The bridge to possible

IPv6 Enabled Cisco Wireless

Josh Halley, Principal Architect – Customer Experience EMEA

Cisco Webex App

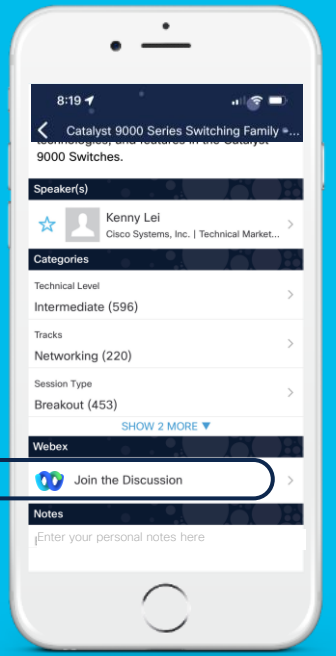
Questions?

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

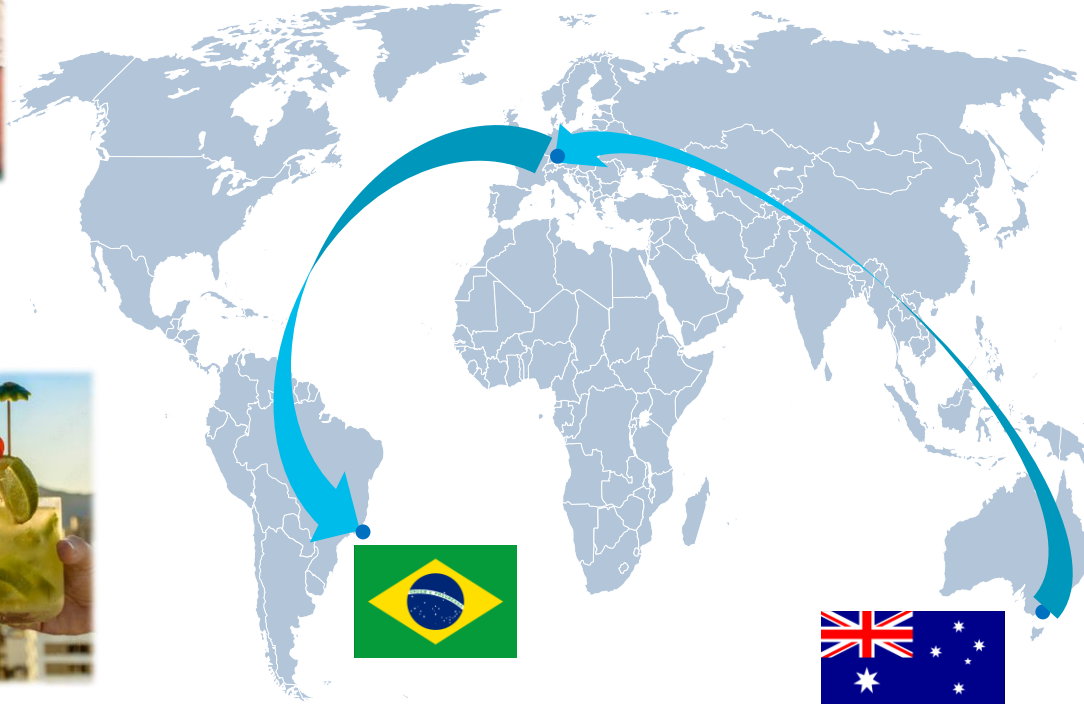
Webex spaces will be moderated until February 24, 2023.



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:

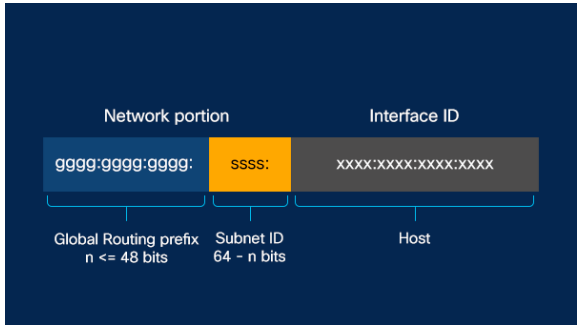
- Detailed IPv6 Protocol learning
- Cisco SD-Access concepts
- Setting up Cisco SD-Access Wireless

Recommended Pre-session Learnings
BRKEWN-2020 : For Wireless SDA
BRKSRT-2116 : Basics of IPv6

IPv6 Basics

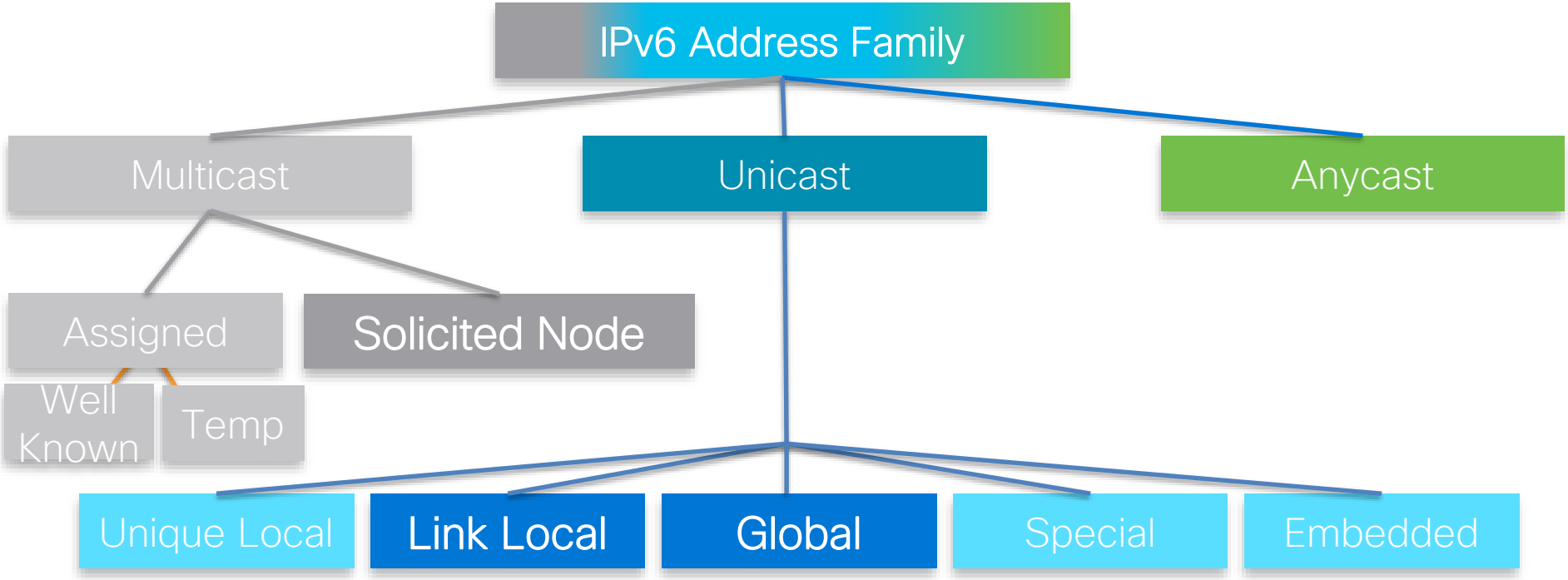
Why IPv6

- 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

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

ff02::1: All IPv6 devices

ff02::2: All IPv6 routers

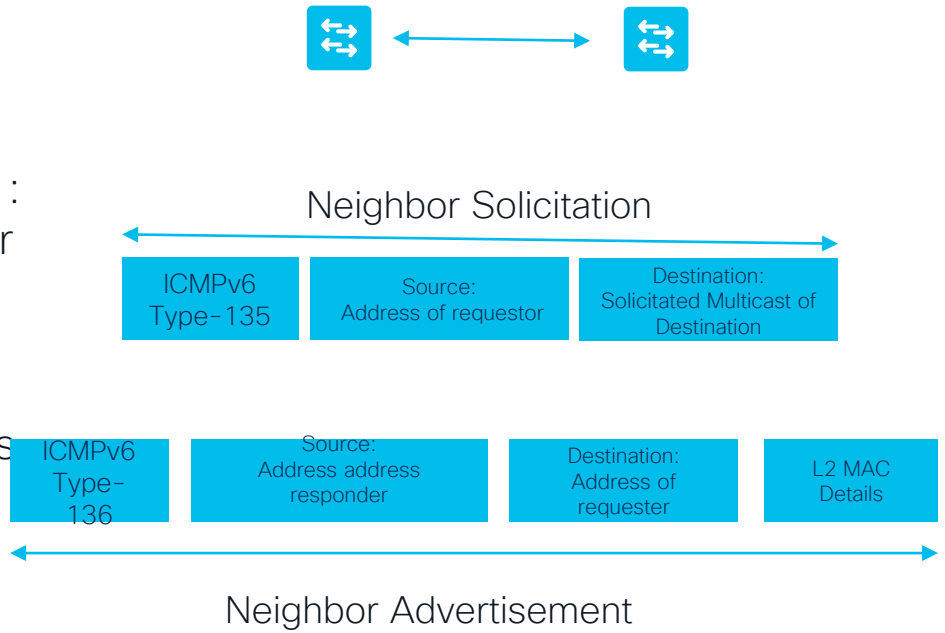
ff02::5: All OSPFv3 routers

ff02::a: All EIGRP (IPv6) routers

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.

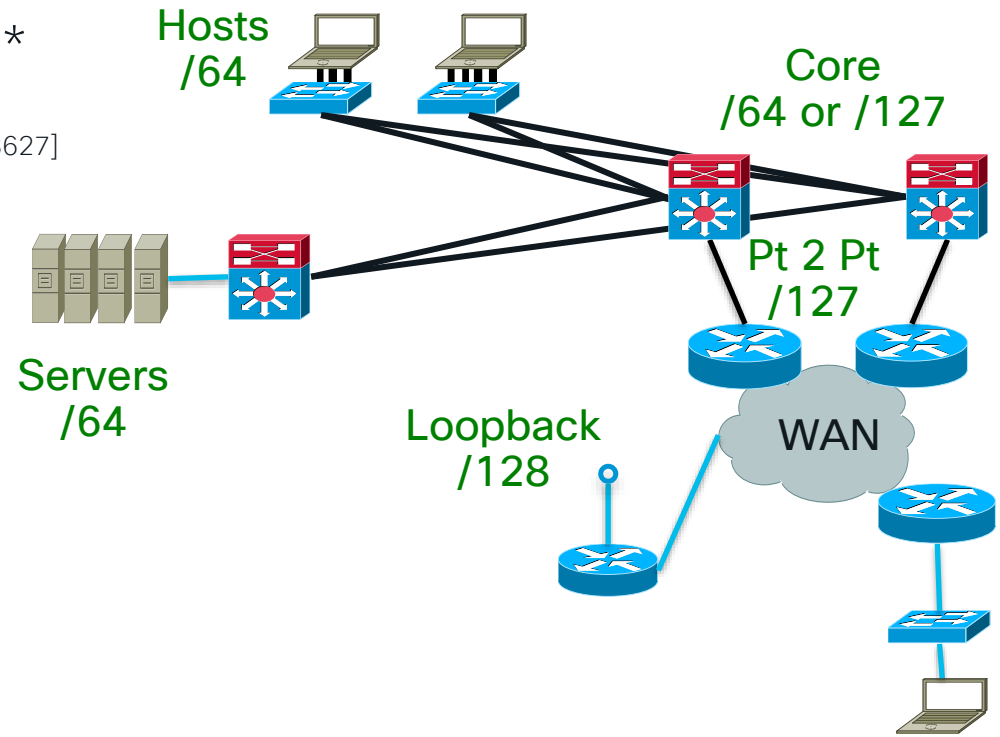
  Other Imp Message ICMPv6 message types:
  - Route Solicitation
  - Router Advertisement



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

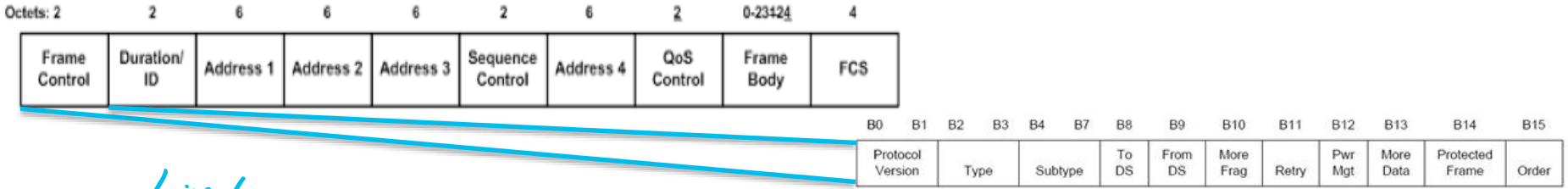


* A prefix length other than a /64 in IPv6 will break the operation of the following technologies:

- 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]

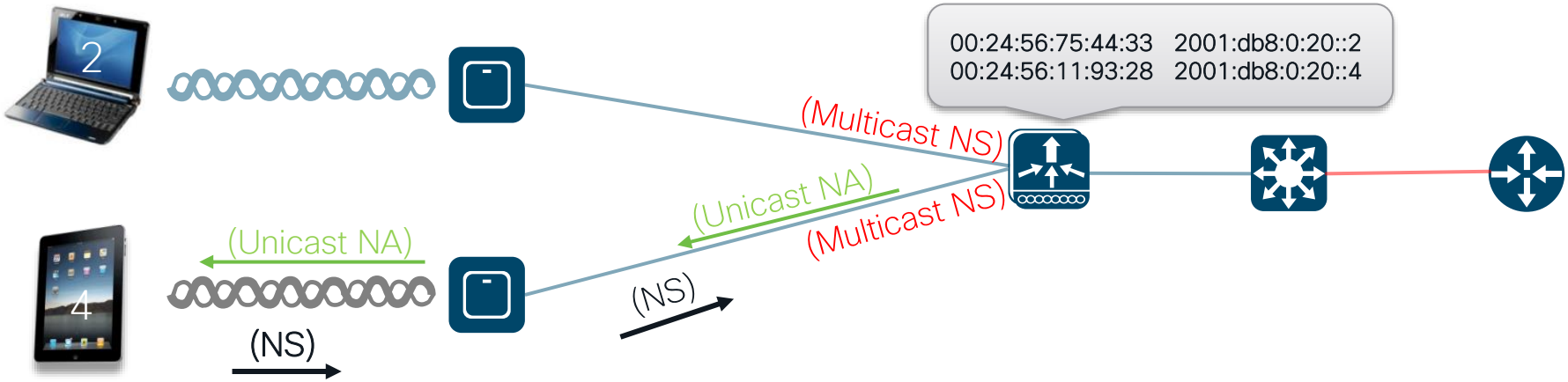
Wi-Fi Multicast Background

- 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



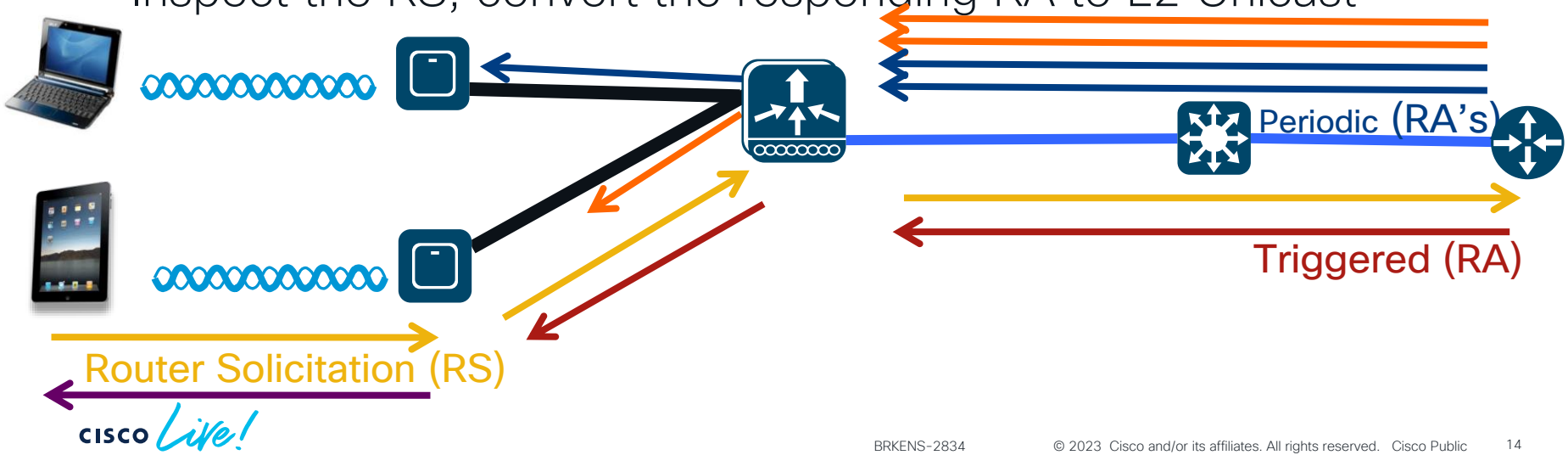
Neighbour Discovery Multicast Suppression

- 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

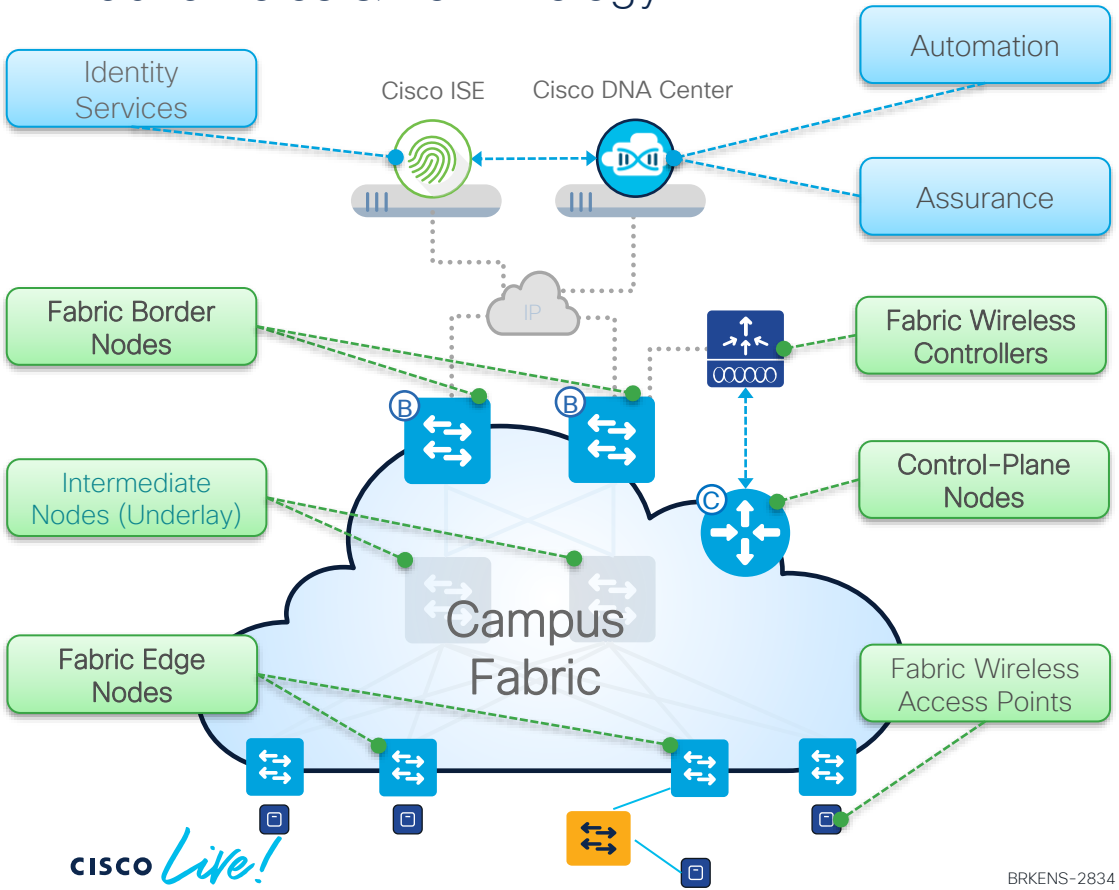
- Scaling the mobility access environment
- NDP process is multicast “chatty”, consumes airtime
- Rate limit RA’s from the legitimate router
- Inspect the RS, convert the responding RA to L2 Unicast



Cisco SDA with IPv6

Cisco SD-Access

Fabric Roles & Terminology

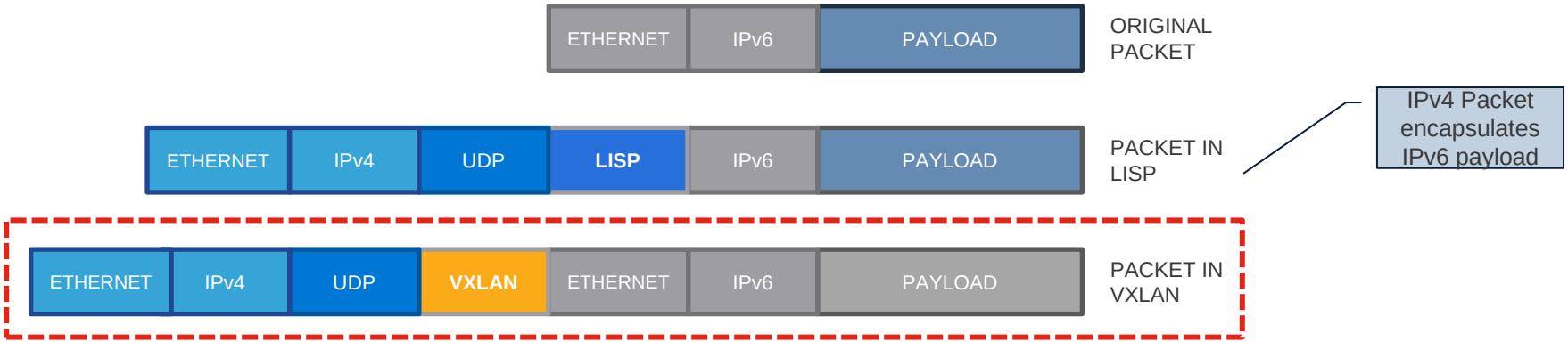


- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context.
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Control Plane Nodes** – Map 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/Supplicant 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

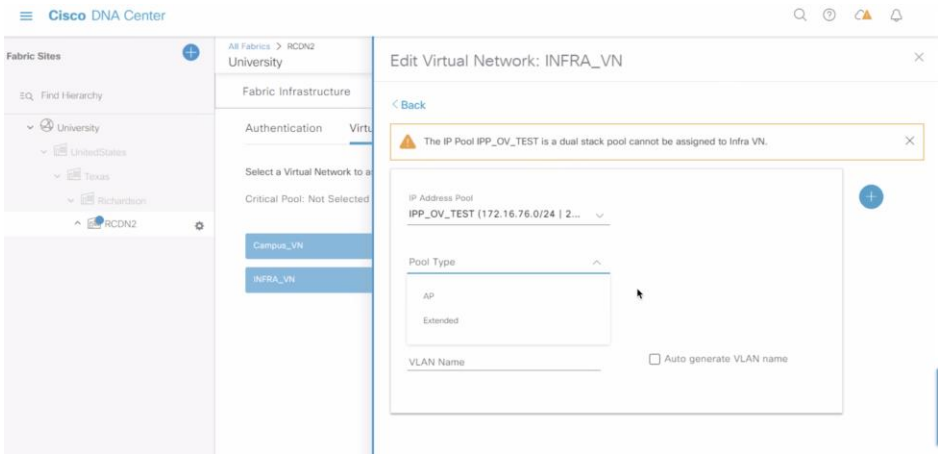
Access Points can only have IPv4 address with current release.

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

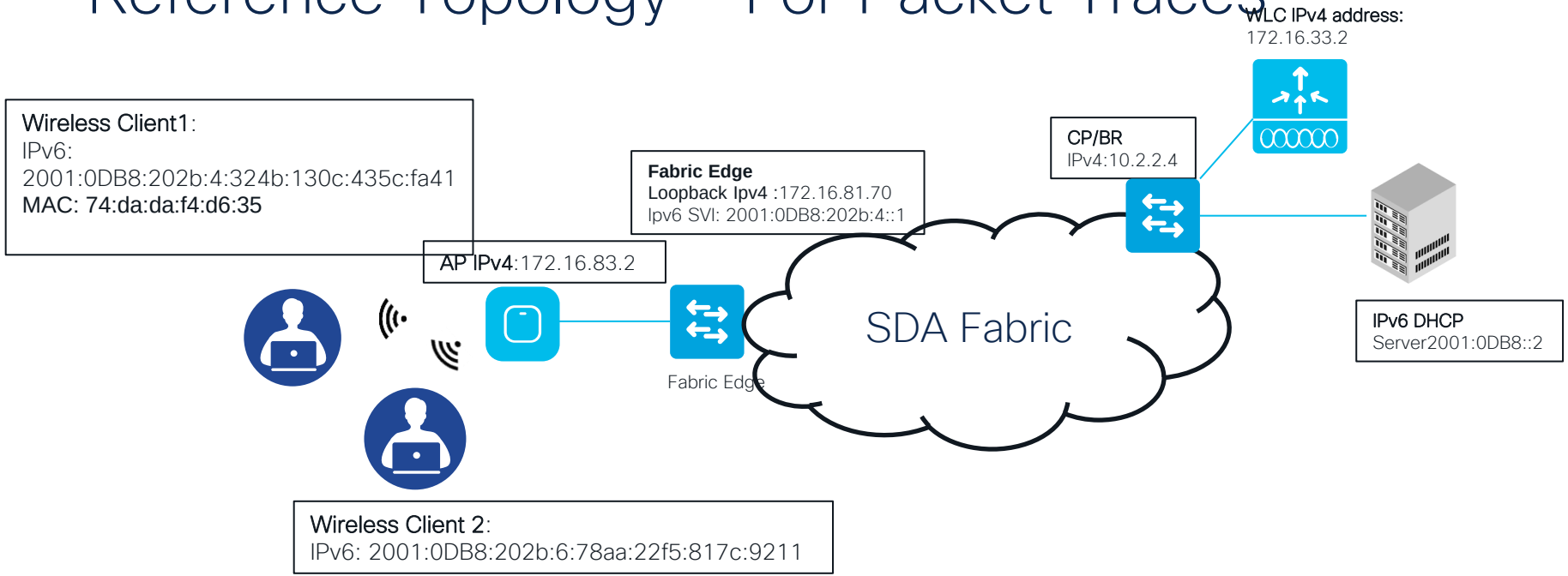
The remaining process is the same.

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

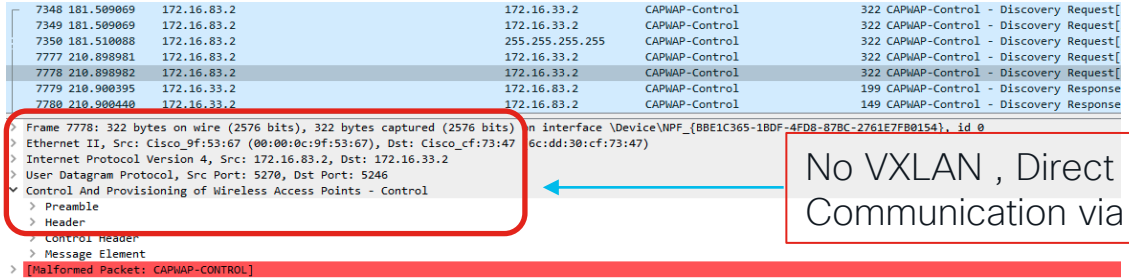
To anticipate future IPv6 AP onboarding support with DNA Center, it is recommended to already begin address planning for these ranges in your sites



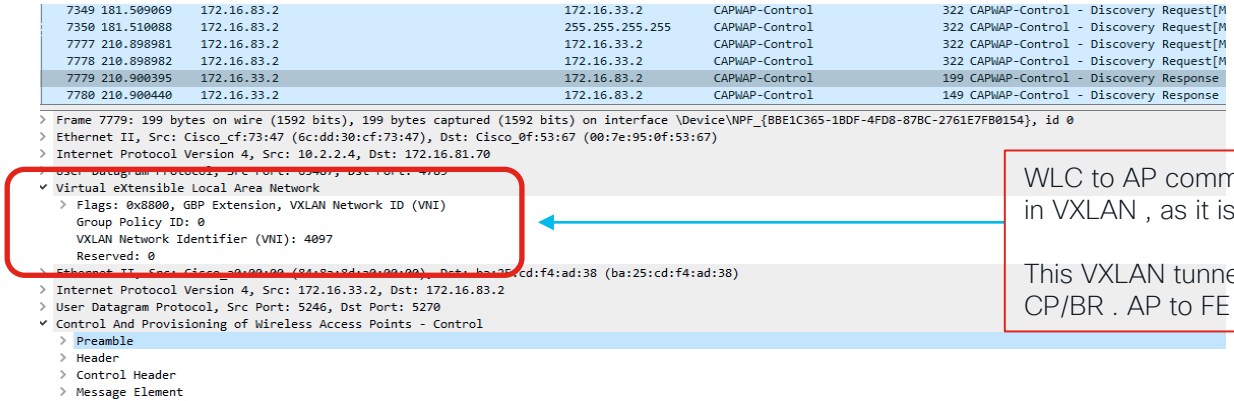
Reference Topology – For Packet Traces



AP-WLC Communication Trace



No VXLAN , Direct Communication via underlay



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.

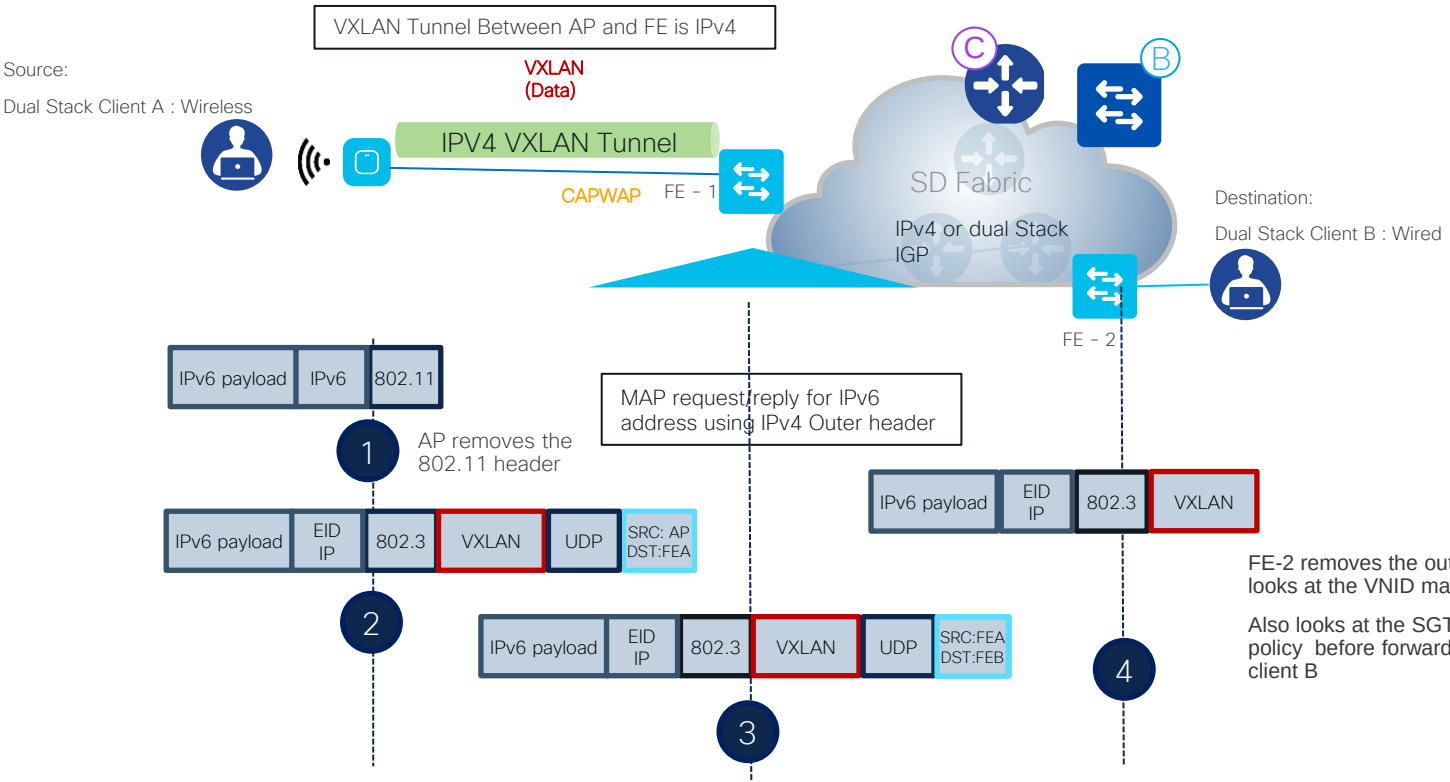
The packet capture shows IPv4 Access Tunnel Communications.

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

FE-2 removes the outer IPv4 header, looks at the VNID maps it to the VLAN.

Also looks at the SGT and apply the policy before forwarding the packet tp client B

RLOC for IPv6 Transport

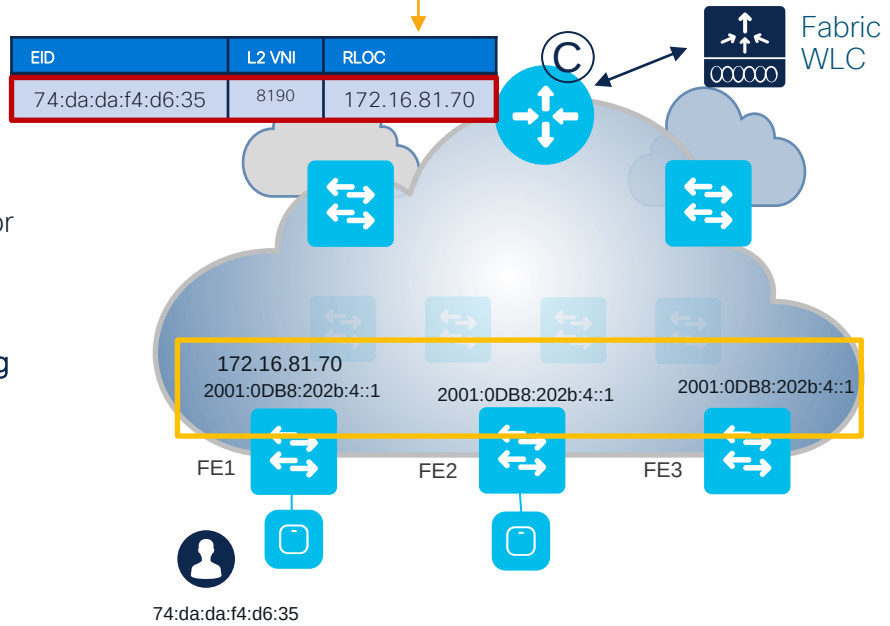
Note-RLOC is still IPV4 as LISP using IPv4

Fabric Mode WLC integrates with the LISP Control Plane

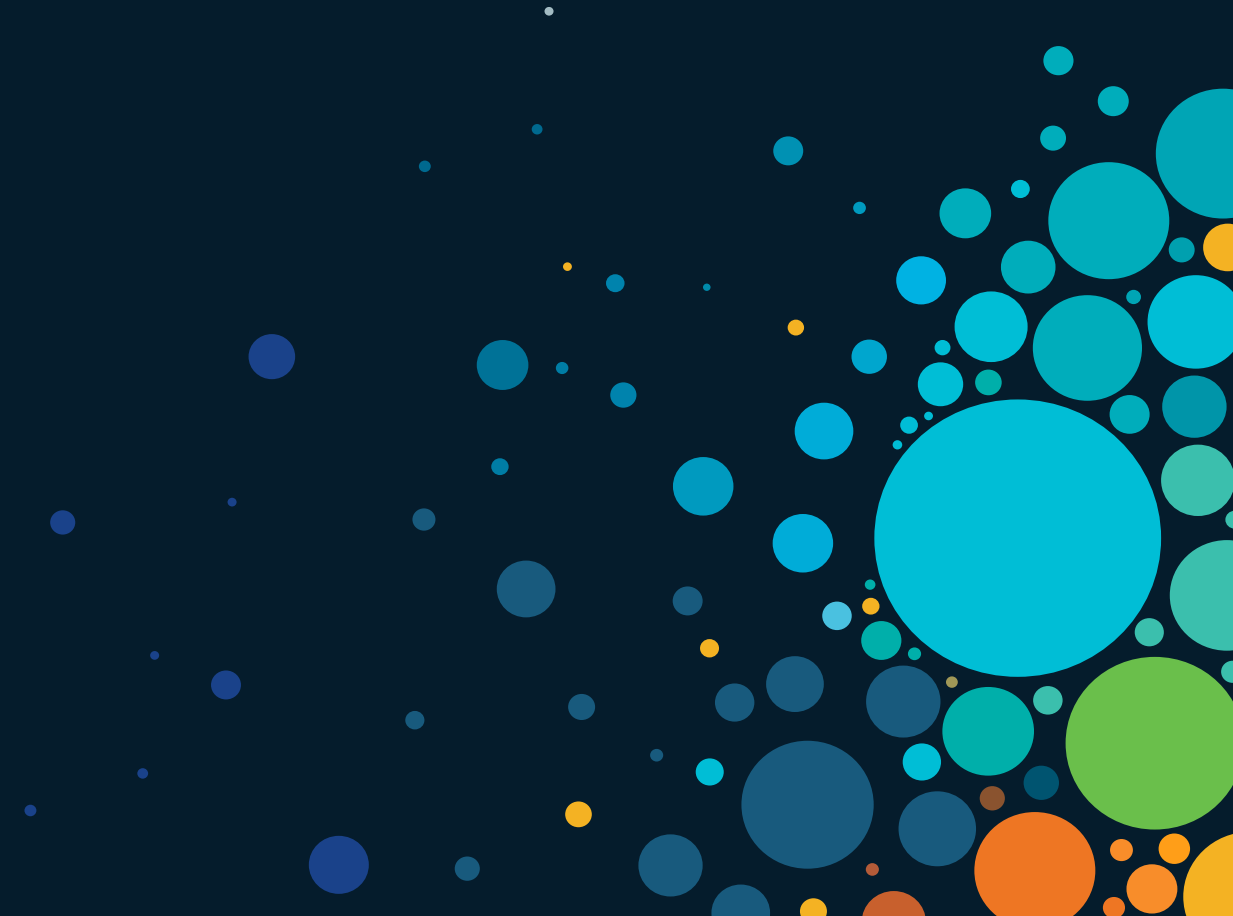
Control Plane is centralized at the WLC for all Wireless functions

- 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)

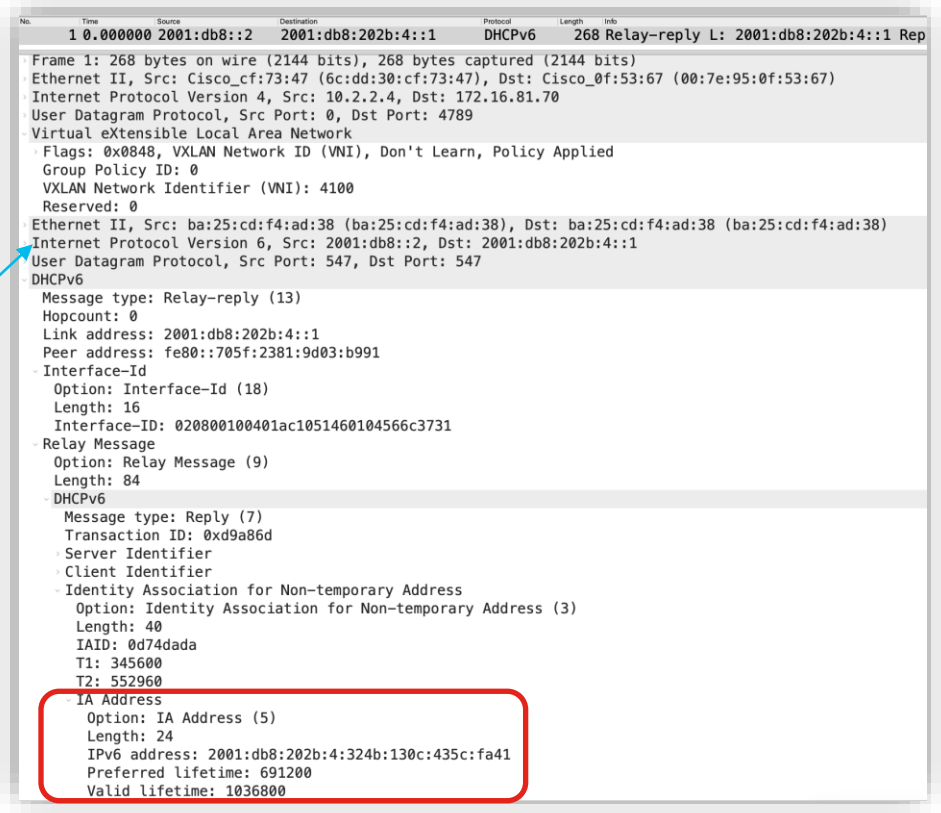


IPv6 Packet Traces

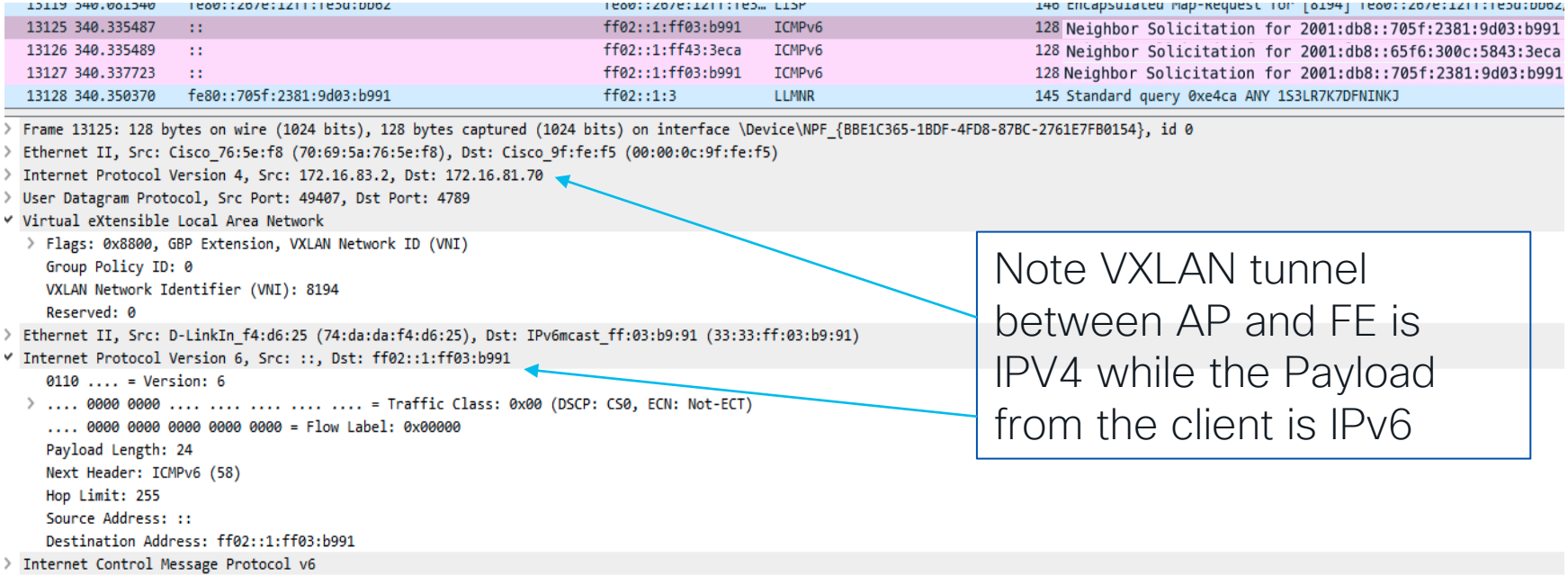


Client IPv6 Address

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

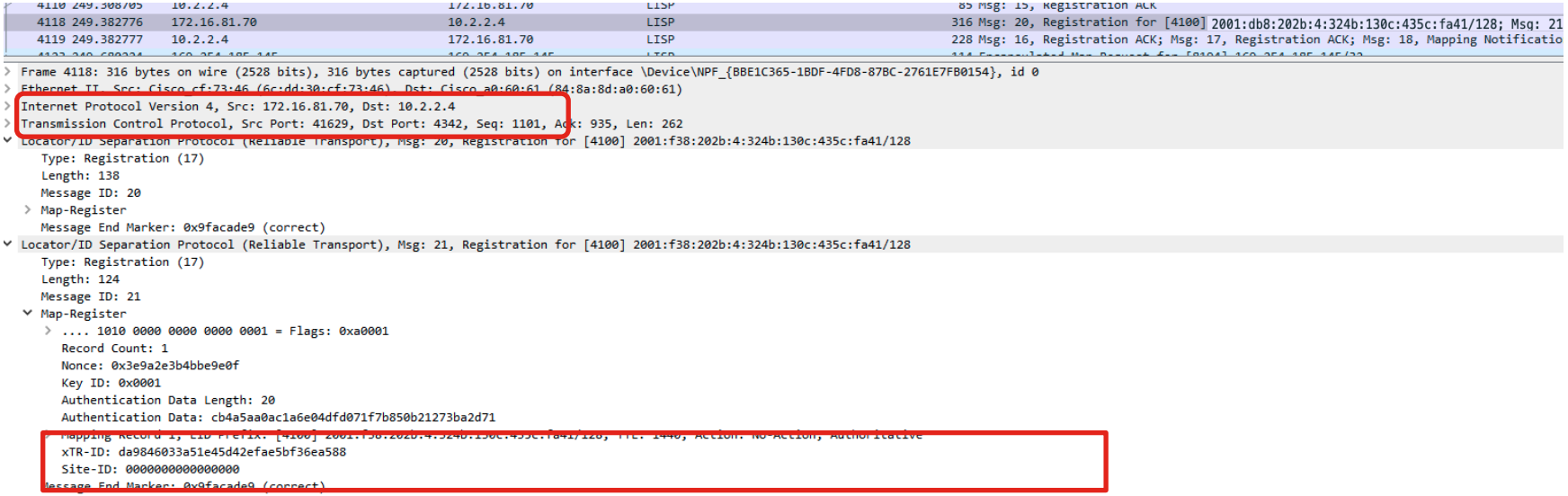


Client IPv6 communication via AP

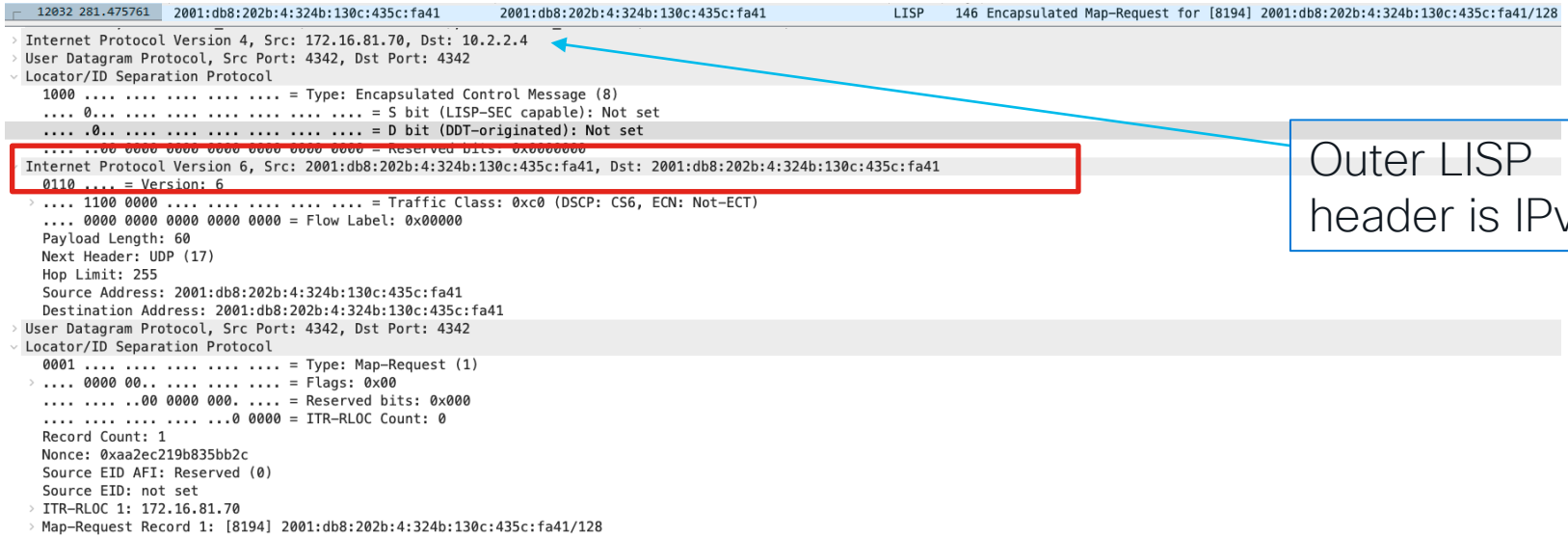


Note VXLAN tunnel between AP and FE is IPV4 while the Payload from the client is IPv6

Map Register for IPv6 client - LISP



IPv6 Map request - LISP



Outer LISP header is IPv4

IPv6 Map Cache on the FE

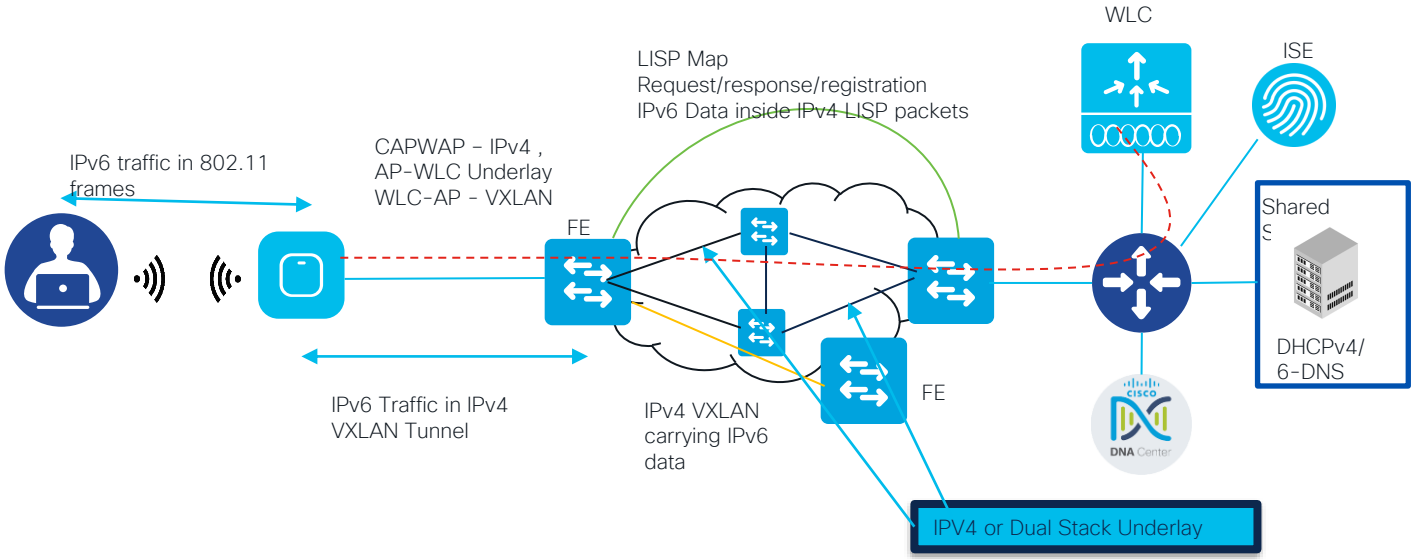
```
Pod2-Edge-2#sh lisp eid-table vrf Campus_VN ipv6 map-cache
LISP IPv6 Mapping Cache for EID-table vrf Campus_VN (IID 4100), 6 entries

::/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	Trustsec SGT	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 foun
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

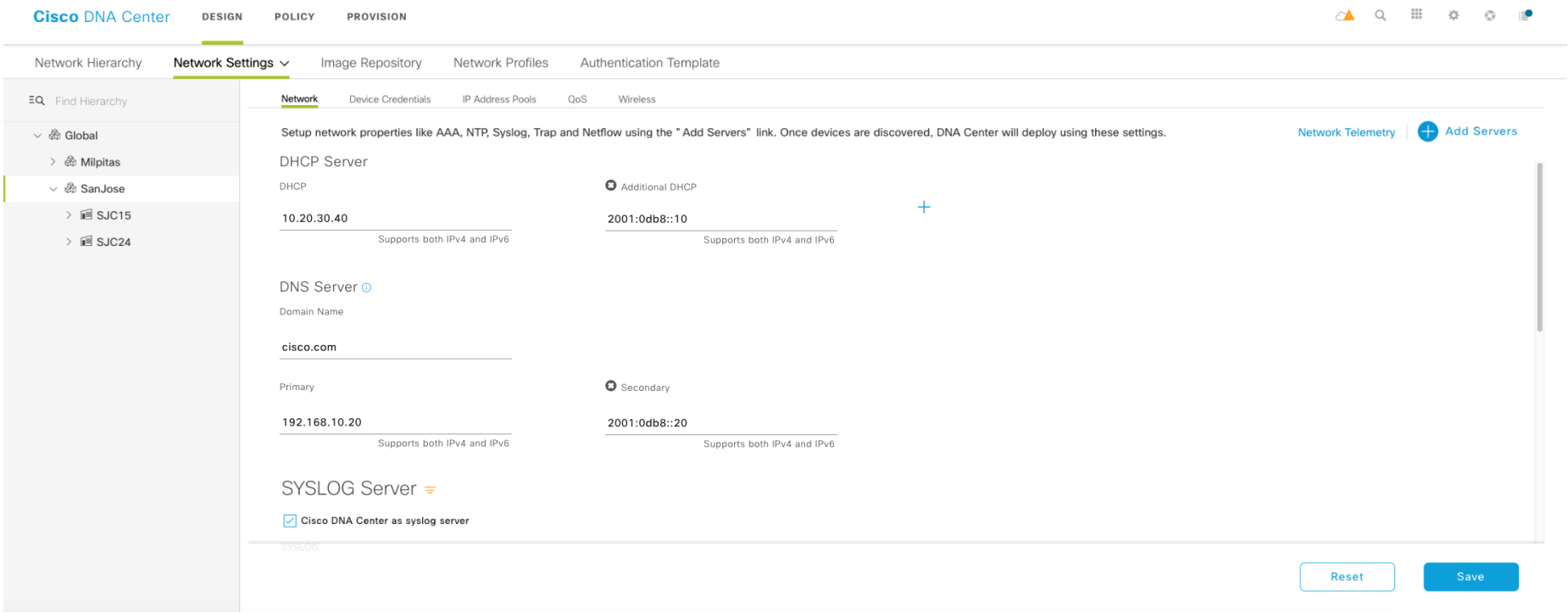
Client IPv6 Address

- Static
- SLAAC [CIDR /64]
- DHCPv6

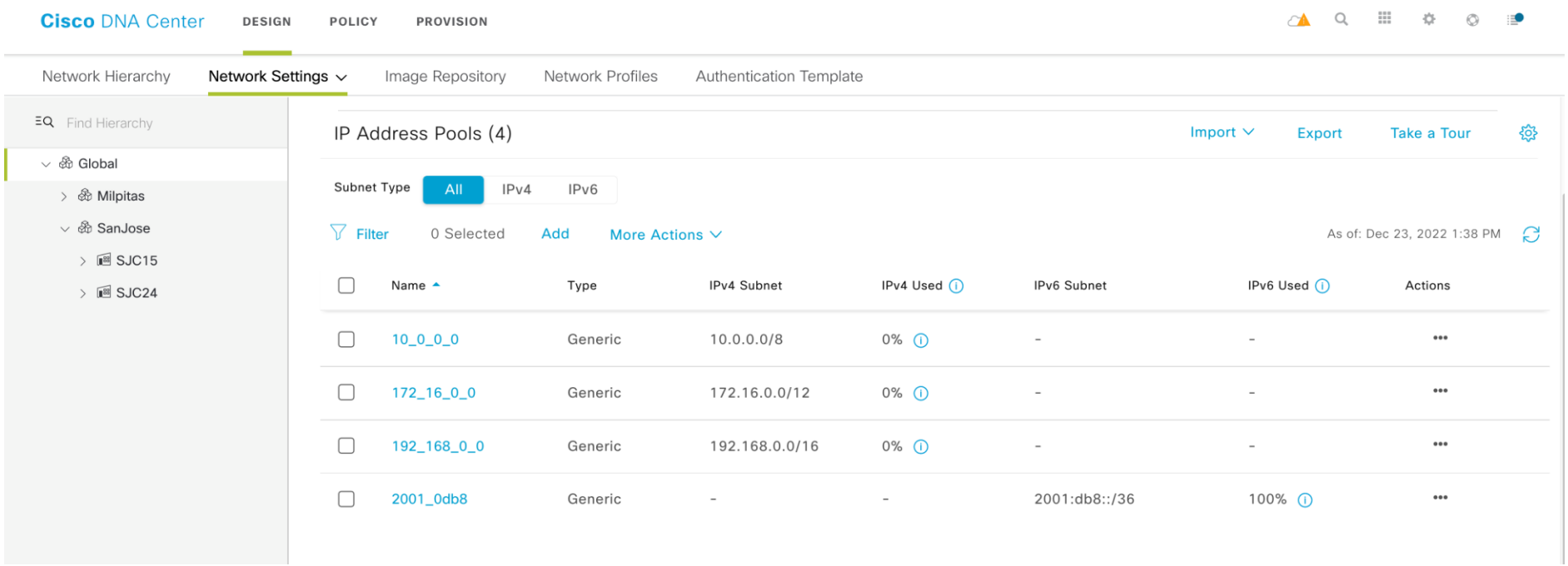
IPv6 address pools with DHCPv6 and DNSv6

- 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

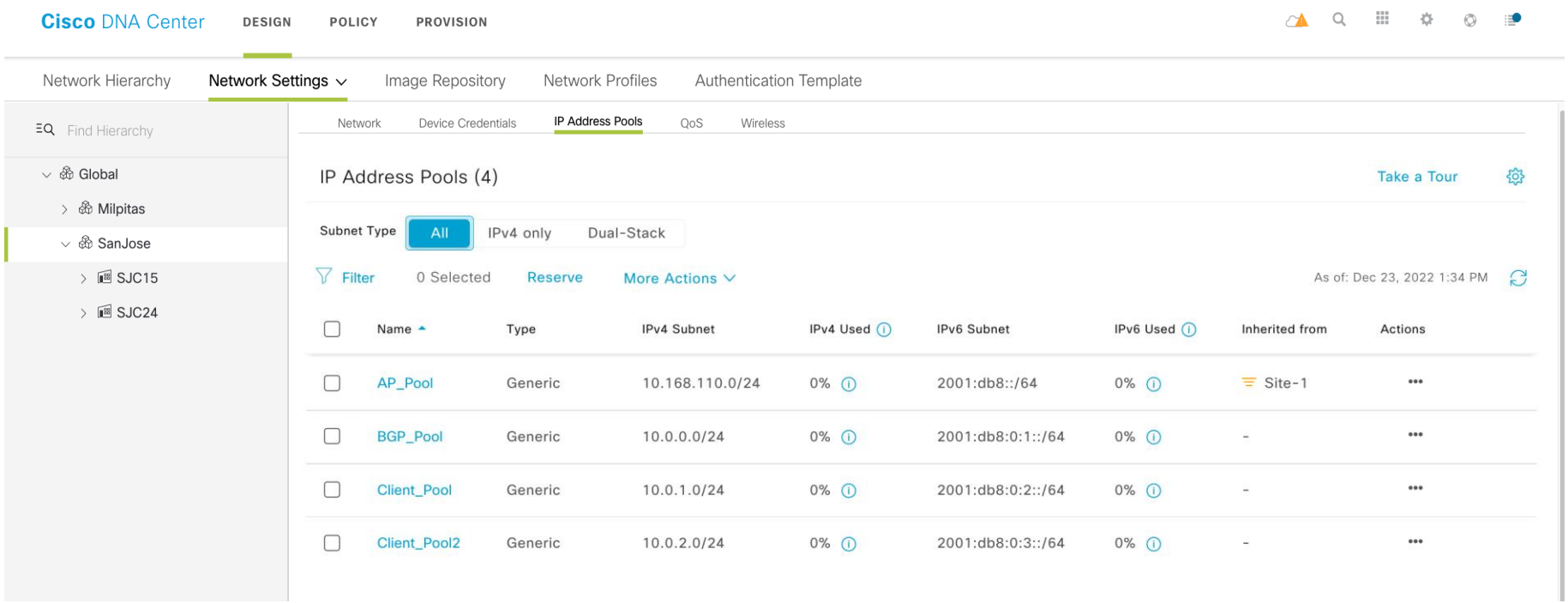
IPv6 DHCP and DNS



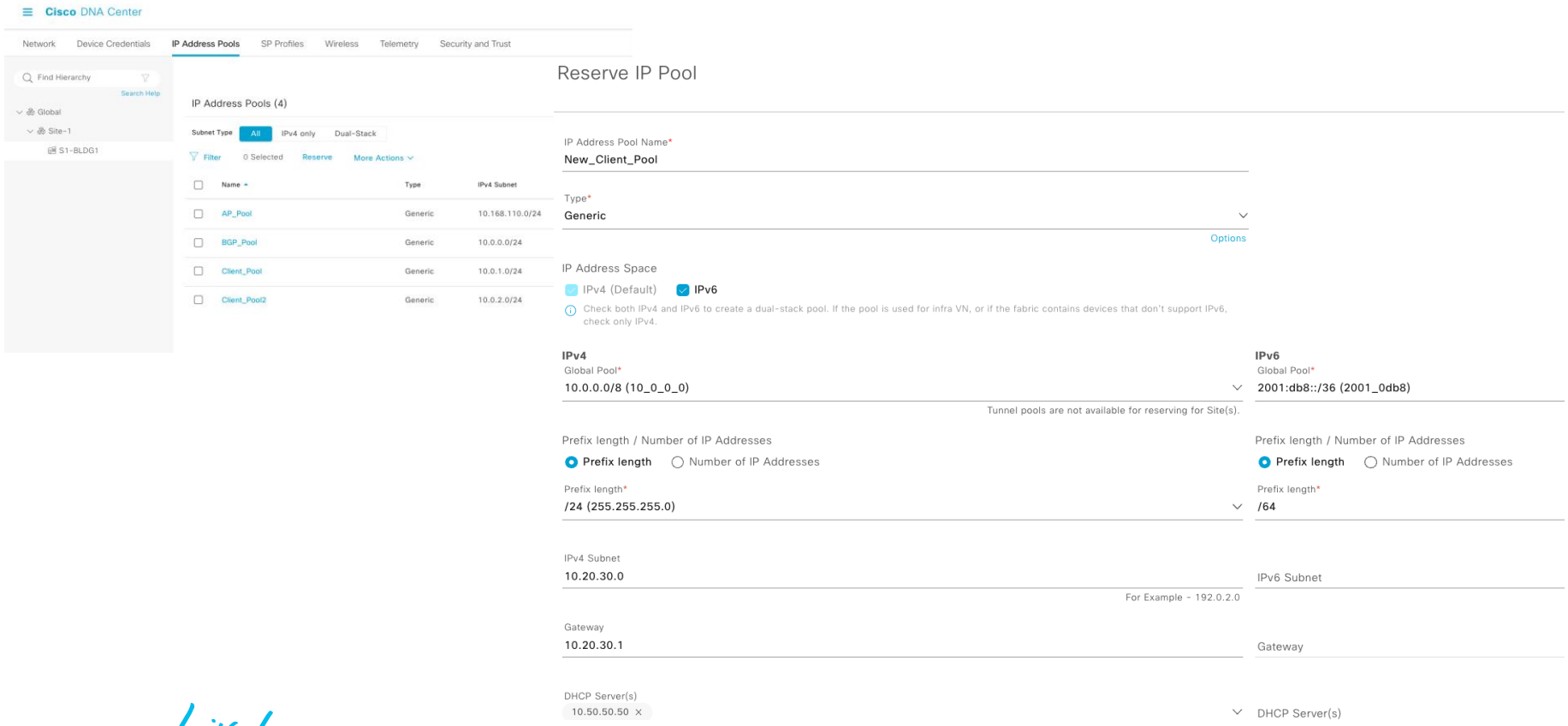
Create IPv4 and IPv6 Pools at Global level



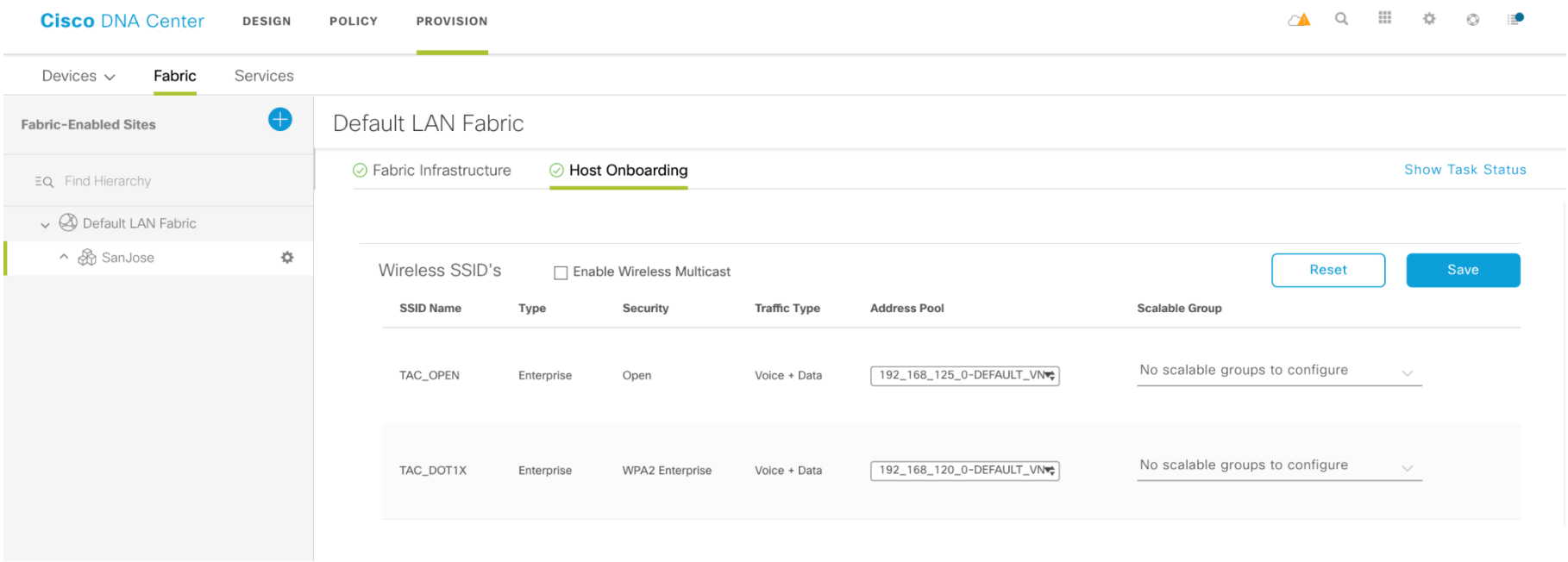
Reserve Pools (IPv4 or Dual stack) at Site level



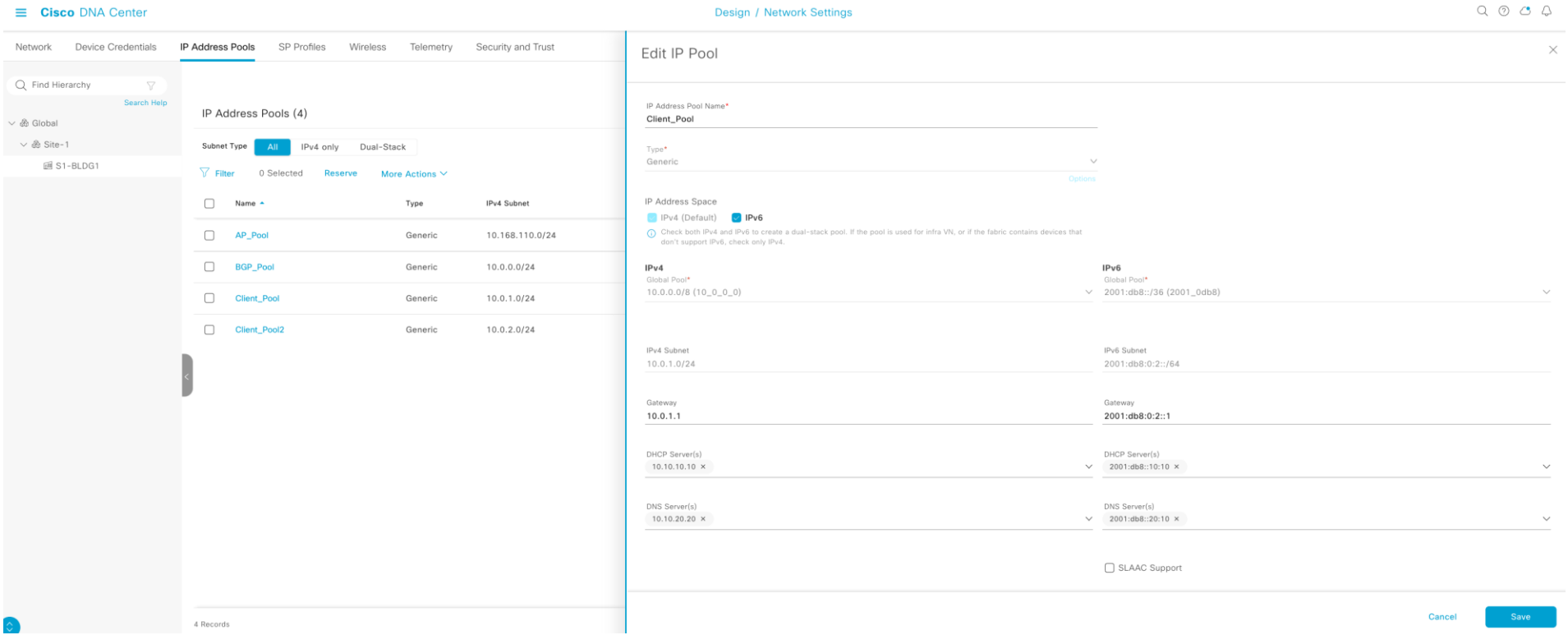
Reserving a Pool (IPv4 or Dual stack)



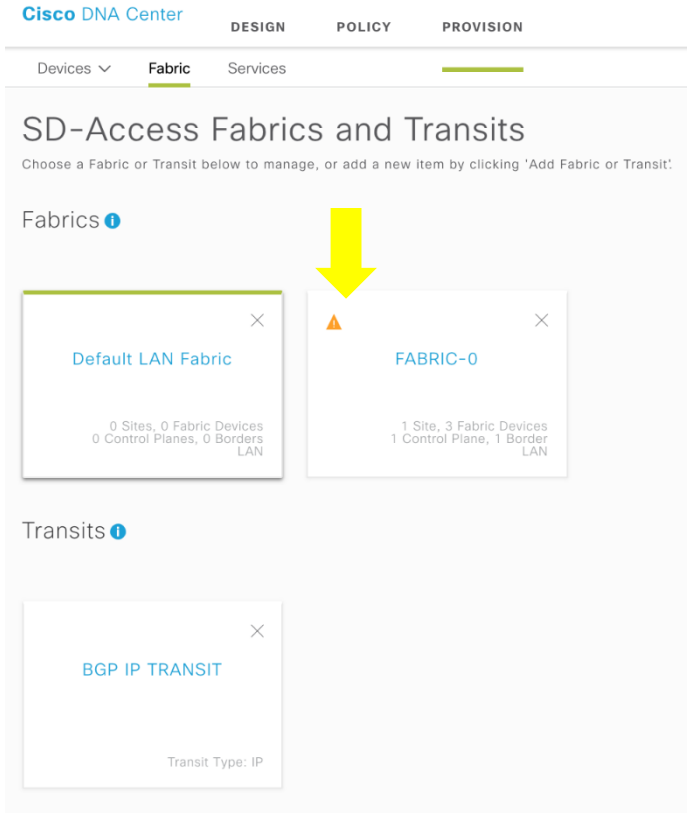
Assign Dual Stack or IPv4 Pools to SSIDs



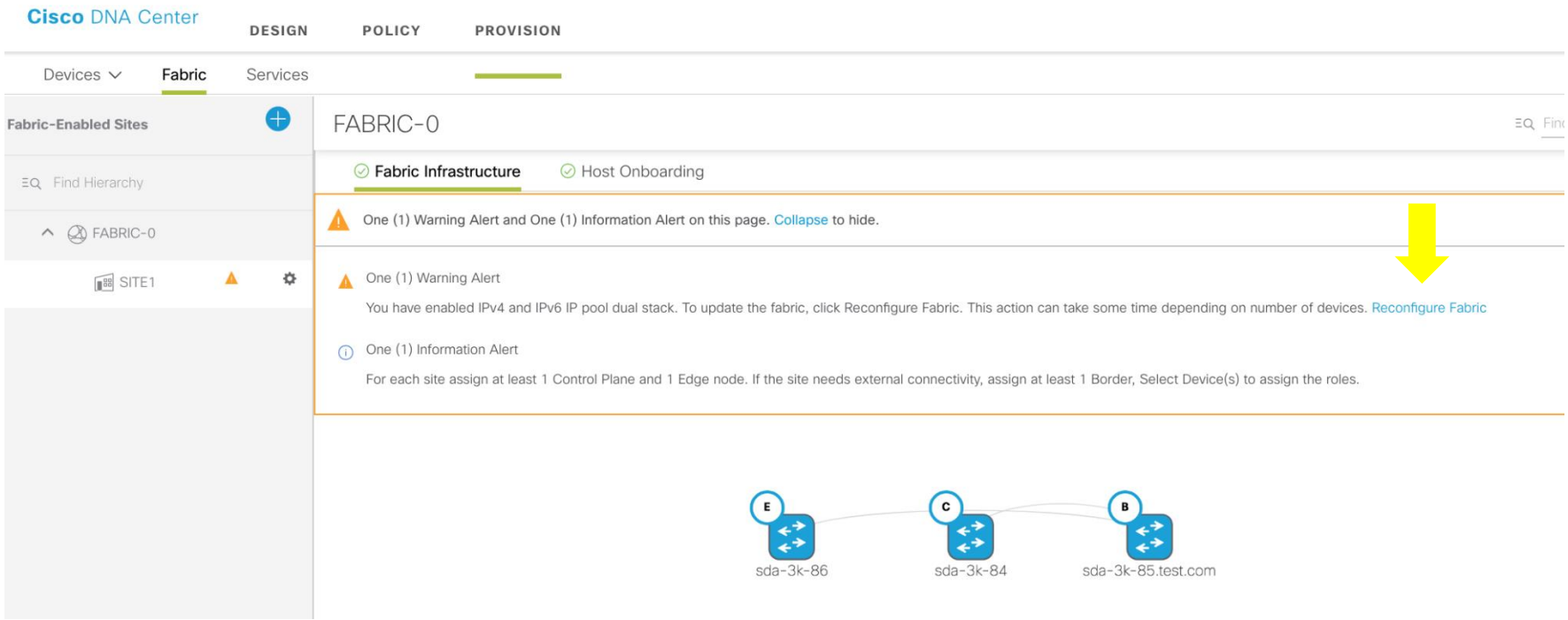
Pool upgrade: Edit pool



Pool upgrade: Warning on fabric page



Pool upgrade: Warning on site



[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

Underlay needs to be IPV4 only or Dual Stack.

Introduce IPv6 Based DHCP/DNS

Complete required configuration for Dual Stack via DNAC.

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.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN