
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Understanding and Troubleshooting Cisco SD-Access Layer 2 Virtual Network

Cheeho Yan, Sr. Technical Leader
Howard Haifeng Zhang, TAC Technical Leader

BRKTRS-2000

Cisco Webex App

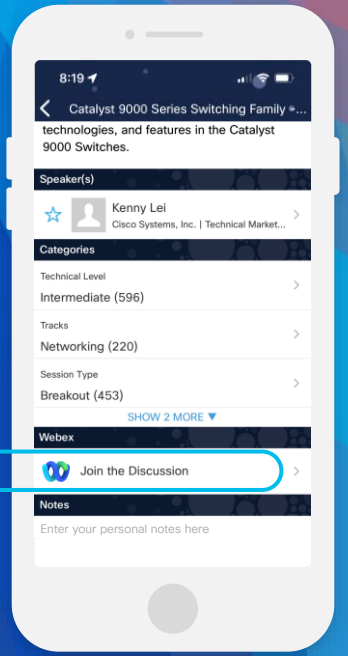
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKTRS-2000

Who is Cheeho?

- Based in San Jose, US
- Joined Cisco in 2000
- Has focused on IBN/SD-Access since 2017
- Enjoys drawing, painting, and exploring national parks
- Degrees in architecture

CCIE #5575, R&S, Security

Enabling Services to Meet Business Needs

Go-Kart Tracks

Free-fall Drop Slides

Business Requirement & Solution

You have deployed or about to deploy SD-Access. You now have one of these new requirements:

- Endpoint entries into the network need to be controlled by a firewall outside the fabric
- Communication between endpoints in different VLANs inside the fabric needs to be inspect by a firewall for compliance
- Venders inside the fabric need to be in their private networks

Solution

Layer 2 Virtual Network

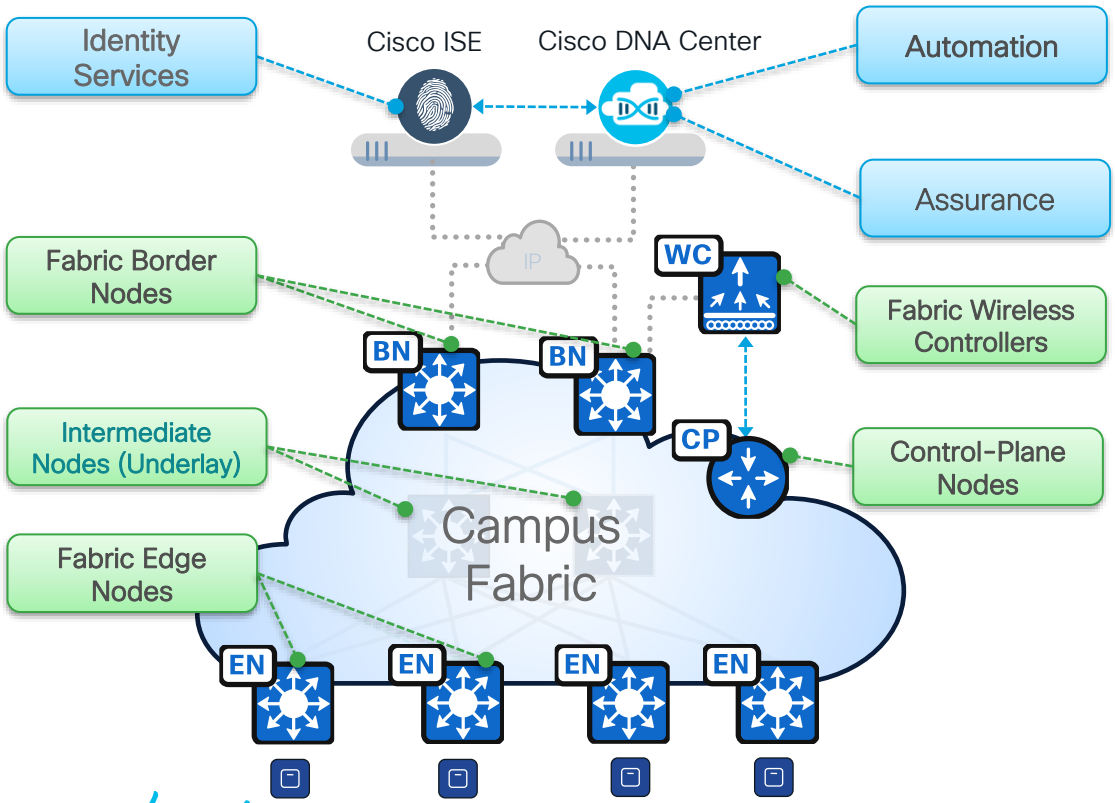
(Gateway Outside the Fabric)

Agenda

- Understanding Layer 2 Virtual Network
- Same Segment Forwarding without Flooding
- Same Segment Forwarding with Flooding
- Configuring Layer 2 Virtual Network
- Troubleshooting
- IP-Directed Broadcast
- Design and Implementation Best Practices

Understanding Layer 2 Virtual Network

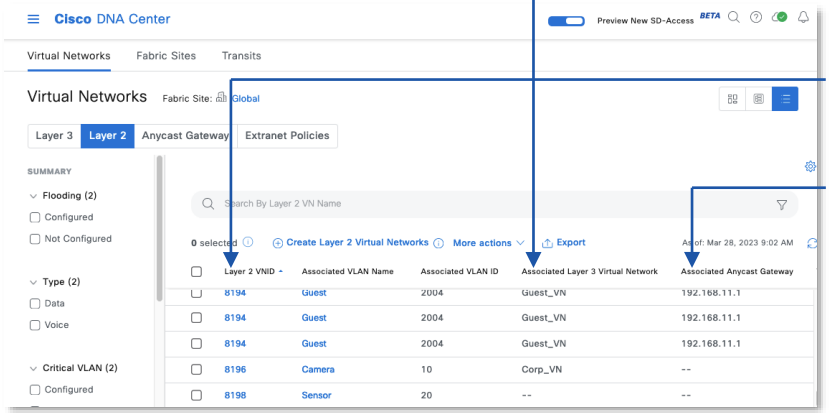
SD-Access Fabric Roles



- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric network status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition

- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

Terminology



L3 VN – Layer 3 Virtual Network, analogous to a VRF in SD-Access

L2 VN – Layer 2 Virtual Network, a virtual switching domain in SD-Access. It is analogous to a VLAN in a traditional network

VNI – Virtual Network Identifier (VXLAN)

L3 VNI - Layer 3 Virtual Network Identifier; as used in SD-Access fabric, a VRF

L2 VNI - Layer 2 Virtual Network Identifier; as used in SD-Access fabric, a VLAN

Anycast L3 Gateway – A common gateway used at Edge nodes. It is instantiated as a Switched Virtual Interface (SVI)

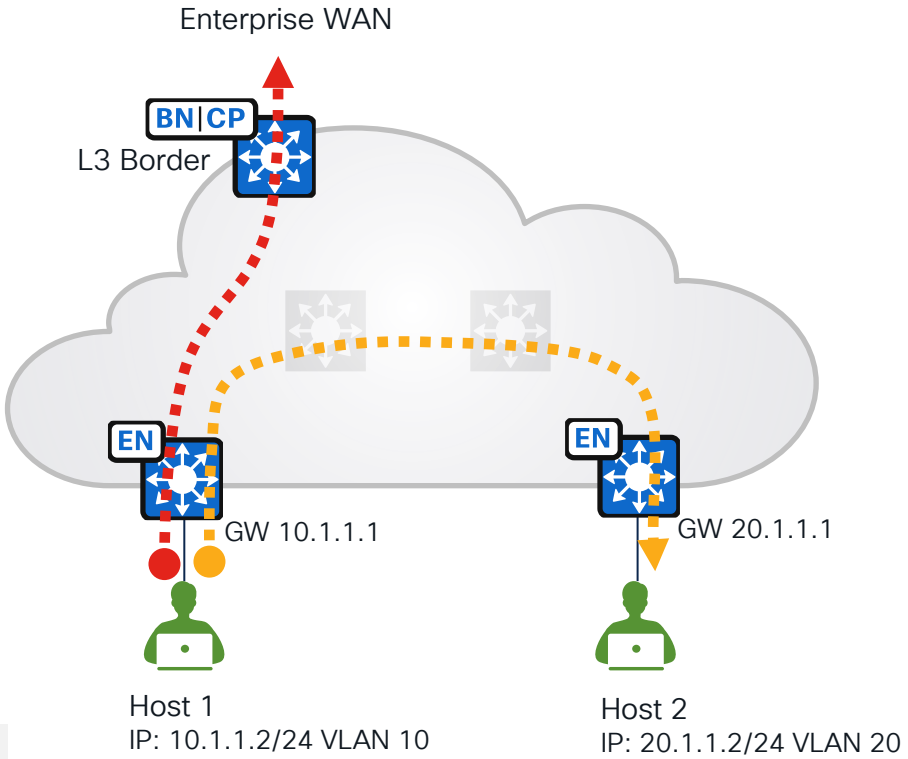
RLOC – Routing Locator (LISP)

Silent Host – A Device that does not announce their presence to the network

Sleeping Host – A Device that can move into power-save mode

Layer 3 Virtual Network

- Anycast gateway for the endpoints is on the Edges (SVI)
- Anycast gateway config is automated
- Traffic towards WAN passes through L3 Border(s)
- IP address pools are defined in Cisco DNA Center
- Unless configured, L2 flooding is disabled and broadcast, unknow unicast, and multicast (BUM) traffic is not flooded across fabric



Typical Use Cases

- Typical client segments in enterprise networks

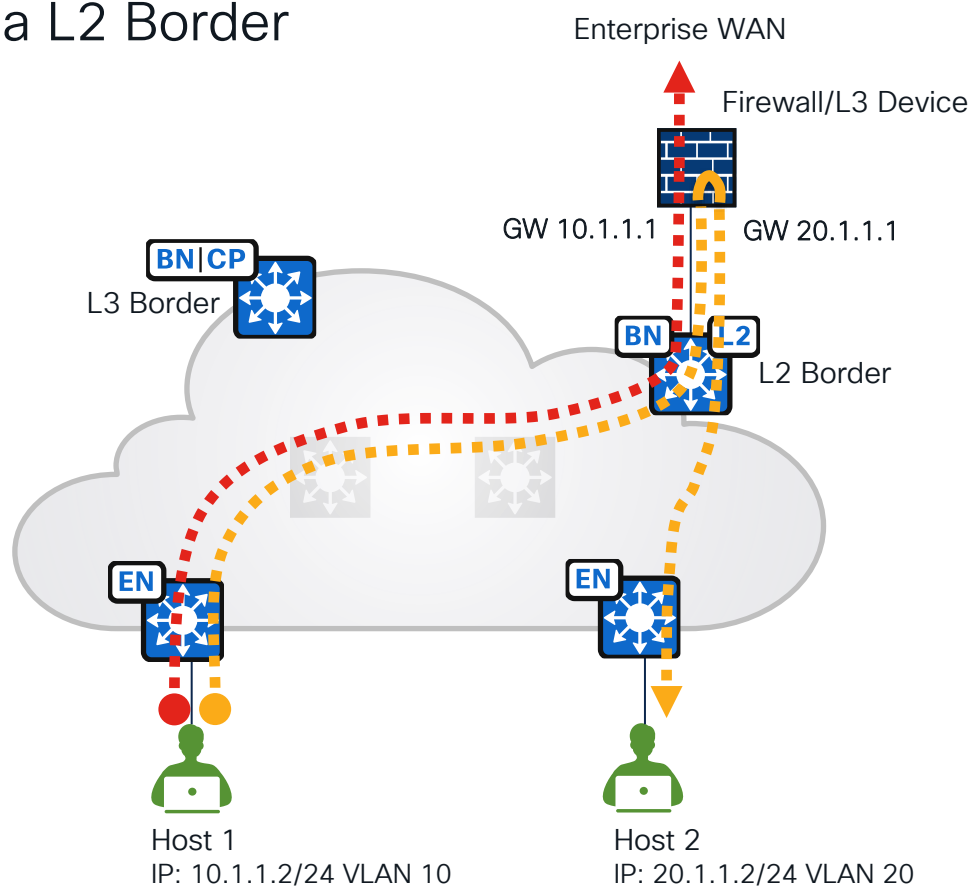
Layer 2 Virtual Network

Gateway Outside the Fabric with a L2 Border

- Gateway for the subnets can be a firewall or a L3 device connected to a L2 Border
- Gateway configs are not covered by Cisco DNA Center
- Traffic towards enterprise WAN passes through L2 Border(s)
- Firewall as the Gateway can inspect inter-VLAN and traffic exiting fabric
- L2 flooding is enabled hence BUM traffic is flooded across fabric

Typical Use Cases

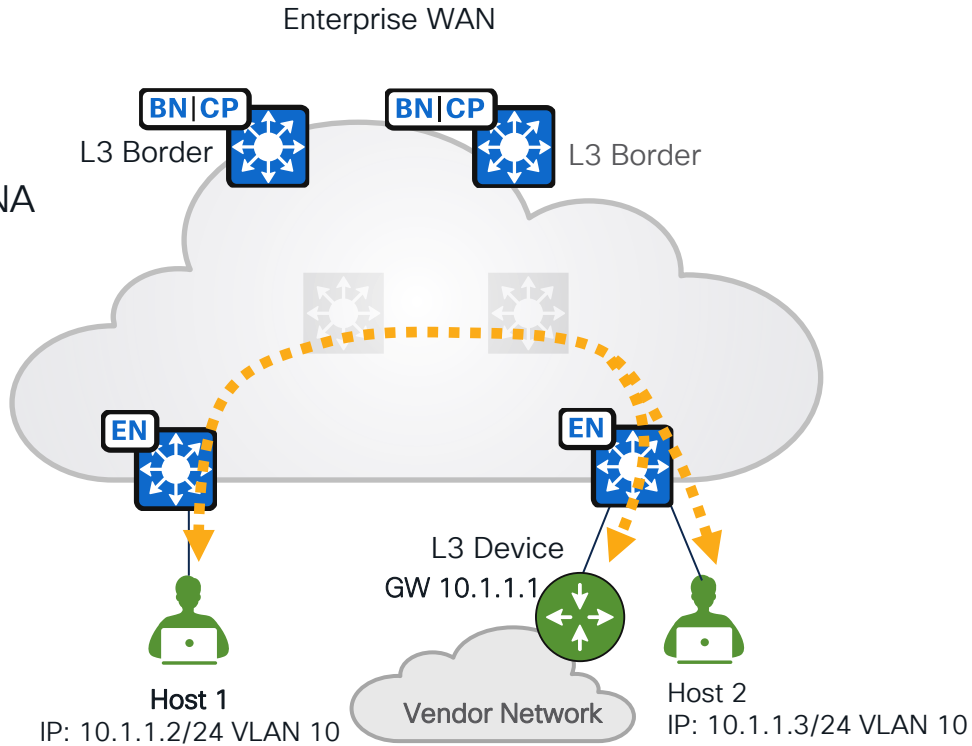
- OT (Operational Technology) segments
- IoT segments
- BMS (Building Management Systems) segments



Layer 2 Virtual Network

Gateway Outside the Fabric without a L2 Border

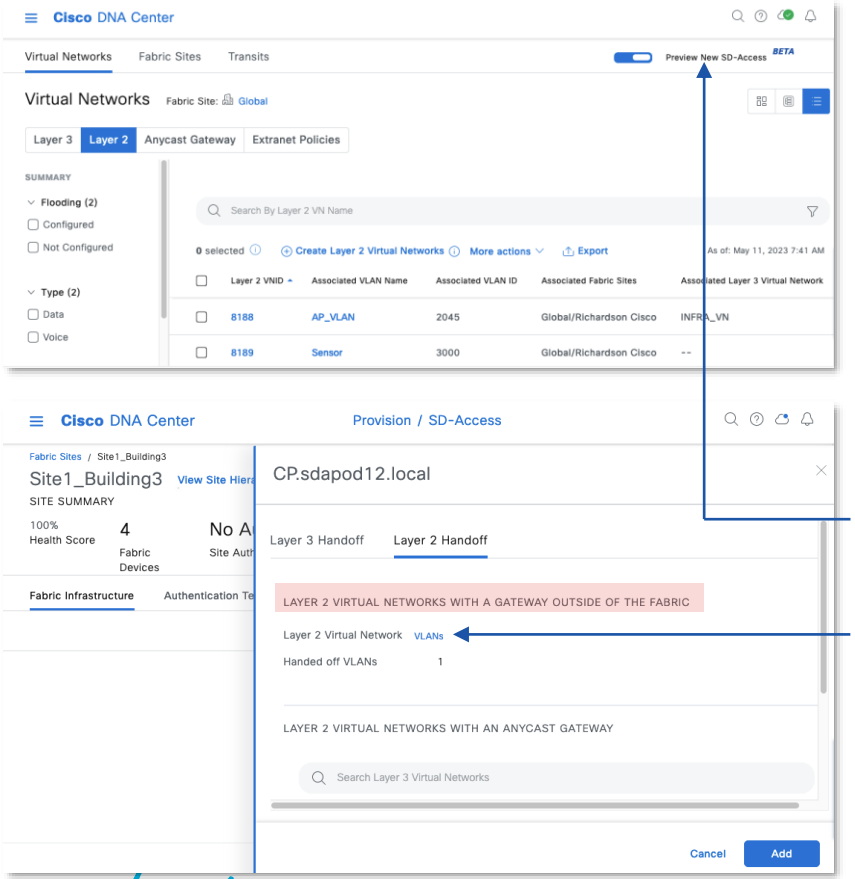
- Endpoint traffic does not exit to enterprise WAN
- A L2 Border is not required
- Vendors can optionally use a private Gateway connected to the Edge for their networks
- Gateway configs are not covered by Cisco DNA Center
- L2 flooding is enabled hence BUM traffic is flooded across fabric



Typical Use Cases

- Airport shop/restaurant segments
- Shopping mall store segments
- Trade show vendor segments

Layer 2 Virtual Network Feature Overview



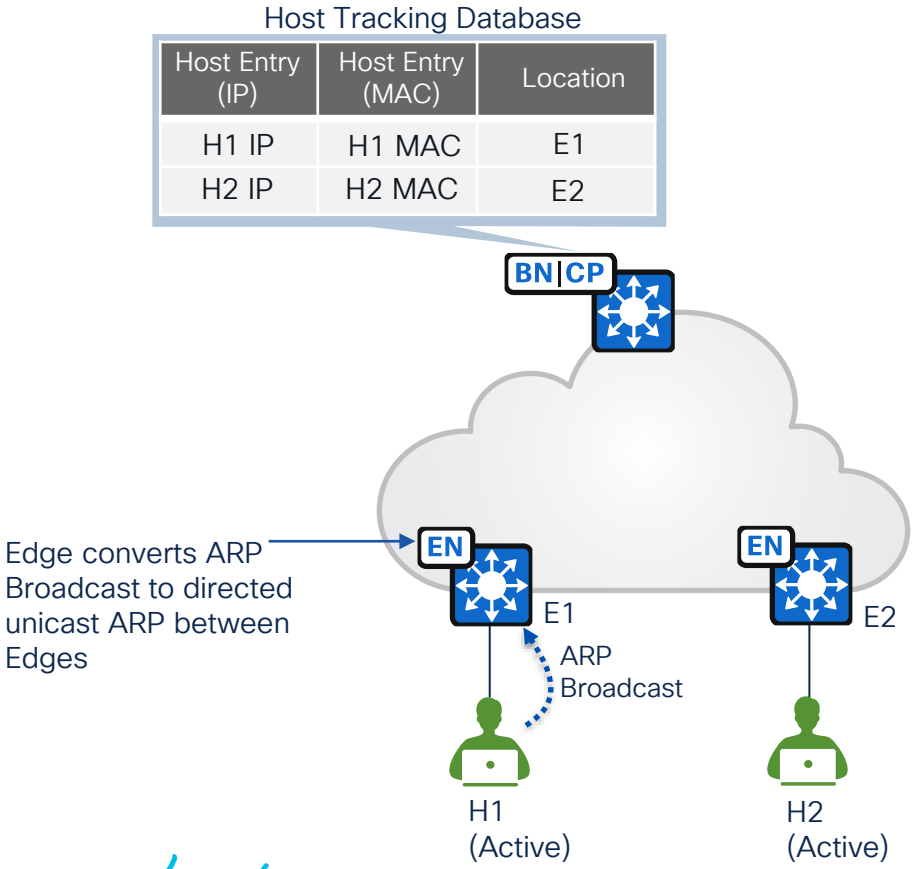
- Feature was introduced in Cisco DNA Center 2.3.3.x
- Wireless support was introduced in 2.3.5.x & IOS-XE 17.10.x
- Does not require a L3 VN
- Removes the overhead of L3 VN association
- Turn on “Preview New SD-Access” to start the L2 VN creation workflow
- VLAN is listed under “LAYER 2 VIRTUAL NETWORKS WITH A GATEWAY OUTSIDE OF THE FABRIC” during Border L2 handoff configuration

L3 VN and L2 VN Comparison

	Layer 3 Virtual Network	Layer 2 Virtual Network
VNI (Virtual Network Interface)	L3 VNI + L2 VNI	L2 VNI
Flooding of BUM traffic (by default)	No	Yes
Gateway	On the fabric Edge (SVI)	Outside the fabric / None
In-Fabric Inter-VLAN traffic and traffic exiting fabric inspected by firewall	No	Yes (When FW is used as gateway)
IP address pools configured in Cisco DNA Center	Yes	No
Same subnet/VLAN endpoint Scale	Very scalable	Number of endpoints in a L2 VN should be limited
Use Cases	Suitable for segments for most enterprise deployments	• Private isolated VLANs • Broadcast is required in a VLAN • Gateway needs to be on the firewall

Same Segment Forwarding without Flooding

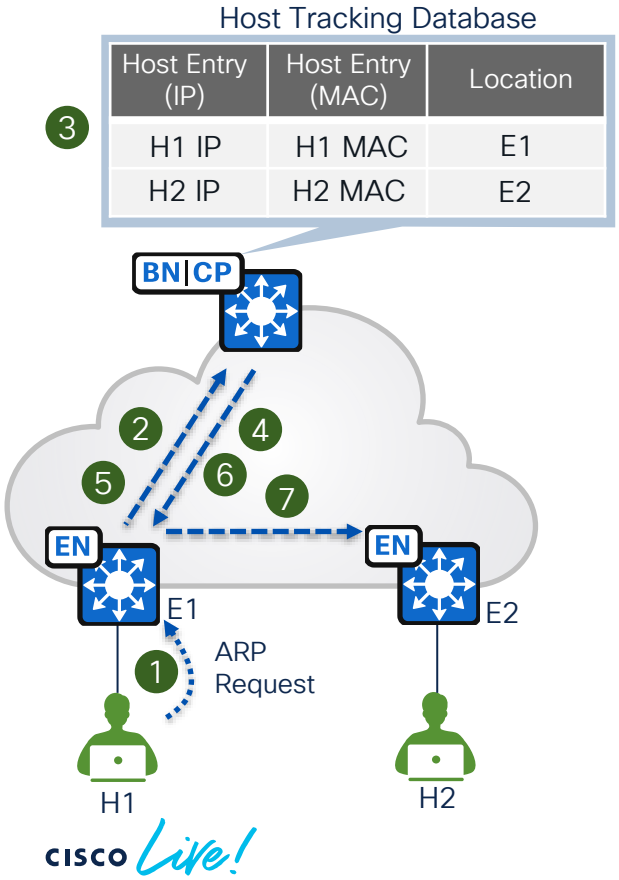
Forwarding without Flooding



- Typical in unicast endpoint communication in L3 VN segments as well
- Control Plane node keeps track of active hosts' MAC and IP addresses in the Host Tracking Database for forwarding
- Edge suppresses broadcasts
- BUM traffic is not flooded

Packet Flow

H1 Communication with H2



1. H1 sends ARP request broadcast for H2's MAC address
2. E1 intercepts ARP broadcast and contacts CP for H2's address
3. CP finds H2's MAC to IP binding in its host tracking database
4. CP replies to E1 with H2's MAC address
5. E1 gets H2's MAC address and consults CP for the location of H2
6. CP replies with H2's location information. E1 installs H2 into its MAP-cache
7. E1 coverts ARP broadcast from H1 to a directed unicast and sends it to E2 in the overlay encapsulating it with the L2 VNI

Assumptions:

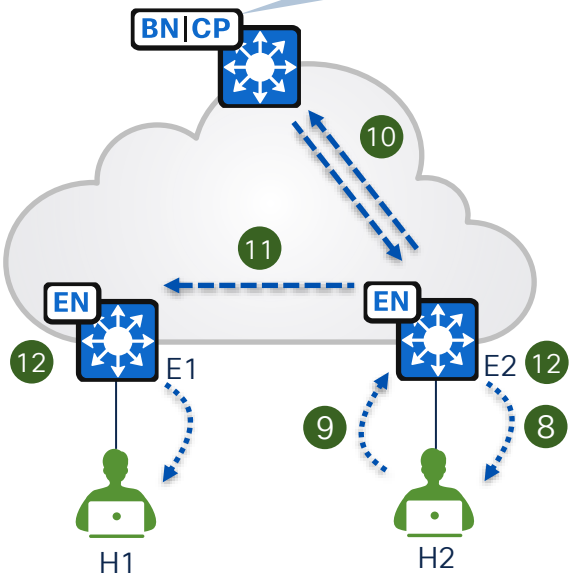
- Edges do not have remote endpoints in their MAP-cache nor MAC tables initially
- Control Plane node has H1 and H2 in its host tracking database

Packet Flow

H1 Communication with H2

Host Tracking Database

Host Entry (IP)	Host Entry (MAC)	Location
H1 IP	H1 MAC	E1
H2 IP	H2 MAC	E2

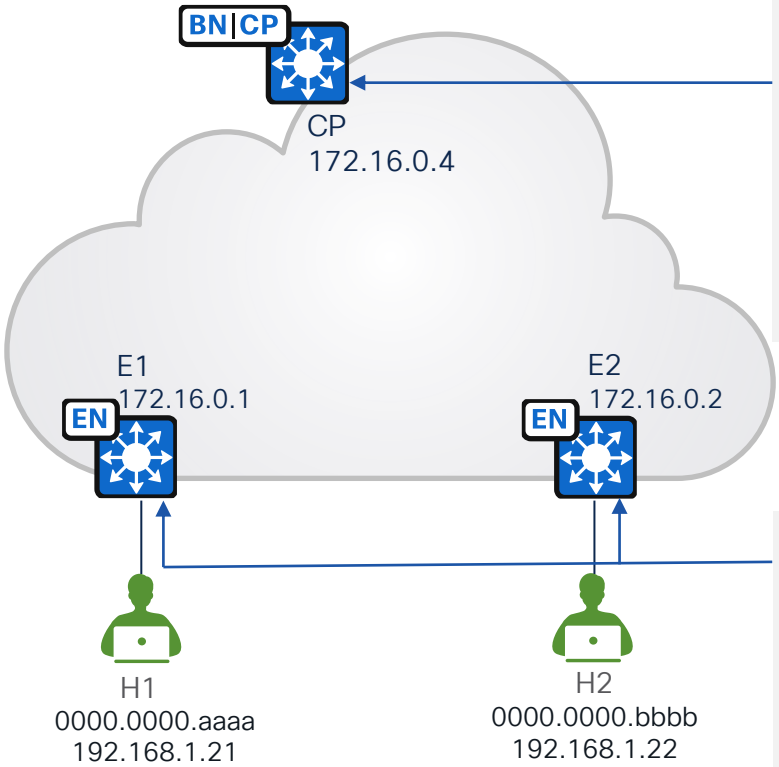


8. E2 decapsulates the ARP request and forwards it to H2
9. H2 unicasts the ARP response for H1 to E2
10. E2 requests and receives from CP the location of H1. E2 installs H1 into its MAP-cache
11. E2 sends the ARP response to E1. E1 forwards it to H1
12. E1 and E2 use their MAP-cache and the L2 VNI to forward to destination nodes

Assumptions:

- Edges do not have remote endpoints in their MAP-cache nor MAC tables initially
- Control Plane node has H1 and H2 in its host tracking database

Initial State



Control Plane has in its host tracking database the IP & MAC addresses of the active endpoints and RLOCs

```
CP#show lisp instance-id 8191 ethernet server
Site Name Last       Up     Who Last          Inst EID Prefix
          Register          Registered        ID
site_uci  never      no     --                8191 any-mac
          00:00:47   yes#   172.16.0.1:31397  8191 0000.0000.aaaa/48
          00:01:10   yes#   172.16.0.2:24161  8191 0000.0000.bbbb/48

CP#show lisp instance-id 8191 ethernet server address
L3 InstID    Host Address         Hardware Address
     4099    192.168.1.21/32      0000.0000.aaaa
     4099    192.168.1.22/32      0000.0000.bbbb
```

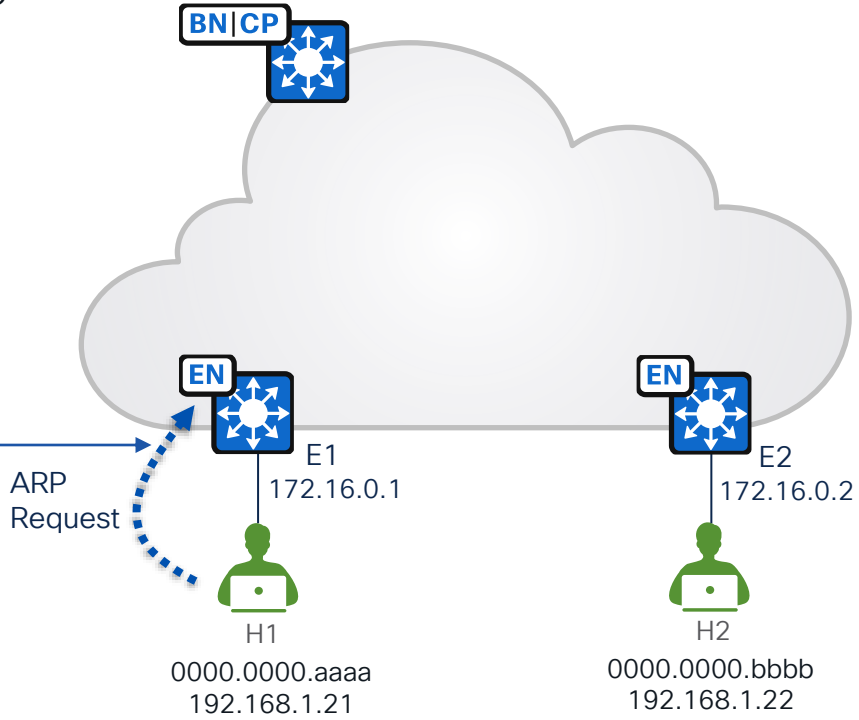
Edges only have the directed connected endpoints in its local database

```
E1#show device-tracking database
    Network Address Link Layer Address Interface  vlan   age     state      Time
DH4 192.168.1.21    0000.0000.aaaa     Te1/0/23   1191   146s    REACHABLE 105s
L   192.168.1.1     0000.0c9f.f8a0     Vl1191     1191   1500mn REACHABLE


E2#show device-tracking database
    Network Address Link Layer Address Interface  vlan   age      state      Time
ARP 192.168.1.22    0000.0000.bbbb     Gi1/0/47   1191   125s     REACHABLE 126s
L   192.168.1.1     0000.0c9f.f8a0     Vl1191     1191   1291mn   REACHABLE
```

1. H1 wants to communicate to H2. Since they are in the same subnet, H1 sends ARP request broadcast for the MAC address of H2

```
E1#debug arp snooping
Arp Snooping debugging is on

Apr  7 09:00:49.619:
ARP Packet (Te1/0/23/1191)
Src: 0000.0000.aaaa,
Dst: ffff.ffff.ffff,
SM: 0000.0000.aaaa,
SI: 192.168.1.21,
TM: 0000.0000.0000,
TI: 192.168.1.22
```

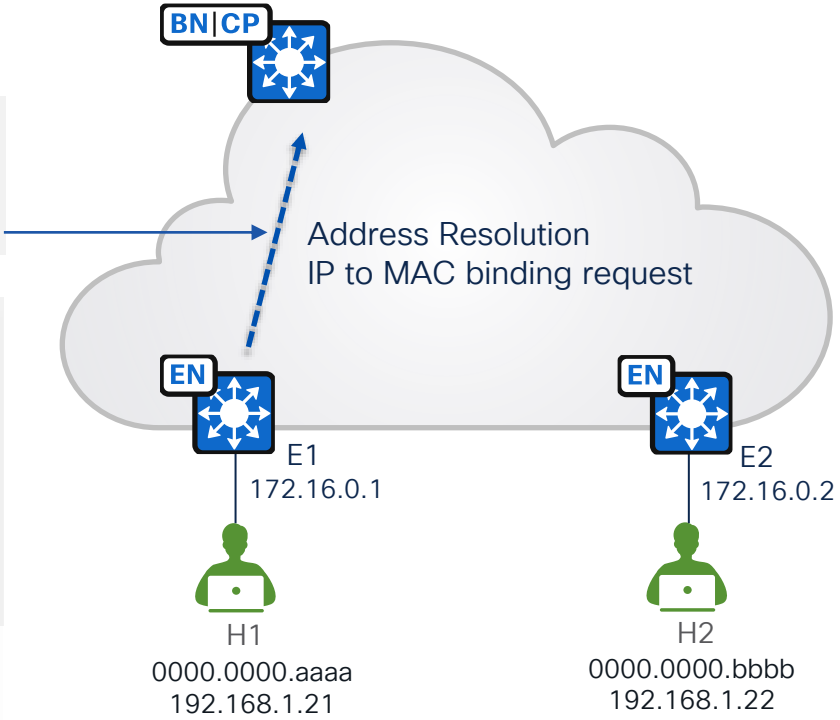
```
▷ Ethernet II, Src: 00:00:00:00:aa:aa, Dst: ff:ff:ff:ff:ff:ff
◢ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:00:00:00:aa:aa
    Sender IP address: 192.168.1.21
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 192.168.1.22
```



2 E1 intercepts the ARP broadcast and contacts Control Plane node for MAC address of H2

```
E1#debug lisp control-plane map-cache

LISP[REMT ]-0: Map Request: Sending request for IID 8191 EID
               192.168.1.22/32, requester 'AR'.
```

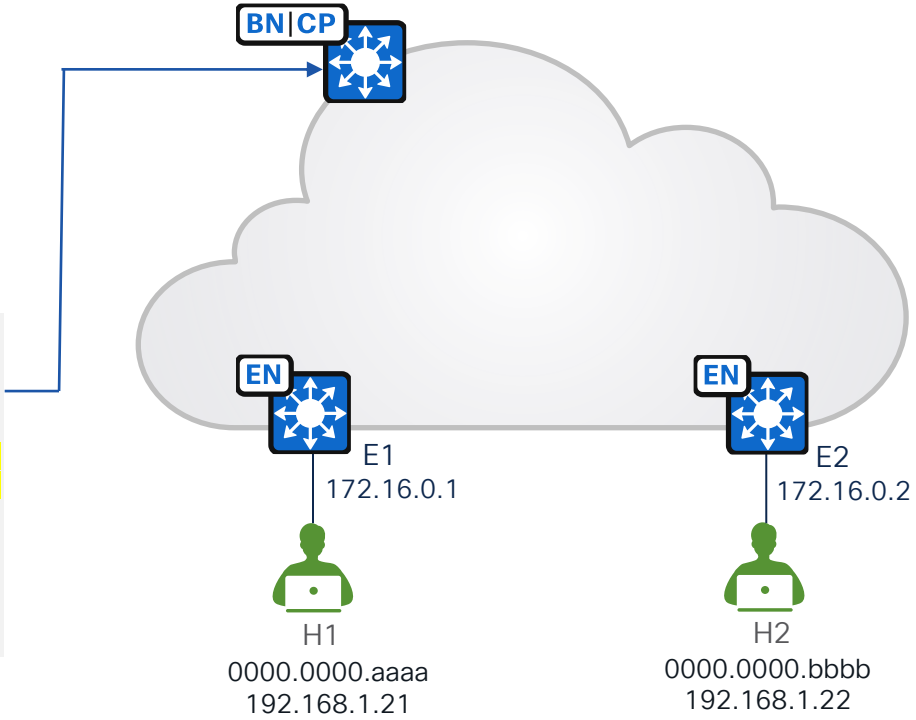
```
▷ Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.16.0.4
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
▷ Locator/ID Separation Protocol
▷ Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.22
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
◢ Locator/ID Separation Protocol
    0001 .... .... .... .... .... = Type: Map-Request (1)
  ▷ .... 0000 00.. .... .... .... = Flags: 0x00
    .... .... ..00 0000 000. .... = Reserved bits: 0x000
    .... .... .... .... ...0 0000 = ITR-RLOC Count: 0
    Record Count: 1
    Nonce: 0xc006a6cd3b58983c
    Source EID AFI: Reserved (0)
    Source EID: not set
  ▷ ITR-RLOC 1: 172.16.0.1
  ▷ Map-Request Record 1: Unknown LCAF Type (53)/32
```



3 Control Plane node consults its Host Tracking Database and finds the IP to MAC binding for H2

Control Plane State

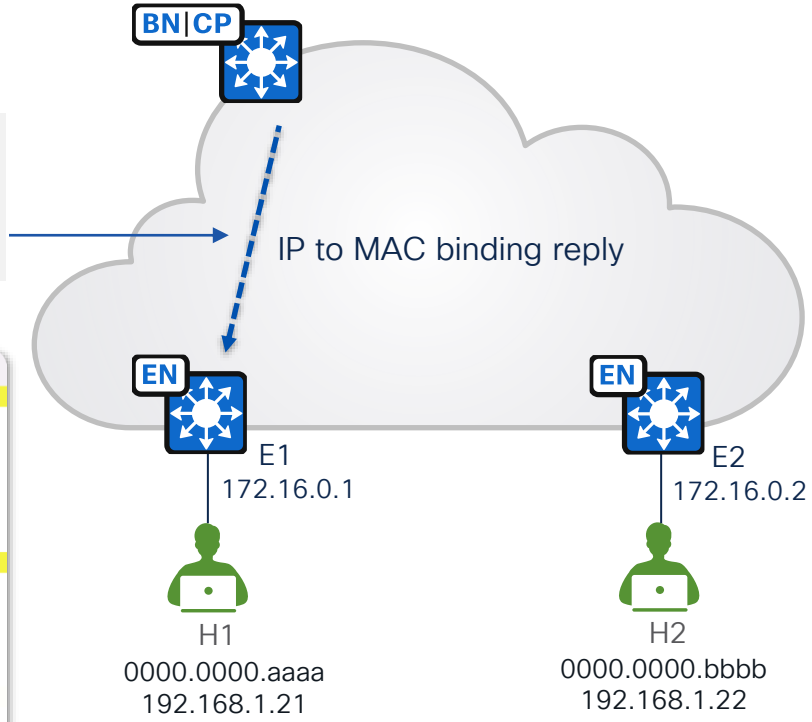
```
CP#show lisp instance-id 8191 ethernet server
Site Name Last      Up     Who Last         Inst EID Prefix
          Register         Registered       ID
site_uci  never     no     --               8191 any-mac
          00:00:47  yes#   172.16.0.1:31397 8191 0000.0000.aaaa/48
          00:01:10  yes#   172.16.0.2:24161 8191 0000.0000.bbbb/48

CP#show lisp instance-id 8191 ethernet server address
L3 InstID    Host Address        Hardware Address
     4099    192.168.1.21/32     0000.0000.aaaa
     4099    192.168.1.22/32     0000.0000.bbbb
```



4 Control Plane node replies back to E1 with the MAC address of H2

```
CP#debug lisp control-plane map-resolver
LISP[MR   ]-0: Received Map-Request with 1 records, first EID IID 8191
192.168.1.22/32, source EID UNSPEC, nonce 0x33FFA302-0x81FB070D.
LISP[MR   ]-0 IID 8191 Eth-ARP: MS EID 192.168.1.22/32: Sending proxy reply to
172.16.0.1.
```

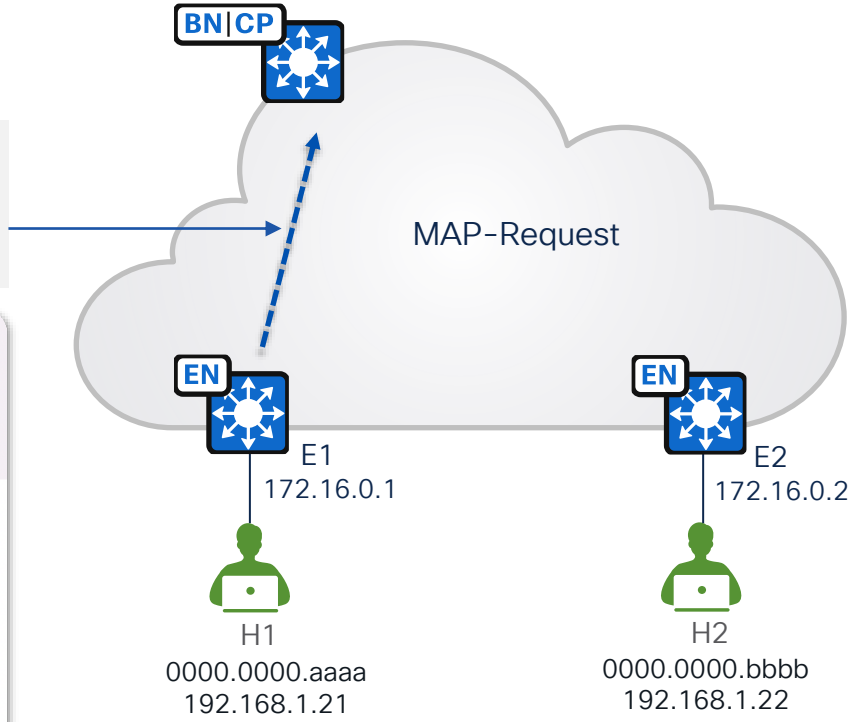
```
▷ Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.1
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
◢ Locator/ID Separation Protocol
    0010 .... .... .... .... .... = Type: Map-Reply (2)
    .... 0... .... .... .... .... = P bit (Probe): Not set
    .... .0.. .... .... .... .... = E bit (Echo-Nonce locator reachability algorithm enabled): Not set
    .... ..0. .... .... .... .... = S bit (LISP-SEC capable): Not set
    .... ...0 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0xdacf97ad005f4a87
  ◢ Mapping Record 1, EID Prefix: Unknown LCAF Type (53)/32, TTL: 1440, Action: No-Action, Not Authoritative
      Record TTL: 1440
      Locator Count: 1
      EID Mask Length: 32
      000. .... .... .... = Action: No-Action (0)
      ...0 .... .... .... = Authoritative bit: Not set
      .... .000 0000 0000 = Reserved: 0x000
      0000 .... .... .... = Reserved: 0x0
      .... 0000 0000 0000 = Mapping Version: 0
      EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    ▷ EID Prefix: Unknown LCAF Type (53)
    ▷ Locator Record 1, RLOC: 00:00:00:00:bb:bb, Unreachable, Priority/Weight: 1/100, Multicast Priority/Weight: 1/100
```



5 Once E1 gets the MAC address for H2, it again consults the Control Plane node on where H2 is located

```
E1#debug lisp control-plane map-cache
LISP[REMT ]-0 IID 8191: Schedule processing of Map-Requests from
              'remote EID prefix' in IPv4.
LISP[REMT ]-0: Map Request: Sending request for IID 8191
               EID 0000.0000.bbbb/48, requester 'remote EID prefix'.
```

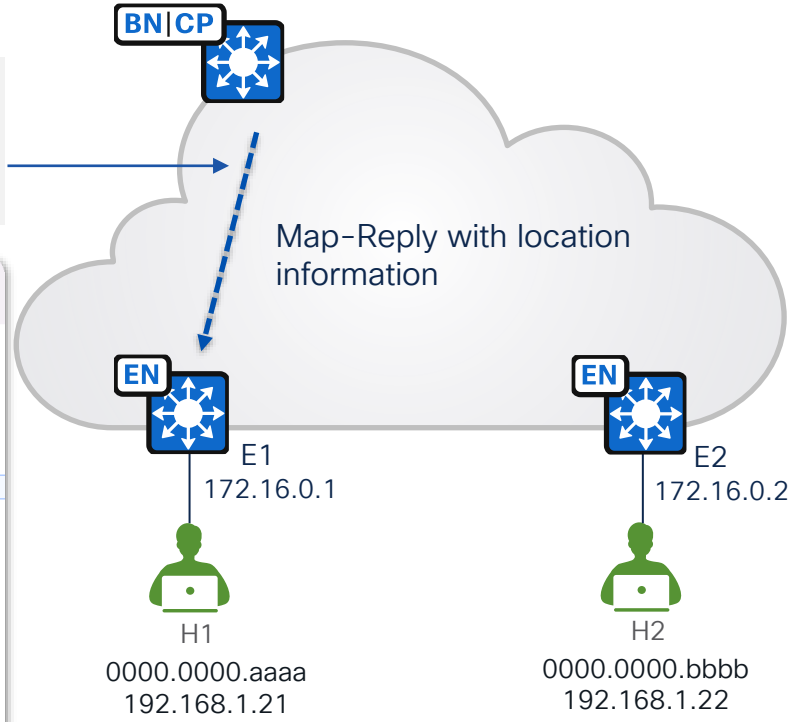
```
▷ Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.16.0.4
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
▷ Locator/ID Separation Protocol
▷ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 0.0.0.0
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
◢ Locator/ID Separation Protocol
    0001 .... .... .... .... .... = Type: Map-Request (1)
  ▷ .... 0100 00.. .... .... .... = Flags: 0x10
    .... .... ..00 0000 000. .... = Reserved bits: 0x000
    .... .... .... .... ...0 0000 = ITR-RLOC Count: 0
    Record Count: 1
    Nonce: 0x849ff6be688dcc66
    Source EID AFI: LISP Canonical Address Format (LCAF) (16387)
  ▷ Source EID: [8191] 00:00:00:00:aa:aa
  ▷ ITR-RLOC 1: 172.16.0.1
  ▷ Map-Request Record 1: [8191] 00:00:00:00:bb:bb/48
  ▷ Map-Reply Record
```



6 Control Plane node replies with H2's location information. E1 installs H2 into its MAP-cache

```
CP#debug lisp control-plane map-resolver
LISP[MR   ]-0: Received Map-Request with 1 records, first EID IID 8191
               0000.0000.bbbb/48, source EID 0000.0000.aaaa,
LISP[MR   ]-0 IID 8191 MAC: MS EID 0000.0000.bbbb/48: Sending proxy
               reply to 172.16.0.1
```

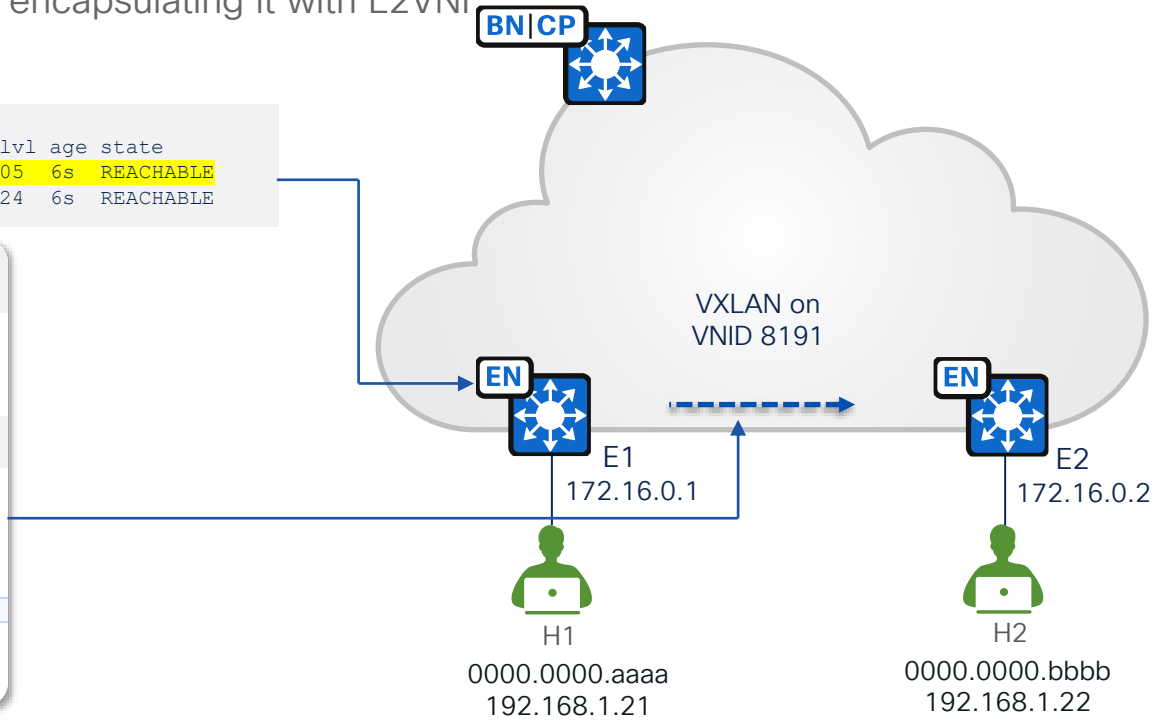
```
▷ Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.1
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
◢ Locator/ID Separation Protocol
    0010 .... .... .... .... .... = Type: Map-Reply (2)
    .... 0... .... .... .... .... = P bit (Probe): Not set
    .... .0.. .... .... .... .... = E bit (Echo-Nonce locator reachability algorithm enabled): Not set
    .... ..0. .... .... .... .... = S bit (LISP-SEC capable): Not set
    .... ...0 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0x849ff6be688dcc66
  ◢ Mapping Record 1, EID Prefix: [8191] 00:00:00:00:bb:bb/48, TTL: 1440, Action: No-Action, Not Authoritative
      Record TTL: 1440
      Locator Count: 1
      EID Mask Length: 48
      000. .... .... .... = Action: No-Action (0)
      ...0 .... .... .... = Authoritative bit: Not set
      .... .000 0000 0000 = Reserved: 0x000
      0000 .... .... .... = Reserved: 0x0
      .... 0000 0000 0000 = Mapping Version: 0
      EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    ▷ EID Prefix: [8191] 00:00:00:00:bb:bb
    ▷ Locator Record 1, RLOC: 172.16.0.2, Reachable, Priority/Weight: 10/10, Multicast Priority/Weight: 10/10
```



7 E1 coverts ARP broadcast from H1 to a directed unicast and sends it to E2 in the overlay encapsulating it with L2VNI

```
E1#show device-tracking database
Network Layer Addr Link Layer Addr Interface vlan prlvl age state
RMT 192.168.1.22   0000.0000.bbbb  L2LI0      1191 0005  6s  REACHABLE
DH4 192.168.1.21   0000.0000.aaaa  Te1/0/23   1191 0024  6s  REACHABLE
```

```
▷ Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.16.0.2
▷ User Datagram Protocol, Src Port: 65408, Dst Port: 4789
◢ Virtual eXtensible Local Area Network
  ▷ Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 8191
    Reserved: 0
▷ Ethernet II, Src: 00:00:00:00:aa:aa, Dst: 00:00:00:00:bb:bb
◢ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:00:00:00:aa:aa
    Sender IP address: 192.168.1.21
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 192.168.1.22
```

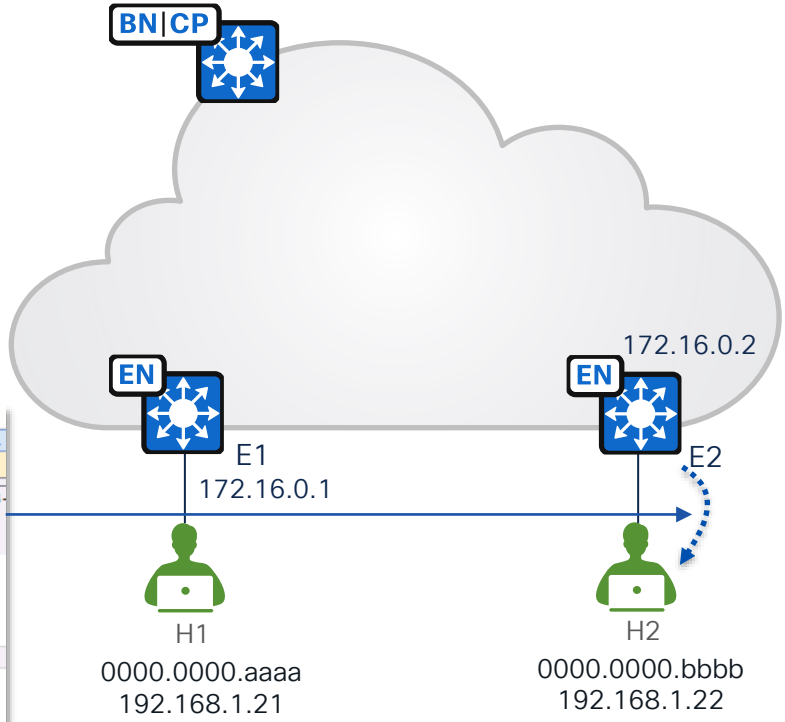


Src-O	Des-O	Source	Destination	Protoco	Length	VXLAN	Info
		00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	60		Who has 192.168.1.22? Tell 192.168.1.21
172.16.0.1	172.16.0.2	00:00:00:00:aa:aa	00:00:00:00:bb:bb	ARP	110	8191	Who has 192.168.1.22? Tell 192.168.1.21

8 E2 decapsulates the ARP request and forwards it to H2

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
13	05:35:56.942397	00:00:00:00:aa:aa	00:00:00:00:bb:bb	ARP	60		Who has 192.168.1.22? Tell 192.168.1.21
14	05:35:56.942438	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	42		192.168.1.22 is at 00:00:00:00:bb:bb

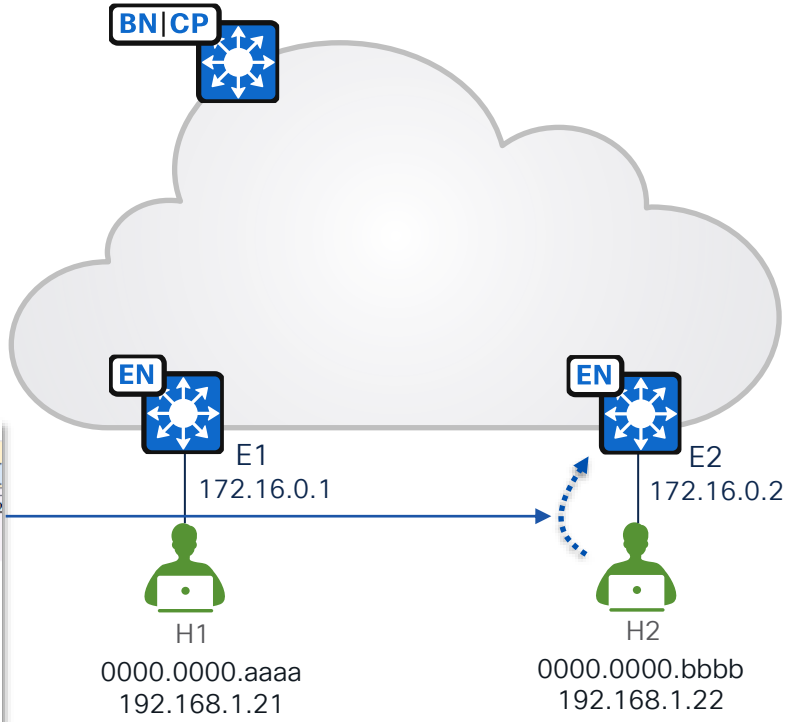
```
▷ Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-
▷ Ethernet II, Src: 00:00:00:00:aa:aa, Dst: 00:00:00:00:bb:bb
◢ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:00:00:00:aa:aa
    Sender IP address: 192.168.1.21
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 192.168.1.22
```



9 H2 unicasts the ARP response for H1 to E2

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
7	05:35:56.784550	00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	42		Who has 192.168.1.22? Tell 192.168.1.21
8	05:35:56.852124	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	60		192.168.1.22 is at 00:00:00:00:bb:bb

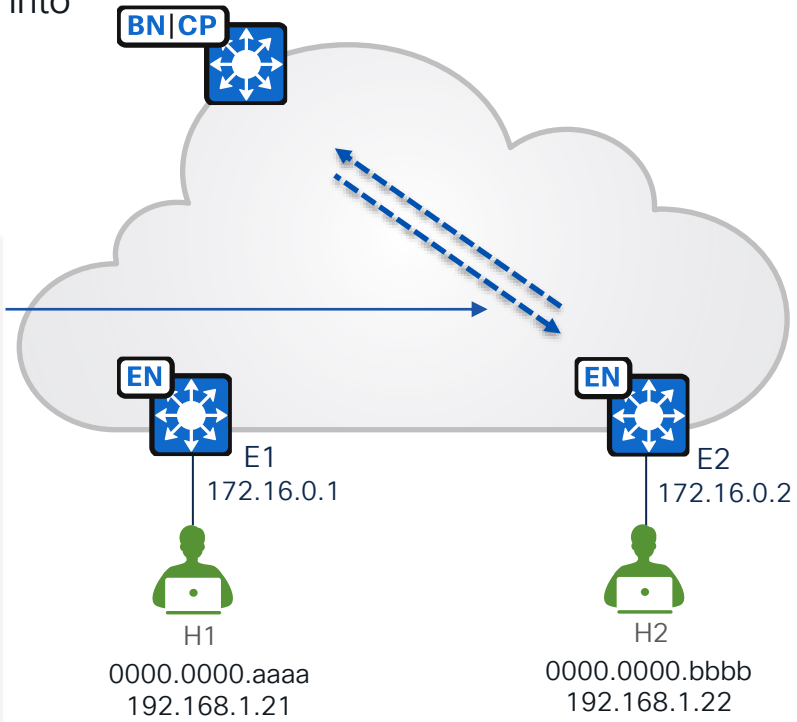
```
▷ Frame 8: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-2
▷ Ethernet II, Src: 00:00:00:00:bb:bb, Dst: 00:00:00:00:aa:aa
◢ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:00:00:00:bb:bb
    Sender IP address: 192.168.1.22
    Target MAC address: 00:00:00:00:aa:aa
    Target IP address: 192.168.1.21
```



10 E2 sends MAP-Request for the location of H1 to Control Plane nodes, and receives MAP-Reply. E2 installs H1 into its MAP-cache

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
784	09:01:31.460585	0.0.0.0	0.0.0.0	LISP	176		Encapsulated Map-Request for [8191] 00:00:00:00:aa:aa/48
785	09:01:31.460925	172.16.0.4	172.16.0.2	LISP	96		Map-Reply for [8191] 00:00:00:00:aa:aa/48

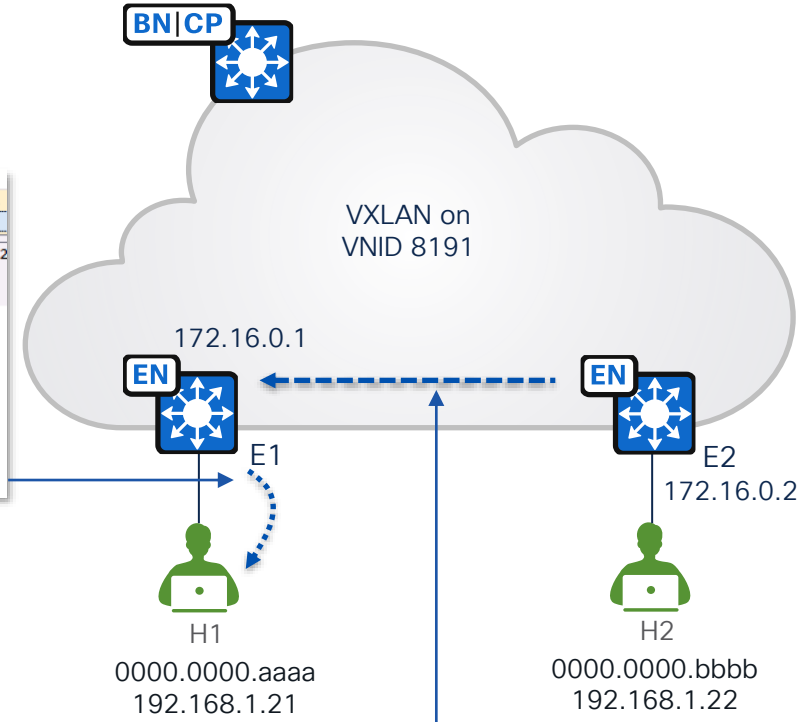
```
▷ Frame 785: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
▷ Ethernet II, Src: 00:00:00:00:00:00, Dst: 00:00:00:00:00:00
▷ Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.2
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
◢ Locator/ID Separation Protocol
    0010 .... .... .... .... .... = Type: Map-Reply (2)
    .... 0... .... .... .... .... = P bit (Probe): Not set
    .... .0.. .... .... .... .... = E bit (Echo-Nonce locator reachability algorithm enabled): Not set
    .... ..0. .... .... .... .... = S bit (LISP-SEC capable): Not set
    .... ...0 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0x220bb80cfdddcb15
  ◢ Mapping Record 1, EID Prefix: [8191] 00:00:00:00:aa:aa/48, TTL: 1440, Action: No-Action, Not Authoritative
      Record TTL: 1440
      Locator Count: 1
      EID Mask Length: 48
      000. .... .... .... = Action: No-Action (0)
      ...0 .... .... .... = Authoritative bit: Not set
      .... .000 0000 0000 = Reserved: 0x000
      0000 .... .... .... = Reserved: 0x0
      .... 0000 0000 0000 = Mapping Version: 0
      EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    ▷ EID Prefix: [8191] 00:00:00:00:aa:aa
    ▷ Locator Record 1, RLOC: 172.16.0.1, Reachable, Priority/Weight: 10/10, Multicast Priority/Weight: 10/10
```



11 H2 unicasts the ARP response to H1. E1 forwards the ARP response to H1

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
7	05:35:56.784550	00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	42		Who has 192.168.1.22? Tell 192.168.1.21
8	05:35:56.852124	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	60		192.168.1.22 is at 00:00:00:00:bb:bb

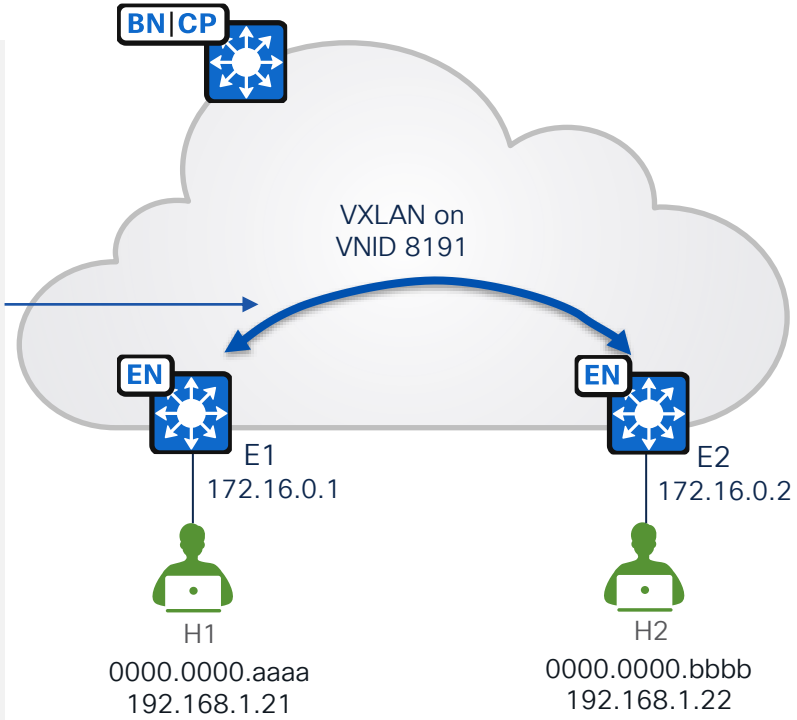
```
▷ Frame 8: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-2
▷ Ethernet II, Src: 00:00:00:00:bb:bb, Dst: 00:00:00:00:aa:aa
◢ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:00:00:00:bb:bb
    Sender IP address: 192.168.1.22
    Target MAC address: 00:00:00:00:aa:aa
    Target IP address: 192.168.1.21
```



No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
28	07:17:17.394885	00:00:00:00:aa:aa	00:00:00:00:bb:bb	ARP	110	8191	Who has 192.168.1.22? Tell 192.168.1.21
30	07:17:17.395853	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	110	8191	192.168.1.22 is at 00:00:00:00:bb:bb

12 Edge nodes will use the map-cache and L2 VNI to forward to destination node

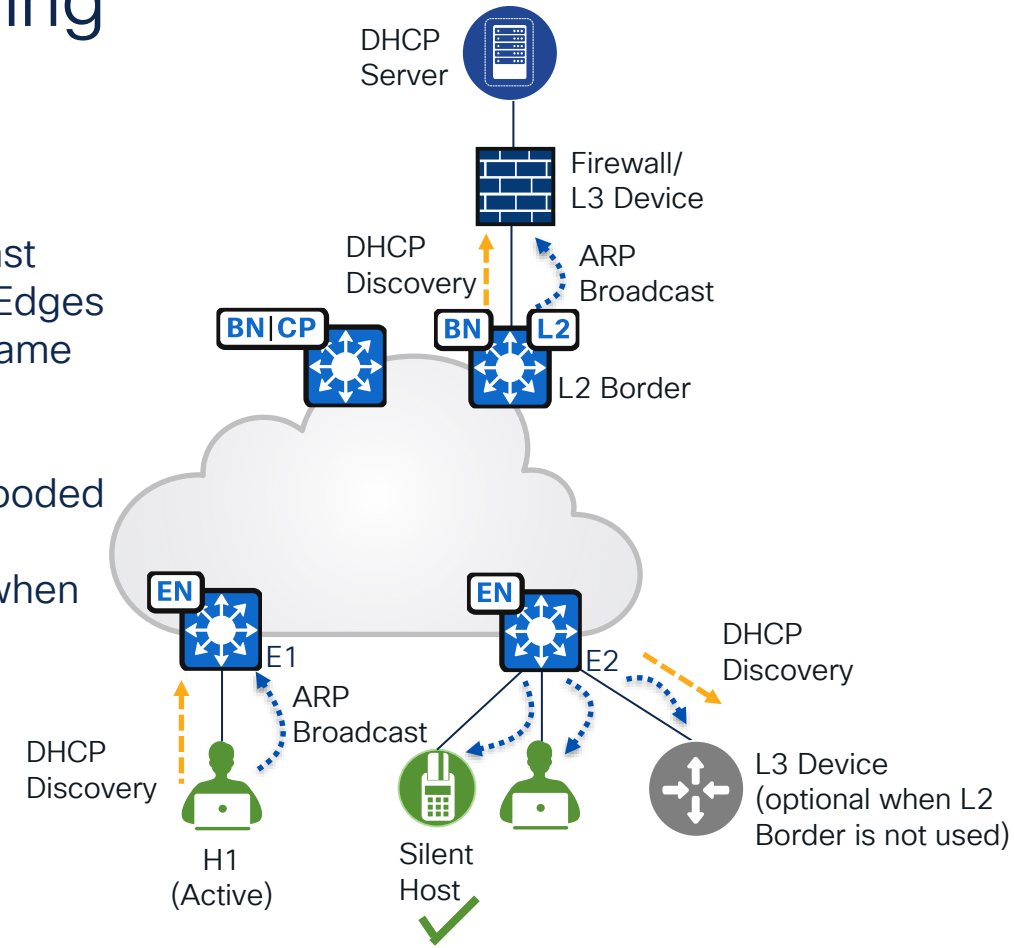
```
E1#show lisp instance-id 8191 ethernet database        <-- Local Entry

0000.0000.aaaa/48, dynamic-eid Auto-L2-group-8191, inherited from default
locator-set rloc_xxxxxxxx
  Uptime: 2d18h, Last-change: 2d18h
  Domain-ID: local
  Service-Insertion: N/A
  Locator      Pri/Wgt  Source     State
  172.16.0.1    10/10   cfg-intf   site-self, reachable

E1#show lisp instance-id 8191 ethernet map-cache       <-- Remote Entry
LISP MAC Mapping Cache for LISP 0 EID-table Vlan 1191 (IID 8191), 1
entries

0000.0000.bbbb/48, uptime: 00:17:05, expires: 23:42:54, via map-reply,
complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.2   00:17:05  up      10/10        -

E1#show mac address-table vlan 1191
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
1191    0000.0000.aaaa    DYNAMIC     Te1/0/23   <-- Local Entry
1191    0000.0000.bbbb    CP_LEARN    L2LI0      <-- Remote Entry
```



Same Segment Forwarding with Flooding

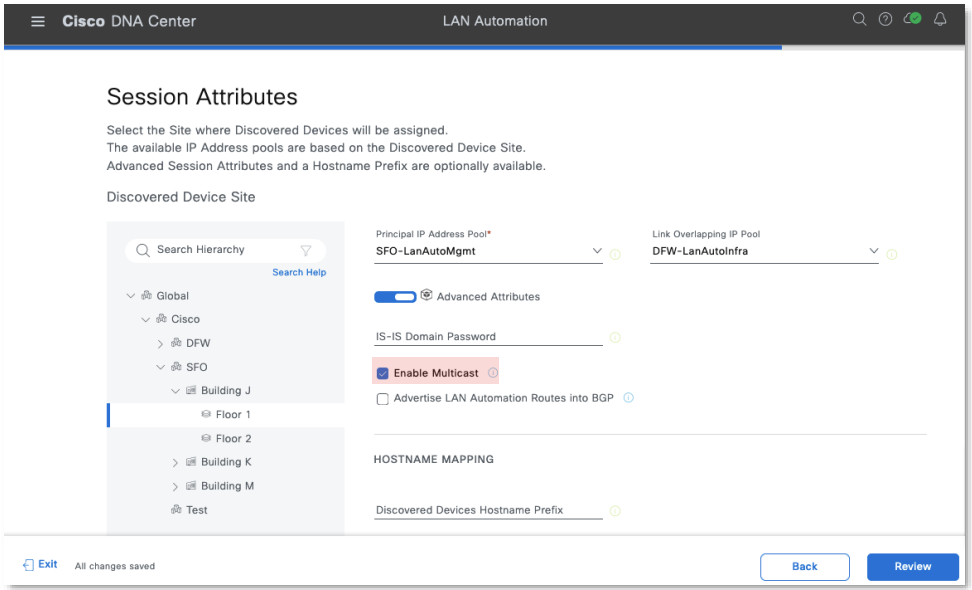
Forwarding with Flooding

- Broadcast, unknown unicast, and multicast (BUM) traffic is forwarded to all ports of Edges & the L2 Border (if used) belong to the same VLAN
- Endpoint DHCP Discovery packets are flooded
- Silent hosts will be known by the fabric when they respond to ARP broadcast



Enabling Underlay Multicast Using Lan Automation

- Multicast needs to be enabled in the underlay for L2 Flooding to work
- The underlay is configured with PIM ASM and the seed devices are selected as Anycast Rendezvous Points (RPs)
- When additional edge nodes are added using Lan Automation, they are configured to use the RP



Enabling Underlay Multicast Using Manual Config

RP Devices (typically redundant Border Nodes)

```
ip multicast-routing
!
interface Loopback60000
 ip address <loopback60000 IP address> 255.255.255.255
 ip router isis
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode
!
ip pim rp-address <loopback60000 IP address >
ip pim register-source Loopback0
!
ip msdp peer <loopback0-other-rp> connect-source Loopback0
```

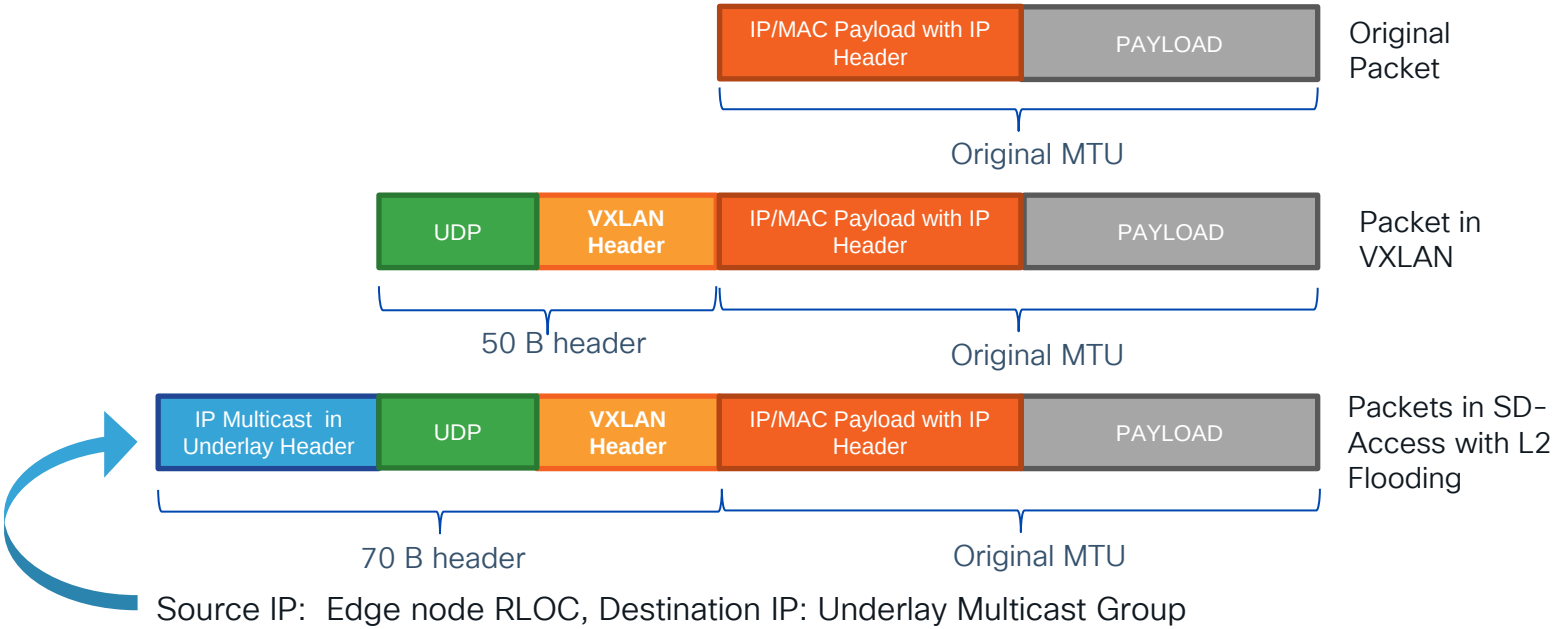
Non-RP Underlay Devices

```
ip multicast-routing
ip pim rp-address <rp IP address>
ip pim register-source Loopback0
interface Loopback0
 ip pim sparse-mode
```

Fabric L3 Interfaces

```
ip pim sparse-mode
```

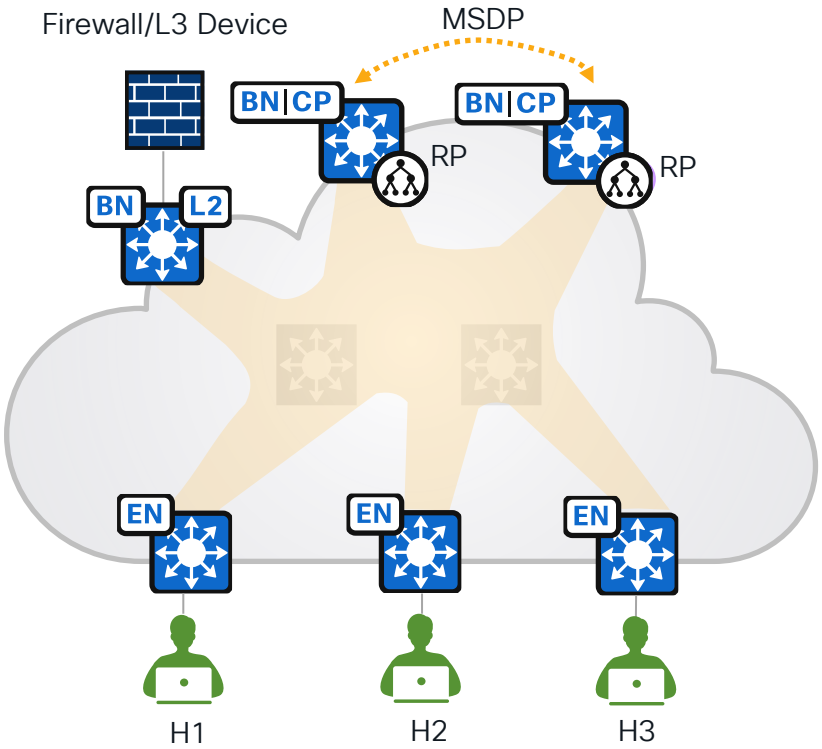
L2 Flooding Packets in SD-Access



Total header size for L2 flooding packets is 70 Bytes. Needs to be accounted for when designing underlay MTU size

L2 Flooding in SD-Access

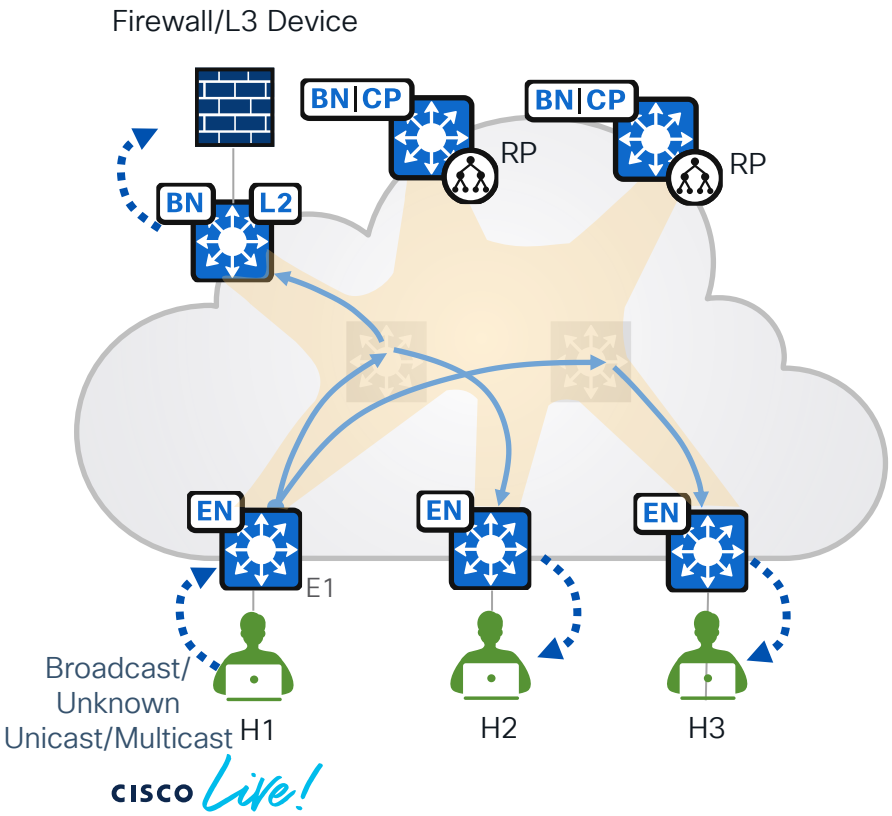
Upon Underlay Multicast Enablement



- Rendezvous Points (RPs) are in the underlay
- MSDP between RPs exchanges information about sources
- PIM-SM is enabled in underlay between fabric devices

L2 Flooding in SD-Access

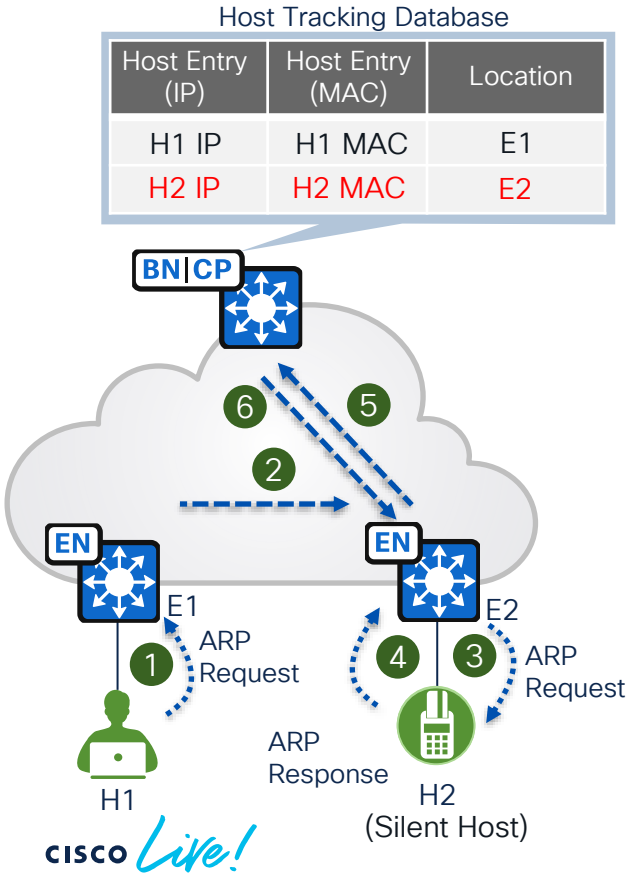
Packet Flows



- When BUM traffic reaches E1, it is encapsulated in VXLAN and sent over via a dedicated multicast group in the underlay
- The underlay devices are responsible for replicating traffic
- All Edge nodes and L2 Borders receive traffic originated by E1

Packet Flow

H1 Communication with H2



1. H1 sends ARP request broadcast for H2's MAC address
2. ARP broadcast is flooded to all Edges including E2 & L2 Border (if used) due to underlay multicast
3. E2 decapsulates the ARP request and forwards it to H2
4. H2 sends an ARP response for H1 to E2. E2 installs H2's IP and MAC addresses into its local database
5. E2 sends MAP-Registration to CP for H2. Other endpoints can start to communicate with the once-silent host
6. E2 requests and receives from CP the location of H1. E2 installs H1 into its MAP-cache

Assumptions:

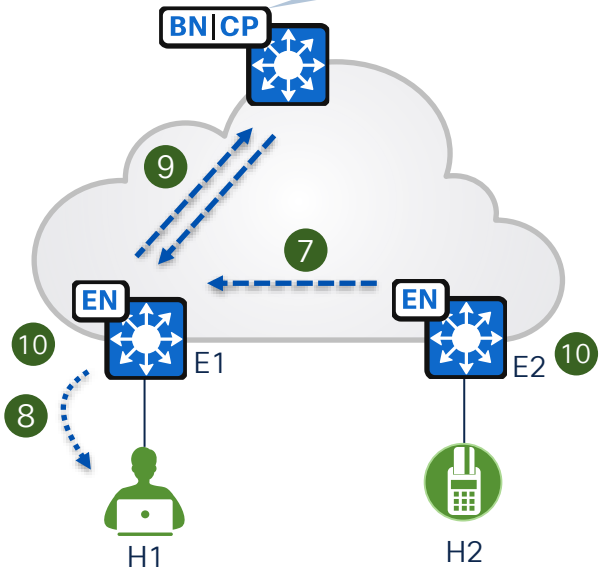
- Edges do not have remote endpoints in their MAP-cache nor ARP tables initially
- Control Plane node does not have H2 in its host tracking database

Packet Flow

H1 Communication with H2

Host Tracking Database

Host Entry (IP)	Host Entry (MAC)	Location
H1 IP	H1 MAC	E1
H2 IP	H2 MAC	E2



7. E2 sends ARP response to E1
8. E1 decapsulates and forwards the ARP response to H1
9. E1 requests and receives from CP the location of H2. E1 installs H2 into its MAP-cache
10. E1 and E2 use their MAP-cache and the L2 VNI to forward to destination nodes

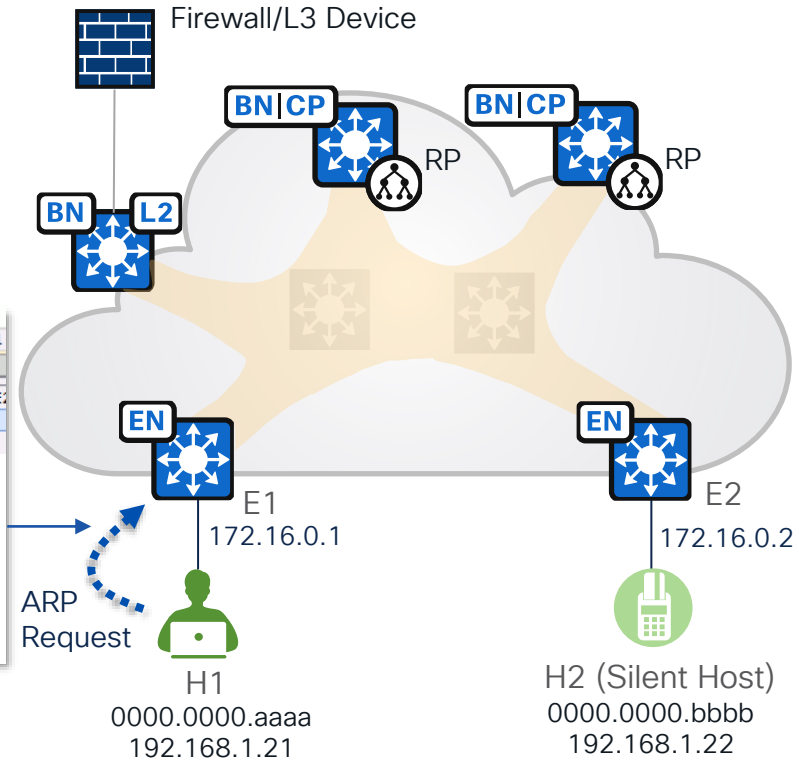
Assumptions:

- Edges do not have remote endpoints in their MAP-cache nor ARP tables initially
- Control Plane node does not have H2 in its host tracking database

1 H1 sends ARP request broadcast for H2's MAC address

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
12	06:54:57.249896	00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	42		Who has 192.168.202.22? Tell 192.168.202.21

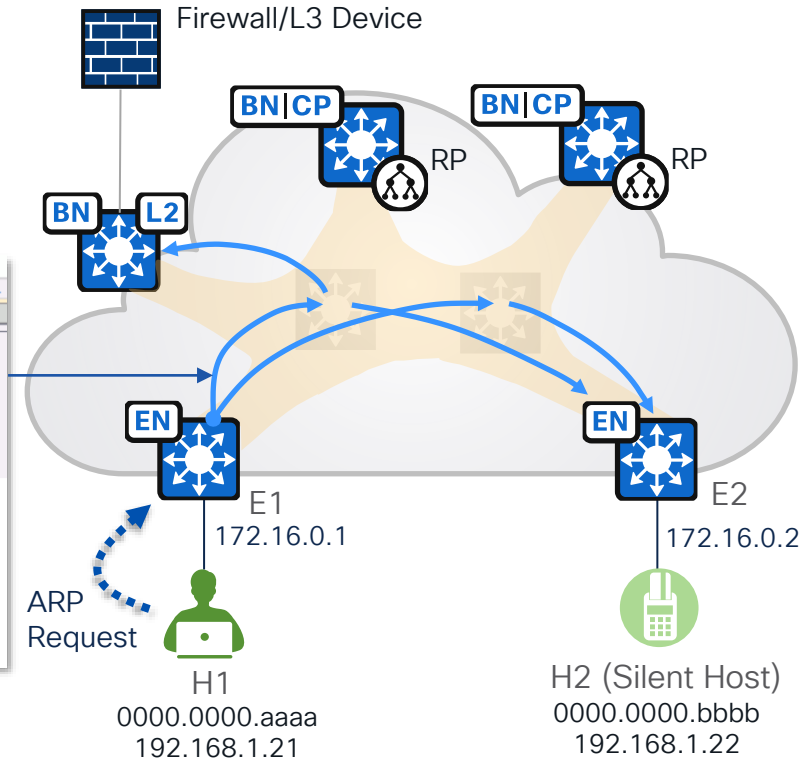
```
Frame 12: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-2AE
Ethernet II, Src: 00:00:00:00:aa:aa, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:00:00:00:aa:aa
    Sender IP address: 192.168.202.21
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 192.168.202.22
```



2 ARP broadcast request is flooded to all Edges including E2 and L2 Border (if used) due to underlay multicast

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
68	08:17:11.483831	00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	110	8202	Who has 192.168.202.22? Tell 192.168.202.21

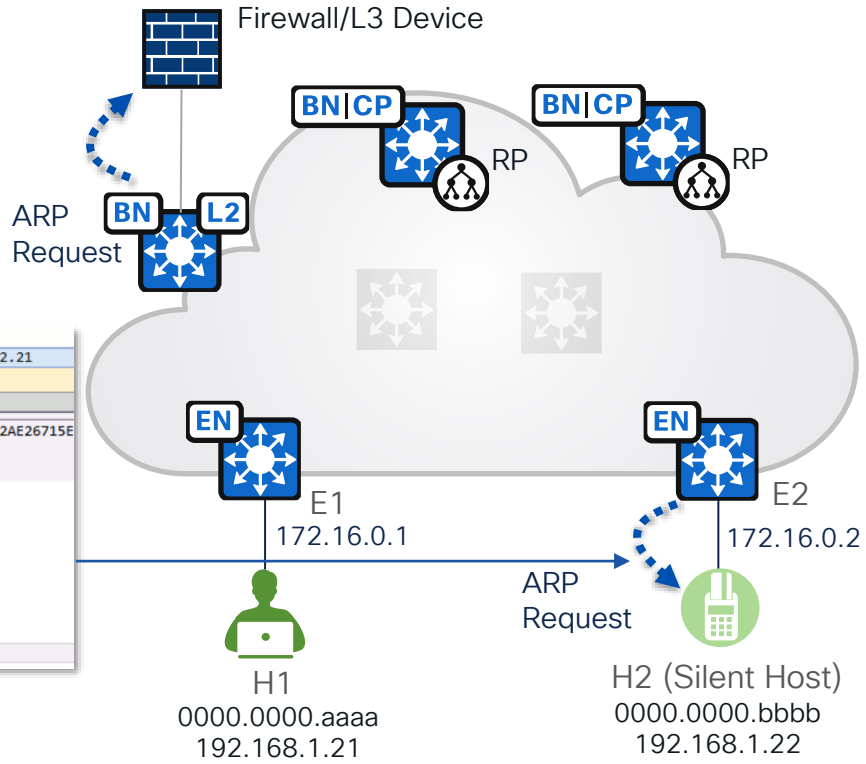
```
Frame 68: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
Ethernet II, Src: 70:0b:4f:81:b0:e4, Dst: 01:00:5e:00:11:01
Internet Protocol Version 4, Src: 172.16.0.1, Dst: 239.0.17.1
User Datagram Protocol, Src Port: 65280, Dst Port: 4789
Virtual eXtensible Local Area Network
Ethernet II, Src: 00:00:00:00:aa:aa, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:00:00:00:aa:aa
    Sender IP address: 192.168.202.21
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 192.168.202.22
```



3 E2 sends the ARP request to H2

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
9	06:54:57.407632	00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	60		Who has 192.168.202.22? Tell 192.168.202.21
10	06:54:57.407671	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	42		192.168.202.22 is at 00:00:00:00:bb:bb

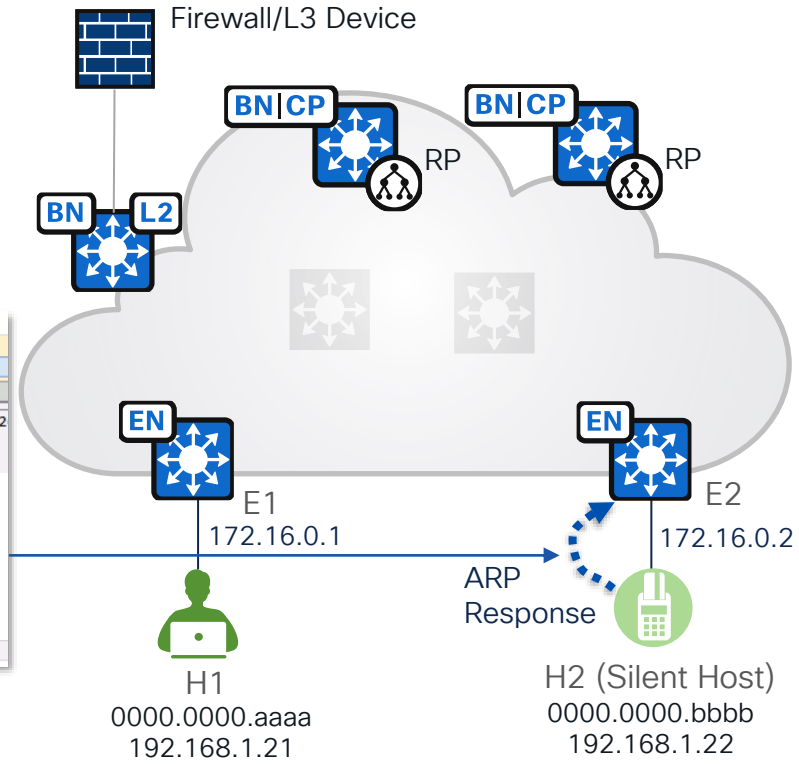
```
Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-2AE26715E
Ethernet II, Src: 00:00:00:00:aa:aa, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:00:00:00:aa:aa
    Sender IP address: 192.168.202.21
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 192.168.202.22
```



4 H2 sends an ARP response for H1 to E2

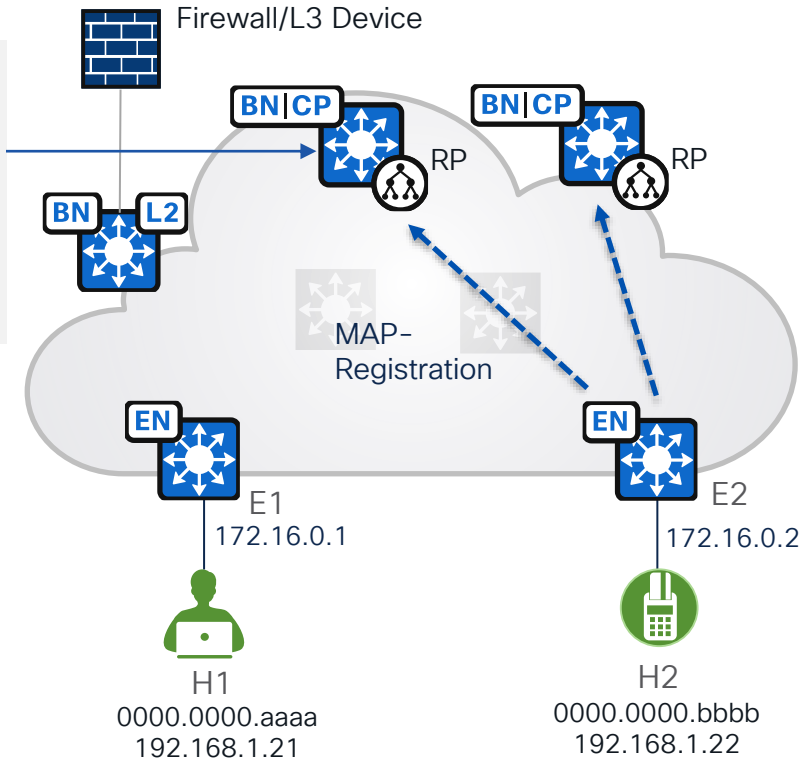
No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
9	06:54:57.407632	00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	60		Who has 192.168.202.22? Tell 192.168.202.21
10	06:54:57.407671	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	42		192.168.202.22 is at 00:00:00:00:bb:bb

```
▷ Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-2AE2
▷ Ethernet II, Src: 00:00:00:00:bb:bb, Dst: 00:00:00:00:aa:aa
◢ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:00:00:00:bb:bb
    Sender IP address: 192.168.202.22
    Target MAC address: 00:00:00:00:aa:aa
    Target IP address: 192.168.202.21
```



5 E2 sends MAP-Registration to Control Plane nodes for H2. Other endpoints can start to communicate with the once-silent host

```
CP#show lisp instance-id 8202 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     --                   8202     any-mac
               00:34:48   yes#   172.16.0.1:54628     8202     0000.0000.aaaa/48
               00:34:48   yes#   172.16.0.2:28358     8202     0000.0000.bbbb/48
               00:31:07   yes#   172.16.0.4:33024     8202     f4bd.9e84.6e42/48
```

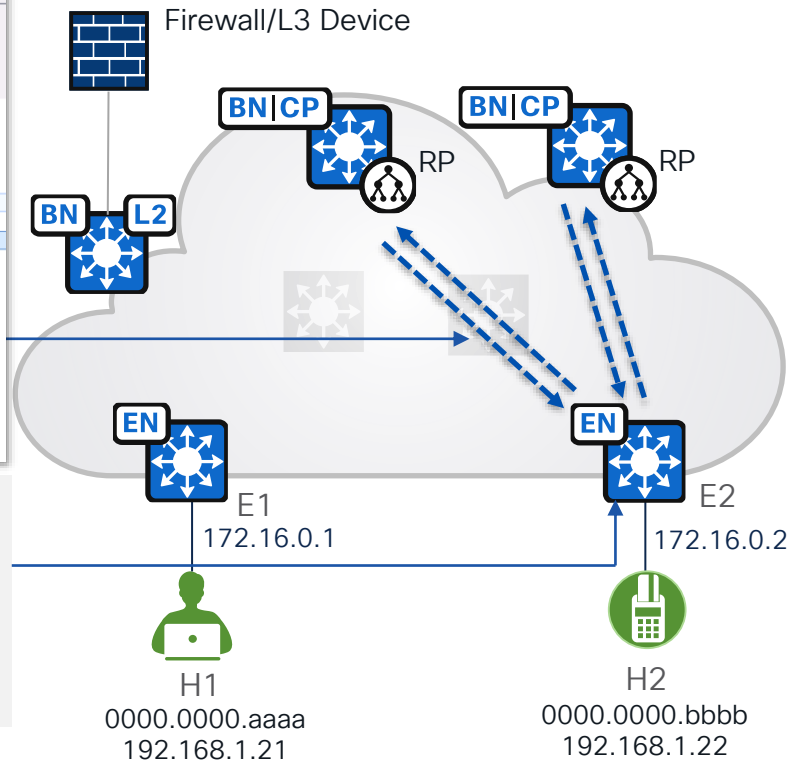


6 E2 requests and receives from Control Plane nodes the location of H1. E2 installs H1 into its MAP-cache

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
439	08:36:15.397159	0.0.0.0	0.0.0.0	LISP	176		Encapsulated Map-Request for [8202] 00:00:00:00:aa:aa/48
440	08:36:15.397457	172.16.0.4	172.16.0.2	LISP	96		Map-Reply for [8202] 00:00:00:00:aa:aa/48

```
▷ Frame 440: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
▷ Ethernet II, Src: 00:00:00:00:00:00, Dst: 00:00:00:00:00:00
▷ Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.2
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
◢ Locator/ID Separation Protocol
    0010 .... .... .... .... .... = Type: Map-Reply (2)
    .... 0... .... .... .... .... = P bit (Probe): Not set
    .... .0.. .... .... .... .... = E bit (Echo-Nonce locator reachability algorithm enabled): Not set
    .... ..0. .... .... .... .... = S bit (LISP-SEC capable): Not set
    .... ...0 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0xe664a39d75592ce4
  ◢ Mapping Record 1, EID Prefix: [8202] 00:00:00:00:aa:aa/48, TTL: 1440, Action: No-Action, Not Authoritative
      Record TTL: 1440
      Locator Count: 1
      EID Mask Length: 48
      000. .... .... .... = Action: No-Action (0)
      ...0 .... .... .... = Authoritative bit: Not set
      .... .000 0000 0000 = Reserved: 0x000
      0000 .... .... .... = Reserved: 0x0
      .... 0000 0000 0000 = Mapping Version: 0
      EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    ▷ EID Prefix: [8202] 00:00:00:00:aa:aa
    ▷ Locator Record 1, RLOC: 172.16.0.1, Reachable, Priority/Weight: 10/10, Multicast Priority/Weight: 10/10
```

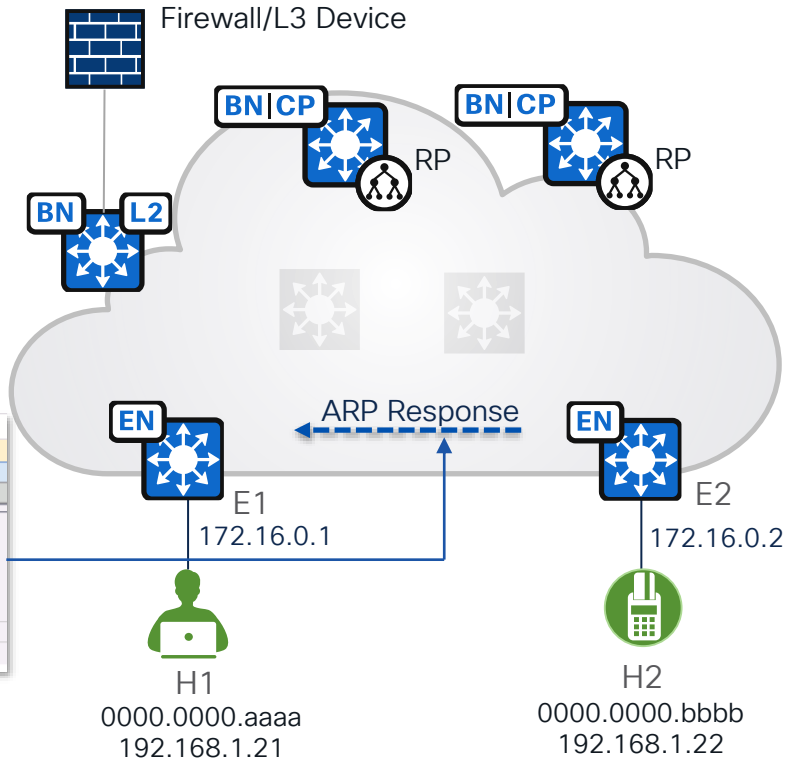
```
E2#show lisp instance-id 8202 ethernet map-cache
LISP MAC Mapping Cache for LISP 0 EID-table Vlan 1202 (IID 8202), 2 entries

0000.0000.aaaa/48, uptime: 00:12:28, expires: 23:47:31, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.1   00:12:28  up       10/10       -
0000.0000.cccc/48, uptime: 00:07:55, expires: 23:52:05, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.4   00:07:55  up       10/10       -
```



7 E2 sends ARP response to E1

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
230	09:03:07.696810	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	110	8202	192.168.202.22 is at 00:00:00:00:bb:bb
231	09:03:07.696827	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	110	8202	192.168.202.22 is at 00:00:00:00:bb:bb

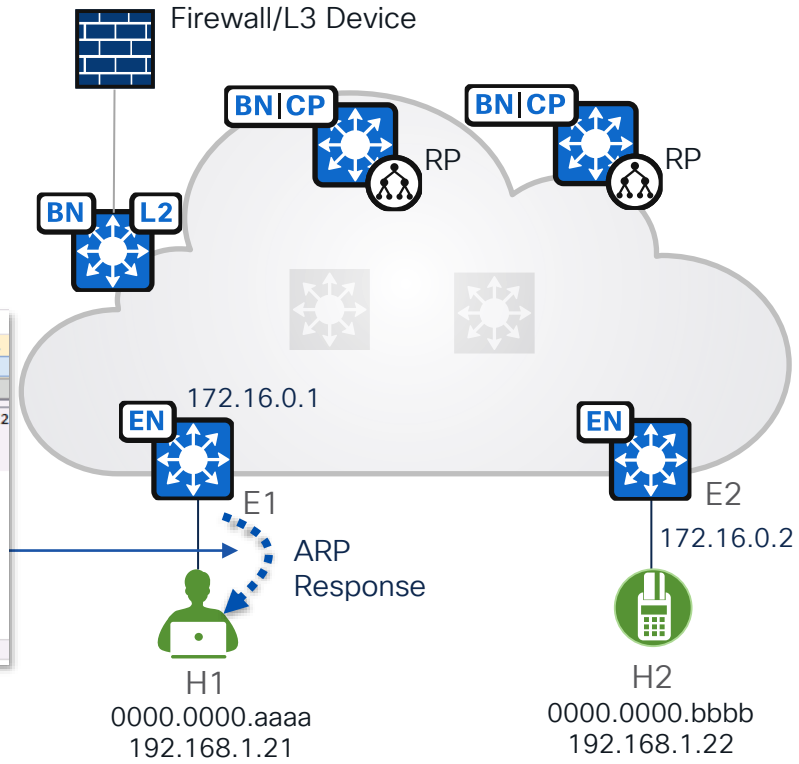
```
▷ Frame 231: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
▷ Ethernet II, Src: 6c:71:0d:04:02:46, Dst: 6c:71:0d:9a:ed:46
▷ Internet Protocol Version 4, Src: 172.16.0.2, Dst: 172.16.0.1
▷ User Datagram Protocol, Src Port: 65291, Dst Port: 4789
▷ Virtual eXtensible Local Area Network
▷ Ethernet II, Src: 00:00:00:00:bb:bb, Dst: 00:00:00:00:aa:aa
▷ Address Resolution Protocol (reply)
```



8 E1 decapsulates and forward the ARP response to H1

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
70	07:40:53.343549	00:00:00:00:aa:aa	ff:ff:ff:ff:ff:ff	ARP	42		Who has 192.168.202.22? Tell 192.168.202.21
71	07:40:53.345500	00:00:00:00:bb:bb	00:00:00:00:aa:aa	ARP	60		192.168.202.22 is at 00:00:00:00:bb:bb

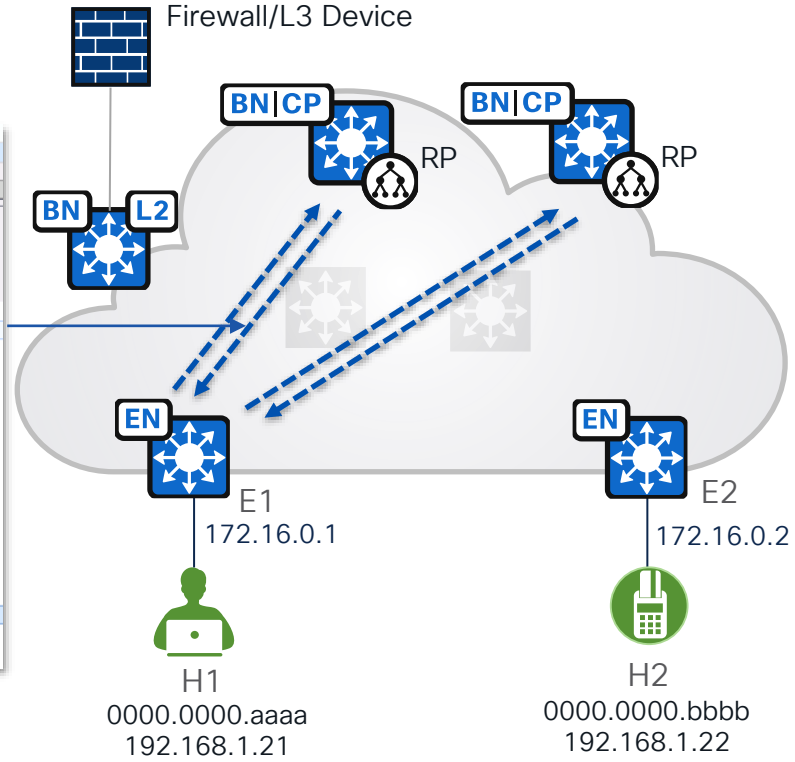
```
Frame 71: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-2AE2
Ethernet II, Src: 00:00:00:00:bb:bb, Dst: 00:00:00:00:aa:aa
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:00:00:00:bb:bb
    Sender IP address: 192.168.202.22
    Target MAC address: 00:00:00:00:aa:aa
    Target IP address: 192.168.202.21
```



9 E1 requests and receives from Control Plane nodes the location of H2. E1 installs H2 into its MAP-cache

No.	Time	Source	Destination	Protocol	Lengt	VXLAN	Info
315	02:58:46.284668	0.0.0.0	0.0.0.0	LISP	176		Encapsulated Map-Request for [8202] 00:00:00:00:bb:bb/48
316	02:58:46.284922	172.16.0.4	172.16.0.2	LISP	96		Map-Reply for [8202] 00:00:00:00:bb:bb/48

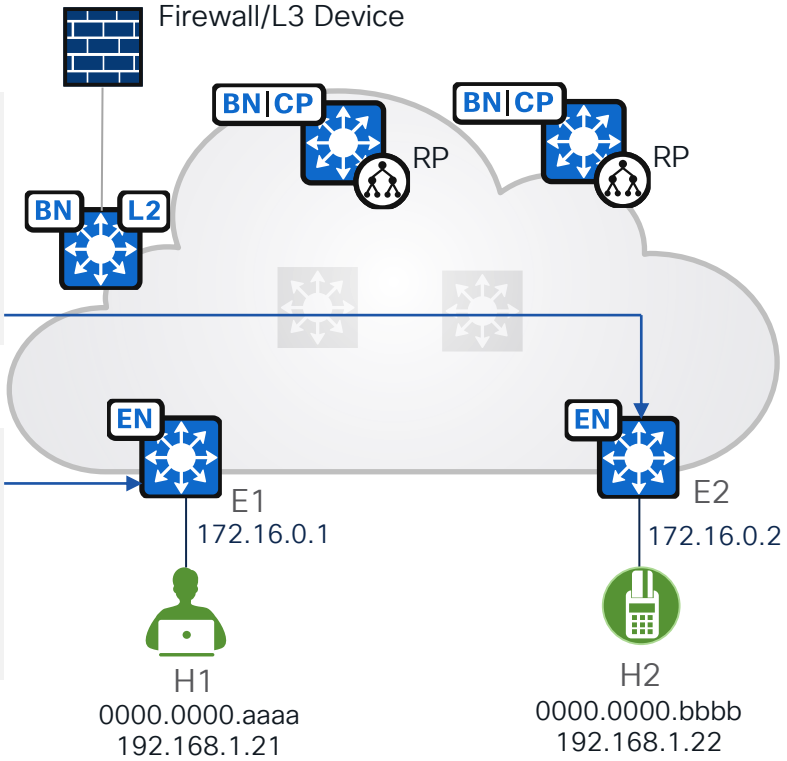
```
Frame 316: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
Ethernet II, Src: 00:00:00:00:00:00, Dst: 00:00:00:00:00:00
Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.2
User Datagram Protocol, Src Port: 4342, Dst Port: 4342
Locator/ID Separation Protocol
    0010 .... .... .... .... .... = Type: Map-Reply (2)
    .... 0... .... .... .... .... = P bit (Probe): Not set
    .... .0.. .... .... .... .... = E bit (Echo-Nonce locator reachability algorithm enabled): Not set
    .... ..0. .... .... .... .... = S bit (LISP-SEC capable): Not set
    .... ...0 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0x60cc22f017e85f72
  Mapping Record 1, EID Prefix: [8202] 00:00:00:00:bb:bb/48, TTL: 1440, Action: No-Action, Not Authoritative
      Record TTL: 1440
      Locator Count: 1
      EID Mask Length: 48
      000. .... .... .... = Action: No-Action (0)
      ...0 .... .... .... = Authoritative bit: Not set
      .... .000 0000 0000 = Reserved: 0x000
      0000 .... .... .... = Reserved: 0x0
      .... 0000 0000 0000 = Mapping Version: 0
      EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    EID Prefix: [8202] 00:00:00:00:bb:bb
    Locator Record 1, RLOC: 172.16.0.2, Reachable, Priority/Weight: 10/10, Multicast Priority/Weight: 10/10
```



10 E1 and E2 use their MAP-cache and the L2 VNI to forward to destination nodes

```
E2#show lisp instance-id 8202 ethernet map-cache
LISP MAC Mapping Cache for LISP 0 EID-table Vlan 1202 (IID 8202), 2 entries

0000.0000.aaaa/48, uptime: 00:00:50, expires: 23:59:10, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.1   00:00:50  up      10/10        -
0000.0000.cccc/48, uptime: 00:00:15, expires: 23:59:45, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.4   00:00:15  up      10/10        -
```

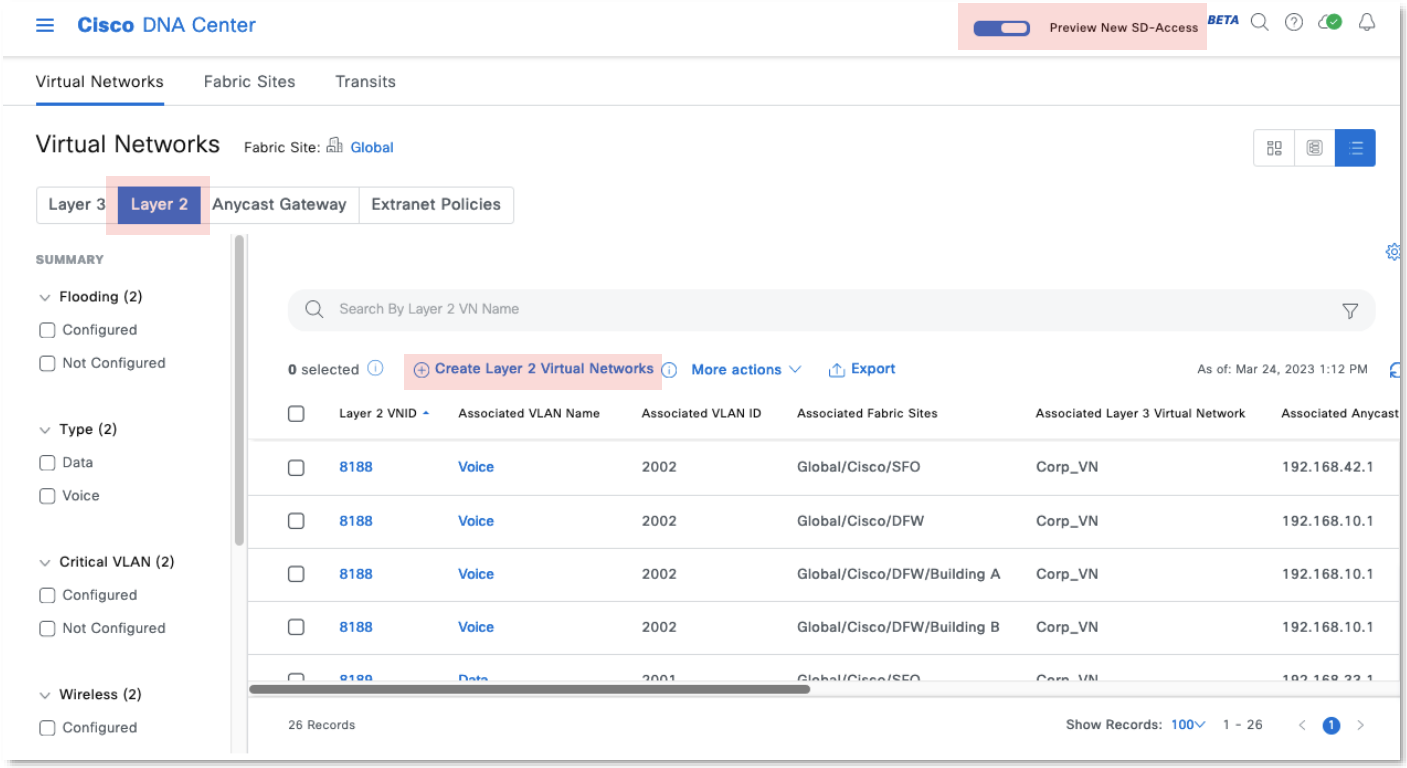
```
E1#show lisp instance-id 8202 ethernet map-cache
LISP MAC Mapping Cache for LISP 0 EID-table Vlan 1202 (IID 8202), 2 entries

0000.0000.bbbb/48, uptime: 00:12:28, expires: 23:47:31, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.2   00:12:28  up      10/10        -
0000.0000.cccc/48, uptime: 00:07:55, expires: 23:52:05, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.4   00:07:55  up      10/10        -
```



Configuring Layer 2 Virtual Network

L2 Virtual Network with L2 Border Configuration

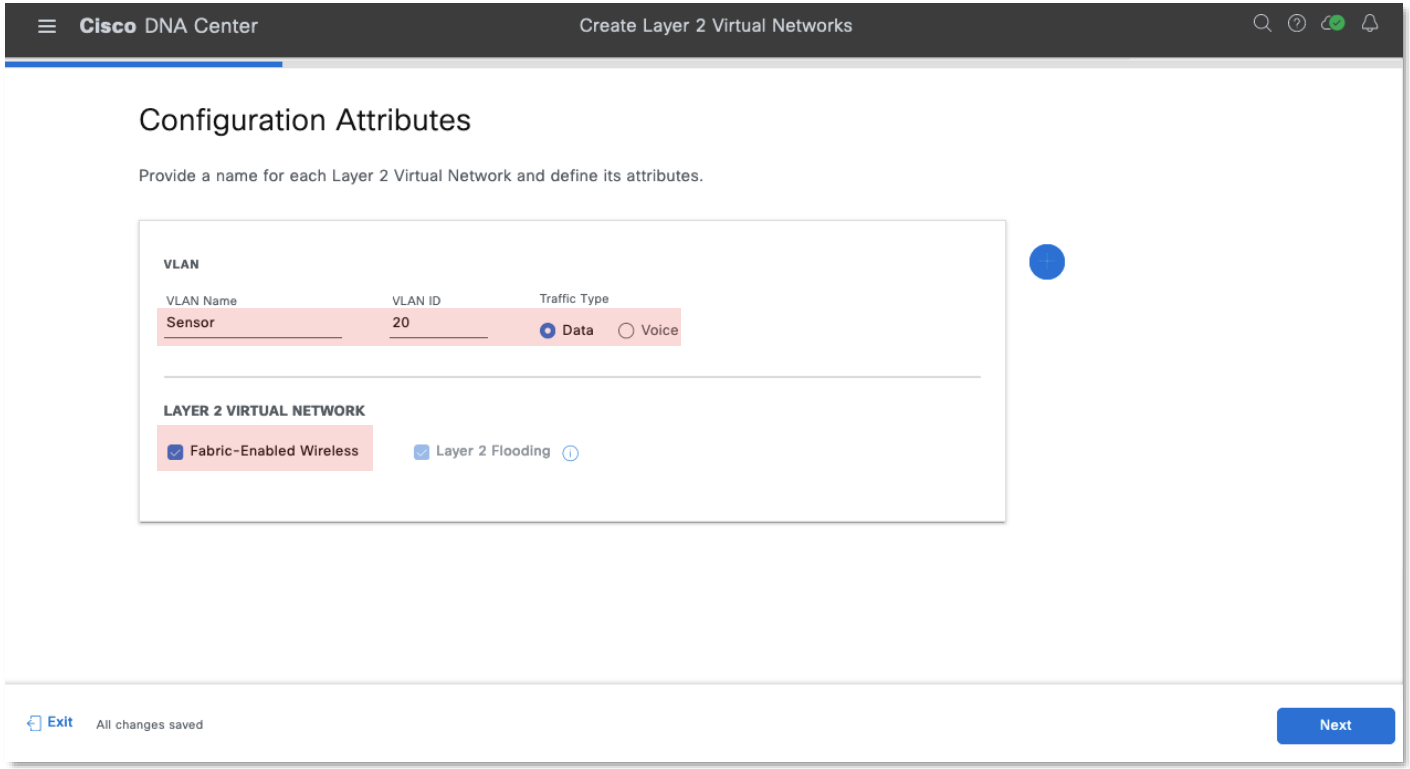
- Start L2 VN Creation Workflow
- Enter L2 VN Attributes
- Associate Fabric Site/Zone
- Verify L2 VN Properties
- Start L2 Border Config Workflow
- Select VLAN
- Select Interface, Enable L2 Handoff, Ext. VLAN



Provision → Virtual Networks → Preview New SD-Access (switch on) → Layer 2 Virtual Networks (select)

L2 Virtual Network with L2 Border Configuration

- Start L2 VN Creation Workflow
- Enter L2 VN Attributes
- Associate Fabric Site/Zone
- Verify L2 VN Properties
- Start L2 Border Config Workflow
- Select VLAN
- Select Interface, Enable L2 Handoff, Ext. VLAN



Select Fabric-Enabled Wireless if needed (Cisco DNA center ≥ 2.3.5.x & IOS-XE ≥ 17.10.x)

L2 Virtual Network with L2 Border Configuration

Start L2 VN Creation Workflow

Enter L2 VN Attributes

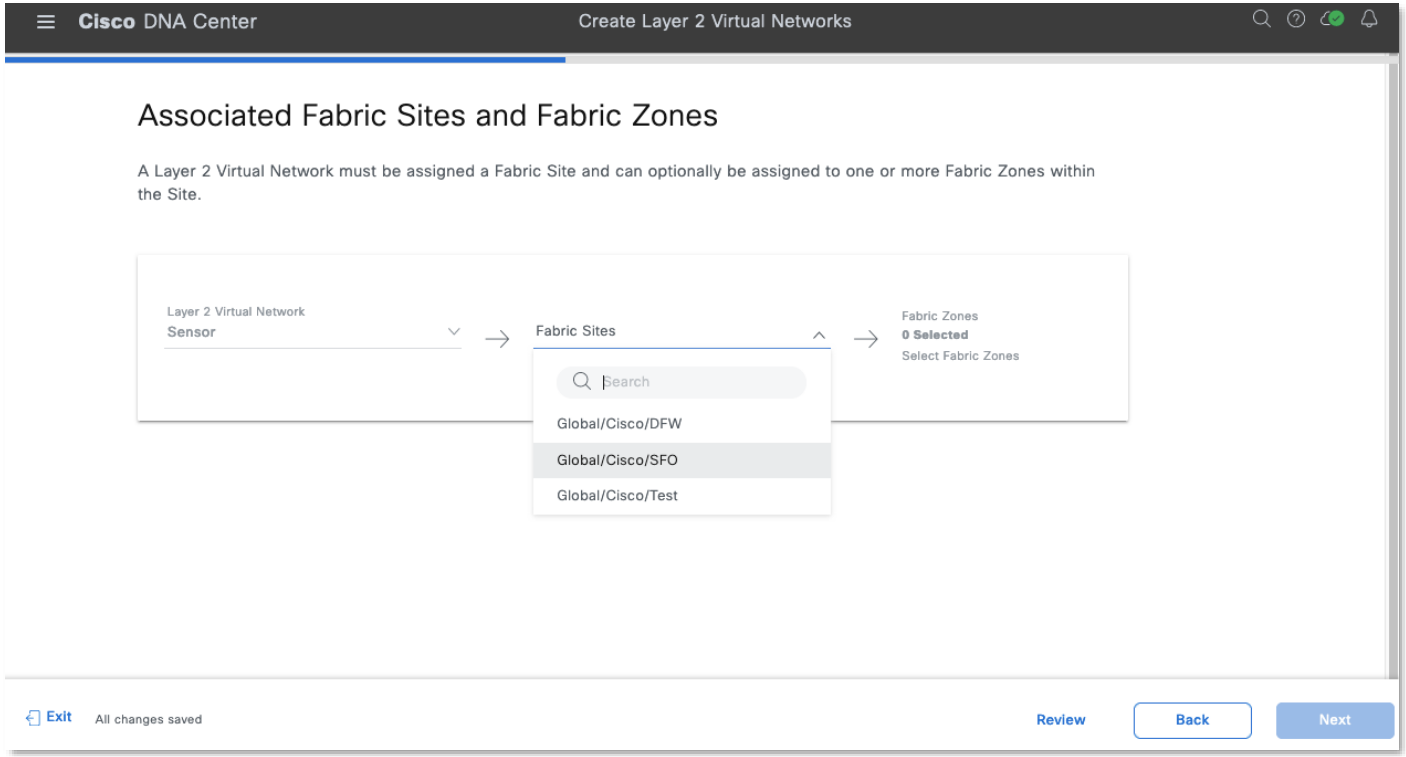
Associate Fabric site/zone

Verify L2 VN Properties

Start L2 Border Config Workflow

Select VLAN

Select Interface, Enable L2 Handoff, Ext. VLAN



- Fabric Zone association is optional

L2 Virtual Network with L2 Border Configuration

Start L2 VN Creation Workflow

Enter L2 VN Attributes

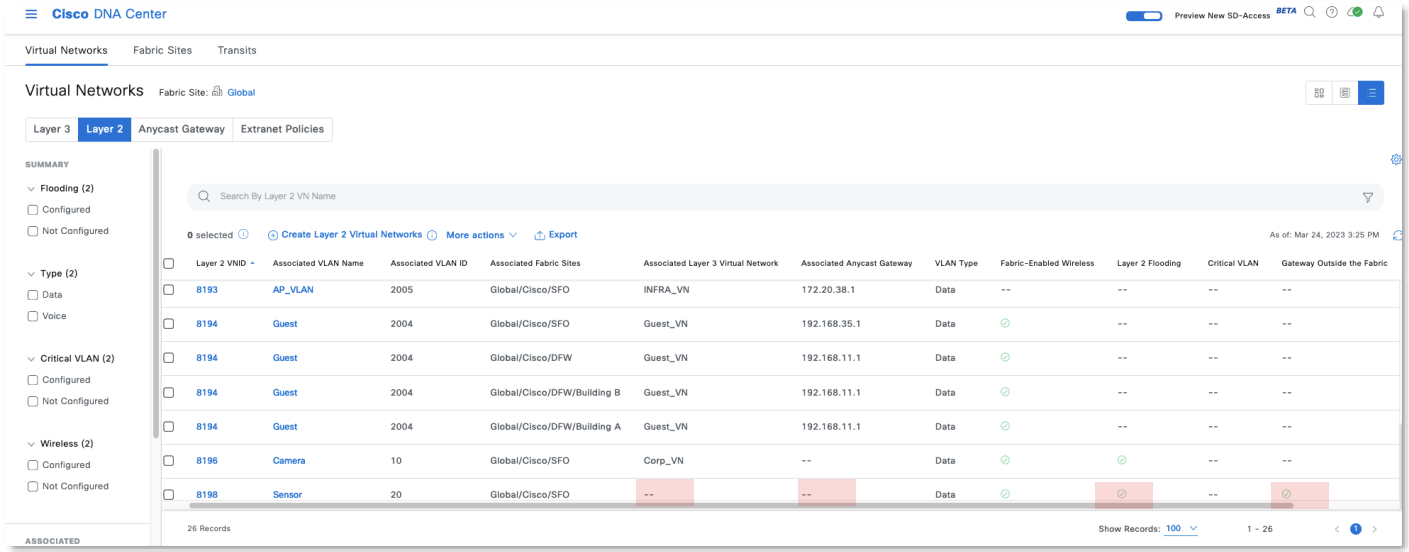
Associate Fabric Site/Zone

Verify L2 VN Properties

Start L2 Border Config Workflow

Select VLAN

Select Interface, Enable L2 Handoff, Ext. VLAN



- No L3 VN is associated. No Anycast gateway is present. L2 Flooding is enabled. Gateway Outside the Fabric is marked

L2 Virtual Network with L2 Border Configuration

Start L2 VN Creation Workflow

Enter L2 VN Attributes

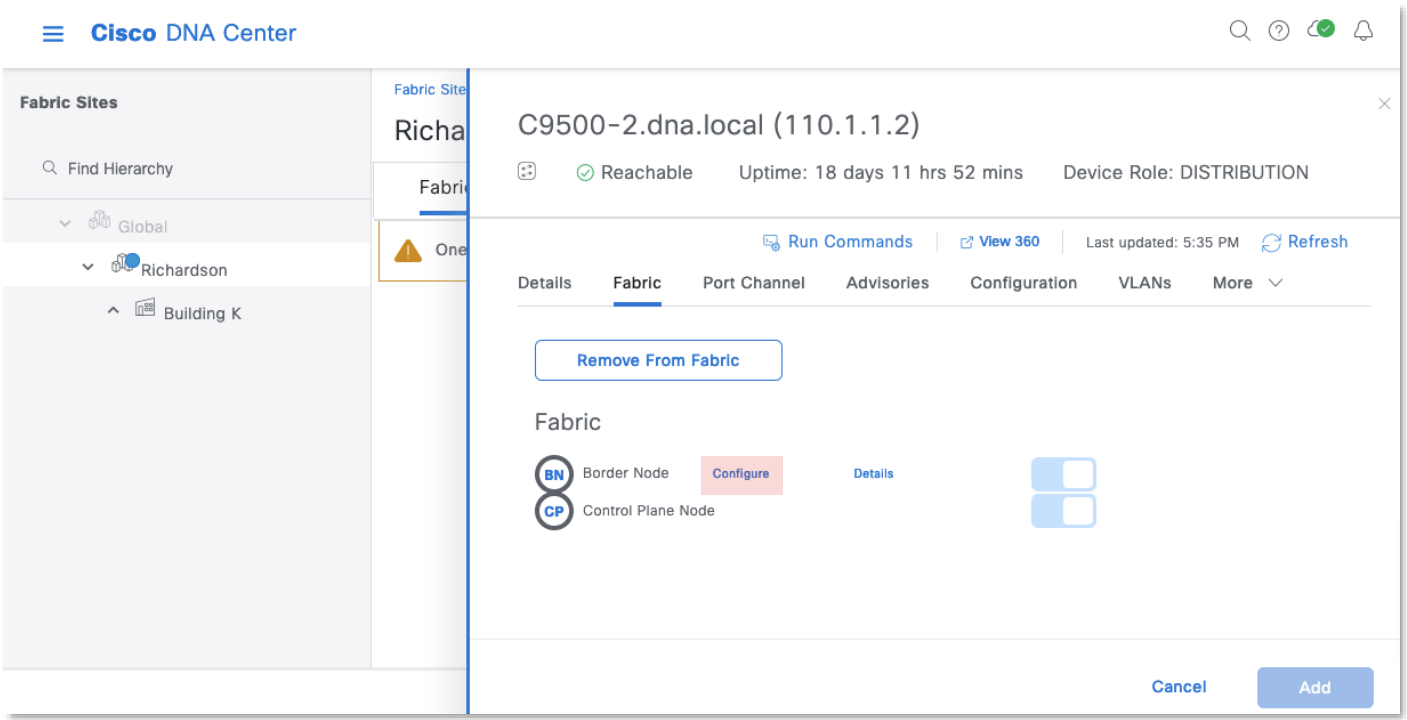
Associate Fabric Site/Zone

Verify L2 VN Properties

Start L2 Border Config Workflow

Select VLAN

Select Interface, Enable L2 Handoff, Ext. VLAN

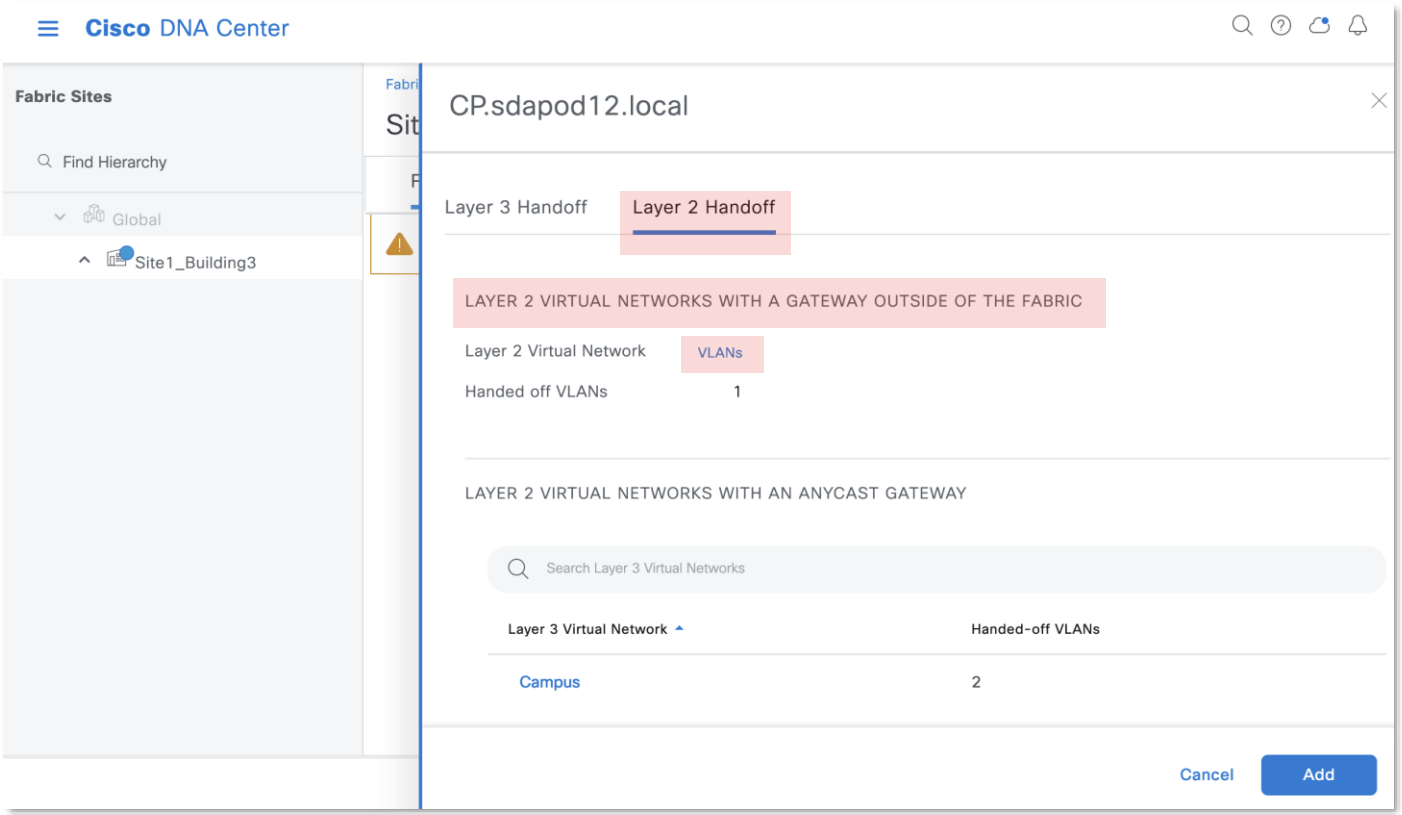


- Perform this and the steps from here if L2 Border is used

Provision → Fabric Sites → (Select Site) → (Select Border)

L2 Virtual Network with L2 Border Configuration

- Start L2 VN Creation Workflow
- Enter L2 VN Attributes
- Associate Fabric Site/Zone
- Verify L2 VN Properties
- Start L2 Border Config Workflow
- **Select VLAN**
- Select Interface, Enable L2 Handoff, Ext. VLAN



L2 Virtual Network with L2 Border Configuration

Start L2 VN Creation Workflow

Enter L2 VN Attributes

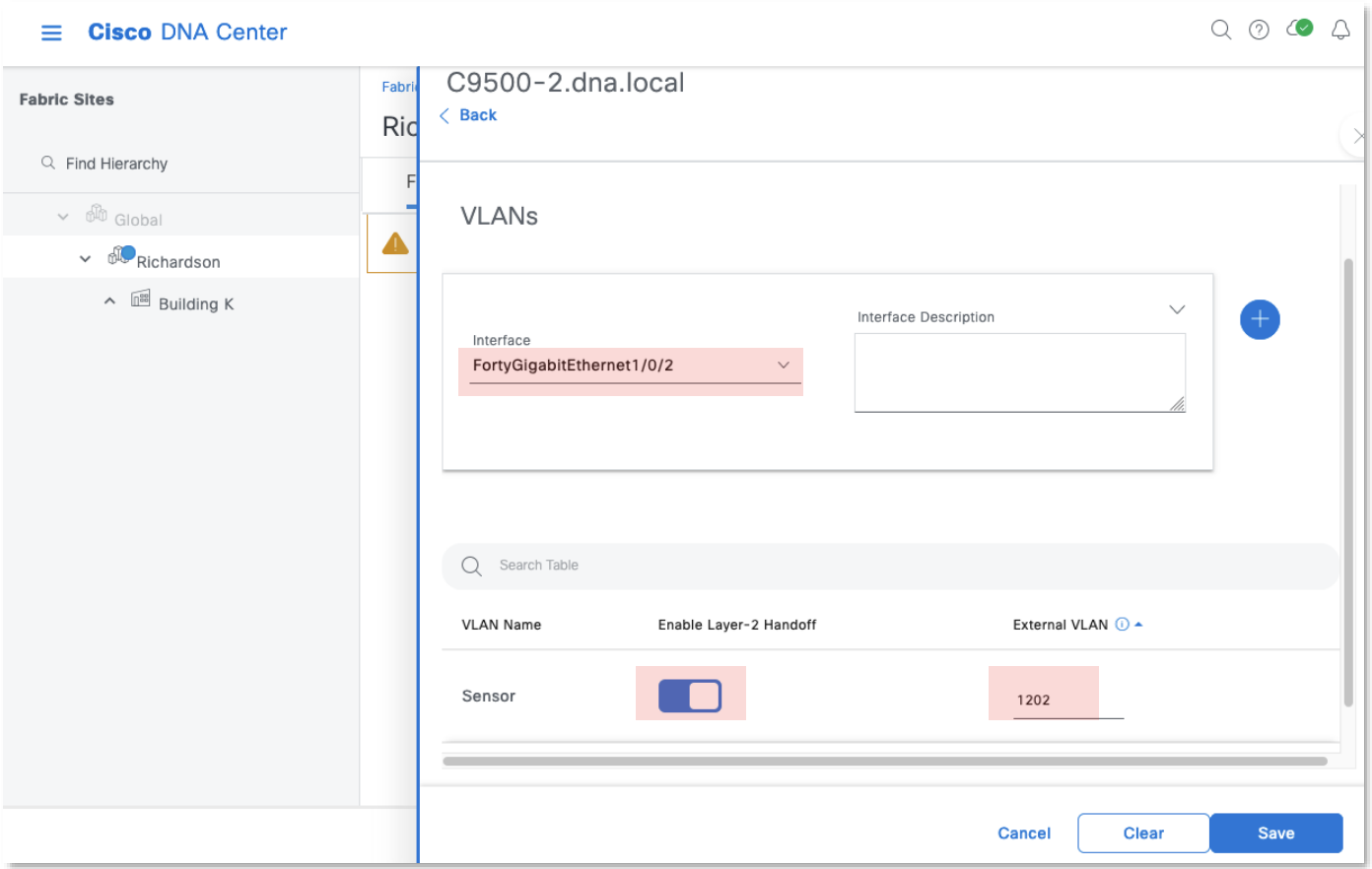
Associate Fabric Site/Zone

Verify L2 VN Properties

Start L2 Border Config Workflow

Select VLAN

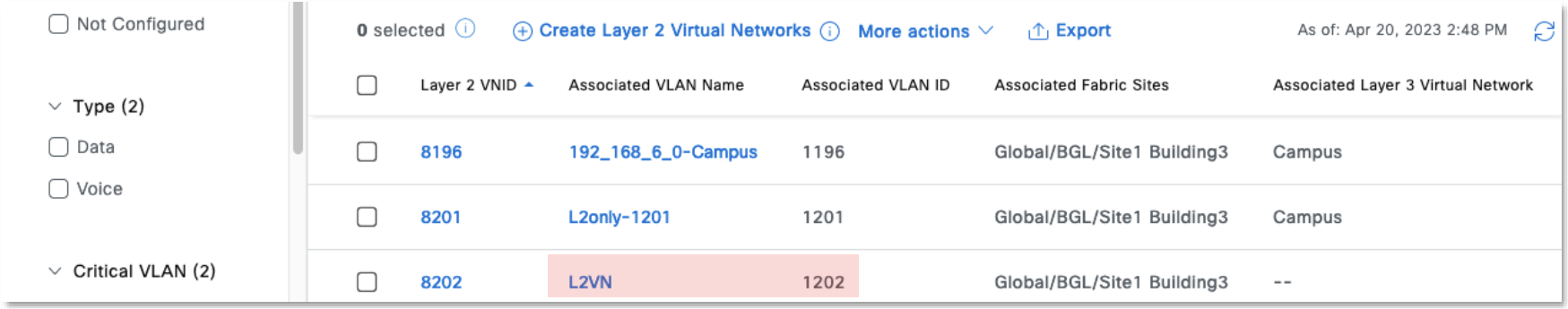
Select Interface, Enable L2 Handoff, Ext. VLAN



Troubleshooting

Multicast Verification

Underlay Multicast is Configured for L2 Flooding



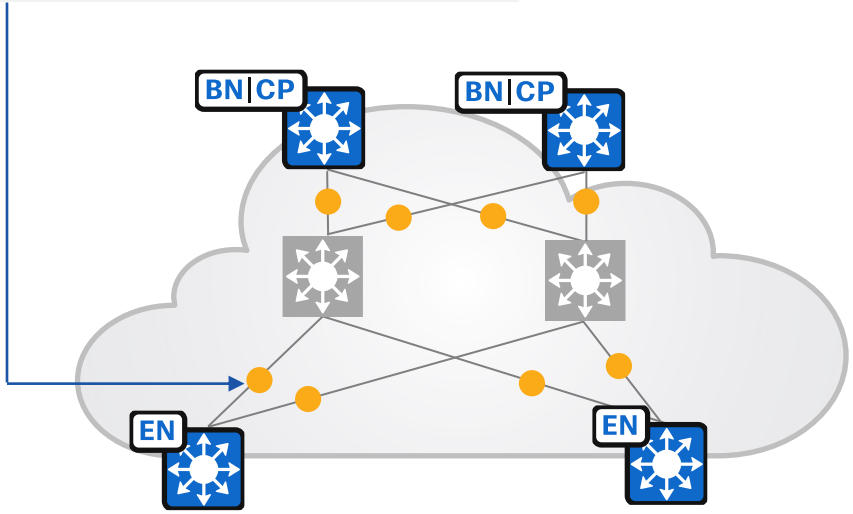

```
 instance-id 8202
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1202
   broadcast-underlay 239.0.17.1
   flood arp-nd
   flood unknown-unicast
   database-mapping mac locator-set
rloc_xxxxxxxx
   exit-service-ethernet
  !
```

```
E1#show ip mroute
….
(*, 239.0.17.1), 1w4d/stopped, RP 172.16.0.4, flags: SJCF
  Incoming interface: TenGigabitEthernet1/0/1, RPF nbr 172.16.1.21
  Outgoing interface list:
    L2LISP0.8202, Forward/Sparse-Dense, 00:01:00/00:01:59, flags:
    L2LISP0.8201, Forward/Sparse-Dense, 1w4d/00:00:14, flags:


(172.16.0.2, 239.0.17.1), 07:17:25/00:01:49, flags: JT
  Incoming interface: TenGigabitEthernet1/0/1, RPF nbr 172.16.1.21
  Outgoing interface list:
    L2LISP0.8202, Forward/Sparse-Dense, 00:01:00/00:01:59, flags:
    L2LISP0.8201, Forward/Sparse-Dense, 07:17:25/00:00:34, flags:
```

Multicast Verification

PIM Neighbor Relationships are Established

```
E1#show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load-balancing Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
172.16.1.21       TenGigabitEthernet1/0/1  1w4d/00:01:44     v2    1 / S P G
```



VLAN Verification

- Vlan is in the running config

```
vlan 1202
 name L2VN
!
```

- LISP tunnel is present for the VLAN

```
E1#show vlan id 1202

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1202 L2VN                             active    L2LI0:8202, Ac0
```

- Local and remote endpoint MAC Addresses are in MAC Address Table

```
E1#show mac address-table vlan 1202
-----------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
1202    0000.0000.aaaa    DYNAMIC     Te1/0/23
1202    0000.0000.bbbb    CP_LEARN    L2LI0
```

Local Endpoint is in Device Tracking Database

- Local endpoint is shown in device-tracking database and LISP database

```
E1#show device-tracking database interface T1/0/23
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
ARP 192.168.202.21        0000.0000.aaaa     Te1/0/23   1202 0005  169s  REACHABLE  73 s

E1#show lisp instance-id 8202 ethernet database
LISP ETR MAC Mapping Database for LISP 0 EID-table Vlan 1202 (IID 8202), LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 0

0000.0000.aaaa/48, dynamic-eid Auto-L2-group-8202, inherited from default locator-set rloc_xxxxxxxx
  Uptime: 00:07:31, Last-change: 00:07:31
  Domain-ID: local
  Service-Insertion: N/A
  Locator     Pri/Wgt  Source     State
  172.16.0.1   10/10   cfg-intf   site-self, reachable
```

Endpoints are Registered to Control Plane Node

```
CP#show lisp instance-id 8202 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     --                   8202     any-mac
               05:46:53  yes#   172.16.0.1:31397     8202     0000.0000.aaaa/48
               02:37:26  yes#   172.16.0.2:24161     8202     0000.0000.bbbb/48

CP#show lisp instance-id 8202 ethernet server 0000.0000.aaaa

Description: map-server configured from Cisco DNA-Center
Allowed configured locators: any
Requested EID-prefix:

  EID-prefix: 0000.0000.aaaa/48 instance-id 8202

    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.16.0.1:31397, last registered 05:48:30, proxy-reply, map-notify

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

MAP Cache is Resolved to the Correct RLOC

- L2 communication within the same segment: remote/destination endpoint MAC is resolved with the destination fabric Edge RLOC
- L3 communication: remote/destination endpoint MAC is always the Gateway MAC address which is outside the fabric and the RLOC will always be the L2 Border

```
E1#show lisp instance-id 8202 ethernet map-cache
LISP MAC Mapping Cache for LISP 0 EID-table Vlan 1202 (IID 8202), 2 entries

0000.0000.bbbb/48, uptime: 00:00:07, expires: 23:59:52, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.2   00:00:07  up      10/10        -
0000.0000.cccc/48, uptime: 00:00:03, expires: 23:59:56, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  172.16.0.4   00:00:03  up      10/10
```

IP-Directed Broadcast

IP-Directed Broadcast in SD-Access

- It is not a L2 VN feature. It is used in L3 VN with L3 Border(s)
- Since it relies on L2 Flooding, we discuss it here
- It is implemented in SD-Access to address communication with endpoints residing in a subnet that fall into:

Silent Host

An endpoint whose location in fabric is not known because it has not sent any packets or frames

Sleeping Host

An endpoint connected in the fabric that moves into passive/power-save mode

Host Actions with IP-Directed Broadcast

ARP Request

ARP request packet with the destination MAC address of *FF FF FF FF FF FF*

Un-silent

Silent Host

If an outside packet towards the silent host reaches the Border, and the Border does not have the silent host's IP it's MAP-cache or ARP cache, Border Node will ARP for it

Magic Packet

- A broadcast frame with a payload containing *FF FF FF FF FF FF* in hexadecimal followed by sixteen (16) repetitions of target machine's MAC address
- Typically sent to UDP destination port 0, 7 or 9

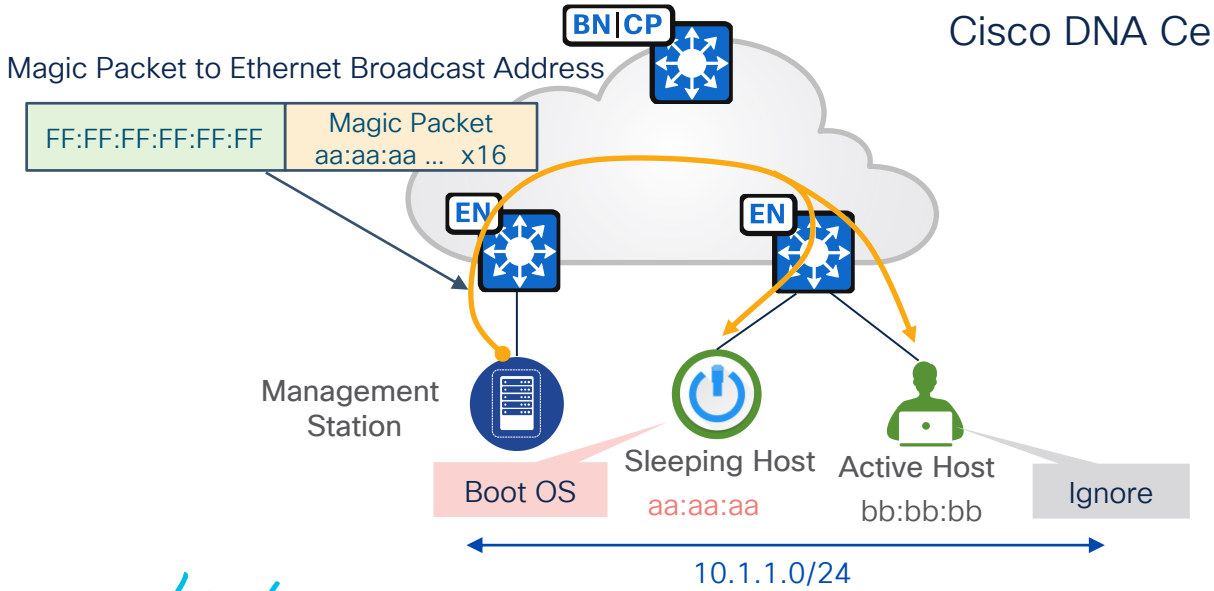
Wake on LAN (WoL)

Sleeping Host

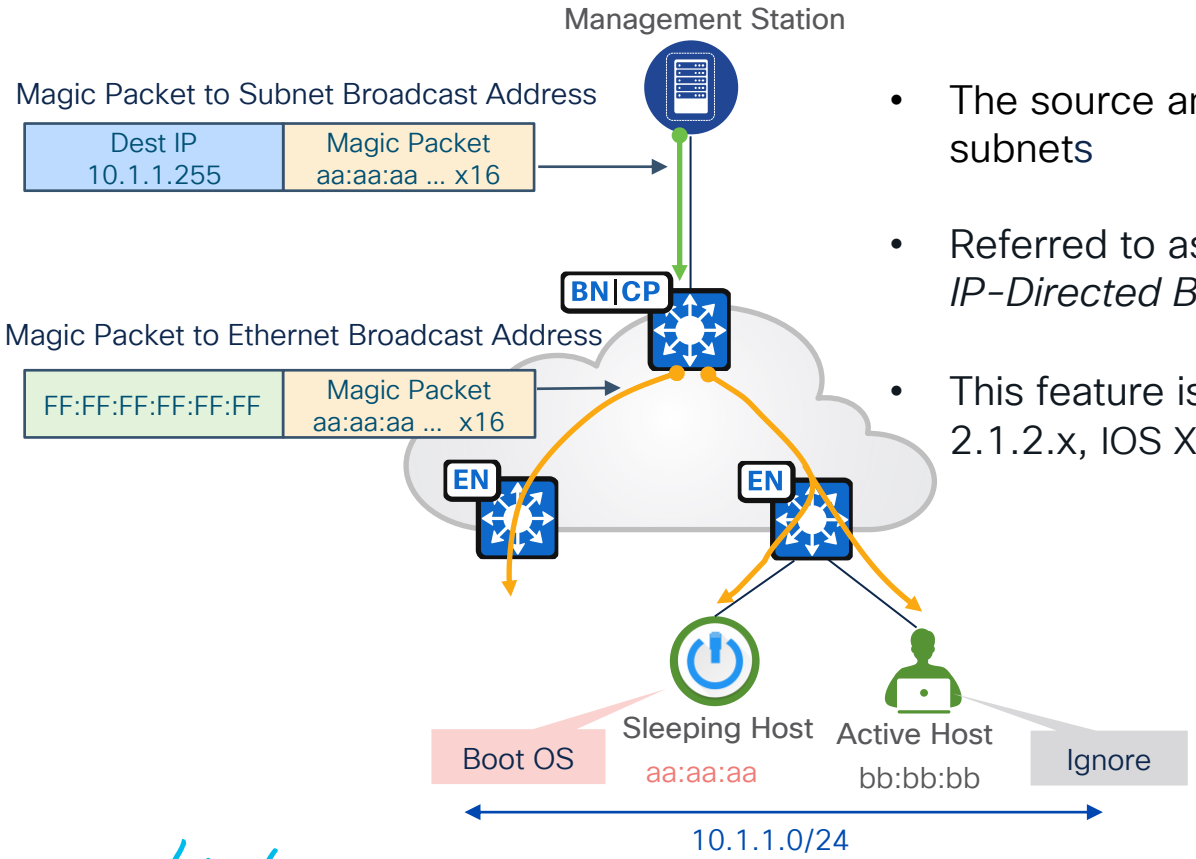
A host outside the fabric wakes the endpoint by sending a Wake on LAN Magic Packet using Subnet-Directed Broadcast + Ethernet Broadcast

Wake on LAN Ethernet Broadcast

- The source and destination are both in the same subnet
- This feature is supported with L2 Flooding in Cisco DNA Center ≥ 1.2.5/6



Wake on LAN Subnet-Directed Broadcast

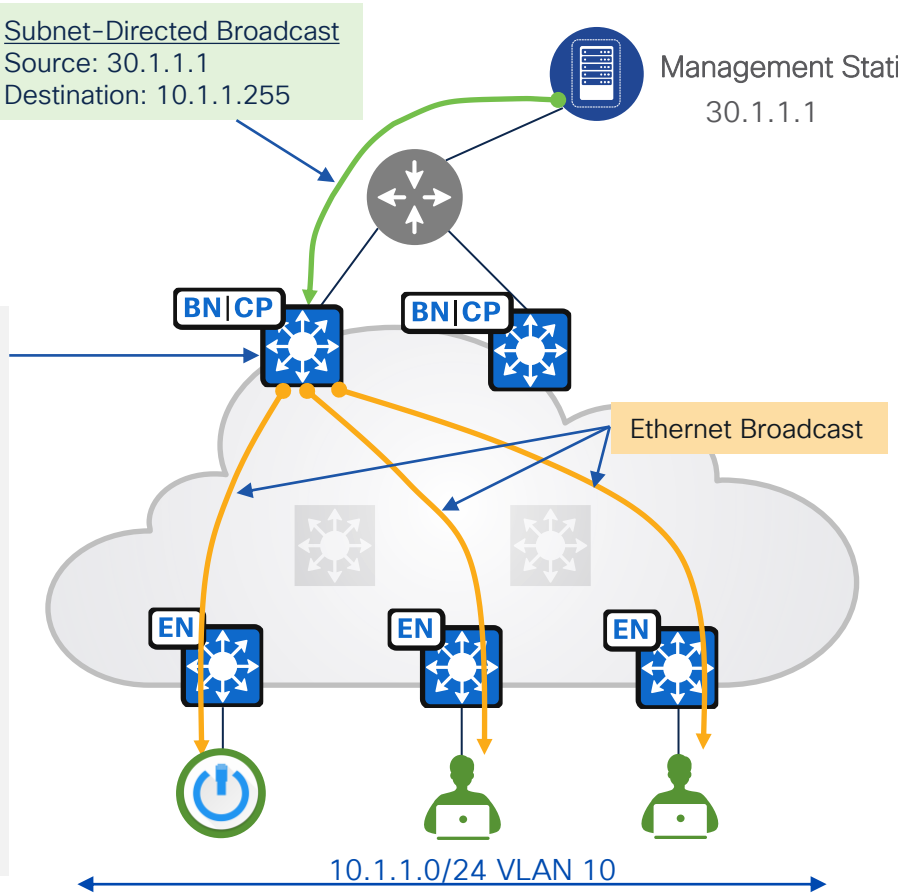


- The source and destination are in different subnets
- Referred to as *Subnet-Directed Broadcast* or *IP-Directed Broadcast*
- This feature is supported in Cisco DNA Center ≥ 2.1.2.x, IOS XE ≥17.3.1

Border Configurations

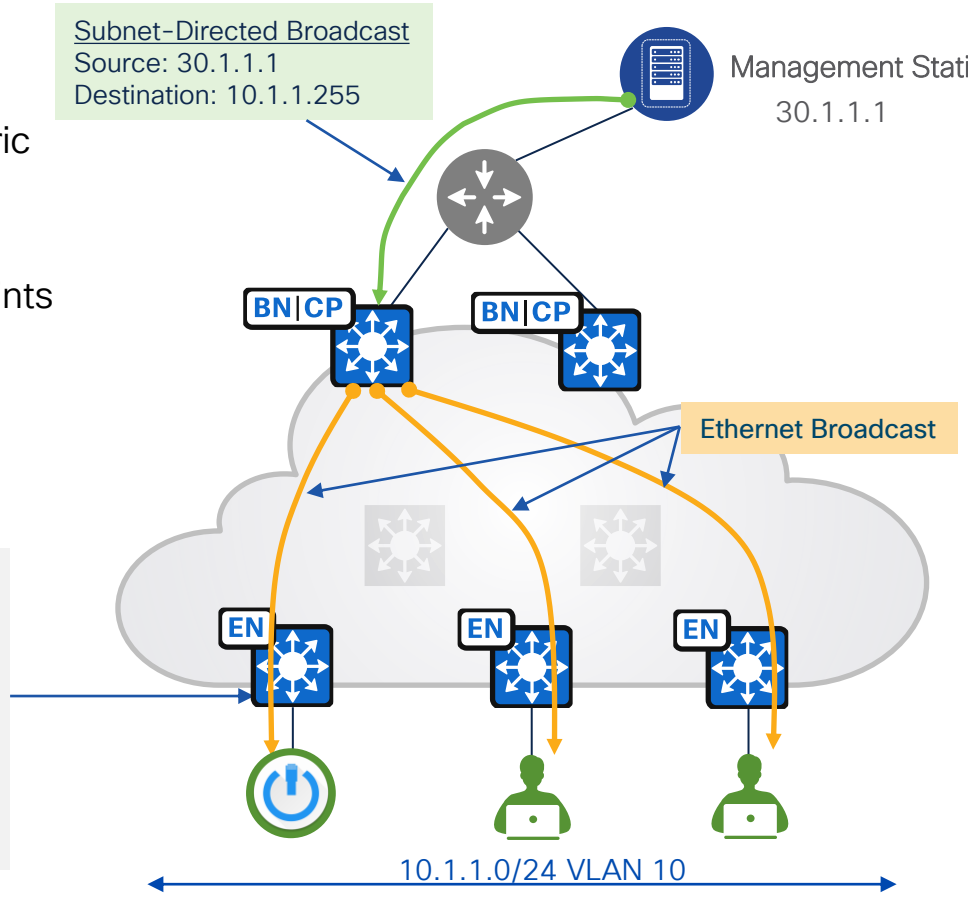
- Cisco DNA Center provisions an SVI on the L3 Border(s) instead of a Loopback
- SVI is enabled with the ***no autostate*** config so that the interface is always in "UP" state

```
interface Vlan10
    vrf forwarding Trusted
    ip directed-broadcast
    no autostate
interface Vlan3032
    description vrf interface to External Border
    vrf forwarding Trusted
    ip network-broadcast
router lisp
 instance-id 8202
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 10
   broadcast-underlay 239.0.17.1
   flood arp-nd
   flood unknown-unicast
   database-mapping mac locator-set <rloc>
```



Edge Configurations

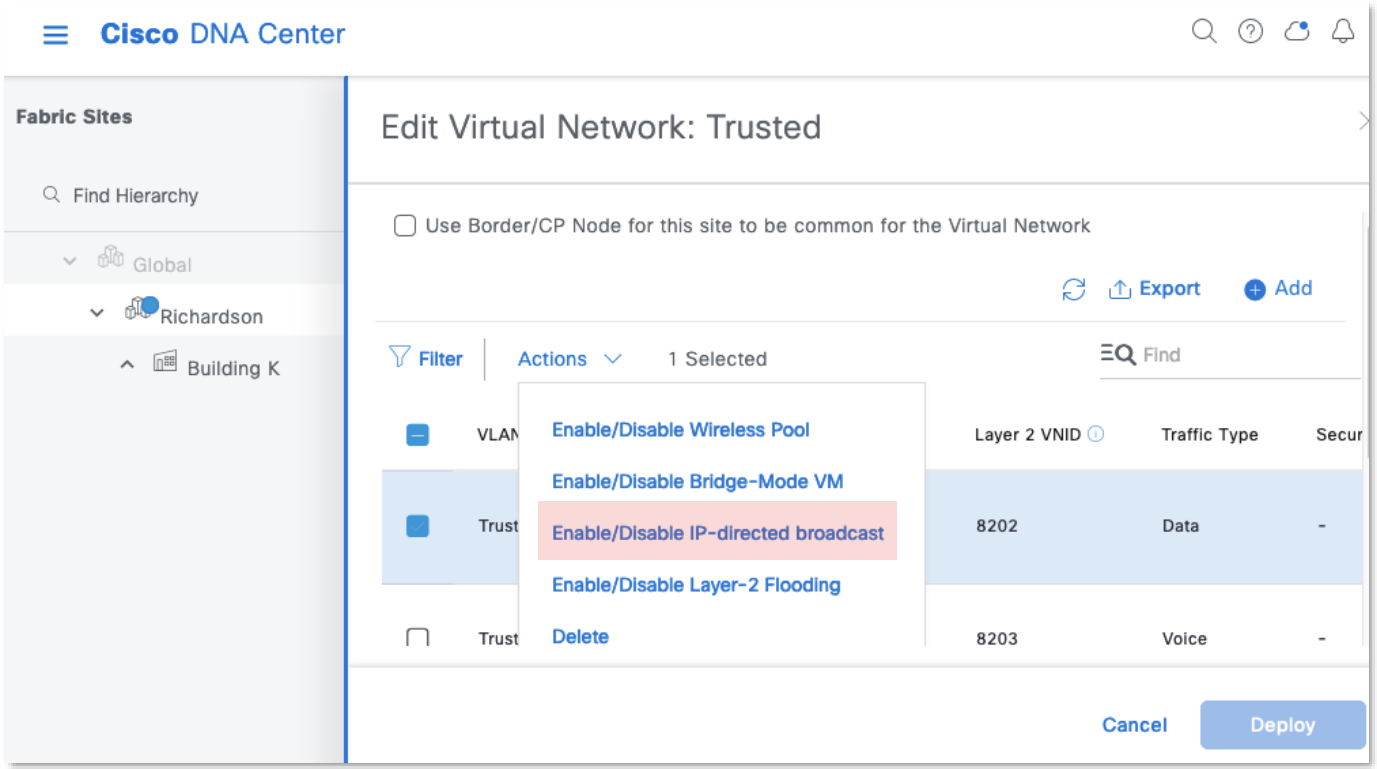
- A subnet-directed broadcast originating from outside of fabric is propagated inside the fabric as broadcast
- When an Edge node receives the frame, it forwards the packet as a broadcast to endpoints in the destination VLAN




```
router lisp
 instance-id 8202
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1035
   broadcast-underlay 239.0.17.1
   flood arp-nd
   flood unknown-unicast
   database-mapping mac locator-set <rloc>
```

IP-Directed Broadcast VLAN Configuration

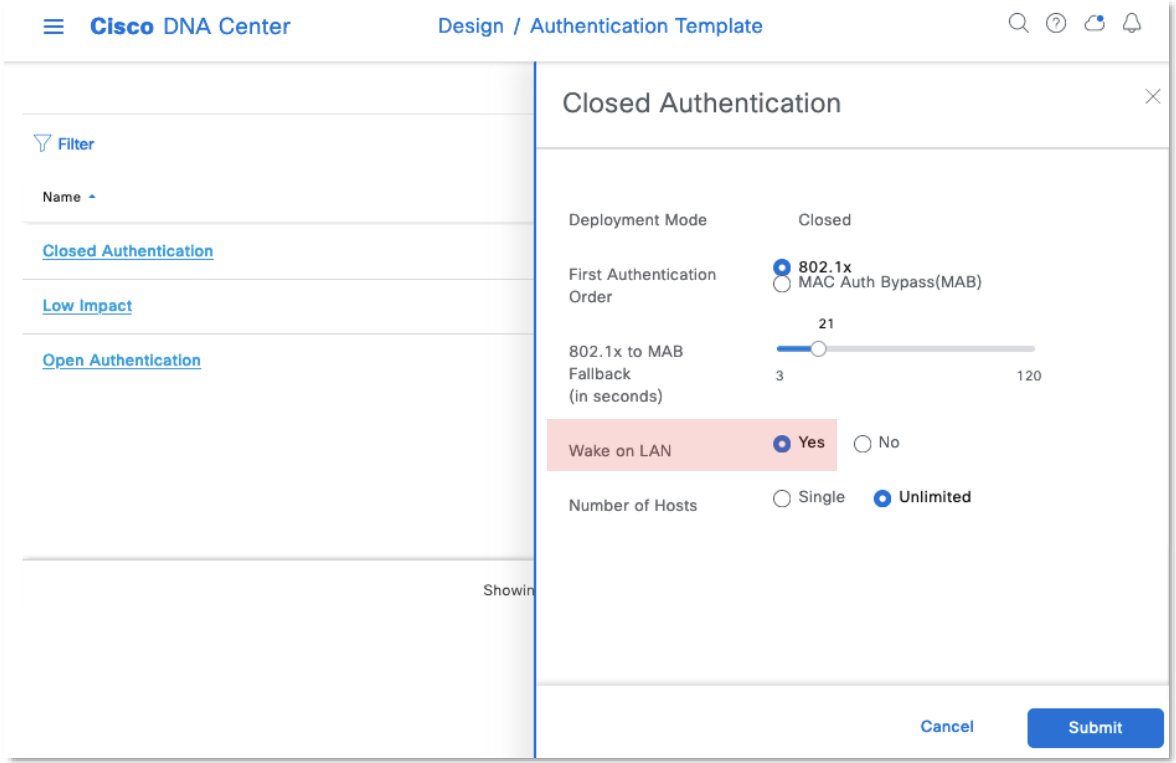
- Turning on IP-Directed broadcast for the subnet turns on L2 Flooding automatically



Provision → Fabric Sites → (Select a Site) → Host Onboarding → Virtual Networks → (Select a Virtual Network) → (Select a VLAN)

Wake on LAN Setting with Authentication Template

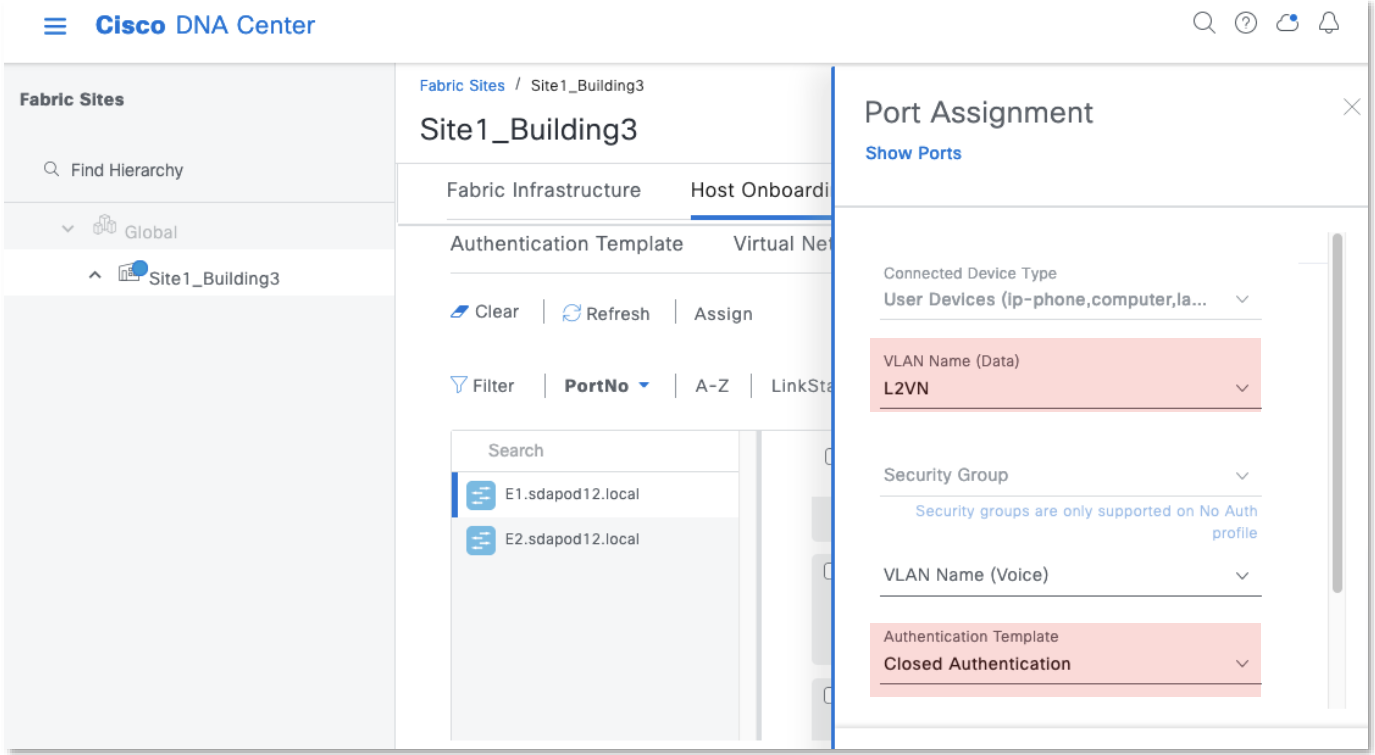
- Wake on LAN needs to be enabled when 802.1x is used (Open/Low Impact/Closed Authentication)



Design → Authentication Template → Closed Authentication/Low Impact/Open Authentication → Wake on LAN → Yes

Wake on LAN Port Configuration

- Static VLAN configuration on port assignment is required (dynamic VLAN not supported)



Provision → Fabric Sites → (Select a Fabric Site) → Host Onboarding → Port Assignment → (Select a switch) → (Select a port)

Design and Implementation Best Practices

Scale Considerations

L2 Border Endpoint Scale

- Consider L2 Border scale for endpoints

Refer to Cisco DNA Center Data Sheet: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html

L2 VN Scale

- Each L2 VN consumes one IP pool
- The sum of L2 VNs and IP pools per site should not exceed the Cisco DNA Center IP pool scale

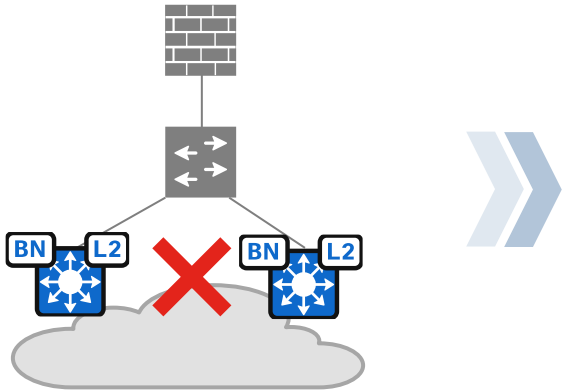
Refer to Cisco DNA Center Data Sheet: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html

VLAN Scale

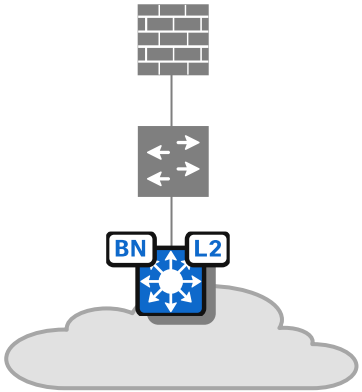
- All endpoints in a L2 VN will receive BUM traffic. Total number of endpoints in the L2 VN should be limited

Layer 2 Border Redundancy

- Multi-homing a VLAN on different L2 Borders connecting to the same external L2 domain is not supported
- To provide redundancy for the L2 Border, consider using switch stack or StackWise Virtual (SVL)



Multiple L2 Borders for the same VLAN

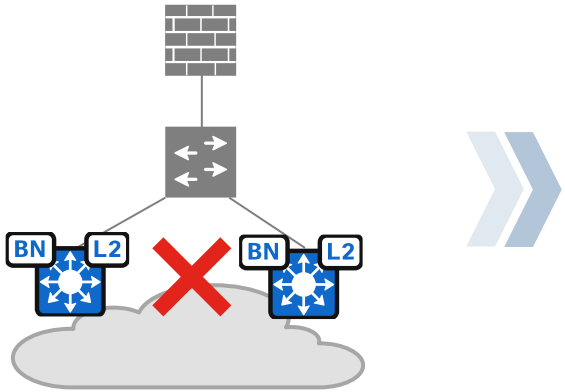


Switch Stack/SVL

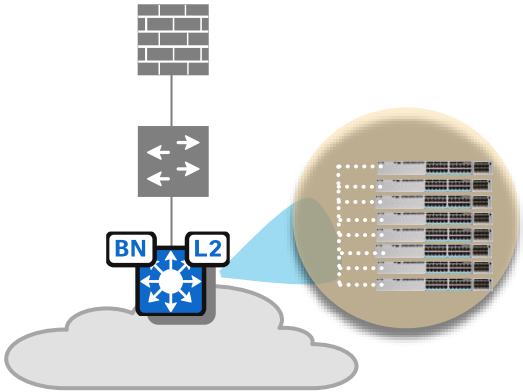
Layer 2 Border Redundancy

Switch Stack

- If the active switch becomes unavailable, the standby switch assumes the role of the active switch and continues to the keep the stack operational
- The stack is normally hosted in a single wiring closet
- Maximum of 8 C9000 switches can be in a stack
- All the stack members must be the same platform



Multiple L2 Borders for the same VLAN

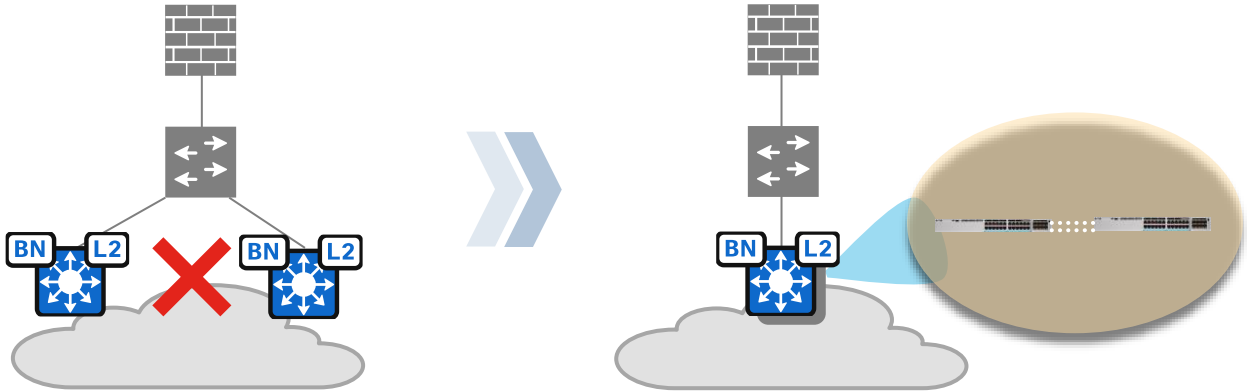


Switch Stack

Layer 2 Border Redundancy

StackWise Virtual (SVL)

- Stacking of only 2 switches
- Supports flexible distances with choices of cables and optics
- C9500 and C9500H are supported from Cisco DNA Center 1.3.3.x. C9400 and C9600 are supported from Cisco DNA Center 2.1.2.X
- ISSU is not supported for SDA

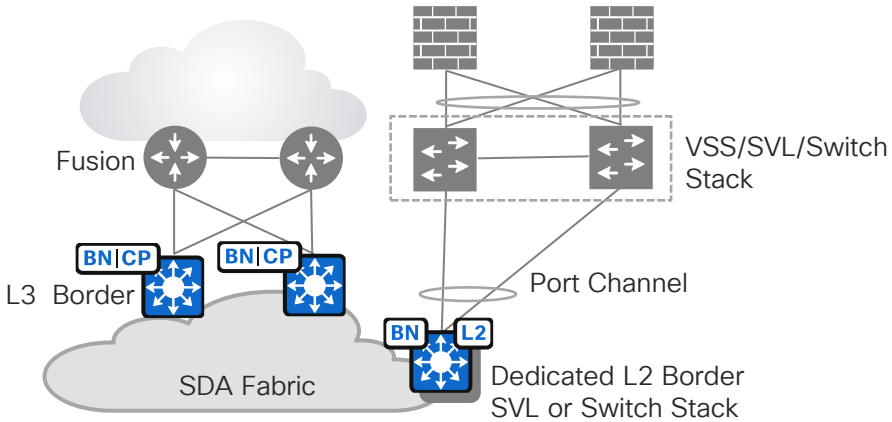


Multiple L2 Borders for the same VLAN

StackWise Virtual (SVL)

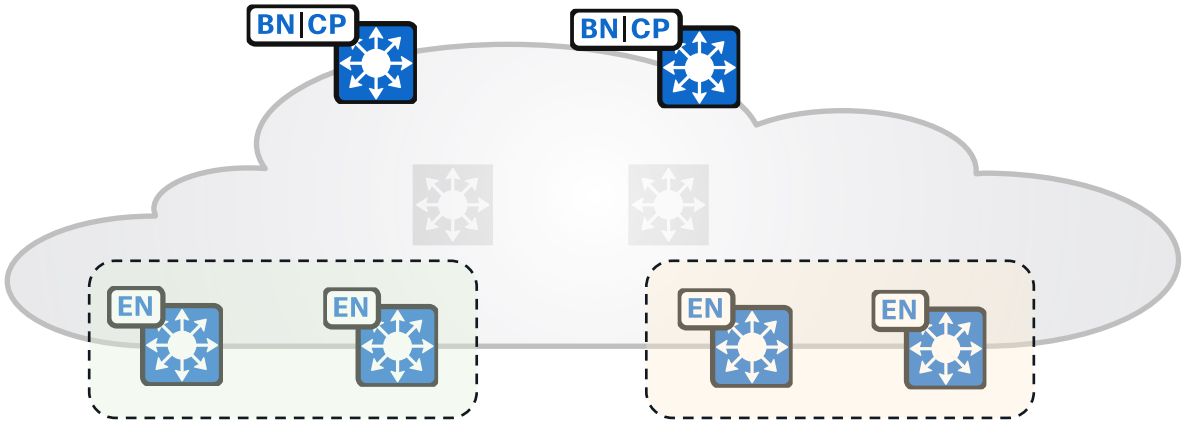
Layer 2 Border Recommendations

- L2 Border is recommended to be on a dedicated device
- If multiple VLANs being L2 handed off are critical, consider using separate L2 Borders each servicing different VLANs
- Use port channel at L2 Border for link redundancy



Layer 2 Virtual Network Recommendations

- Evaluate business requirement to determine whether a L2 VN or a L3 VN should be used
- If a L2 VN is needed only in certain part of the network, consider putting the L2 VN into a Fabric Zone to reduce the number of fabric Edges participate in the flooding



Fabric Zone: 1
Edge: 1-2
L2 VN: Sensor

Fabric Zone: 2
Edge: 3-4
L2 VN: None

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.

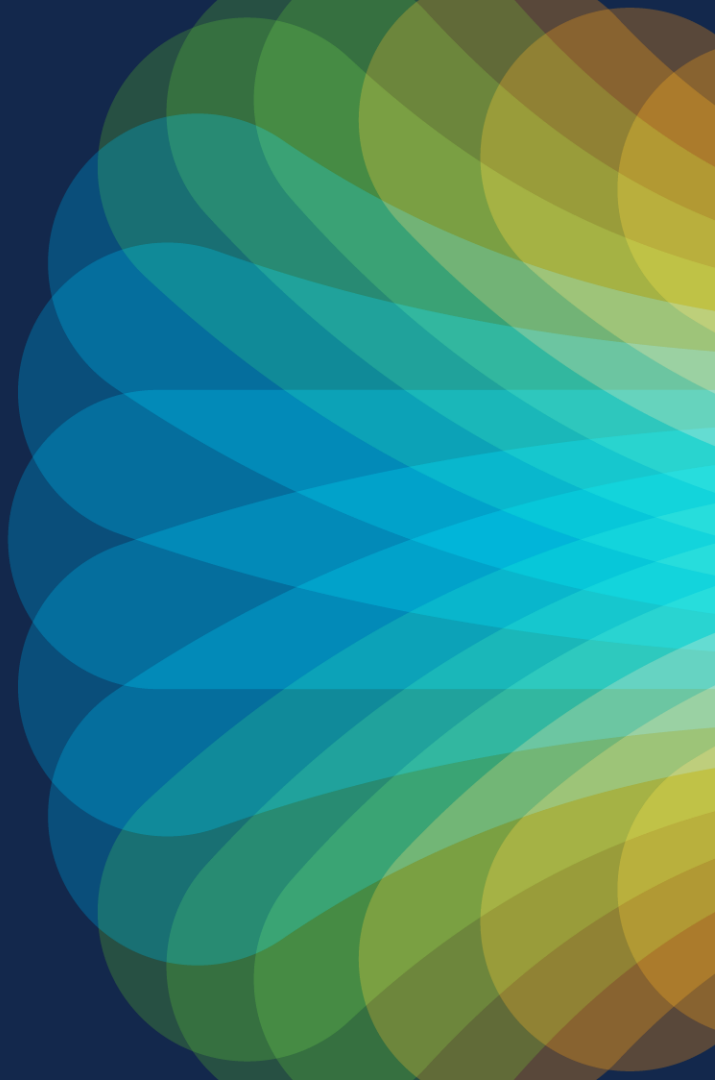
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

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

The bridge to possible

Thank you



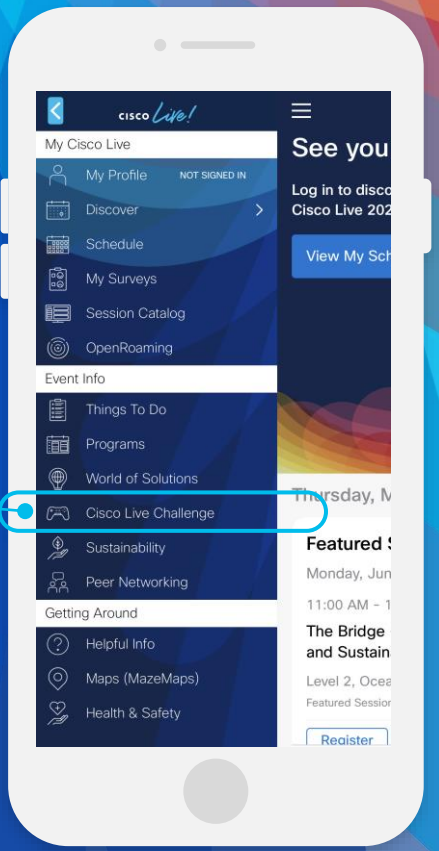
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive