



The bridge to possible

# IPv6 Enabled Cisco Wireless

Josh Halley, Principal Architect – Customer Experience EMEA

# 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 until February 24, 2023.





# Agenda

- Why IPv6 and Wireless
- WiFi Design – Traditional vs SDA
- LISP and VxLAN with IPv6
- IPv6 Wireless Client
- Packet Traces and Client traffic flows
- IPv6 Configuration DNAC
- Conclusion

# Who is Josh?



# About this Session

This Session is for:

- Understanding IPv6 support in Cisco SD-Access
- Understanding the LISP and VXLAN mechanism to support client IPv6.
- Look into the details of Packet/Frames captures on IPv6 communication
- Additional configuration on DNA-C to support IPv6 wireless clients.

This session is not for:

- Detailed IPv6 Protocol learning
- Cisco SD-Access concepts
- Setting up Cisco SD-Access Wireless

## Recommended Pre-session Learnings

BRKEWN-2020 : For Wireless SDA

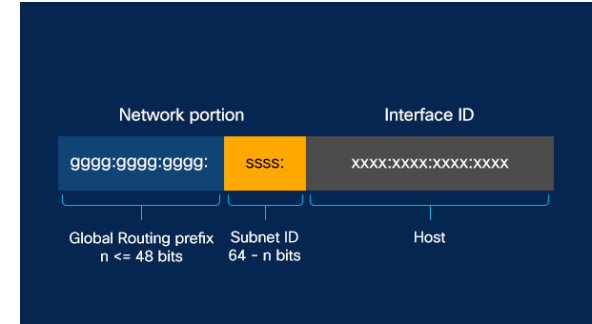
BRKSRT-2116 : Basics of IPv6

# IPv6 Basics



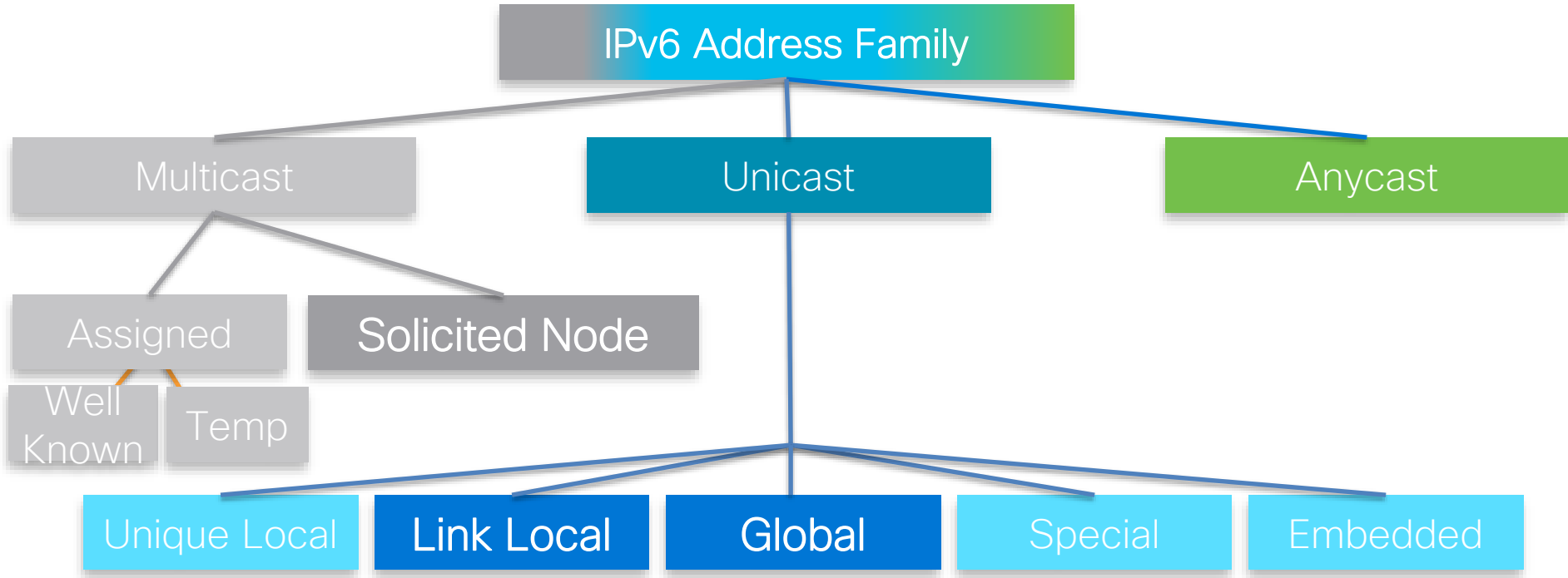
# Why IPv6

- Public IPv4 addresses are exhausted – we all know this.
- But also, IPv6 is more efficient
  - No Broadcast , ARP is replaced by new methods.
  - So many IP's we do not need NAT/PAT
  - Improved header
  - Stateless autoconfiguration – Works without DHCP



128-bit  
addresses

# IPv6 Addressing



**\*IPv6 does not use broadcast addressing**



# IPv6 Solicited Node Multicast

- Used by every device having IPv6 Address.
- Device responsibility to compute and join this address.
- Used for IPv6 Neighbor Discovery
- These addresses start with FF02::1:FF

ff02::1: All IPv6 devices

ff02::2: All IPv6 routers

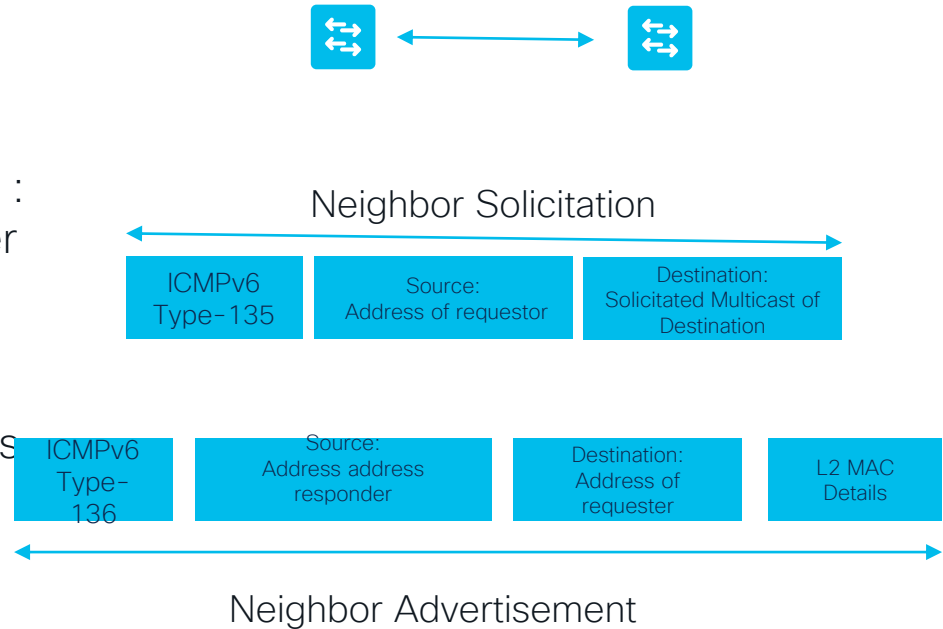
ff02::5: All OSPFv3 routers

ff02::a: All EIGRP (IPv6) routers

Representation	IPv6 Multicast Address
Preferred	ff00:0000:0000:0000:0000:0000:0000/8
Leading 0s omitted	ff00:0:0:0:0:0:0:0/8
Compressed	ff00::/8

# No ARP and No broadcast

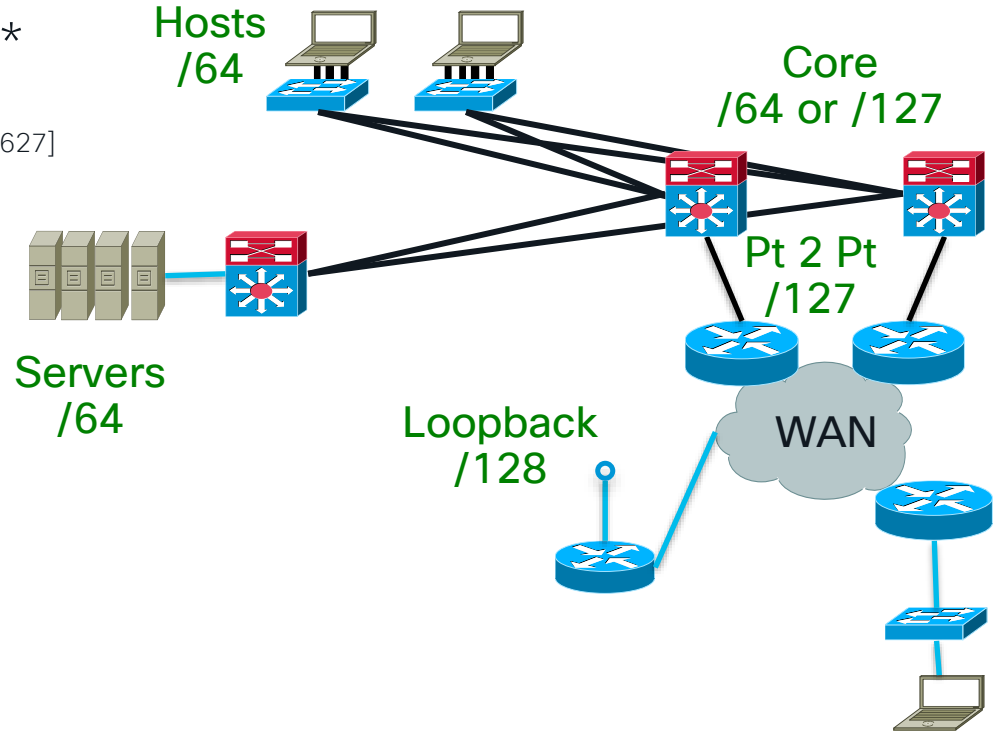
- ND (Neighbor discovery) replaces ARP
  - ND uses ICMPv6 and solicitate node multicast address.
  - Two Types of messages:
    1. Neighbor Solicitation Message :  
To find layer-2 address of other IPv6 address on the local link.
    2. Neighbor Advertisement message : reply to Neighbor solicitation message with details including Layer-2 address.
- Other Imp Message ICMPv6 message types:
- Route Solicitation
  - Router Advertisement



# Prefix Length Considerations

Refer to these sessions for detailed IPv6 Address planning  
BRKENT-2109 / BRKIPV-3340 / TECIPV-2000

- Anywhere a host exists use /64 \*
- Point to Point /127 [Consider impact of RFC3627]
- Loopback or Anycast /128

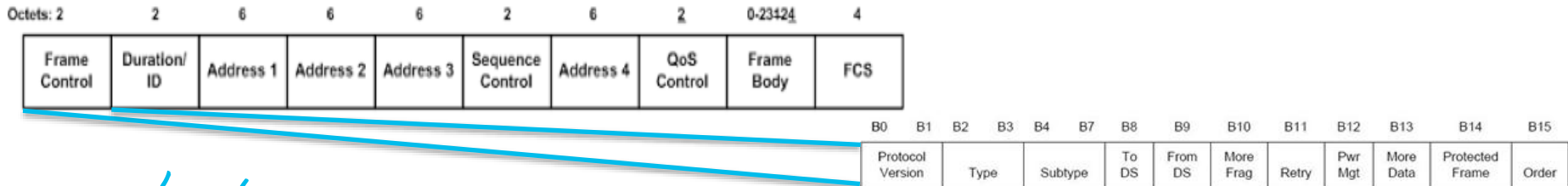


\* A prefix length other than a /64 in IPv6 will break the operation of the following technologies:

- Neighbor Discovery (ND)
- Secure Neighbor Discovery (SEND) [RFC3971]
- Privacy extensions [RFC4941]
- Parts of Mobile IPv6 [RFC4866]
- Protocol Independent Multicast - Sparse Mode (PIM-SM) with Embedded-RP [RFC3956]
- Site Multihoming by IPv6 Intermediation (SHIM6) [SHIM6]

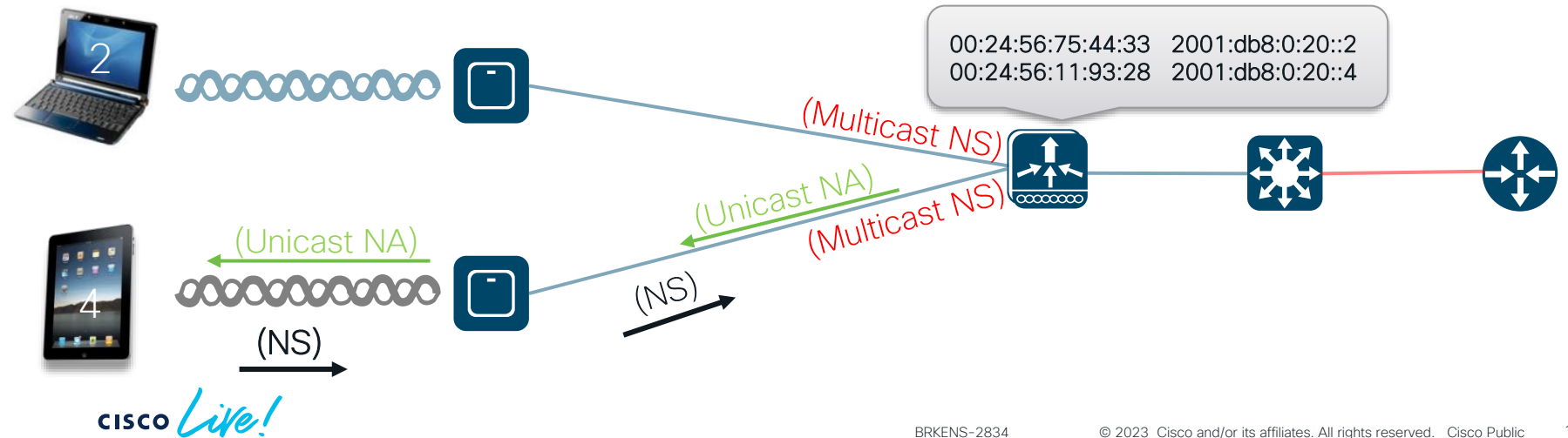
# Wi-Fi Multicast Background

- Radio is a shared media
  - Hosts must “awaken” to see if Multicast is for them
  - Multicast packets are not acknowledged or retransmitted
  - AP transmits bcast/mcast frames at the lowest possible rate
  - Broadcast/Multicast up to 10x more time in air
    - IEEE 802.11a mcast: 6 Mbps, ucast up to 54 Mbps
    - IEEE 802.11n mcast: 15 Mbps, ucast up to 150 Mbps
- 802.11 Header:
  - Protected Frame Field delineates acknowledged frames



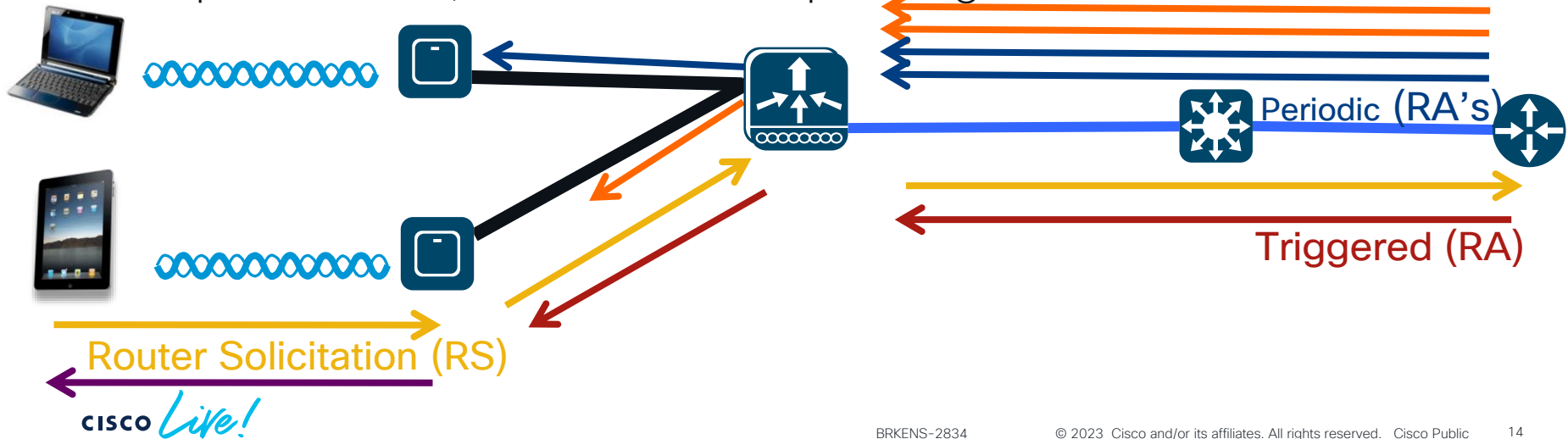
# Neighbour Discovery Multicast Suppression

- Scaling 802.11 multicast reliability issues
- NDP process is multicast “chatty”, Unicasting reduces the effect
- Caching allows the Controller to “proxy” the NA, based on gleaning



# Router Advertisement Throttler

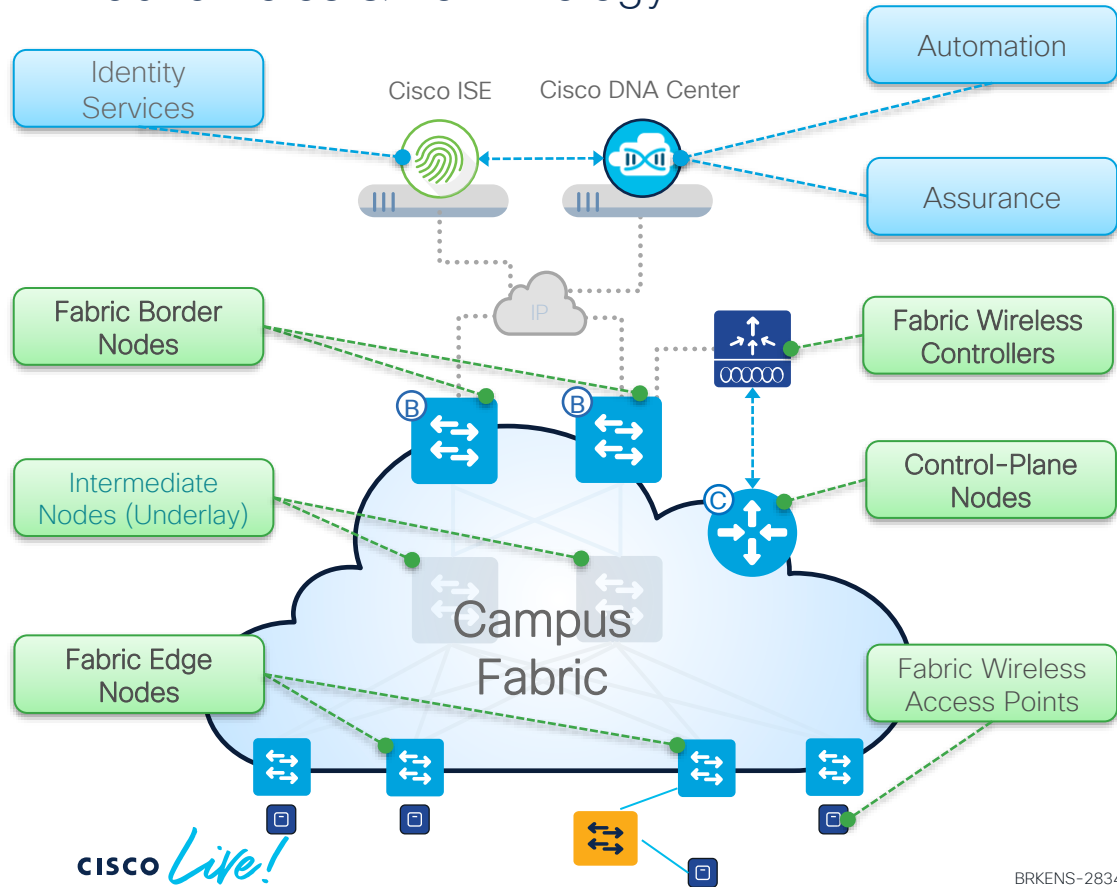
- Scaling the mobility access environment
- NDP process is multicast “chatty”, consumes airtime
- Rate limit RA’s from the legitimate router
- Inspect the RS, convert the responding RA to L2 Unicast



# Cisco SDA with IPv6

# Cisco SD-Access

## Fabric Roles & Terminology

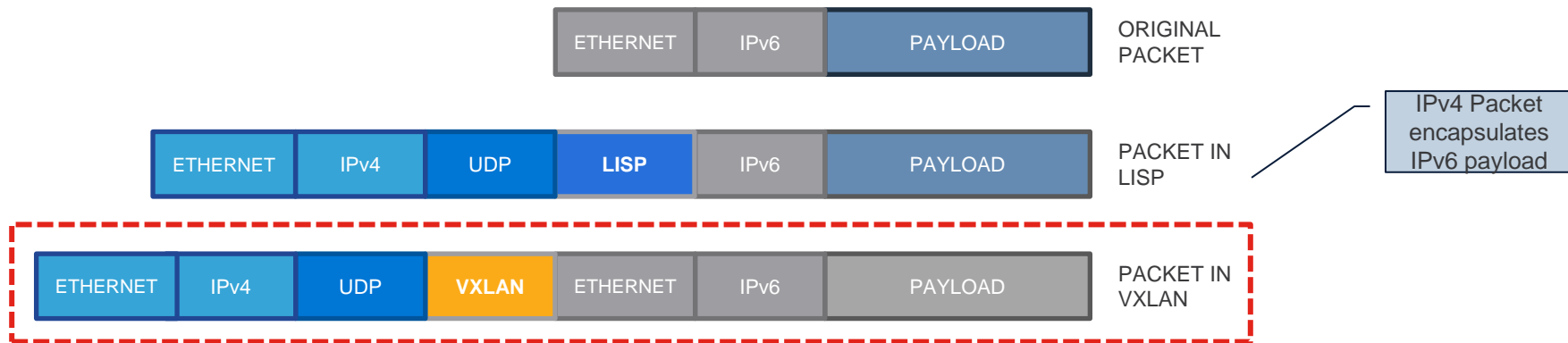


- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context.
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Control Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric.
- **Extended/Supplciant Based/Policy Extended Nodes**  
An edge access device that connects Wired Endpoints to the SDA Fabric via a Fabric Edge Node
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric
- **Wireless Access Points**– Wireless RADIO device to provide client access using 802.11



# IPv6 traffic inside LISP/VXLAN

1. Control-Plane based on LISP
2. Data-Plane based on VXLAN



# IPv4 AP Join – Steps in Fabric

All steps are similar for IPv6, however APs can only have IPv4 address in current release.

1. FE port is configured to onboard AP.
2. AP connects to FE port , via CDP AP notifies FE about its presence (This allows FE to assign right VLAN)
3. AP gets the IP address from DHCP server and FE registers AP & updates CP with AP details.
4. AP joins WLC via Traditional Methods (DHCP Option 43 or DNS)
5. WLC checks if AP is Fabric capable and Queries the CP for AP RLOC Information (e.g RLOC Requested/Response Received)
6. CP replies with the RLOC IP of the AP to the WLC
7. WLC registers the AP MAC in CP.
8. CP updates the FE with the details from WLC about the AP (This tells FE to initiate VXLAN tunnel with the AP)
9. FE processes the information and creates VXLAN tunnel with AP. At this point, AP will advertise Fabric Enabled SSID

IPv6 AP based discovery differs, through the usage of IPv6 DHCP Option 52 or CAPWAP discovery via AP Multicast Address FF01::18C

# AP join

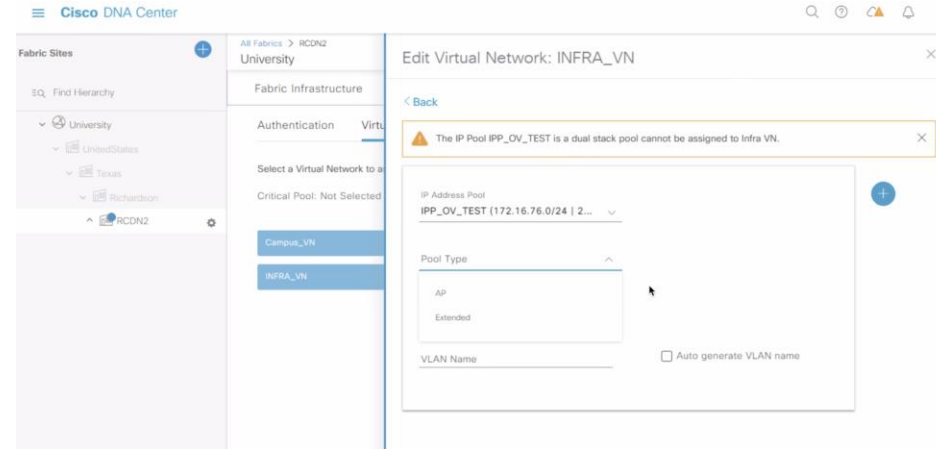
Access Points can only have IPv4 address with current release.

This means, **assigned** AP pools under Infra VN cannot be mapped with dual Stack IP Pools.

The remaining process is the same.

- AP to WLC communication is via Underlay CAPWAP.
- WLC to AP communication is via Overlay (VXLAN) CAPWAP

To anticipate future IPv6 AP onboarding support with DNA Center, it is recommended to already begin address planning for these ranges in your sites



# Reference Topology – For Packet Traces

WLC IPv4 address:  
172.16.33.2

Wireless Client1:

IPv6:

2001:0DB8:202b:4:324b:130c:435c:fa41

MAC: 74:da:da:f4:d6:35

AP IPv4:172.16.83.2

**Fabric Edge**

Loopback Ipv4 :172.16.81.70

Ipv6 SVI: 2001:0DB8:202b:4::1

CP/BR

IPv4:10.2.2.4

SDA Fabric

IPv6 DHCP  
Server2001:0DB8::2

Wireless Client 2:

IPv6: 2001:0DB8:202b:6:78aa:22f5:817c:9211

# AP-WLC Communication Trace

7348	181.509069	172.16.83.2	172.16.33.2	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[
7349	181.509069	172.16.83.2	172.16.33.2	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[
7350	181.510088	172.16.83.2	255.255.255.255	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[
7777	210.898981	172.16.83.2	172.16.33.2	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[
7778	210.898982	172.16.83.2	172.16.33.2	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[
7779	210.900395	172.16.33.2	172.16.83.2	CAPWAP-Control	199 CAPWAP-Control - Discovery Response
7780	210.900440	172.16.33.2	172.16.83.2	CAPWAP-Control	149 CAPWAP-Control - Discovery Response

```
> Frame 7778: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface \Device\NPF_{BBE1C365-1BDF-4FD8-87BC-2761E7F80154}, id 0
> Ethernet II, Src: Cisco_9f:53:67 (00:00:0c:9f:53:67), Dst: Cisco_cf:73:47 (6c:dd:30:cf:73:47)
> Internet Protocol Version 4, Src: 172.16.83.2, Dst: 172.16.33.2
> User Datagram Protocol, Src Port: 5270, Dst Port: 5246
> Control And Provisioning of Wireless Access Points - Control
  > Preamble
  > Header
  > Control Header
  > Message Element
[Malformed Packet: CAPWAP-CONTROL]
```

No VXLAN , Direct  
Communication via underlay

7349	181.509069	172.16.83.2	172.16.33.2	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[M
7350	181.510088	172.16.83.2	255.255.255.255	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[M
7777	210.898981	172.16.83.2	172.16.33.2	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[M
7778	210.898982	172.16.83.2	172.16.33.2	CAPWAP-Control	322 CAPWAP-Control - Discovery Request[M
7779	210.900395	172.16.33.2	172.16.83.2	CAPWAP-Control	199 CAPWAP-Control - Discovery Response
7780	210.900440	172.16.33.2	172.16.83.2	CAPWAP-Control	149 CAPWAP-Control - Discovery Response

```
> Frame 7779: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF_{BBE1C365-1BDF-4FD8-87BC-2761E7F80154}, id 0
> Ethernet II, Src: Cisco_cf:73:47 (6c:dd:30:cf:73:47), Dst: Cisco_0f:53:67 (00:7e:95:0f:53:67)
> Internet Protocol Version 4, Src: 10.2.2.4, Dst: 172.16.81.70
> User Datagram Protocol, Src Port: 5246, Dst Port: 5270
```

```
> Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 4097
    Reserved: 0
> Ethernet II, Src: Cisco_0f:53:67 (00:7e:95:0f:53:67), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
> Internet Protocol Version 4, Src: 172.16.33.2, Dst: 172.16.83.2
> User Datagram Protocol, Src Port: 5246, Dst Port: 5270
> Control And Provisioning of Wireless Access Points - Control
  > Preamble
  > Header
  > Control Header
  > Message Element
```

WLC to AP communication is encapsulated  
in VXLAN , as it is coming via Fabric.

This VXLAN tunnel is between FE and  
CP/BR . AP to FE is not yet established.

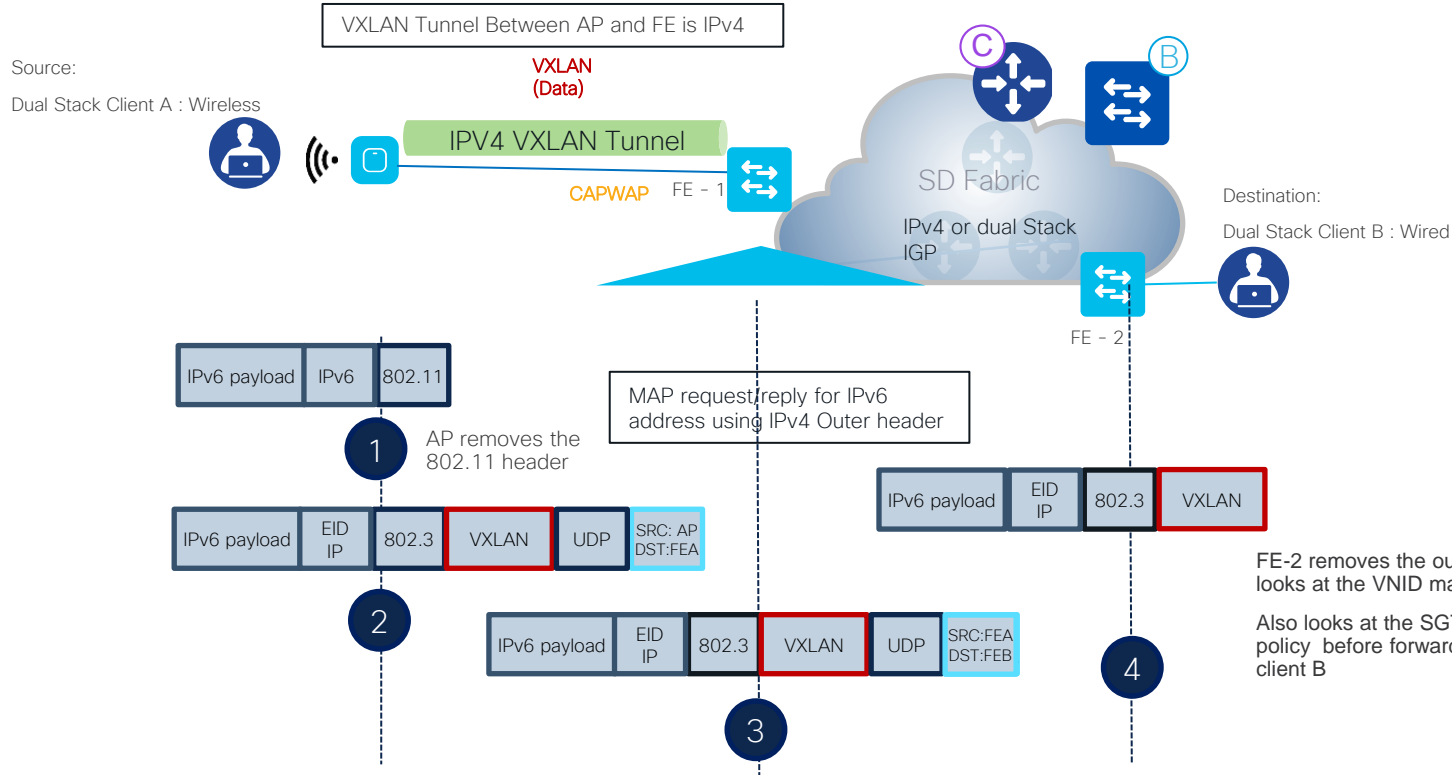
The packet capture shows IPv4 Access Tunnel Communications.

Once available – we expect a similar flow would take place with IPv6

# Client On-boarding : Dual Stack / IPv6

1. Client joins the Fabric enabled SSID on the AP
2. WLC knows the AP RLOC
3. Client Authenticates and WLC registers the Client L2 details with CP and updates AP.
4. Client initiates the IPv6 Addressing from configured methods – SLAAC/DHCPv6.
5. FE triggers IPv6 client registration to CP HTDB
6. AP to. FE and FE to other destinations use the VXLAN and LISP IPv6 encapsulation within IPv4 frames.

# Client Traffic Flows – Dual Stack

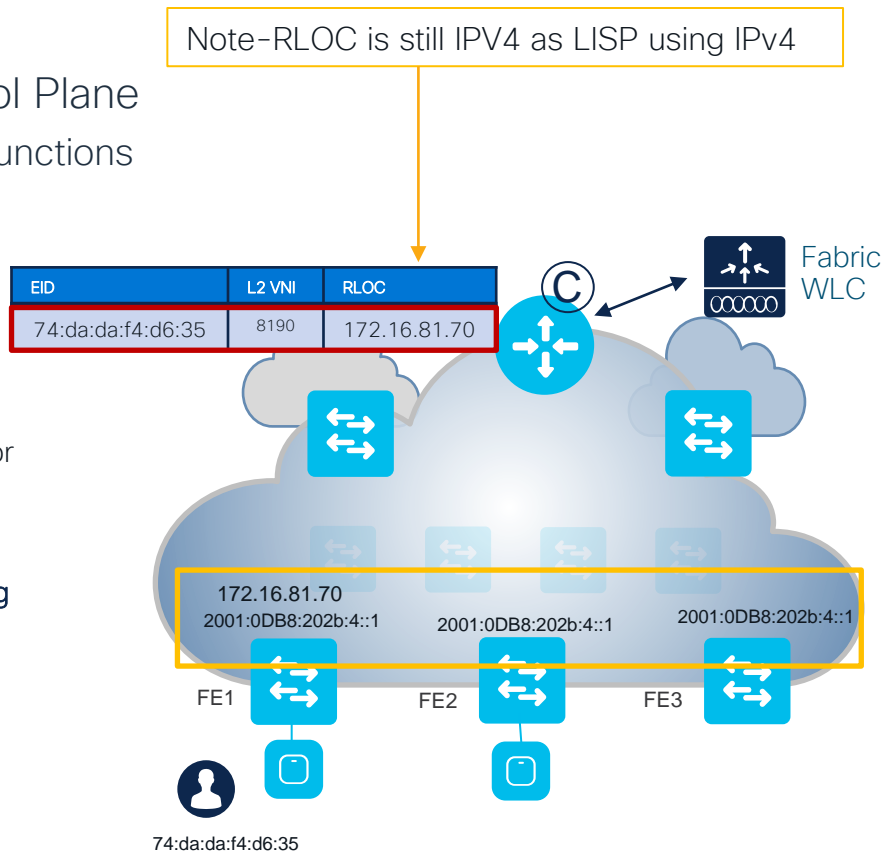


As current LISP implementation Uses IPv4, underlay routing must support IPv4 or dual stack

# RLOC for IPv6 Transport

Fabric Mode WLC integrates with the LISP Control Plane  
**Control Plane is centralized** at the WLC for all Wireless functions

- WLC is still responsible for : AP image/config, Radio Resource Management (RRM) and client session management and roaming
- For Fabric integration:
  - For wireless, **client MAC address is used as EID**
  - WLC interacts with the Host Tracking DB on Control-Plane node for Client **MAC address registration** with SGT and L2 VNI
  - The VN information is a **Layer 2 VN (L2 VNID)** information, and it's mapped to a VLAN on the FEs
  - WLC is responsible for **updating the Host Tracking DB with roaming** information for wireless clients
  - Fabric enabled WLC needs to be co-located at the same site with APs (latency between AP and WLC needs to be < 20 ms)

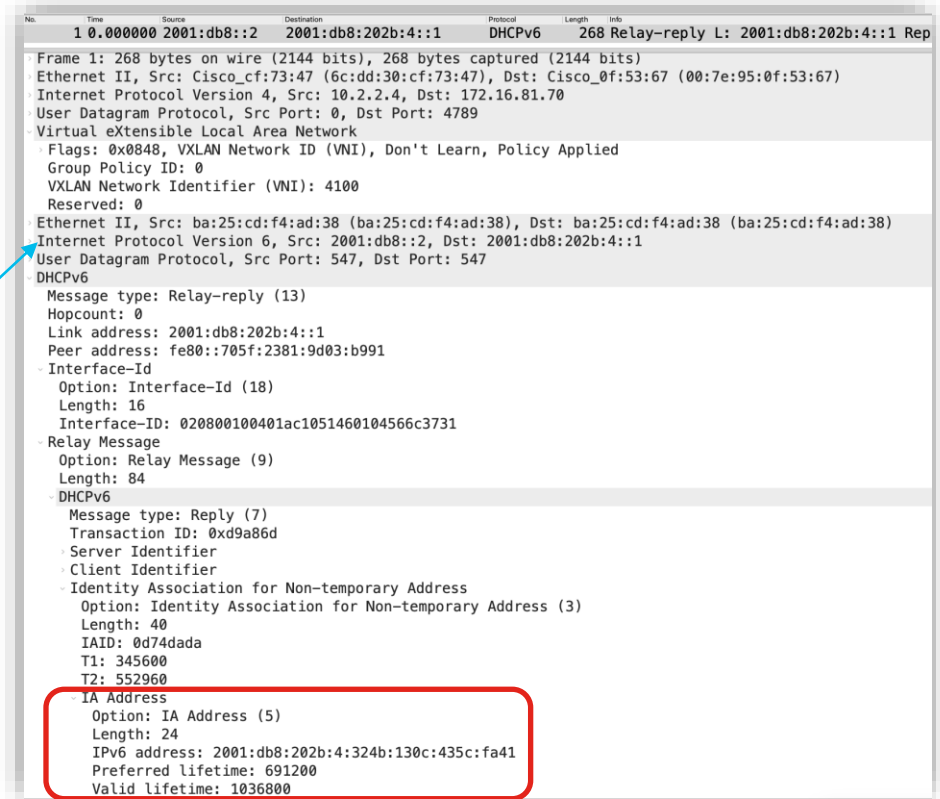




# IPv6 Packet Traces

# Client IPv6 Address

Capture is from Fabric Edge , Note the Source is DHCPv6 server and destination is FE G/w



```
No.    Time           Source                Destination            Protocol  Length  Info
1 0.000000 2001:db8::2          2001:db8:202b:4::1     DHCPv6   268     Relay-reply L: 2001:db8:202b:4::1 Rep

Frame 1: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface 0
Ethernet II, Src: Cisco_cf:73:47 (6c:dd:30:cf:73:47), Dst: Cisco_0f:53:67 (00:7e:95:0f:53:67)
Internet Protocol Version 4, Src: 10.2.2.4, Dst: 172.16.81.70
User Datagram Protocol, Src Port: 0, Dst Port: 4789
Virtual eXtensible Local Area Network
  Flags: 0x0848, VXLAN Network ID (VNI), Don't Learn, Policy Applied
  Group Policy ID: 0
  VXLAN Network Identifier (VNI): 4100
  Reserved: 0
Ethernet II, Src: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
Internet Protocol Version 6, Src: 2001:db8::2, Dst: 2001:db8:202b:4::1
User Datagram Protocol, Src Port: 547, Dst Port: 547
DHCPv6
  Message type: Relay-reply (13)
  Hopcount: 0
  Link address: 2001:db8:202b:4::1
  Peer address: fe80::705f:2381:9d03:b991
  Interface-Id
    Option: Interface-Id (18)
    Length: 16
    Interface-ID: 020800100401ac1051460104566c3731
  Relay Message
    Option: Relay Message (9)
    Length: 84
  DHCPv6
    Message type: Reply (7)
    Transaction ID: 0xd9a86d
    Server Identifier
    Client Identifier
    Identity Association for Non-temporary Address
      Option: Identity Association for Non-temporary Address (3)
      Length: 40
      IAID: 0d74dada
      T1: 345600
      T2: 552960
    IA Address
      Option: IA Address (5)
      Length: 24
      IPv6 address: 2001:db8:202b:4:324b:130c:435c:fa41
      Preferred lifetime: 691200
      Valid lifetime: 1036800
```

# Client IPv6 communication via AP

13119	340.061340	fe80::207e:1211:fe30:0002	fe80::207e:1211:fe30:0002	LISP	146 Encapsulated map-request for [0194] fe80::207e:1211:fe30:0002
13125	340.335487	::	ff02::1:ff03:b991	ICMPv6	128 Neighbor Solicitation for 2001:db8::705f:2381:9d03:b991
13126	340.335489	::	ff02::1:ff43:3eca	ICMPv6	128 Neighbor Solicitation for 2001:db8::65f6:300c:5843:3eca
13127	340.337723	::	ff02::1:ff03:b991	ICMPv6	128 Neighbor Solicitation for 2001:db8::705f:2381:9d03:b991
13128	340.350370	fe80::705f:2381:9d03:b991	ff02::1:3	LLMNR	145 Standard query 0xe4ca ANY 1S3LR7K7DFNINKJ

> Frame 13125: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface \Device\NPF\_{BBE1C365-1BDF-4FD8-87BC-2761E7FB0154}, id 0

> Ethernet II, Src: Cisco\_76:5e:f8 (70:69:5a:76:5e:f8), Dst: Cisco\_9f:fe:f5 (00:00:0c:9f:fe:f5)

> Internet Protocol Version 4, Src: 172.16.83.2, Dst: 172.16.81.70

> User Datagram Protocol, Src Port: 49407, Dst Port: 4789

✓ Virtual eXtensible Local Area Network

> Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)

Group Policy ID: 0

VXLAN Network Identifier (VNI): 8194

Reserved: 0

> Ethernet II, Src: D-LinkIn\_f4:d6:25 (74:da:da:f4:d6:25), Dst: IPv6mcast\_ff:03:b9:91 (33:33:ff:03:b9:91)

✓ Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff03:b991

0110 .... = Version: 6

> .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... 0000 0000 0000 0000 0000 = Flow Label: 0x00000

Payload Length: 24

Next Header: ICMPv6 (58)

Hop Limit: 255

Source Address: ::

Destination Address: ff02::1:ff03:b991

> Internet Control Message Protocol v6

Note VXLAN tunnel  
between AP and FE is  
IPV4 while the Payload  
from the client is IPv6

# Map Register for IPv6 client - LISP

```
4110 249.308705 10.2.2.4 172.16.81.70 LISP 80 Msg: 15, Registration ACK
4118 249.382776 172.16.81.70 10.2.2.4 LISP 316 Msg: 20, Registration for [4100] 2001:db8:202b:4:324b:130c:435c:fa41/128; Msg: 21
4119 249.382777 10.2.2.4 172.16.81.70 LISP 228 Msg: 16, Registration ACK; Msg: 17, Registration ACK; Msg: 18, Mapping Notification
4123 249.600334 172.16.81.70 10.2.2.4 LISP 316 Msg: 21, Registration for [4100] 2001:f38:202b:4:324b:130c:435c:fa41/128

> Frame 4118: 316 bytes on wire (2528 bits), 316 bytes captured (2528 bits) on interface \Device\NPF_{BBE1C365-1BDF-4FD8-87BC-2761E7F80154}, id 0
> Ethernet II, Src: Cisco cf:73:46 (6c:dd:30:cf:73:46), Dst: Cisco a0:60:61 (8d:8a:8d:a0:60:61)
> Internet Protocol Version 4, Src: 172.16.81.70, Dst: 10.2.2.4
> Transmission Control Protocol, Src Port: 41629, Dst Port: 4342, Seq: 1101, Ack: 935, Len: 262
▼ Locator/ID Separation Protocol (Reliable Transport), Msg: 20, Registration for [4100] 2001:f38:202b:4:324b:130c:435c:fa41/128
  Type: Registration (17)
  Length: 138
  Message ID: 20
  > Map-Register
    Message End Marker: 0x9facade9 (correct)
▼ Locator/ID Separation Protocol (Reliable Transport), Msg: 21, Registration for [4100] 2001:f38:202b:4:324b:130c:435c:fa41/128
  Type: Registration (17)
  Length: 124
  Message ID: 21
▼ Map-Register
  > .... 1010 0000 0000 0000 0001 = Flags: 0xa0001
    Record Count: 1
    Nonce: 0x3e9a2e3b4bbe9e0f
    Key ID: 0x0001
    Authentication Data Length: 20
    Authentication Data: cb4a5aa0ac1a6e04dfd071f7b850b21273ba2d71
    Mapping Record 1, L20 Prefix: [4100] 2001:f38:202b:4:324b:130c:435c:fa41/128, IFL: 1440, Action: No Action, Authoritative
    xTR-ID: da9846033a51e45d42efae5bf36ea588
    Site-ID: 0000000000000000
    Message End Marker: 0x9facade9 (correct)
```

# IPv6 Map request - LISP

```
12032 281.475761 2001:db8:202b:4:324b:130c:435c:fa41 2001:db8:202b:4:324b:130c:435c:fa41 LISP 146 Encapsulated Map-Request for [8194] 2001:db8:202b:4:324b:130c:435c:fa41/128
> Internet Protocol Version 4, Src: 172.16.81.70, Dst: 10.2.2.4
> User Datagram Protocol, Src Port: 4342, Dst Port: 4342
> Locator/ID Separation Protocol
  1000 .... = Type: Encapsulated Control Message (8)
  .... 0... = S bit (LISP-SEC capable): Not set
  .... 0... = D bit (DDT-originated): Not set
  .... 0000 0000 0000 0000 0000 0000 = Reserved bits: 0x00000000
  Internet Protocol Version 6, Src: 2001:db8:202b:4:324b:130c:435c:fa41, Dst: 2001:db8:202b:4:324b:130c:435c:fa41
  0110 .... = Version: 6
  > .... 1100 0000 .... = Traffic Class: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  .... 0000 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 60
  Next Header: UDP (17)
  Hop Limit: 255
  Source Address: 2001:db8:202b:4:324b:130c:435c:fa41
  Destination Address: 2001:db8:202b:4:324b:130c:435c:fa41
> 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
  .... .... 0000 0000 = ITR-RLoc Count: 0
  Record Count: 1
  Nonce: 0xaa2ec219b835bb2c
  Source EID AFI: Reserved (0)
  Source EID: not set
  > ITR-RLoc 1: 172.16.81.70
  > Map-Request Record 1: [8194] 2001:db8:202b:4:324b:130c:435c:fa41/128
```

Outer LISP  
header is IPv4

# IPv6 Map Cache on the FE

```
Pod2-Edge-2#sh lisp eid-table vrf Campus_VN ipv6 map-cache
LISP IPv6 Mapping Cache for EID-table vrf Campus_VN (IID 4100), 6 entries

::/0, uptime: 6w4d, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
2001:DB8:202B:3::/64, uptime: 3w1d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2001:DB8:202B:4::/64, uptime: 3w1d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2001:DB8:202B:4:324B:130C:435C:FA41/128, uptime: 00:00:05, expires: 23:59:54, via map-reply, self, complete
  Locator      Uptime    State    Pri/Wgt    Encap-IID
  172.16.81.70 00:00:05 up, self  10/10      -
2001:DB8:202B:6::/64, uptime: 1w2d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR

Pod2-Edge-2#
```

# IPv6 Traffic between Clients on same AP

Source	Destination	Protocol	Layer 2 VNI	Source Port	Info
2001:db8:202b:4:324b:130c:435c:fa41	2001:db8:202b:6:78aa:22f5:817c:9211	ICMPv6	8192	7936	Echo (ping) request id=0x0001, seq=148, hop limit=63 (no response found)
2001:db8:202b:4:324b:130c:435c:fa41	2001:db8:202b:6:78aa:22f5:817c:9211	ICMPv6	8194	7936	Echo (ping) request id=0x0001, seq=148, hop limit=64 (reply in 3)
2001:db8:202b:6:78aa:22f5:817c:9211	2001:db8:202b:4:324b:130c:435c:fa41	ICMPv6	8192	7936	Echo (ping) reply id=0x0001, seq=148, hop limit=64 (request in 2)

Frame 2: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface \Device\NPF\_{BBE1C365-1BDF-4FD8-87BC-2761E7FB0154}, id 0

Ethernet II, Src: Cisco\_76:5e:f8 (70:69:5a:76:5e:f8), Dst: Cisco\_9f:fe:f5 (00:00:0c:9f:fe:f5)

Internet Protocol Version 4, Src: 172.16.83.2, Dst: 172.16.81.70

User Datagram Protocol, Src Port: 49407, Dst Port: 4789

Virtual eXtensible Local Area Network

Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)

Group Policy ID: 7936

VXLAN Network Identifier (VNI): 8194

Reserved: 0

Ethernet II, Src: D-LinkIn\_f4:d6:25 (74:da:da:f4:d6:25), Dst: Cisco\_9f:fa:85 (00:00:0c:9f:fa:85)

Internet Protocol Version 6, Src: 2001:db8:202b:4:324b:130c:435c:fa41, Dst: 2001:db8:202b:6:78aa:22f5:817c:9211

Internet Control Message Protocol v6

Type: Echo (ping) request (128)

Code: 0

Checksum: 0x066f [correct]

[Checksum Status: Good]

Identifier: 0x0001

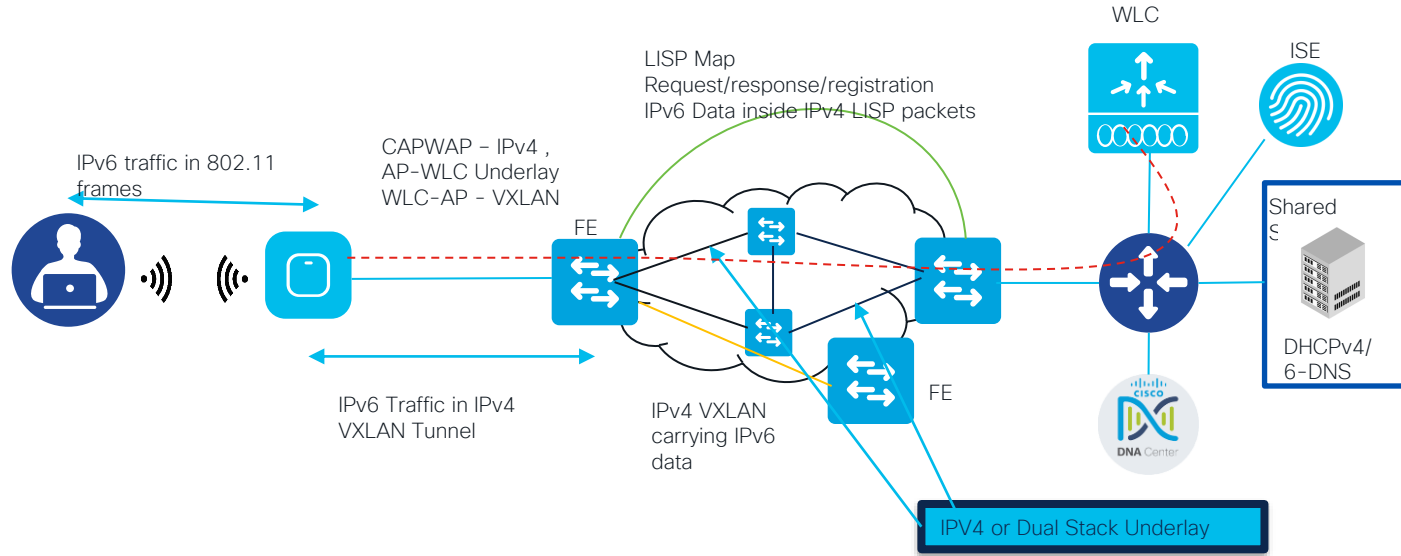
Sequence: 148

[\[Response In: 3\]](#)

Data (32 bytes)



# Summarizing flow





# IPv6 Configuration via DNAC

# IPv6 Features supported

- Address pools with DHCPv6 and DNSv6
- Host onboarding
- Multicast source/receiver inside/outside the fabric
- L2/L3 border handoff
- Clients connected behind Extended node EN/ Policy Extended Nodes
- First hop security features like RA guard and DHCP guard.

## WLC Support for IPv6

- Catalyst 9800 Series WLC
- eWLC
- Embedded WLC

### Client IPv6 Address

- Static
- SLAAC [CIDR /64]
- DHCPv6

# IPv6 address pools with DHCPv6 and DNSv6

- Address pools can be IPv4 only or dual-stack
- IPv6 DHCP and DNS needed for pool with IPv6. ISE, Syslog and SNMP server still IPv4.
- First create IPv4 and IPv6 pools at global level. 3 ways:
  - Manually configure
  - Import from IPAM server
  - Import from CSV file
- Then reserve pools (IPv4 or dual-stack) at site level

# IPv6 DHCP and DNS

Cisco DNA Center

DESIGNPOLICYPROVISION

Network Hierarchy

Network Settings

Image Repository

Network Profiles

Authentication Template

Find Hierarchy

Global

Milpitas

SanJose

SJC15

SJC24

Network

Device Credentials

IP Address Pools

QoS

Wireless

Setup network properties like AAA, NTP, Syslog, Trap and Netflow using the "Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings.

Network Telemetry

Add Servers

DHCP Server

DHCP

Additional DHCP

10.20.30.40

2001:0db8::10

Supports both IPv4 and IPv6

Supports both IPv4 and IPv6

DNS Server

Domain Name

cisco.com

Primary

Secondary

192.168.10.20

2001:0db8::20

Supports both IPv4 and IPv6

Supports both IPv4 and IPv6

SYSLOG Server

Cisco DNA Center as syslog server

SYSLOG

Reset

Save

# Create IPv4 and IPv6 Pools at Global level

Cisco DNA Center

DESIGNPOLICYPROVISION

Network Hierarchy

Network Settings

Image Repository

Network Profiles

Authentication Template

Find Hierarchy

Global

Milpitas

SanJose

SJC15

SJC24

IP Address Pools (4)

ImportExportTake a Tour

Subnet TypeAllIPv4IPv6

Filter0 SelectedAddMore Actions

As of: Dec 23, 2022 1:38 PM

	Name	Type	IPv4 Subnet	IPv4 Used	IPv6 Subnet	IPv6 Used	Actions
<input type="checkbox"/>	10_0_0_0	Generic	10.0.0.0/8	0%	-	-	...
<input type="checkbox"/>	172_16_0_0	Generic	172.16.0.0/12	0%	-	-	...
<input type="checkbox"/>	192_168_0_0	Generic	192.168.0.0/16	0%	-	-	...
<input type="checkbox"/>	2001_0db8	Generic	-	-	2001:db8::/36	100%	...

# Reserve Pools (IPv4 or Dual stack) at Site level

**Cisco DNA Center**   DESIGN   POLICY   PROVISION

Network Hierarchy   **Network Settings**   Image Repository   Network Profiles   Authentication Template

Find Hierarchy

- Global
  - Milpitas
  - SanJose**
    - SJC15
    - SJC24

IP Address Pools

Subnet Type: **All**   IPv4 only   Dual-Stack

Filter   0 Selected   Reserve   More Actions

As of: Dec 23, 2022 1:34 PM

<input type="checkbox"/>	Name	Type	IPv4 Subnet	IPv4 Used	IPv6 Subnet	IPv6 Used	Inherited from	Actions
<input type="checkbox"/>	AP_Pool	Generic	10.168.110.0/24	0% <span>1</span>	2001:db8::/64	0% <span>1</span>	Site-1	...
<input type="checkbox"/>	BGP_Pool	Generic	10.0.0.0/24	0% <span>1</span>	2001:db8:0:1::/64	0% <span>1</span>	-	...
<input type="checkbox"/>	Client_Pool	Generic	10.0.1.0/24	0% <span>1</span>	2001:db8:0:2::/64	0% <span>1</span>	-	...
<input type="checkbox"/>	Client_Pool2	Generic	10.0.2.0/24	0% <span>1</span>	2001:db8:0:3::/64	0% <span>1</span>	-	...

# Reserving a Pool (IPv4 or Dual stack)

Cisco DNA Center

Network

Device Credentials

IP Address Pools

SP Profiles

Wireless

Telemetry

Security and Trust

Find Hierarchy

Search Help

Global

Site-1

S1-BLDG1

IP Address Pools (4)

Subnet Type

All

IPv4 only

Dual-Stack

Filter

0 Selected

Reserve

More Actions

<input type="checkbox"/>	Name	Type	IPv4 Subnet
<input type="checkbox"/>	AP_Pool	Generic	10.168.110.0/24
<input type="checkbox"/>	BGP_Pool	Generic	10.0.0.0/24
<input type="checkbox"/>	Client_Pool	Generic	10.0.1.0/24
<input type="checkbox"/>	Client_Pool2	Generic	10.0.2.0/24

Reserve IP Pool

IP Address Pool Name\*

New\_Client\_Pool

Type\*

Generic

Options

IP Address Space

☐ IPv4 (Default)

☒ IPv6

Check both IPv4 and IPv6 to create a dual-stack pool. If the pool is used for infra VN, or if the fabric contains devices that don't support IPv6, check only IPv4.

IPv4

Global Pool\*

10.0.0.0/8 (10\_0\_0\_0)

Tunnel pools are not available for reserving for Site(s).

IPv6

Global Pool\*

2001:db8::/36 (2001\_0db8)

Prefix length / Number of IP Addresses

☒ Prefix length

☐ Number of IP Addresses

Prefix length\*

/24 (255.255.255.0)

Prefix length / Number of IP Addresses

☒ Prefix length

☐ Number of IP Addresses

Prefix length\*

/64

IPv4 Subnet

10.20.30.0

For Example - 192.0.2.0

IPv6 Subnet

Gateway

10.20.30.1

Gateway

DHCP Server(s)

10.50.50.50 x

DHCP Server(s)

CISCO Live!

# Assign Dual Stack or IPv4 Pools to SSIDs

**Cisco DNA Center**DESIGNPOLICYPROVISION

Devices ▾FabricServices

Fabric-Enabled Sites+  
Find Hierarchy  
Default LAN Fabric  
SanJose ⚙

Default LAN Fabric  
Fabric Infrastructure  
Host OnboardingShow Task Status  
Wireless SSID's☐ Enable Wireless MulticastResetSave  

SSID Name	Type	Security	Traffic Type	Address Pool	Scalable Group
TAC_OPEN	Enterprise	Open	Voice + Data	192_168_125_0-DEFAULT_VN	No scalable groups to configure
TAC_DOT1X	Enterprise	WPA2 Enterprise	Voice + Data	192_168_120_0-DEFAULT_VN	No scalable groups to configure



# Pool upgrade: Edit pool

Cisco DNA Center

Network

Device Credentials

IP Address Pools

SP Profiles

Wireless

Telemetry

Security and Trust

Find Hierarchy

Search Help

Global

Site-1

S1-BLDG1

IP Address Pools (4)

Subnet Type

All

IPv4 only

Dual-Stack

Filter

0 Selected

Reserve

More Actions

<input type="checkbox"/>	Name	Type	IPv4 Subnet
<input type="checkbox"/>	AP_Pool	Generic	10.168.110.0/24
<input type="checkbox"/>	BGP_Pool	Generic	10.0.0.0/24
<input type="checkbox"/>	Client_Pool	Generic	10.0.1.0/24
<input type="checkbox"/>	Client_Pool2	Generic	10.0.2.0/24

4 Records

Design / Network Settings

Edit IP Pool

IP Address Pool Name\*

Client\_Pool

Type\*

Generic

Options

IP Address Space

IPv4 (Default)

IPv6

Check both IPv4 and IPv6 to create a dual-stack pool. If the pool is used for infra VN, or if the fabric contains devices that don't support IPv6, check only IPv4.

IPv4

Global Pool\*

10.0.0.0/8 (10\_0\_0\_0)

IPv6

Global Pool\*

2001:db8::/36 (2001\_0db8)

IPv4 Subnet

10.0.1.0/24

IPv6 Subnet

2001:db8:0:2::/64

Gateway

10.0.1.1

Gateway

2001:db8:0:2::1

DHCP Server(s)

10.10.10.10 X

DHCP Server(s)

2001:db8::10:10 X

DNS Server(s)

10.10.20.20 X

DNS Server(s)

2001:db8::20:10 X

☐ SLAAC Support

Cancel

Save

# Pool upgrade: Warning on fabric page

Cisco DNA Center

DESIGN POLICY PROVISION

Devices ▾ **Fabric** Services


## SD-Access Fabrics and Transits

Choose a Fabric or Transit below to manage, or add a new item by clicking 'Add Fabric or Transit'.

### Fabrics ⓘ

Default LAN Fabric

0 Sites, 0 Fabric Devices  
0 Control Planes, 0 Borders  
LAN

 FABRIC-0

1 Site, 3 Fabric Devices  
1 Control Plane, 1 Border  
LAN

### Transits ⓘ

BGP IP TRANSIT

Transit Type: IP



FABRIC-0

1 Site, 3 Fabric Devices  
1 Control Plane, 1 Border  
LAN

# Pool upgrade: Warning on site

Cisco DNA Center

DESIGN POLICY PROVISION

Devices ▾ Fabric Services

Fabric-Enabled Sites +

Find Hierarchy

FABRIC-0

SITE1

FABRIC-0

One (1) Warning Alert and One (1) Information Alert on this page. [Collapse](#) to hide.

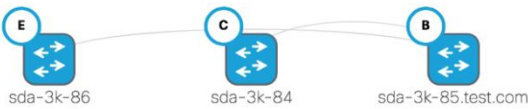
One (1) Warning Alert

You have enabled IPv4 and IPv6 IP pool dual stack. To update the fabric, click Reconfigure Fabric. This action can take some time depending on number of devices. [Reconfigure Fabric](#)

One (1) Information Alert

For each site assign at least 1 Control Plane and 1 Edge node. If the site needs external connectivity, assign at least 1 Border, Select Device(s) to assign the roles.

sda-3k-86 sda-3k-84 sda-3k-85.test.com



## Tech-Node for DNAC IPv6 Configuration

# Lessons Learnt

- Single Client can have multiple IPv6 addresses.
- For large fabric, it means 3 times or larger addresses to be tracked.
- Check for TCAM capacity on the border nodes
  - \*Control Plane Scale does not depend on the TCAM, it consumes only memory
- Choose the right Platform and design *for border nodes*.
- Ensure IPv6 configuration and routing is complete for communication outside Fabric.
- Ensure that Dual Stack Pools are mapped with SSID [Host Onboarding]

# Conclusion and Summary



# Points to Note

- IPv4 pool can be upgraded to dual-stack. Dual-stack pool CANNOT be downgraded to IPv4; need to release whole pool.
- Support for IOS-XE platforms (16.9.2+), AireOS 8.10.x+
- Dual stack pool CANNOT be assigned to Infra VN (APs and extended nodes).
- Underlay IPv6 configuration needs to be done manually.
- Wired IPv6 communication uses the same flow as described in this document from FE.

# IPv6 SDA wireless Adoption

1

Underlay needs to be IPV4 only or Dual Stack.

2

Introduce IPv6 Based DHCP/DNS

3

Complete required configuration for Dual Stack via DNAC.

4

Introduce Dual Stack Client communication for (Non-guest SSID)

# A special thank you to my colleague

Vinay Saini



# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).



The bridge to possible

# Thank you

CISCO *Live!*

CISCO *Live!*

