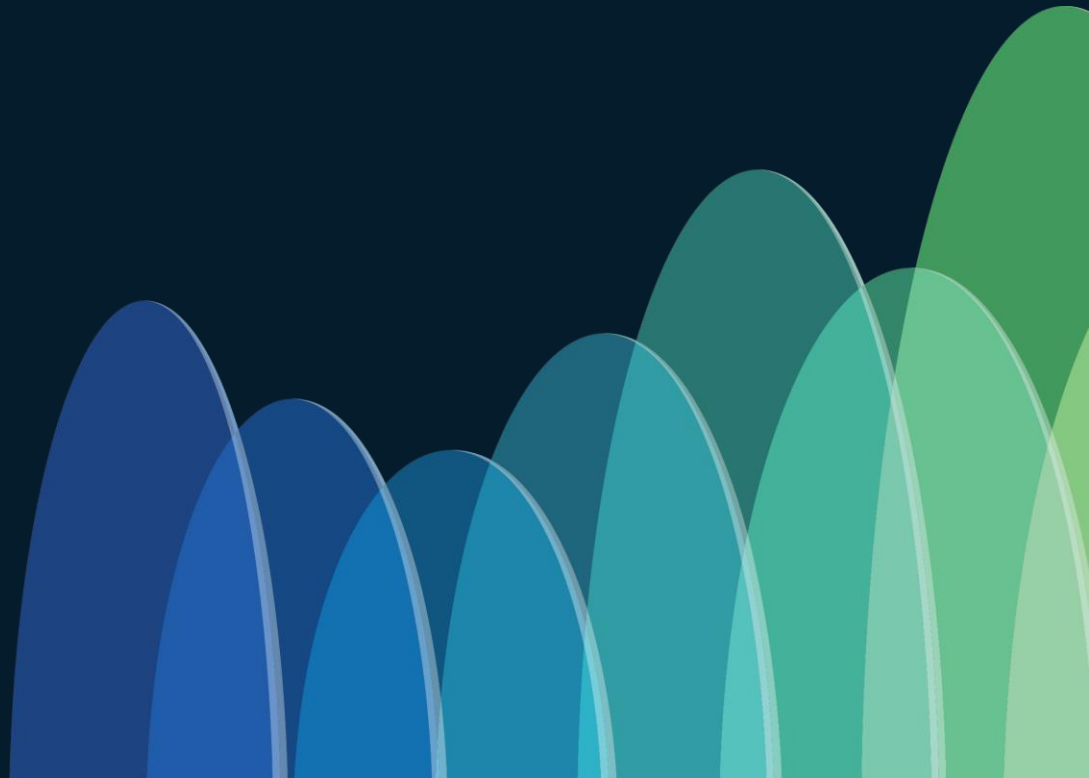


Expectations

- This is a 3000 series presentation which means there will be technical detail.
- There is less detailed presentations for SD-Access design and operations, see ciscolive.com recordings.
- May not have time to cover all the slides. Skipped slides will be in the PDF published to ciscolive.com for reference.
- The principals that follow apply to SD-Access Transit, but it's not explicitly covered in this presentation. For SD-Access Transit deep dive please see BRKENS-2816 on ciscolive.com.

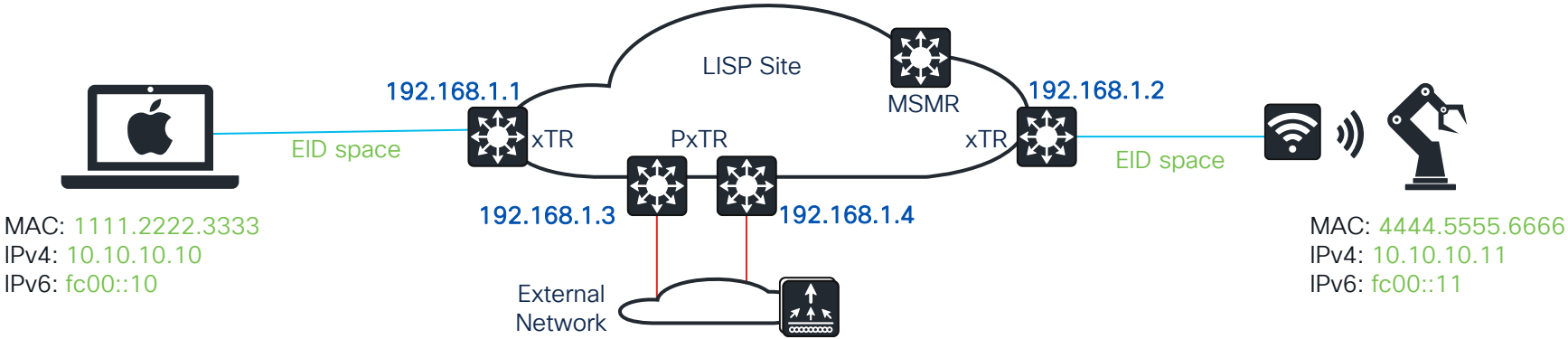
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fundamentals



LISP principles

- LISP is an acronym for locator ID separation protocol.
- An EID (endpoint ID) is mapped to an RLOC (routing locator).
- An EID can be many things: MAC address, IPv4/IPv6 host routes, IPv4/IPv6 summary routes, or network services like default ETR (default route).



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Terminology

LISP	Description	SD-Access
PITR (Proxy Ingress Tunnel Router)	Connects non-LISP and LISP sites. Advertises aggregated EID prefixes to attract and encapsulate traffic for forwarding to LISP sites.	N/A
PETR (Proxy Egress Tunnel Router)	Connects non-LISP and LISP sites. Registers external EID to RLOC mappings, decapsulates tunneled data and passes to external networks.	N/A
PxTR	PITR and PETR capabilities co-located on the same device.	Border Node

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Terminology

LISP	Description	SD-Access
MS (Map Server)	Authenticates and accepts LISP registrations of EID-to-RLOC mappings. Publishes registrations to subscribers.	N/A
MR (Map Resolver)	Accepts Map Request (lookup) messages and forwards to the appropriate Map Server for EID-to-RLOC resolution. Sends Negative Map Replies for unknown EIDs.	N/A
MSMR	MS and MR capabilities co-located on the same device.	Control Plane Node

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

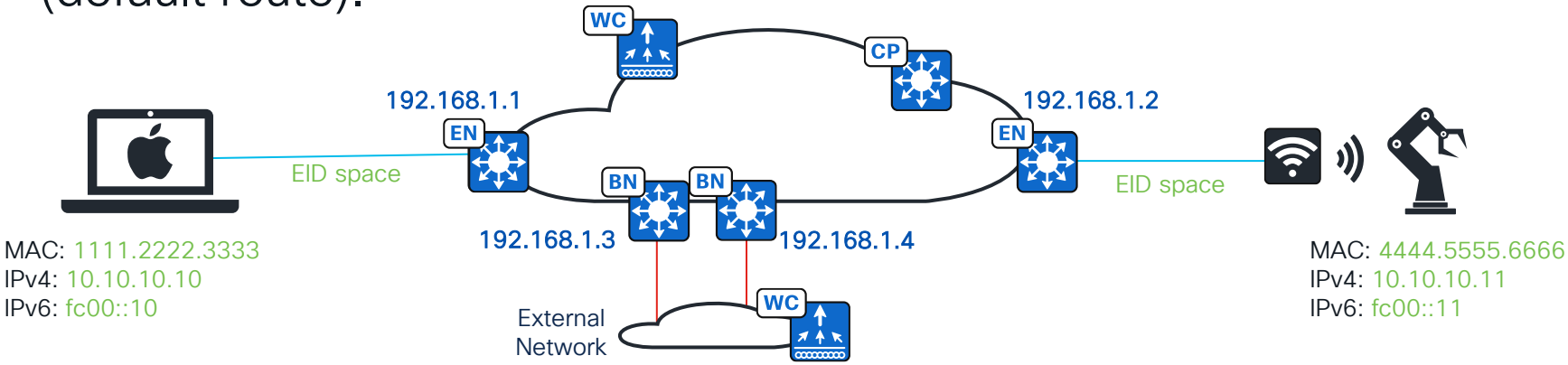
Terminology

LISP	Description	SD-Access
ITR (Ingress Tunnel Router)	Receives packets from attached endpoints that are destined for EIDs, looks up the corresponding RLOC, and encapsulates the packets before forwarding them to the appropriate ETR or PETR.	N/A
ETR (Egress Tunnel Router)	Receives encapsulated packets, decapsulates, and forwards the unencapsulated packets to their intended destinations within the ETR's local EID space.	N/A
xTR	ITR and ETR capabilities co-located on the same device.	Edge Node

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-Access principles

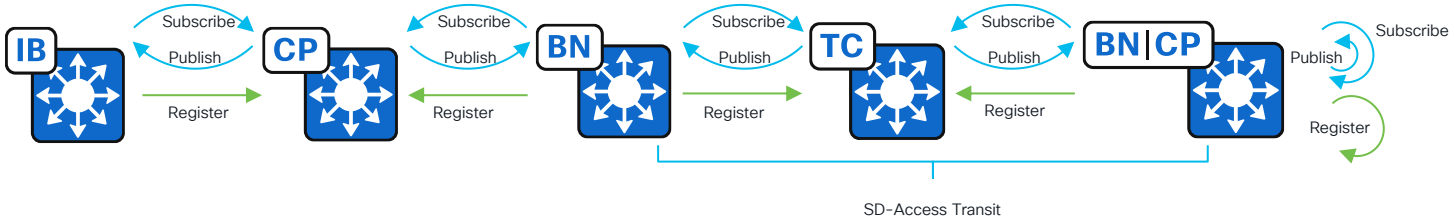
- LISP is an acronym for Locator ID Separation Protocol.
- An EID (Endpoint ID) is mapped to an RLOC (Routing Locator).
- An EID can be many things: MAC address, IPv4/IPv6 host routes, IPv4/IPv6 summary routes, or network services like default ETR (default route).



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

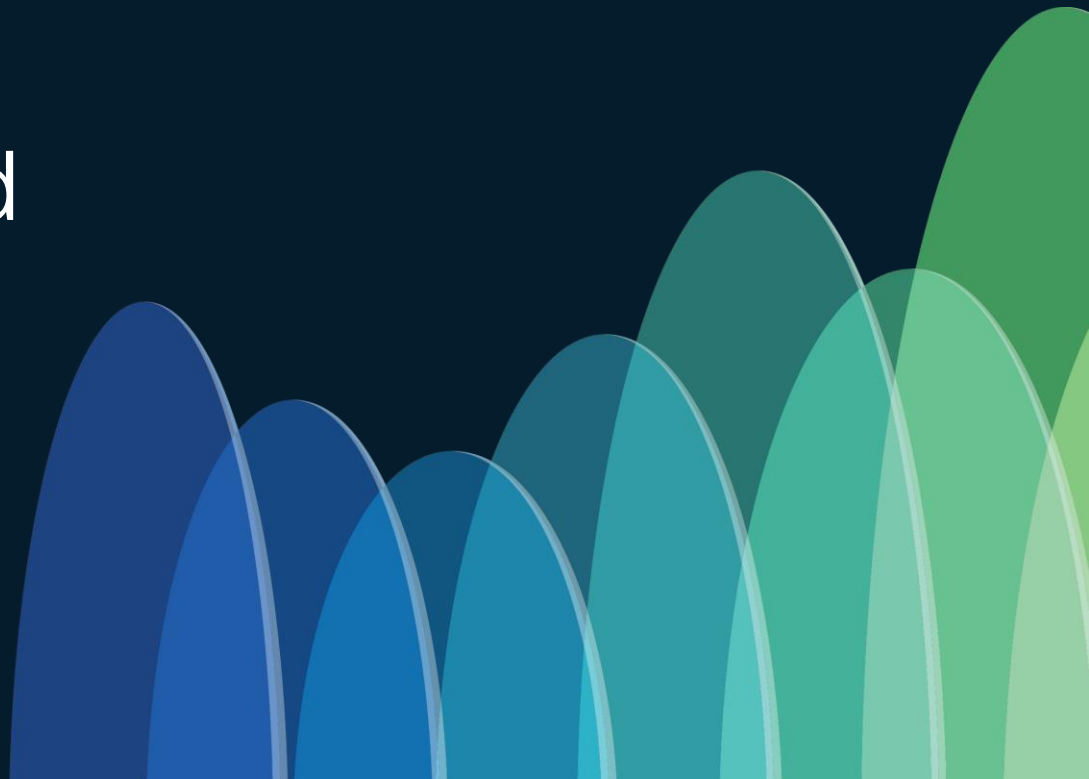
LISP Publish / Subscribe

- Border nodes:
  - Register EID to RLOC mappings.
  - Subscribe to Control Plane Node IPv4 and IPv6 reachability information.
  - May send map requests (lookups), if there's an Extranet Policy.
- Control plane nodes
  - Receive and store EID to RLOC registrations.
  - Publish reachability information to subscribers.
  - May resolve Border Node map requests if there's an extranet policy.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

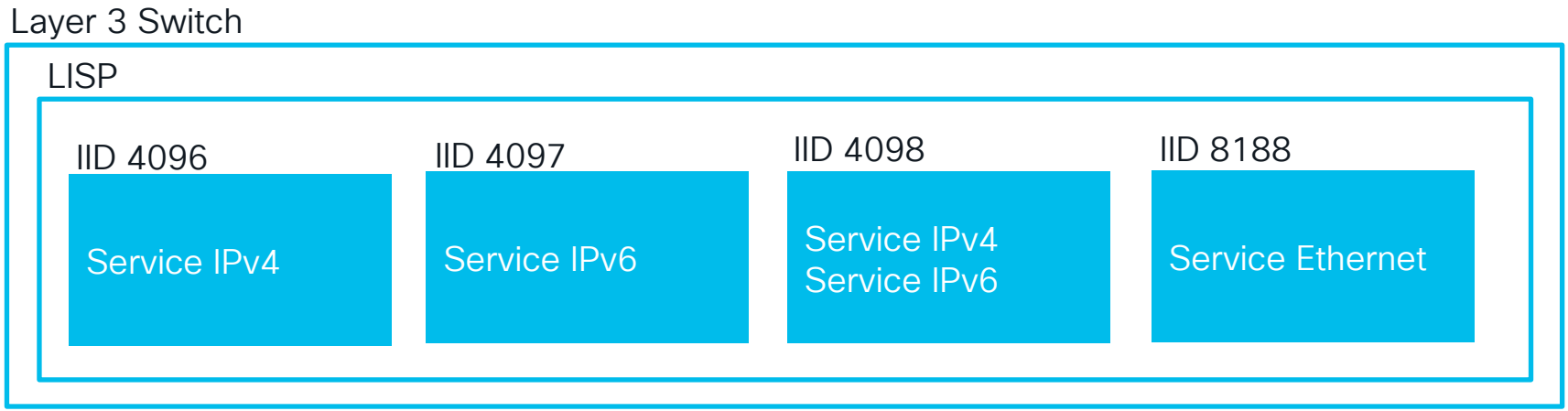
Virtualisation and Configuration



cisco Live!

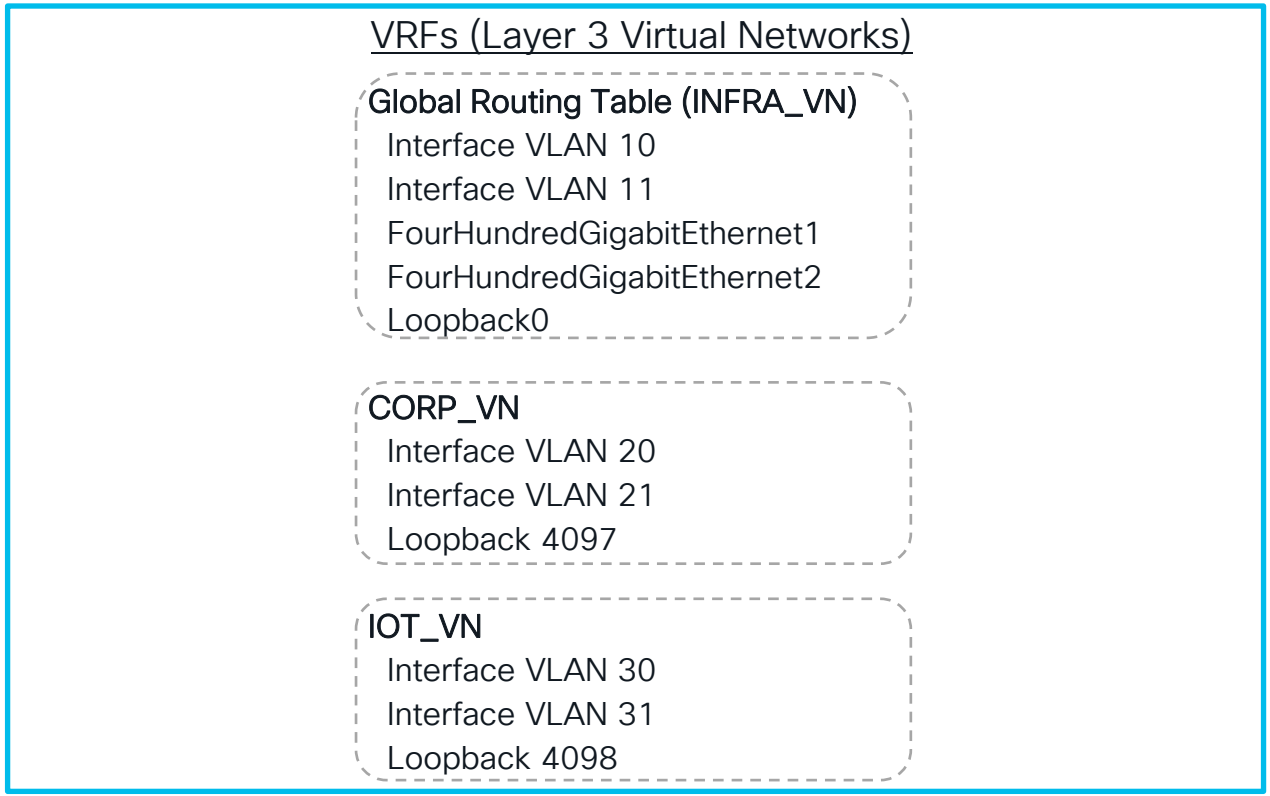
LISP virtualisation

- LISP is virtualised through Instance IDs (IIDs) which are isolated from each other.
- LISP tracks and resolves:
  - MAC EIDs
  - IPv4 EIDs
  - IPv6 EIDs



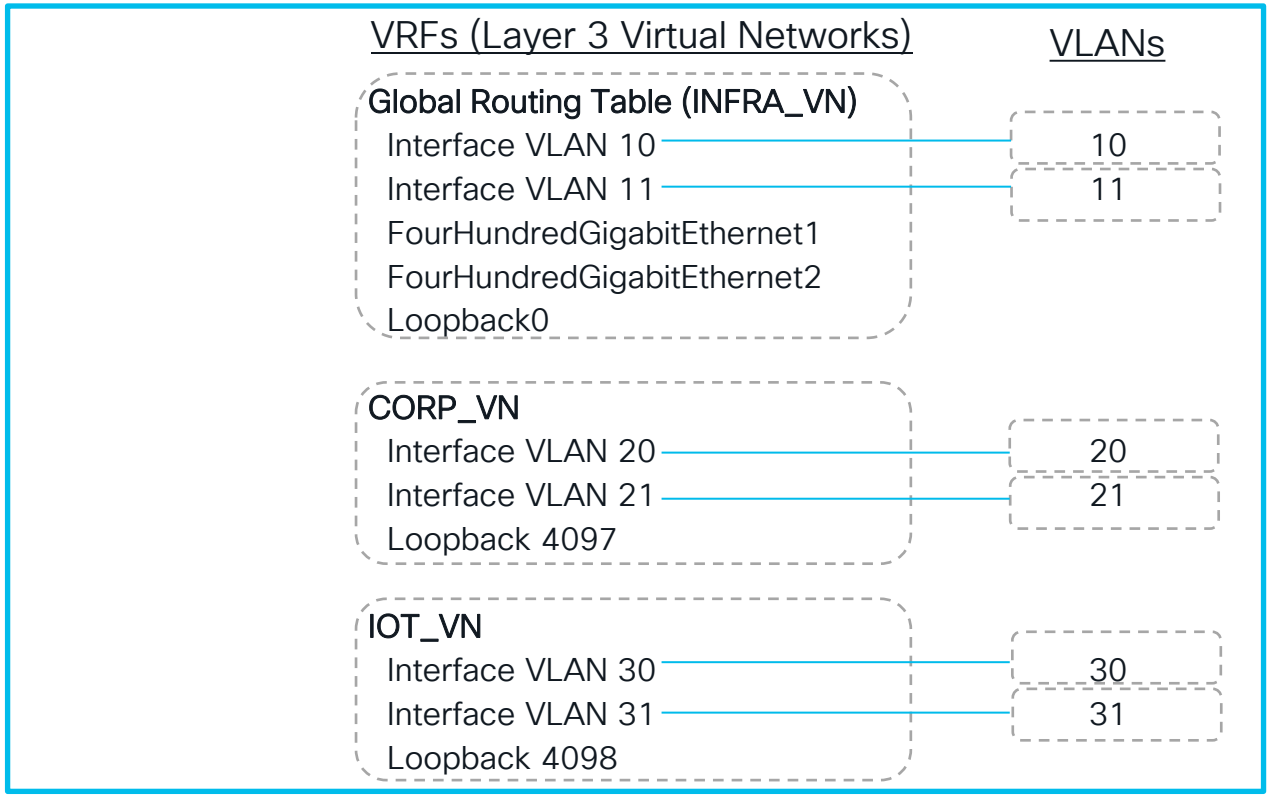
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 3 Border Node service mapping



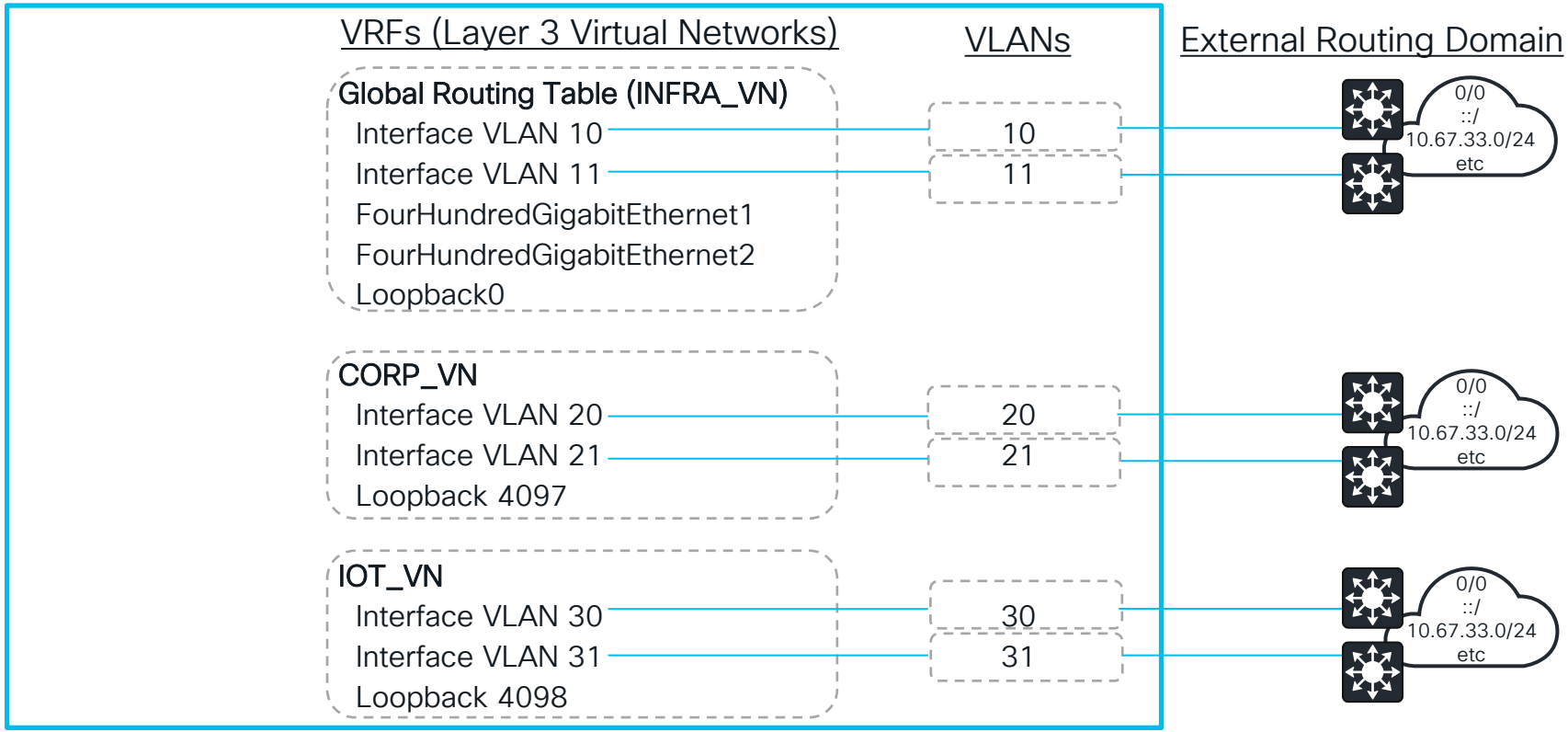
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 3 Border Node service mapping



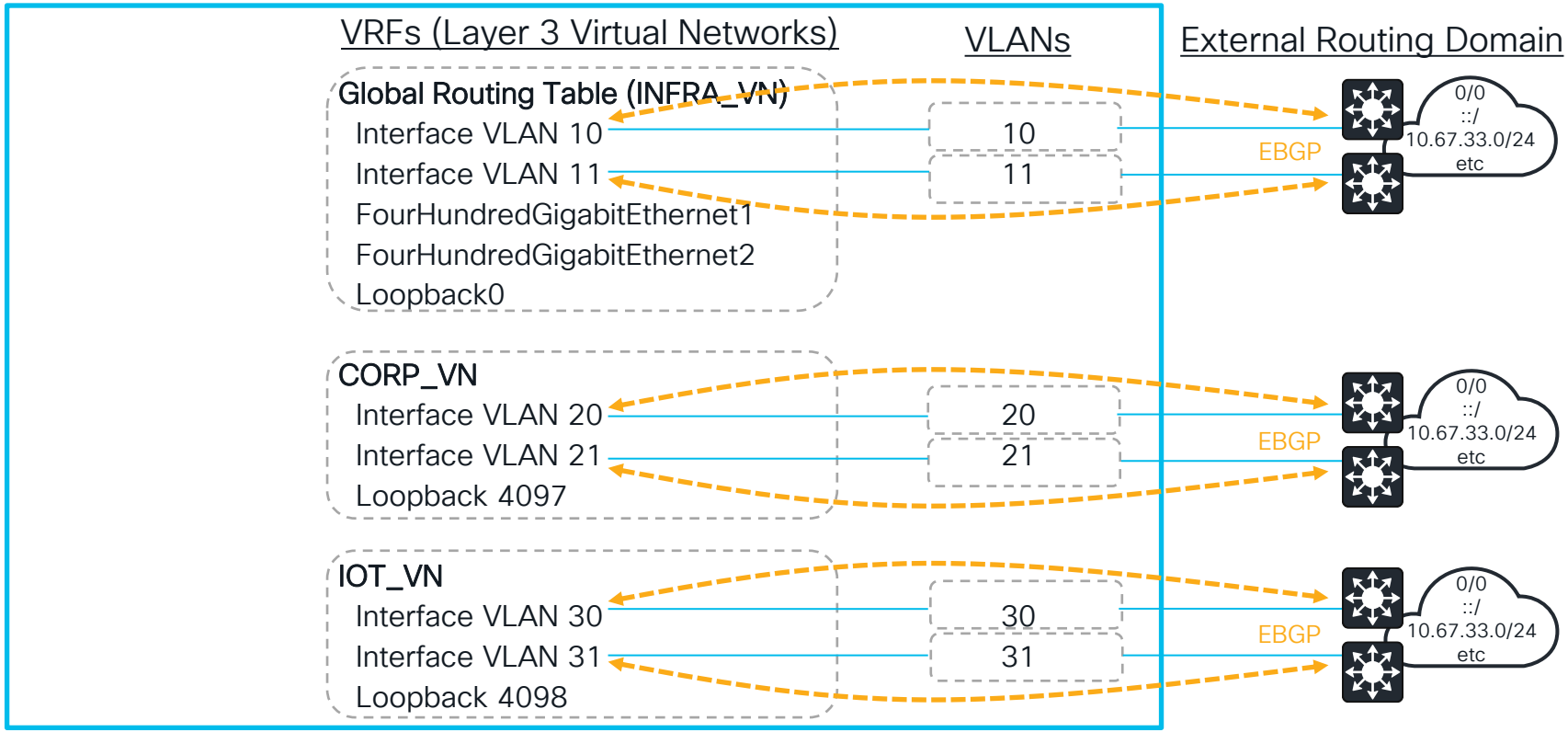
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 3 Border Node service mapping



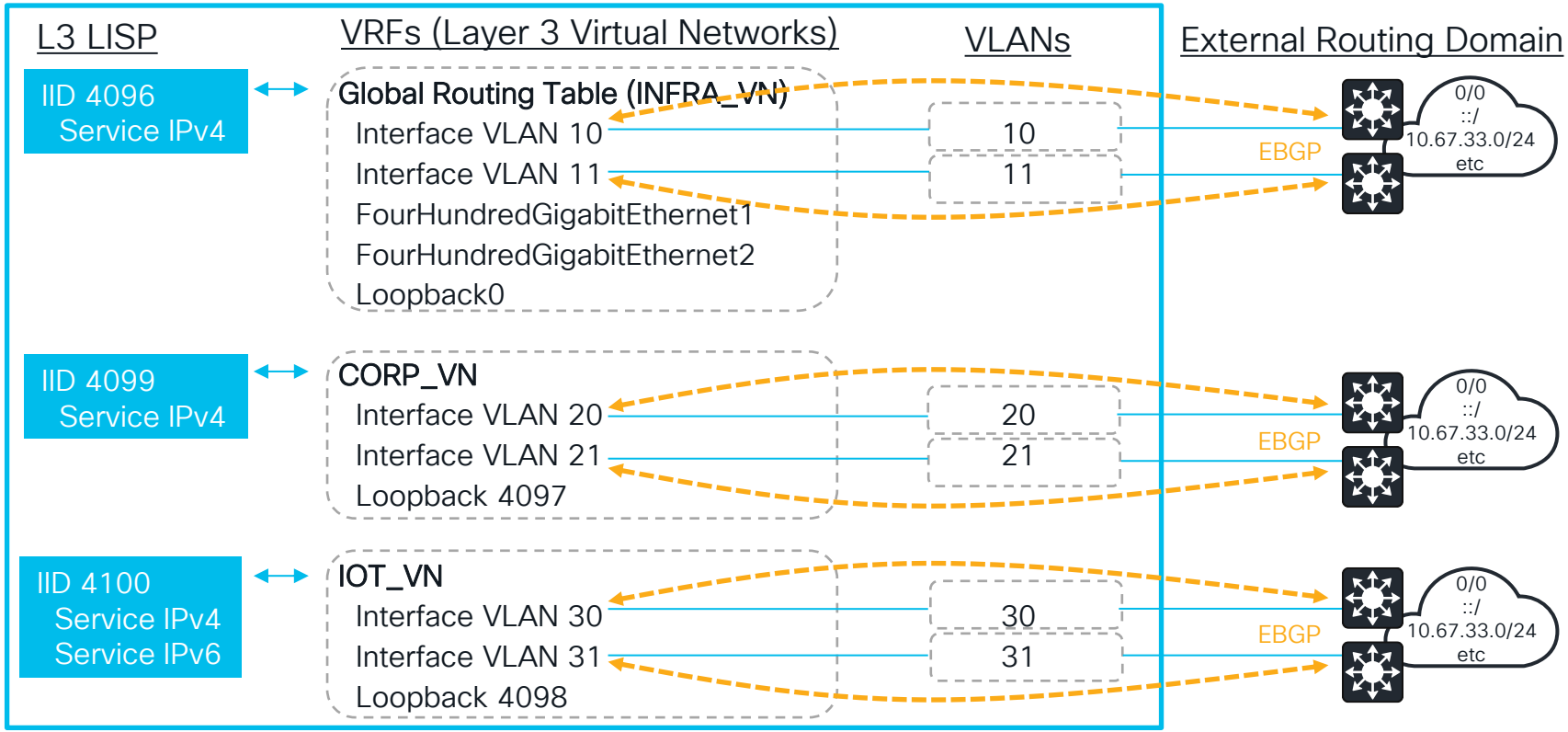
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 3 Border Node service mapping



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 3 Border Node service mapping



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 3 Border Node service mapping

```
!BN1
!
vrf definition CORP_VN
vrf definition IOT_VN
!
interface Loopback0
 ip address 192.168.8.1 255.255.255.255
!
interface Vlan222
 ip address 172.29.0.114 255.255.255.252
!
interface Vlan236
 vrf forwarding CORP_VN
 ip address 172.29.4.51 255.255.255.248
!
interface Vlan237
 vrf forwarding IOT_VN
 ip address 172.29.4.59 255.255.255.248
!
router bgp 65106
 address-family ipv4
  neighbor 172.29.0.113 activate
 address-family ipv4 vrf CORP_VN
  neighbor 172.29.4.49 activate
 address-family ipv4 vrf IOT_VN
  neighbor 172.29.4.57 activate
!continued in next column --->
```

VRFs aka L3VNs

Interfaces in VRFs

External BGP peers aka Fusion Devices

```
!--> continued from previous next column
!
router lisp
 service ipv4
  etr
  proxy-etr
  proxy-itr 192.168.8.1
 service ethernet
  itr
  etr
 !
 instance-id 4097
  service ipv4
   eid-table default
 !
instance-id 4099
  service ipv4
   eid-table vrf CORP_VN
 !
 instance-id 4100
  service ipv4
   eid-table vrf IOT_VN
!
```

Default IPv4 settings for L3 IIDs

Default settings for L2 IIDs

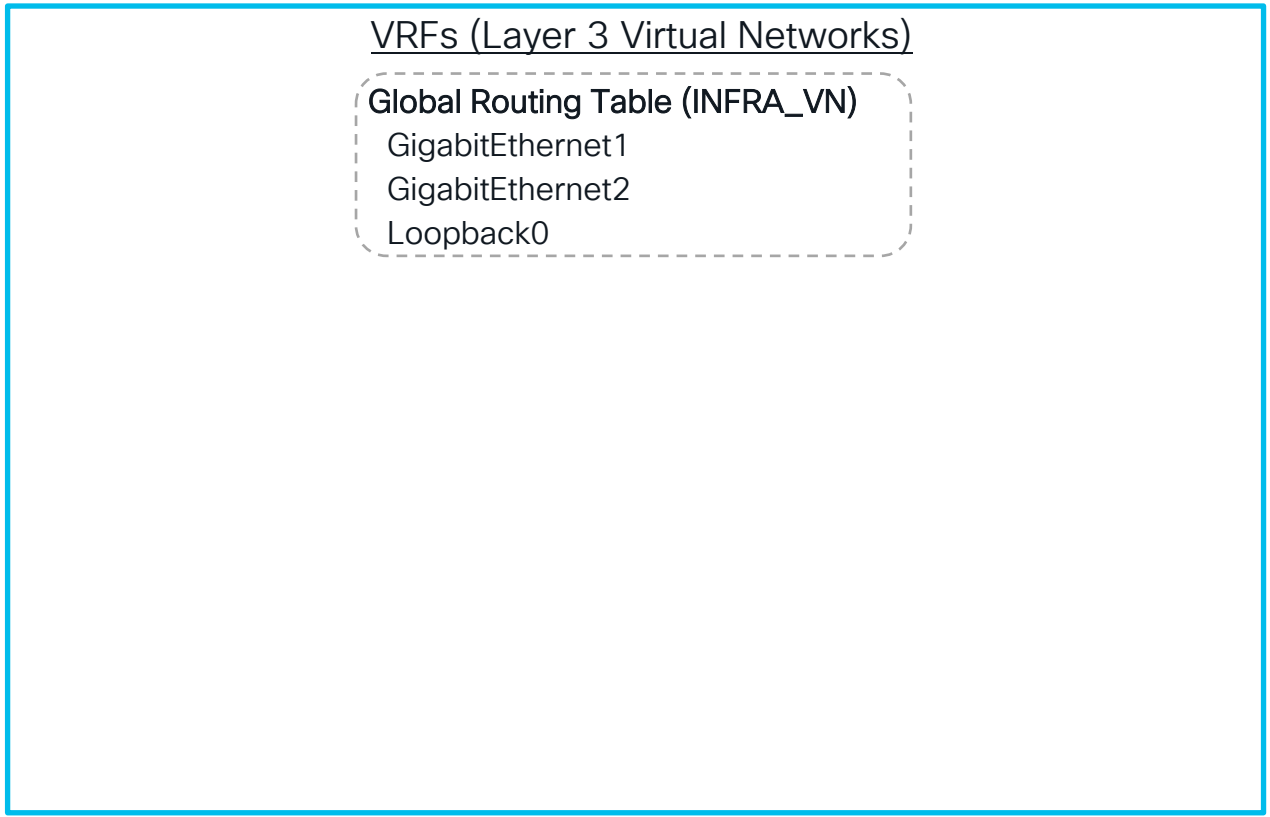
IID with IPv4 enabled in default routing table aka Global Routing Table aka ‘INFRA_VN’

IID with IPv4 enabled in VRF ‘CORP_VN’

IID with IPv4 enabled in VRF ‘IOT_VN’

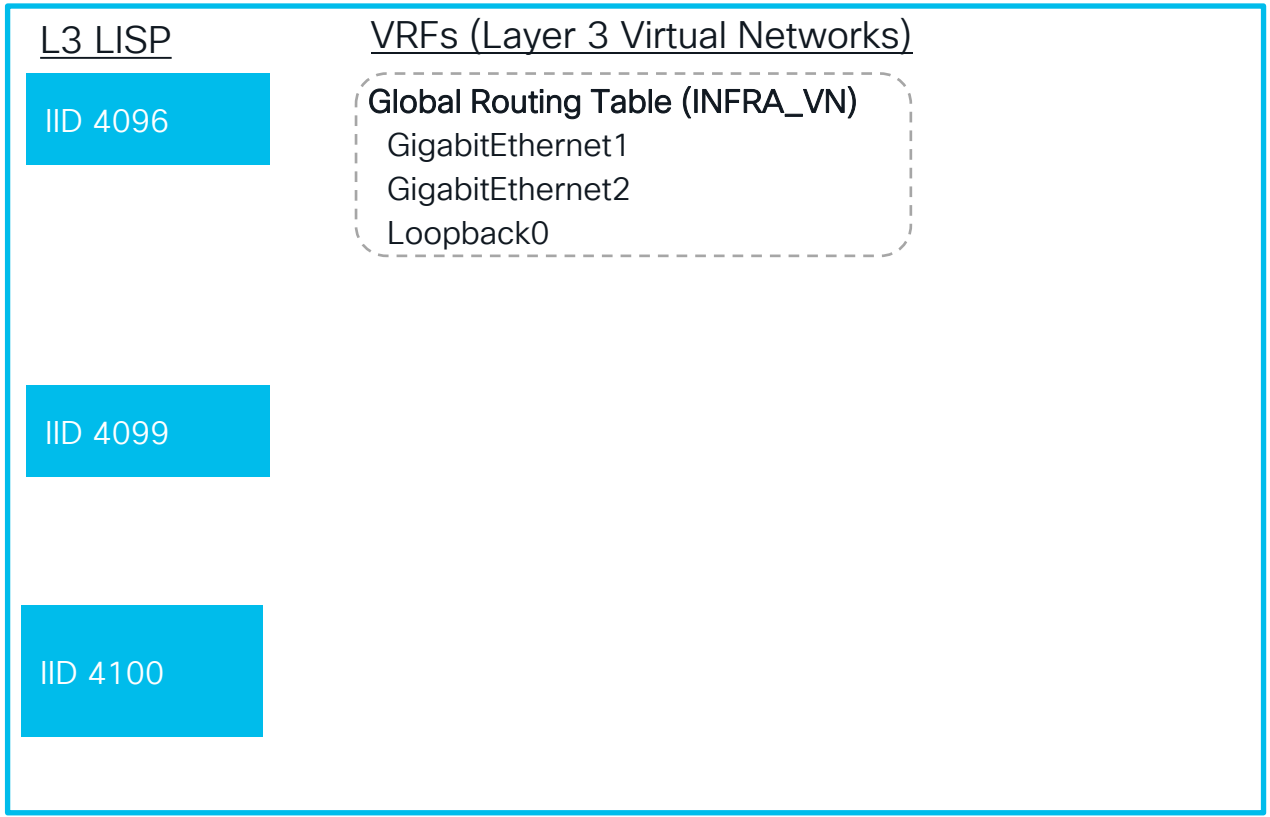
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Node service mapping



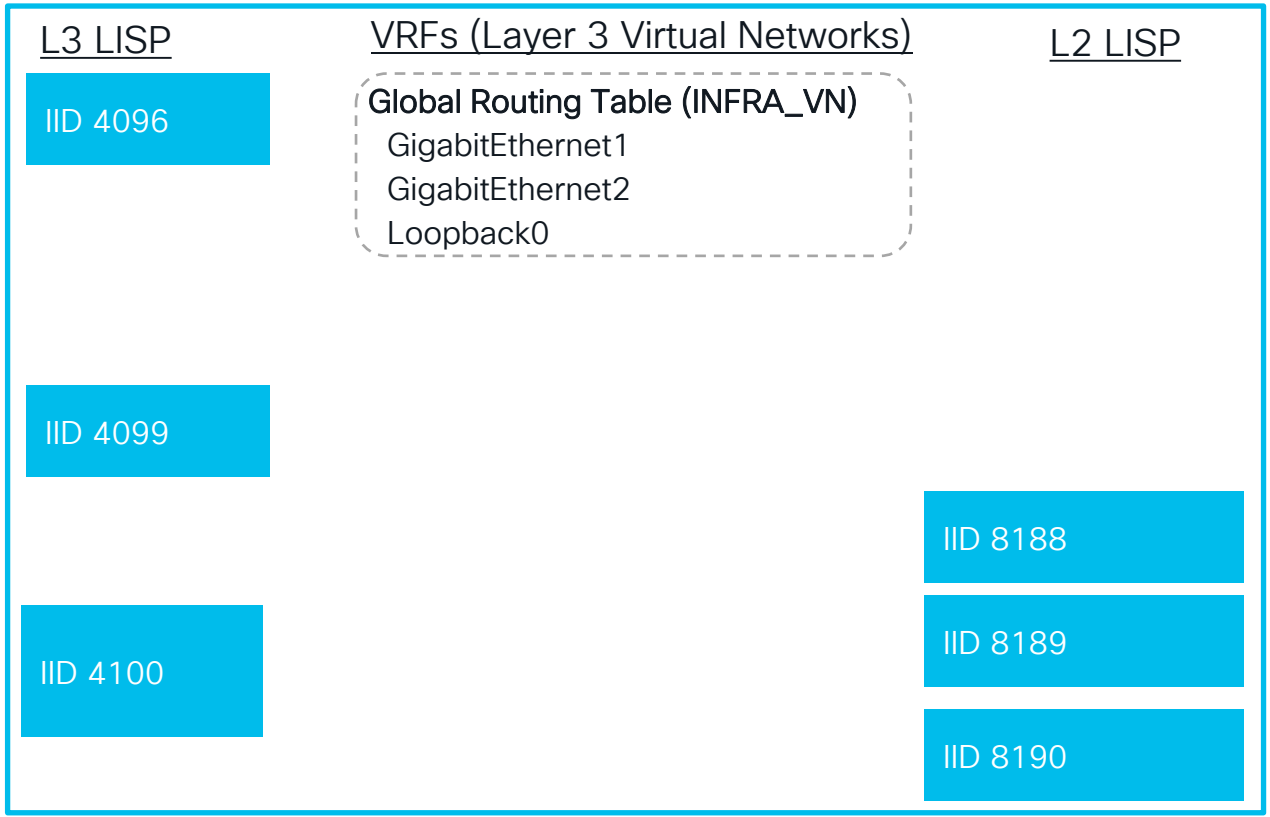
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Node service mapping



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Node service mapping



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Node service mapping

```
!CP1
!
interface Loopback1023
 ip address 172.31.136.1 255.255.255.255
!
router lisp
 !
 service ipv4
  map-server
  map-resolver
  exit-service-ipv4
 !
 service ethernet
  map-server
  map-resolver
  exit-service-ethernet
 !
 site site_uci
  eid-record instance-id 4097 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4097 172.31.136.0/24 accept-more-specifics
  eid-record instance-id 4099 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4099 10.4.3.0/24 accept-more-specifics
  eid-record instance-id 4100 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4100 10.3.3.0/24 accept-more-specifics
  eid-record instance-id 8188 any-mac
  eid-record instance-id 8189 any-mac
  eid-record instance-id 8190 any-mac
  allow-locator-default-etr instance-id 4097 ipv4
  allow-locator-default-etr instance-id 4099 ipv4
  allow-locator-default-etr instance-id 4100 ipv4
```

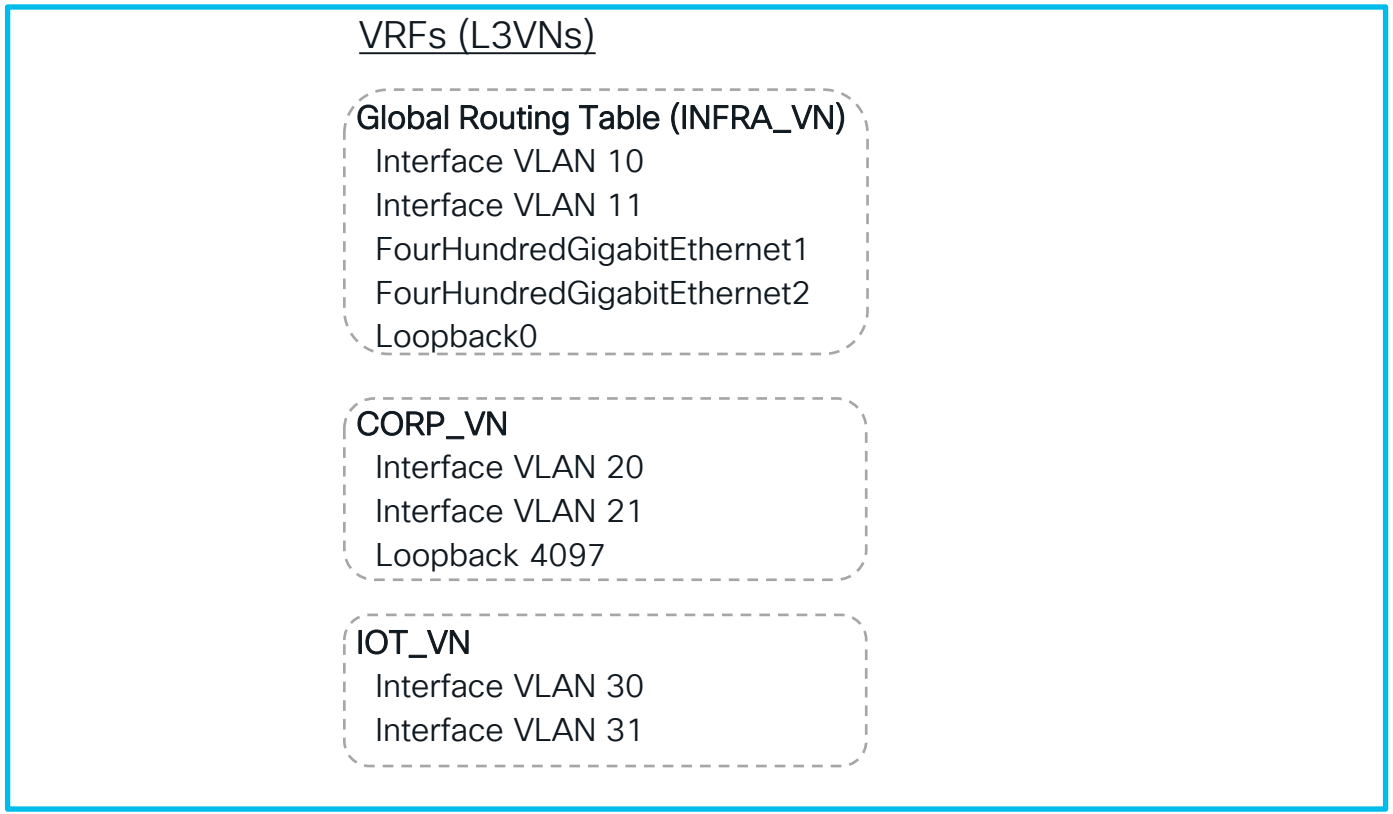
Default IPv4 settings for L3 IIDs

Default settings for L2 IIDs

EID registrations to be accepted per IID

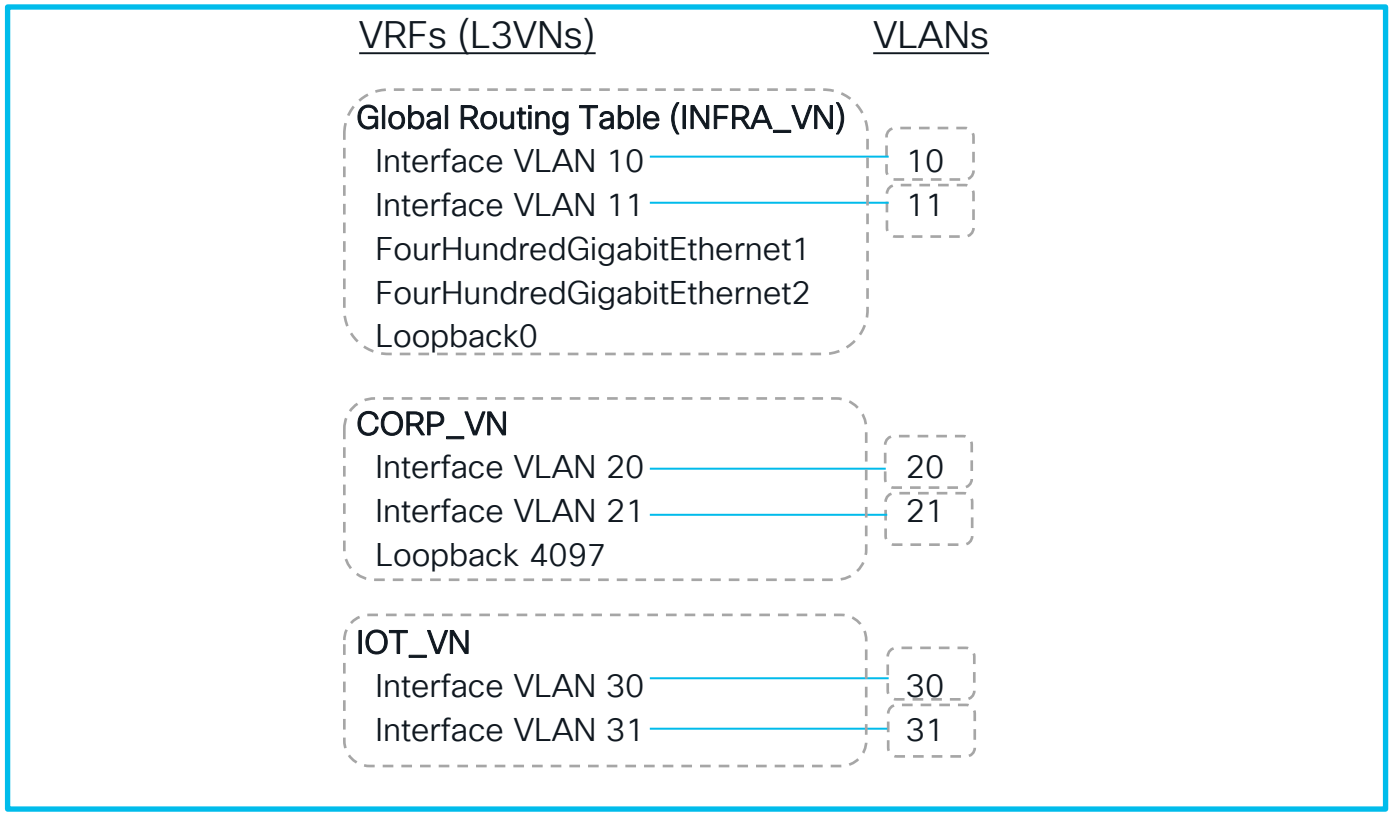
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node service mapping



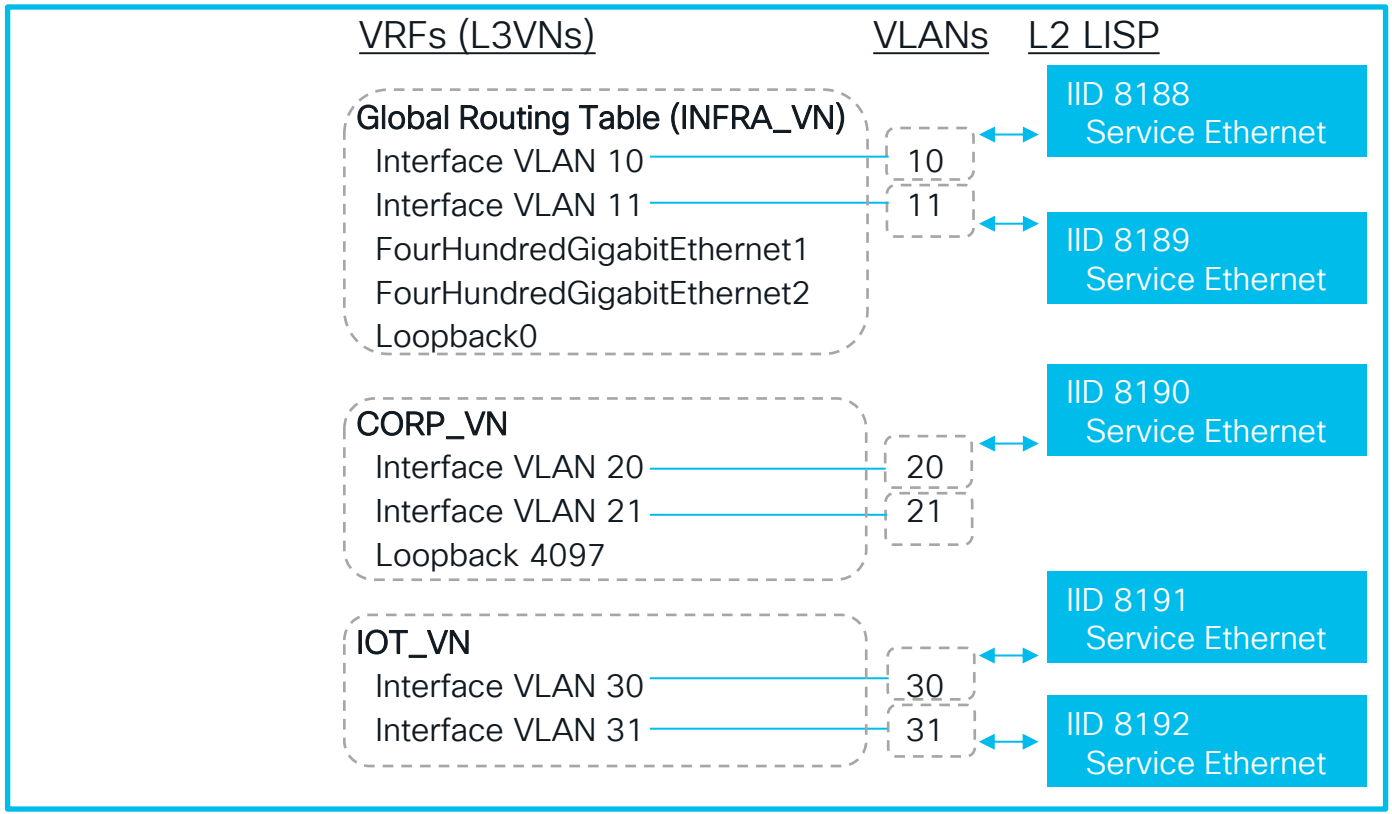
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node service mapping



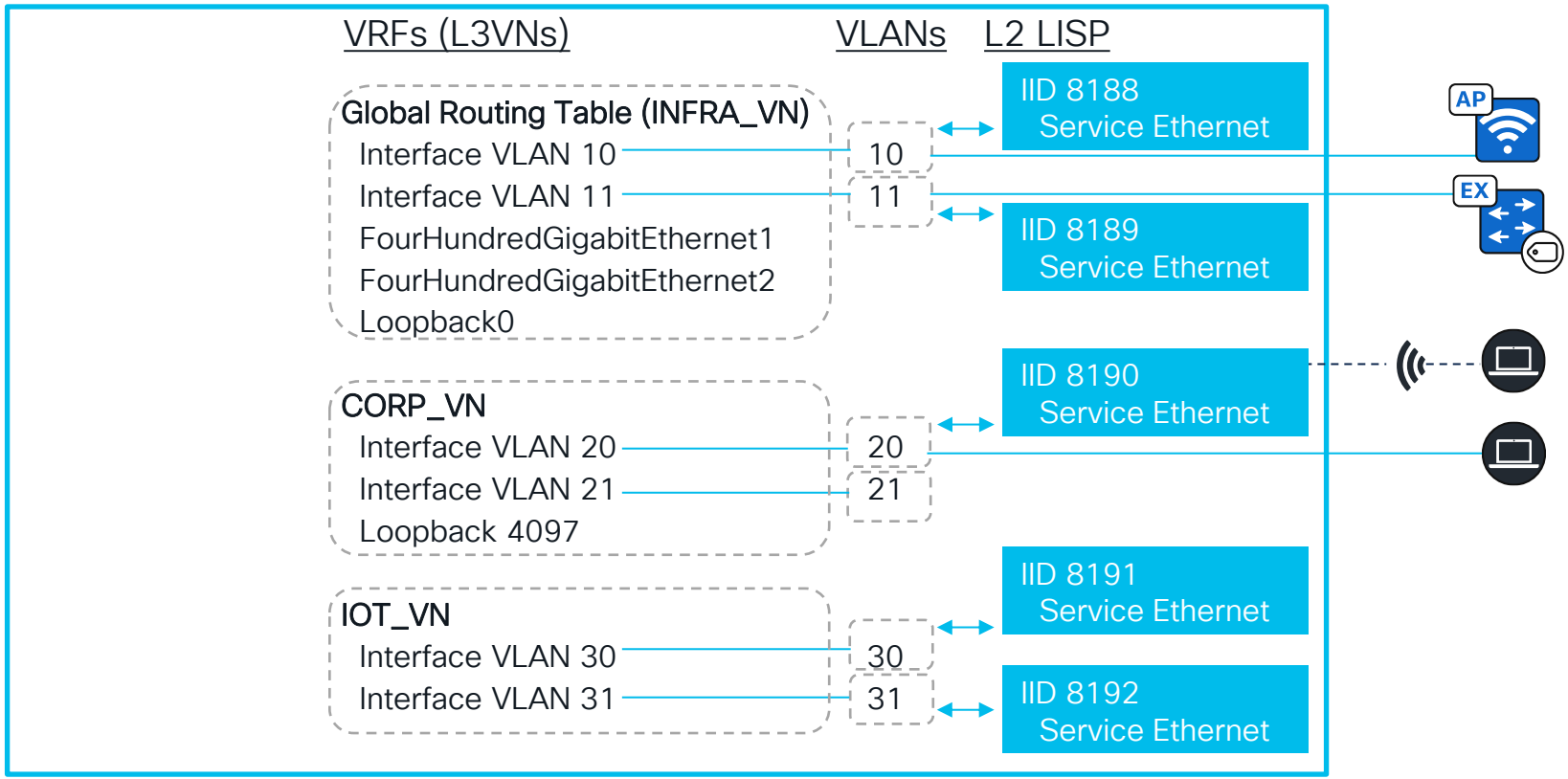
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node service mapping



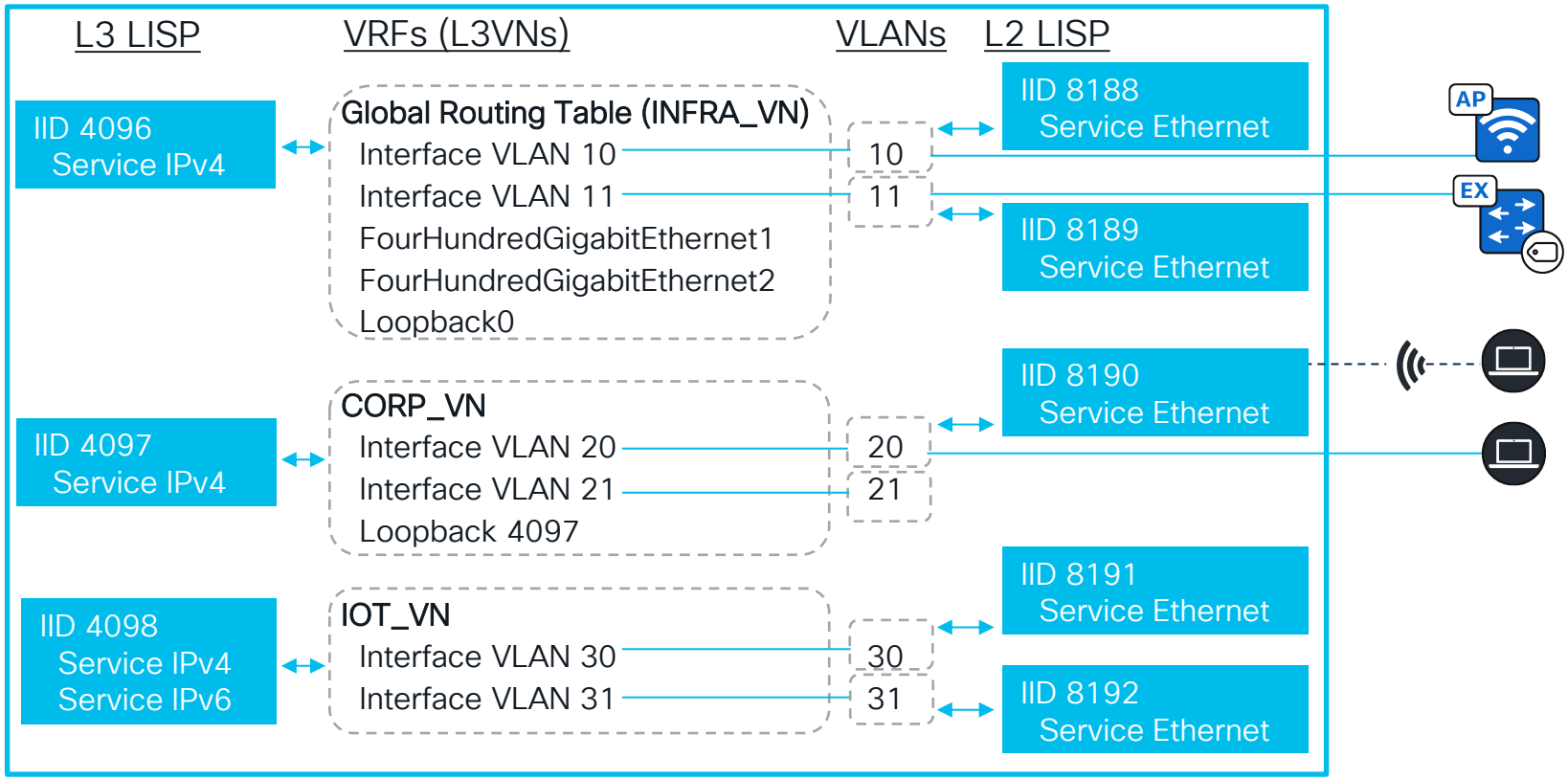
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node service mapping



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node service mapping



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node service mapping

```
!EN1
!
vrf definition CORP_VN
vrf definition IOT_VN
!
interface Loopback0
 ip address 172.31.216.76 255.255.255.255
!
interface TenGigabitEthernet1/1/1
 ip address 172.31.216.82 255.255.255.254
!
interface TenGigabitEthernet2/1/1
 ip address 172.31.216.80 255.255.255.254
!
interface Vlan1021
 vrf forwarding IOT_VN
 ip address 10.3.3.1 255.255.255.0
!
interface Vlan1022
 vrf forwarding CORP_VN
 ip address 10.4.3.1 255.255.255.0
!
interface Vlan1023
 ip address 172.31.136.1 255.255.255.0
!
router lisp
 service ipv4
  etr
  proxy-itr 172.31.216.76
 service ethernet
  itr
  etr
 !
 !router lisp continued in next column --->
```

VRFs aka L3VNs

Interfaces in VRFs

Default IPv4 settings for L3 IIDs

Default settings for L2 IIDs

```
!--> router lisp continued from previous next column
!
 instance-id 4097
  service ipv4
   eid-table default
 !
 instance-id 4099
  service ipv4
   eid-table vrf CORP_VN
 !
 instance-id 4100
  service ipv4
   eid-table vrf IOT_VN
 !
 instance-id 8188
  service ethernet
   eid-table vlan 1021
 !
 instance-id 8189
  service ethernet
   eid-table vlan 1022
 !
 instance-id 8190
  service ethernet
   eid-table vlan 1023
```

IID with IPv4 enabled in default routing table aka global routing table aka ‘INFRA_VN’

IID with IPv4 enabled in VRF ‘CORP_VN’

IID with IPv4 enabled in VRF ‘IOT_VN’

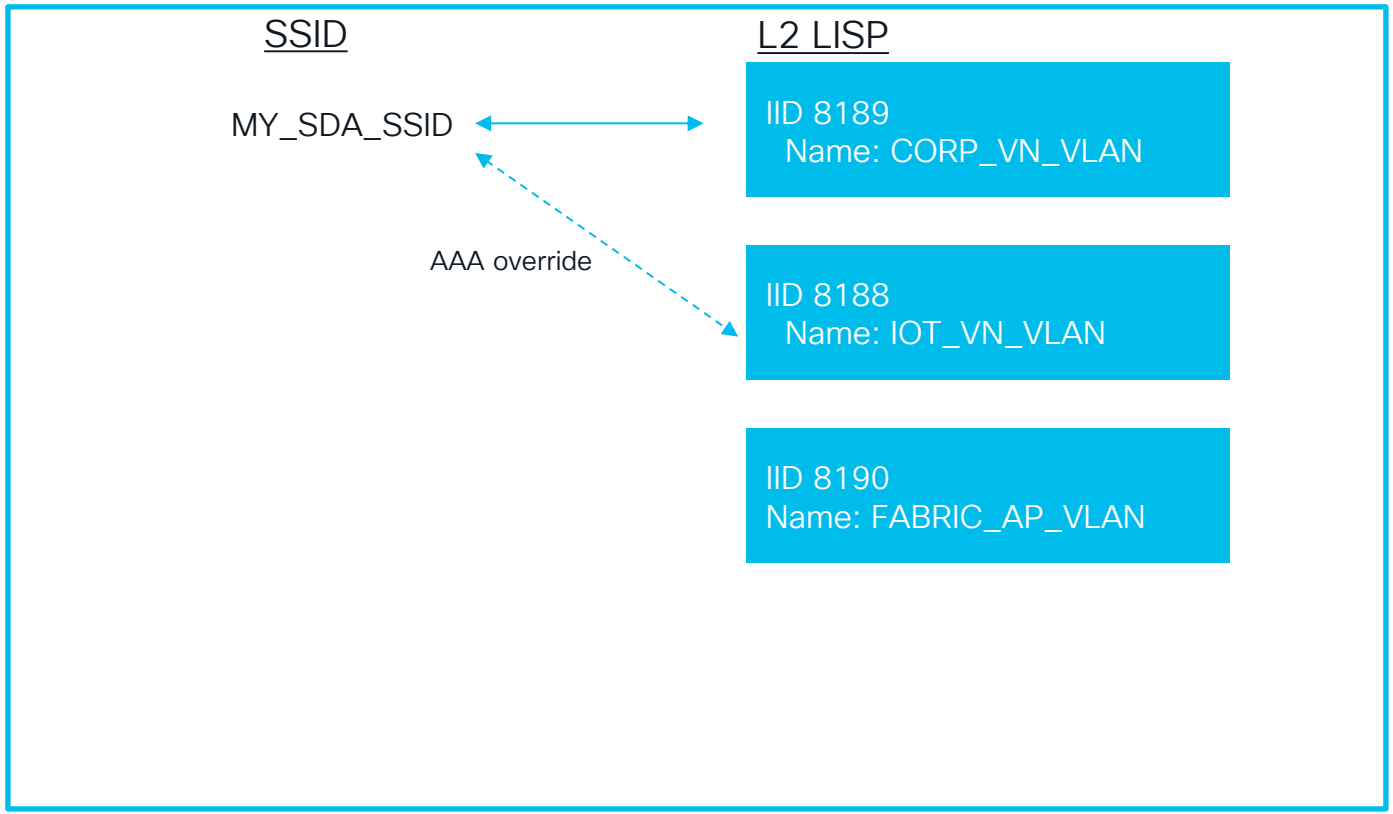
IID with L2 enabled for access VLAN 1021

IID with L2 enabled for access VLAN 1022

IID with L2 enabled for access VLAN 1023

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric WLC service mapping



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric WLC configuration

```
!WLC
!
wireless fabric name IOT_VN_VLAN l2-vnid 8188 control-plane-name default-control-plane
wireless fabric name CORP_VN_VLAN l2-vnid 8189 control-plane-name default-control-plane
!
wireless fabric name FABRIC_AP_VLAN l2-vnid 8190 l3-vnid 4097 ip 172.31.136.0 255.255.255.0 control-plane-name
!
wireless profile policy SDA_jedolphi_profile
 fabric SDA_jedolphi_profile
!
wlan SDA_jedolphi_profile 17 MY_SDA_SSID
!
wireless profile fabric SDA_jedolphi_profile
 client-l2-vnid 8189
```

SD-Access L2 IIDs with Fabric Enabled Wireless enabled

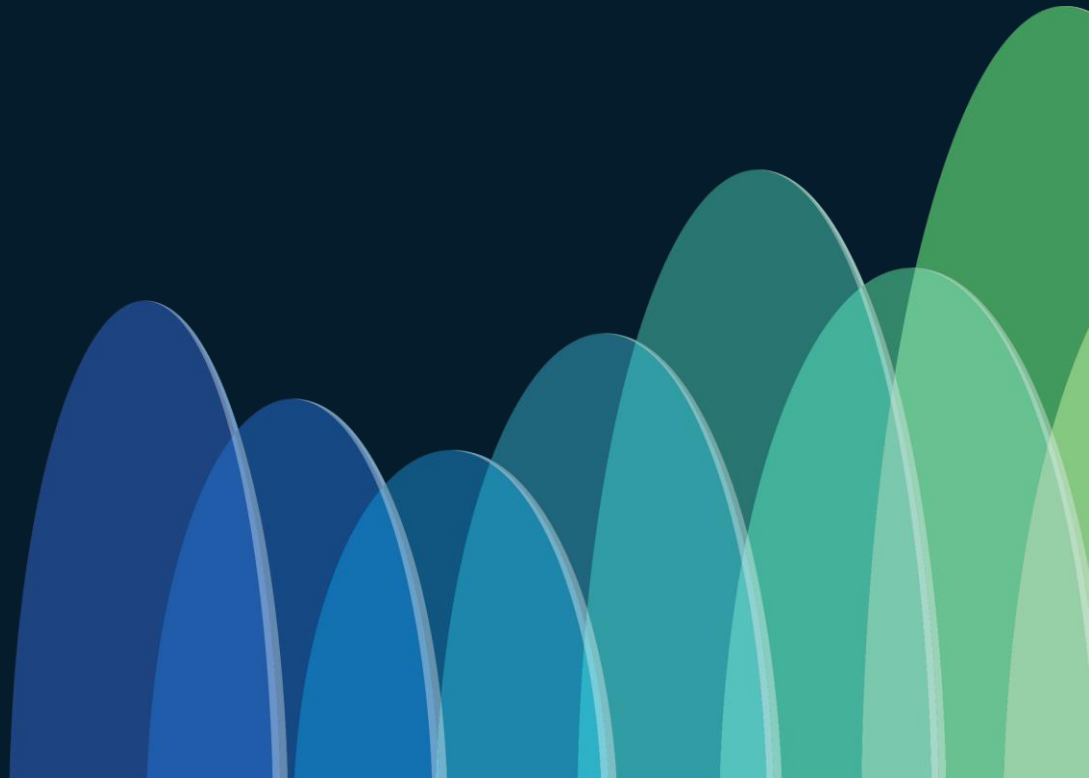
SD-Access INFRA_VN Fabric AP subnet

Fabric Enabled Wireless SSID

Default L2 IID, if no AAA override

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node Default ETR Registration

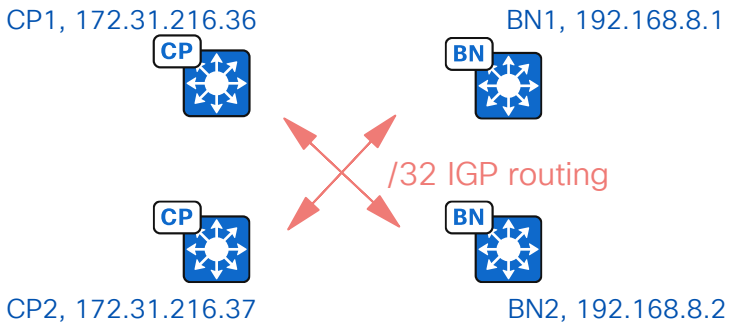


Default ETR

- Think of default ETR (egress tunnel router) as a gateway of last resort within the LISP domain.
- In a LISP Pub/Sub network an External Border Node will:
  - Register as a reachable default ETR if there is usable default route in RIB for the VRF associated with the LISP L3 IID. A default route from any routing protocol is valid.
  - Register as an unreachable default ETR if there is no usable default route in RIB for the VRF associated with the LISP L3 IID.
- INFRA_VN does not implement default ETR and instead uses RIB for default route.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

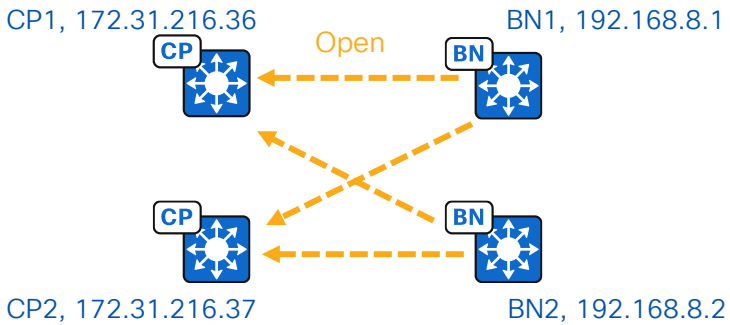
Border Node default ETR registration



Timeline:
1. CPs and BNs boot.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

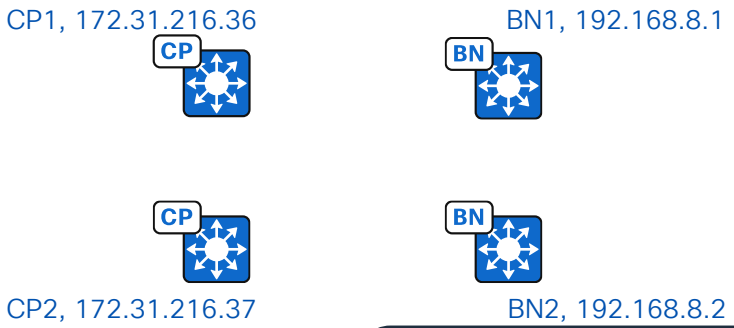
Border Node default ETR registration



Timeline:
1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration



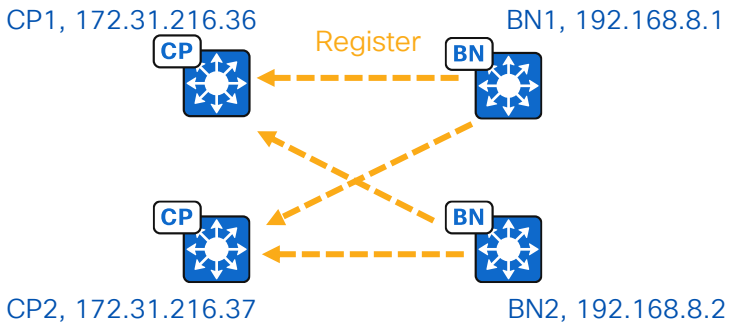
Timeline:
1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.

BNs open LISP peering sessions with CPs

```
BN2#show lisp session

Sessions for VRF default, total: 2, established: 2
Peer                  State      Up/Down        In/Out    Users
172.31.216.36:4342    Up         00:23:23       71/17     7
172.31.216.37:4342    Up         00:23:23       73/17     7
BN2#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration



Timeline:

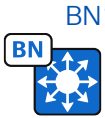
1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.
3. External BNs register default ETR as unreachable (priority 255) per user-defined L3VN. INFRA_VN is not configured for default ETR.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration

External BNs register default ETR as unreachable (priority 255) per L3VN

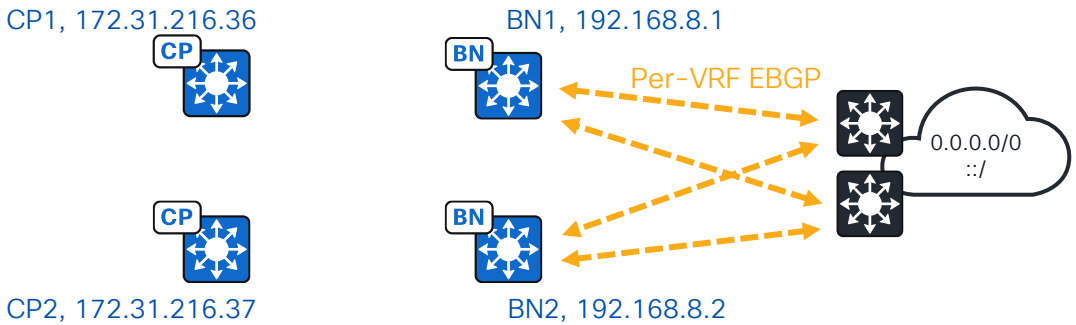
```
CP1#show lisp remote-locator-set default-etrs
Codes:
ETR = ETR Type (Default = Default-ETR, Service = Service-ETR)
SI  = Service Insertion Type
ID  = Service Insertion ID
-   = No service insertion config type defined
DS  = Default-ETR Firewall Service Insertion
SS  = Service-ETR Firewall Service Insertion
P   = Primary/Direct in use, Backup not available
PB  = Primary/Direct in use, Backup available
B   = Backup in use, Primary/Direct not available
BP  = Backup in use, Primary/Direct available
MT  = Multisite Service Insertion
 * = This locator has multiple service EID configured.

LISP remote-locator-set default-etr-locator-set-ipv4 Information

 RLOC           Pri/Wgt/Metric     Inst       Domain-ID/MH-ID  ETR       SI/ID
 192.168.8.1    255/10 /-          4099       2070054968/34872 Default
 192.168.8.1    255/10 /-          4100       2070054968/34872 Default
 192.168.8.2    255/10 /-          4099       2070054968/34872 Default
 192.168.8.2    255/10 /-          4100       2070054968/34872 Default

CP1#
```



ser-defined L3VN. INFRA_VN is not configured for

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration



Timeline:

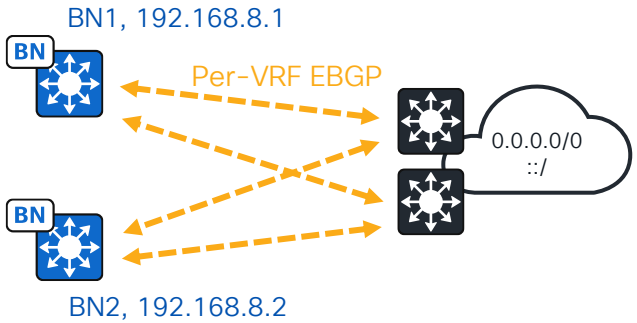
1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.
3. External BNs register default ETR as unreachable (priority 255) per user-defined L3VN. INFRA_VN is not configured for default ETR.
4. External BNs to external network EBGP sessions come up and 0.0.0.0/0 is added to BN RIB per VRF.
   Note: It could be any routing protocol protocol programming default route to RIB, but BGP is recommended.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration

Default route learned per External BN VRF

```
BN2#show ip route vrf * | i 0.0.0.0|Routing Table
Gateway of last resort is 192.0.2.2 to network 0.0.0.0
i*L2   0.0.0.0/0 [115/10] via 192.0.2.2, 1w4d, HundredGigE1/0/32
       10.0.0.0/24 is subnetted, 1 subnets
Routing Table: CORP_VN
Gateway of last resort is 172.29.4.49 to network 0.0.0.0
B*     0.0.0.0/0 [20/0] via 172.29.4.49, 1w4d
       10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
Routing Table: IOT_VN
Gateway of last resort is 172.29.4.57 to network 0.0.0.0
B*     0.0.0.0/0 [20/0] via 172.29.4.57, 1w4d
       10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
BN2#
```

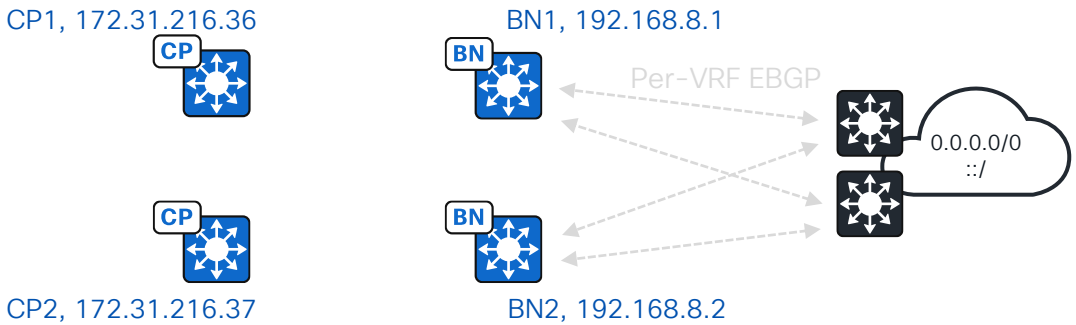


Timeline:

1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.
3. External BNs register default ETR as unreachable (priority 255) per user-defined L3VN. INFRA_VN is not configured for default ETR.
4. External BNs to external network EBGP sessions come up and 0.0.0.0/0 is added to BN RIB per VRF.
   Note: It could be any routing protocol protocol programming default route to RIB, but BGP is recommended.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration



Timeline:

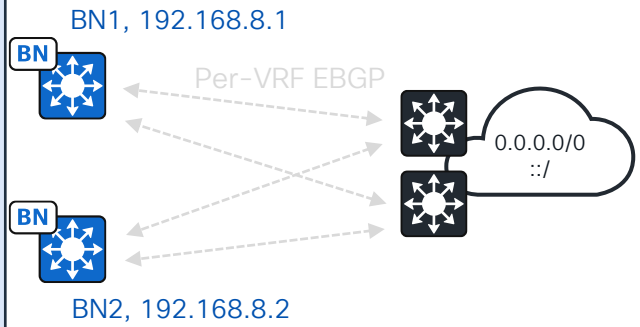
1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.
3. External BNs register default ETR as unreachable (priority 255) per user-defined L3VN. INFRA_VN is not configured for default ETR.
4. External BNs to external network EBGP sessions come up and 0.0.0.0/0 is added to BN RIB per VRF.
   Note: It could be any routing protocol protocol programming default route to RIB, but BGP is recommended.
5. External BN LISP database is updated per IID with a default route.
   Note: LISP database holds authoritative local EID-to-RLOC mappings and is used for registrations.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration

External BN LISP database is updated per IID with default ETR

```
BN1#show lisp instance-id * ipv4 database
================================================
Output for router lisp 0 instance-id 4097
================================================
% No local database entries configured.
================================================
Output for router lisp 0 instance-id 4099
================================================
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf CORP_VN (IID 4099), LSBs: 0x3
Entries total 6, no-route 0, inactive 0, do-not-register 0
0.0.0.0/0, locator-set DEFAULT_ETR_LOCATOR, default-ETR
  Uptime: 5d01h, Last-change: 18:35:11
  Domain-ID: local
  Metric: 0
  Service-Insertion: N/A
  Locator       Pri/Wgt  Source     State
  192.168.8.1   10/10    cfg-intf   site-self, reachable
    Affinity-id: 0 , 0
================================================
Output for router lisp 0 instance-id 4100
================================================
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf IOT_VN (IID 4100), LSBs: 0x3
Entries total 6, no-route 0, inactive 0, do-not-register 0
0.0.0.0/0, locator-set DEFAULT_ETR_LOCATOR, default-ETR
  Uptime: 01:23:31, Last-change: 00:05:20
  Domain-ID: local
  Metric: 0
  Service-Insertion: N/A
  Locator       Pri/Wgt  Source     State
  192.168.8.1   10/10    cfg-intf   site-self, reachable
    Affinity-id: 0 , 0
BN1#
```



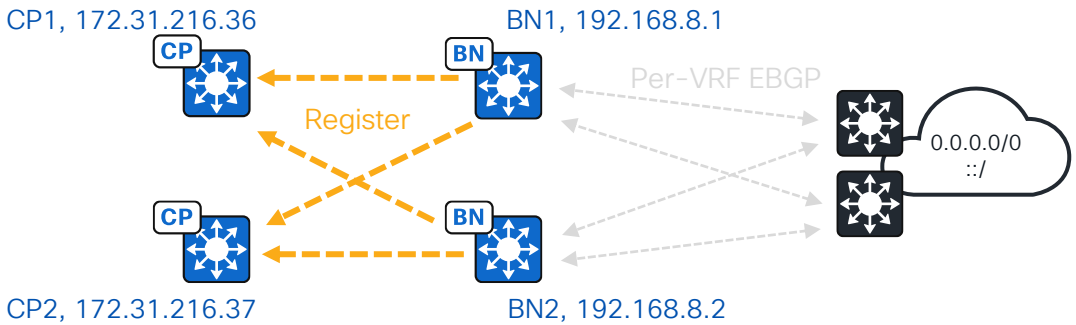
efined L3VN. INFRA_VN is not configured for

added to BN RIB per VRF.
is recommended.

strations.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration



Timeline:

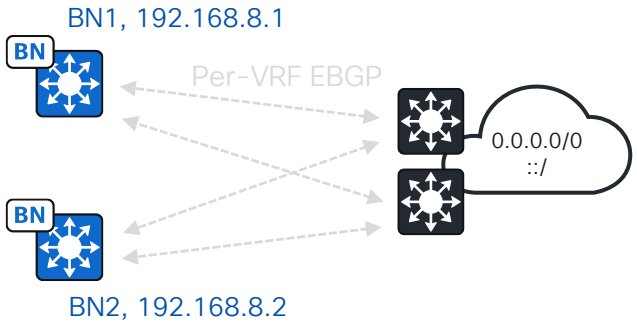
1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.
3. External BNs register default ETR as unreachable (priority 255) per user-defined L3VN. INFRA_VN is not configured for default ETR.
4. External BNs to external network EBGP sessions come up and 0.0.0.0/0 is added to BN RIB per VRF.
   Note: It could be any routing protocol protocol programming default route to RIB, but BGP is recommended.
5. External BN LISP database is updated per IID with a default route.
   Note: LISP database holds authoritative local EID-to-RLOC mappings and is used for registrations.
6. The addition of default route to LISP database triggers a default ETR registration to CP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration

LISP database default ETR triggers default ETR registration to CP

```
CP1#show lisp remote-locator-set default-etrs
Codes:
ETR = ETR Type (Default = Default-ETR, Service = Service-ETR)
SI  = Service Insertion Type
ID  = Service Insertion ID
-   = No service insertion config type defined
DS  = Default-ETR Firewall Service Insertion
SS  = Service-ETR Firewall Service Insertion
P   = Primary/Direct in use, Backup not available
PB  = Primary/Direct in use, Backup available
B   = Backup in use, Primary/Direct not available
BP  = Backup in use, Primary/Direct available
MT  = Multisite Service Insertion
 * = This locator has multiple service EID configured.

LISP remote-locator-set default-etr-locator-set-ipv4 Information

 RLOC           Pri/Wgt/Metric     Inst       Domain-ID/MH-ID  ETR       SI/ID
 192.168.8.1    10/10 /0           4099       2070054968/34872 Default   PB/-
 192.168.8.1    10/10 /0           4100       2070054968/34872 Default   PB/-
 192.168.8.2    10/10 /0           4099       2070054968/34872 Default   PB/-
 192.168.8.2    10/10 /0           4100       2070054968/34872 Default   PB/-

CP1#
```



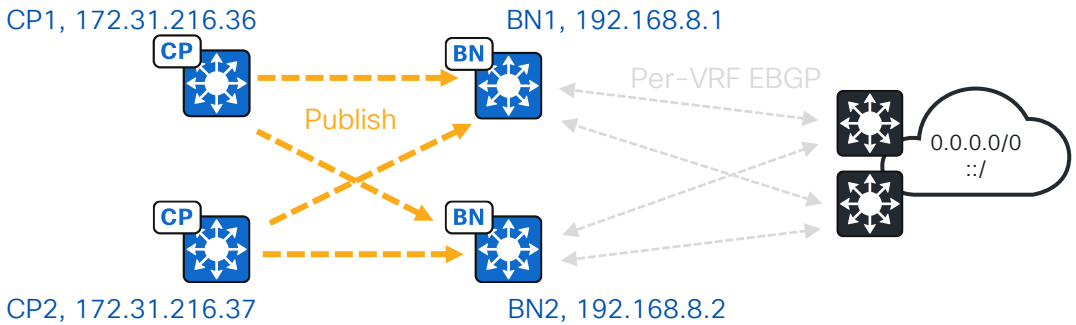
-defined L3VN. INFRA_VN is not configured for

) is added to BN RIB per VRF.
BGP is recommended.

5. External BN LISP database is updated per IID with a default route.
   Note: LISP database holds authoritative local EID-to-RLOC mappings and is used for registrations.
6. The addition of default route to LISP database triggers a default ETR registration to CP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration



Timeline:

1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.
3. External BNs register default ETR as unreachable (priority 255) per user-defined L3VN. INFRA_VN is not configured for default ETR.
4. External BNs to external network EBGP sessions come up and 0.0.0.0/0 is added to BN RIB per VRF.
   Note: It could be any routing protocol protocol programming default route to RIB, but BGP is recommended.
5. External BN LISP database is updated per IID with a default route.
   Note: LISP database holds authoritative local EID-to-RLOC mappings and is used for registrations.
6. The addition of default route to LISP database triggers a default ETR registration to CP.
7. CP IPv4/IPv6 registrations are published to Subscribers (BNs).

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration

CP1, 172.31.216.36

CP2, 172.31.216.37

Timeline:

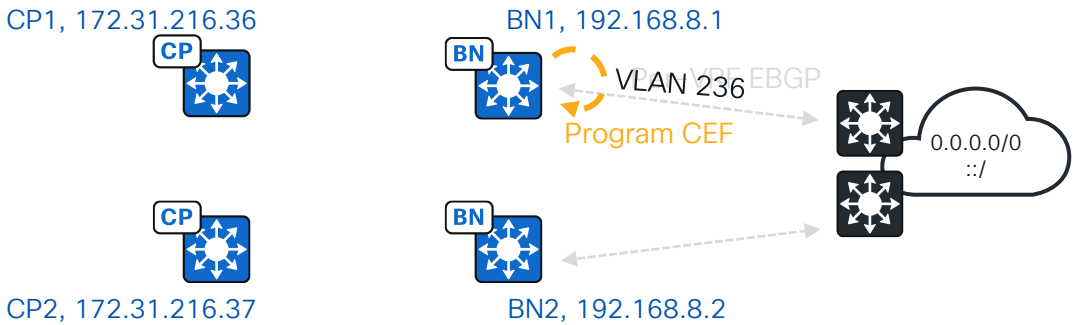
1. CPs and BNs boot.
2. BNs open LISP peering sessions with CPs.
3. External BNs register default ETR as unreachable (priority 25
   default ETR.
4. External BNs to external network EBGP sessions come up an
   Note: It could be any routing protocol protocol programming default route
5. External BN LISP database is updated per IID with a default r
   Note: LISP database holds authoritative local EID-to-RLOC mappings and is
6. The addition of default route to LISP database triggers a defa
7. CP IPv4/IPv6 registrations are published to Subscribers (BNs).

CP IPv4/IPv6 registrations are published to Subscribers (BNs)

```
BN1#show lisp instance-id 4099 ipv4 publication 0.0.0.0/0
Publication Information for LISP 0 EID-table vrf CORP_VN (IID 4099)

  EID-prefix: 0.0.0.0/0
    ...
    Publisher 172.31.216.36:4342
      last published 00:33:53, TTL never, Expires: never
      publisher epoch 0, entry epoch 0
      entry-state unknown-eid-forward
      xTR-ID 0xEBDD7D7E-0x3760F5B7-0x30A76456-0x64CF563F
      site-ID unspecified
      Domain-ID 2070054968
      Multihoming-ID 34872
      Locator         Pri/Wgt  State     Encap-IID   Domain-ID/MH-ID   Metric
      192.168.8.1     10/10    up        -           2070054968/34872   0
      192.168.8.2     10/10    up        -           2070054968/34872   0

    Publisher 172.31.216.37:4342
      last published 00:33:53, TTL never, Expires: never
      publisher epoch 0, entry epoch 0
      entry-state unknown-eid-forward
      xTR-ID 0xEBDD7D7E-0x3760F5B7-0x30A76456-0x64CF563F
      site-ID unspecified
      Domain-ID 2070054968
      Multihoming-ID 34872
      Locator         Pri/Wgt  State     Encap-IID   Domain-ID/MH-ID   Metric
      192.168.8.1     10/10    up        -           2070054968/34872   0
      192.168.8.2     10/10    up        -           2070054968/34872   0

  Merge Locator Information
      Locator         Pri/Wgt  State     Encap-IID  RDP-Len Src-Address
      192.168.8.1     10/10    up        -          0       172.31.216.36
      192.168.8.2     10/10    up        -          0       172.31.216.36
BN1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration



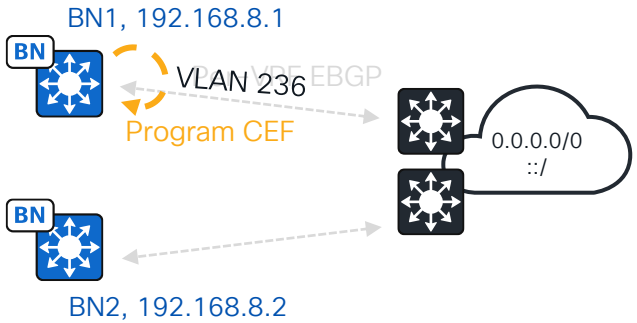
Timeline:
8. External BN prefers RIB default route over LISP map cache default route. EBGP default route is programmed to CEF. LISP map cache default route via alternate External BN is programmed to CEF if BN-local RIB default route fails.
Note: LISP map cache stores dynamically learned EID-to-RLOC mappings used for packet forwarding.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node default ETR registration

RIB default route is programmed to CEF in preference to LISP default route. LISP default route effectively functions as backup.

```
BN1#show ip cef vrf CORP_VN 0.0.0.0/0 detail
0.0.0.0/0, epoch 0, flags [cover dependents, subtree context, rib only
nolabel, default route]
  SC owned,sourced: LISP generalised SMR - [disabled, not inheriting,
0x74A3D01BFCF0 locks: 11]
  Covered dependent prefixes: 1
    notify cover updated: 1
  1 IPL source [no flags]
  recursive via 172.29.4.49
    attached to Vlan236
BN1#
BN1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BN1(config)#int vl236
BN1(config-if)#shut
BN1(config-if)#^Z
BN1#show ip cef vrf CORP_VN 0.0.0.0/0 detail
0.0.0.0/0, epoch 0, flags [cover dependents, subtree context, rib only
nolabel, check lisp eligibility, default route]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000000
  LISP remote EID: 0 packets 0 bytes fwd action encap, cfg as EID space
  SC owned,sourced: LISP generalised SMR - [disabled, inheriting,
0x74A3D01BFD08 locks: 11]
  LISP source path list
    nexthop 192.168.8.2 LISP0.4099
  Covered dependent prefixes: 2
    notify cover updated: 2
  3 IPL sources [no flags]
  nexthop 192.168.8.2 LISP0.4099
BN1#
```

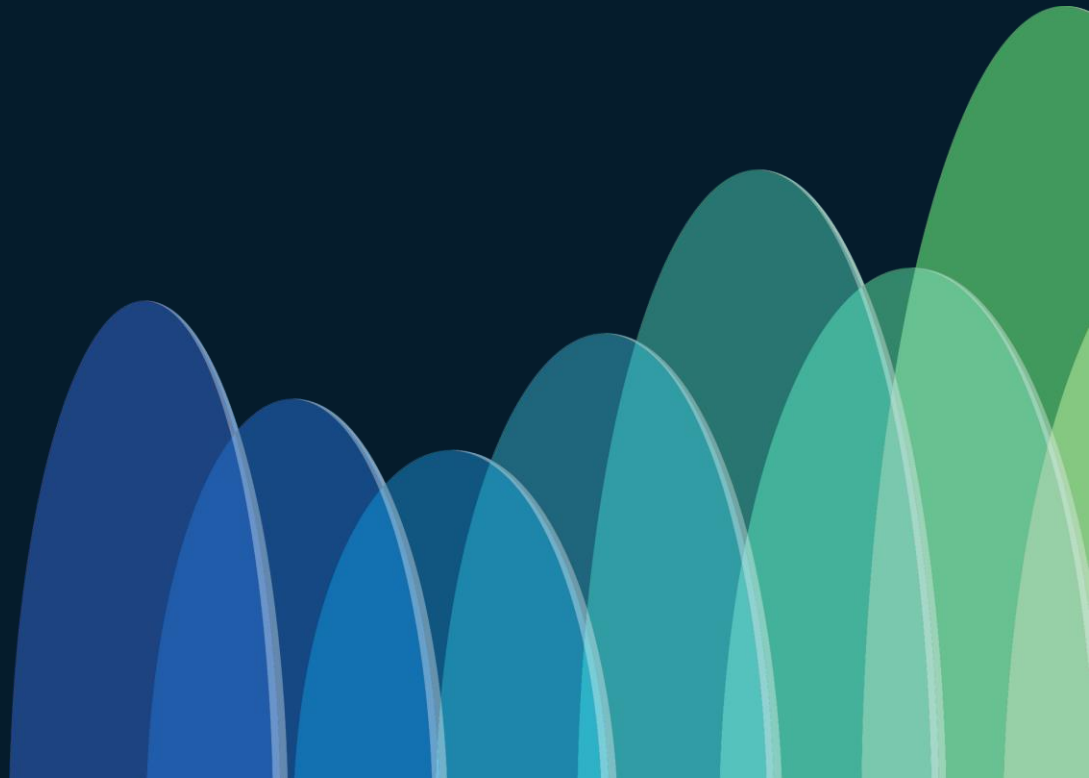


Tim
8. E
map
Note

ute. EBGP default route is programmed to CEF. LISP
F if BN-local RIB default route fails.
cket forwarding.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

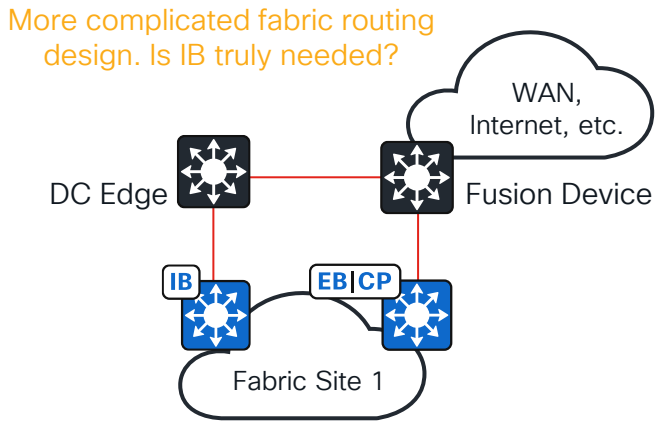
Border Node Specific Route Registration

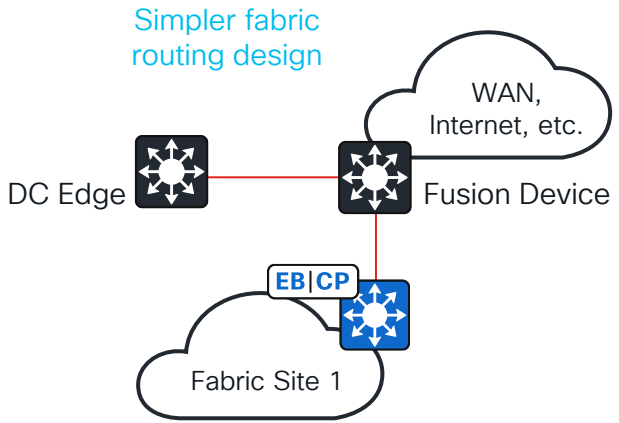


cisco Live!

Internal Border Node

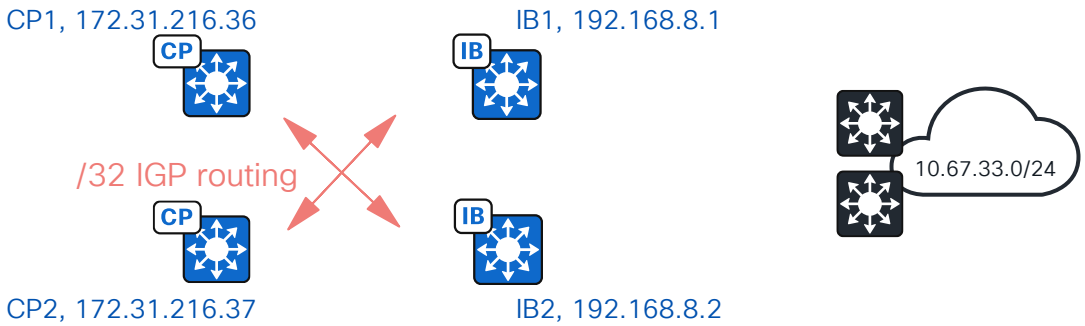
- External Border Nodes (EB) do not import routes to LISP.
- Internal Border Nodes (IB) import BGP routes to LISP.
  - Non-BGP routes are not imported to LISP.
  - IB is usually not required if all SD-Access to external network traffic will follow default ETR. Do not use IB if not truly required; design for simple routing outcomes.





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration



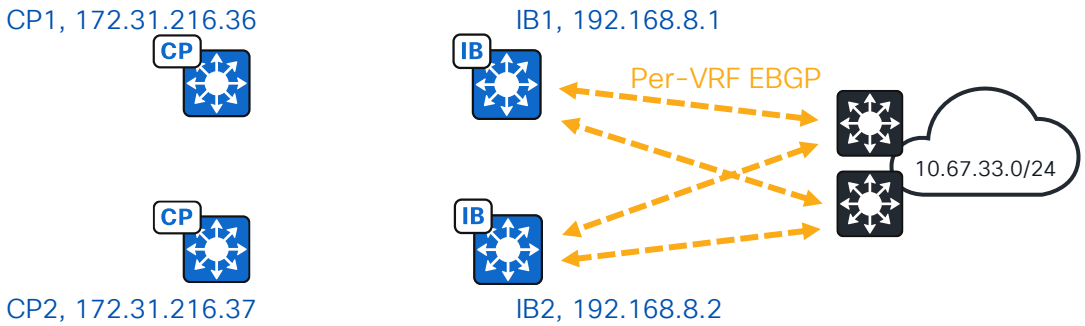
Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration



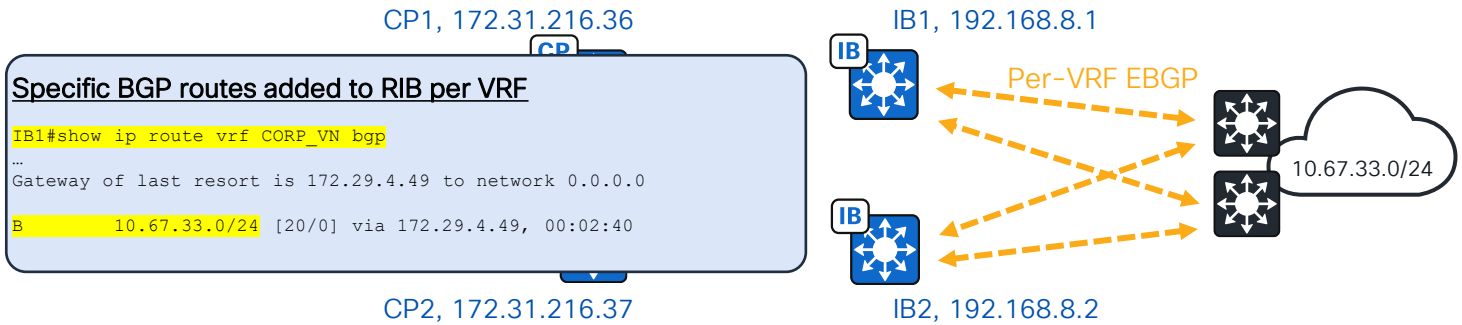
Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.
3. IB to external network BGP session comes up. EBGP 10.67.33.0/24 specific route is added to IB RIB per VRF.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration



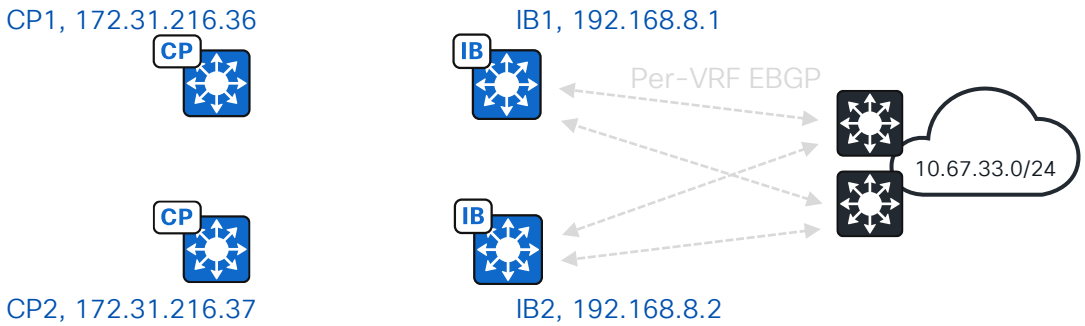
Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.
3. IB to external network BGP session comes up. EBGP 10.67.33.0/24 specific route is added to IB RIB per VRF.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration



Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.
3. IB to external network BGP session comes up. EBGP 10.67.33.0/24 specific route is added to IB RIB per VRF.
4. IB BGP prefixes are imported to LISP database per IID.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used as a source for LISP registrations.

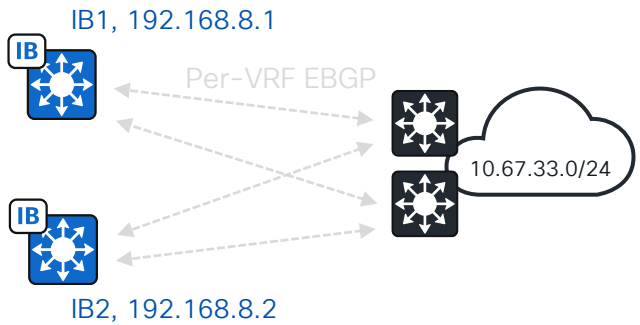
*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration

IB EBGP prefixes are imported to LISP database per IID

```
IB1#show lisp instance-id 4099 ipv4 database
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf CORP_VN (IID 4099),
LSBs: 0x3
Entries total 7, no-route 0, inactive 0, do-not-register 0
...
10.67.33.0/24, route-import, inherited from default locator-set
rloc_4d514e0d-935e-499f-9380-95cebe9e394d, auto-discover-rlocs
  Uptime: 00:05:31, Last-change: 00:05:31
  Domain-ID: local, tag: 733777
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State
  192.168.8.1    10/10    cfg-intf   site-self, reachable
  192.168.8.2    10/10    auto-disc  site-other, report-reachable
IB1#
```



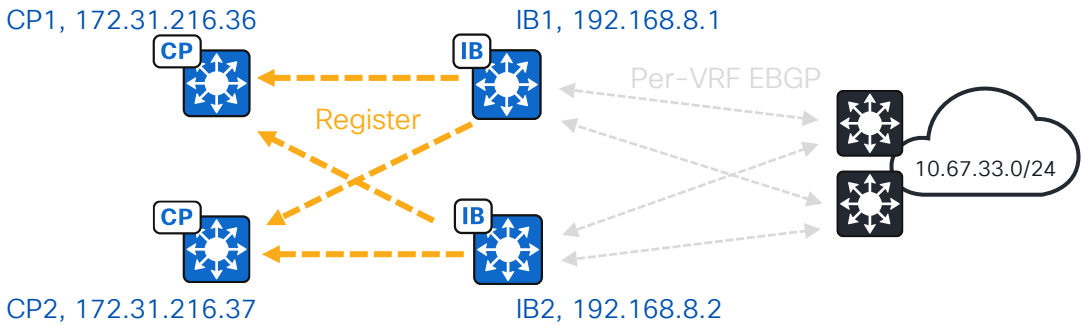
Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.
3. IB to external network BGP session comes up. EBGP 10.67.33.0/24 specific route is added to IB RIB per VRF.
4. IB BGP prefixes are imported to LISP database per IID.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used as a source for LISP registrations.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration



Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.
3. IB to external network BGP session comes up. EBGP 10.67.33.0/24 specific route is added to IB RIB per VRF.
4. IB BGP prefixes are imported to LISP database per IID.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used as a source for LISP registrations.
5. New LISP database entry triggers route registration.

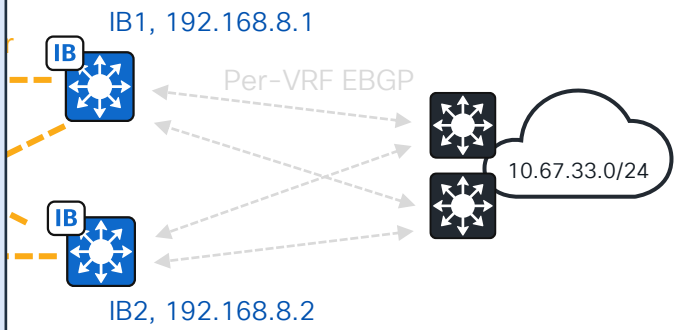
*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration

Imported specific route 10.67.33.0/24 is registered to CP

```
CP1#show lisp instance-id 4099 ipv4 server 10.67.33.0
LISP Site Registration Information

Site name: site_uci
Description: map-server configured from Catalyst Center
Allowed configured locators: any
Requested EID-prefix:

  EID-prefix: 10.67.33.0/24 instance-id 4099
    First registered:     00:22:40
    Last registered:      00:22:40
    Routing table tag:    733777, from registration
    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
    …
    Merged locators
      Locator       Local  State      Pri/Wgt  Scope      Registering ETR     RDP
      192.168.8.1   yes    up         10/10    IPv4 none  192.168.8.1:28219   [-]
      192.168.8.2   yes    up         10/10    IPv4 none  192.168.8.2:18554   [-]
CP1#
```



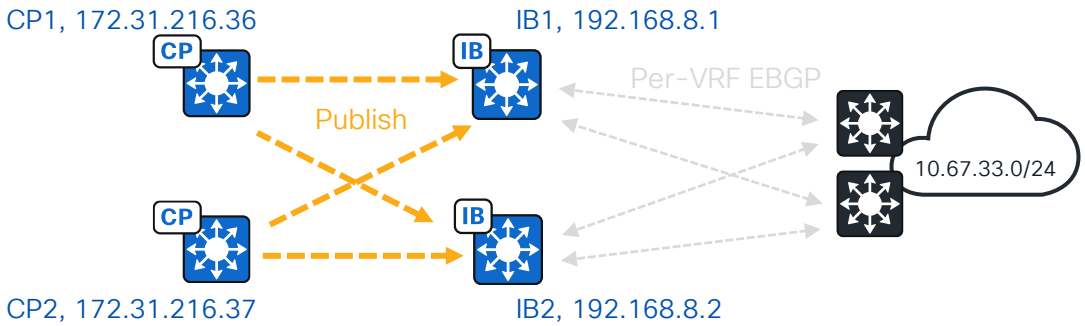
cific route is added to IB RIB per VRF.

e for LISP registrations.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration



Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.
3. IB to external network BGP session comes up. EBGP 10.67.33.0/24 specific route is added to IB RIB per VRF.
4. IB BGP prefixes are imported to LISP database per IID.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used as a source for LISP registrations.
5. New LISP database entry triggers route registration.
6. CP IPv4/IPv6 registrations are published to Subscribers (all BNs).

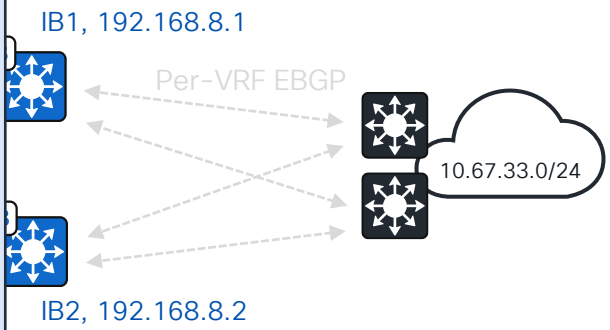
*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration

Imported specific route 10.67.33.0/24 is published by CP to all site

```
IB1#show lisp instance-id 4099 ipv4 publication
Publication Information for LISP 0 EID-table vrf CORP_VN (IID 4099)
Entries total 8
EID Prefix                Last        Last            Encap-IID
                          Published   Publisher
10.67.33.0/24             00:41:02    172.31.216.36   -
IB1#
IB1#show lisp instance-id 4099 ipv4 publication 10.67.33.0/24
Publication Information for LISP 0 EID-table vrf CORP_VN (IID 4099)
 * Indicates the selected rlocs used by consumers

  EID-prefix: 10.67.33.0/24
    ...

 Publisher 172.31.216.36:4342
      last published 00:00:32, TTL never, Expires: never
      ...
      Locator       Pri/Wgt   State     Encap-IID  RDP
      192.168.8.1   10/10     up        -          [-]
      192.168.8.2   10/10     up        -          [-]

    Publisher 172.31.216.37:4342
      last published 00:00:32, TTL never, Expires: never
      ...
      Locator       Pri/Wgt   State     Encap-IID  RDP
      192.168.8.1   10/10     up        -          [-]
      192.168.8.2   10/10     up        -          [-]

  Merge Locator Information
      Locator       Pri/Wgt   State     Encap-IID  RDP-Len Src-Address
      192.168.8.1   10/10     up        -          0       172.31.216.36
      192.168.8.2   10/10     up        -          0       172.31.216.36
IB1#
```



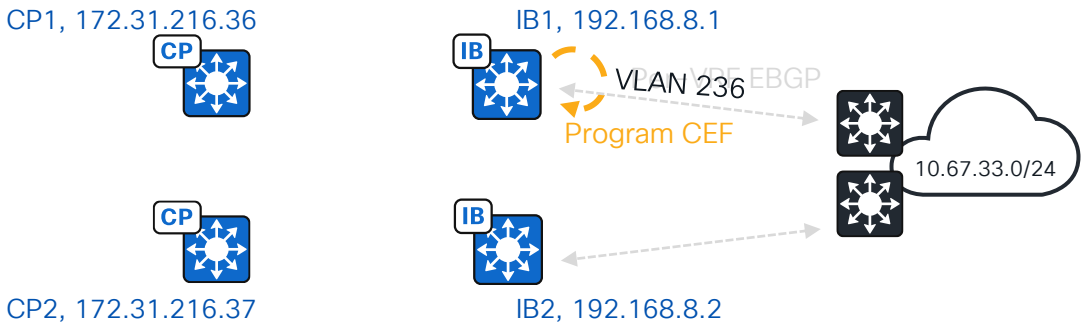
route is added to IB RIB per VRF.

SP registrations.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration



Timeline:

1. CPs and IBs boot.
2. IBs open LISP peering sessions with CPs*.
3. IB to external network BGP session comes up. EBGP 10.67.33.0/24 specific route is added to IB RIB per VRF.
4. IB BGP prefixes are imported to LISP database per IID.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used as a source for LISP registrations.
5. New LISP database entry triggers route registration.
6. CP IPv4/IPv6 registrations are published to Subscribers (all BNs).
7. IB prefers RIB specific route over LISP specific route. EBGP specific route is programmed to CEF. LISP specific route via alternate IB is programmed to CEF if IB-local RIB specific route fails.

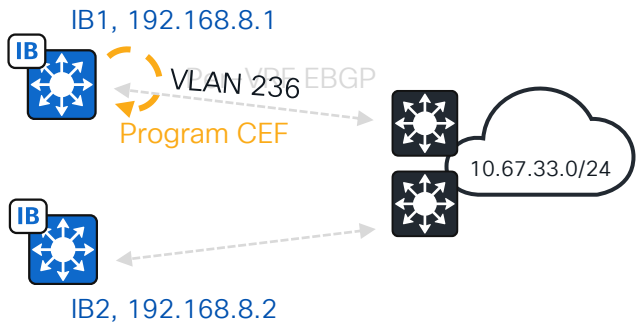
*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Border Node specific route registration

RIB specific route is programmed to CEF in preference to LISP specifc route. LISP specific route effectively functions as backup

```
IB1#show ip cef vrf CORP_VN 10.67.33.0/24 detail
10.67.33.0/24, epoch 0, flags [subtree context, rib only nolabel]
  SC owned,sourced: LISP local EID -
  LISP EID attributes: localEID Yes, c-dynEID No, d-dynEID No, a-dynEID No
  SC owned,sourced: LISP generalised SMR - [disabled, not inheriting,
0x700CA7FA04F0 locks: 1]
  2 IPL sources [no flags]
  recursive via 172.29.4.49
    attached to Vlan236
IB1#
IB1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IB1(config)#int vl236
IB1(config-if)#sh
IB1(config-if)#^Z
IB1#show ip cef vrf CORP_VN 10.67.33.0/24 detail
10.67.33.0/24, epoch 0, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 1 packets 576 bytes fwd action encap, cfg as EID space
  SC owned,sourced: LISP generalised SMR - [enabled, inheriting,
0x700CA7FA0520 locks: 1]
  LISP source path list
    nexthop 192.168.8.2 LISP0.4099
  3 IPL sources [no flags]
  nexthop 192.168.8.2 LISP0.4099
IB1#
```

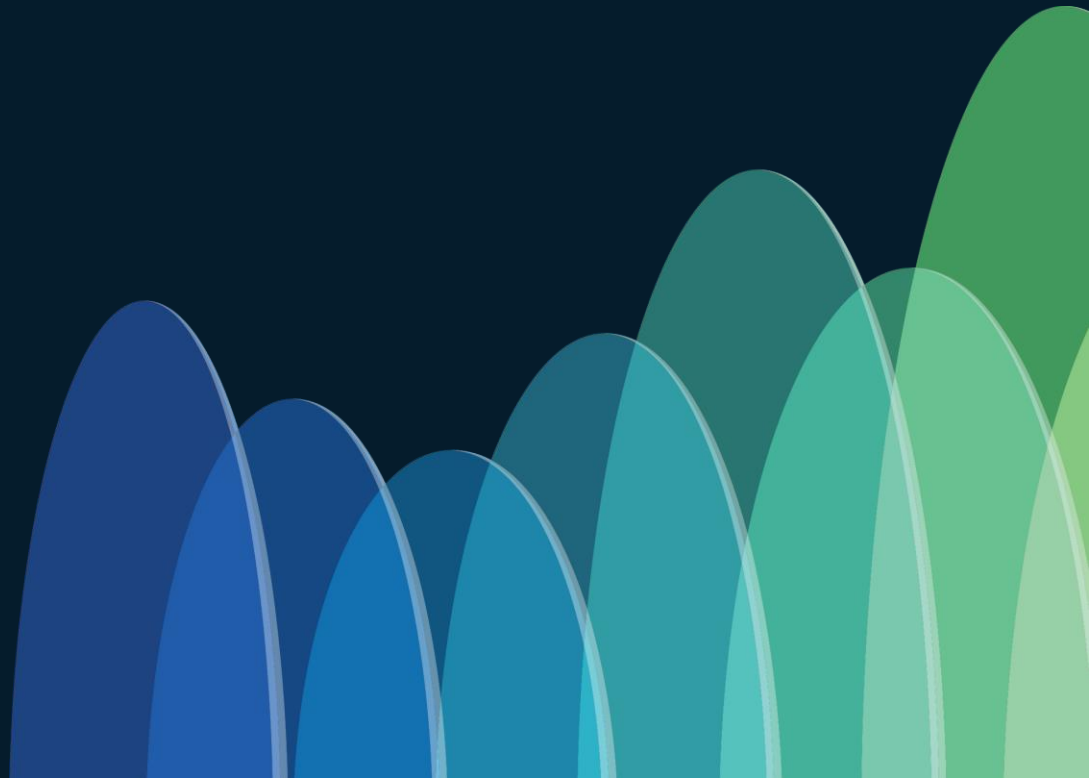


Tir
1.
2.
3. 4 specific route is added to IB RIB per VRF.
4.
source for LISP registrations.
5.
6.
7. ic route is programmed to CEF. LISP specific route via alternate IB is programmed to CEF if IB-local RIB specific route fails.

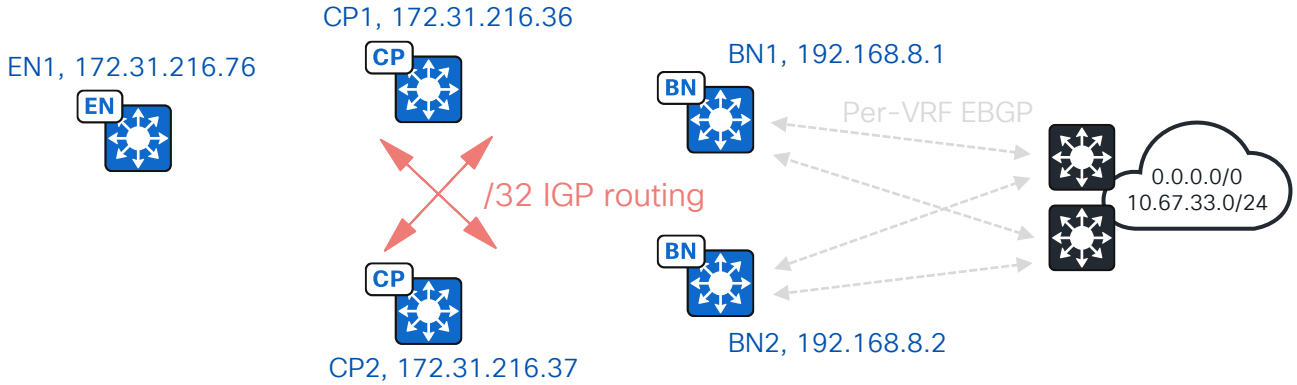
*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node Bootstrapping



Edge Node bootstrapping



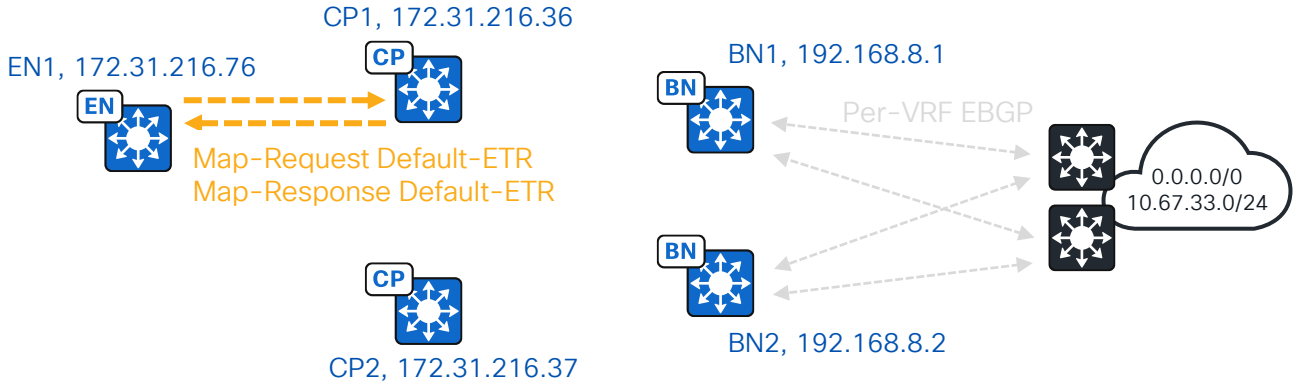
Timeline:

1. Default ETRs and specific routes are registered with CPs*.
2. Edge Node boots.
3. Edge Node opens LISP peering session with CPs*.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node bootstrapping



Timeline:

1. Default ETRs and specific routes are registered with CPs*.
2. Edge Node boots.
3. Edge Node opens LISP peering session with CPs*.
4. Edge Node automatically queries default ETR per IID. Response is received and LISP map cache is programmed.
   Note: LISP map cache stores dynamically learned EID-to-RLOC mappings used for packet forwarding.

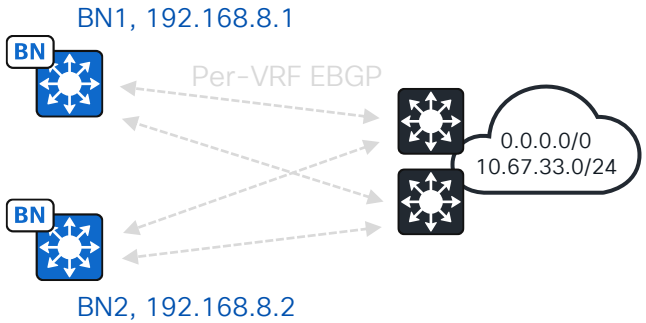
*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node bootstrapping

Edge Node LISP map cache is programmed with default route

```
EN1#show lisp instance-id * ipv4 map-cache
================================================
Output for router lisp 0 instance-id 4097
================================================
LISP IPv4 Mapping Cache for LISP 0 EID-table default (IID 4097), 1 entries
!Note there is default ETR configured for INFRA_VN
================================================
Output for router lisp 0 instance-id 4099
================================================
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf CORP_VN (IID 4099), 2 entries

0.0.0.0/0, uptime: 00:23:50, expires: 00:05:58, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
  PETR           Uptime    State      Pri/Wgt     Encap-IID  Metric
  192.168.8.1    00:23:50  up         10/10        -         0
  192.168.8.2    00:23:50  up         10/10        -         0

================================================
Output for router lisp 0 instance-id 4100
================================================
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf IOT_VN (IID 4100), 2 entries

0.0.0.0/0, uptime: 00:23:50, expires: 00:05:58, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
  PETR           Uptime    State      Pri/Wgt     Encap-IID  Metric
  192.168.8.1    00:23:50  up         10/10        -         0
  192.168.8.2    00:23:50  up         10/10        -         0

EN1#
```

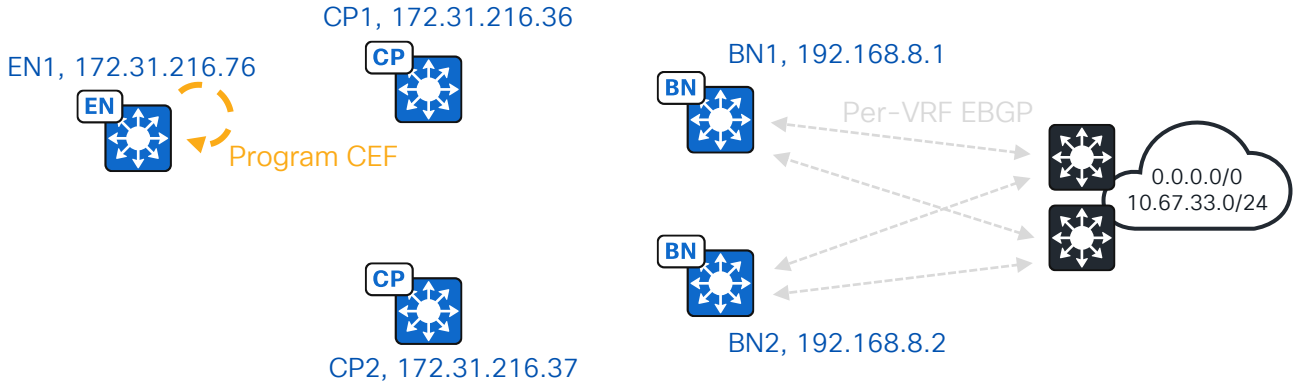


ved and LISP map cache is programmed.
ket forwarding.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node bootstrapping



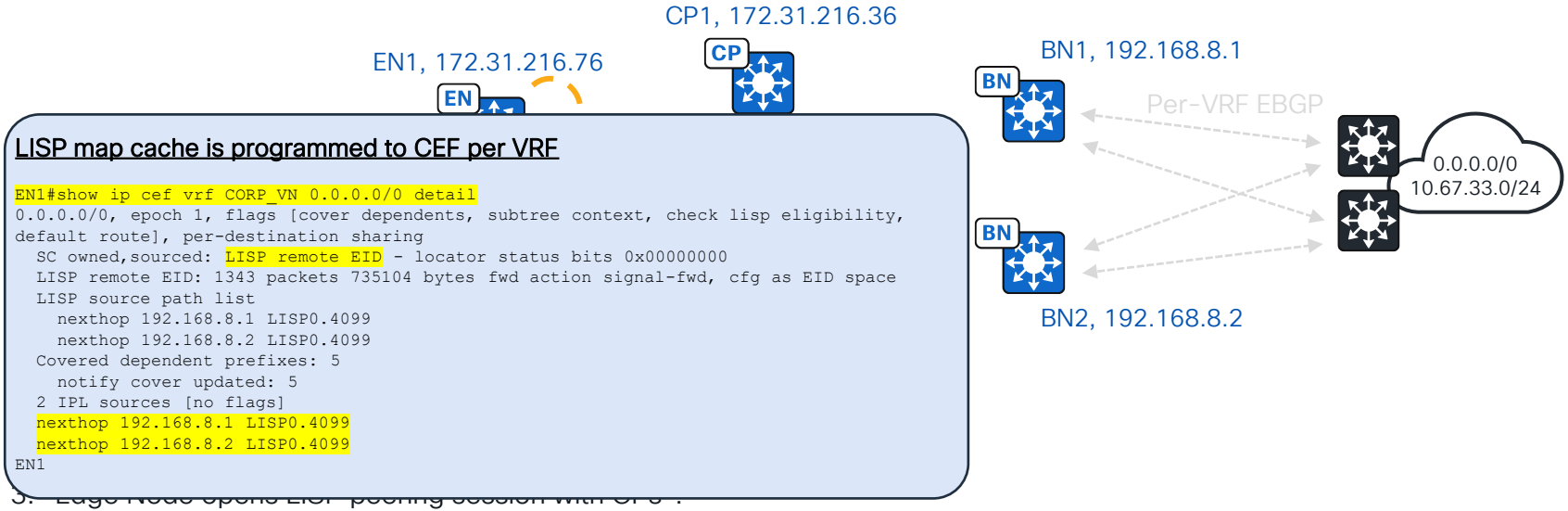
Timeline:

1. Default ETRs and specific routes are registered with CPs*.
2. Edge Node boots.
3. Edge Node opens LISP peering session with CPs*.
4. Edge Node automatically queries default ETR per IID. Response is received and map cache is programmed.
   Note: LISP map cache stores dynamically learned EID-to-RLOC mappings used for packet forwarding.
5. LISP map cache is programmed to CEF per VRF.
   Note: CEF (Cisco Express Forwarding) is a Layer 3 IP-switching technology that optimizes network performance and scalability.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Node bootstrapping

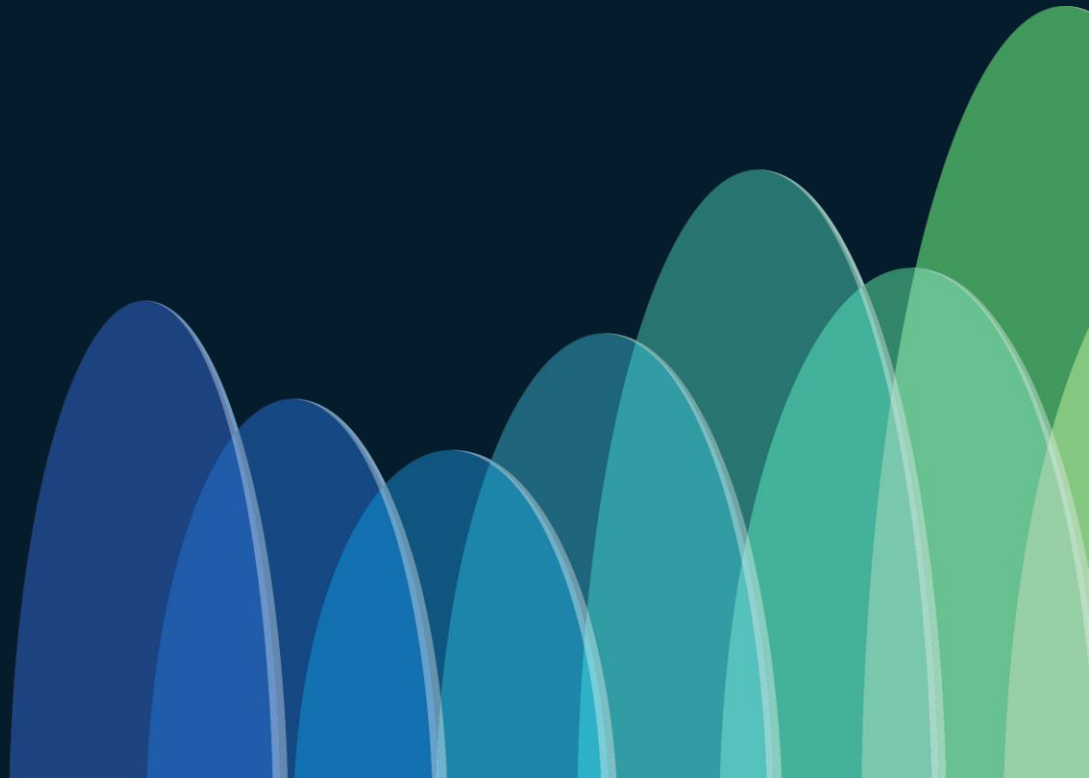


3. Edge Node opens LISP peering session with CP 1.
4. Edge Node automatically queries default ETR per IID. Response is received and map cache is programmed.
   Note: LISP map cache stores dynamically learned EID-to-RLOC mappings used for packet forwarding.
5. LISP map cache is programmed to CEF per VRF.
   Note: CEF (Cisco Express Forwarding) is a Layer 3 IP-switching technology that optimizes network performance and scalability.

*See previous section for animations and show commands

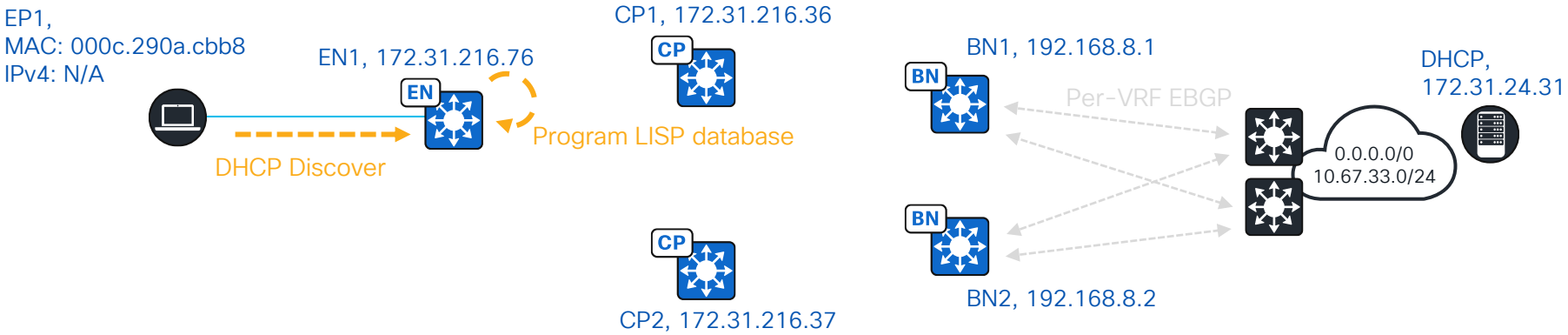
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired Endpoint Onboarding and Registration



cisco Live!

Wired endpoint onboarding and registration

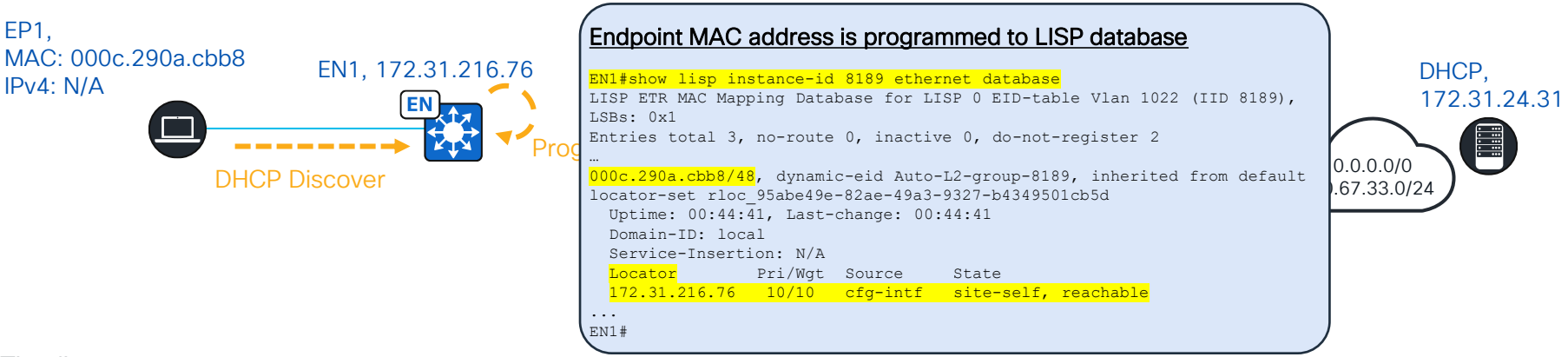


Timeline:

1. Wired endpoint connects into an access VLAN.
2. If the endpoint is configured for DHCP then a DHCP request is flooded into access VLAN.
3. Edge Node detects new MAC address and programs into associated LISP L2 IID database.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

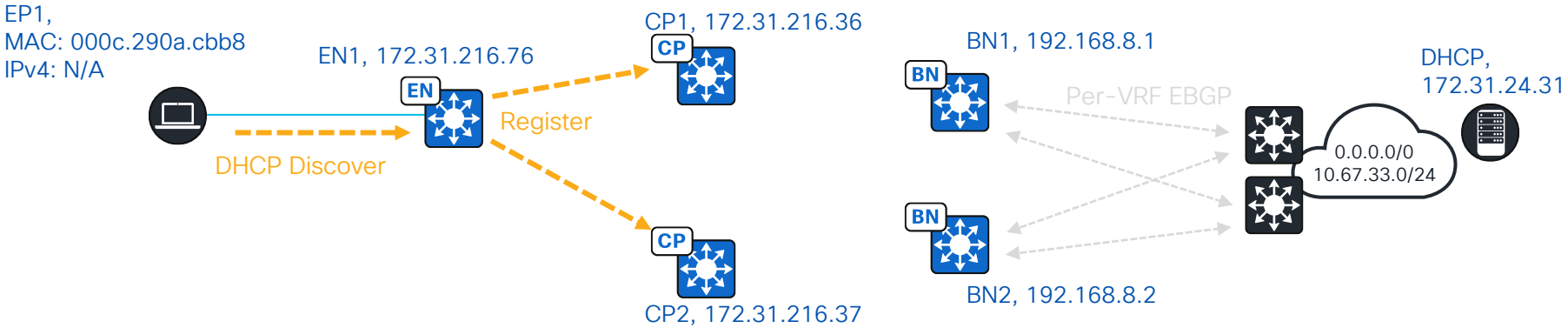


Timeline:

1. Wired endpoint connects into an access VLAN.
2. If the endpoint is configured for DHCP then a DHCP request is flooded into access VLAN.
3. Edge Node detects new MAC address and programs into associated LISP L2 IID database.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

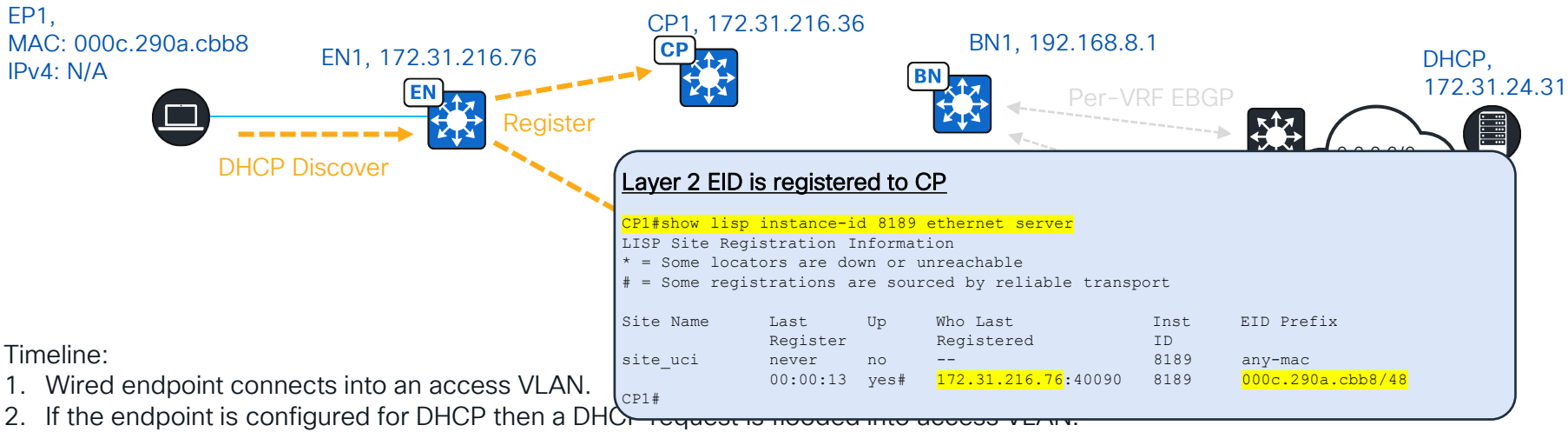


Timeline:

1. Wired endpoint connects into an access VLAN.
2. If the endpoint is configured for DHCP then a DHCP request is flooded into access VLAN.
3. Edge Node detects new MAC address and programs into associated LISP L2 IID database.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.
4. New LISP database entry triggers EID registration.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

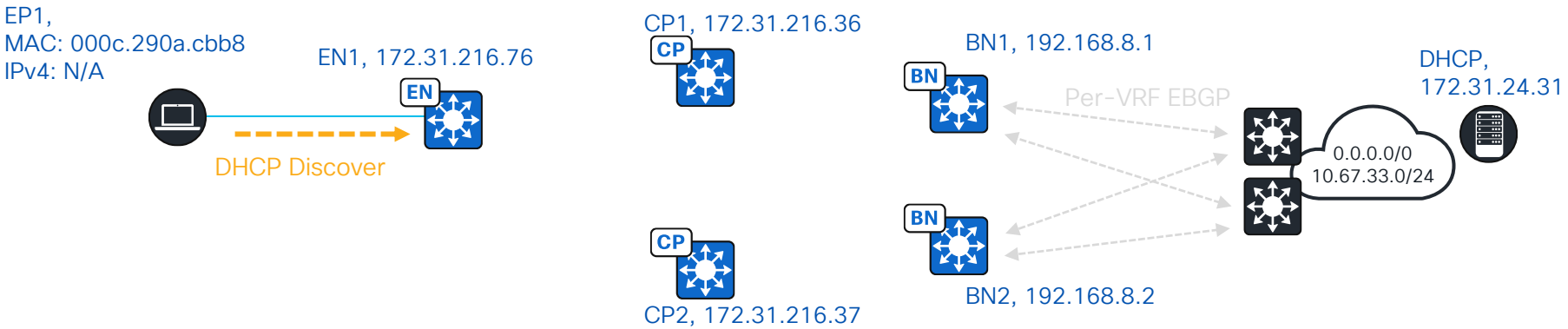


Timeline:

1. Wired endpoint connects into an access VLAN.
2. If the endpoint is configured for DHCP then a DHCP request is flooded into access VLAN.
3. Edge Node detects new MAC address and programs into associated LISP L2 IID database.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.
4. New LISP database entry triggers EID registration.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

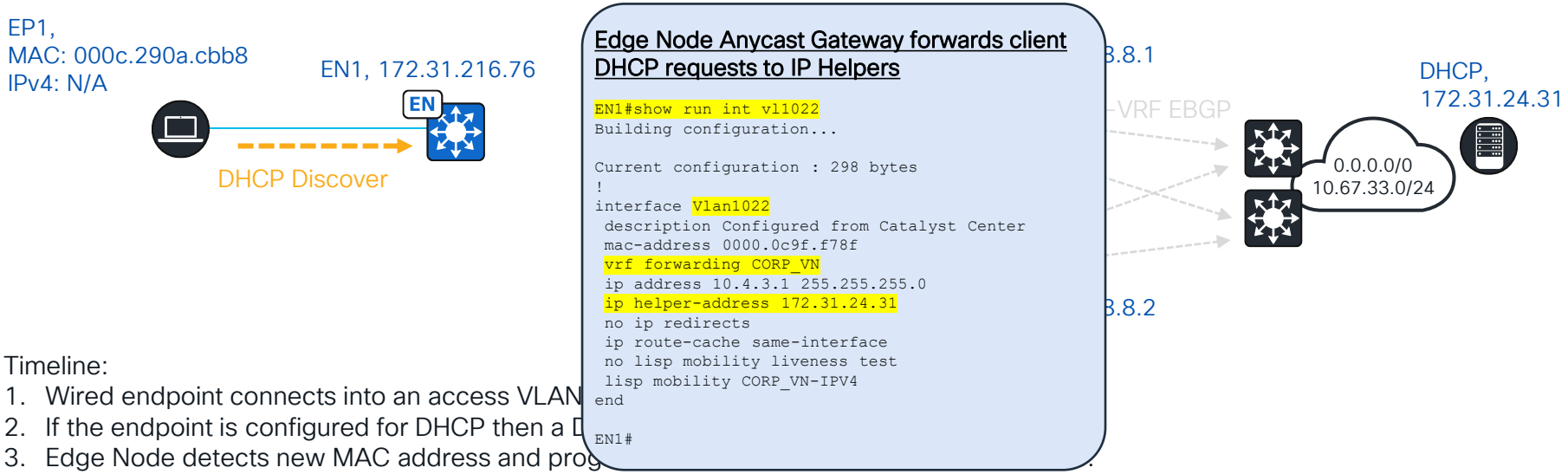


Timeline:

1. Wired endpoint connects into an access VLAN.
2. If the endpoint is configured for DHCP then a DHCP request is flooded into access VLAN.
3. Edge Node detects new MAC address and programs into associated LISP L2 IID database.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.
4. New LISP database entry triggers EID registration.
5. Edge Node SVI (Anycast Gateway) is configured to forward DHCP requests to IP Helpers.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

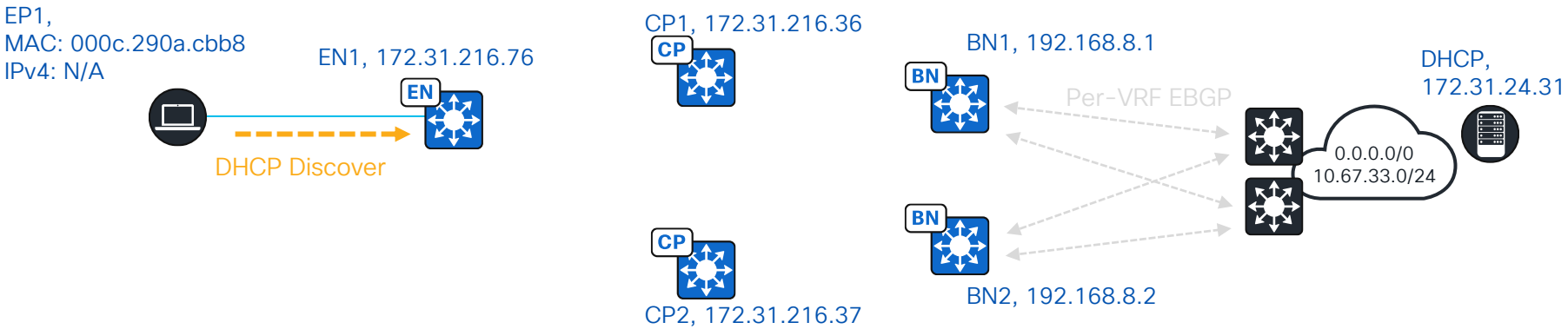


Timeline:

1. Wired endpoint connects into an access VLAN
2. If the endpoint is configured for DHCP then a D
3. Edge Node detects new MAC address and prog
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.
4. New LISP database entry triggers EID registration.
5. Edge Node SVI (Anycast Gateway) is configured to forward DHCP requests to IP Helpers.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

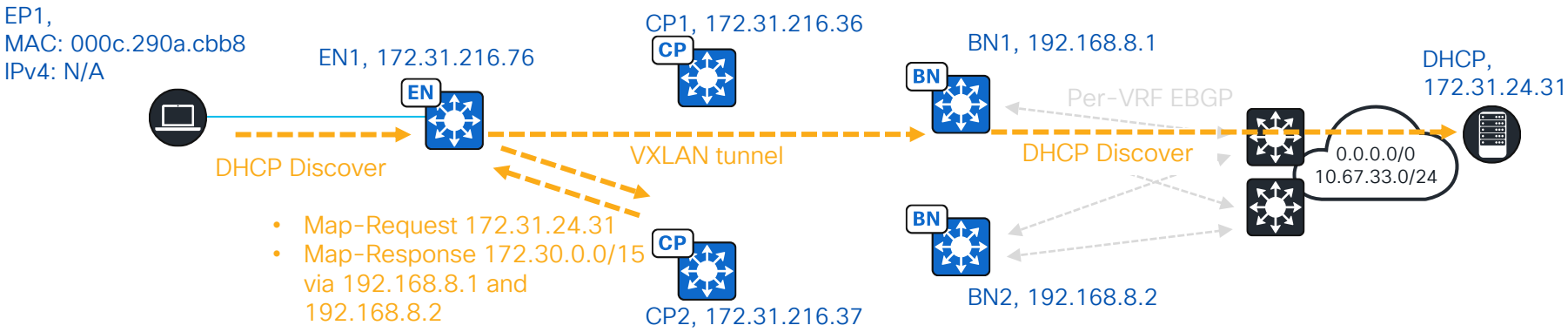


Timeline:

1. Wired endpoint connects into an access VLAN.
2. If the endpoint is configured for DHCP then a DHCP request is flooded into access VLAN.
3. Edge Node detects new MAC address and programs into associated LISP L2 IID database.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.
4. New LISP database entry triggers EID registration.
5. Edge Node SVI (Anycast Gateway) is configured to forward DHCP requests to IP Helpers.
6. Edge Node encodes its Loopback0 interface IP address into the DHCP request option 82 and sends towards the IP Helper address.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

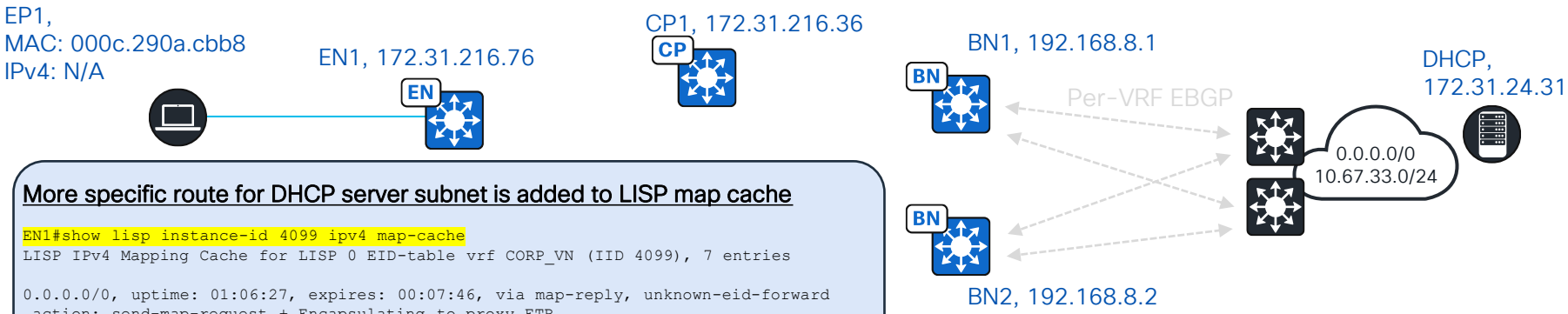


Timeline:

1. Wired endpoint connects into an access VLAN.
2. If the endpoint is configured for DHCP then a DHCP request is flooded into access VLAN.
3. Edge Node detects new MAC address and programs into associated LISP L2 IID database.
   Note: LISP database holds authoritative EID-to-RLOC mappings and is used for registrations.
4. New LISP database entry triggers EID registration.
5. Edge Node SVI (Anycast Gateway) is configured to forward DHCP requests to IP Helpers.
6. Edge Node encodes its Loopback0 interface IP address into the DHCP request option 82 and sends towards the IP Helper address.
7. Edge Node matches default ETR LISP map cache entry for IP Helper address and encapsulates in VXLAN towards default ETRs. In parallel Edge Node queries Control Plane for IP Helper address.
   Note: previously it was shown that default route map cache was programmed as “send-map-request + Encapsulating to proxy ETR”

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration



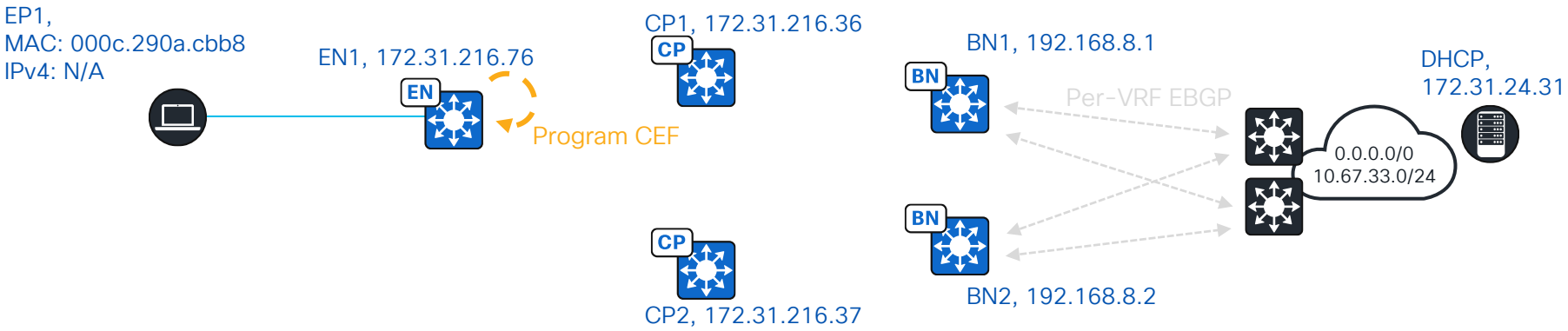
More specific route for DHCP server subnet is added to LISP map cache

```
EN1#show lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf CORP_VN (IID 4099), 7 entries

0.0.0.0/0, uptime: 01:06:27, expires: 00:07:46, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
   PETR          Uptime    State      Pri/Wgt     Encap-IID  Metric
   192.168.8.1   01:06:27  up         10/10       -          0
   192.168.8.2   01:06:27  up         10/10       -          0
172.30.0.0/15, uptime: 00:16:34, expires: 00:13:13, via map-reply, unknown-eid-forward
   PETR          Uptime    State      Pri/Wgt     Encap-IID  Metric
   192.168.8.1   00:00:34  up         10/10       -          0
   192.168.8.2   00:00:34  up         10/10       -          0
EN1#
```

T
1
2 to access VLAN.
3 P L2 IID database.
ions.
4. New LISP database entry triggers EID registration.
5. Edge Node SVI (Anycast Gateway) is configured to forward DHCP requests to IP Helpers.
6. Edge Node encodes its Loopback0 interface IP address into the DHCP request option 82 and sends towards the IP Helper address.
7. Edge Node matches default ETR LISP map cache entry for IP Helper address and encapsulates in VXLAN towards default ETRs. In parallel Edge Node queries Control Plane for IP Helper address.
   Note: previously it was shown that default route map cache was programmed as “send-map-request + Encapsulating to proxy ETR”

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration



Timeline:

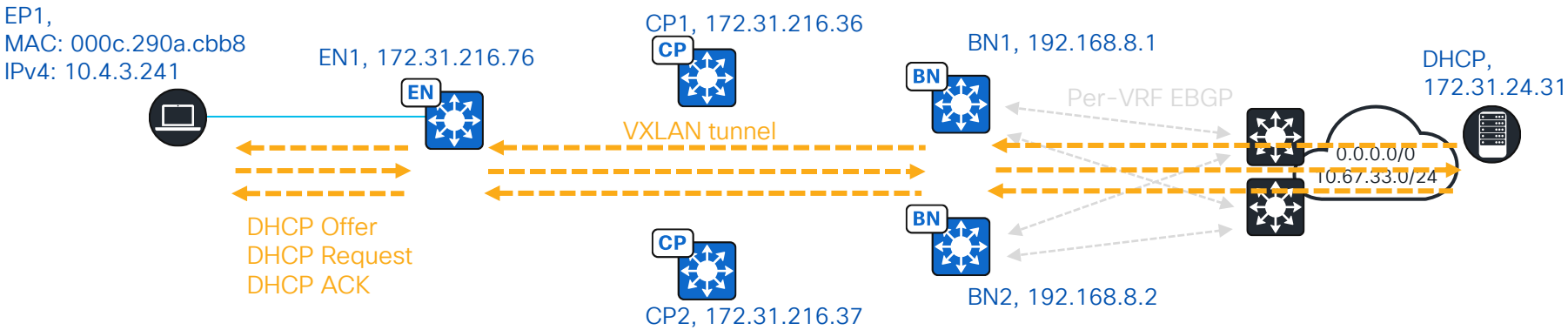
8. DHCP server LISP map cache entry is programmed into Edge Node CEF.

LISP map cache is programmed to CEF

```
EN1#show ip cef vrf CORP_VN 172.31.24.31 detail
172.30.0.0/15, epoch 1, flags [subtree context, check lisp eligibility], per-
destination sharing
  SC owned,sourced: LISP remote EID - locator status bits 0x00000000
  LISP remote EID: 5 packets 2622 bytes fwd action encap
  LISP source path list
    nexthop 192.168.8.1 LISP0.4099
    nexthop 192.168.8.2 LISP0.4099
  2 IPL sources [no flags]
  nexthop 192.168.8.1 LISP0.4099
  nexthop 192.168.8.2 LISP0.4099
EN1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

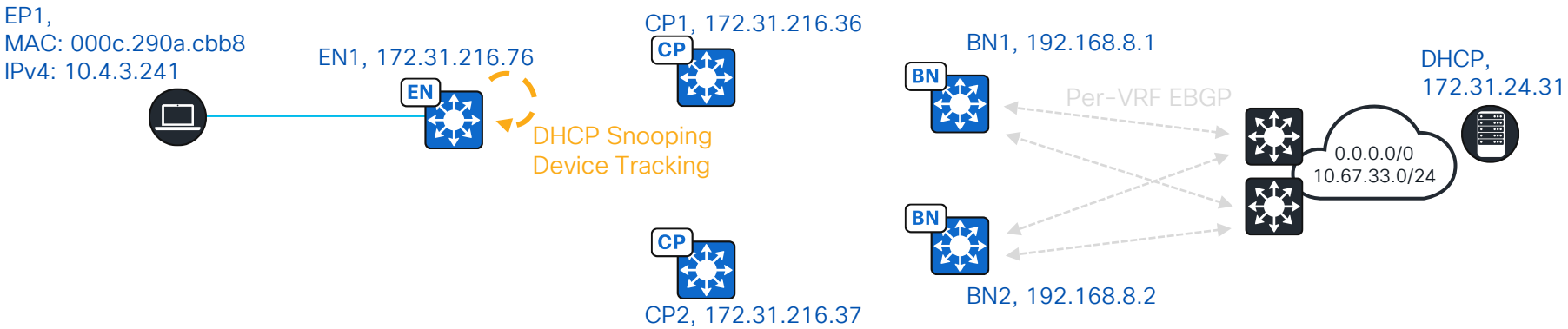


Timeline:

8. DHCP server LISP map cache entry is programmed into Edge Node CEF.
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration



Timeline:

8. DHCP server LISP map cache entry is programmed into Edge Node CEF.
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

EP1,
MAC: 000c.290a.cbb8
IPv4: 10.4.3.241

EN1

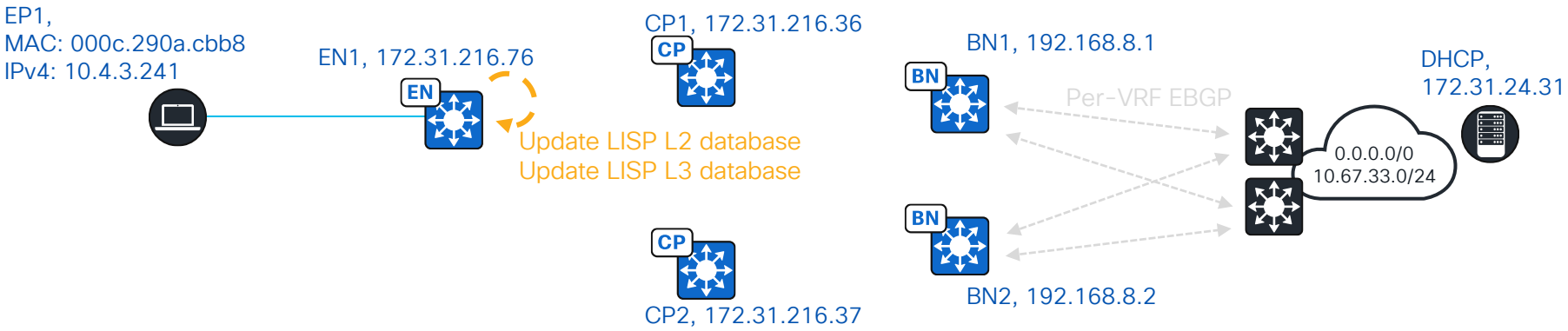
Timeline:
8. DHCP server LISP map cac
9. DHCP server makes an offe
completes with request and AC
10. Edge Node DHCP Snoopin
11. Edge Node Device Trackin

Endpoint details are entered into DHCP snooping table and Device Tracking database

```
EN1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:0C:29:0A:CB:B8   10.4.3.241       3511        dhcp-snooping   1022  GigabitEthernet1/0/24
Total number of bindings: 1

EN1#
EN1#
EN1#show device-tracking database
Binding Table has 6 entries, 3 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6
DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
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        state
Time left
DH4 10.4.3.241                               000c.290a.cbb8         Gi1/0/24   1022       0024       53s
REACHABLE  189 s try 0(3479 s)

EN1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

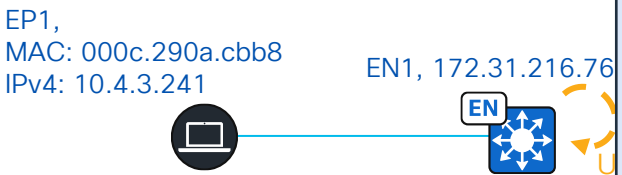


Timeline:

8. DHCP server LISP map cache entry is programmed into Edge Node CEF.
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration



Endpoint L3 details are programmed into LISP databases

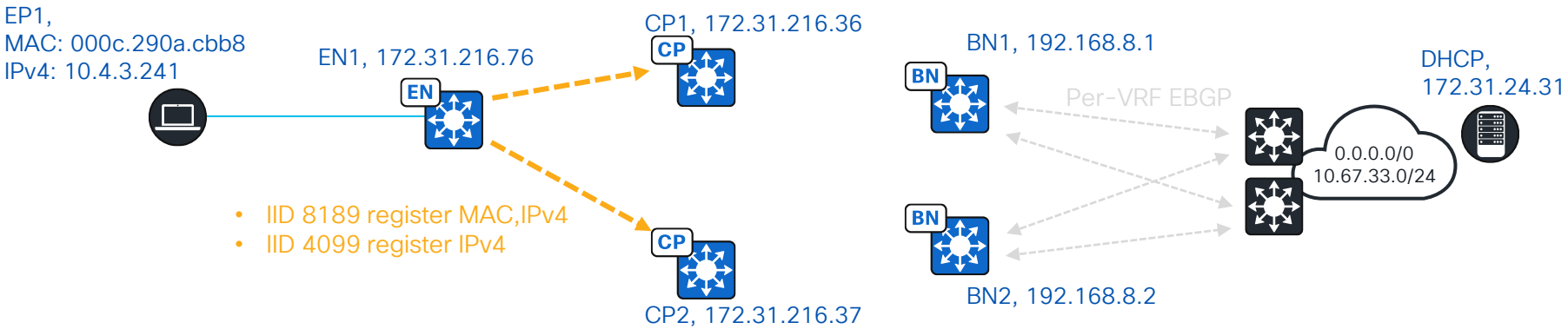
```
EN1#show lisp instance-id 8189 ethernet database address-resolution
LISP ETR Address Resolution for LISP 0 EID-table Vlan 1022 (IID 8189)
(*) -> entry being deleted

Hardware Address       L3 InstID Host Address
000c.290a.cbb8              4099 10.4.3.241/32
                            4099 FE80::75DD:E4E8:BFAF:E078/128
                            4099 2001:420:504A:2001::100/128
EN1#
EN1#show lisp instance-id 4099 ipv4 database
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf CORP_VN (IID 4099), LSBs: 0x1
Entries total 2, no-route 0, inactive 0, do-not-register 1
...
10.4.3.241/32, dynamic-eid CORP_VN-IPV4, inherited from default locator-set rloc_95abe49e-82ae-
49a3-9327-b4349501cb5d
  Uptime: 01:27:33, Last-change: 01:27:33
  Domain-ID: local
  Service-Insertion: N/A
  Locator         Pri/Wgt  Source     State
  172.31.216.76    10/10   cfg-intf   site-self, reachable
EN1
```

Timeline:

8. DHCP server LISP map cache entry is prog
9. DHCP server makes an offer, DHCP respons
completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

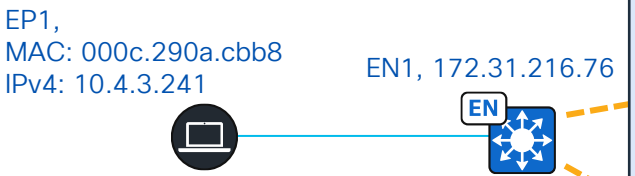


Timeline:

8. DHCP server LISP map cache entry is programmed into Edge Node CEF.
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.
13. Updates to LISP databases trigger LISP registrations.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration



- IID 8189 register MAC,IP
- IID 4099 register IPv4

Endpoint MAC-to-IP and IP addresses are registered to LISP CP

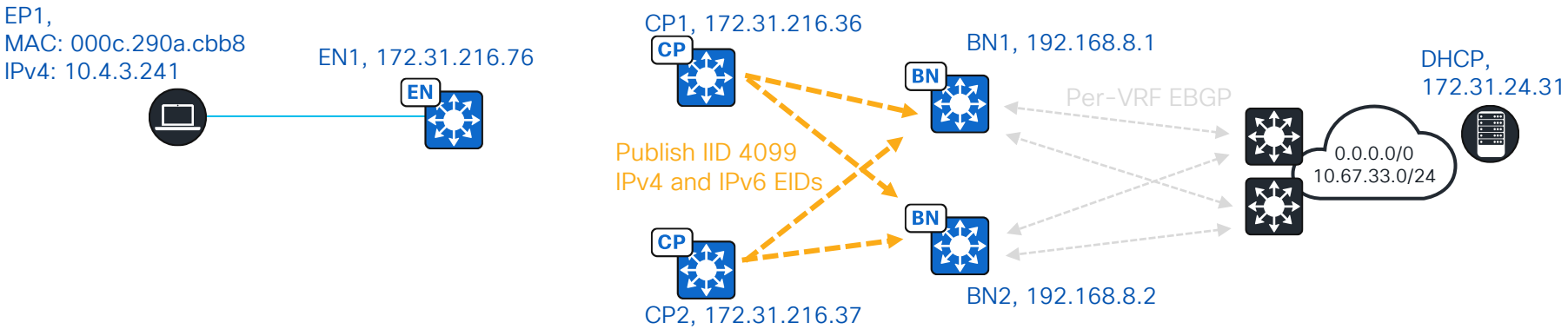
```
CP1#show lisp instance-id 8189 ethernet server address-resolution

Address-resolution data for router lisp 0 instance-id 8189

L3 InstID     Host Address                                Hardware Address
     4099     10.4.3.241/32                               000c.290a.cbb8
     4099     2001:420:504A:2001::100/128                 000c.290a.cbb8
     4099     FE80::75DD:E4E8:BFAF:E078/128               000c.290a.cbb8
CP1#
CP1#
CP1#show lisp instance-id 4099 ipv4 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     --                    4099     0.0.0.0/0
               never     no     --                    4099     10.4.3.0/24
               01:37:31  yes#   172.31.216.76:46300   4099     10.4.3.241/32
               5w3d      yes#   192.168.8.1:28219     4099     10.67.33.0/24
               5w3d      yes#   192.168.8.1:28219     4099     172.29.4.48/29
CP1#
```

Timeline:

8. DHCP server LISP map cache entry is progr
9. DHCP server makes an offer, DHCP respons
completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.
13. Updates to LISP databases trigger LISP registrations.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

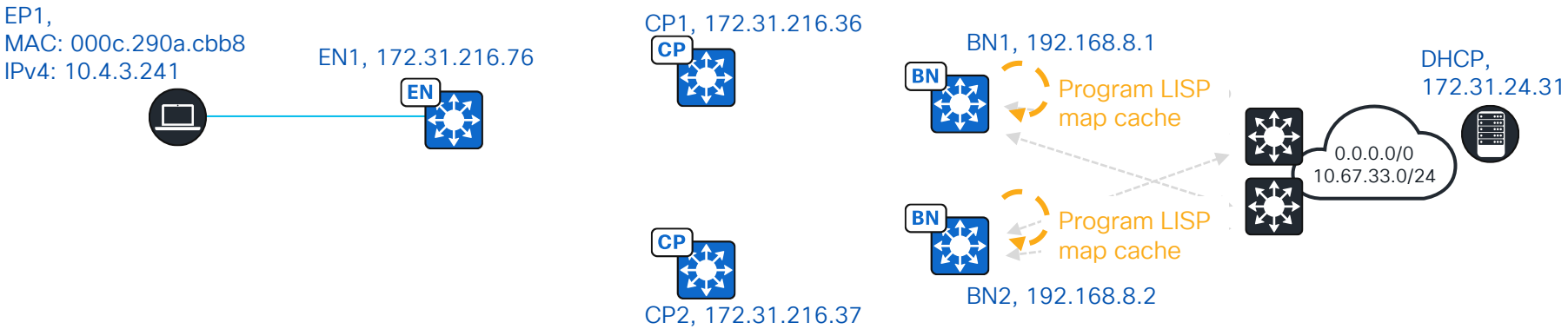


Timeline:

8. DHCP server LISP map cache entry is programmed into Edge Node CEF.
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.
13. Updates to LISP databases trigger LISP registrations.
14. LISP L3 IID registrations are published to all Border Nodes.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

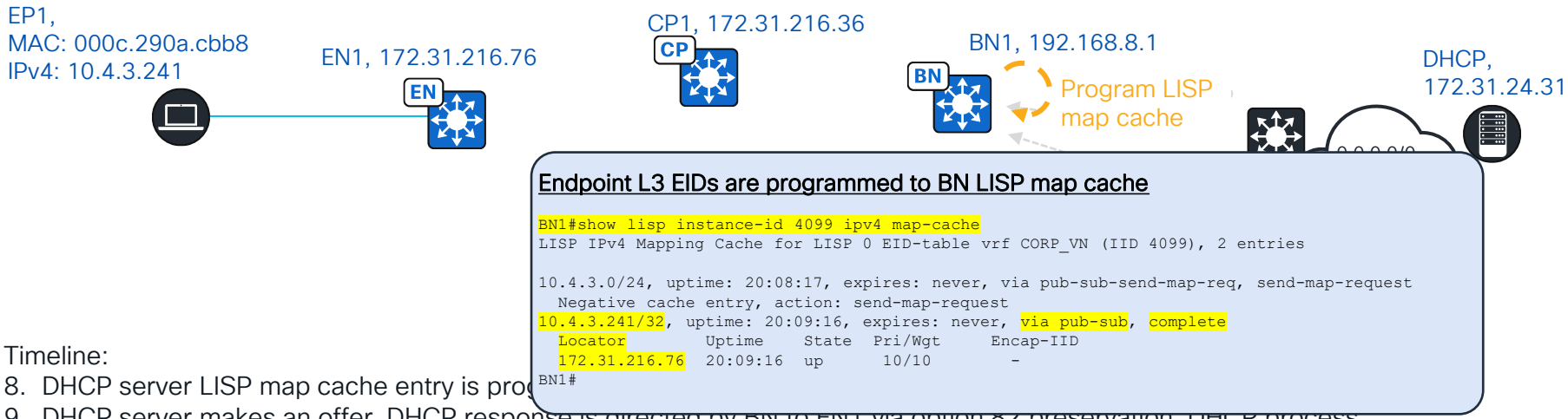


Timeline:

8. DHCP server LISP map cache entry is programmed into Edge Node CEF.
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.
13. Updates to LISP databases trigger LISP registrations.
14. LISP L3 IID registrations are published to all Border Nodes.
15. LISP publications are programmed to map cache.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

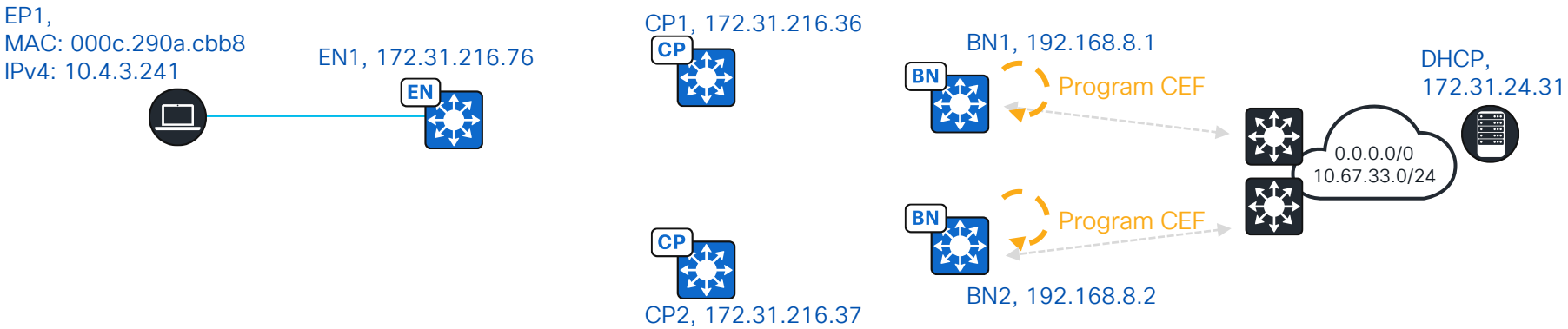


Timeline:

8. DHCP server LISP map cache entry is prog
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.
13. Updates to LISP databases trigger LISP registrations.
14. LISP L3 IID registrations are published to all Border Nodes.
15. LISP publications are programmed to map cache.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration

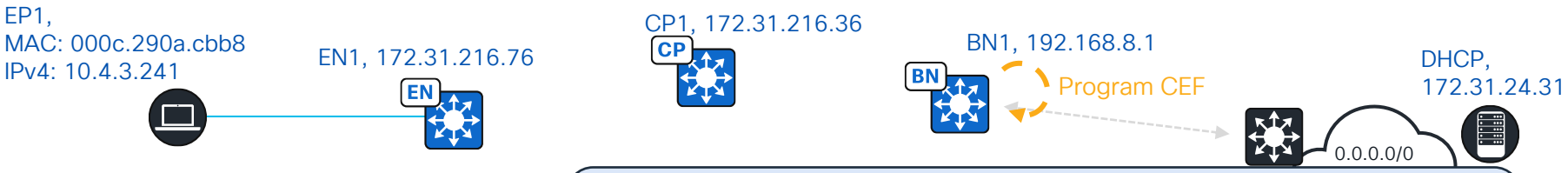


Timeline:

8. DHCP server LISP map cache entry is programmed into Edge Node CEF.
9. DHCP server makes an offer, DHCP response is directed by BN to EN1 via option 82 preservation. DHCP process completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.
13. Updates to LISP databases trigger LISP registrations.
14. LISP L3 IID registrations are published to all Border Nodes.
15. LISP publications are programmed to map cache.
16. LISP map cache is programmed to CEF.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired endpoint onboarding and registration



LISP map cache is programmed CEF

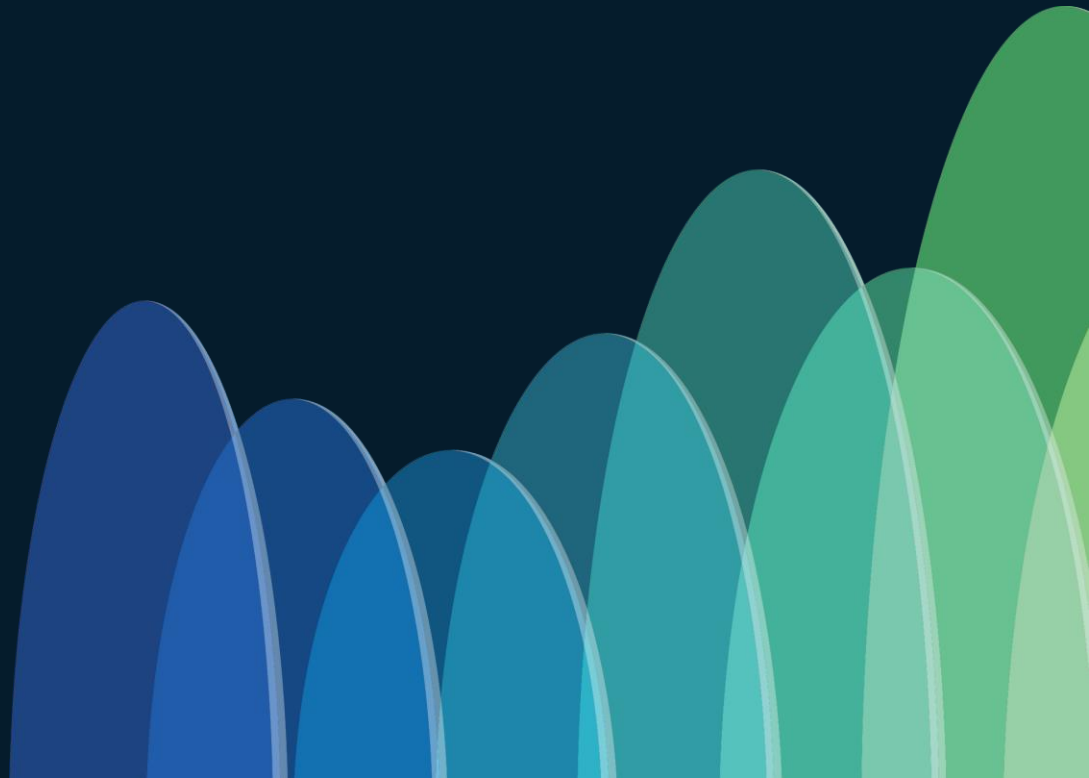
```
BN1#show ip cef vrf CORP_VN 10.4.3.241 detail
10.4.3.241/32, epoch 0, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 2 packets 1152 bytes fwd action encap, cfg as EID space
  SC inherited: LISP generalised SMR - [disabled, inheriting, 0x700CA7FA04F0 locks: 12]
  LISP source path list
    nexthop 172.31.216.76 LISP0.4099
  2 IPL sources [no flags]
  nexthop 172.31.216.76 LISP0.4099
BN1#
```

Timeline:

8. DHCP server LISP map cache entry is progra
9. DHCP server makes an offer, DHCP response
completes with request and ACK.
10. Edge Node DHCP Snooping table is populated with endpoint MAC address and IP address.
11. Edge Node Device Tracking database is populated with endpoint MAC address and IP address.
12. Device Tracking updates LISP L2 and L3 databases with endpoint IP details.
13. Updates to LISP databases trigger LISP registrations.
14. LISP L3 IID registrations are published to all Border Nodes.
15. LISP publications are programmed to map cache.
16. LISP map cache is programmed to CEF.

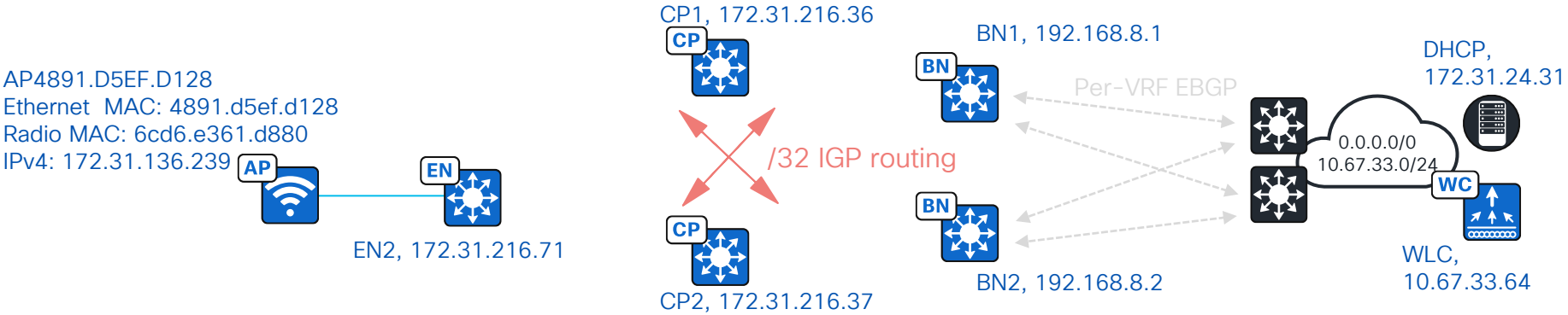
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP Onboarding and Registration



cisco Live!

Fabric AP onboarding and registration

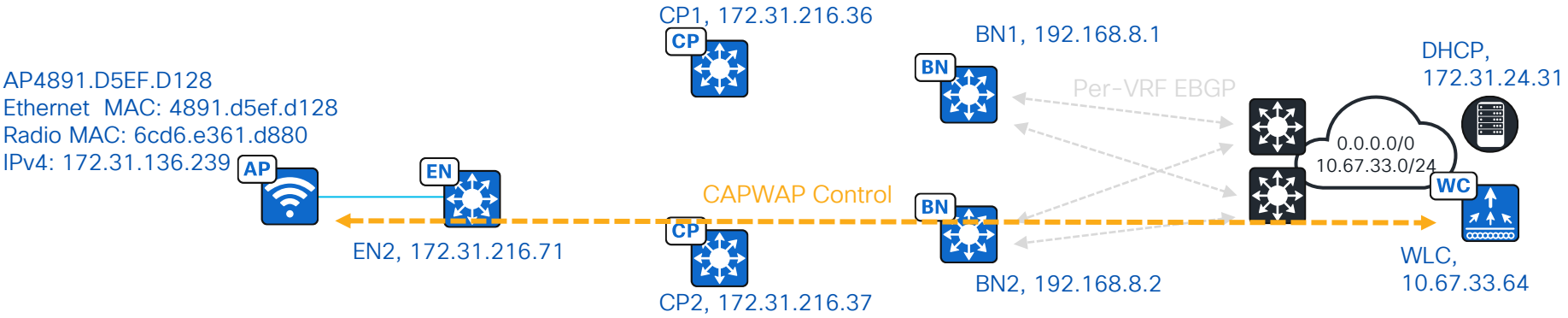


Timeline:

1. As explained in Wired Endpoint Onboarding and Registration section:
    a. AP (Endpoint) connects to INFRA_VN.
    b. Edge Node detects new MAC address and programs into associated LISP L2 database. New LISP database entry triggers EID registration.
    c. AP sends DHCP Discover. Edge Node SVI (Anycast Gateway) is configured to forward DHCP Discover to IP Helpers. Edge Node encodes its Loopback0 interface IP address into the DHCP request option 82 and sends towards the IP Helper address.
    Note INFRA_VN uses RIB for endpoint (AP, Extended Node) to external network routing and LISP for the return traffic.
    d. DHCP server makes an offer, DHCP response is directed by BN to EN2 via option 82 preservation. DHCP process completes with request and ACK. The AP (endpoint) obtains an IP address. DHCP Snooping and Device Tracking are updated.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration

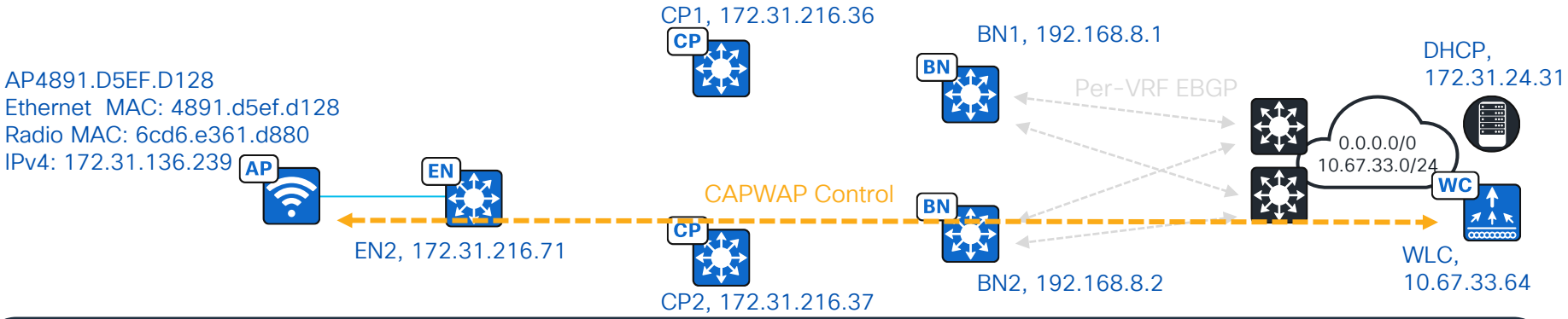


Timeline:

2. AP Discovery Phase executes and CAPWAP control tunnel established between Fabric AP and Fabric WLC.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration

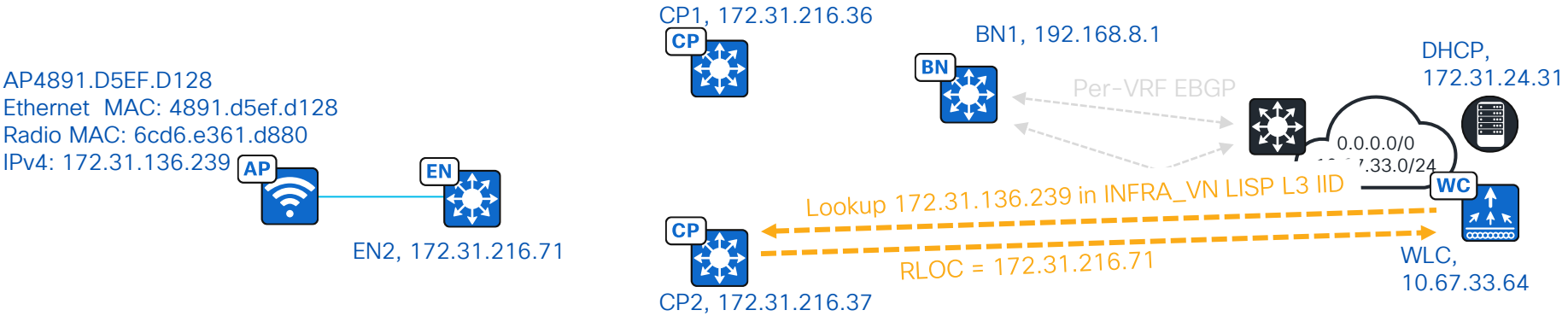


CAPWAP control tunnel is established

```
WLC#show ap summary
Number of APs: 1

CC = Country Code
RD = Regulatory Domain

AP Name                          Slots AP Model             Ethernet MAC    Radio MAC      CC   RD   IP Address                                  State
Location
-------------------------------------------------------------------------------------------------------------------------------------------------------------
------
AP4891.D5EF.D128                 4     C9136I-Z             4891.d5ef.d128  6cd6.e361.d880 AU   -Z   172.31.136.239                              Registered
default location

WLC#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration

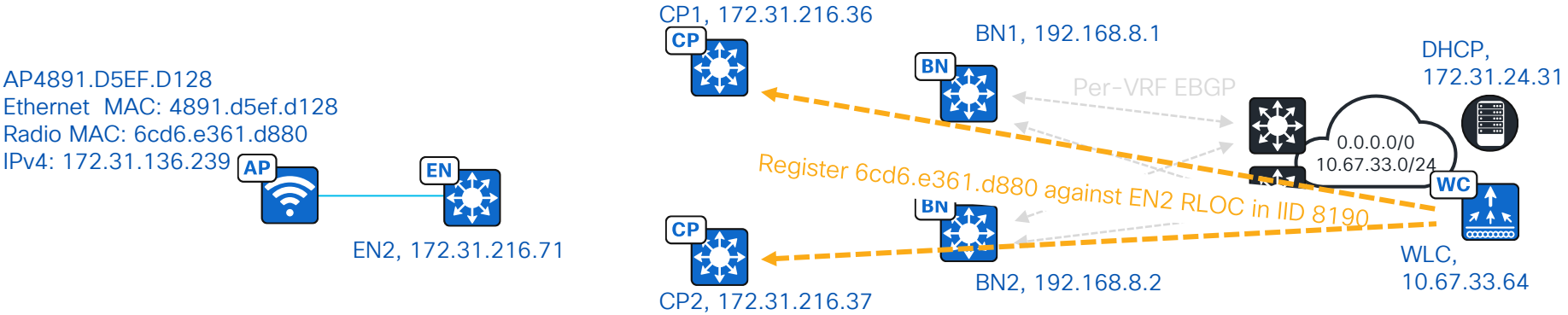


Timeline:

2. AP Discovery Phase executes and CAPWAP control tunnel established between Fabric AP and Fabric WLC.
3. WLC queries CP for EN RLOC associated with Fabric AP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration

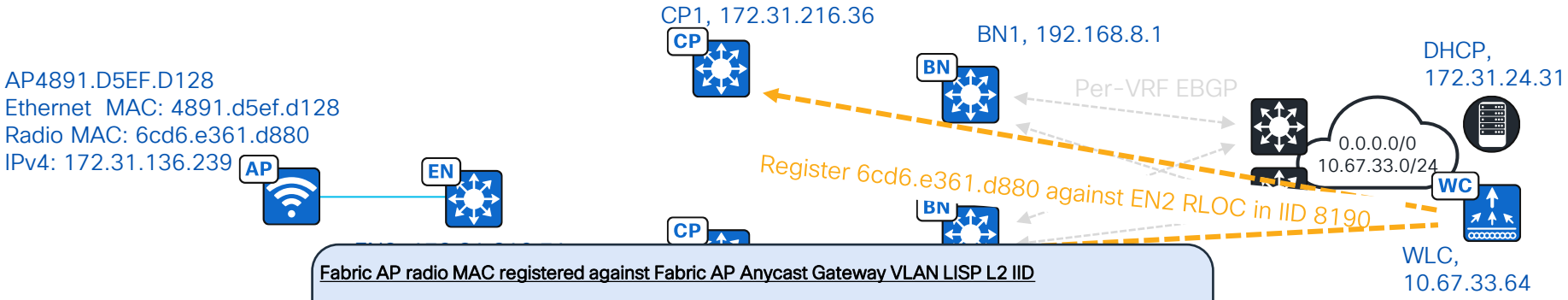


Timeline:

2. AP Discovery Phase executes and CAPWAP control tunnel established between Fabric AP and Fabric WLC.
3. WLC queries CP for EN RLOC associated with Fabric AP.
4. WLC registers radio MAC with EN RLOC in INFRA_VN LISP L2 IID.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration



Timeline:

2. AP Discovery Phase e
3. WLC queries CP for E
4. WLC registers radio M

WLC.

Fabric AP radio MAC registered against Fabric AP Anycast Gateway VLAN LISP L2 IID

```
CP1#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
               00:00:05   yes#   172.31.216.71:44001   8190     4891.d5ef.d128/48
               00:00:05   yes#   10.67.33.64:55795     8190     6cd6.e361.d880/48
CP1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration

AP4891.D5EF.D128
Ethernet MAC: 4891.d5ef.d128
Radio MAC: 6cd6.e361.d880
IPv4: 172.31.136.239

EN2, 172.31.216.71

Timeline:
2. AP Discovery Phase executes and CAPWAP c
3. WLC queries CP for EN RLOC associated with
4. WLC registers radio MAC with EN RLOC in INF

Fabric AP radio MAC registered against Fabric AP Anycast Gateway LISP L2 IID

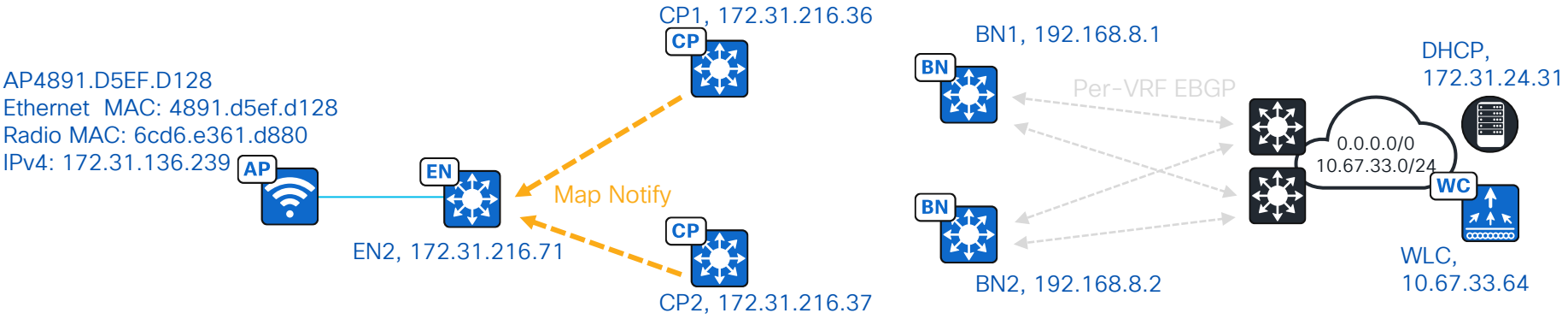
```
CP1#show lisp instance-id 8190 ethernet server 6cd6.e361.d880
LISP Site Registration Information

Site name: site_uci
Description: map-server configured from Catalyst Center
Allowed configured locators: any
Requested EID-prefix:

  EID-prefix: 6cd6.e361.d880/48 instance-id 8190
    ...
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 10.67.33.64:55795
      last registered 00:26:49, no proxy-reply, no map-notify
      TTL 1d00h, no merge, hash-function sha2
      state complete, no security-capability
      nonce 0x00000000-0x00000000
      xTR-ID N/A
      site-ID N/A
      sourced by reliable transport
      Affinity-id: 0 , 0
      WLC AP bit: Set
      Locator         Local  State      Pri/Wgt  Scope        RDP
      172.31.216.71   yes    up           0/0    IPv4 none    [-]
CP1#
```

,
1.24.31

3.64

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration

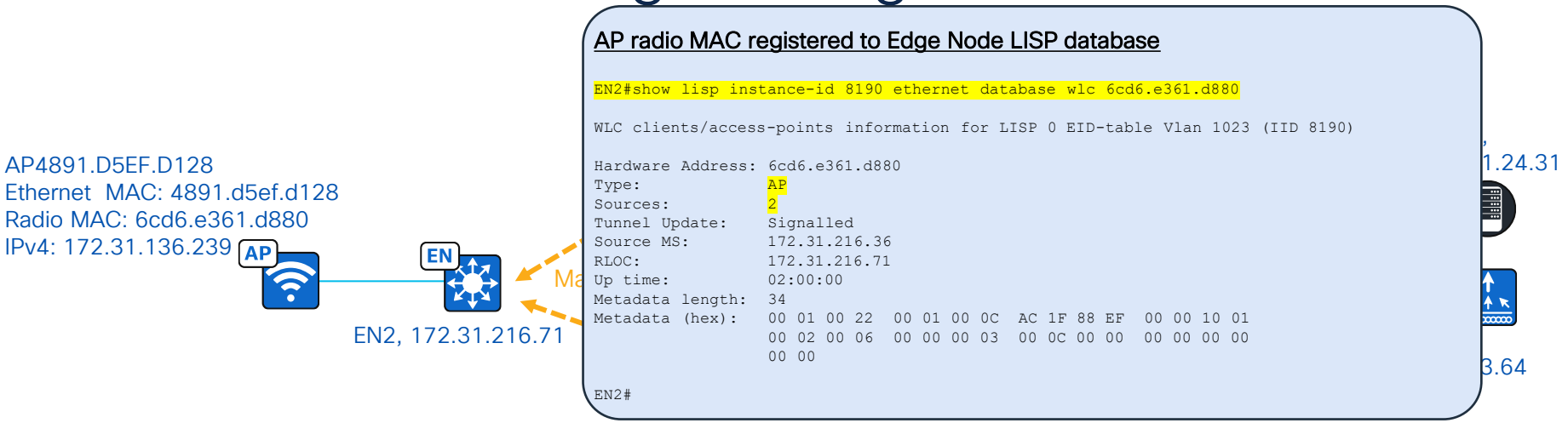


Timeline:

2. AP Discovery Phase executes and CAPWAP control tunnel established between Fabric AP and Fabric WLC.
3. WLC queries CP for EN RLOC associated with Fabric AP.
4. WLC registers radio MAC with EN RLOC in INFRA_VN LISP L2 IID.
5. CP sends Map Notify to EN instructing to build Access Tunnel (VXLAN tunnel) between Edge and AP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration



AP radio MAC registered to Edge Node LISP database

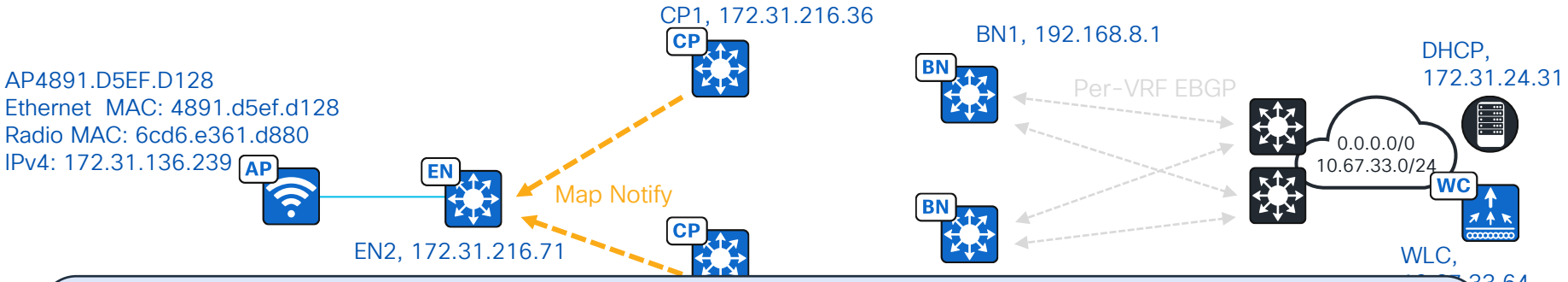
```
EN2#show lisp instance-id 8190 ethernet database wlc 6cd6.e361.d880

WLC clients/access-points information for LISP 0 EID-table Vlan 1023 (IID 8190)

Hardware Address: 6cd6.e361.d880
Type:             AP
Sources:          2
Tunnel Update:    Signalled
Source MS:        172.31.216.36
RLOC:             172.31.216.71
Up time:          02:00:00
Metadata length:  34
Metadata (hex):   00 01 00 22  00 01 00 0C  AC 1F 88 EF  00 00 10 01
                  00 02 00 06  00 00 00 03  00 0C 00 00  00 00 00 00
                  00 00

EN2#
```

Timeline:

2. AP Discovery Phase executes and CAPWAP control tunnel established between Fabric AP and Fabric WLC.
3. WLC queries CP for EN RLOC associated with Fabric AP.
4. WLC registers radio MAC with EN RLOC in INFRA_VN LISP L2 IID.
5. CP sends Map Notify to EN instructing to build Access Tunnel (VXLAN tunnel) between Edge and AP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric AP onboarding and registration

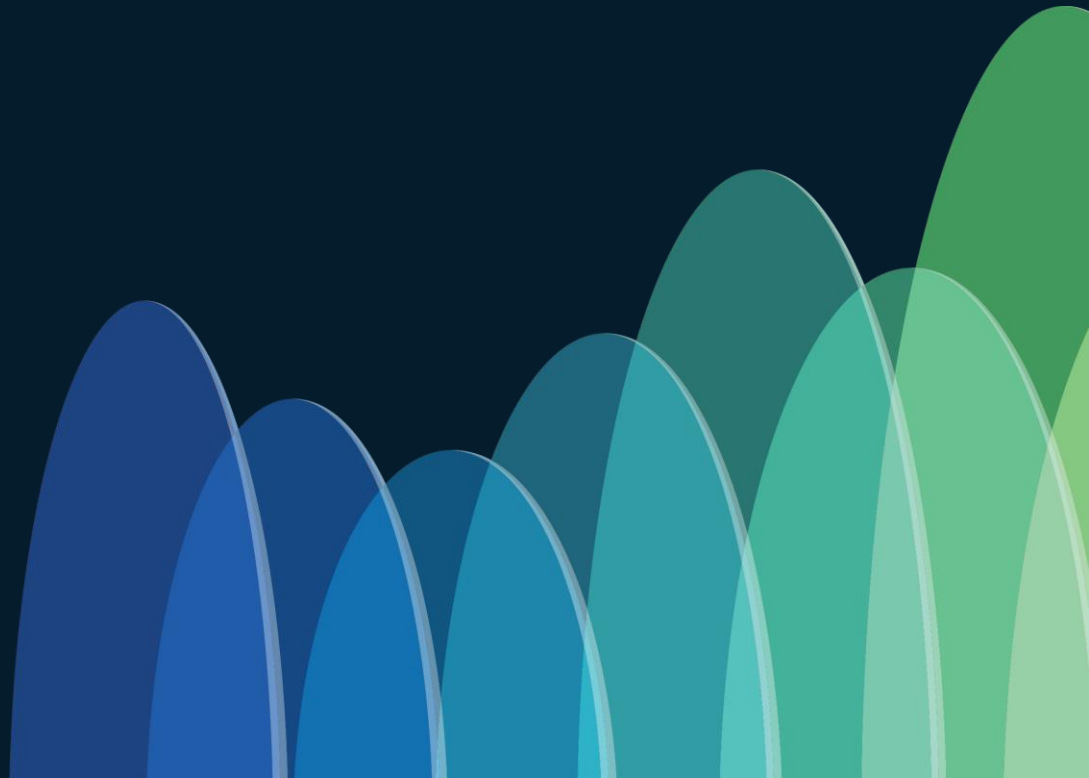


Access Tunnel (VXLAN tunnel) between Edge Node and AP is established

```
EN2#show access-tunnel summary

Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 1

Name    RLOC IP(Source)                                 AP IP(Destination)                              VRF ID  Source Port  Destination Port
------  ----------------------------------------------  ----------------------------------------------  ------  -----------  ----------------
Ac1     172.31.216.71                                   172.31.136.239                                  0       N/A          4789


Name   IfId           Uptime
------ ---------- --------------------
Ac1    0x00000070    0 day,  02:02:19

EN2#
```

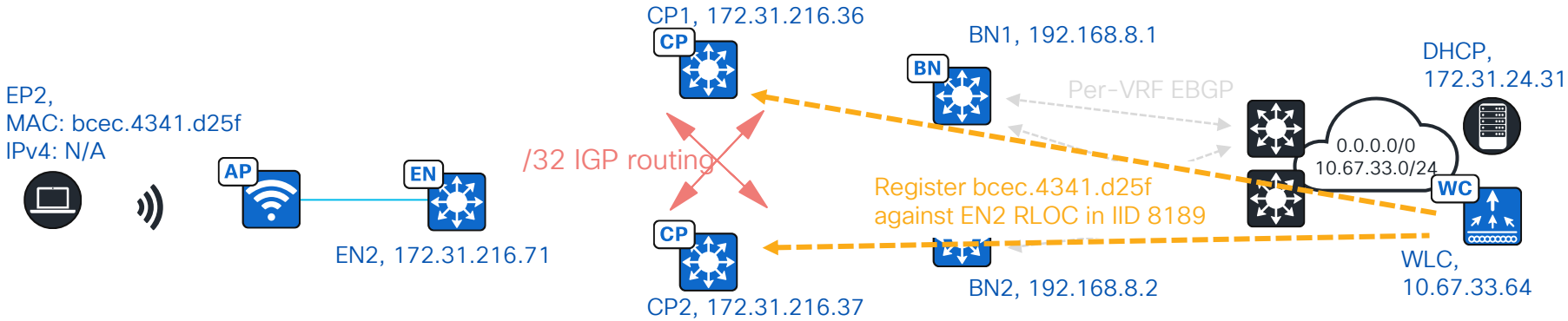

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless Endpoint Onboarding and Registration



cisco Live!

Wireless endpoint onboarding

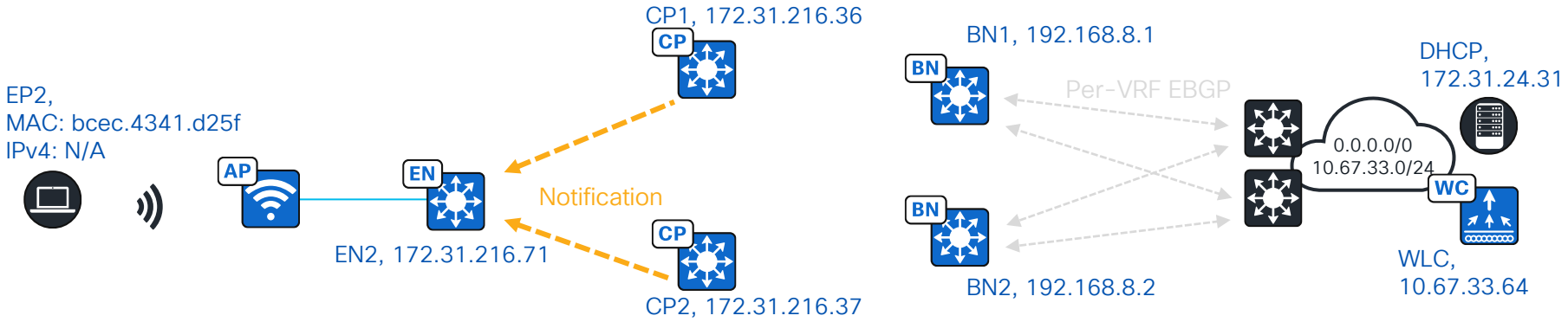


Timeline:

1. Wireless endpoint authenticates to a Fabric SSID.
2. Fabric WLC registers wireless endpoint MAC against EN RLOC in LISP L2 IID.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding



Timeline:

1. Wireless endpoint authenticates to a Fabric SSID.
2. Fabric WLC registers wireless endpoint MAC against EN RLOC in LISP L2 IID.
3. CP notifies Edge Node of endpoint MAC. L2 LISP database entry created, MAC address table populated and Device Tracking L2 entry created.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding

EP2,
MAC: bcec.4341.d25f
IPv4: N/A

P,
31.24.31

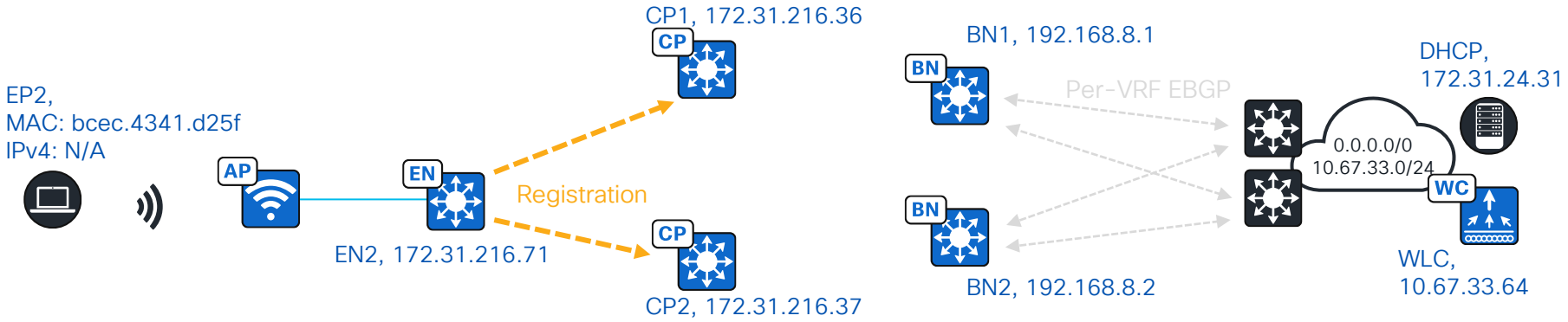
Timeline:
1. Wireless endpoint authenticates to a Fabric
2. Fabric WLC registers wireless endpoint MA
3. CP notifies Edge Node of endpoint MAC. L2 Tracking L2 entry created.

Edge Node MAC address table and LISP database populated with wireless endpoint L2 EID.

```
EN2#show mac address-table vlan 1022
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
...
1022    bcec.4341.d25f    CP_LEARN    Ac1

Total Mac Addresses for this criterion: 3
Total Mac Addresses installed by LISP: REMOTE: 0
EN2#
EN2#
EN2#show lisp instance-id 8189 ethernet database
LISP ETR MAC Mapping Database for LISP 0 EID-table Vlan 1022 (IID 8189), LSBs: 0x1
Entries total 3, no-route 0, inactive 0, do-not-register 2
...
bcec.4341.d25f/48, dynamic-eid Auto-L2-group-8189, inherited from default locator-set
rloc_00b55af7-fbfe-481a-91fe-e8fd56ae3dc0
  Uptime: 00:15:02, Last-change: 00:15:02
  Domain-ID: local
  Service-Insertion: N/A
  Locator         Pri/Wgt  Source     State
  172.31.216.71    10/10   cfg-intf   site-self, reachable
EN2#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding

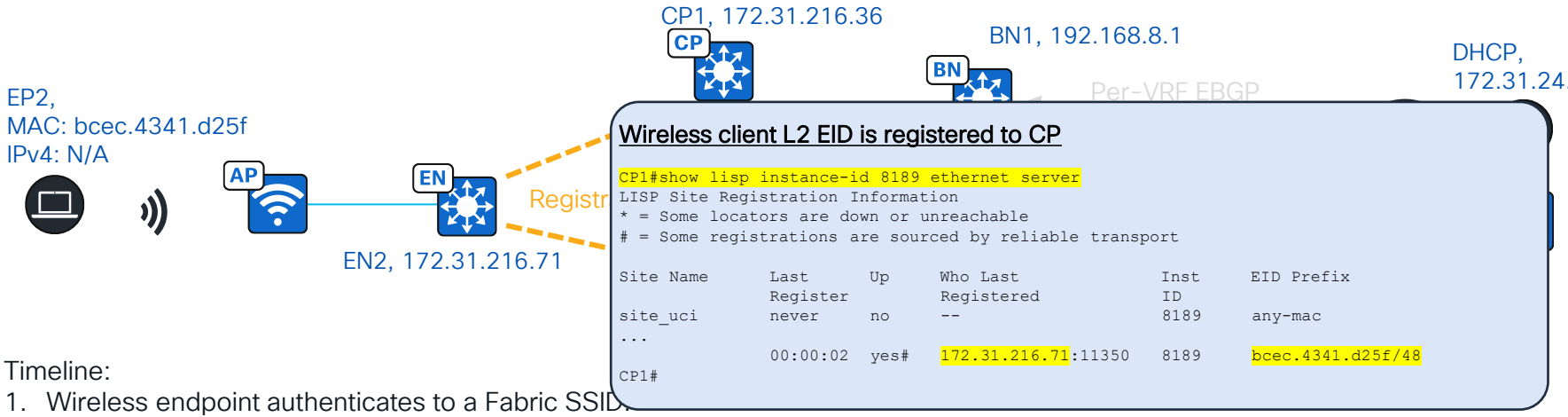


Timeline:

1. Wireless endpoint authenticates to a Fabric SSID.
2. Fabric WLC registers wireless endpoint MAC against EN RLOC in LISP L2 IID.
3. CP notifies Edge Node of endpoint MAC. L2 LISP database entry created, MAC address table populated and Device Tracking L2 entry created.
4. Edge Node registers endpoint MAC address to CP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding

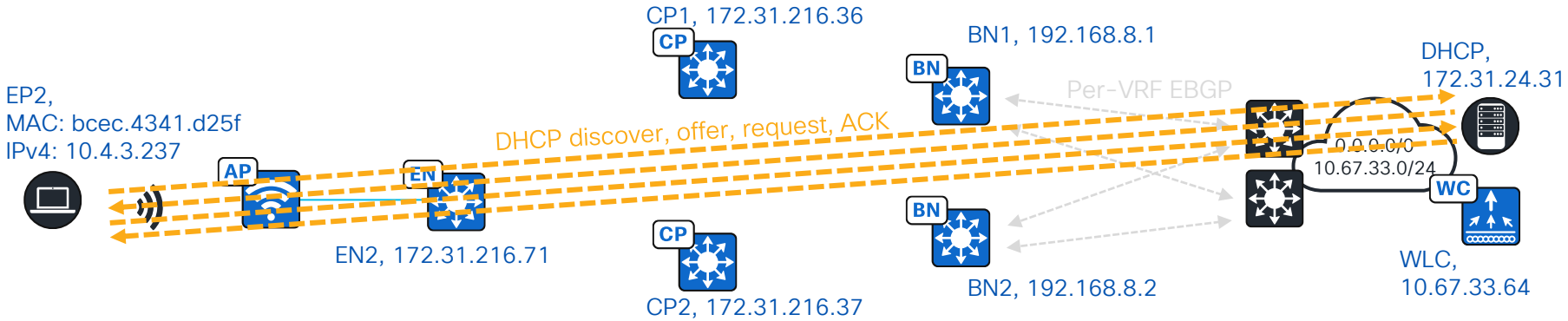


Timeline:

1. Wireless endpoint authenticates to a Fabric SSID.
2. Fabric WLC registers wireless endpoint MAC against EN RLOC in LISP L2 IID.
3. CP notifies Edge Node of endpoint MAC. L2 LISP database entry created, MAC address table populated and Device Tracking L2 entry created.
4. Edge Node registers endpoint MAC address to CP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding



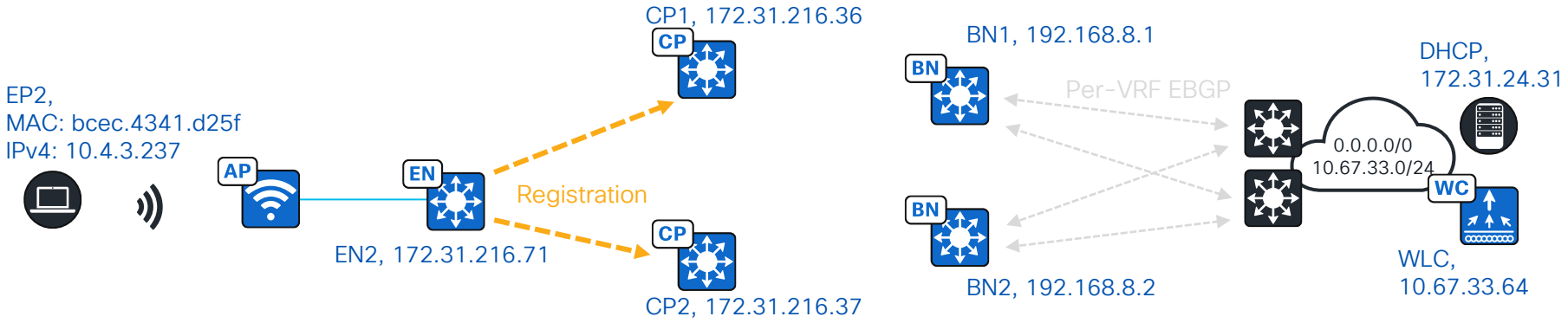
Timeline:

5. As explained in Wired Endpoint Onboarding and Registration section:
    a. Endpoint sends DHCP Discover. Edge Node SVI (Anycast Gateway) is configured to forward DHCP Discover to IP Helpers. Edge Node encodes its Loopback0 interface IP address into the DHCP request option 82 and sends towards the IP Helper address*.
    b. Edge Node matches default route map-cache entry for IP Helper address and encapsulates in VXLAN towards PETRs. In parallel Edge Node queries Control Plane for IP Helper address and the resulting more-specific LISP entry is programmed to map-cache and CEF*.
    c. DHCP transaction concludes, and the endpoint obtains an IP address. DHCP Snooping, Device Tracking and LISP Database are updated with endpoint details. Device Tracking updates LISP L2 and L3 databases with endpoint IP details*.

*See previous section for animations and show commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

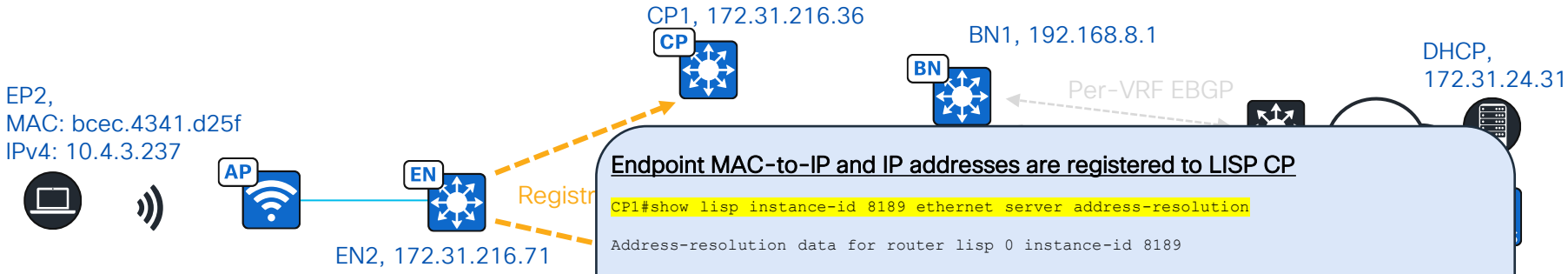
Wireless endpoint onboarding



Timeline:
6. Updates to LISP L2 and L3 databases trigger registrations.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding



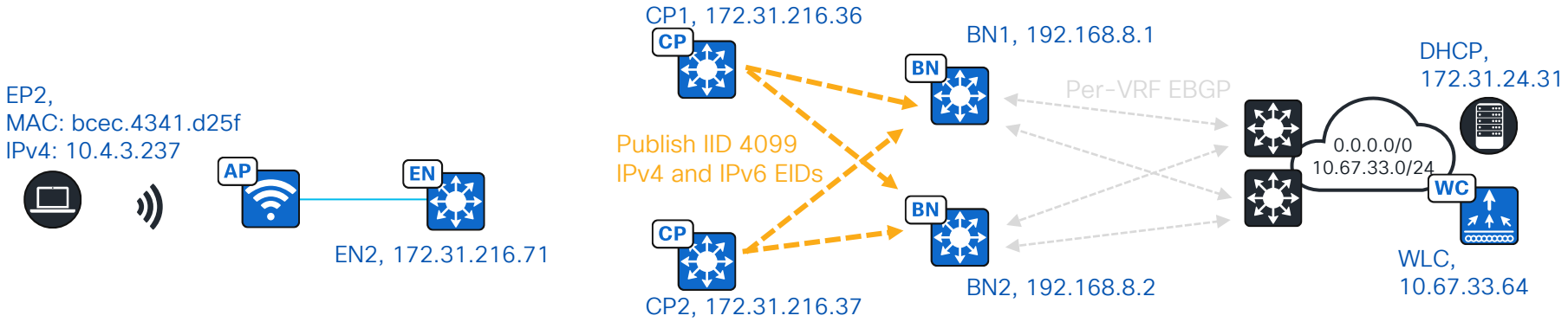
Timeline:
6. Updates to LISP L2 and L3 databases trigger reg

Endpoint MAC-to-IP and IP addresses are registered to LISP CP

```
CP1#show lisp instance-id 8189 ethernet server address-resolution

Address-resolution data for router lisp 0 instance-id 8189

L3 InstID     Host Address                                Hardware Address
      4099     10.4.3.237/32                              bcec.4341.d25f
      4099     10.4.3.241/32                              000c.290a.cbb8
      4099     FE80::20C:29FF:FE0A:CBB8/128               000c.290a.cbb8
CP1#
CP1#
CP1#show lisp instance-id 4099 ipv4 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     --                    4099     0.0.0.0/0
               never      no     --                    4099     10.4.3.0/24
               00:02:43   yes#   172.31.216.71:11350   4099     10.4.3.237/32
               3d10h      yes#   172.31.216.76:40090   4099     10.4.3.241/32
               3d21h      yes#   192.168.8.2:50693     4099     10.67.33.0/24
               3d21h      yes#   192.168.8.2:50693     4099     172.29.4.48/29
CP1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding



Timeline:
6. Updates to LISP L2 and L3 databases trigger registrations.
7. LISP L3 IID registrations are published to all Border Nodes.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding

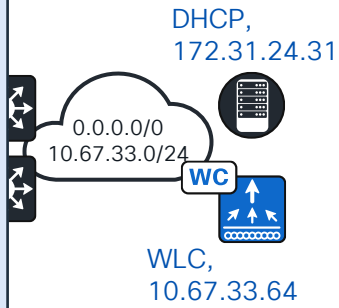
EP2,
MAC: bcec.4341.d25f
IPv4: 10.4.3.237

EN2, 172.31.216

Timeline:
6. Updates to LISP L2 and L3 databases trig
7. LISP L3 IID registrations are published to

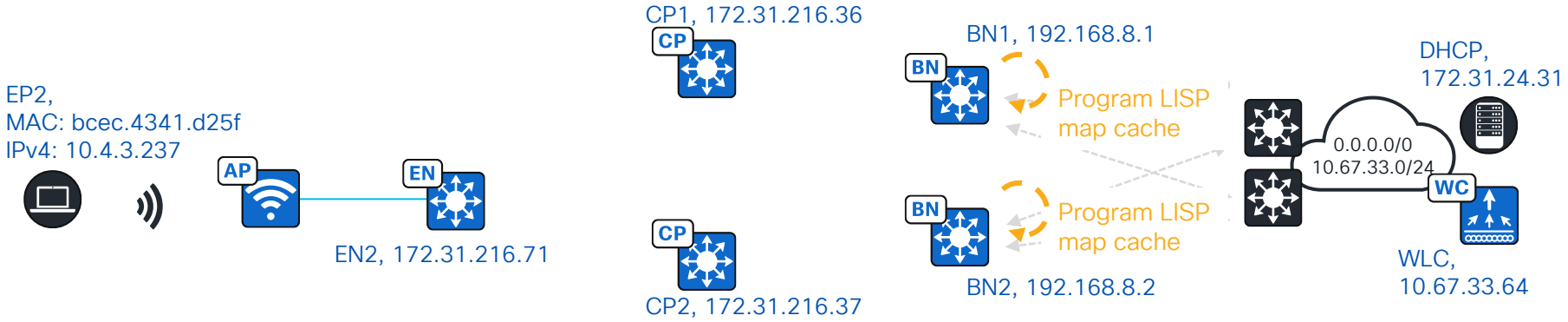
Endpoint L3 EIDs are published to BN

```
BN1#show lisp instance-id 4099 ipv4 publication
Publication Information for LISP 0 EID-table vrf CORP_VN (IID 4099)
Entries total 6
EID Prefix                Last        Last            Encap-IID
...
10.4.3.237/32             00:08:56    172.31.216.37   -

BN1#
BN1#show lisp instance-id 4099 ipv4 publication 10.4.3.237/32
Publication Information for LISP 0 EID-table vrf CORP_VN (IID 4099)
 * Indicates the selected rlocs used by consumers

  EID-prefix: 10.4.3.237/32
    First published:      00:09:17
    Last published:       00:09:17
    State:                complete
    Exported to:          map-cache, RIB

    Publisher 172.31.216.37:4342
      last published 00:09:17, TTL never, Expires: never
      ...
      Locator         Pri/Wgt  State     Encap-IID  RDP
      172.31.216.71    10/10   up        -          [-]

    Publisher 172.31.216.36:4342
      last published 00:09:17, TTL never, Expires: never
      ...
      Locator         Pri/Wgt  State     Encap-IID  RDP
      172.31.216.71    10/10   up        -          [-]

  Merge Locator Information
      Locator         Pri/Wgt  State     Encap-IID  RDP-Len Src-Address
      172.31.216.71*   10/10   up        -          0       172.31.216.37
BN1#
```



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

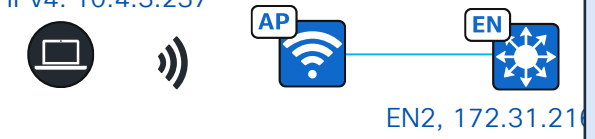
Wireless endpoint onboarding



Timeline:
6. Updates to LISP L2 and L3 databases trigger registrations.
7. LISP L3 IID registrations are published to all Border Nodes.
8. Publications are programmed to LISP map cache.

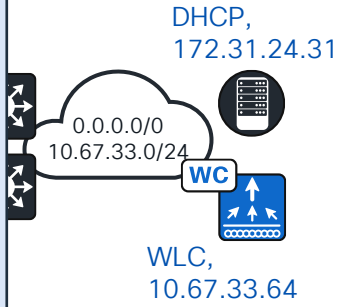
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding



Publications are programmed to LISP map cache

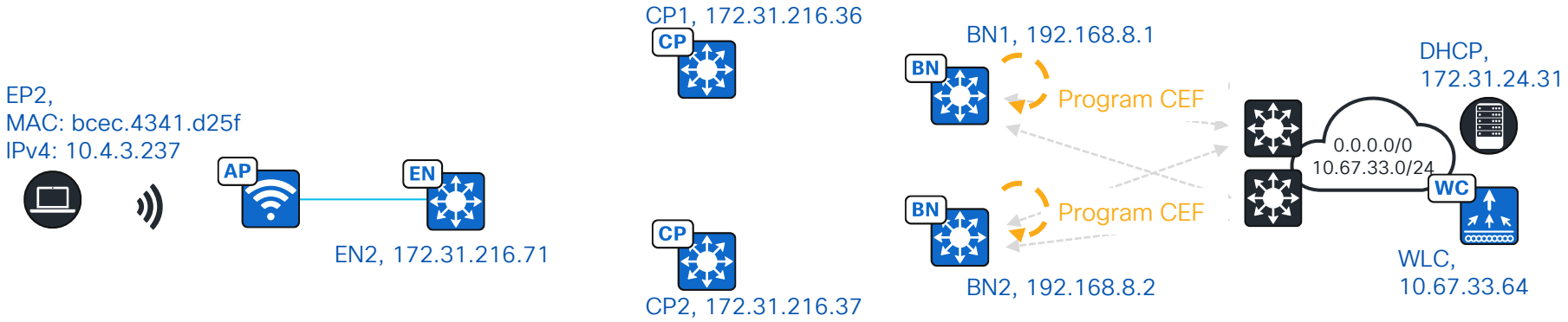
```
BN1#show lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf CORP_VN (IID 4099), 5
entries

0.0.0.0/0, uptime: 3d21h, expires: never, via pub-sub, unknown-eid-forward
  PETR          Uptime    State      Pri/Wgt     Encap-IID  Metric
  192.168.8.2   3d21h     up         10/10       -          0
10.4.3.0/24, uptime: 3d21h, expires: never, via pub-sub-send-map-req, send-
map-request
  Negative cache entry, action: send-map-request
10.4.3.237/32, uptime: 00:00:22, expires: never, via pub-sub, complete
  Locator         Uptime    State  Pri/Wgt     Encap-IID
  172.31.216.71   00:14:22  up     10/10       -
10.4.3.241/32, uptime: 3d10h, expires: never, via pub-sub, complete
  Locator         Uptime    State  Pri/Wgt     Encap-IID
  172.31.216.76   3d10h     up     10/10       -
10.67.33.0/24, uptime: 3d21h, expires: never, via pub-sub, complete
  Locator         Uptime    State  Pri/Wgt     Encap-IID
  192.168.8.2   3d21h     up     10/10       -
BN1#
```



Timeline:
6. Updates to LISP L2 and L3 databases trig
7. LISP L3 IID registrations are published to
8. Publications are programmed to LISP map

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

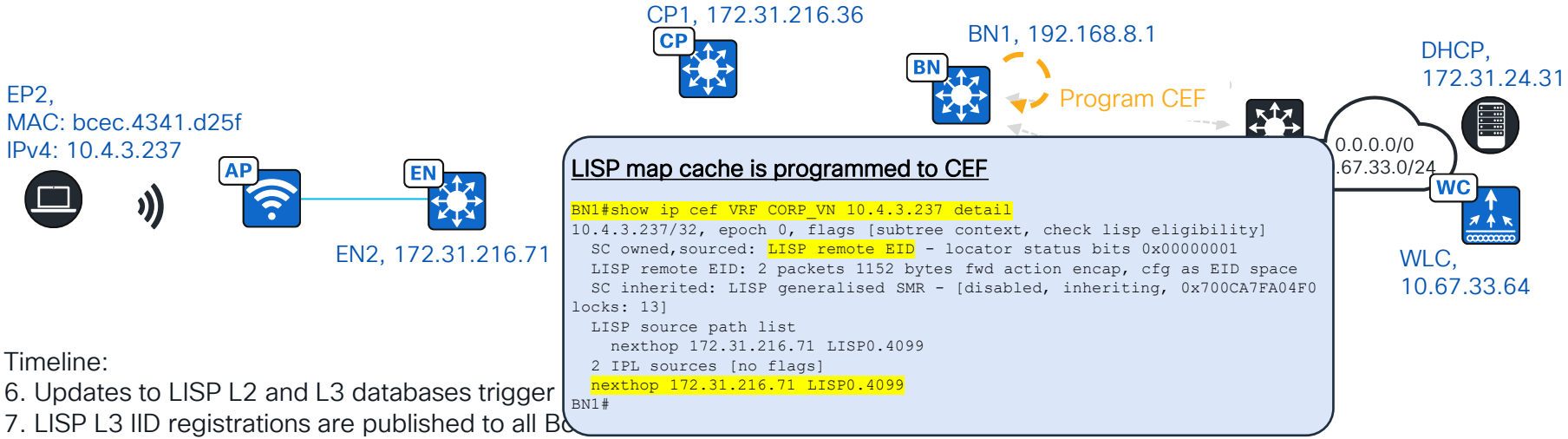
Wireless endpoint onboarding



Timeline:
6. Updates to LISP L2 and L3 databases trigger registrations.
7. LISP L3 IID registrations are published to all Border Nodes.
8. Publications are programmed to LISP map cache.
9. LISP map cache is programmed to CEF.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless endpoint onboarding

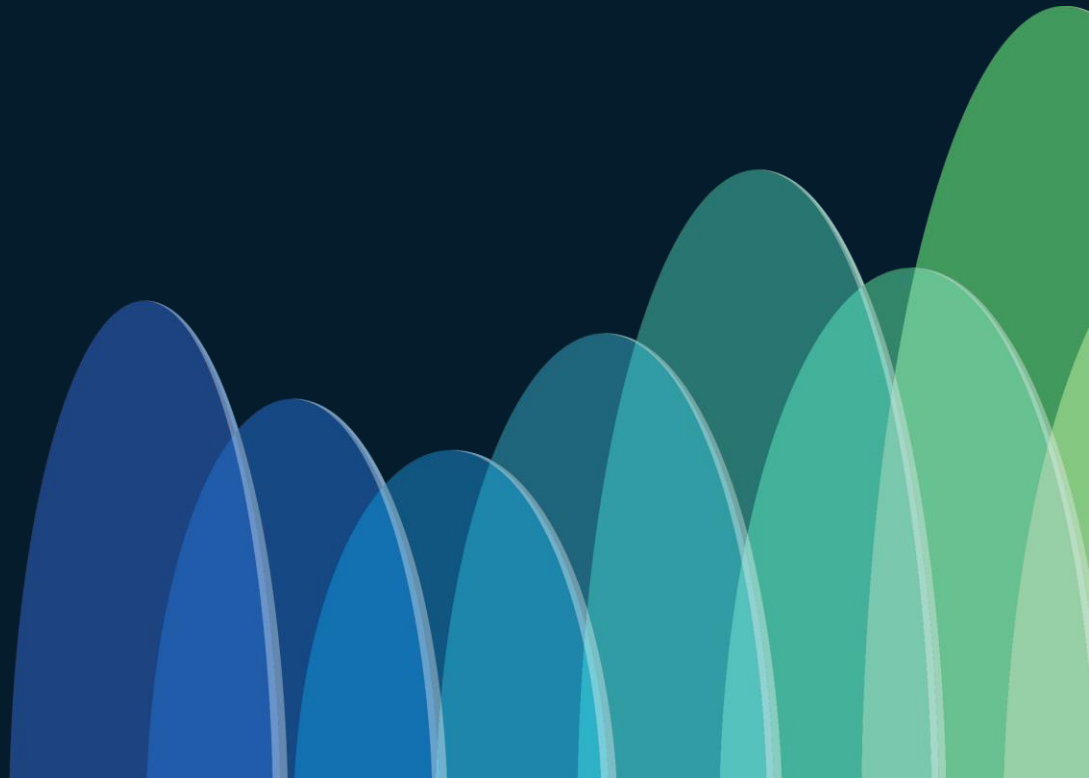


Timeline:

6. Updates to LISP L2 and L3 databases trigger
7. LISP L3 IID registrations are published to all Bo
8. Publications are programmed to LISP map cache.
9. LISP map cache is programmed to CEF.

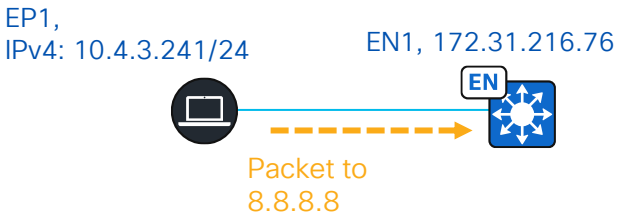
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

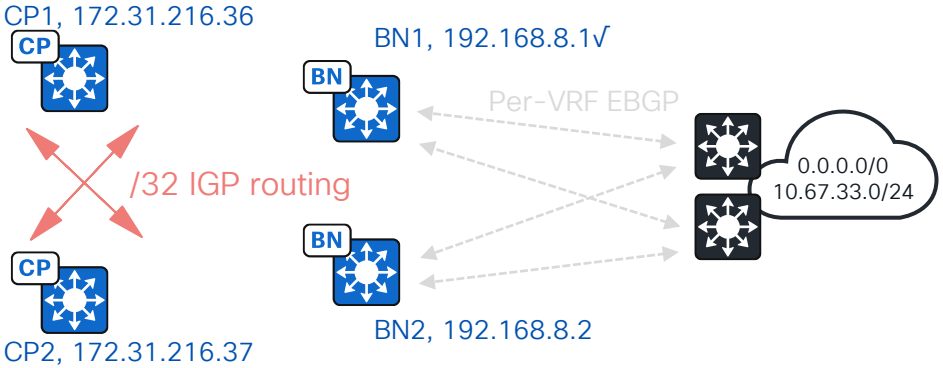
Fabric Endpoint Packet Handling



cisco Live!

Fabric to external packet handling



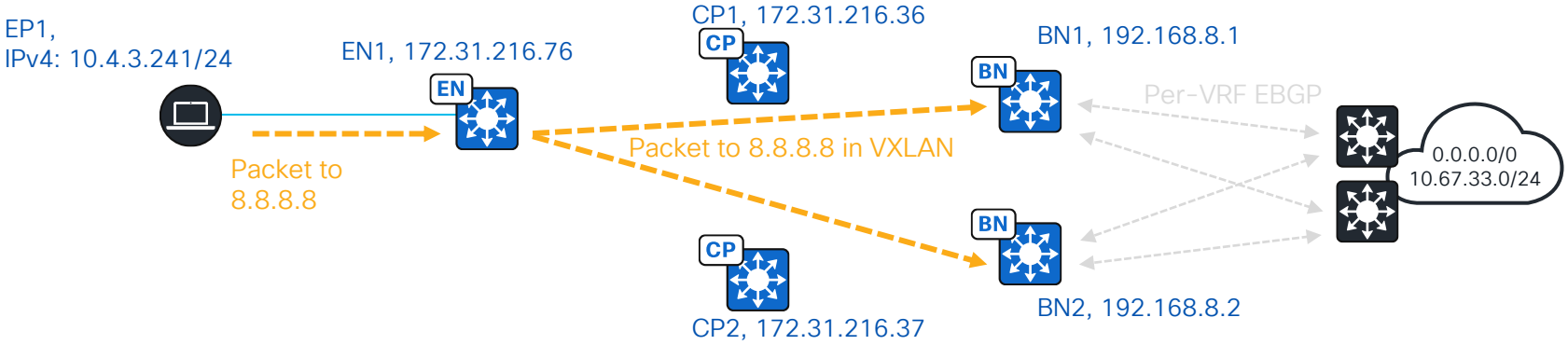


Timeline:

1. EP1 sends a packet to its default gateway.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric to external packet handling

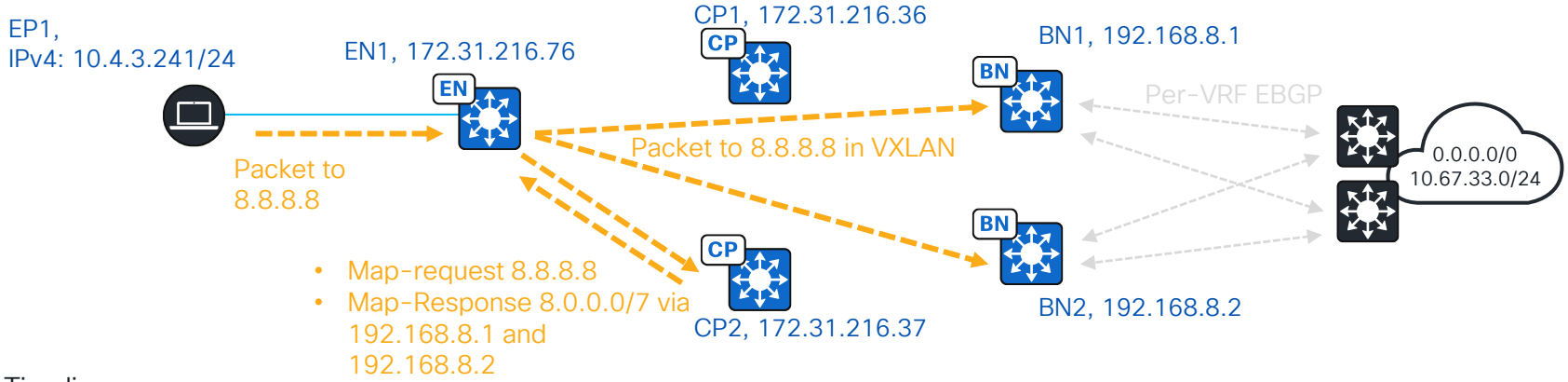


Timeline:

1. EP1 sends a packet to its default gateway.
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF (which is derived from 0.0.0.0 LISP map cache as explained in the Edge Node Bootstrapping section), and is forwarded to a BN.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric to external packet handling

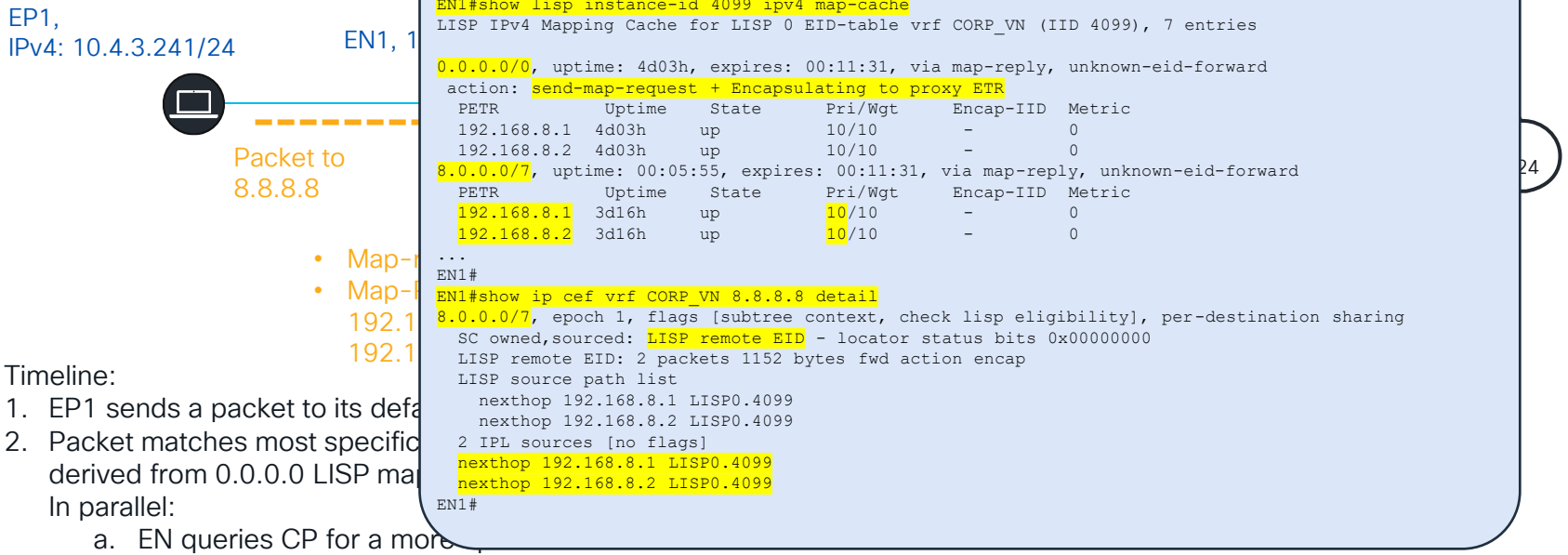


Timeline:

1. EP1 sends a packet to its default gateway.
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF (which is derived from 0.0.0.0 LISP map cache as explained in the Edge Node Bootstrapping section), and is forwarded to a BN. In parallel:
    a. EN queries CP for a more specific route.
    b. CP replies, a more specific Edge Node LISP map cache entry is programmed and a more more specific CEF entry is programmed. Further packets from endpoints will match the more specific CEF entry.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric to external packet handling



LISP map cache and CEF are programmed for non-fabric destination via PETR

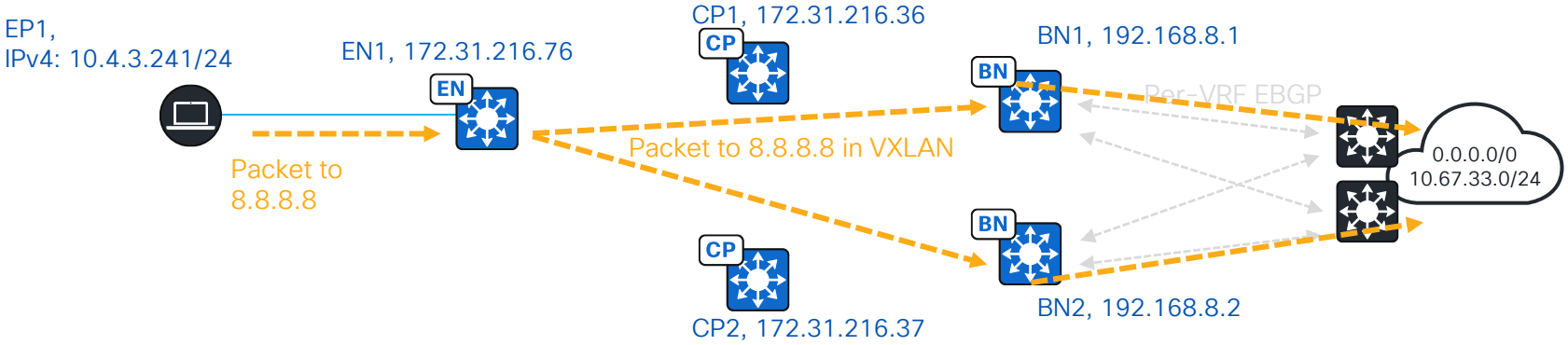
```
EN1#show lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf CORP_VN (IID 4099), 7 entries

0.0.0.0/0, uptime: 4d03h, expires: 00:11:31, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
  PETR          Uptime    State      Pri/Wgt     Encap-IID  Metric
  192.168.8.1   4d03h     up         10/10        -         0
  192.168.8.2   4d03h     up         10/10        -         0
8.0.0.0/7, uptime: 00:05:55, expires: 00:11:31, via map-reply, unknown-eid-forward
  PETR          Uptime    State      Pri/Wgt     Encap-IID  Metric
  192.168.8.1   3d16h     up         10/10        -         0
  192.168.8.2   3d16h     up         10/10        -         0
...
EN1#
EN1#show ip cef vrf CORP_VN 8.8.8.8 detail
8.0.0.0/7, epoch 1, flags [subtree context, check lisp eligibility], per-destination sharing
  SC owned,sourced: LISP remote EID - locator status bits 0x00000000
  LISP remote EID: 2 packets 1152 bytes fwd action encap
  LISP source path list
    nexthop 192.168.8.1 LISP0.4099
    nexthop 192.168.8.2 LISP0.4099
  2 IPL sources [no flags]
  nexthop 192.168.8.1 LISP0.4099
  nexthop 192.168.8.2 LISP0.4099
EN1#
```

Timeline:

1. EP1 sends a packet to its defa
2. Packet matches most specific
   derived from 0.0.0.0 LISP ma
   In parallel:
   a. EN queries CP for a more
   b. CP replies, a more specific Edge Node LISP map cache entry is programmed and a more more specific CEF entry is programmed. Further packets from endpoints will match the more specific CEF entry.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric to external packet handling

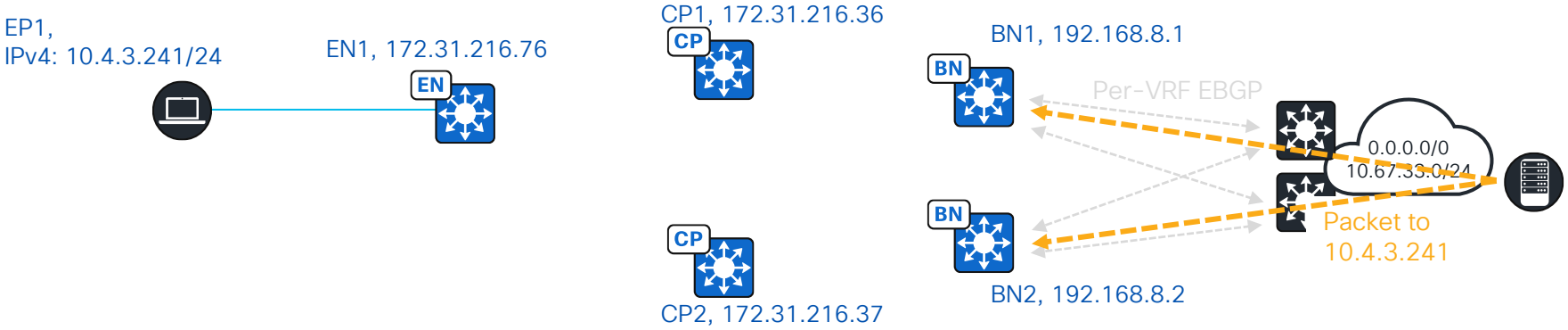


Timeline:

1. EP1 sends a packet to its default gateway.
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF (which is derived from 0.0.0.0 LISP map cache as explained in the Edge Node Bootstrapping section), and is forwarded to a BN.
   In parallel:
   a. EN queries CP for a more specific route.
   b. CP replies, a more specific Edge Node LISP map cache entry is programmed and a more more specific CEF entry is programmed. Further packets from endpoints will match the more specific CEF entry.
3. BN matches most appropriate RIB entry and routes towards destination.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

External to fabric packet handling

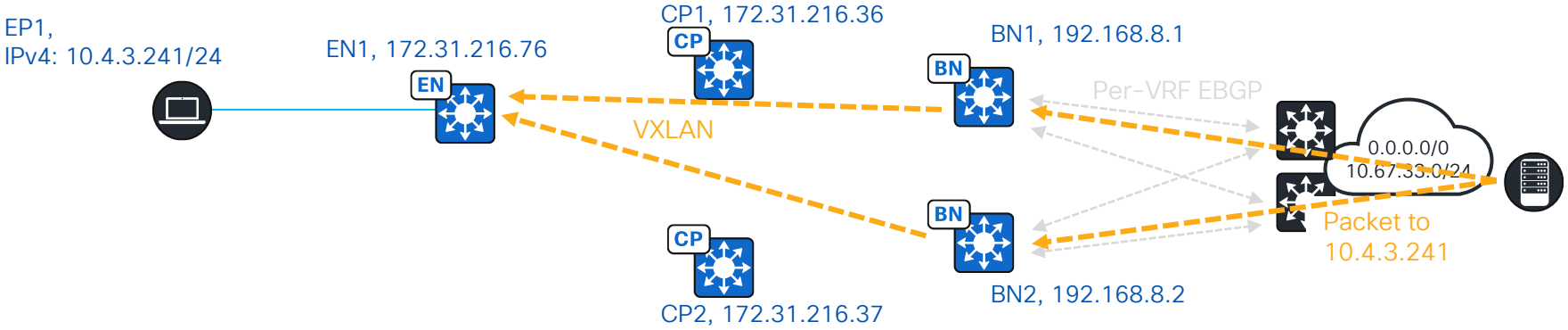


Timeline:

1. Host outside Fabric sends packet to wired or wireless endpoint connected to the Fabric.
2. Packet is routed to a BN.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

External to fabric packet handling

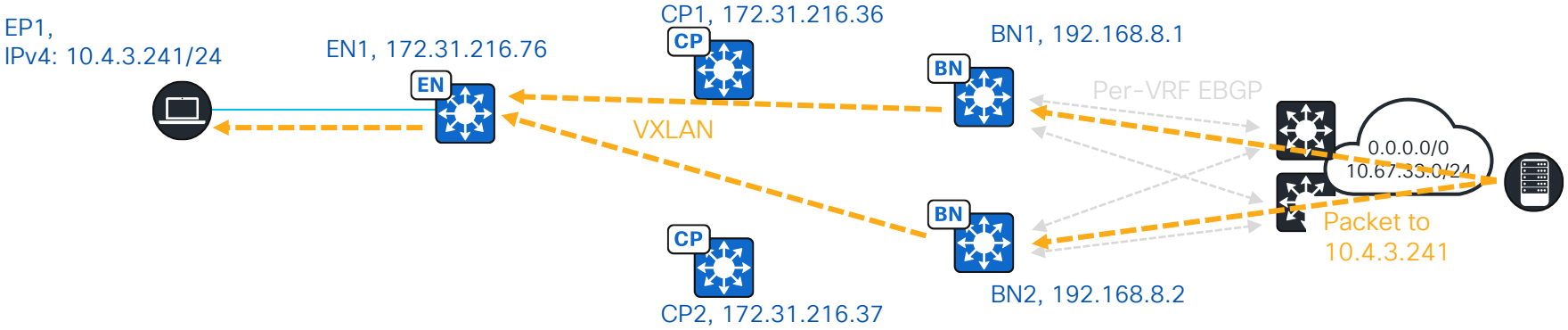


Timeline:

1. Host outside Fabric sends packet to wired or wireless endpoint connected to the Fabric.
2. Packet is routed to a BN.
3. BN matches the host route in CEF which was derived from LISP map cache and forwards to associated RLOC.
   Note: See Endpoint Onboarding and Registration sections for details of how this host route was added to CEF.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

External to fabric packet handling

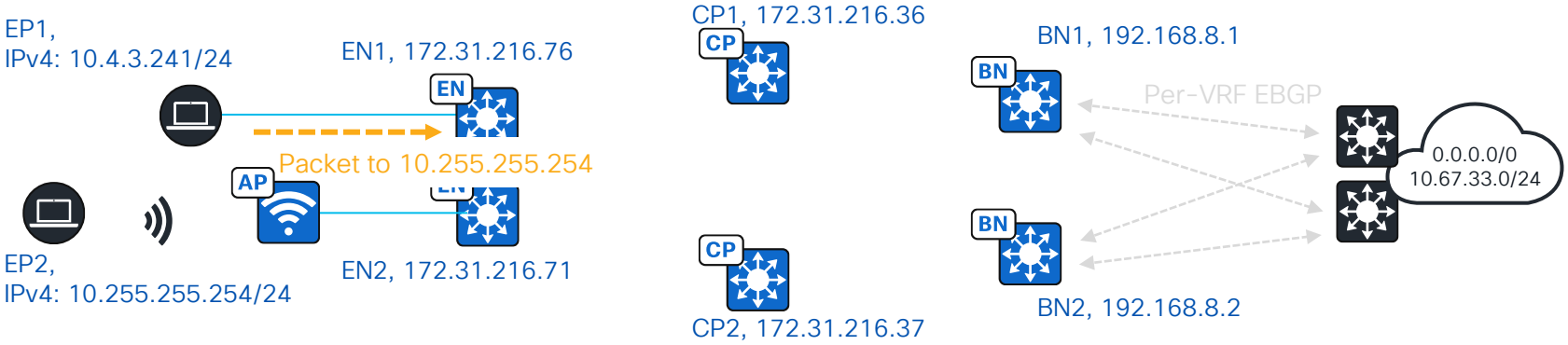


Timeline:

1. Host outside Fabric sends packet to wired or wireless endpoint connected to the Fabric.
2. Packet is routed to a BN.
3. BN matches the host route in CEF which was derived from LISP map cache and forwards to associated RLOC.
   Note: See Endpoint Onboarding and Registration sections for details of how this host route was added to CEF.
4. EN forwards to destination endpoint.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric inter-subnet packet handling

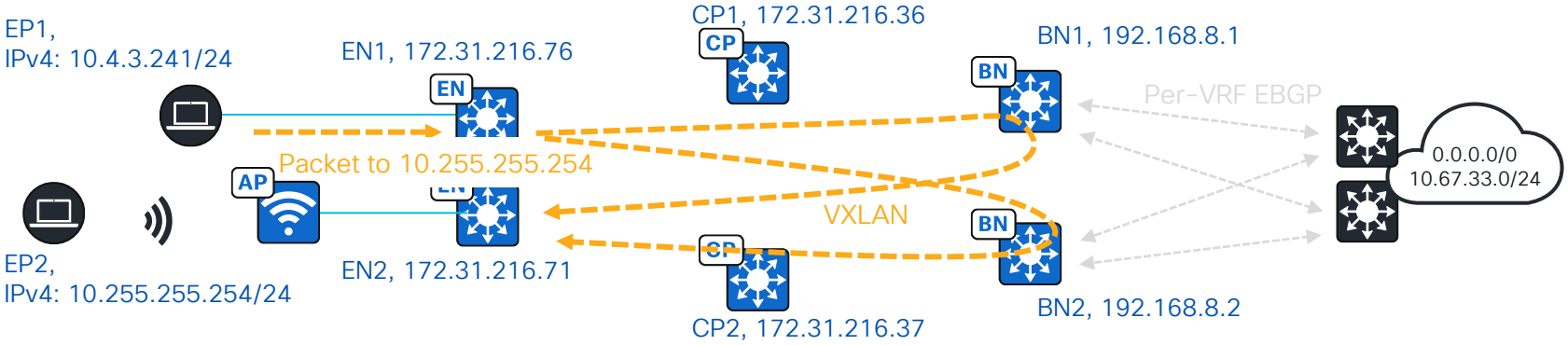


Timeline:

1. EP1 sends a packet to EP2 at 10.255.255.237 via default gateway (Edge Node Anycast Gateway).

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric inter-subnet packet handling

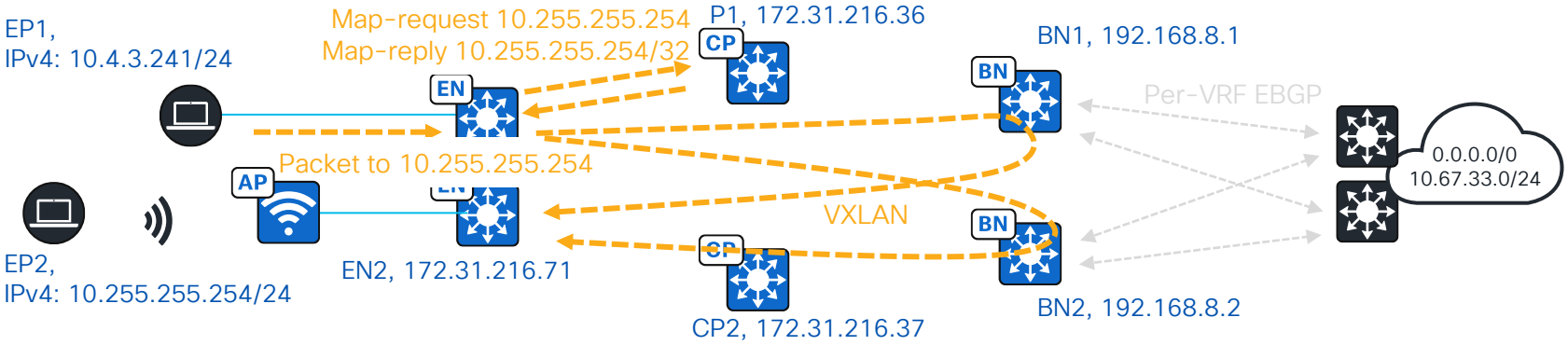


Timeline:

1. EP1 sends a packet to EP2 at 10.255.255.237 via default gateway (Edge Node Anycast Gateway).
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF which is derived from 0.0.0.0 in LISP map cache, and is forwarded to a BN.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric inter-subnet packet handling

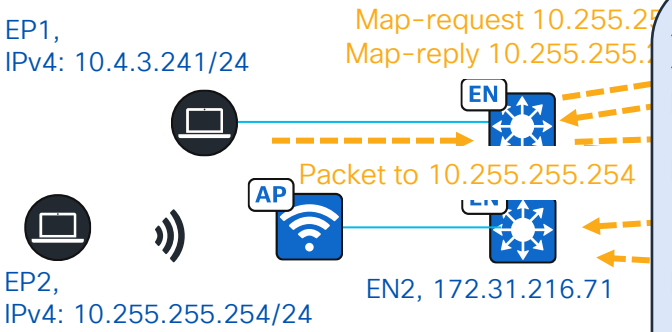


Timeline:

1. EP1 sends a packet to EP2 at 10.255.255.237 via default gateway (Edge Node Anycast Gateway).
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF which is derived from 0.0.0.0 in LISP map cache, and is forwarded to a BN.
   In parallel:
   a. EN queries CP for a more specific route.
   b. CP replies, a more specific map cache entry is programmed and a more more specific CEF entry is programmed. Further packets from EP1 to EP2 will match the more specific CEF entry.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric inter-subnet packet handling



Timeline:

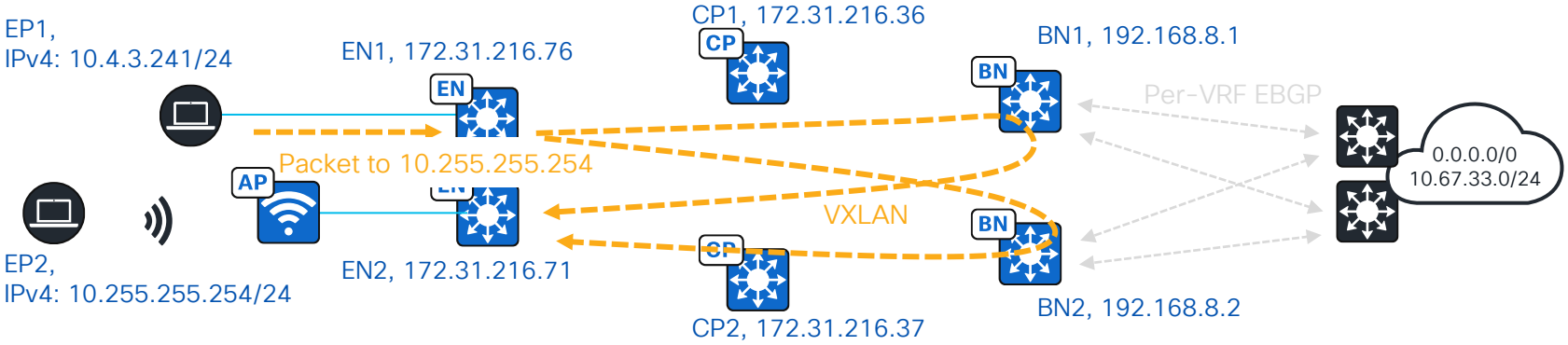
1. EP1 sends a packet to EP2 at 10.255.255.23
2. Packet matches most specific CEF entry. In th
   derived from 0.0.0.0 in LISP map cache, and
   In parallel:
   a. EN queries CP for a more specific rou
   b. CP replies, a more specific map cache
      Further packets from EP1 to EP2 will n

EN1 LISP map cache and CEF are programmed for direct routing to the on-fabric destination IP address

```
EN1#show lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf CORP_VN (IID 4099), 7 entries

0.0.0.0/0, uptime: 4d04h, expires: 00:14:13, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
  PETR          Uptime    State      Pri/Wgt     Encap-IID  Metric
  192.168.8.1   4d04h     up          10/10        -         0
  192.168.8.2   4d04h     up          10/10        -         0
10.255.255.254/32, uptime: 00:00:13, expires: 23:59:46, via map-reply, complete
  Locator         Uptime    State  Pri/Wgt     Encap-IID
  172.31.216.71   00:00:13  up      10/10        -
...
EN1#
EN1#
EN1#show ip cef vrf CORP_VN 10.255.255.254 detail
10.255.255.254/32, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 2 packets 1152 bytes fwd action encap, dynamic EID need encap
  SC inherited: LISP cfg dyn-EID - LISP configured dynamic-EID
  LISP EID attributes: localEID No, c-dynEID Yes, d-dynEID No, a-dynEID No
  SC inherited: LISP generalised SMR - [enabled, inheriting, 0x7388C3E73890 locks: 3]
  LISP source path list
    nexthop 172.31.216.71 LISP0.4099
  2 IPL sources [no flags]
  nexthop 172.31.216.71 LISP0.4099
EN1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric inter-subnet packet handling

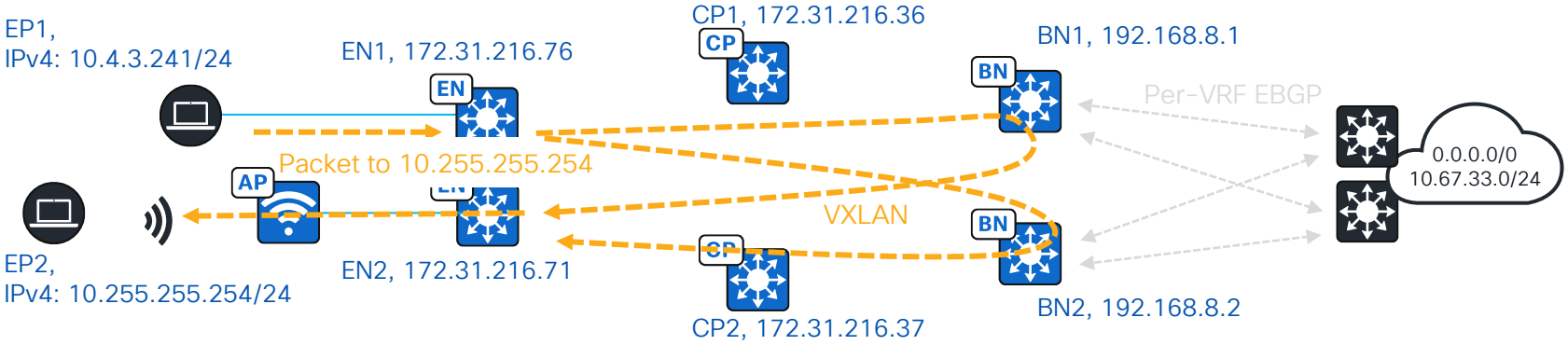


Timeline:

1. EP1 sends a packet to EP2 at 10.255.255.237 via default gateway (Edge Node Anycast Gateway).
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF which is derived from 0.0.0.0 in LISP map cache, and is forwarded to a BN.
   In parallel:
   a. EN queries CP for a more specific route.
   b. CP replies, a more specific map cache entry is programmed and a more more specific CEF entry is programmed. Further packets from EP1 to EP2 will match the more specific CEF entry.
3. For the first packet from EP1 to EP2, BN matches host CEF entry and hairpins back to EN2 in VXLAN.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric inter-subnet packet handling

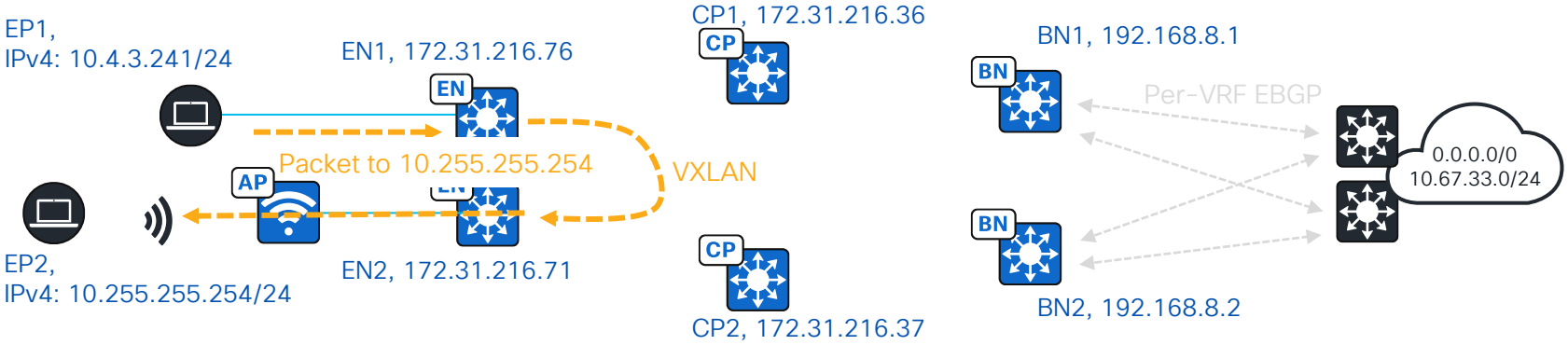


Timeline:

1. EP1 sends a packet to EP2 at 10.255.255.237 via default gateway (Edge Node Anycast Gateway).
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF which is derived from 0.0.0.0 in LISP map cache, and is forwarded to a BN.
   In parallel:
   a. EN queries CP for a more specific route.
   b. CP replies, a more specific map cache entry is programmed and a more more specific CEF entry is programmed. Further packets from EP1 to EP2 will match the more specific CEF entry.
3. For the first packet from EP1 to EP2, BN matches host CEF entry and hairpins back to EN2 in VXLAN.
4. EN2 sends out access tunnel towards EP2.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric inter-subnet packet handling

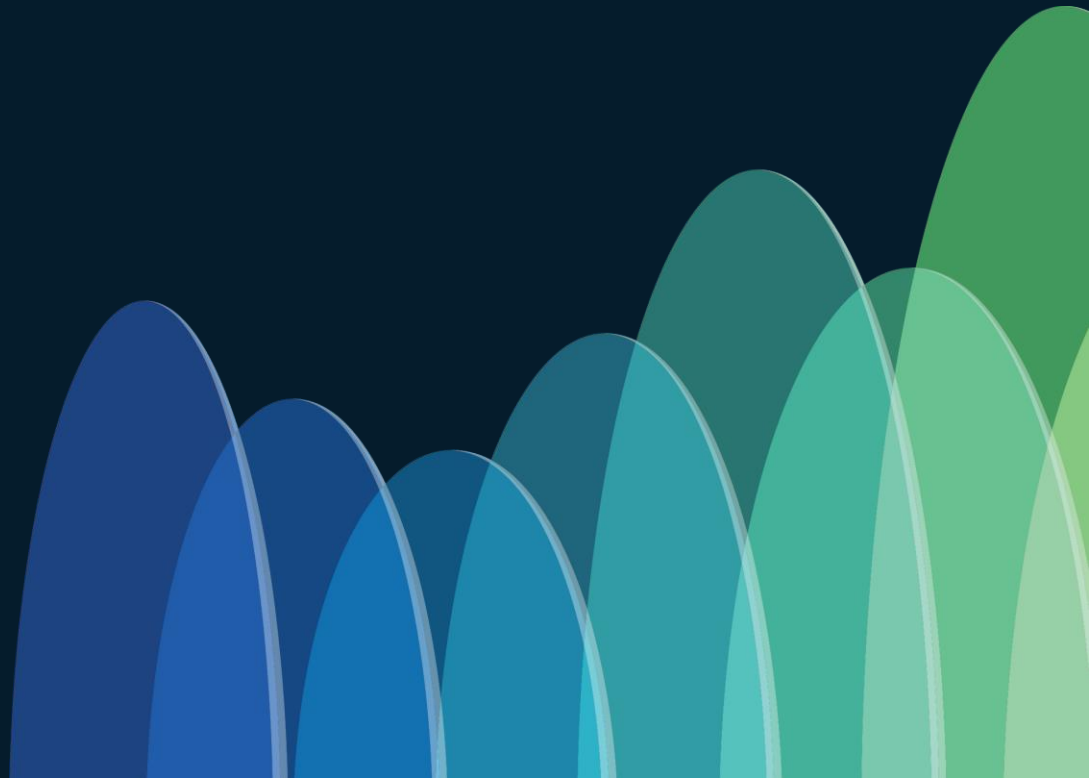


Timeline:

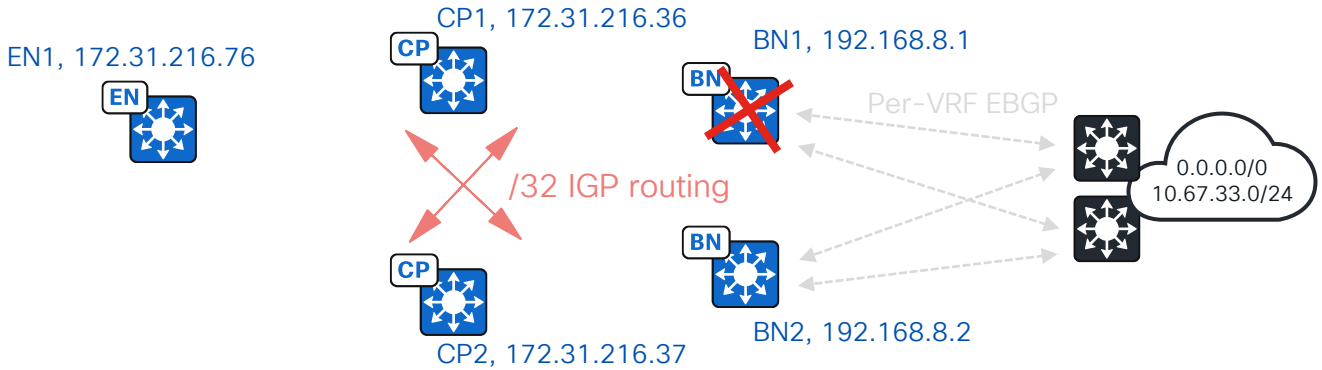
1. EP1 sends a packet to EP2 at 10.255.255.237 via default gateway (Edge Node Anycast Gateway).
2. Packet matches most specific CEF entry. In this case as the first packet in the flow it matches 0.0.0.0 in CEF which is derived from 0.0.0.0 in LISP map cache, and is forwarded to a BN.
   In parallel:
   a. EN queries CP for a more specific route.
   b. CP replies, a more specific map cache entry is programmed and a more more specific CEF entry is programmed. Further packets from EP1 to EP2 will match the more specific CEF entry.
3. For the first packet from EP1 to EP2, BN matches host CEF entry and hairpins back to EN2 in VXLAN.
4. EN2 sends out access tunnel towards EP2.
5. Further EP1 to EP2 packets route directly from EN1 to EN2 in VXLAN.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR Node Failure



Default ETR node failure

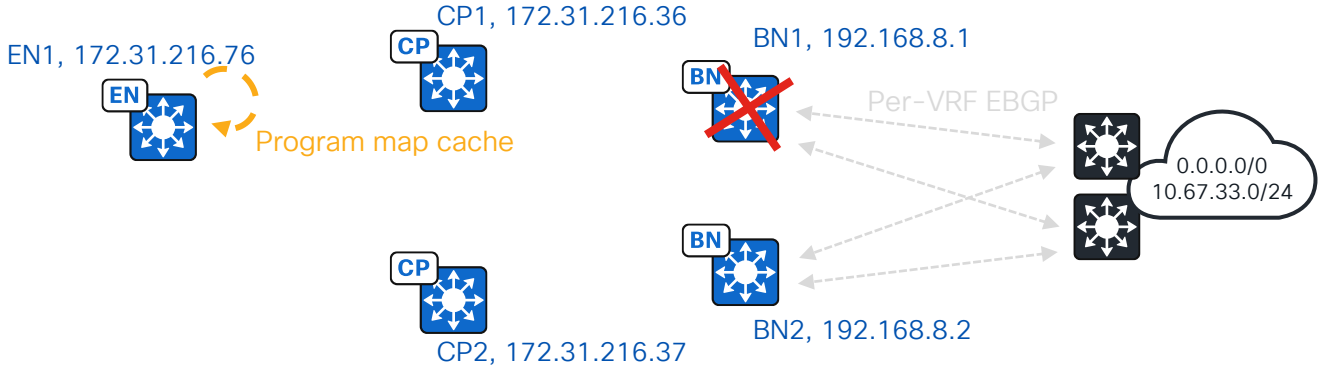


Timeline:

1. External BNs are up and registered as valid default ETRs.
2. BN1 fails.
3. Underlay IGP converges and /32 entry for BN1 RLOC is withdrawn.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR node failure



Timeline:

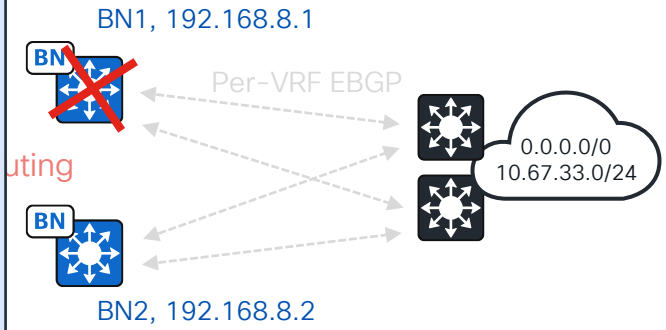
1. External BNs are up and registered as valid default ETRs.
2. BN1 fails.
3. Underlay IGP converges and /32 entry for BN1 RLOC is withdrawn.
4. On all fabric nodes LISP map cache updates to treat BN1 RLOC as invalid.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR node failure

RLOC withdrawn from IGP causes RLOC reject in LISP map cache

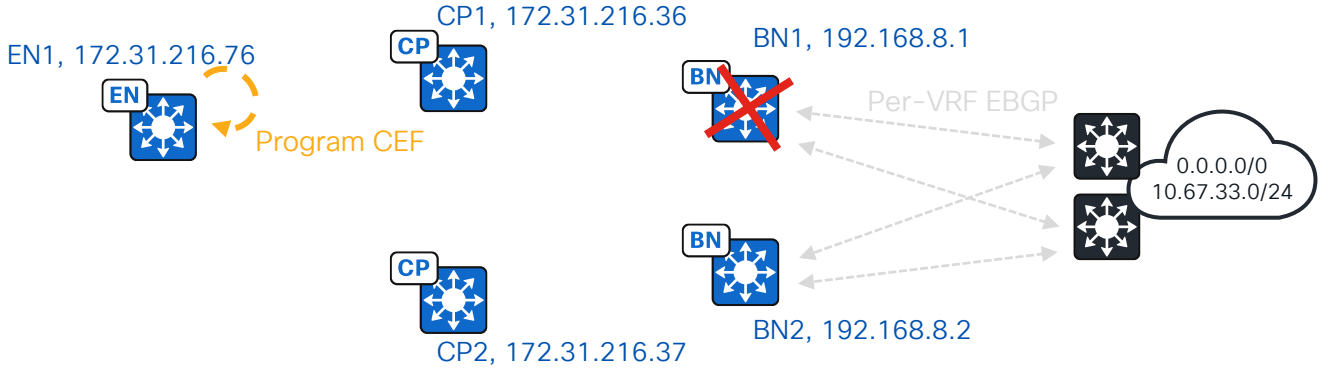
```
EN1#show lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf CORP_VN (IID 4099), 7 entries

0.0.0.0/0, uptime: 3w0d, expires: 00:08:27, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
   PETR           Uptime     State       Pri/Wgt     Encap-IID  Metric
   192.168.8.1    3w0d       route-rejec 10/10        -         0
   192.168.8.2    3w0d       up          10/10        -         0
8.0.0.0/7, uptime: 6d06h, expires: 00:08:27, via map-reply, unknown-eid-forward
   PETR           Uptime     State       Pri/Wgt     Encap-IID  Metric
   192.168.8.1    2w6d       route-rejec 10/10        -         0
   192.168.8.2    2w6d       up          10/10        -         0
64.0.0.0/2, uptime: 02:57:57, expires: 00:14:40, via map-reply, unknown-eid-forward
   PETR           Uptime     State       Pri/Wgt     Encap-IID  Metric
   192.168.8.1    2w6d       route-rejec 10/10        -         0
   192.168.8.2    2w6d       up          10/10        -         0
128.0.0.0/3, uptime: 1w2d, expires: 00:08:28, via map-reply, unknown-eid-forward
   PETR           Uptime     State       Pri/Wgt     Encap-IID  Metric
   192.168.8.1    2w6d       route-rejec 10/10        -         0
   192.168.8.2    2w6d       up          10/10        -         0
EN1#
```



4. On all fabric nodes LISP map cache updates to treat BN1 RLOC as invalid.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR node failure



Timeline:

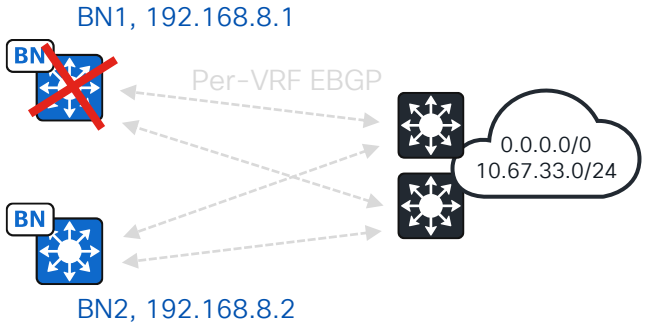
1. External BNs are up and registered as valid default ETRs.
2. BN1 fails.
3. Underlay IGP converges and /32 entry for BN1 RLOC is withdrawn.
4. On all fabric nodes LISP map cache updates to treat BN1 RLOC as invalid.
5. LISP map cache update triggers CEF update.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR node failure

EN1 LISP map cache and CEF are programmed for direct routing to the on-fabric destination IP addresss

```
EN1#show ip cef vrf CORP_VN 0.0.0.0/0 detail
0.0.0.0/0, epoch 1, flags [cover dependents, subtree context, check lisp eligibility,
default route]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000000
  LISP remote EID: 1652 packets 875864 bytes fwd action signal-fwd, cfg as EID space
  LISP source path list
    nexthop 192.168.8.2 LISP0.4099
  Covered dependent prefixes: 6
    notify cover updated: 6
  2 IPL sources [no flags]
  nexthop 192.168.8.2 LISP0.4099
EN1#
```

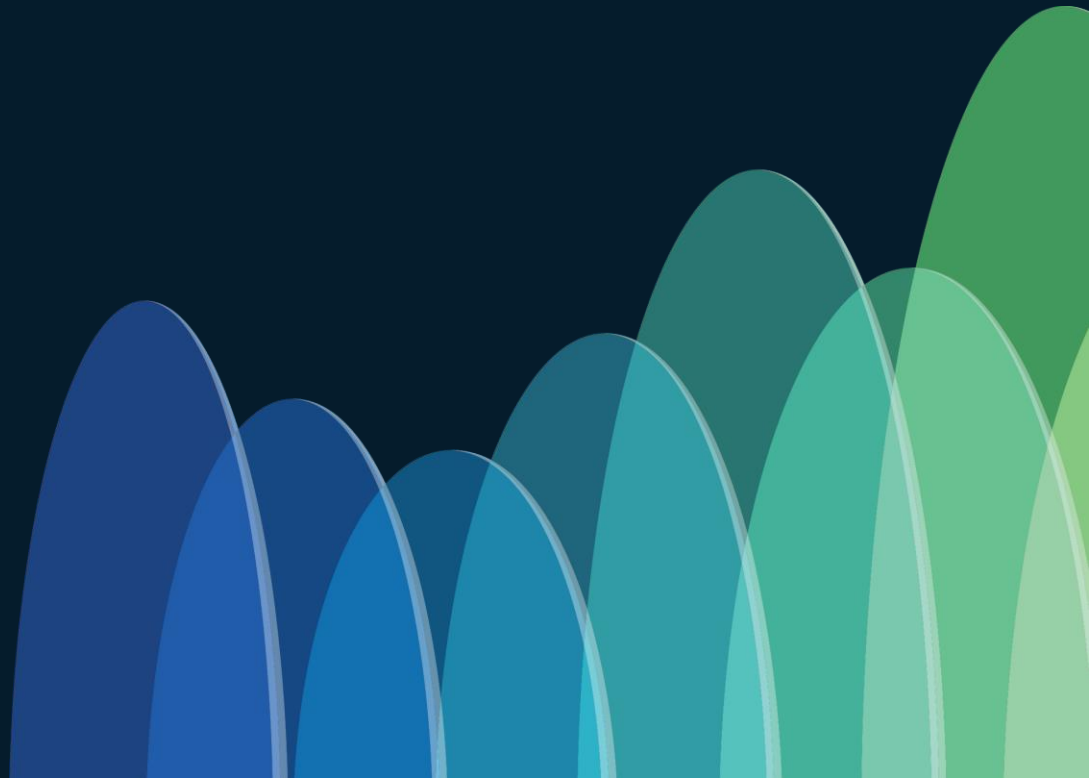


Timeline:

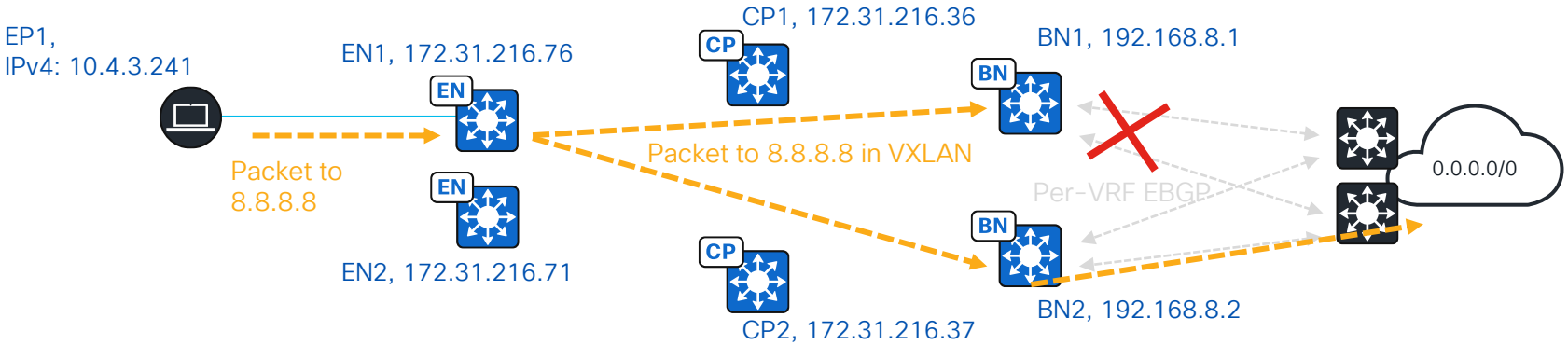
1. External BNs are up and registered as valid default ETRs.
2. BN1 fails.
3. Underlay IGP converges and /32 entry for BN1 RLOC is withdrawn.
4. On all fabric nodes LISP map cache updates to treat BN1 RLOC as invalid.
5. LISP map cache update triggers CEF update.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR Route Failure



Default ETR route failure

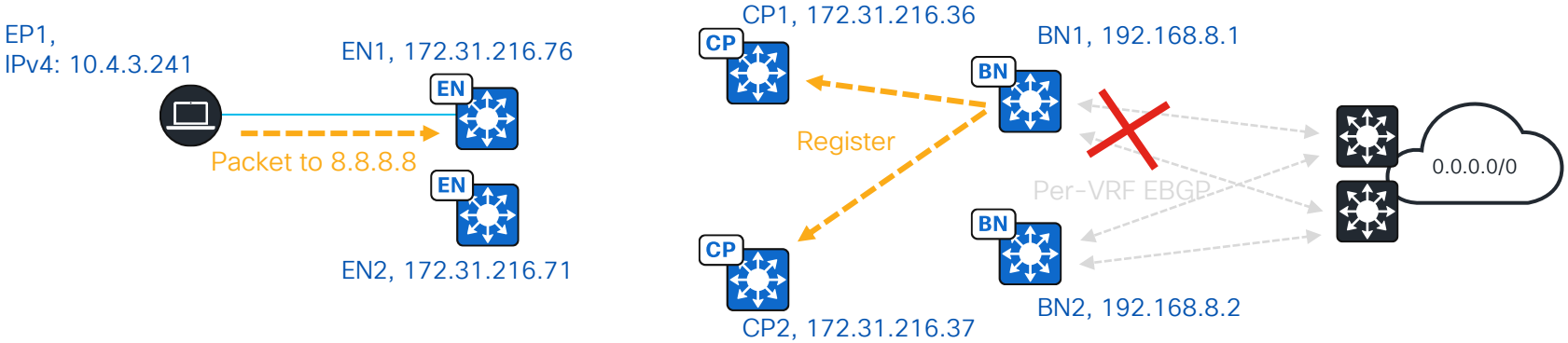


Timeline:

1. Default route withdrawn from BN VRF RIB.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR route failure



Timeline:

1. Default route withdrawn from BN VRF RIB.
2. BN registers default ETR with an unreachable priority.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

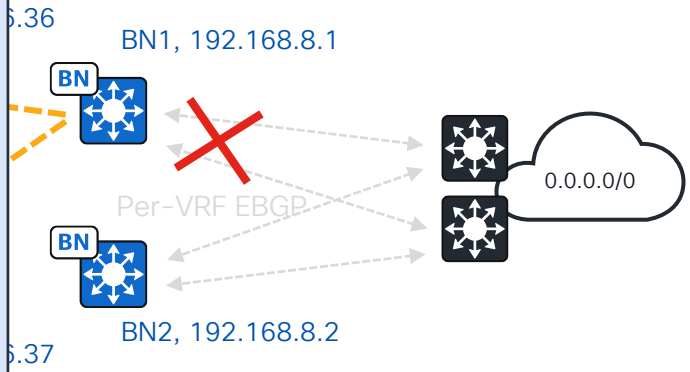
Default ETR route failure

Default ETR is unreachable due to priority 255 (higher is worse)

```
CP1#show lisp remote-locator-set default-etrs
Codes:
ETR = ETR Type (Default = Default-ETR, Service = Service-ETR)
SI  = Service Insertion Type
ID  = Service Insertion ID
-   = No service insertion config type defined
DS  = Default-ETR Firewall Service Insertion
SS  = Service-ETR Firewall Service Insertion
P   = Primary/Direct in use, Backup not available
PB  = Primary/Direct in use, Backup available
B   = Backup in use, Primary/Direct not available
BP  = Backup in use, Primary/Direct available
MT  = Multisite Service Insertion
 * = This locator has multiple service EID configured.

LISP remote-locator-set default-etr-locator-set-ipv4 Information

 RLOC          Pri/Wgt/Metric     Inst       Domain-ID/MH-ID  ETR       SI/ID
 192.168.8.1   255/10 /-          4099       2070054968/34872  Default   B /-
 192.168.8.2   10/10 /0           4099       2070054968/34872  Default   P /-

CP1#
```

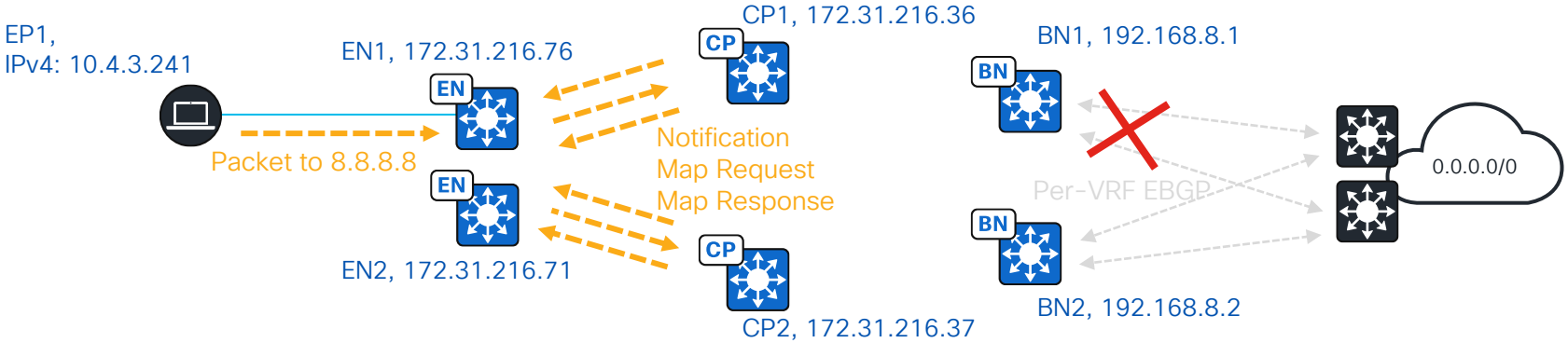
EP1,
IPv4:

Timeli
1. De
2. BN



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR route failure



Timeline:

1. Default route withdrawn from BN VRF RIB.
2. BN registers default ETR with an unreachable priority.
3. Edge Nodes are notified of default ETR down. Edge Nodes walk all impacted LISP map cache entries for refresh.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

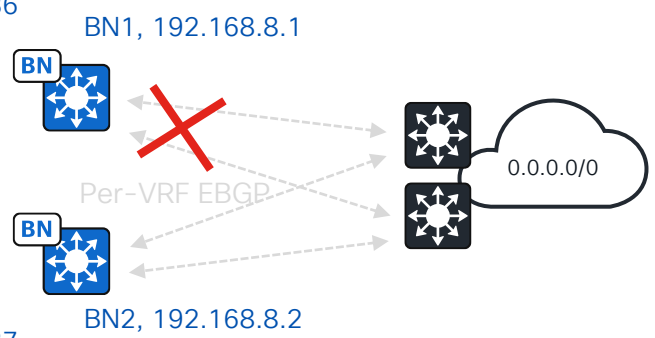
Default ETR route failure

LISP map cache is refreshed to avoid BN without external network reachabilitiy

```
EN1#show lisp instance-id 4099 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf CORP_VN (IID 4099), 8 entries

0.0.0.0/0, uptime: 2w1d, expires: 00:14:38, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
   PETR          Uptime    State       Pri/Wgt     Encap-IID  Metric
   192.168.8.1   2w1d      admin-down  255/10        -         -
   192.168.8.2   2w1d      up           10/10        -         0
...
8.0.0.0/7, uptime: 00:01:21, expires: 00:14:38, via map-reply, unknown-eid-forward
   PETR          Uptime    State       Pri/Wgt     Encap-IID  Metric
   192.168.8.1   2w0d      admin-down  255/10        -         -
   192.168.8.2   2w0d      up           10/10        -         0
...
EN1#
```

16.36

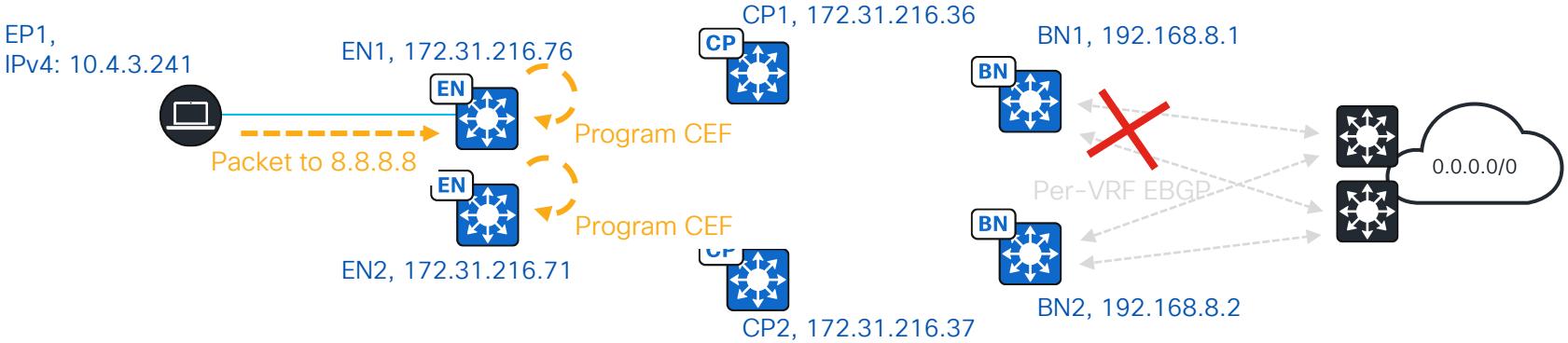
16.37



1. Default route withdrawn from BN via RIB.
2. BN registers default ETR with an unreachable priority.
3. Edge Nodes are notified of default ETR down. Edge Nodes walk all impacted LISP map cache entries for refresh.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR route failure



Timeline:

1. Default route withdrawn from BN VRF RIB.
2. BN registers default ETR with an unreachable priority.
3. Edge Nodes are notified of default ETR down. Edge Nodes walk all impacted LISP map cache entries for refresh.
4. Updated map cache is programmed to CEF.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

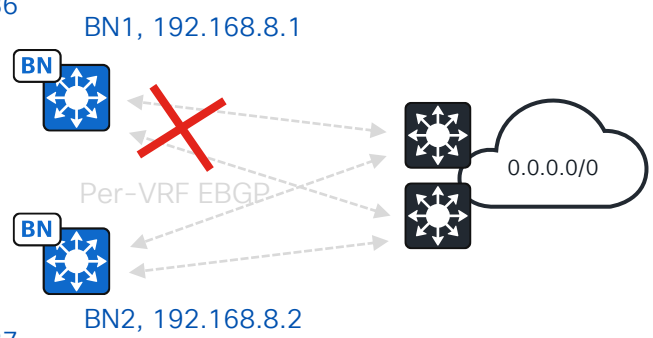
Default ETR route failure

CEF is programmed from updated LISP map cache

```
EN1#show ip cef vrf CORP_VN 0.0.0.0/0 detail
0.0.0.0/0, epoch 1, flags [cover dependents, subtree context, check lisp
eligibility, default route]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000000
  LISP remote EID: 1031 packets 562544 bytes fwd action signal-fwd, cfg as EID
space
  LISP source path list
    nexthop 192.168.8.2 LISP0.4099
  Covered dependent prefixes: 7
    notify cover updated: 7
  2 IPL sources [no flags]
  nexthop 192.168.8.2 LISP0.4099
EN1#
EN1#show ip cef vrf CORP_VN 8.8.8.8 detail
8.0.0.0/7, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000000
  LISP remote EID: 45 packets 25920 bytes fwd action encap
  LISP source path list
    nexthop 192.168.8.2 LISP0.4099
  2 IPL sources [no flags]
  nexthop 192.168.8.2 LISP0.4099
EN1#
```

16.36

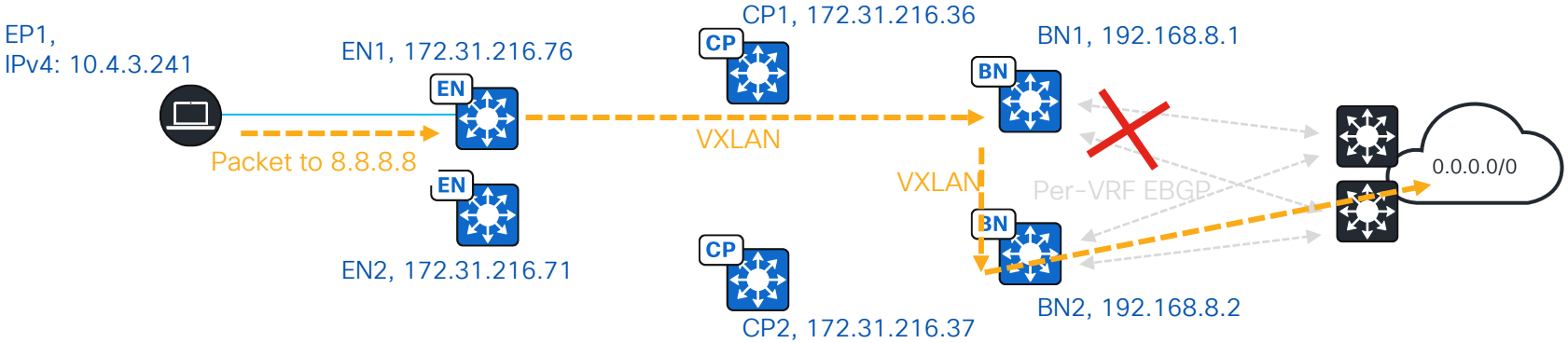
16.37



pacted LISP map cache entries for refresh.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default ETR route failure

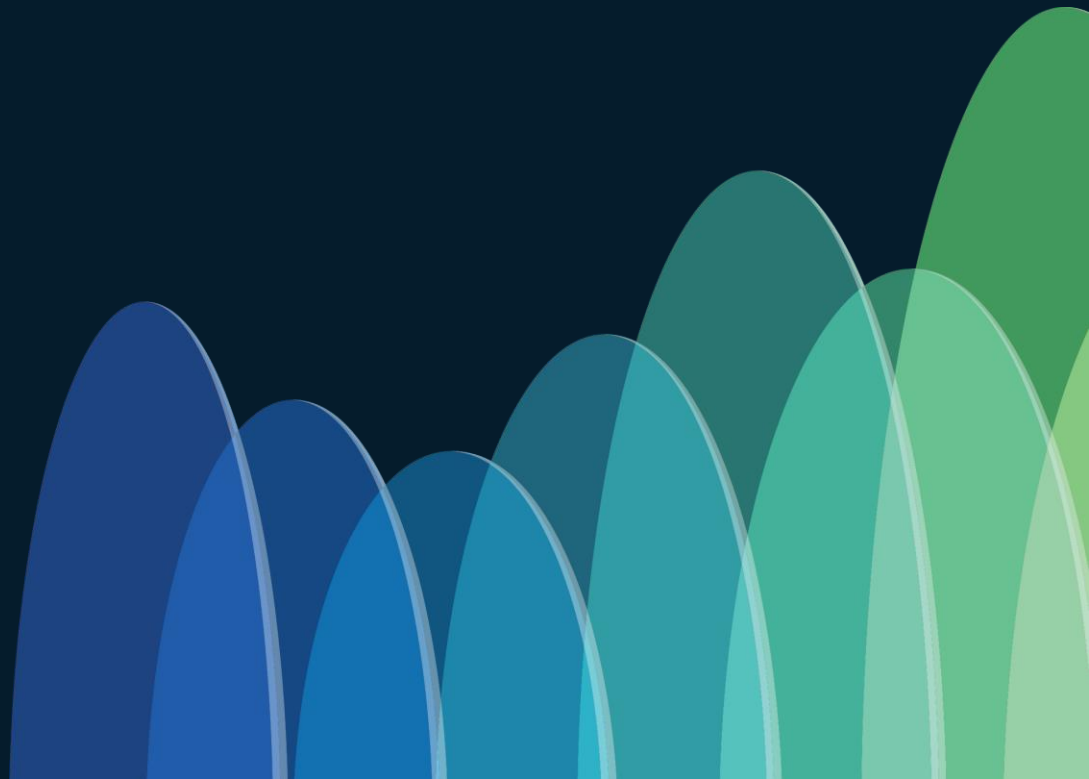


Timeline:

1. Default route withdrawn from BN VRF RIB.
2. BN registers default ETR with an unreachable priority.
3. Edge Nodes are notified of default ETR down. Edge Nodes walk all impacted LISP map cache entries for refresh.
4. Updated map cache is programmed to CEF.
5. Any packets in flight during BN1 route failure will be rerouted by BN1 to a usable default ETR.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

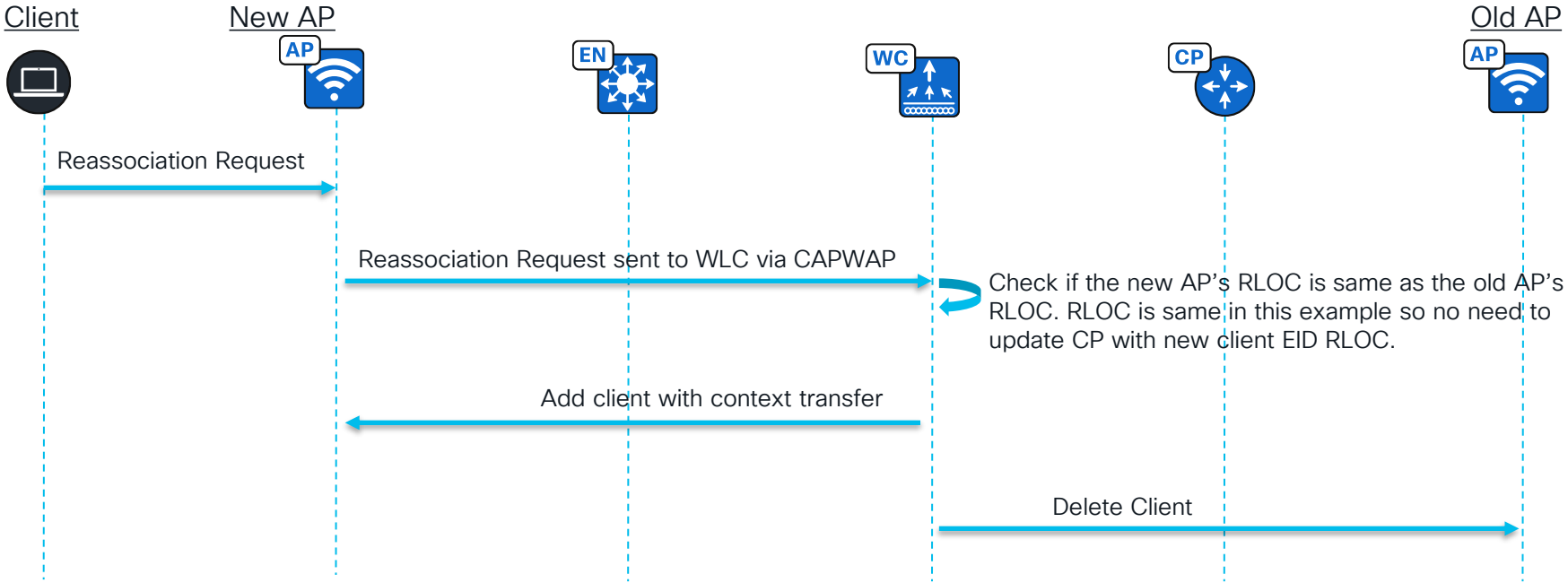
Fabric Enabled Wireless Roaming



cisco Live!

Fabric Enabled Wireless roaming

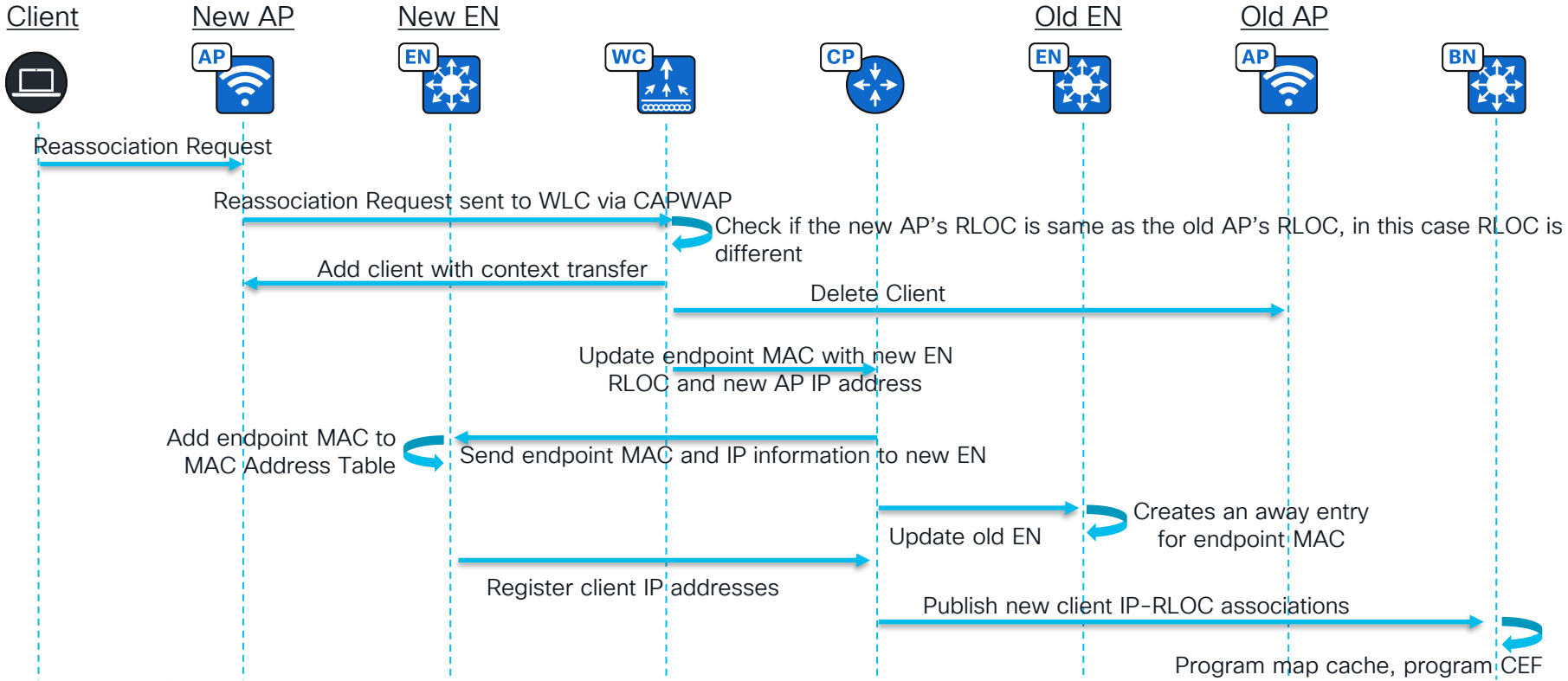
Between APs on same Edge Node



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric Enabled Wireless roaming

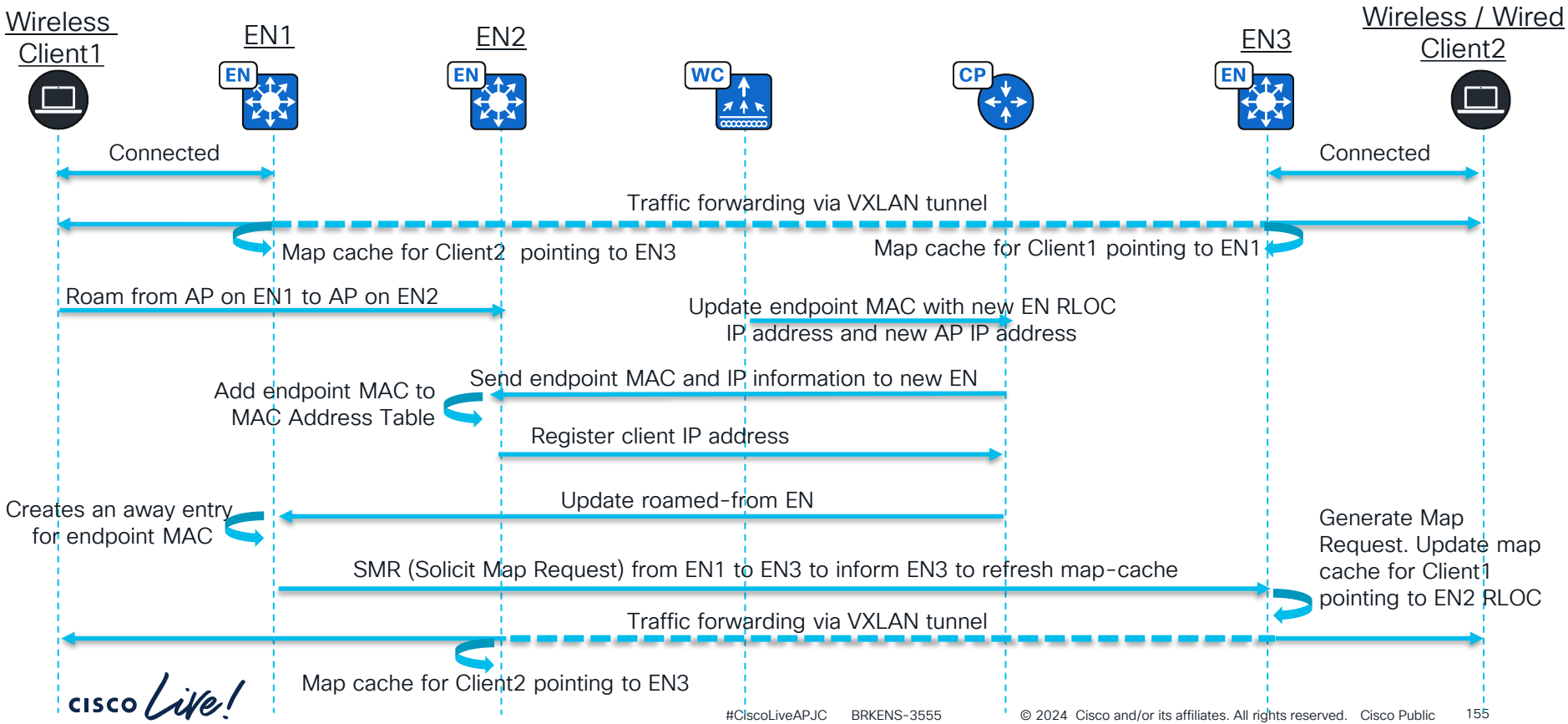
Between APs on different Edge Nodes



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

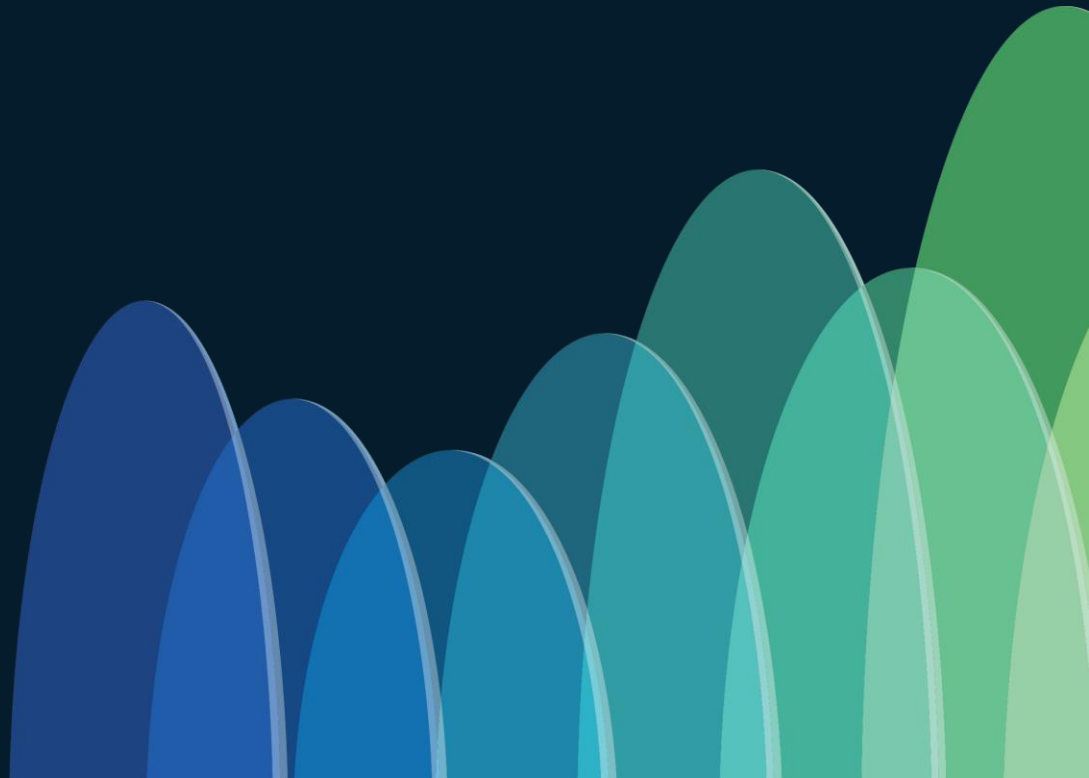
Fabric Enabled Wireless roaming

Roaming and traffic convergence



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

First Hop Security



cisco Live!

Switch Integrated Security Features

- SISF was architected to enhance security for Layer 2 domains. It's used by IOS XE switches and WLCs, NXOS and ACI.
- SD-Access uses a subset of SISF capabilities.
- Fundamental to SISF is Device Tracking which detects and tracks what is connected to a Layer 2 domain. In the context of SD-Access, Device Tracking applies to Edge Nodes and Extended Nodes.
- Device Tracking database is populated by gleaning packets from endpoints e.g. DHCP, ARP, ND, data.

```
EN1#show device-tracking database
Binding Table has 8 entries, 4 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet,
API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
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        state      Time left
DH4 10.255.255.254                         000c.290a.cbb8         Gi1/0/24   1024       0024       177s       REACHABLE  70 s try 0(2346 s)
ND  FE80::20C:29FF:FE0A:CBB8               000c.290a.cbb8         Gi1/0/24   1024       0005       123s       REACHABLE  119 s try 0
L   10.255.255.1                          0000.0c9f.f2fd         Vl1024     1024       0100       6019mn     REACHABLE
L   10.4.3.1                              0000.0c9f.f78f         Vl1022     1022       0100       6073mn     REACHABLE
DH4 10.4.3.237                             bcec.4341.d25f         Ac1        1022       0024       74s        REACHABLE  175 s(3463 s)

EN1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SISF is fundamental to SD-Access security

- In SD-Access SISF protects against:
  - Anycast Gateway MAC and IP theft as of IOS XE 17.9
  - Endpoint MAC and IP theft as of IOS XE 17.9
  - IP spoofing
  - IP address exhaustion (sets a maximum of IPs per MAC)
  - Rogue IPv6 DHCP Servers and Router Advertisements
- These protections are implemented by Device Tracking Policies and other SISF features.
  - A Device Tracking Policy is either manual (CLI) or programmatic (implemented by a feature e.g. LISP, DHCP Snooping, etc.)
  - Manual policy overrides programmatic and port policy overrides VLAN. For IP per MAC limit “preference high” is prioritized and then the most restrictive value it prioritized

```
EN2#show device-tracking policies
Target               Type  Policy               Feature                   Target range
Gi1/0/1              PORT  IPDT_POLICY          Device-tracking           vlan all
...
Gi1/0/24             PORT  IPDT_POLICY          Device-tracking           vlan all
vlan 1021            VLAN  DT-PROGRAMMATIC      Device-tracking           vlan all
vlan 1021            VLAN  LISP-DT-GLEAN-VLAN   Device-tracking           vlan all
vlan 1021            VLAN  LISP-AR-RELAY-VLAN   Address Resolution Relay  vlan all
vlan 1022            VLAN  DT-PROGRAMMATIC      Device-tracking           vlan all
vlan 1022            VLAN  LISP-DT-GUARD-VLAN   Device-tracking           vlan all
vlan 1023            VLAN  DT-PROGRAMMATIC      Device-tracking           vlan all
vlan 1023            VLAN  LISP-DT-GUARD-VLAN-MULTI-IP Device-tracking    vlan all
EN1#
```

Manual

Programmatic

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Common SD-Access Device Tracking polices

```
EN1#show device-tracking policy IPDT_POLICY
Device-tracking policy IPDT_POLICY configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
```

```
EN1#show device-tracking policy DT-PROGRAMMATIC
Device-tracking policy DT-PROGRAMMATIC configuration:
  security-level glean
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1
  tracking (downlink only) enable
```

```
EN1#show device-tracking policy LISP-DT-GUARD-VLAN-MULTI-IP
Device-tracking policy LISP-DT-GUARD-VLAN-MULTI-IP configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1000 preference high
  limit address-count for IPv6 per mac 1000
  origin fabric
  tracking enable reachable-lifetime 240
```

```
EN1#show device-tracking policy LISP-DT-GUARD-VLAN
Device-tracking policy LISP-DT-GUARD-VLAN configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4
  limit address-count for IPv6 per mac 12
  origin fabric
  tracking enable reachable-lifetime 240
```

```
EN1#show device-tracking policy LISP-DT-GLEAN-VLAN
Device-tracking policy LISP-DT-GLEAN-VLAN configuration:
  security-level glean
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4
  limit address-count for IPv6 per mac 12
  origin fabric
  tracking enable reachable-lifetime 240
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device Tracking guard and glean

Guard. Device Tracking extracts and verifies the IP and MAC address of packets entering the network. Packets that violate policy are dropped.

```
EN1#show device-tracking policy LISP-DT-GUARD-VLAN
Device-tracking policy LISP-DT-GUARD-VLAN
configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4
  limit address-count for IPv6 per mac 12
  origin fabric
  tracking enable reachable-lifetime 240
```

Glean. Device Tracking extracts the IP and MAC address of packets entering the network but does not perform IP and MAC theft/spoofing checks.

```
EN1#show device-tracking policy LISP-DT-GLEAN-VLAN
Device-tracking policy LISP-DT-GLEAN-VLAN
configuration:
  security-level glean
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4
  limit address-count for IPv6 per mac 12
  origin fabric
  tracking enable reachable-lifetime 240
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example 1

- A wired endpoint connected to VLAN 1022 on G1/0/24 is subject to these four:

```
EN1#show device-tracking policies interface g1/0/24
Target               Type  Policy               Feature                  Target range
Gi1/0/24             PORT  IPDT_POLICY          Device-tracking          vlan all
EN1#show device-tracking policies vlan 1022
Target               Type  Policy               Feature                  Target range
vlan 1022            VLAN  DT-PROGRAMMATIC      Device-tracking          vlan all
vlan 1022            VLAN  LISP-DT-GUARD-VLAN   Device-tracking          vlan all
vlan 1022            VLAN  LISP-AR-RELAY-VLAN   Address Resolution Relay  vlan all
EN1#
```

- Adding it all up that means:

```
security-level guard
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP6
gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
tracking enable
limit address-count for IPv4 per mac 1
limit address-count for IPv6 per mac 12
```

Manual, from IPDT_POLICY on G1/0/24 interface

Programmatic, from DT-PROGRAMMATIC

Programmatic, from LISP-DT-GUARD-VLAN

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example 2

- A wireless endpoint connected to VLAN 1022 is subject to these three:

```
EN1#show device-tracking policies vlan 1022
Target               Type  Policy               Feature                  Target range
vlan 1022            VLAN  DT-PROGRAMMATIC      Device-tracking          vlan all
vlan 1022            VLAN  LISP-DT-GUARD-VLAN   Device-tracking          vlan all
vlan 1022            VLAN  LISP-AR-RELAY-VLAN   Address Resolution Relay  vlan all
EN1#
```

- Adding it all up that means:

```
security-level guard
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP6
gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
tracking enable
limit address-count for IPv4 per mac 1
limit address-count for IPv6 per mac 12
```

Programmatic, from LISP-DT-GUARD-VLAN

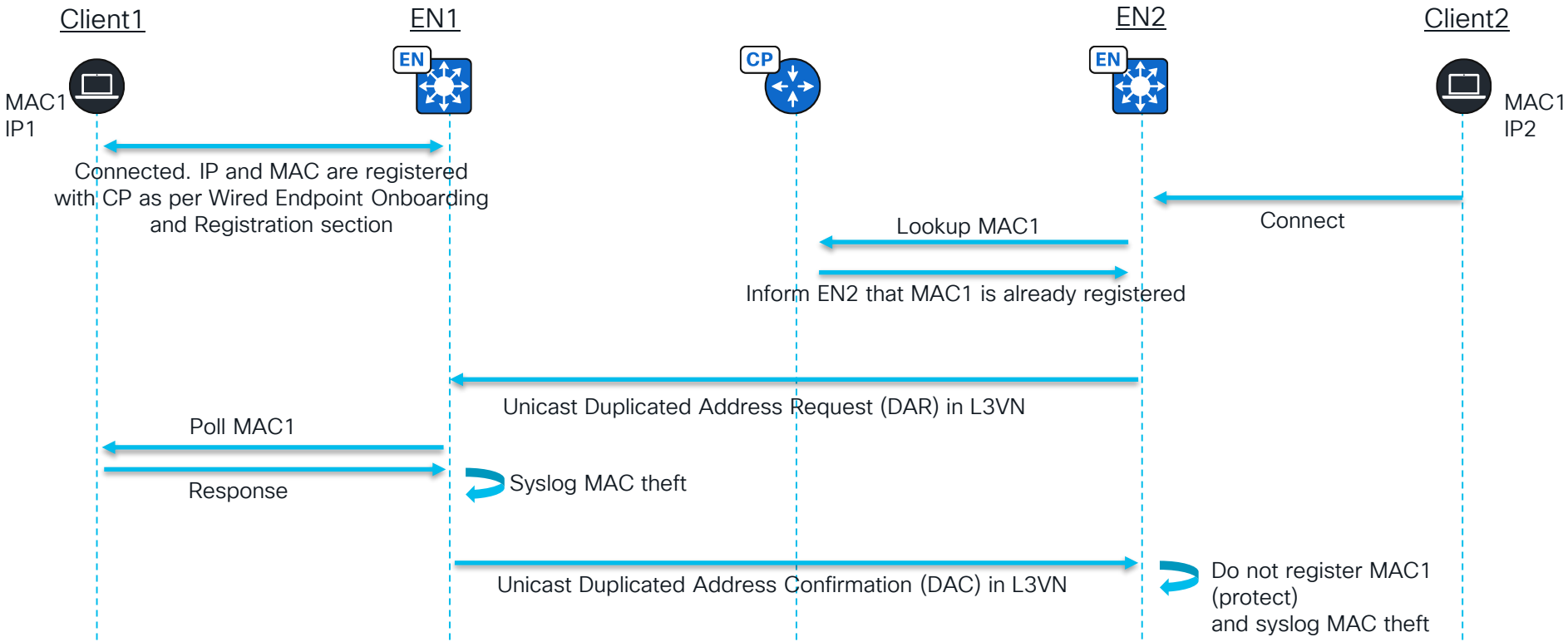
Programmatic, from LISP-DT-GUARD-VLAN

Programmatic, from DT-PROGRAMMATIC

Programmatic, from LISP-DT-GUARD-VLAN

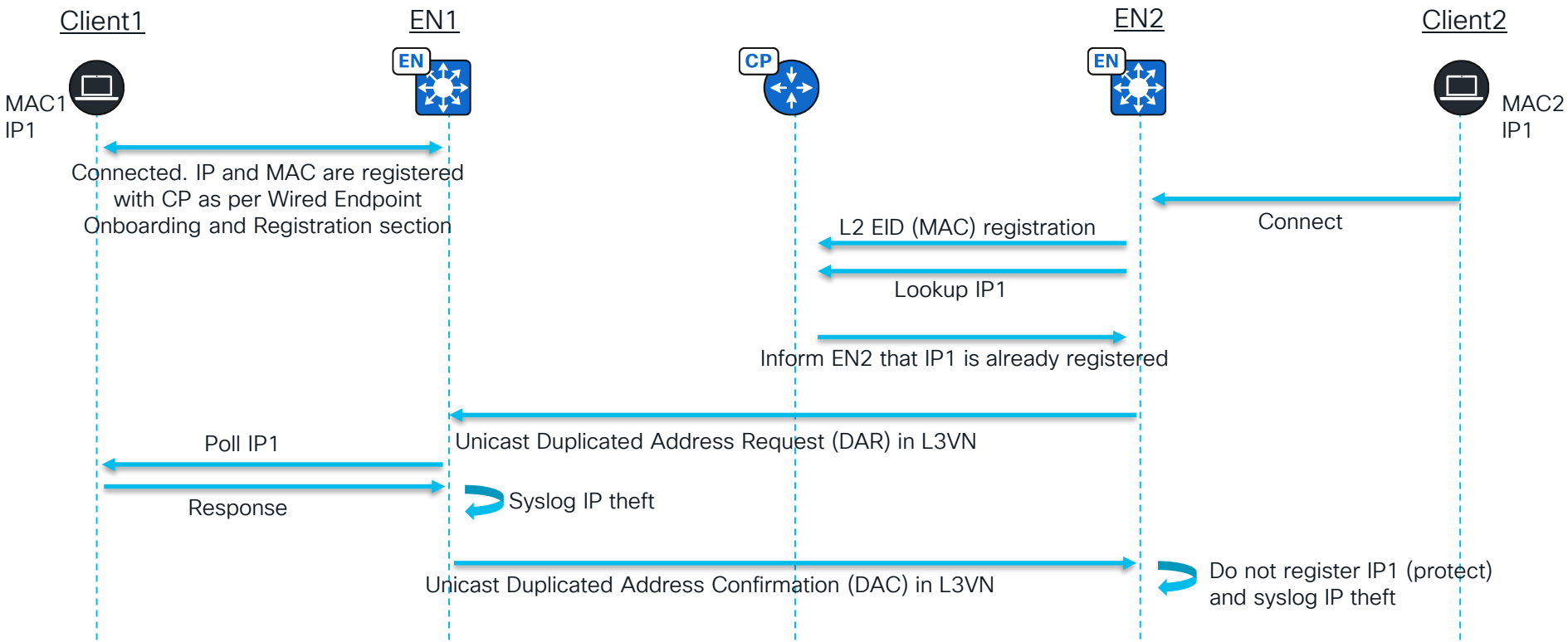
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device Tracking guard and MAC theft



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device Tracking guard and IP theft



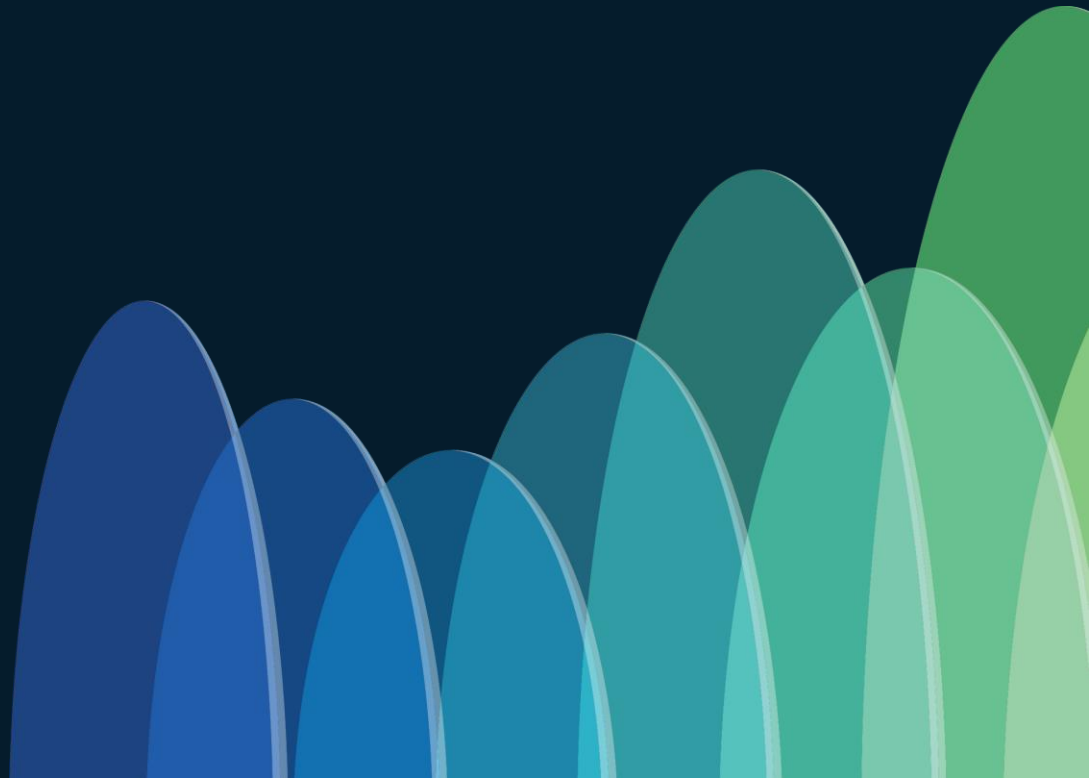
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device Tracking guard on Fabric-Enabled Wireless

- Fabric WLC provides MAC integrity.
- Using the same principles just shown, Device Tracking protects against IP theft and spoofing.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion



Conclusion

- LISP pulls only necessary routing information into the network access layer. Pull-based routing enables:
  - Resource optimization on Edge Nodes for scale and performance.
  - Fabric switching at the very network edge, including switches traditionally in L2 mode e.g. 9200, 9200CX, IE9300, and more in future.
  - A true end-to-end routed network foundation (underlay), no L2, no fragility associated with L2.
  - A common data plane for greater wireless throughput and scale compared to centrally switched and locally switched wireless.
- SD-Access natively implements a range of First Hop Security functions.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

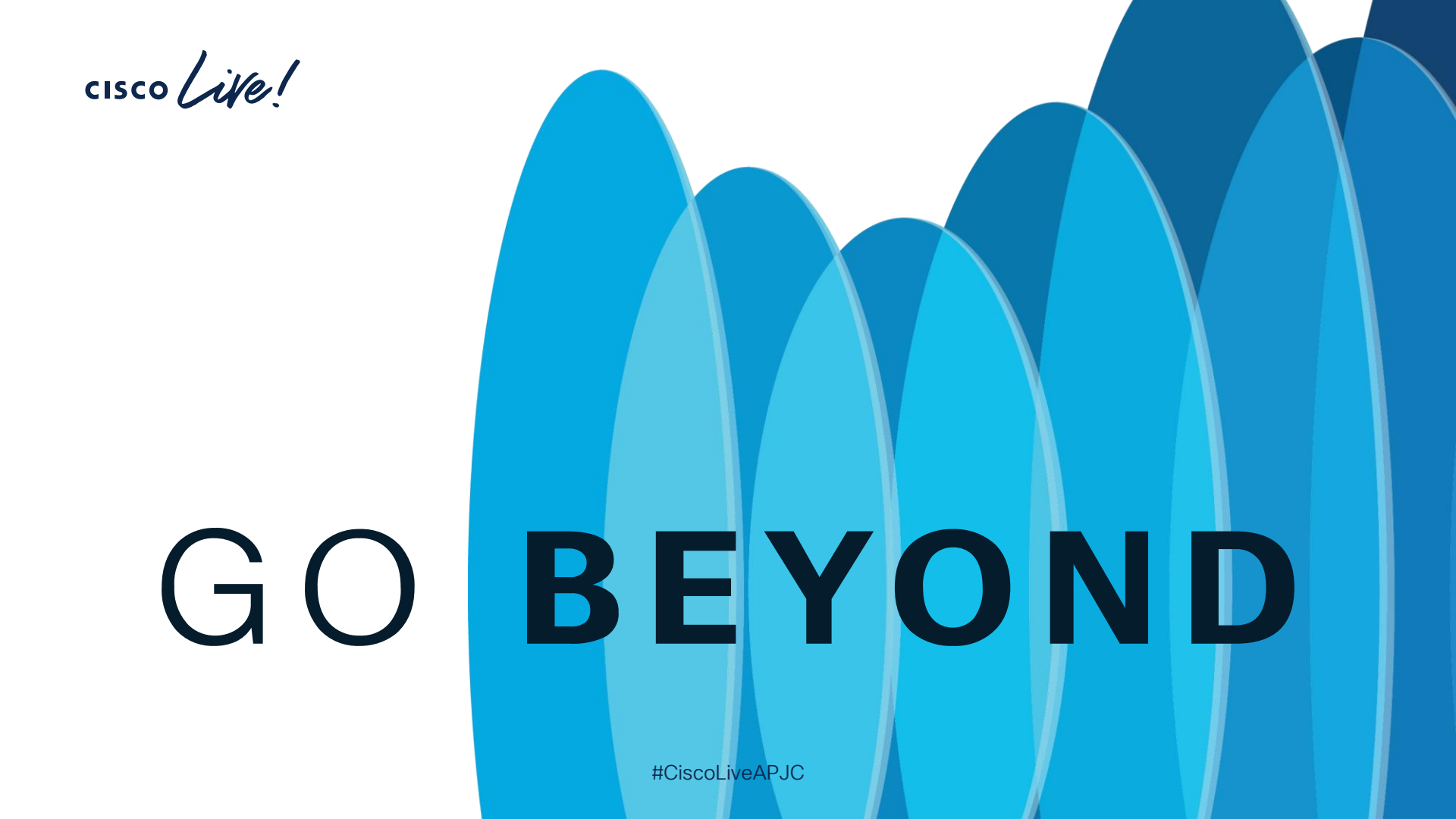
Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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

Contact me: Webex jedolphin@cisco.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC