The bridge to possible

# Cisco Software Defined Access - LISP

## Migration Strategies

Kedar Karmarkar, Principal Engineer
Technical Marketing

BRKENS-2827

cisco Live!

#CiscoLive

# Cisco Live US SD-Access/ISE Learning Map

## Sunday–2nd

- TECENS-2820 9AM
  Cisco Software-Defined Access LISP: Architecture Overview

## Monday–3rd

- BRKENS-2810 8:30AM
  Cisco Software-Defined Access LISP Solution Fundamentals
- BRKENS-2800 9:30AM
  Cisco SD-Access Zero-Touch Provisioning Using LAN Automation
- BRKENS-2811 1PM
  Connecting Cisco SD-Access LISP to the World: Use Cases and Segmentation
- LTRENS-2419 1PM
  SD-Access LISP Pub/Sub Wired Lab
- BRKENS-2816 3PM
  Cisco SD-Access Transit: Advanced Design Principles
- BRKSEC-2100 10:30AM
  ISE Your Meraki Network with Group Based Adaptive Policy
- BRKENS-1802 2:30PM
  SD-Access Success Stories: Concept to Reality by Petrobras and Ford Motor
- BRKSEC-2091 3PM
  Cisco ISE Performance, Scalability and Best Practices
- BRKENS-1852 4PM
  TrustSec Refresh Reinforced with Latest Segmentation Innovations

## Tuesday–4th

- BRKENS-2502 10:30AM
  Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment
- BRKENS-1801 4PM
  SD-Access Success Stories: Concept to Reality by Stanford Health and Yale University

## Wednesday–5th

- BRKENS-2833 10:30AM
  LISP: Optimized Control Plane for Software-Defined Access
- BRKENS-2819 2:30PM
  Cisco SD-Access and Multi-Domain Segmentation
- CIUG-1003 2:30PM
  Zero Trust with Software-Defined Access Roadmap Update
- BRKENS-2821 4:00PM
  Cisco SD-Access LISP VXLAN Fabric for Manufacturing Verticals

## Thursday–6th

- BRKENS-2827 11:00AM
  Cisco SD-Access Migration Tools and Strategies

Catalyst Center

Cisco SD-Access LISP

ISE

Cisco ISE

BU-led sessions

cisco Live!

# Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2827

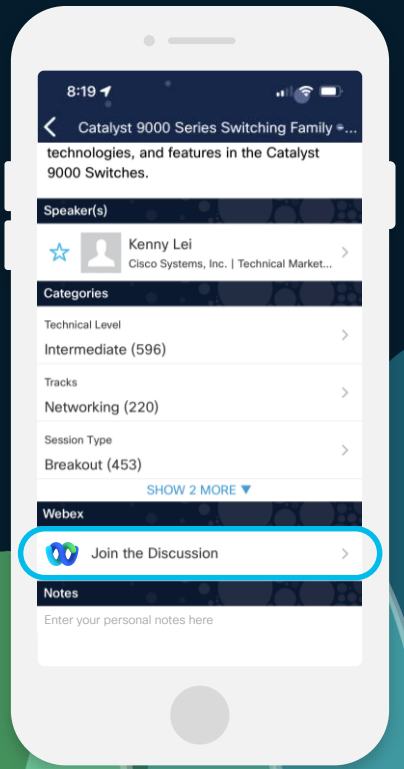
## Questions?

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 7, 2024.

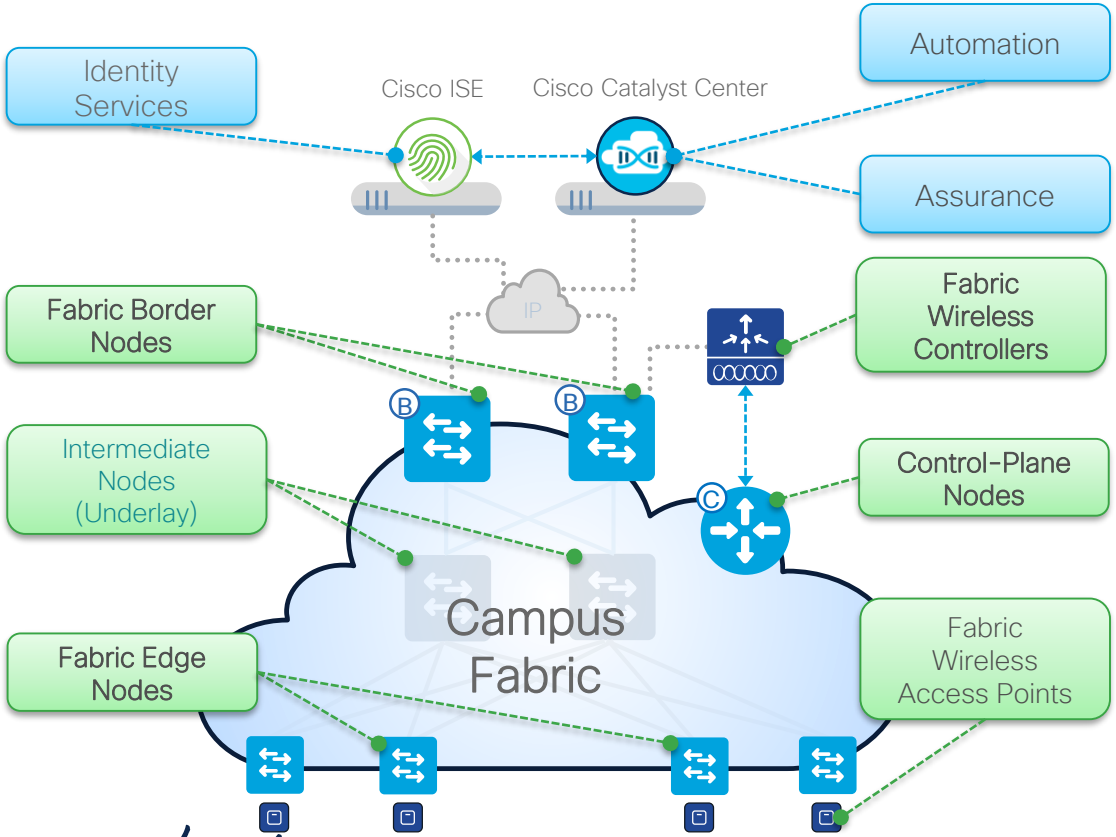


- 24 years with Cisco and 28 total
- Switching, Wireless, SDN Controllers, SDWAN
- Back to Switching with Software-Defined Access
- When not working, I am out taking pictures of military aircraft and old warbirds

**Kedar Karmarkar**

Principal Technical Marketing Engineer

# Cisco SD-Access-LISP
## Fabric Roles & Terminology




- **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 device 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 L3 network(s) to the SD-Access-LISP fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access-LISP fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access-LISP fabric

# Options for deployment

- Cisco Catalyst Center automated configuration of a Cisco SDA-LISP Fabric -
  - Includes SDA-LISP Automation Workflows and Integrations
  - Best practice standardized configurations
  - Includes SDA-LISP Assurance

OR

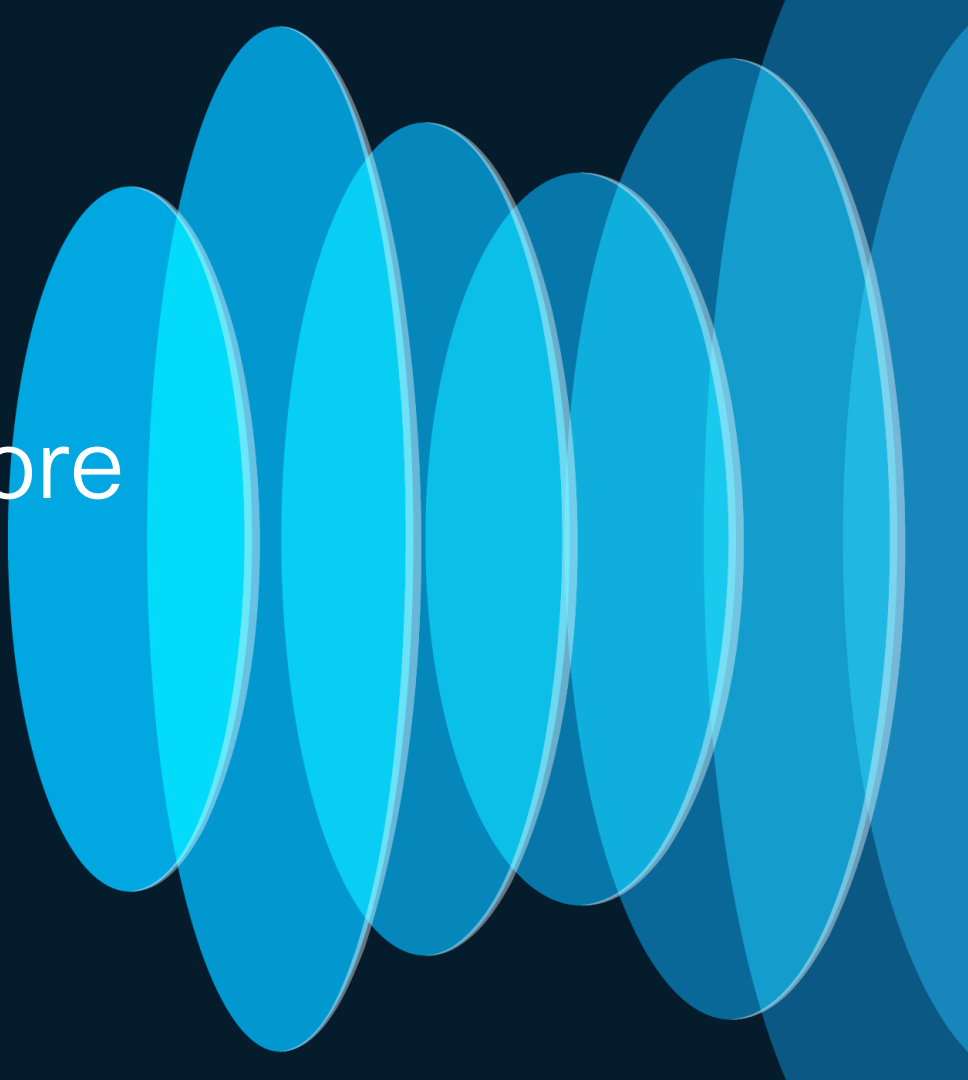
- CLI/Programable Configuration of Cisco LISP Fabric -
  - Open integration with heterogenous tooling (CLI, Ansible, NSO, etc)
  - Agile customization within the parameters of the LISP Fabric validated design
  - Can support Cisco Catalyst Center Device and Client Assurance
  - Subset of features supported compared to what is available with Cisco Catalyst Center.

# Agenda

- Considerations Before You Migrate
- Migrate L2 Access with new subnet/s
- Migrate L2 Access with existing subnet/s
- Migrate MPLS-VPN designs
- Migrated Routed Access Campus Designs
- Migrate Wireless and integrate into Fabric
- What Next?

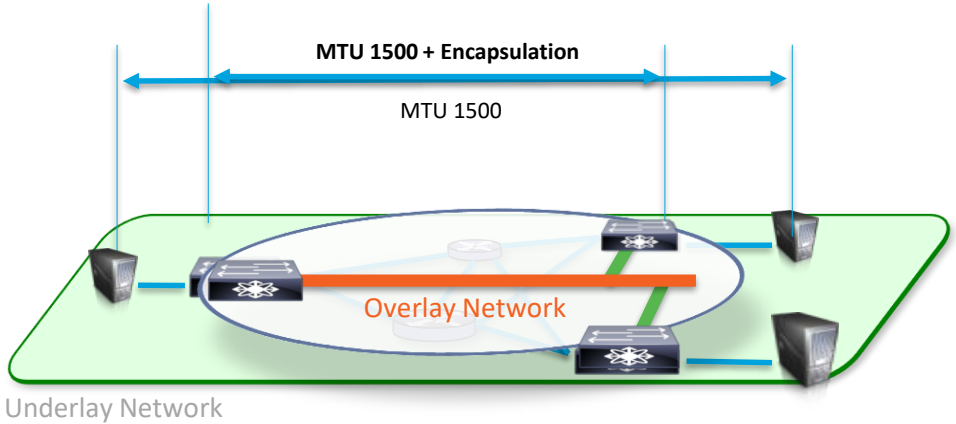
# Considerations before you start migration

Small things that matter much!!



# Existing Network MTU

- **VXLAN** adds **50 bytes** to the Original Ethernet Frame in the Overlay
- Avoid Fragmentation by adjusting the network MTU
- Ensure Jumbo Frame support on switches in the underlay network



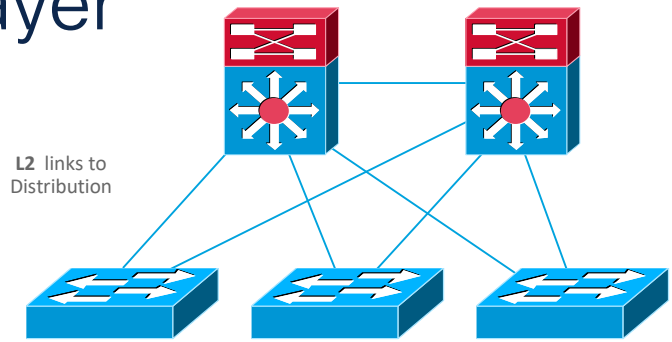
# TCP MSS

- TCP MSS adjust is supported in 16.9.1s and later
- Available only on Catalyst 3K and 9K only and **works only on TCP based applications**
- Applied to the overlay SVI on Fabric Edges via Template Editor
- PMTUD is being explored as a solution for UDP traffic.

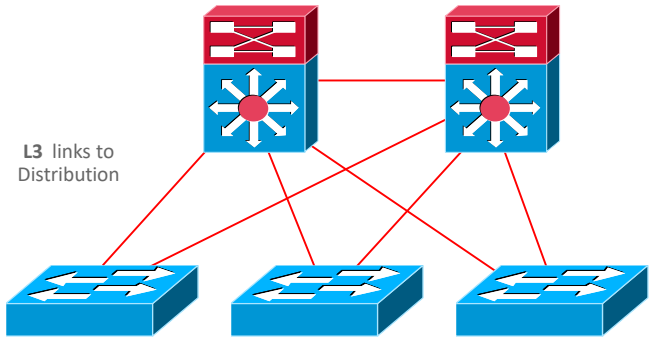
*As of now, Jumbo MTU is mandatory on all switches.*

# Re-configuration of Access Layer

- Layer-2 **Switched Access** today
- L2 Links




- **Routed Access** tomorrow
- L3 Links



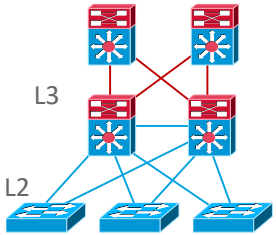
# Physical Network Topology

## Cisco SD-Access fabric runs over most topologies:

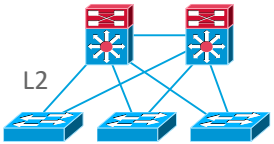
- Traditional 3-tier hierarchical network
- Collapsed core/aggregation
- Routed access
- U-topology

- **Ideal to start with routed access** – allows fabric to extend to very edge of campus network with minimum impact.
- Ensure that all switches have IP reachability to infrastructure elements

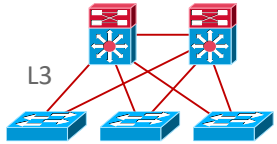
follow campus CVDs with routed access:
www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html



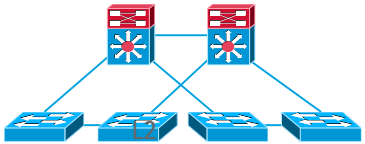
3-Tier Hierarchical



Collapsed Core



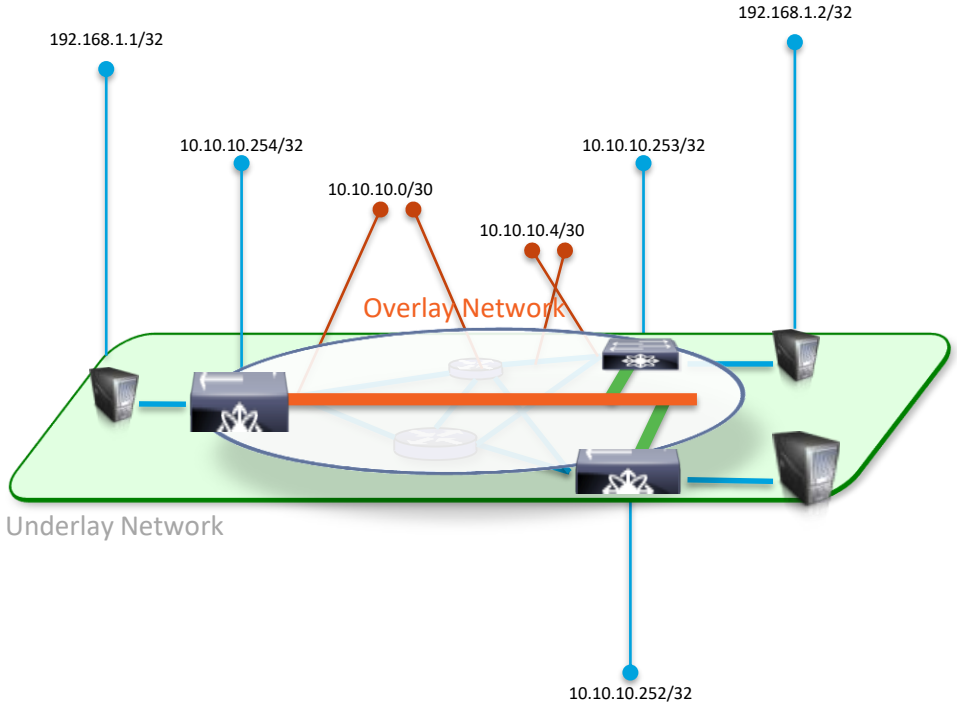
Routed Access


U-Topology

# IP Addressing for Underlay and Overlay

## Know your IP addressing and IP scale requirements

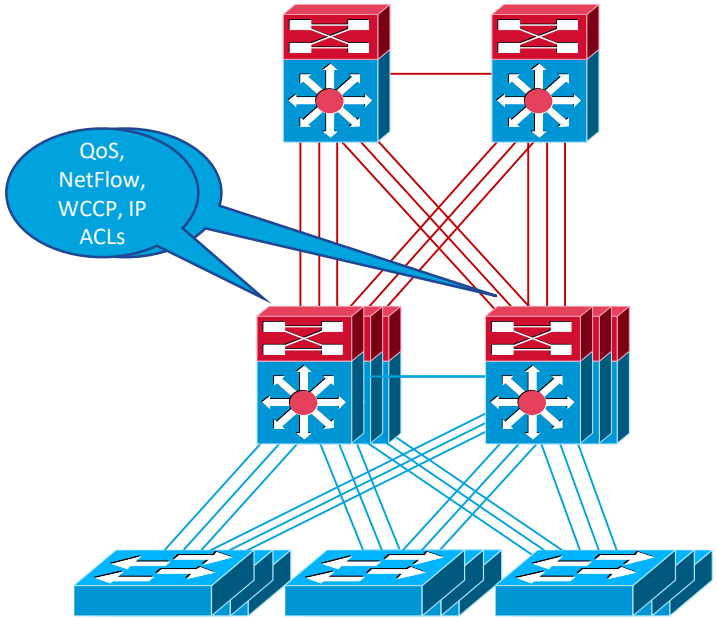
- **IPv4 only underlay** (today)
- Fabric uses Loopback 0 as Source-Interface for Encapsulation
- Best to use single Aggregate for all Underlay Links and Loopbacks



# Features enabled today

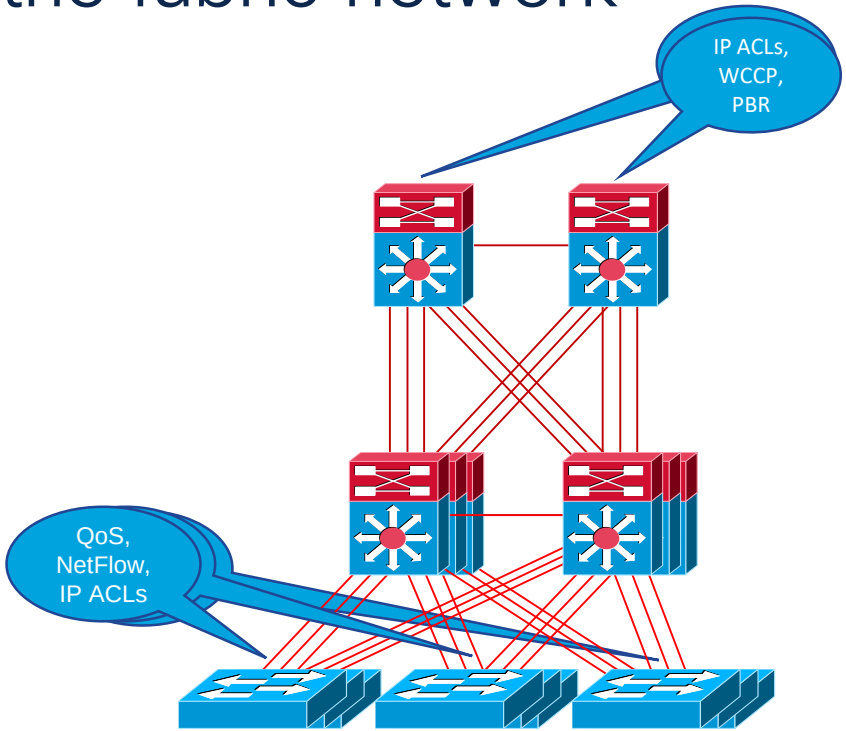
## Where are policies applied today?

- For example, features like QoS, NetFlow, Policy-based Routing, IP ACLs?
- **Need to move** the policy enforcement point(s) down at the **Access layer** or **outside the fabric**



# Move to different points in the fabric network

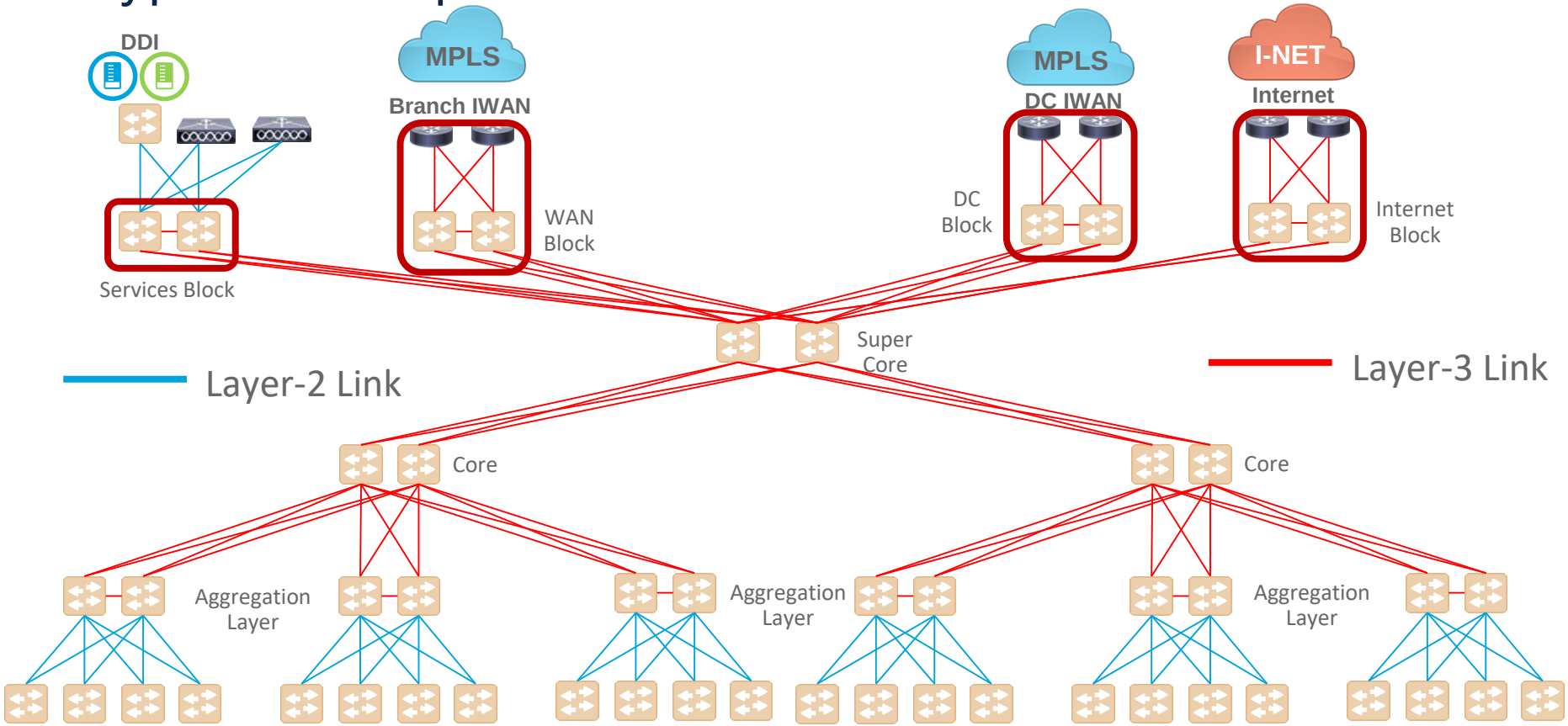
- **Move some** Policy enforcement point(s) **down to the Access Layer.** For example, IP ACLs, QoS, NetFlow can be applied at the Access layer
- **Move some** Policy enforcement point(s) **outside the SD-Access fabric.** For example, PBR, WCCP can be applied external to the fabric.



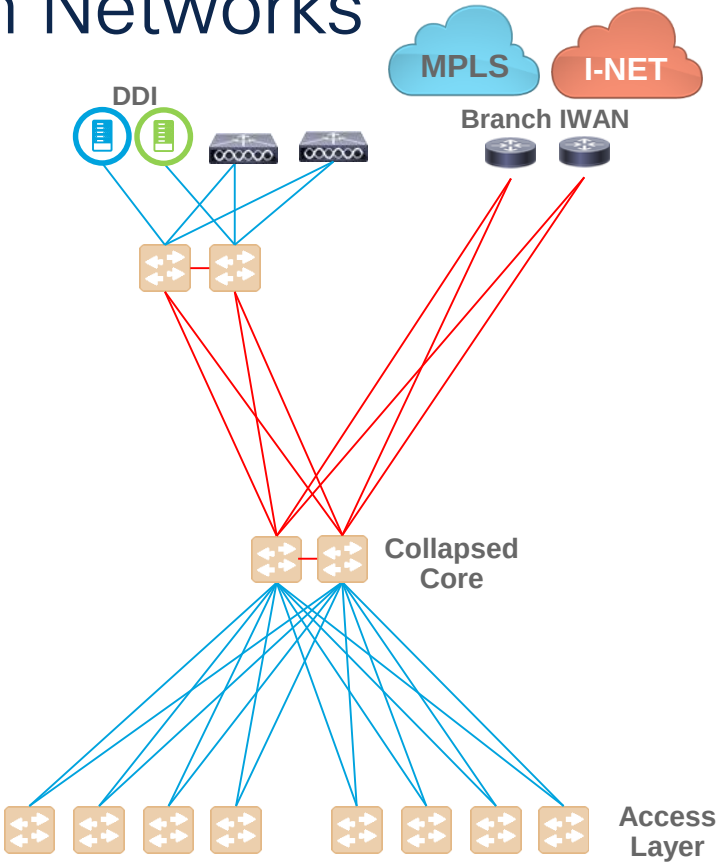
# Two Basic Types of Deployments

- Campus Networks/(Large Sites)
- Branch Networks/(Small Sites)

# Typical Campus Networks



# Typical Branch Networks



# Two Basic Approaches to Migration

- Parallel Deployment (all at once)
- Incremental Deployment (one at a time)

# Migration Approaches: Parallel vs Incremental

| Parallel | Incremental |
| --- | --- |
| Best for Branch (small scale) deployments | Best for Campus (any size) |
| Requires cable runs to create a new parallel network | Requires a couple of cables from new access and distribution switches |
| Power and outlets for the parallel network | Incremental power and outlet requirement |
| Legacy hardware in existing network | Legacy hardware in existing network |
| Upgrade most of the network infrastructure | Upgrade most of the network infrastructure |
| Clean slate (leaving behind any complexity in the old design) | Will need to carry forward the constraints of the old design in the underlay |
| Test users in a complete new network | Test of functionality is partial |
| Easy Rollback of migrated users | Easy Rollback of migrated users |

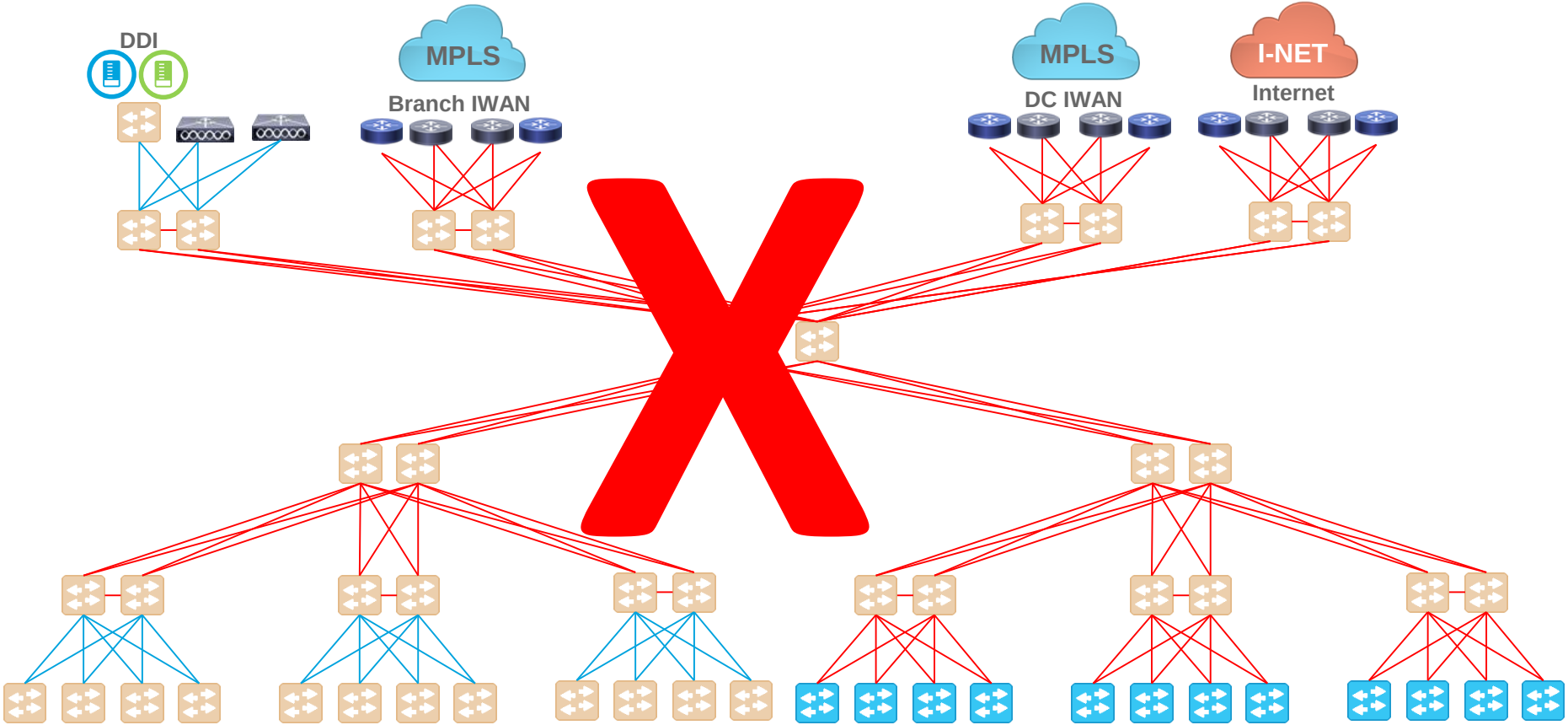
IMPLEMENTATION

RESOURCES

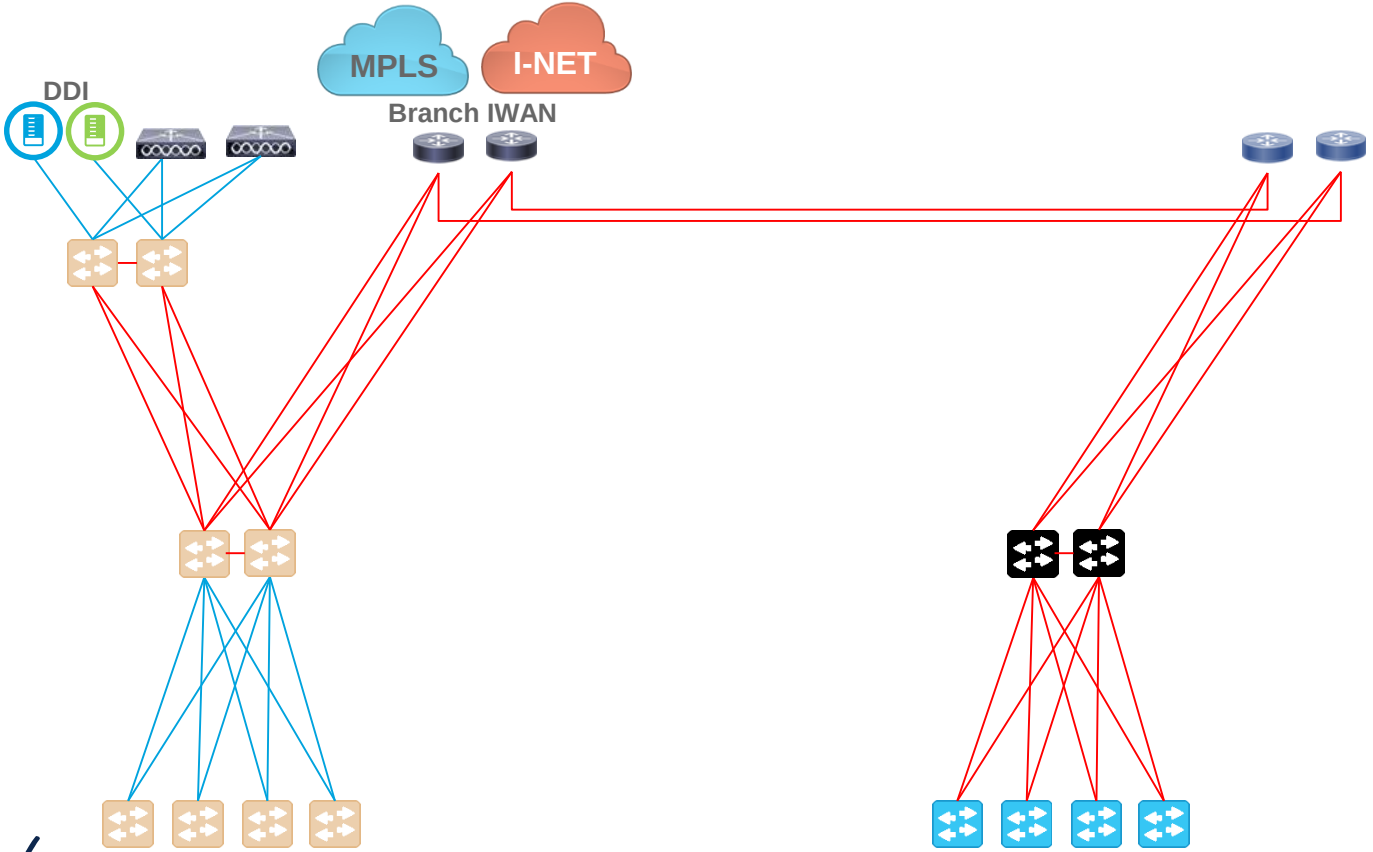
RESOURCES

IMPLEMENTATION

# Parallel Install may not feasible for Campus Networks

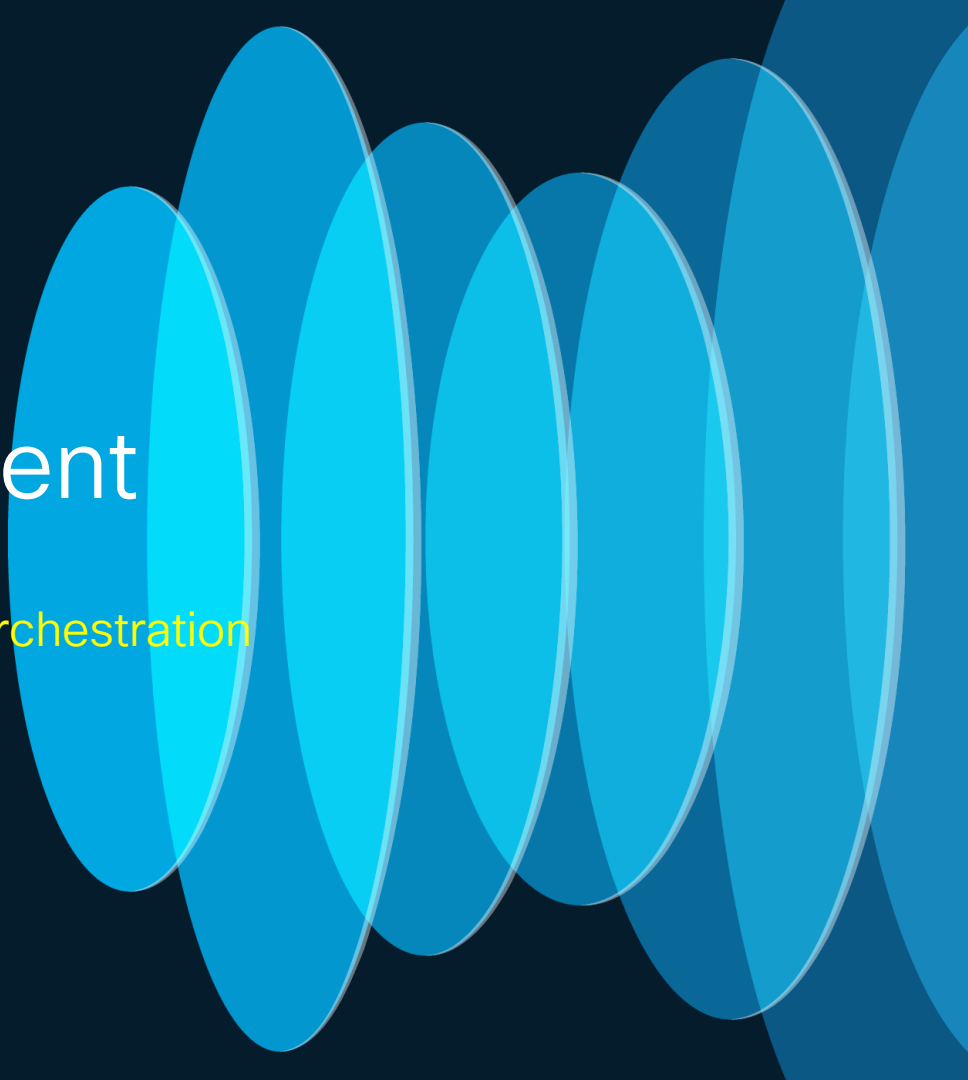


# Parallel Install for Branch Networks



# Installing Management Components

## Brains behind automation and policy orchestration

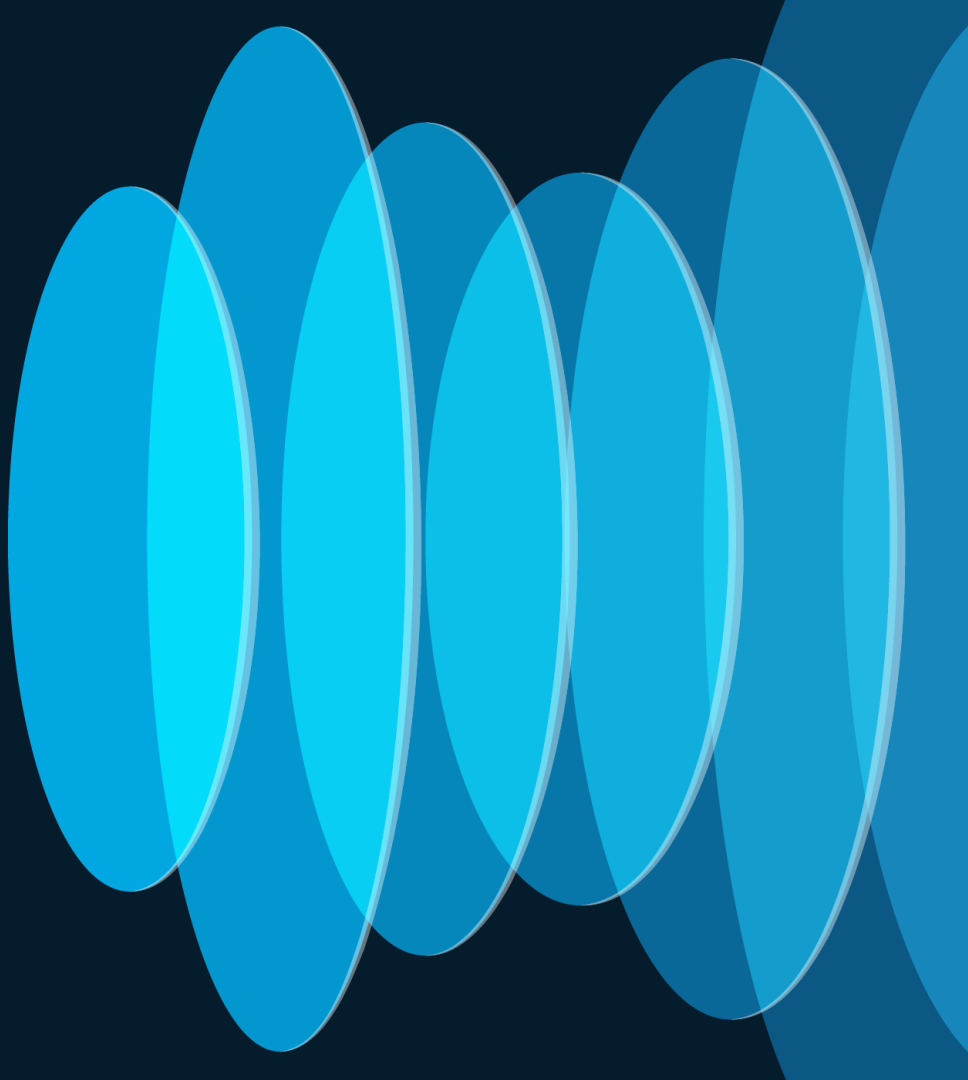


cisco Live!

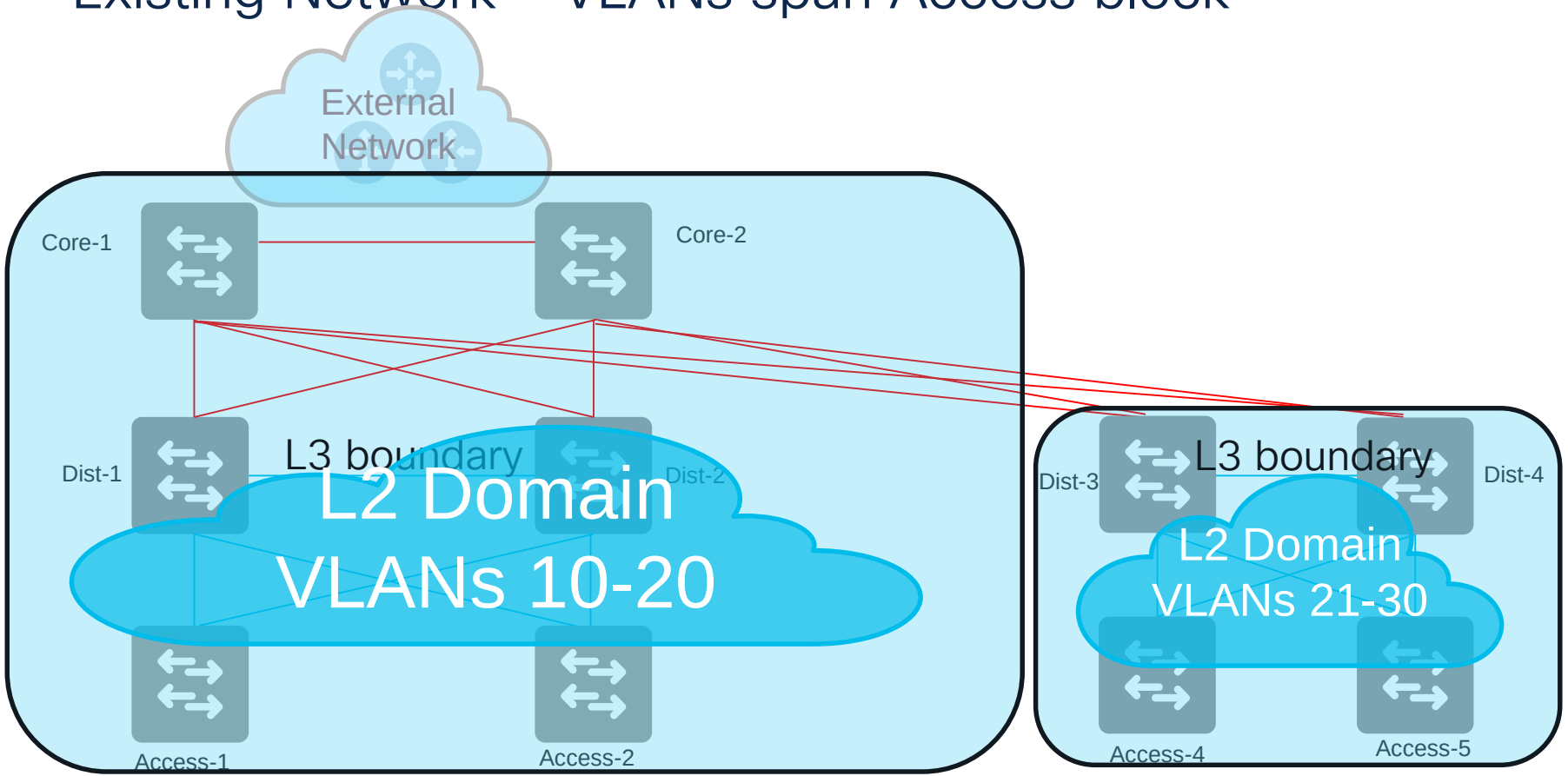
# Install Cisco Catalyst Center and ISE

- Install Cisco Catalyst Center and ISE
- Create Network Hierarchy of Sites
- Create Network environment for NTP, DHCP, and other management entities
- Create Virtual Networks
- Integrate ISE with Cisco Catalyst Center
- Define policies in Cisco Catalyst Center or ISE whichever applicable
- Create network templates to be provisioned on switches, routers, WLCs
- Discover the devices

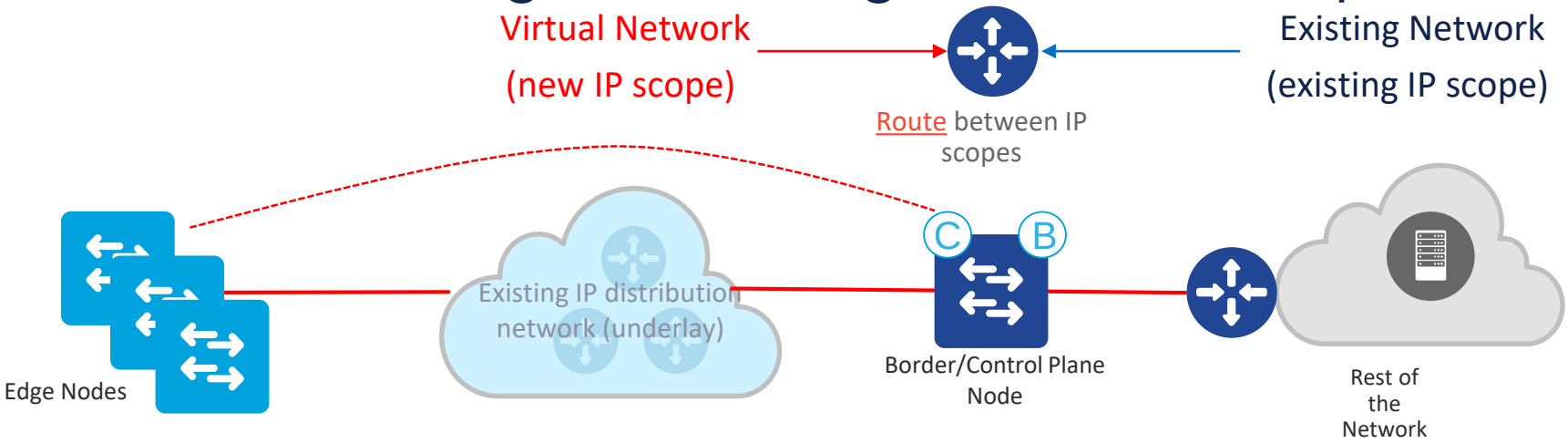
# Migrate L2 Access



# Existing Network – VLANs span Access block



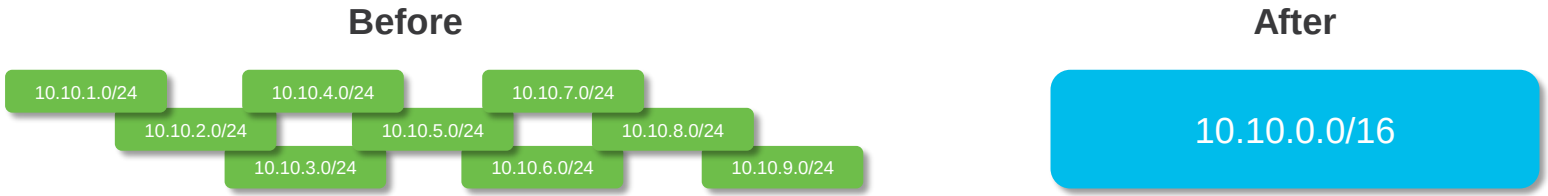
# Incremental Migration – High Level concept



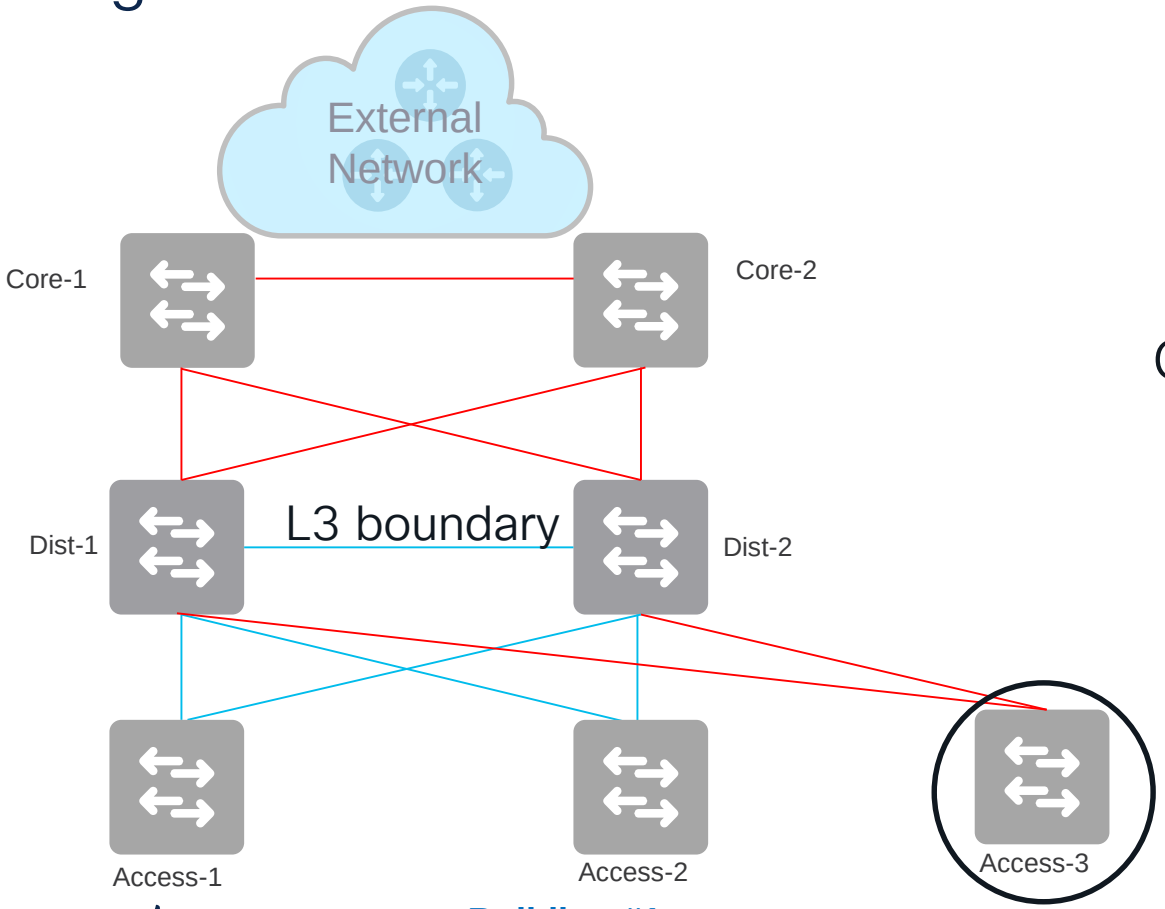

- Deploy a **Border/Control Plane node** and an **Edge node**
- A virtual network with new address is formed over the existing network
- **Incrementally** add Fabric Edge nodes
- The virtual network connects to the existing/external network via the border

# Considerations for using new subnets to transition

- Immediately realize the advantages of bigger subnets, but lesser subnets that are optimized for Cisco SD-Access
- Design for the present and the future
- Add DHCP scope and size
- Update existing firewall rules for that one big subnet
- Not a big issue for endpoints with IP stacks that work well with DHCP



# Migrate L2 Access – Insert new Access Switch



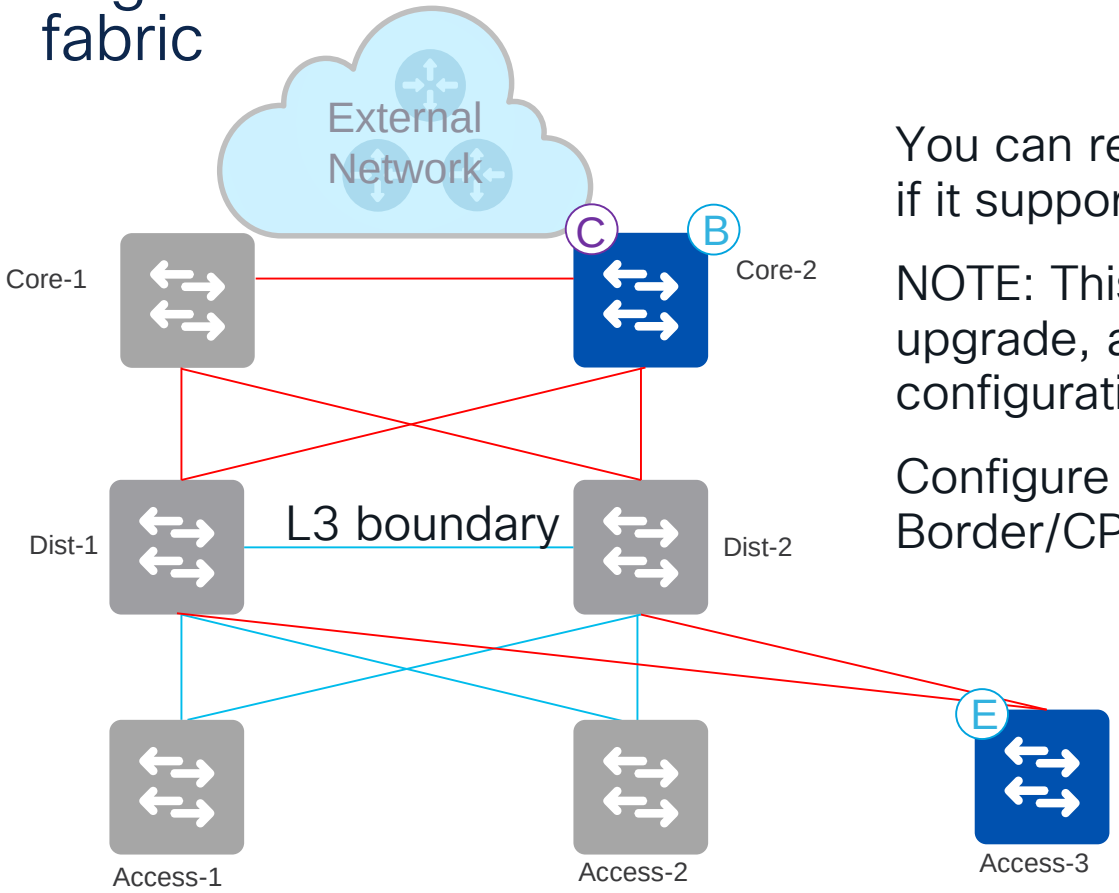

Connect a new switch in the access layer and connect to distribution layer with **Routed Access**

# Prepping the Switch and underlay

Set following on the Fabric nodes and other nodes in the underlay

- Set MTU to 9100 on the switch and the existing network.
- Configure ‘ip routing’
- Set ‘username’ and ’password’ for device access
- Configure VTY and console lines for device access
- Configure NTP
- Configure SNMP, syslog
- Configure Loopback0 (/32) for RLOC, and underlay IP addresses
- Configure multicast in the underlay if you want to run native multicast in the fabric

# Migrate L2 Access – Re-use Core as Border/CP node for fabric

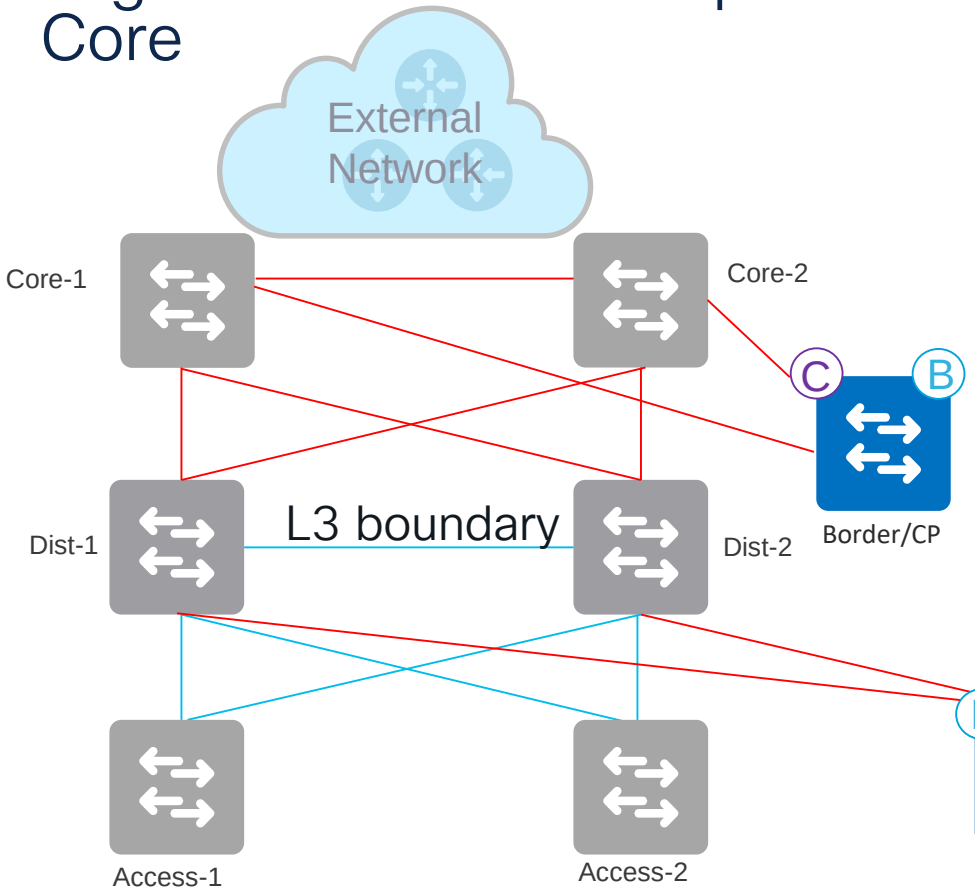



You can reuse an existing Core switch if it supports Fabric functionality

NOTE: This may require software upgrade, and adding new fabric overlay configurations

Configure the Fabric Edge and Border/CP from Cisco Catalyst Center

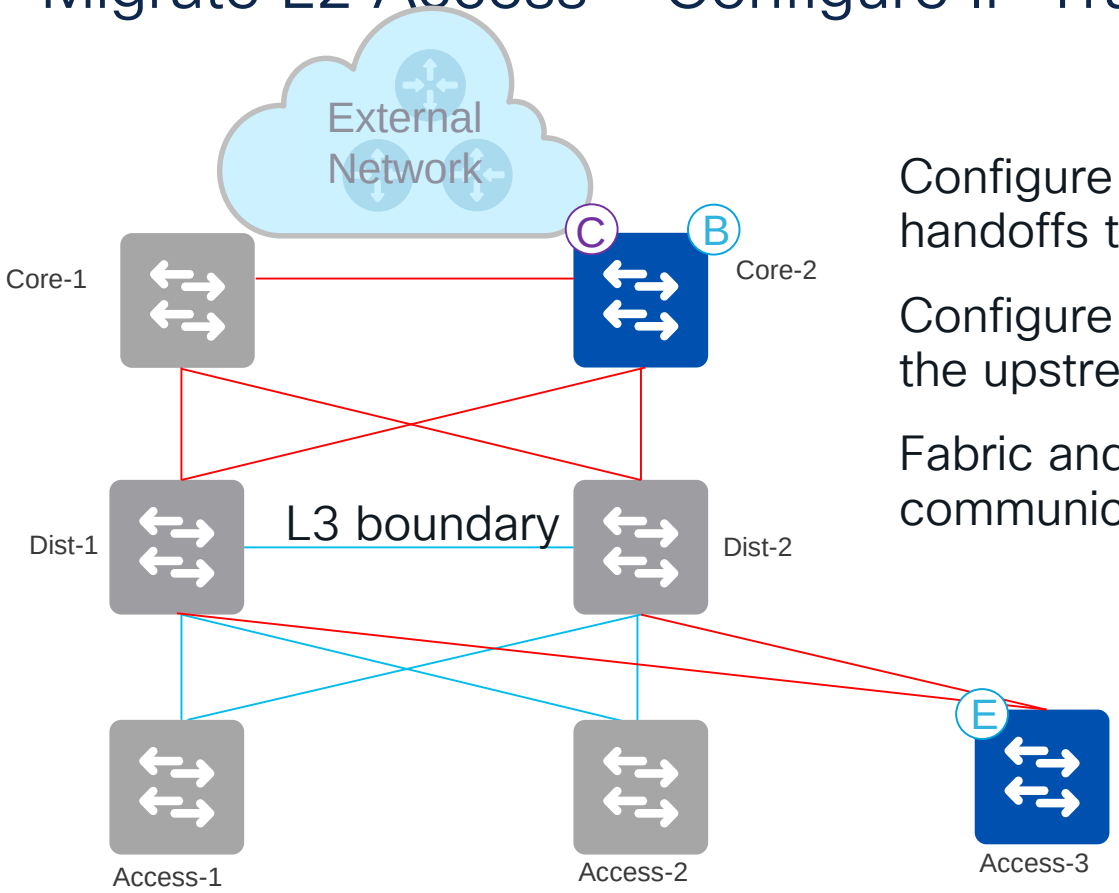
# Migrate L2 Access – Option of connecting Border/CP to Core




If the existing core does not support Fabric functionality,

Connect a new switch to the existing core layer that will be a Border/Control Plane node

# Migrate L2 Access – Configure IP Transit handoff



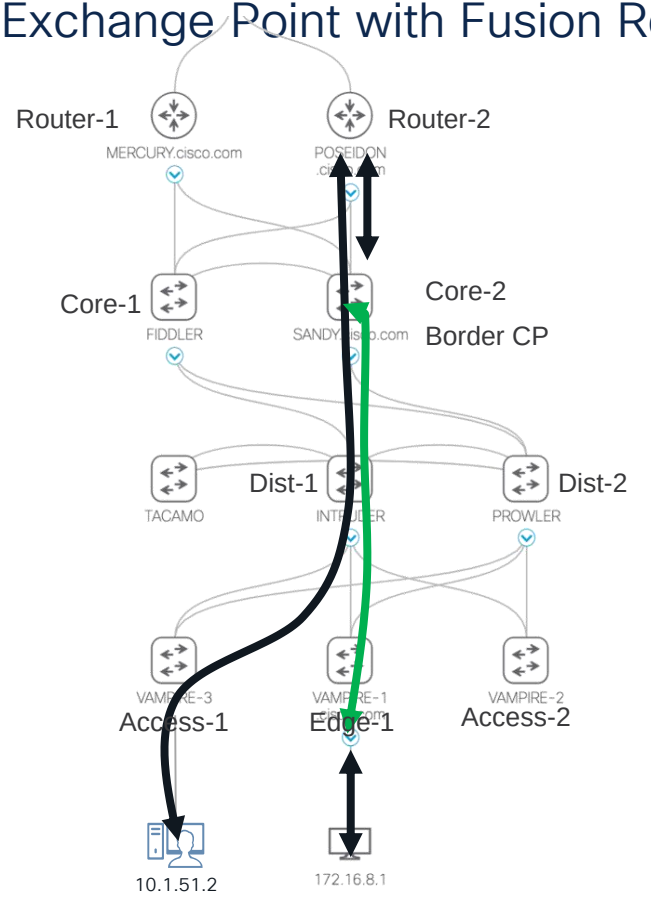

Configure the respective IP Transit VRF handoffs to the upstream router

Configure the required route-leaking at the upstream router

Fabric and existing network traffic will communicate via the upstream router

# Communications in SD-Access-LISP Fabric

## East-West: Fabric Border is Exchange Point with Fusion Router

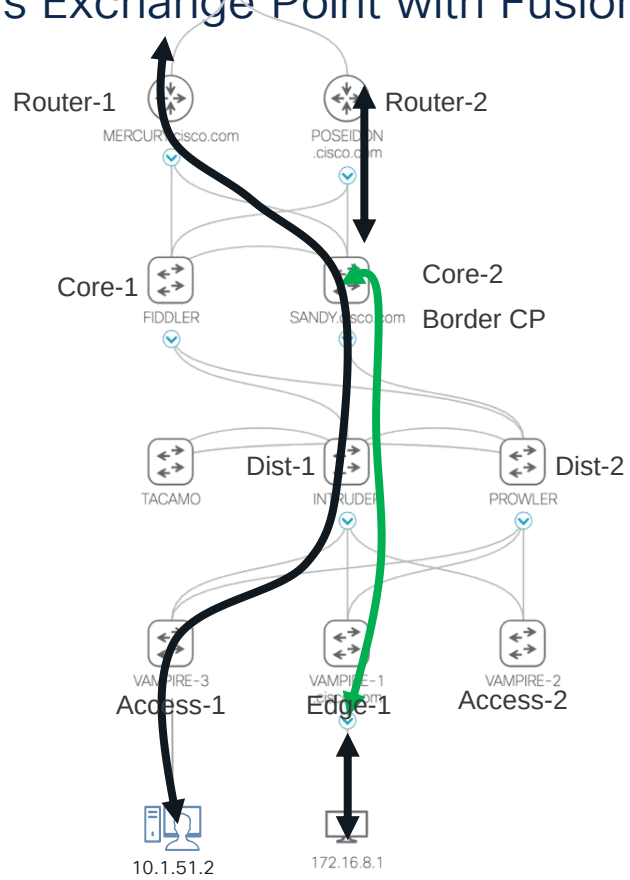



Un-encapsulated packet

VXLAN encapsulated packet

# Communications in SD-Access-LISP Fabric

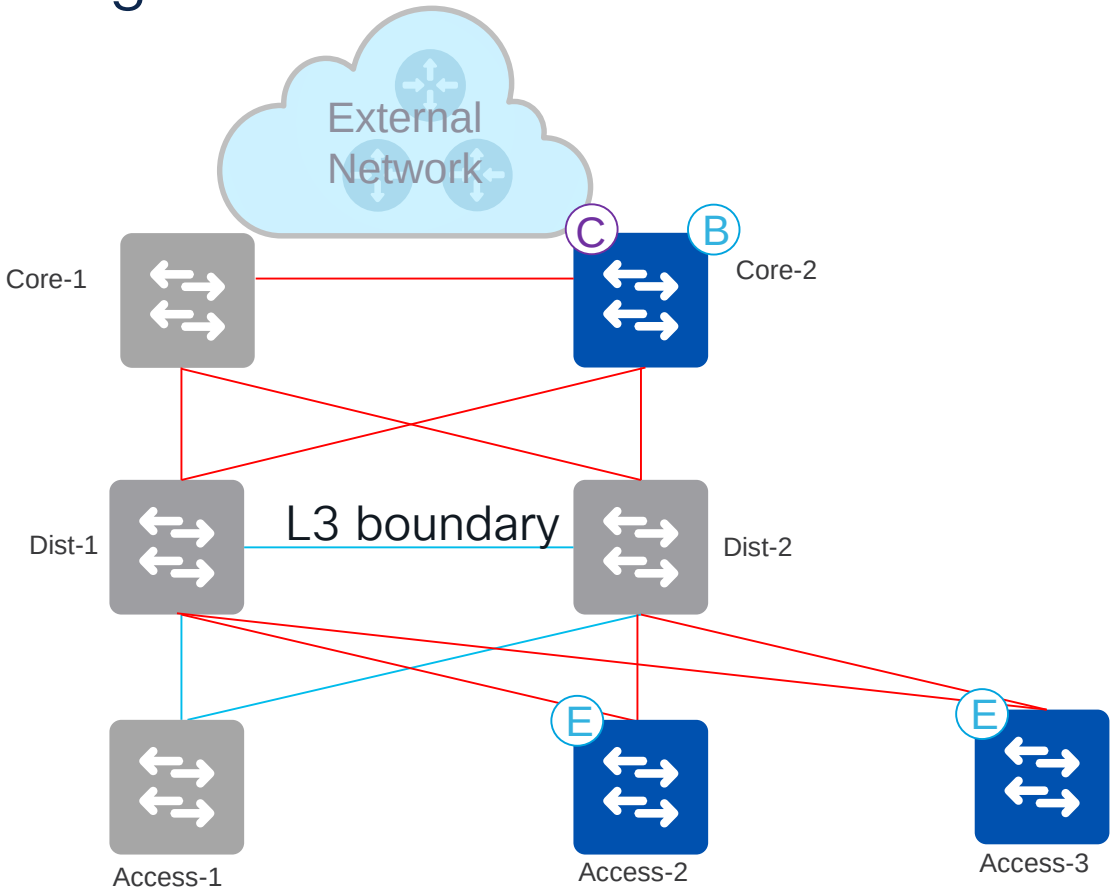
## North-South: Fabric Border is Exchange Point with Fusion Router



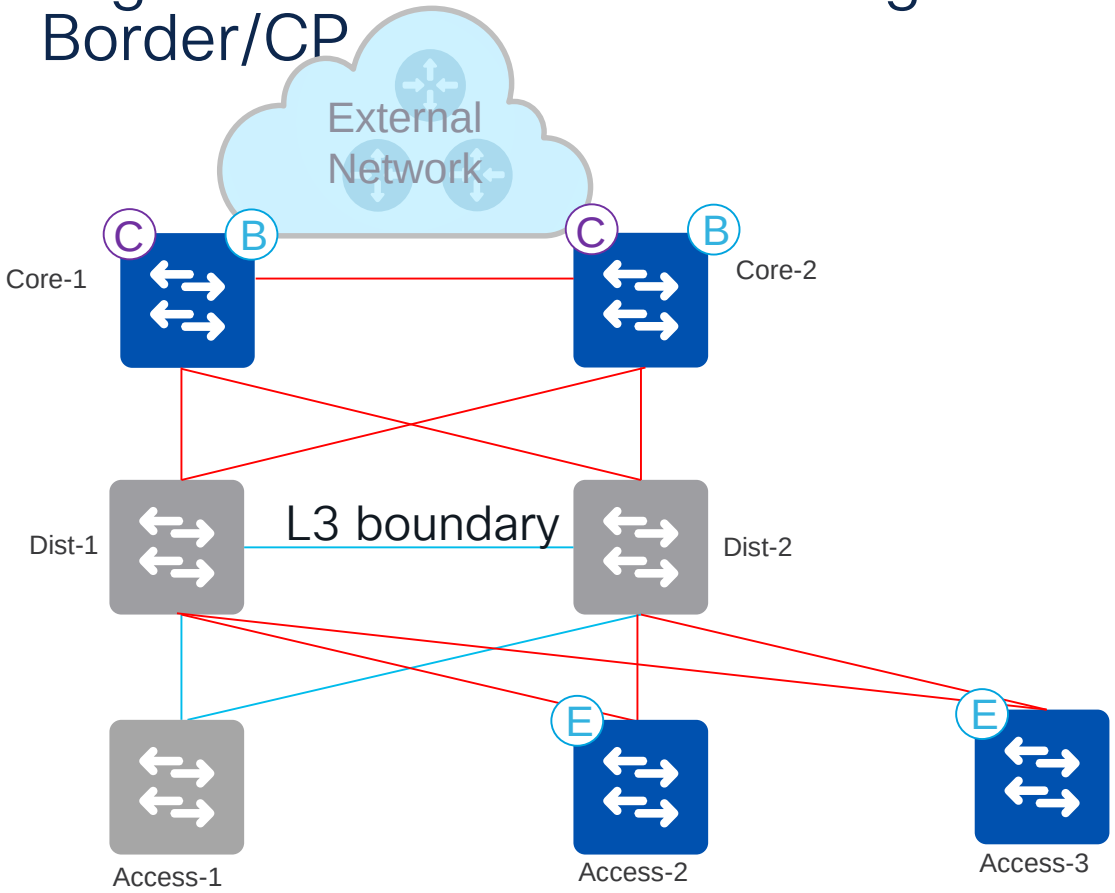

Un-encapsulated packet

VXLAN encapsulated packet

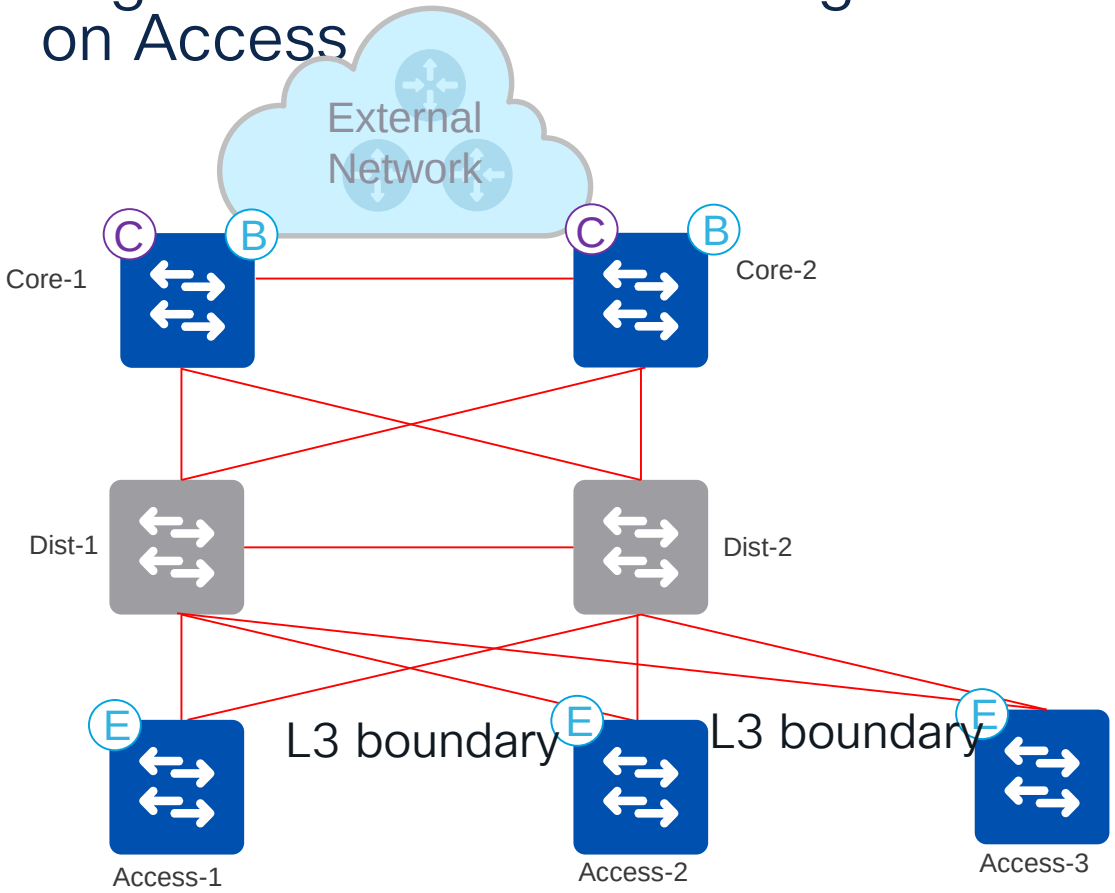
# Migrate L2 Access – Rollover



# Migrate L2 Access – Reconfigure Second Core to be Border/CP

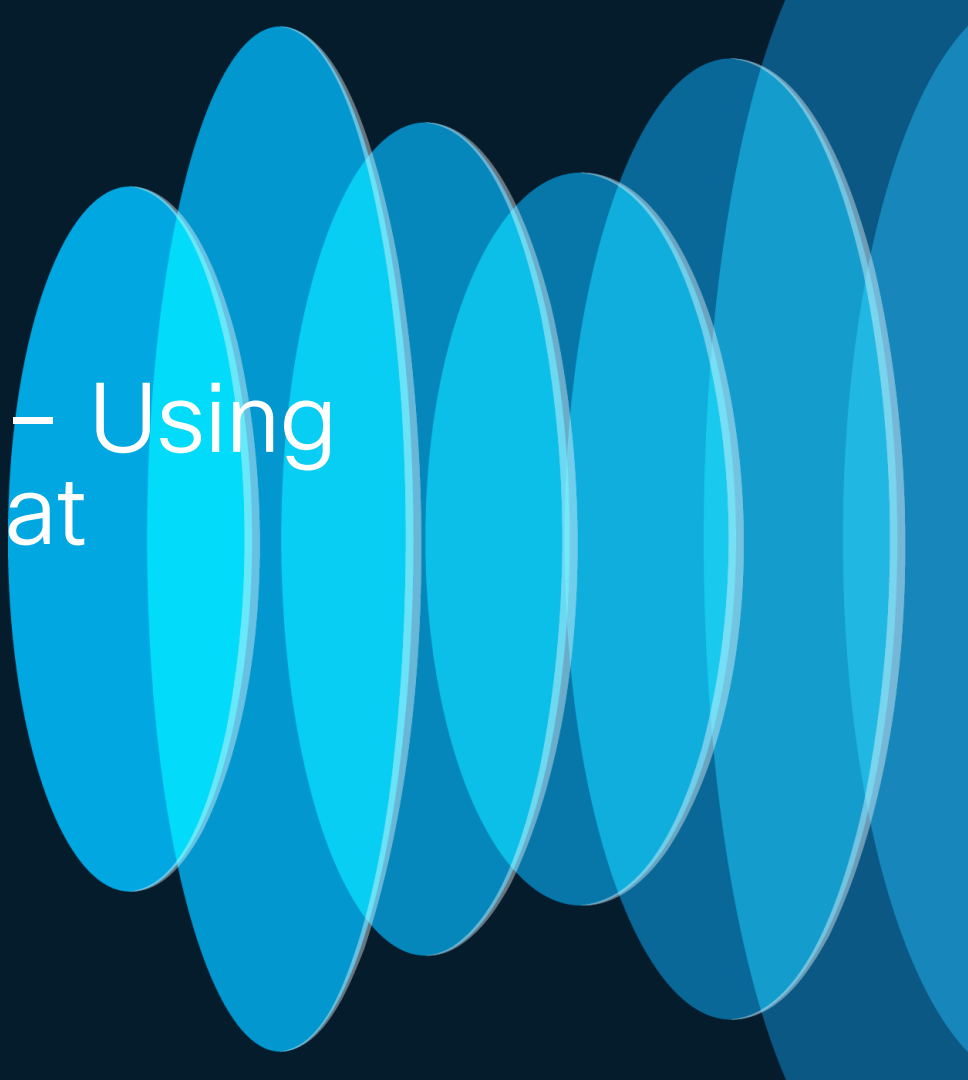


# Migrate L2 Access – Configure Fabric Edge functionality on Access



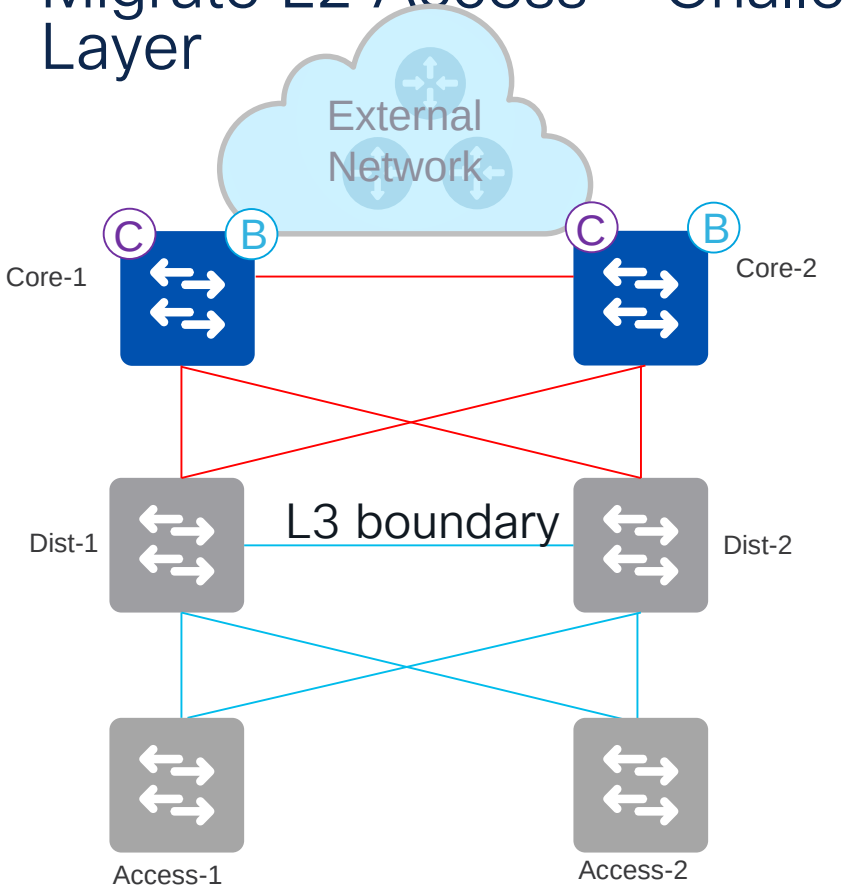
# Migrate L2 Access – Using Fabric Edge nodes at Distribution

Get Ready, Strap In, here we go!!



cisco Live!

# Migrate L2 Access – Challenge in converting Access Layer

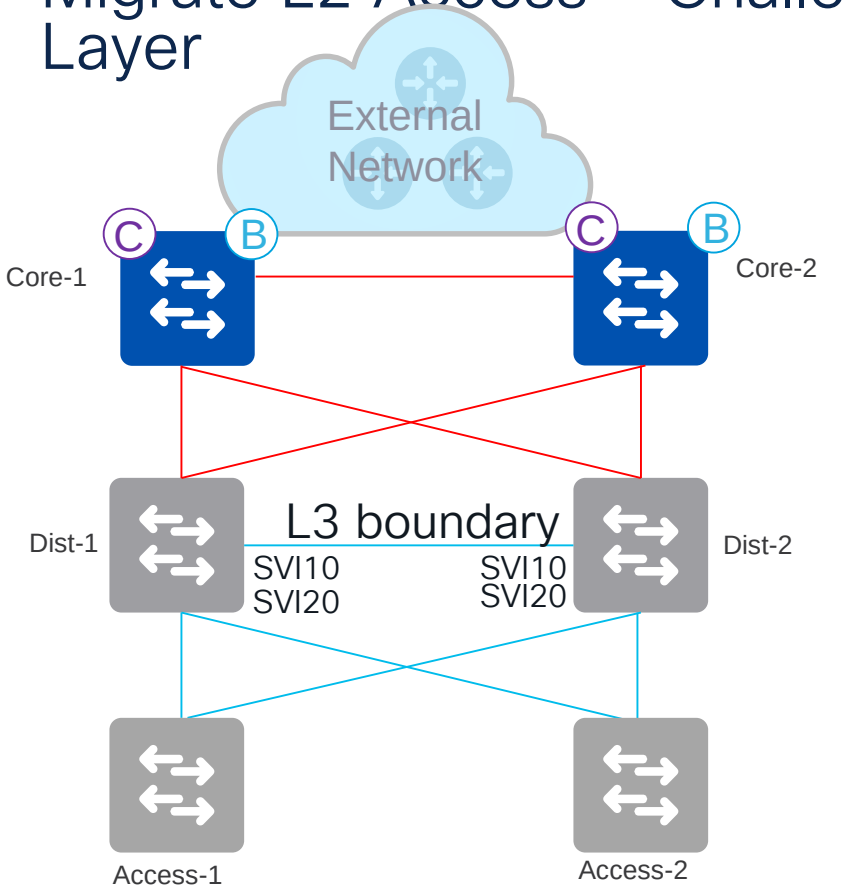



Access layer not compatible with SD-Access-LISP functionality

Critical or high-risk environment to move into fabric

Need a quick win from a segmentation perspective

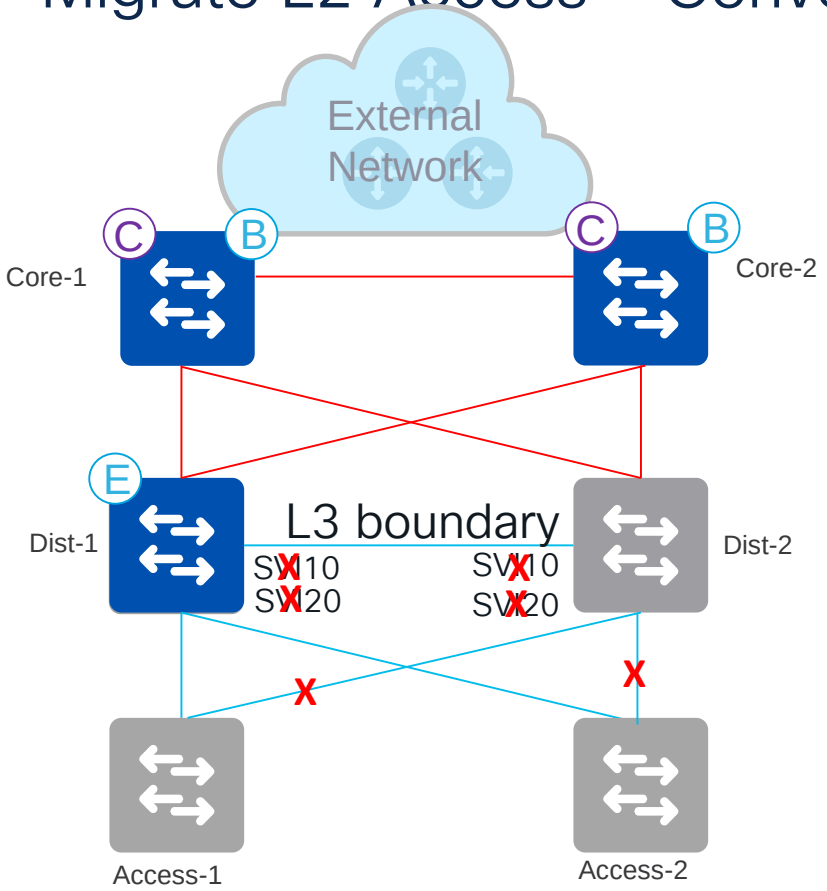
# Migrate L2 Access – Challenge in converting Access Layer




Consider Vlan 10 (10.1.1.0/24) and Vlan 20 (10.1.2.0/24) presence on the existing network switches

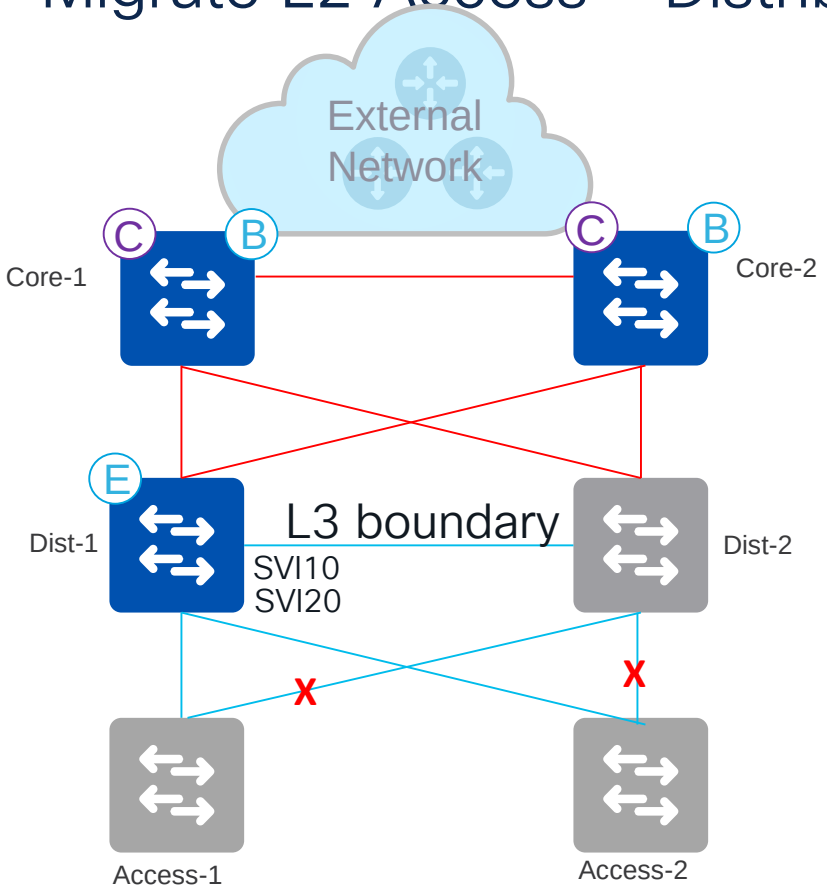
SVI of Vlan 10 and Vlan 20 is on Distribution Switches

# Migrate L2 Access – Convert Distribution to Fabric Edge



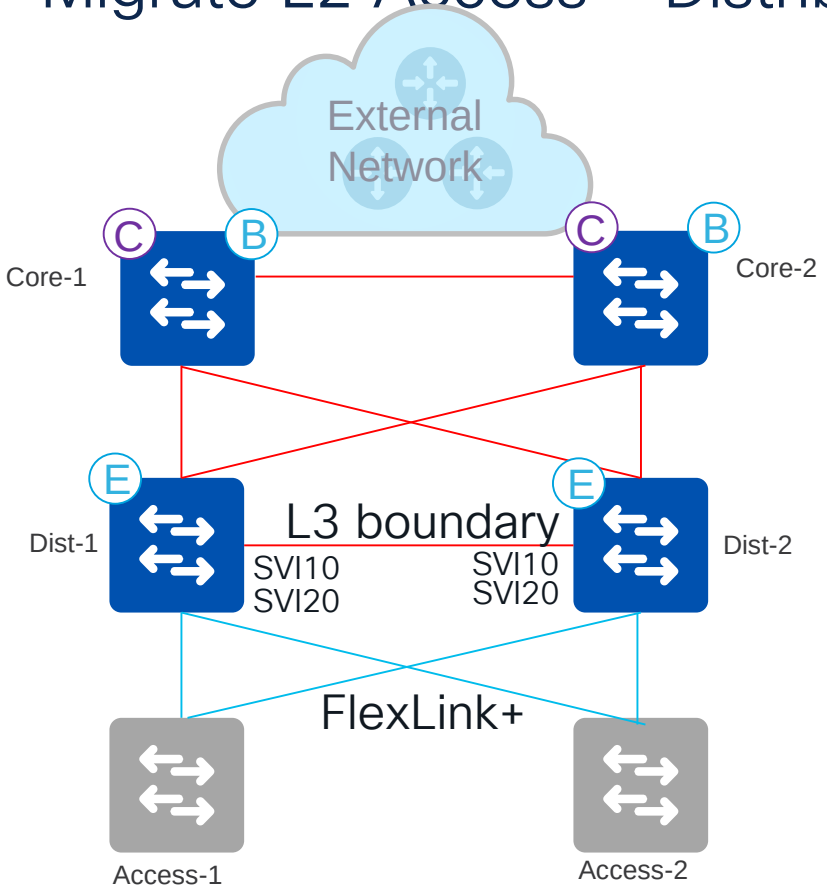

- Easier and a quick way to migrate network into fabric
- Shutdown SVIs on Dist-1 and Dist-2
- Shutdown duplicate Trunk links
- Single connect from Access to Distribution (FE)
- Configure Dist-1 as a Fabric Edge
- Use custom Vlan # feature to configure same Vlan as existing network

# Migrate L2 Access – Distribution to Fabric Edge




Redundancy provided by In-System redundancy in distribution node eg: SVL or StackWise or Redundant Supervisors in modular chassis

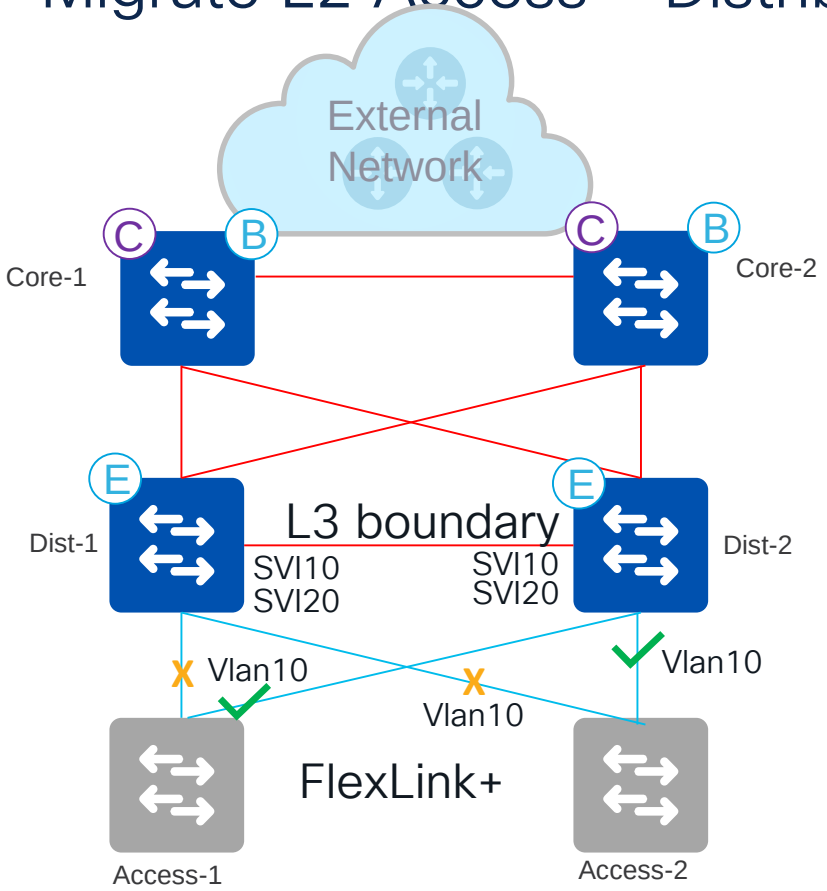
# Migrate L2 Access – Distribution #2 to Fabric Edge




Configure Dist-2 as another Fabric Edge

Dual-connect with FlexLink+ on the L2 switches – Active/Standby mode only.

# Migrate L2 Access – Distribution #2 to Fabric Edge



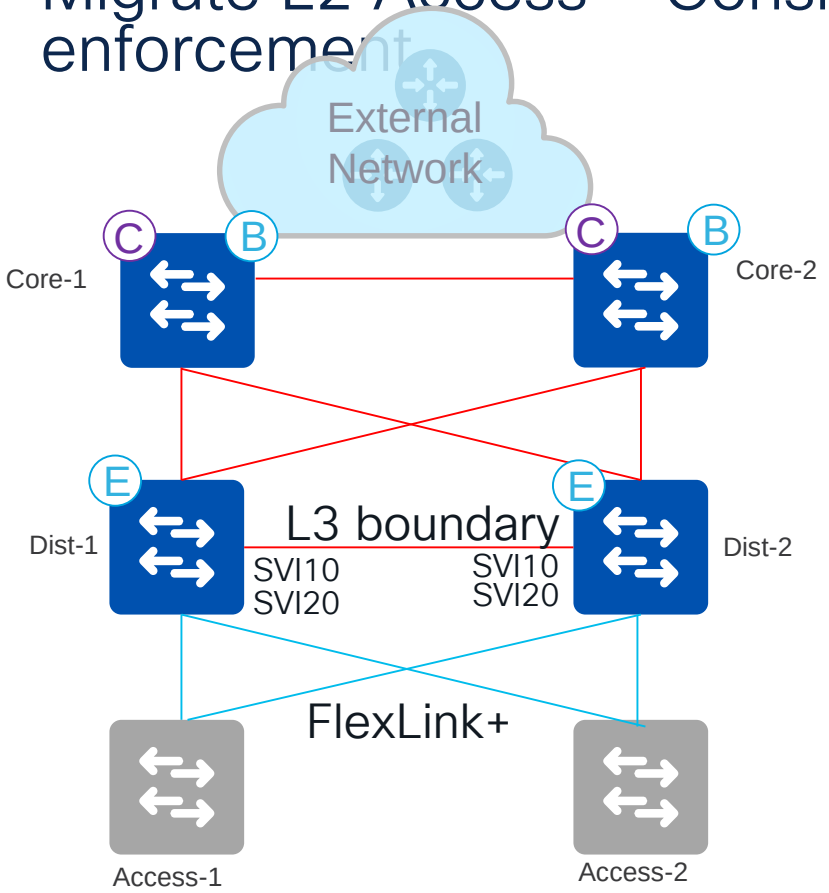

Configure Dist-2 as another Fabric Edge

Dual-connect with FlexLink+ on the L2 switches – Active/Standby mode only.

Load-balancing of VLANs supported across Fabric Edges/Dist switches

For example Dist-1 is active for Vlan20, and Dist-2 is active for Vlan10.

# Migrate L2 Access – Considerations for SGACL enforcement

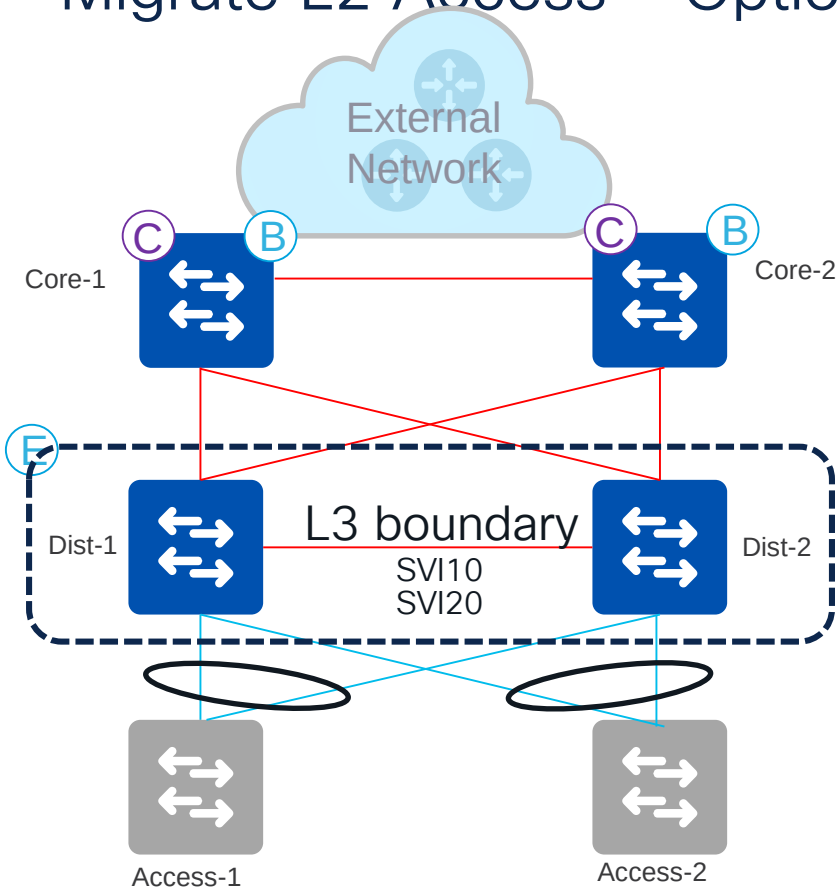



Consider scale of local endpoints that can be onboarded on an individual fabric edge node

E-W micro-segmentation from the Fabric Edge nodes, not on the Access switches

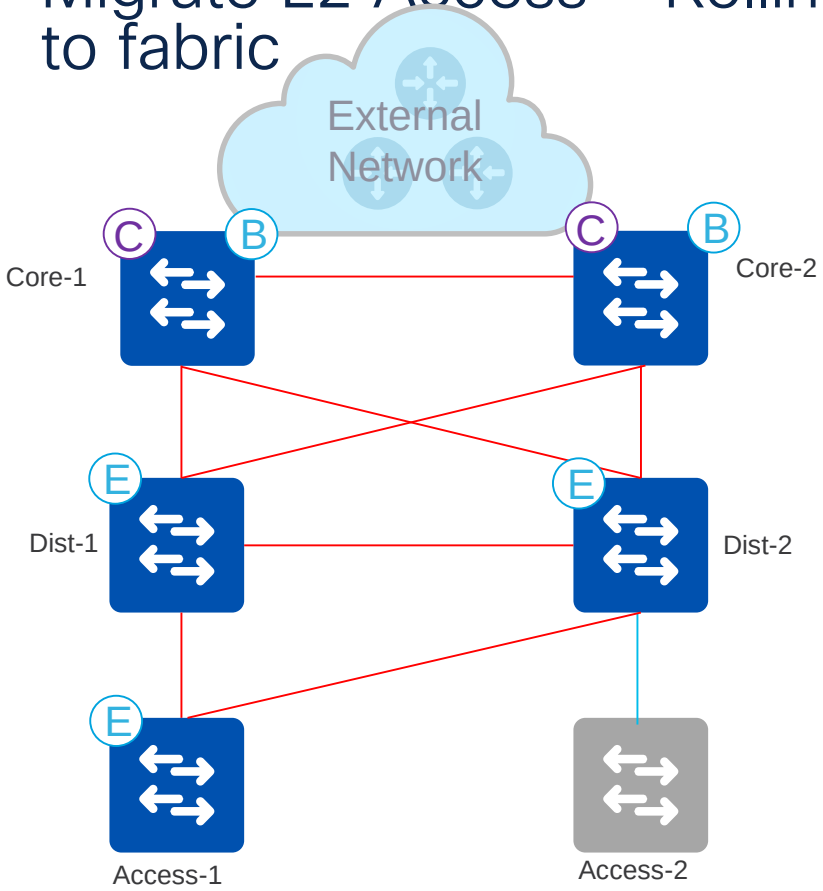
SGACL Policy enforcement point will be Distribution that act as Fabric Edges

# Migrate L2 Access – Option to load-balance




Build SVL pair of distribution layer for redundancy and additional usage of links for bandwidth

# Migrate L2 Access – Rolling migration to convert Access to fabric

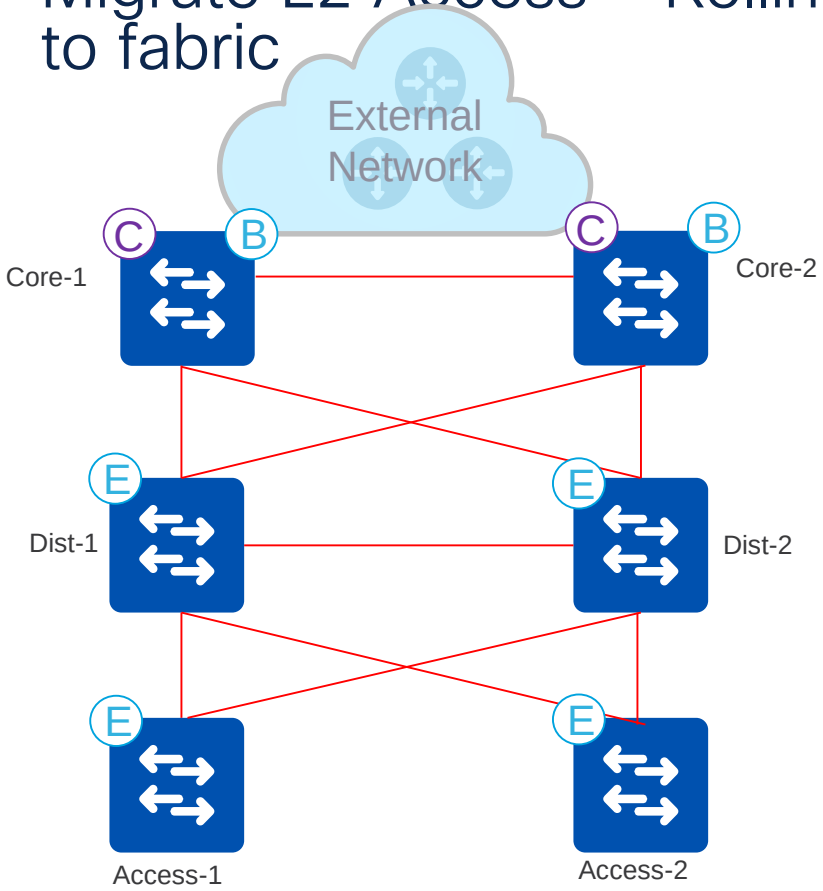



Connect Access with Routed Links to Distribution

Prep the switch with Loopback0 and other management configurations

Discover the device and configure Fabric Edge functionality using Cisco Catalyst Center

# Migrate L2 Access – Rolling migration to convert Access to fabric

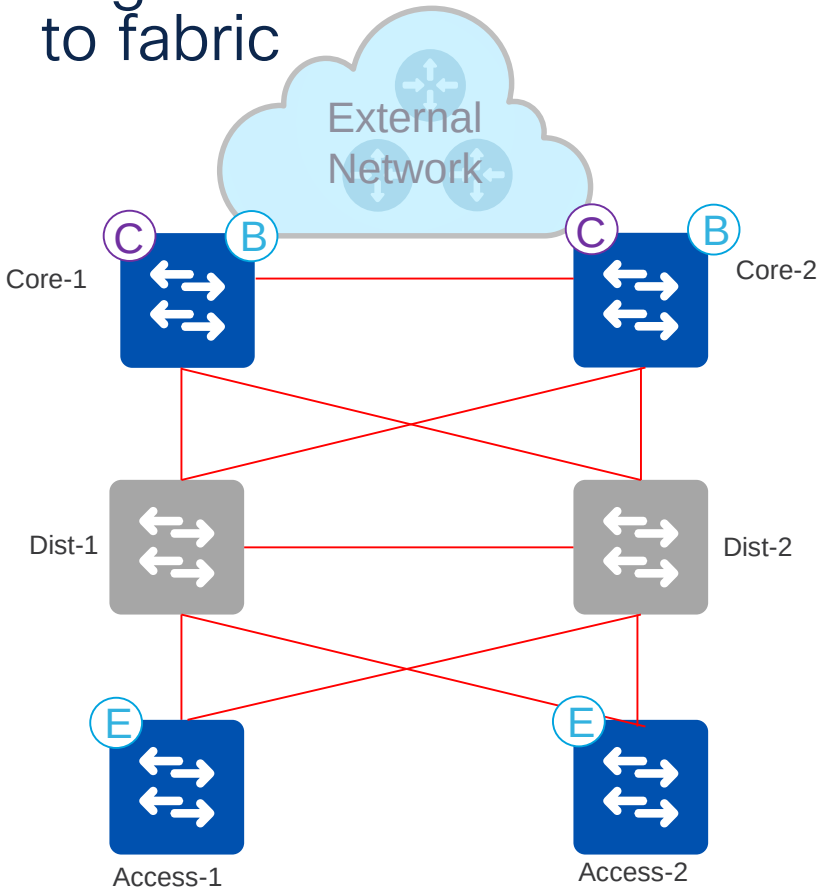



Connect Access with Routed Links to Distribution

Prep the switch with Loopback0 and other management configurations

Discover the device and configure Fabric Edge functionality using Cisco DNA Center

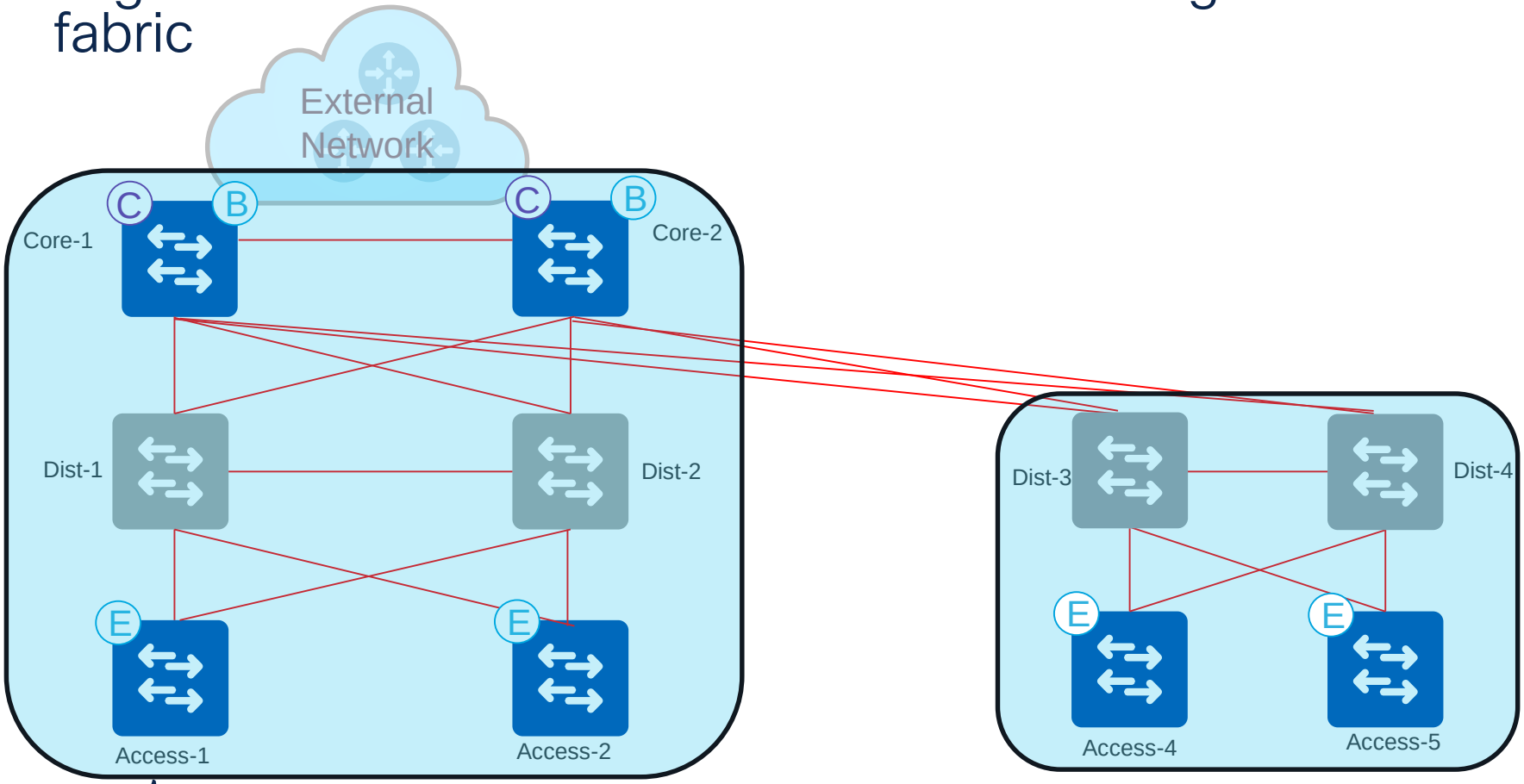
# Migrate L2 Access – Rolling migration to convert Access to fabric




Once the Access layer is converted to Fabric Edge, de-configure the Distribution to normal switches aka intermediate nodes

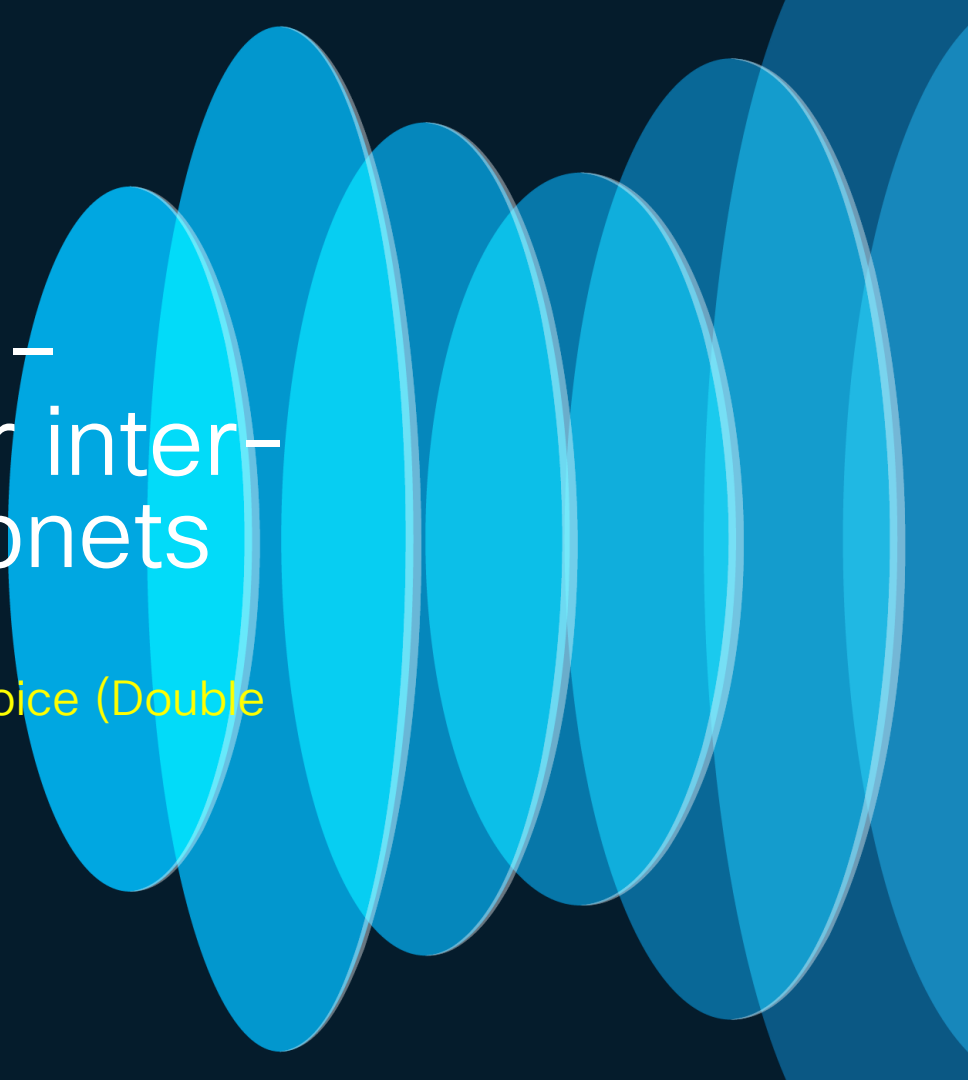
Follow similar procedure in Building #2, to create the fabric in entire campus

# Migrate L2 Access – End state of network migrated to fabric

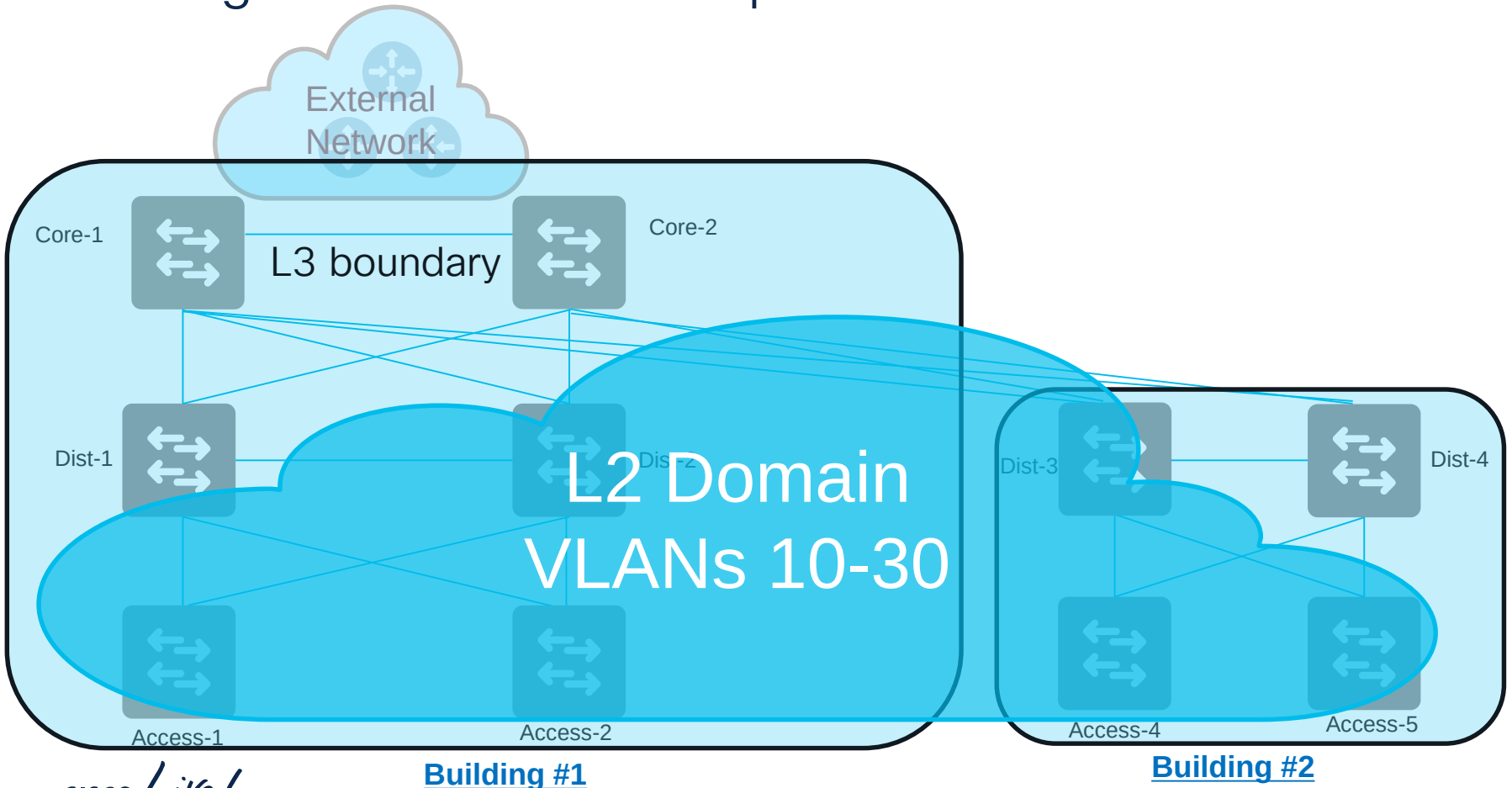


# Migrate L2 Access – Using L2 Border for inter-operating same subnets in and out of Fabric

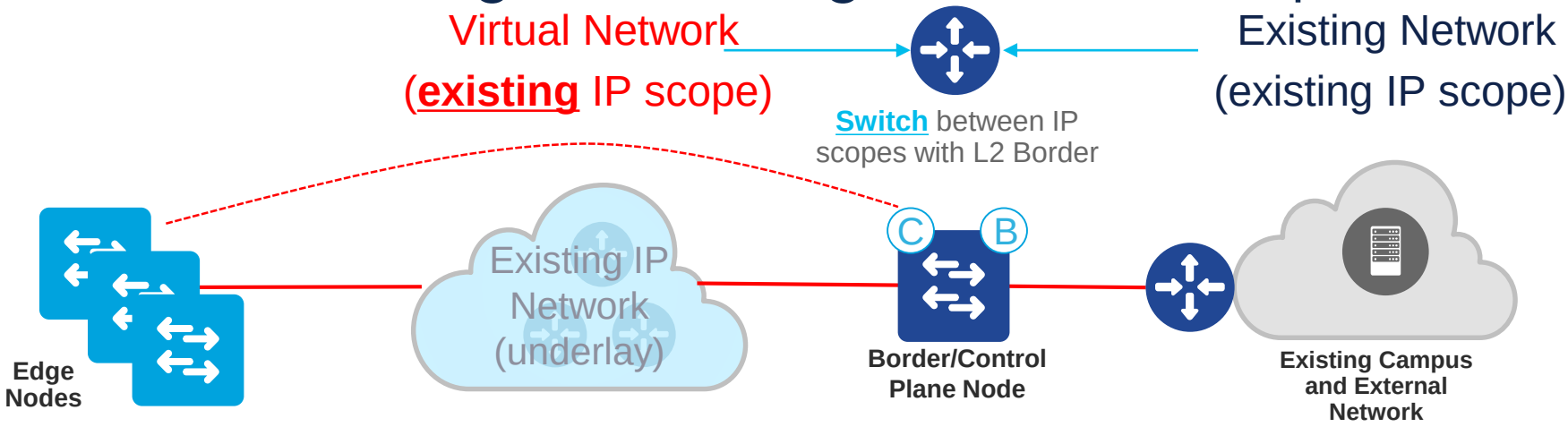
Get Ready, Get a beverage of your choice (Double Espresso) Strap In, here we go!!



# Existing Network – VLANs span Distribution Blocks

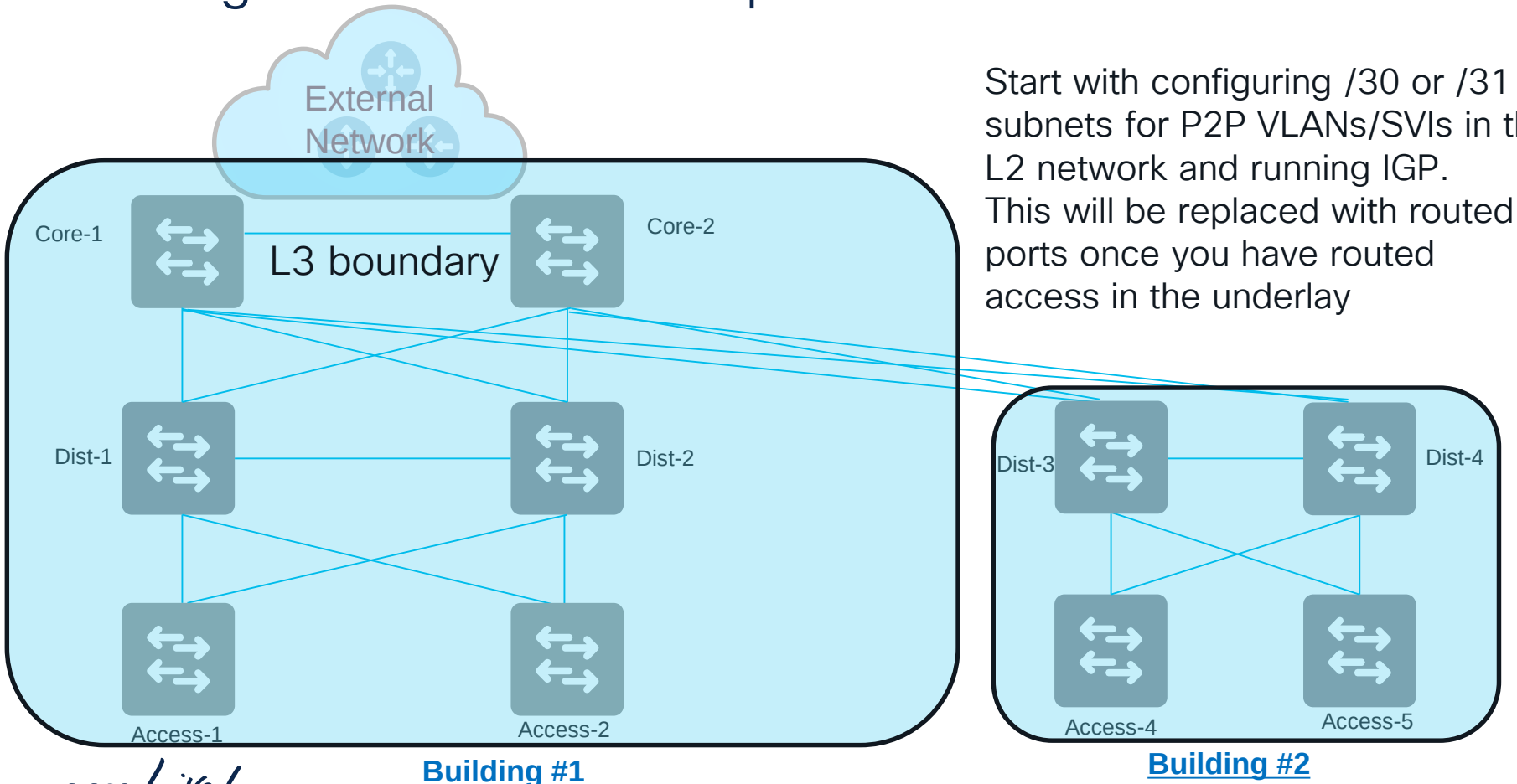


# Incremental Migration – High Level concept



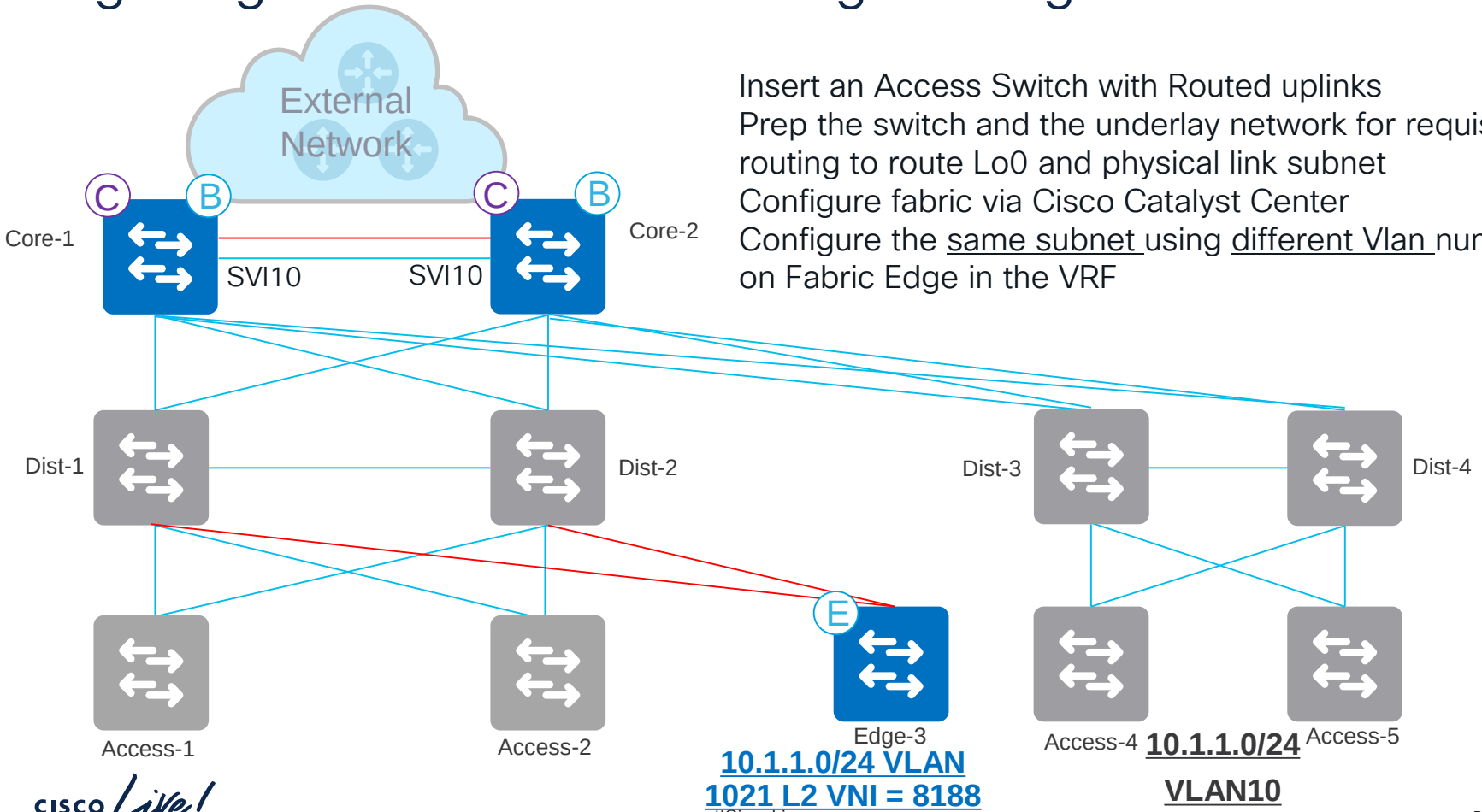

- Deploy a Border node and incrementally add Edge Nodes
- A virtual network is formed over the existing (underlay) network
- The virtual network(s) uses same subnet address as existing network
- The network in fabric connects to the old network through the L2 border

# Existing Network – VLANs span Distribution Blocks



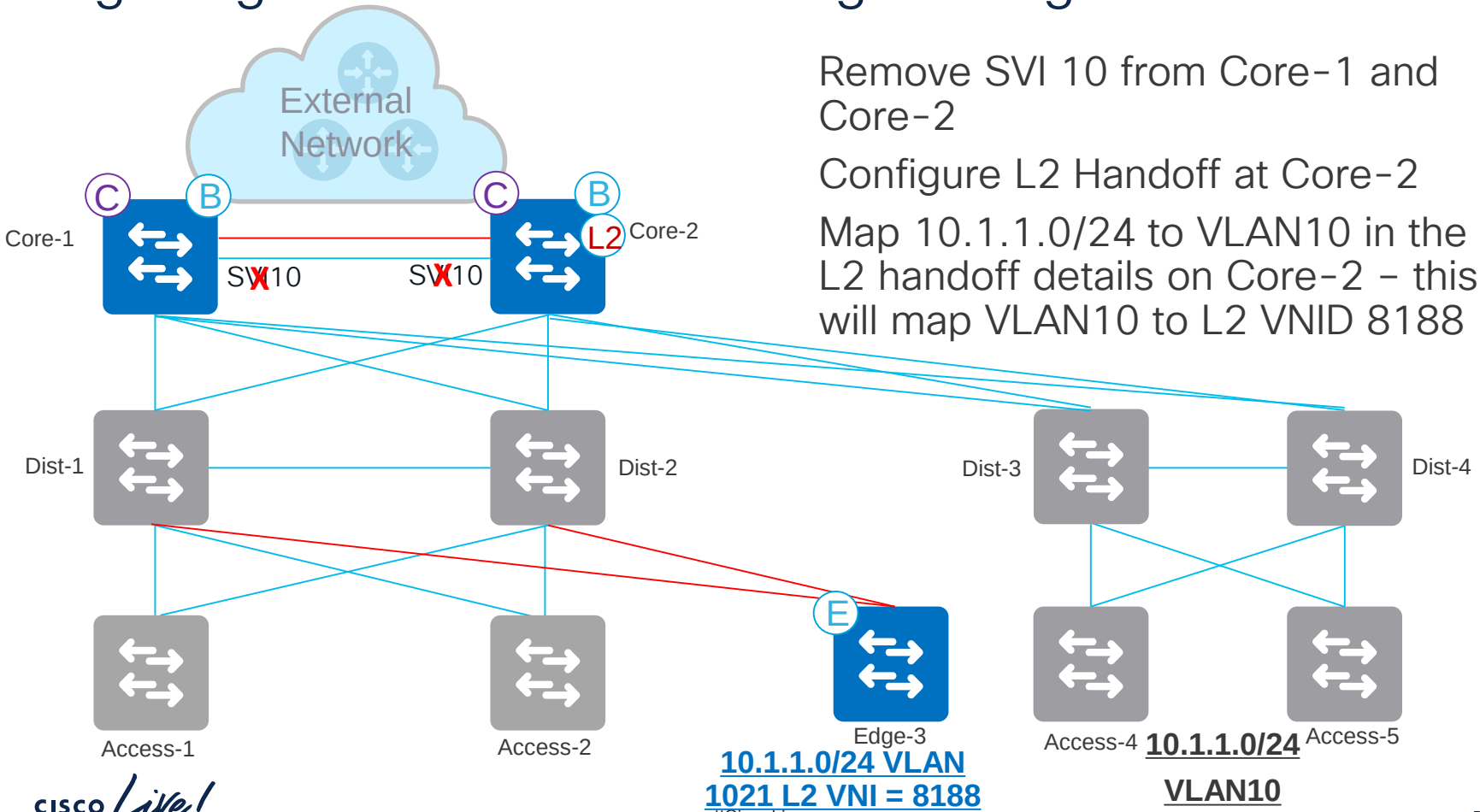

Start with configuring /30 or /31 subnets for P2P VLANs/SVIs in the L2 network and running IGP.
This will be replaced with routed ports once you have routed access in the underlay

# Migrating to SD-Access retaining existing subnets




Insert an Access Switch with Routed uplinks
Prep the switch and the underlay network for requisite routing to route Lo0 and physical link subnet
Configure fabric via Cisco Catalyst Center
Configure the same subnet using different Vlan number on Fabric Edge in the VRF

# Migrating to SD-Access retaining existing subnets

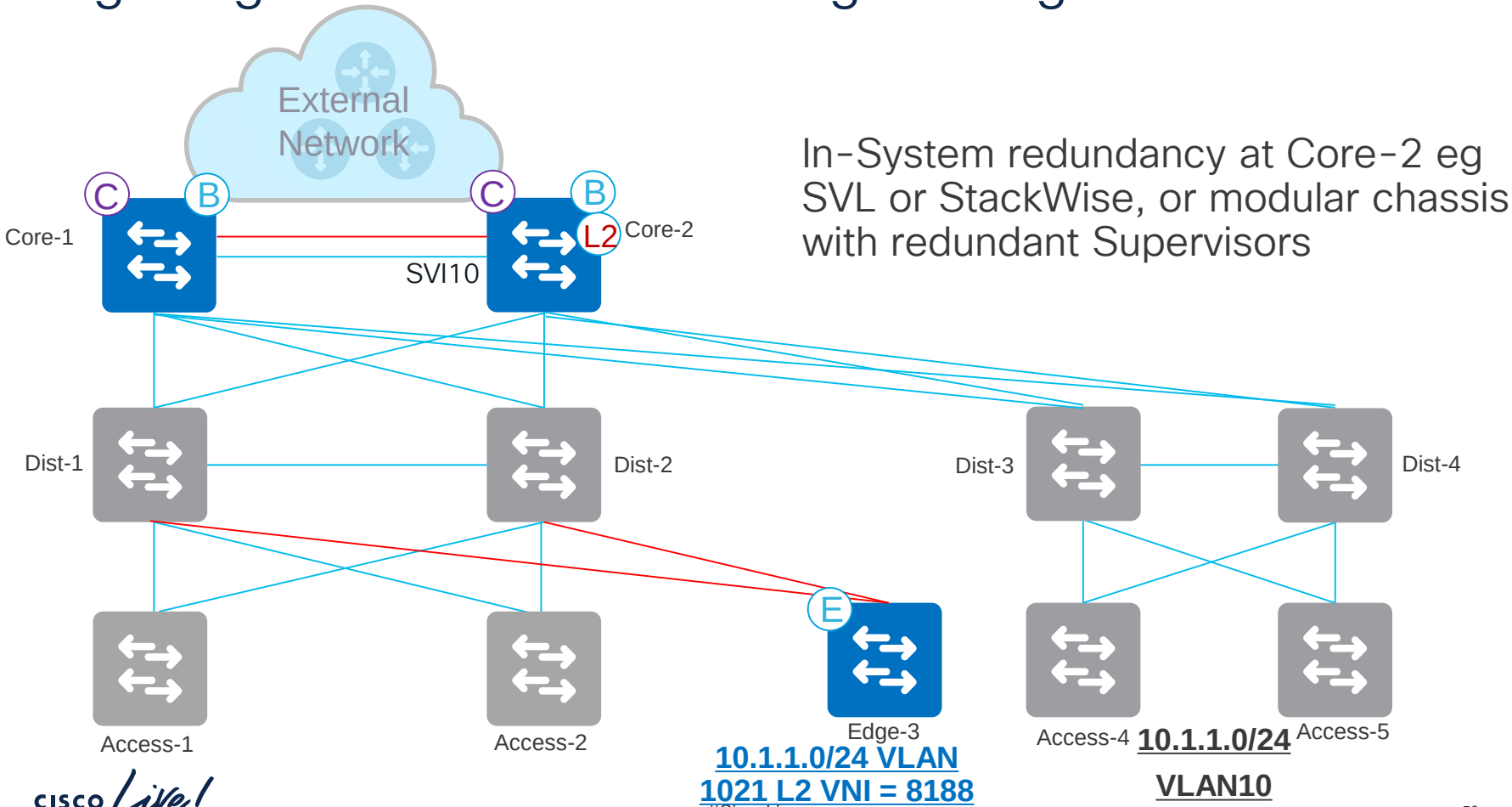



Remove SVI 10 from Core-1 and Core-2

Configure L2 Handoff at Core-2

Map 10.1.1.0/24 to VLAN10 in the L2 handoff details on Core-2 – this will map VLAN10 to L2 VNID 8188

# Migrating to SD-Access retaining existing subnets




In-System redundancy at Core-2 eg SVL or StackWise, or modular chassis with redundant Supervisors

# Layer-2 Border Scale

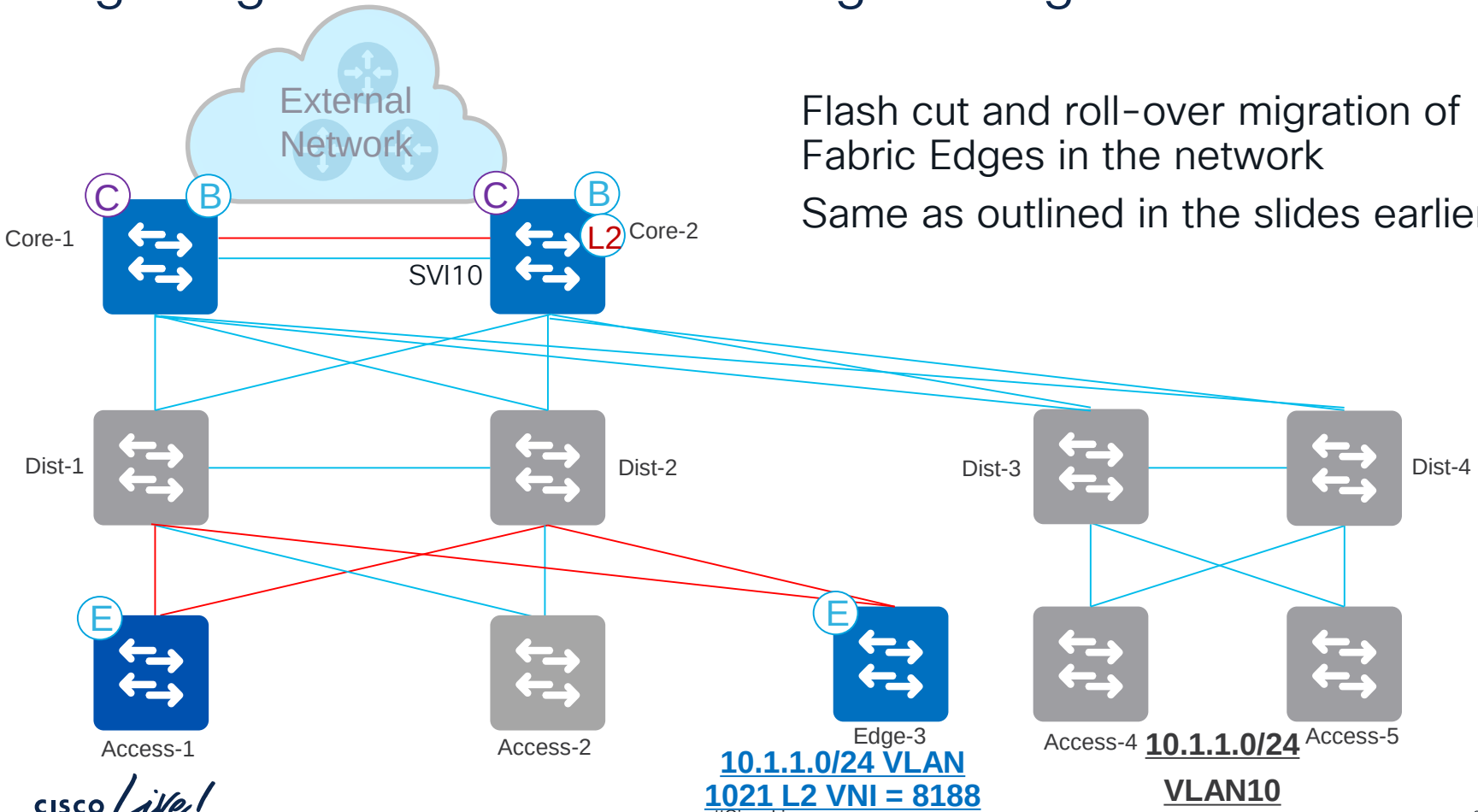
**Table 9. Cisco SD-Access Layer-2 handoff border node scale considerations**

| Cisco SD-Access Layer-2 handoff border node scale considerations | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Family** | **Cisco Catalyst** | | | | | | | | | | | **Nexus** | **ASR 1000, 4000 Series ISR** | |
| **Device** | **3850** | **6800** | **9300/L** | **9300X** | **9400** | **9400X** | **9500** | **9500H** | **9500X** | **9600** | **9600X** | **7700** | **8 GB RAM** | |
| **Endpoints** | Supported | Supported | 8,000 | 32,000 | 16,000 | 100,000 | 16,000 | 32,000 | 256,000 | 32,000 | 256,000 | NOT supported | NOT supported | N s |

Cisco DNA Center 2.3.5 Data Sheet

These numbers are the sum of the total numbers of endpoints both inside and outside the fabric site when the site has a border node with a Layer-2 handoff.

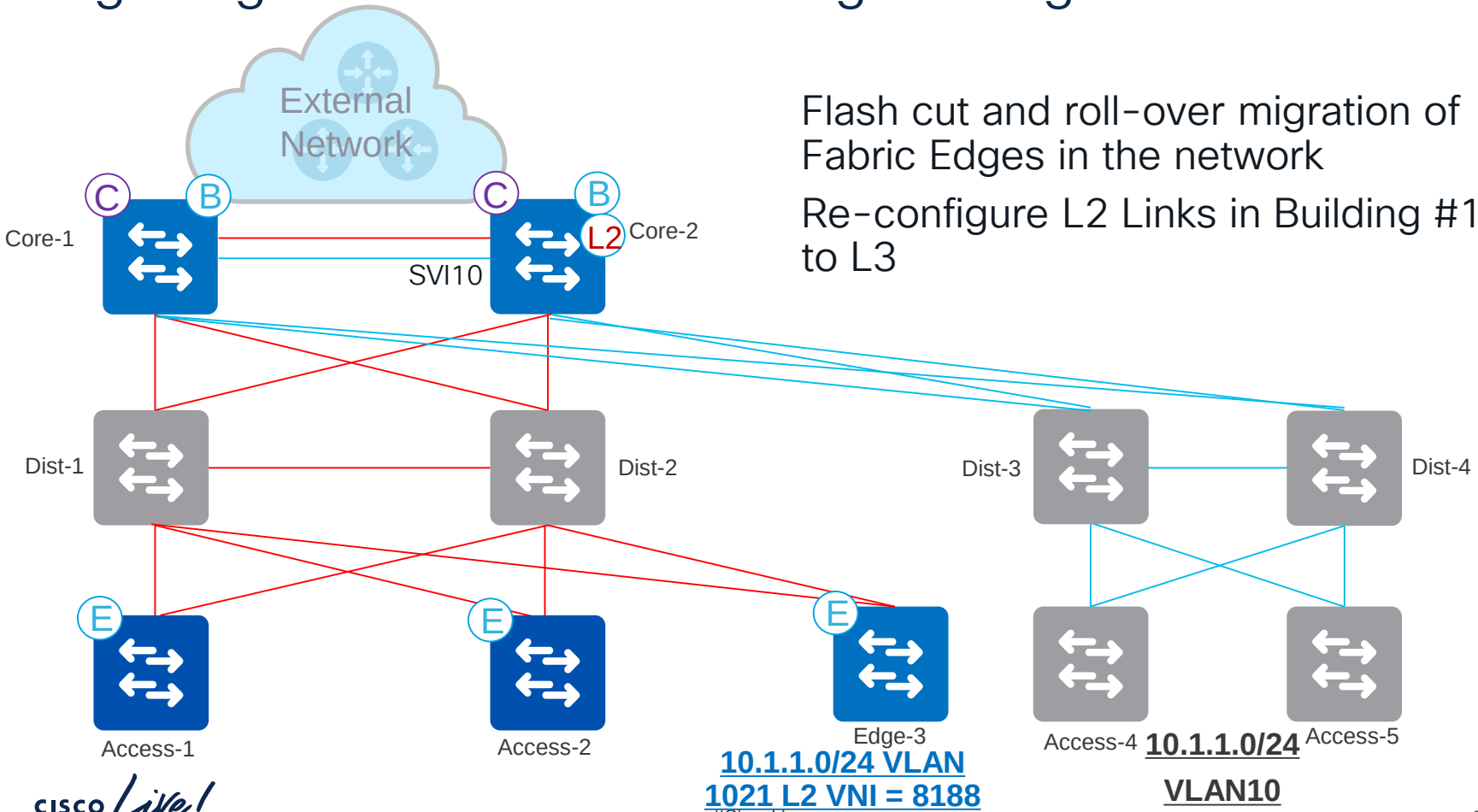
# Migrating to SD-Access retaining existing subnets




Flash cut and roll-over migration of Fabric Edges in the network

Same as outlined in the slides earlier

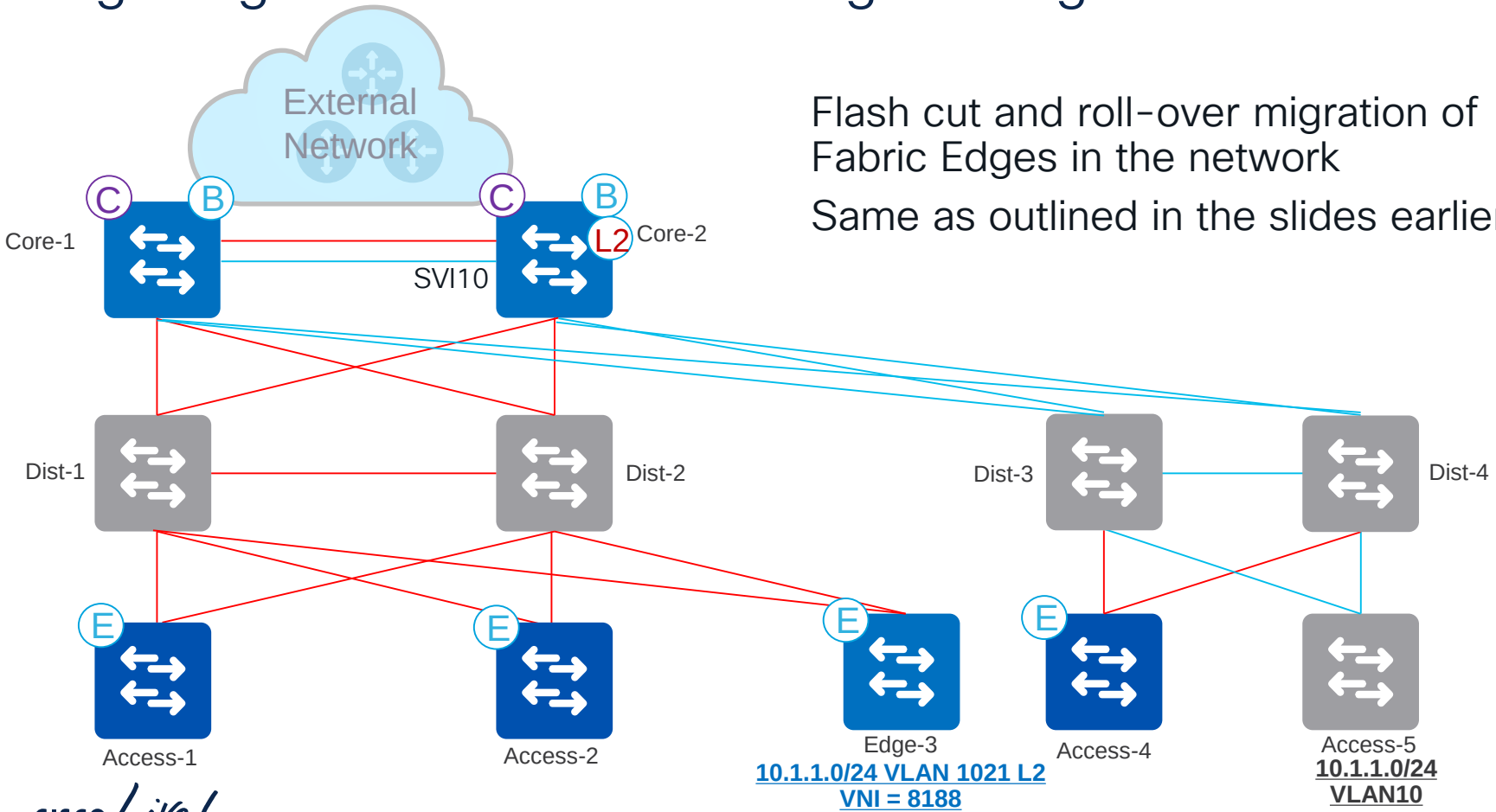
# Migrating to SD-Access retaining existing subnets




Flash cut and roll-over migration of Fabric Edges in the network

Re-configure L2 Links in Building #1 to L3

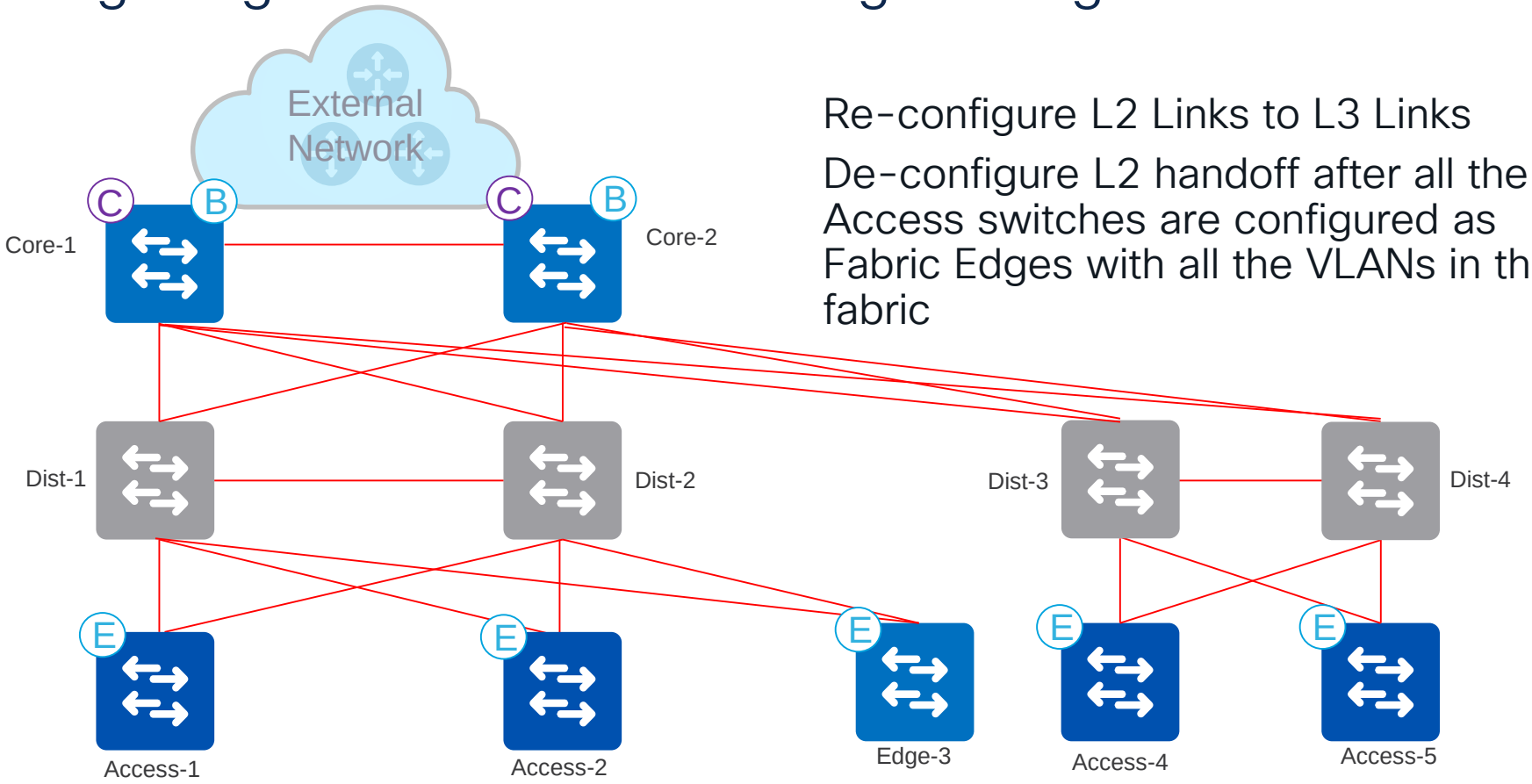
# Migrating to SD-Access retaining existing subnets




Flash cut and roll-over migration of Fabric Edges in the network

Same as outlined in the slides earlier

# Migrating to SD-Access retaining existing subnets

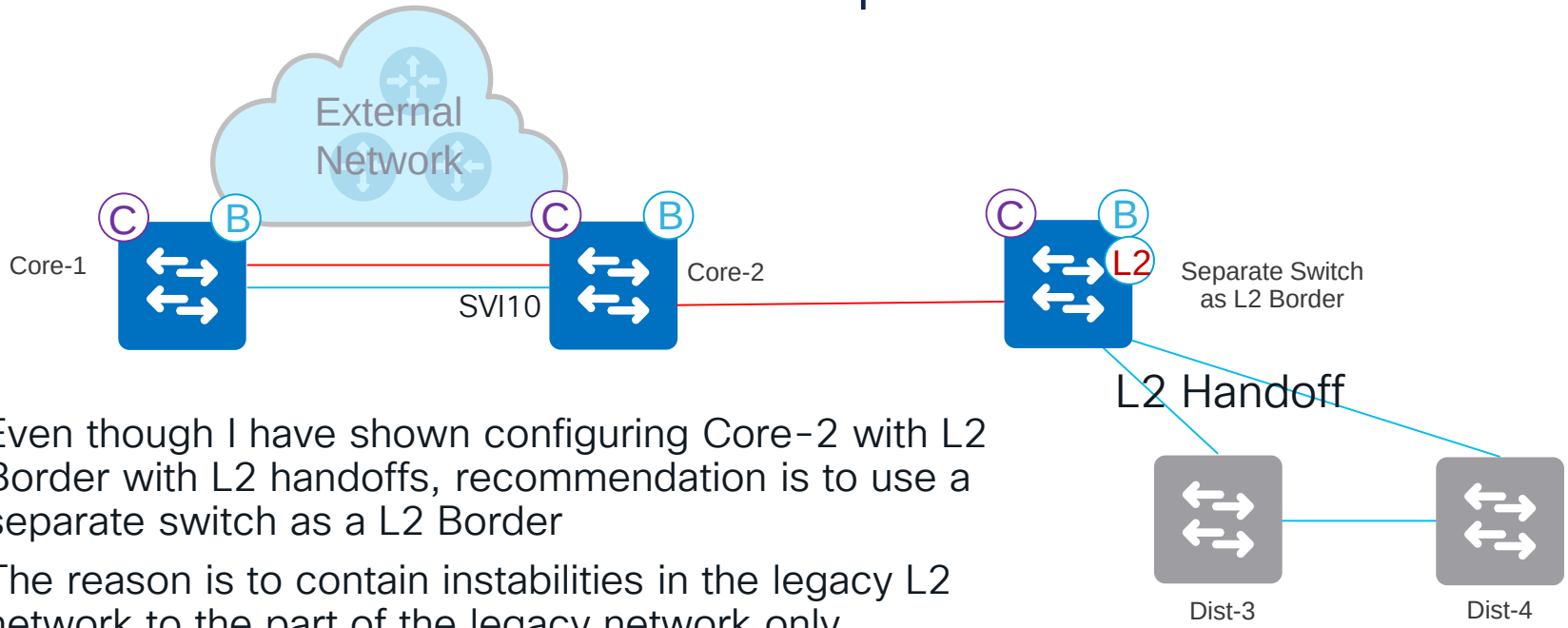



Re-configure L2 Links to L3 Links

De-configure L2 handoff after all the Access switches are configured as Fabric Edges with all the VLANs in the fabric

**10.1.1.0/24 VLAN 1021 L2 VNI = 8188**

# Recommendation to use a separate Switch as L2 Border




Even though I have shown configuring Core-2 with L2 Border with L2 handoffs, recommendation is to use a separate switch as a L2 Border

The reason is to contain instabilities in the legacy L2 network to the part of the legacy network only

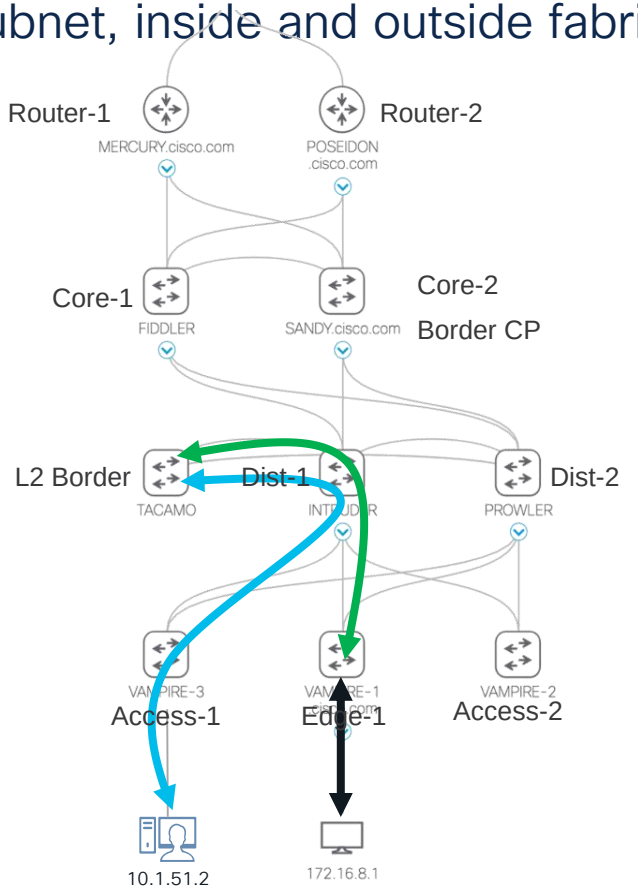
Else the Border/CP are exposed to the instabilities and may bring down both the fabric network and the legacy network

# When to use a L2 Border and Fabric Edge to connect L2 Domain

| Use L2 Border when .. | Use Fabric Edge when .. |
| --- | --- |
| There are same subnets inside the fabric and outside the fabric | Want to absorb L2 subnets within a fabric |

# Communications in SD-Access Fabric

## East-West: Hosts in same subnet, inside and outside fabric



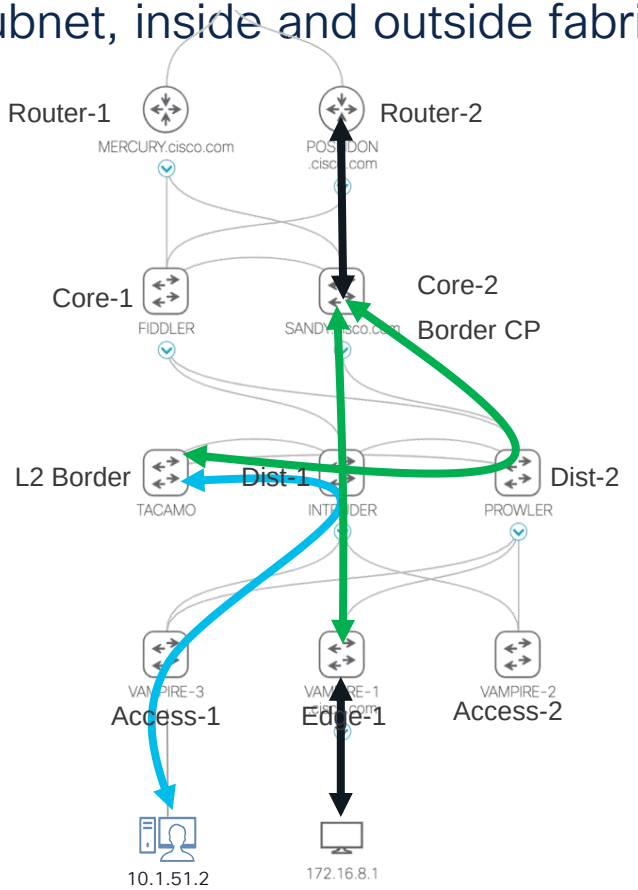

Bridged packet

Un-encapsulated packet

VXLAN encapsulated packet

# Communications in SD-Access Fabric

## East-West: Hosts in same subnet, inside and outside fabric

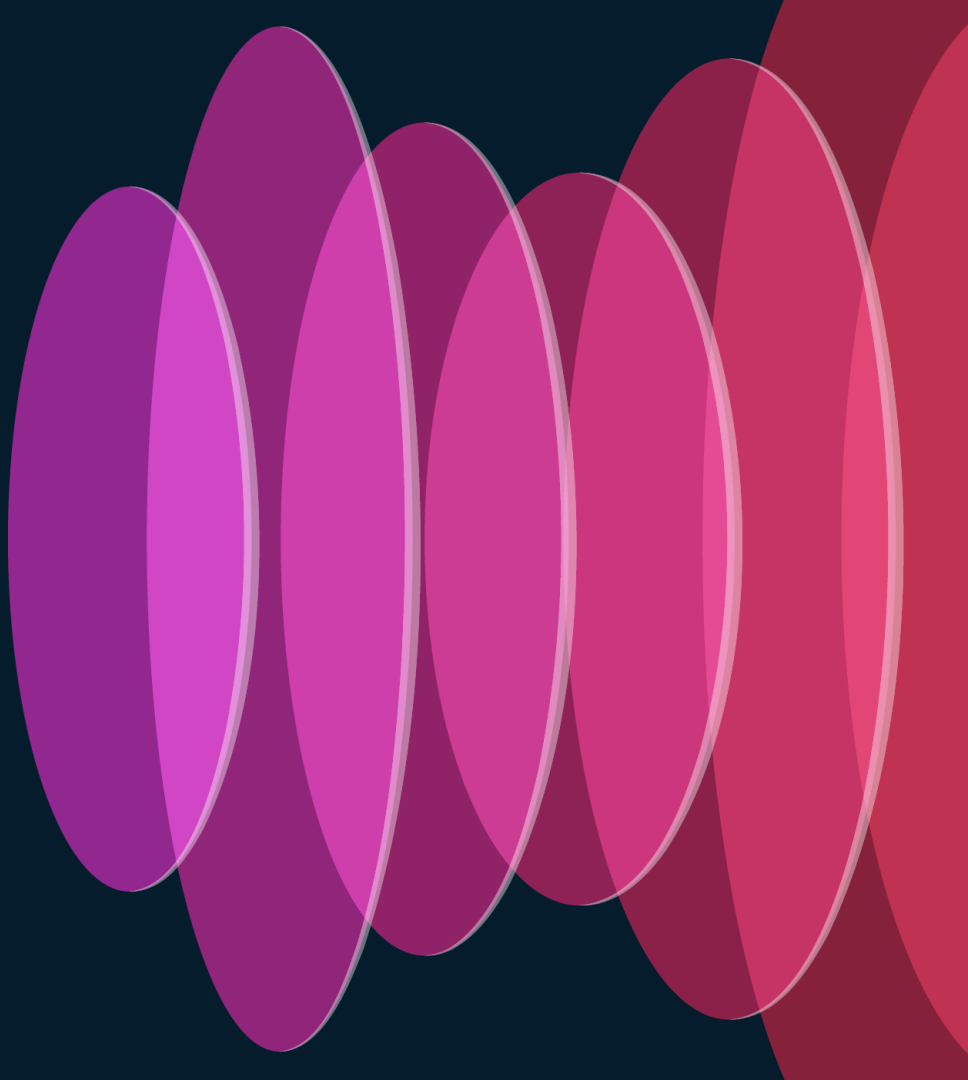



Bridged packet

Un-encapsulated packet

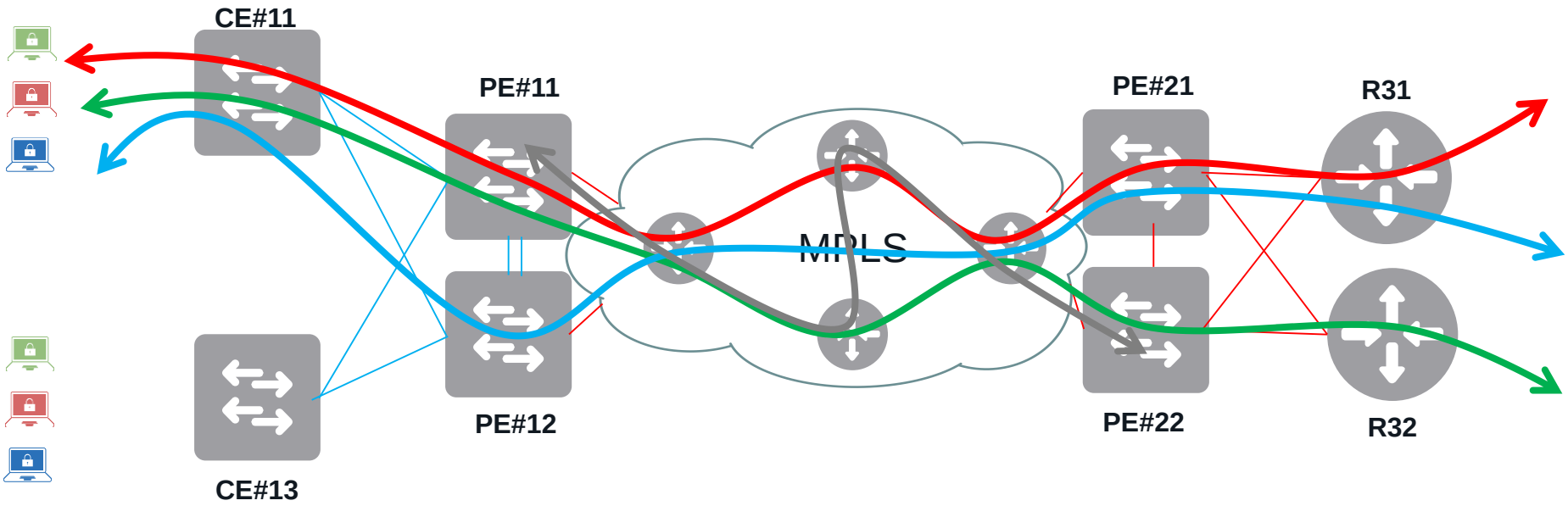
VXLAN encapsulated packet

# Migrating MPLS – VPN to SD-Access LISP

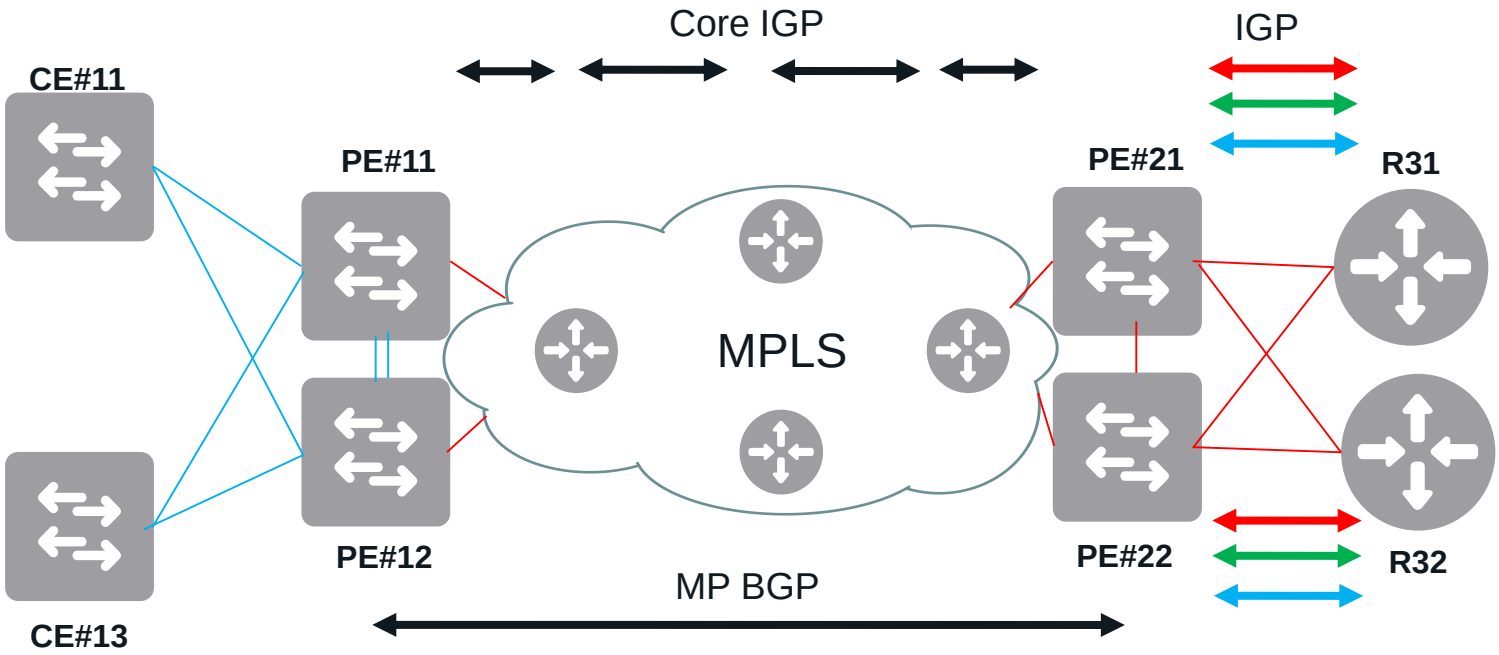


cisco Live!

# Existing Network with MPLS VPN



# IGP Design In The Existing Network



# Two Options to migrate

- Use new switches as fabric nodes – separate than MPLS nodes
- Co-exist Fabric functionality on MPLS PE nodes
- The above is relevant in Layer-2 designs where Access switches (to which endpoints connect) are Layer-2 and Layer-3 interfaces are on the MPLS PE nodes.

# Recommendations

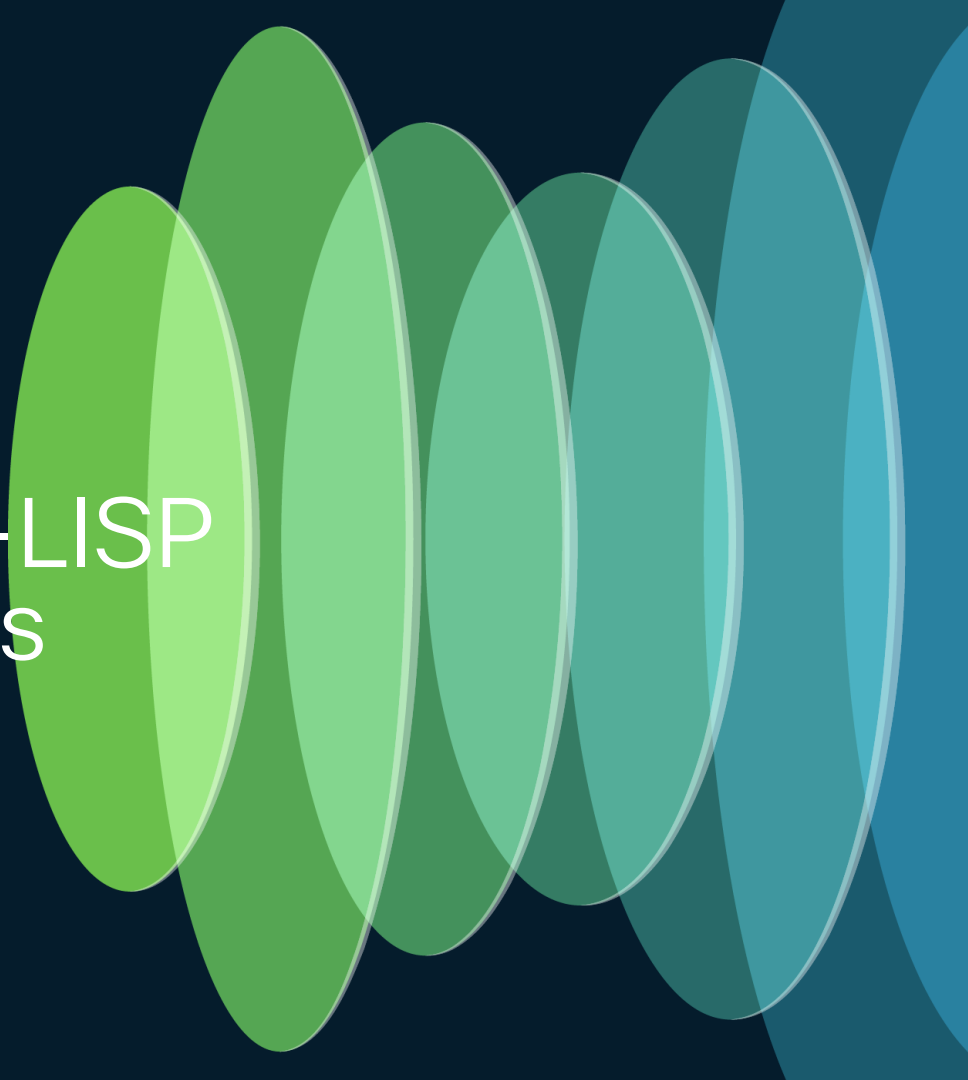
- Use different VRFs for MPLS VPN and LISP VXLAN fabric
- Route-leak external to fabric preferably on a firewall or upstream switch/router
- Or, map the SDA-LISP VRF to the MPLS VPN VRF at upstream switch/router
- Configure a MPLS Label filter to NOT generate Labels for Loopback0 networks of LISP VXLAN Fabric nodes
- Above provides a common underlay for both LISP VXLAN and MPLS VPN

# Configure Label Filter on all PE/P nodes in MPLS network

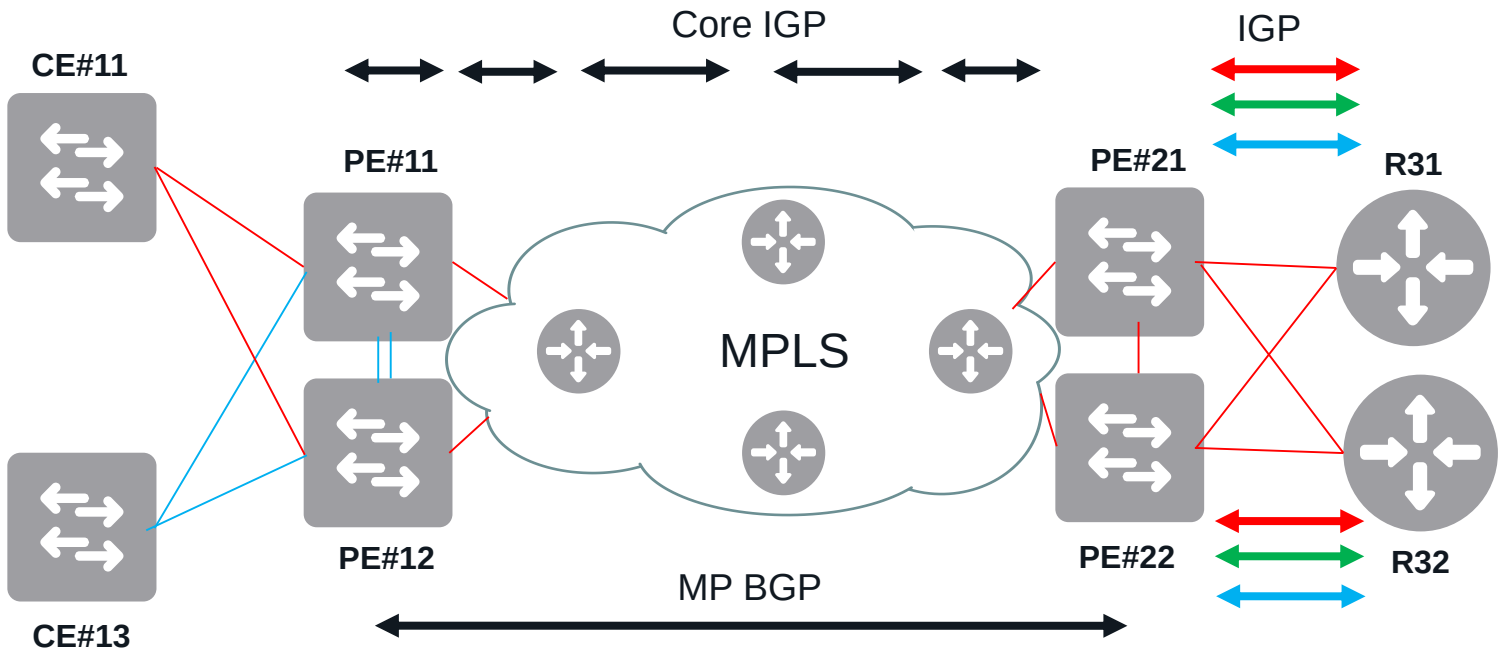
```
mpls ldp router-id Loopback1 force
ip prefix-list DenyLo0 seq 5 deny 10.1.20.5/32
ip prefix-list DenyLo0 seq 7 deny 10.1.20.3/32
ip prefix-list DenyLo0 seq 10 permit 0.0.0.0/0 le 32
!
mpls ldp label
 allocate global prefix-list DenyLo0
```

- Create an IP Prefix-List to “deny” /32 Loopback interfaces used for LISP VXLAN fabric
- This will NOT generate MPLS labels for the Loopback interfaces used for LISP VXLAN fabric
- Traffic for MPLS VPN will be label-switched through the underlay
- Traffic for LISP VXLAN fabric will be IP-switched through the underlay
- Provides a consistent underlay for both MPLS VPN and LISP VXLAN fabric

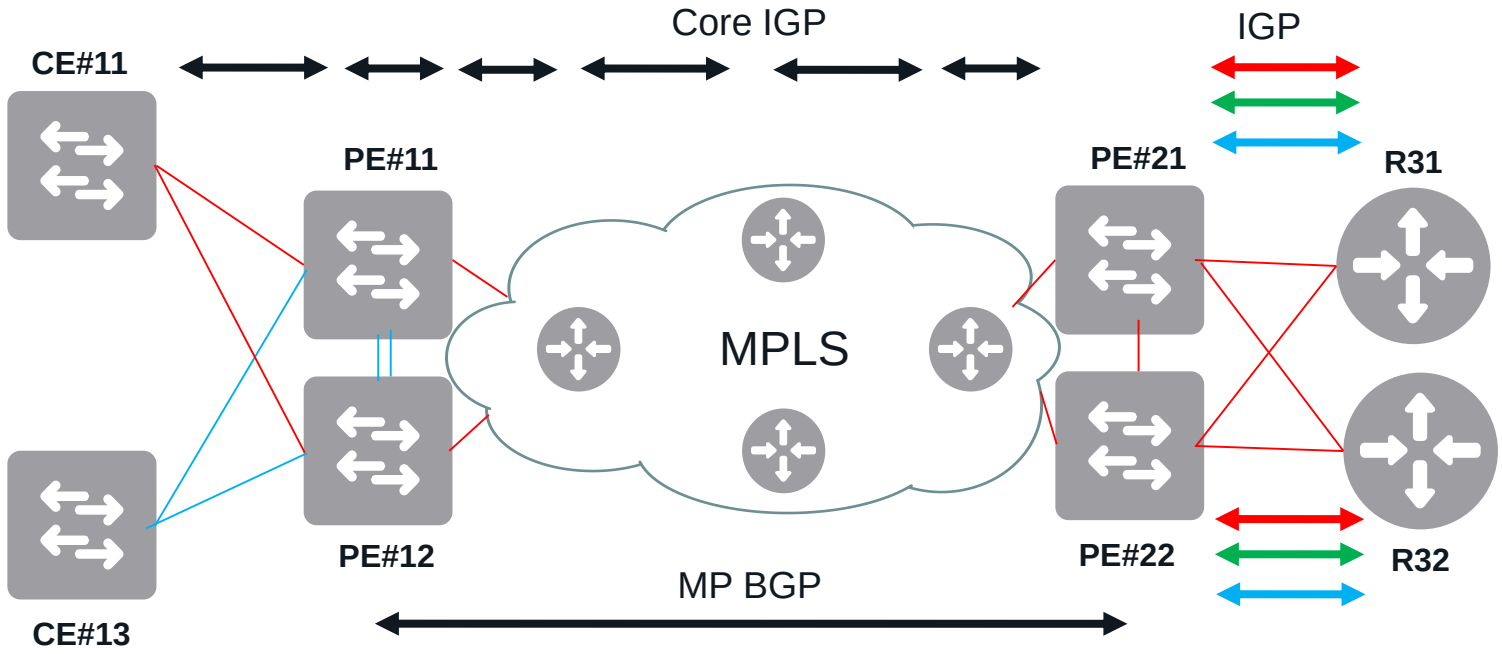
# Option 1: Separation of SDA-LISP and MPLS PE nodes



# Insert a new Switch in Access Layer



# Extend IGP to Access → Common Underlay




Intent is to make the underlay for the MPLS consistent with the underlay for the SDA-LISP overlay network

# Migrating to SDA-LISP over MPLS Core

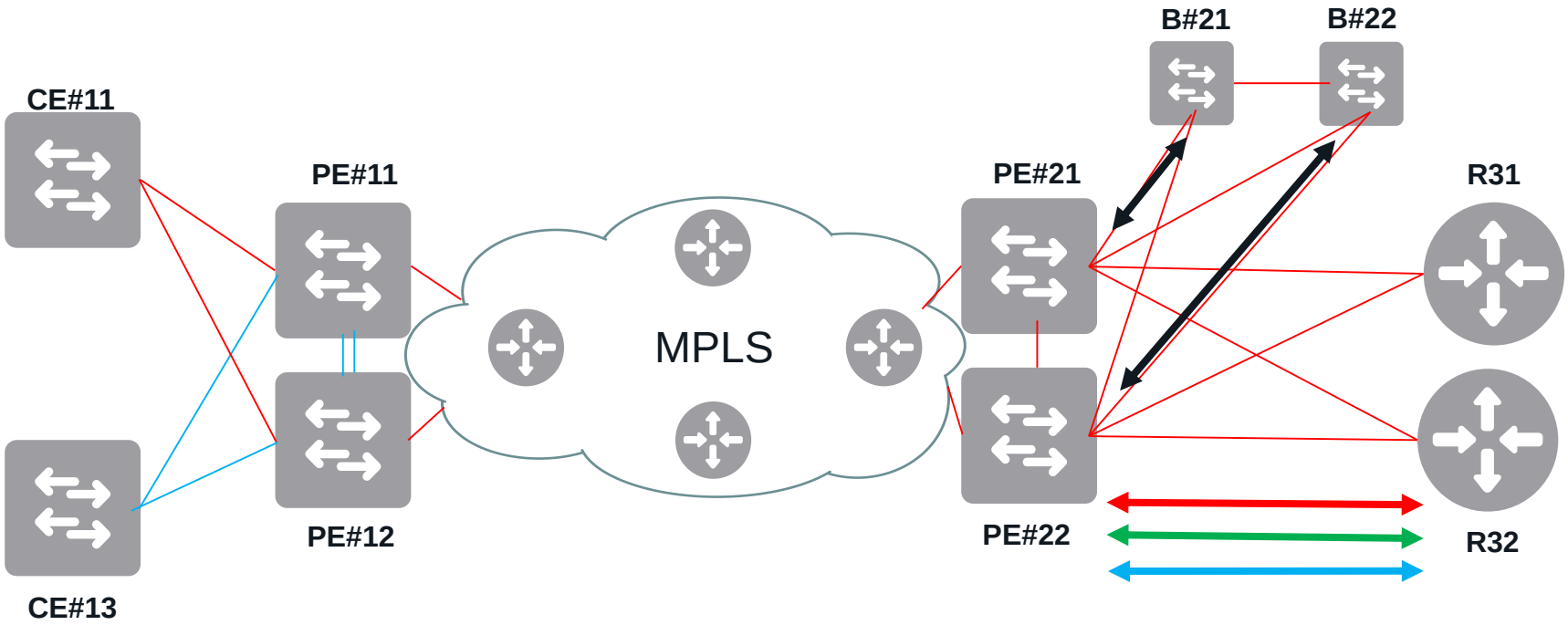
## Converting to Routed Access in first Fabric Edge

Option #1

- Re-configure link between the access to distribution as routed link
- Configure Loopback0 interface on the switch
- Configure “mtu 9100” across all switches
- Configure IGP (preferably what is used in core, OSPF) between the three switches (access, and two distribution switches)
- Advertise the Loopback0 and physical subnet into core
- Check for East-West traffic of existing network – that should not be impacted

# Insert Potential Default Border/Control Plane at PE

Option #1




Extend IGP to the new potential Border/CP nodes to make the underlay consistent for both SDA and MPLS

# Migrating to SDA-LISP over MPLS Core

## Adding Potential Border/Control Planes to existing PE switches

Option #1

- Insert potential Border/Control Plane jump-off switches off of the PE switch in existing network
- Configure routed links between the two switches and the PE switches
- Configure Loopback0 interface on the switch
- Configure “mtu 9100”
- Configure IGP (preferably what is used in core, OSPF) between the four switches (access, and two distribution switches)
- Advertise the Loopback0 and physical subnet into core – Also update ip prefix-list to not generate LDP labels for this loopback
- Check for East-West traffic of existing network – that should not be impacted

# Configure Label Filter on all PE/P nodes in MPLS network

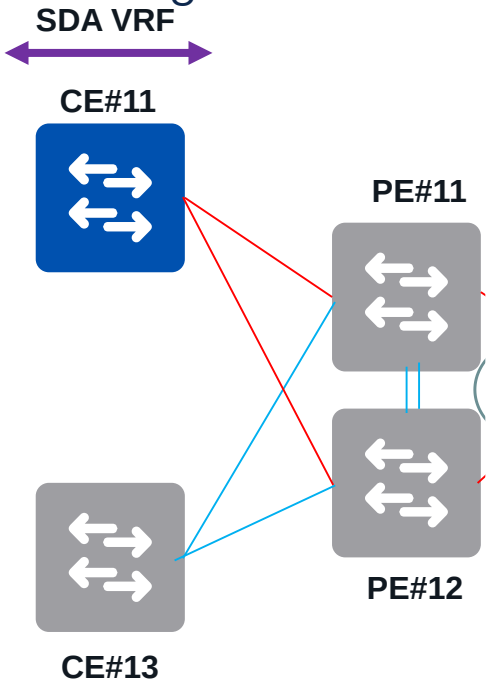
```
mpls ldp router-id Loopback1 force
ip prefix-list DenyLo0 seq 5 deny 10.1.20.5/32
ip prefix-list DenyLo0 seq 7 deny 10.1.20.3/32
ip prefix-list DenyLo0 seq 10 permit 0.0.0.0/0 le 32
!
mpls ldp label
 allocate global prefix-list DenyLo0
```

- Create an IP Prefix-List to “deny” /32 Loopback interfaces used for LISP VXLAN fabric
- This will NOT generate MPLS labels for the Loopback interfaces used for LISP VXLAN fabric
- Traffic for MPLS VPN will be label-switched through the underlay
- Traffic for LISP VXLAN fabric will be IP-switched through the underlay
- Provides a consistent underlay for both MPLS VPN and LISP VXLAN fabric

# Recommendations for Fabric Edge Placement Choice

## Configure Fabric Edge functionality

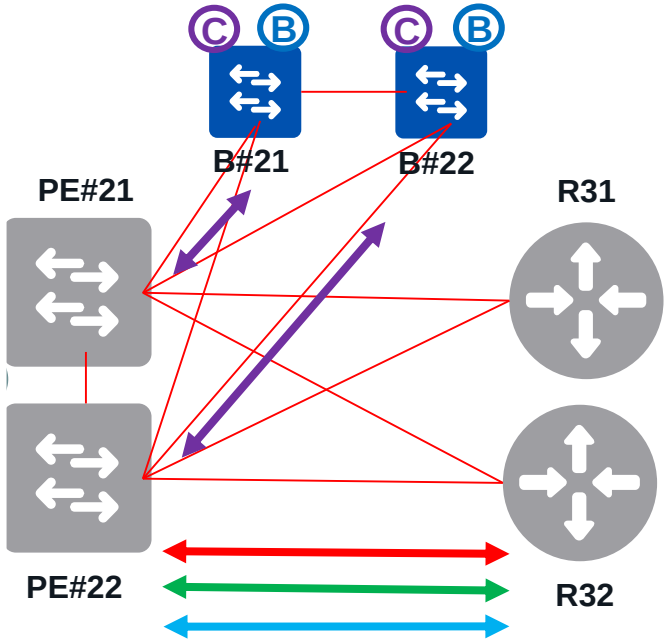
Option #1




**Configure the new switch as the Fabric Edge with Routed Access to Distribution block**

# Recommendations for Border/CP Design Choic
## Configure Border/CP functionality

Option #1




**Either map new VRF 1:1 between MPLS VPN and SDA,**
**OR**
**Create new VRF for SDA-LISP and manage inter-VRF comms at Firewall**

# Migrating to SDA-LISP over MPLS Core

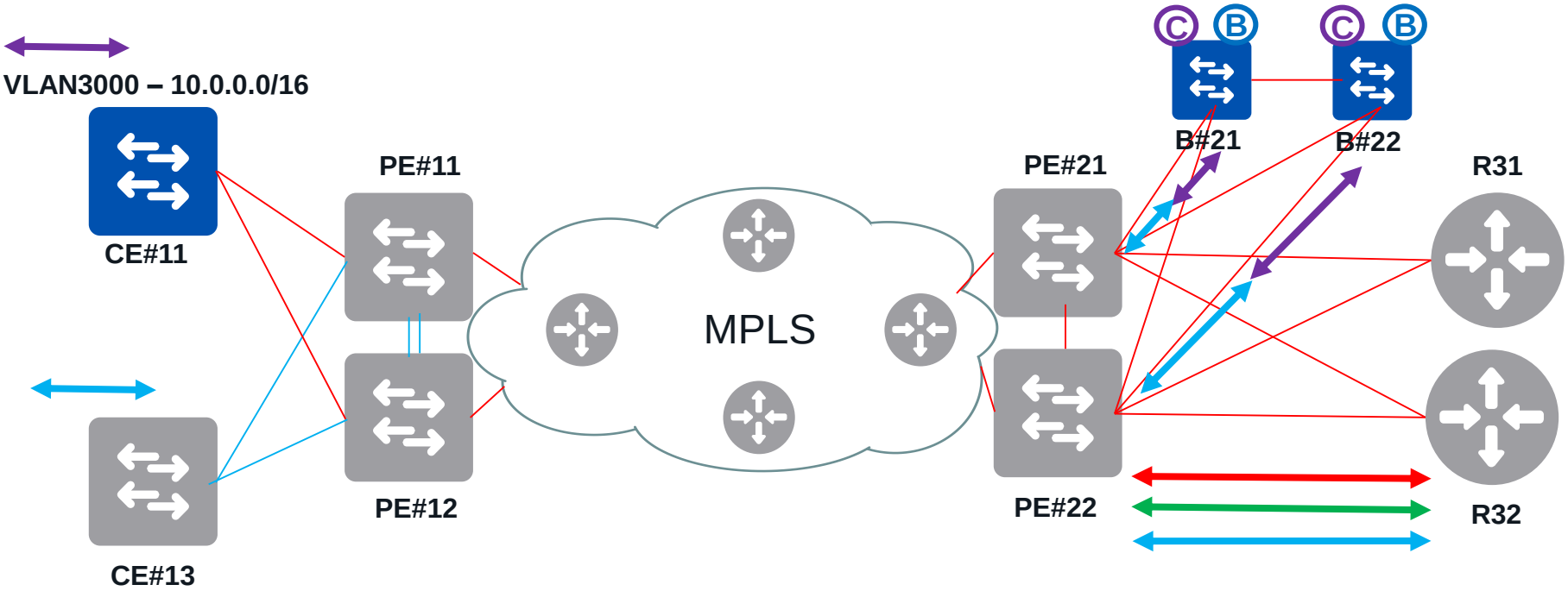
## Provision Fabric on Edge and Default Border/Control Plane

Option #1

- Using Catalyst Center, configure the access switch to be a fabric edge, while configuring the jump-off switches as default border and control plane nodes.
- Check for E-W, N-S traffic of existing network – that should not be impacted

# Provision IP Pool using new subnet

Option #1



# Migrating to SDA-LISP over MPLS Core

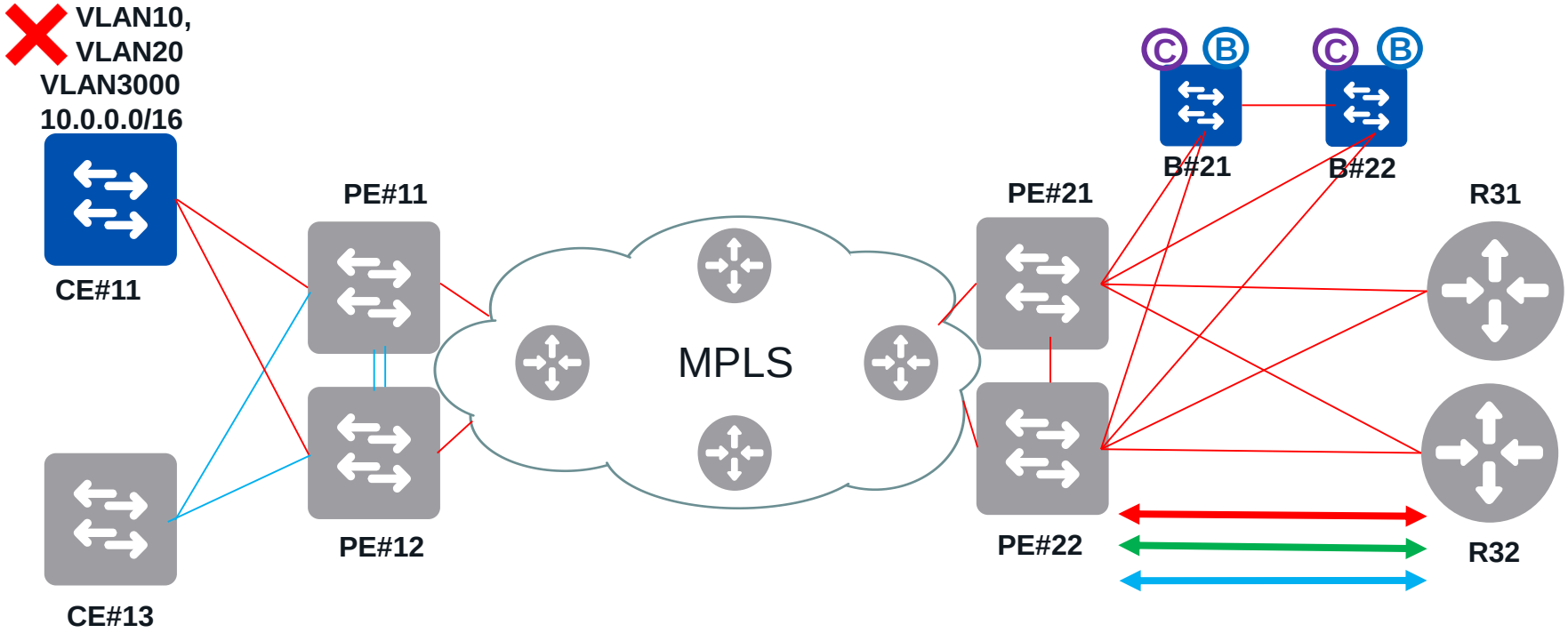
## Provision IP Pool with new subnet

Option #1

- Using Catalyst Center, provision an IP Pool using new subnet in new Purple VRF
- Setup external connectivity on the Borders – mapping SDA-LISP VRFs into MPLS VPN VRF to route this prefix externally
- In the above example, I have the SDA-LISP VRF mapped into the Blue VRF at the PE connecting into the SDA Border
- Fabric traffic will come into the Edge, go to the Border, and then from the Border over to the Blue VRF into MPLS VPN and either go to the access switch in Blue VRF at the left bottom of the picture denoted by the Blue arrow

# Conversion of Fabric Edge to full Routed Access

Option #1



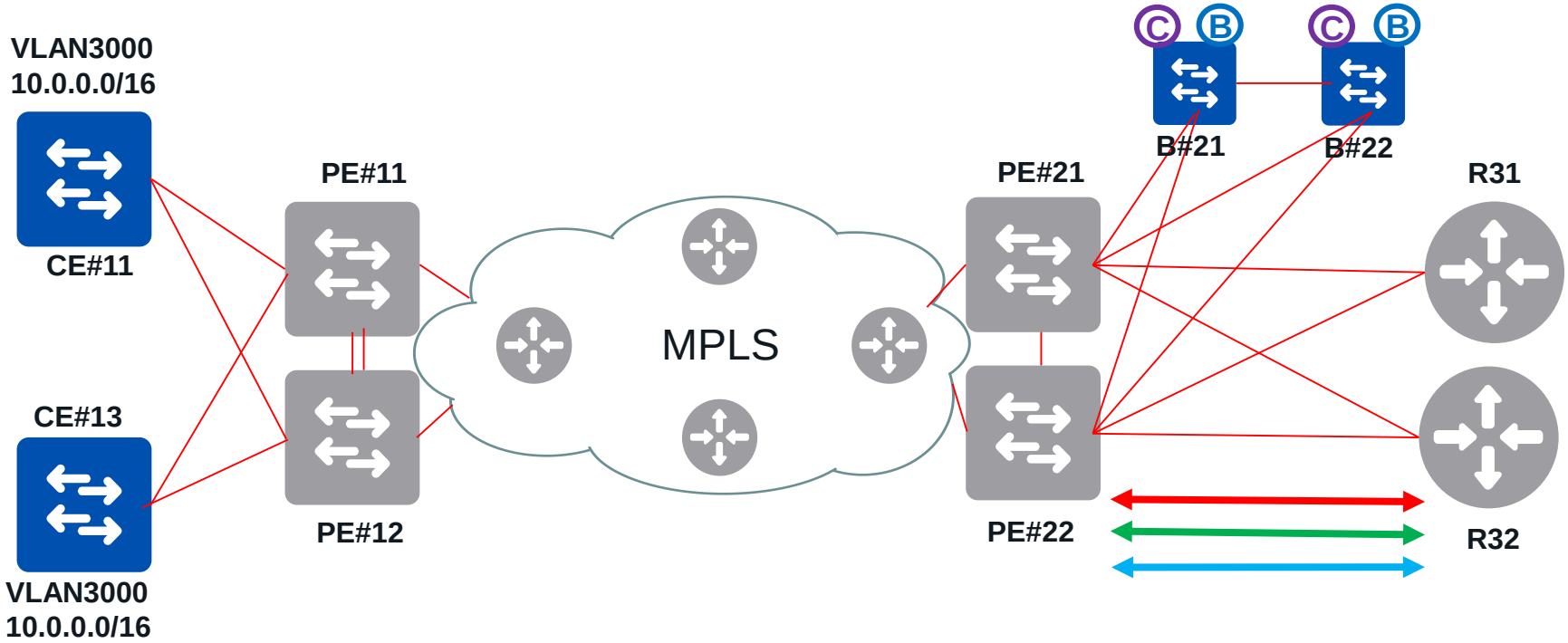
# Migrating to SDA-LISP over MPLS Core
## Converting to full Routed Access

Option #1

- Use Catalyst Center to provision multiple IP Pools in fabric
- Setup external connectivity on the Borders – mapping SDA-LISP VRFs into MPLS VPN VRF to route this prefix externally
- Flash-cut or install a new switch in the access layer.
- Move/Configure the links to routed access from access to distribution.

# Incrementally add additional Fabric Edges

Option #1



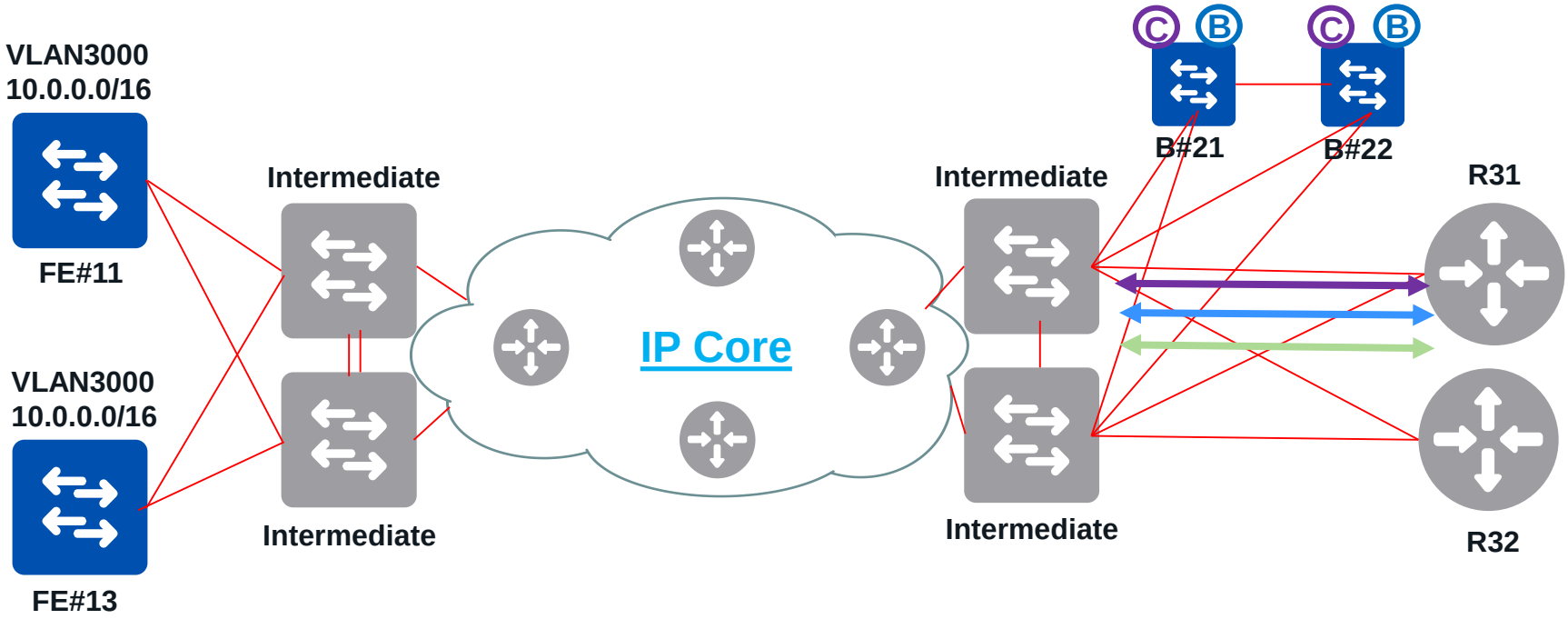
# Migrating to SDA-LISP over MPLS Core
## Incremental Fabric Edge provisioning

Option #1

- Use Catalyst Center to provision additional fabric edges in the network
- Repeat the same steps from before converting L2 Access to routed access and eventual fabric edge conversion

# Moving away from MPLS to an IP Core

Option #1

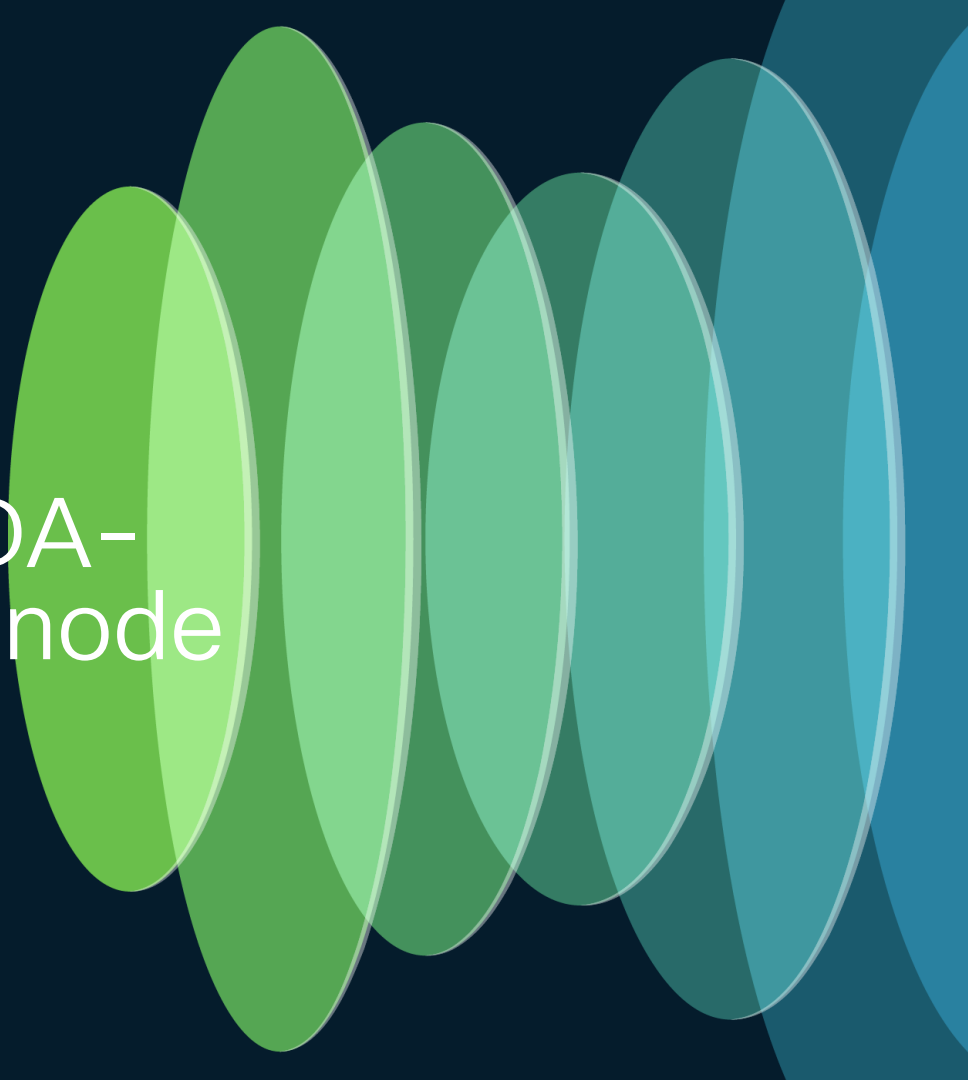


# Migrating to SDA-LISP over MPLS Core
## Moving to an IP Core

Option #1

- Once all the prefixes are moved away from MPLS VPN and into SD-Access, there will not be any need to retain MPLS VPN configurations in the network
- Remove MPLS VPN and eventually MPLS from the network core
- Moving to a IP Core and classic Cisco SD-Access-LISP solution

# Option 2: Co-Existence of SDA-LISP and MPLS PE node



# Co-existing MPLS PE and SDA-LISP fabric node
## Considerations

Option #2

- Manage scale of hardware entries on that device
- On the Cat9K, indirect prefixes use TCAM, /32 entries use HASH table
- In the case, where L3 boundary is at CE, only TCAM will be used for indirect prefixes – and if the L3 boundary is at the PE /32 entries are populated in HASH table which is a separate resource for storing hardware entries
- In the mixed case, it is a mix of indirect and host entries and hence TCAM and HASH table would be utilized
- In any case, there is no infinite scale so as it applies to any scenario, scale has to be managed – it is a special consideration hence the call-out

# Co-existing MPLS PE and SDA-LISP fabric nod
## Catalyst Center considerations

Option #2

- Use different VRFs for MPLS VPN and SDA-LISP VN – the reason being Catalyst Center will deploy different configurations for SDA-LISP VN and not touch existing VRF configurations needed for MPLS VPN
- When selecting Dot1x authentication parameters, start with “No Authentication” – so Catalyst Center does not overwrite/add existing downstream/edge port configuration with dot1x authentication commands
- Catalyst Center will modify/overwrite downstream/edge port configurations that are in “switchport dynamic auto” mode – or in other words – are in default-interface configuration
- If downstream/edge ports are already configured with “switchport mode access/trunk” or are routed ports, Catalyst Center will NOT modify any configuration on those ports.

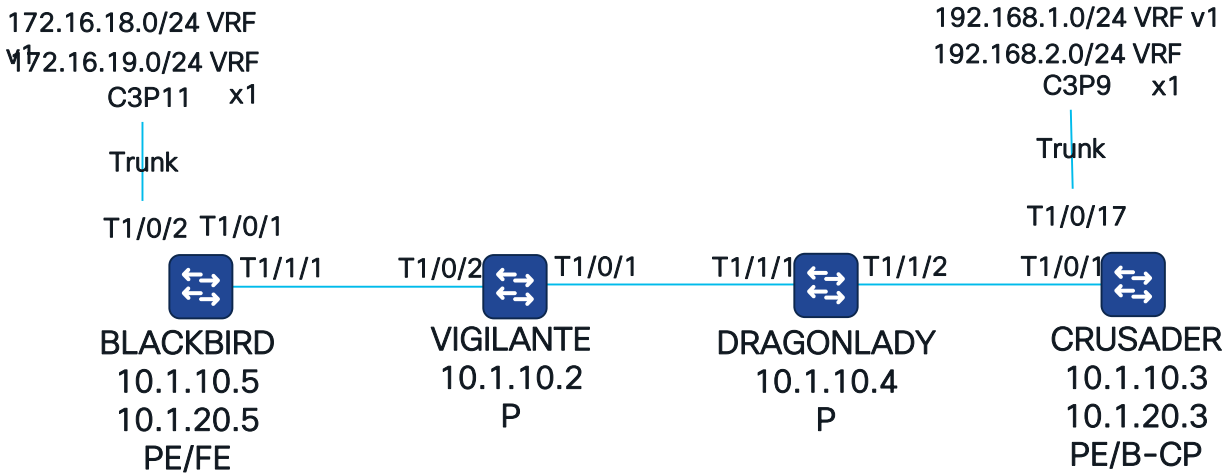
# Recommendations

Option #2

- Use different VRFs for MPLS VPN and LISP VXLAN fabric
- Route-leak external to fabric preferably on a firewall or upstream switch/router
- Configure a MPLS Label filter to NOT generate Labels for Loopback0 networks of LISP VXLAN Fabric nodes

# Topology

Option #2

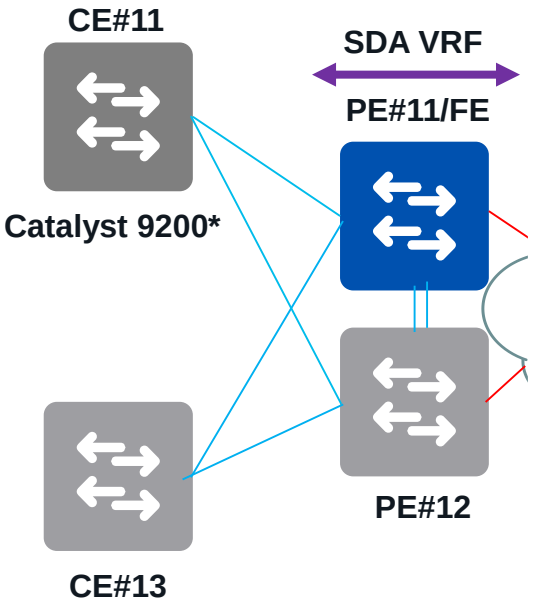



Loopback1 – 10.1.10.5 for MPLS VPN  VRF v1 – MPLS VPN
Loopback0 – 10.1.20.5 for LISP VXLAN  VRF x1 – LISP VXLAN VN

# Recommendations for Fabric Edge Placement Choice

## Co-existing Fabric Edge functionality with MPLS PE functionality

Option #2




**If access switch is a Catalyst 9200-class of device, then the recommendation is to keep it as a L2-switch and NOT make it as a Fabric Edge. Instead make the existing PE in addition to act as a FE**

# Different Loopbacks on PE/FE

Option #2

```
BLACKBIRD#s int lo1
Building configuration...
Current configuration : 100 bytes
!
interface Loopback1
 description Loopback for MPLS VPN
 ip address 10.1.10.5 255.255.255.255
end
```

```
BLACKBIRD#s int lo0
Building configuration...
Current configuration : 109 bytes
!
interface Loopback0
 description Loopback for LISP VXLAN fabric
 ip address 10.1.20.5 255.255.255.255
end
```

Use Loopback0 specifically for SDA-LISP since Cisco Catalyst Center uses Loopback0 to automate configuration

In case using Lo0 for MPLS VPN, create Lo1 using the same IP and use “mpls ldp router-id loopback1 force”

# Different Loopbacks on PE/Border-CP

Option #2

```
CRUSADER#s int lo1
Building configuration...
Current configuration : 100 bytes
!
interface Loopback1
 description Loopback for MPLS VPN
 ip address 10.1.10.3 255.255.255.255
end
```

```
CRUSADER#s int lo0
Building configuration...
Current configuration : 109 bytes
!
interface Loopback0
 description Loopback for LISP VXLAN fabric
 ip address 10.1.20.3 255.255.255.255
end
```

Use Loopback0 specifically for SDA-LISP since Cisco DNAC uses Loopback0 to automate configuration

In case using Lo0 for MPLS VPN, create Lo1 and use “mpls ldp router-id loopback1 force”

# Configure Label Filter on all PE/P nodes in MPLS network

```
mpls ldp router-id Loopback1 force
ip prefix-list DenyLo0 seq 5 deny 10.1.20.5/32
ip prefix-list DenyLo0 seq 7 deny 10.1.20.3/32
ip prefix-list DenyLo0 seq 10 permit 0.0.0.0/0 le 32
!
mpls ldp label
 allocate global prefix-list DenyLo0
```

- Create an IP Prefix-List to “deny” /32 Loopback interfaces used for LISP VXLAN fabric
- This will NOT generate MPLS labels for the Loopback interfaces used for LISP VXLAN fabric
- Traffic for MPLS VPN will be label-switched through the underlay
- Traffic for LISP VXLAN fabric will be IP-switched through the underlay
- Provides a consistent underlay for both MPLS VPN and LISP VXLAN fabric

# Result of Label Filter on all PE/P nodes in MPLS network

Option #2

BLACKBIRD#sh mpls forwarding

| Local Label | Outgoing Label | Prefix or Tunnel Id | Bytes Label Switched | Outgoing interface | Next Hop |
|---|---|---|---|---|---|
| 16 | Pop Label | 10.1.10.2/32 | 0 | Te1/1/1 | 10.1.8.254 |
| 17 | Pop Label | 10.1.7.0/24 | 0 | Te1/1/1 | 10.1.8.254 |
| 18 | 18 | 10.1.10.4/32 | 0 | Te1/1/1 | 10.1.8.254 |
| 19 | 19 | 10.1.9.0/24 | 0 | Te1/1/1 | 10.1.8.254 |
| 20 | 21 | 10.1.10.3/32 | 78559297200 | Te1/1/1 | 10.1.8.254 |
| 21 | No Label | IPv4 VRF[V] | 0 | aggregate/v1 | |

VIGILANTE#sh mpls forwarding

| Local Label | Outgoing Label | Prefix or Tunnel Id | Bytes Label Switched | Outgoing interface | Next Hop |
|---|---|---|---|---|---|
| 18 | Pop Label | 10.1.10.4/32 | 0 | Te1/0/1 | 10.1.7.253 |
| 19 | Pop Label | 10.1.9.0/24 | 0 | Te1/0/1 | 10.1.7.253 |
| 21 | 21 | 10.1.10.3/32 | 393499484482 | Te1/0/1 | 10.1.7.253 |
| 23 | Pop Label | 10.1.10.5/32 | 735631 | Te1/0/2 | 10.1.8.253 |

There are no labels generated for 10.1.20.3/32 and 10.1.20.5/32 above which are the Loopback interfaces on PE/FE used for LISP VXLAN fabric

# Different VRFs on PE/FE

Option #2

```
BLACKBIRD#s | sec vrf defini
vrf definition v1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
  route-target export 1:1
  route-target import 1:1
 exit-address-family

vrf definition x1
 !
 address-family ipv4
 exit-address-family
```

MPLS VPN VRF v1

LISP VXLAN fabric VRF x1

# Different VRFs on PE/FE, and PE/Border-CP

Option #2

```
BLACKBIRD#s | sec vrf defini
vrf definition v1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
  route-target export 1:1
  route-target import 1:1
 exit-address-family

vrf definition x1
 !
 address-family ipv4
 exit-address-family
```

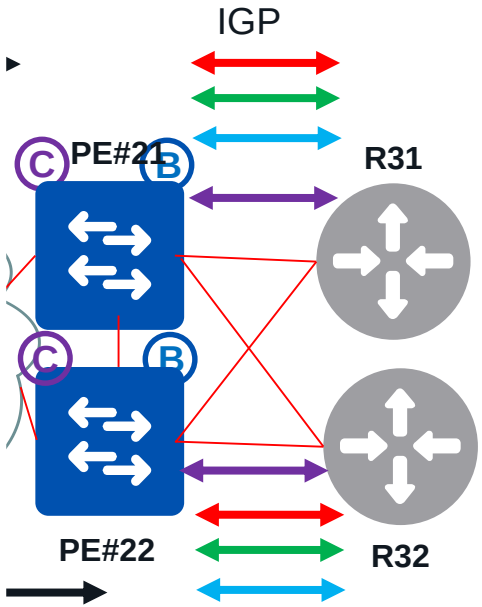
```
CRUSADER#s | sec vrf defini
vrf definition v1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
 exit-address-family

vrf definition x1
 rd 1:40
 !
 address-family ipv4
  route-target export 1:40
  route-target import 1:40
 exit-address-family
```

# Recommendations for Border/CP Design Choice

## Co-existing Border/CP along with MPLS PE functionality

Option #2




**Separate VRFs for MPLS VPN and SDA-LISP**
**Manage scale of existing MPLS VPN VRF prefixes and SDA-LISP VRF prefixes**
**Manage VRF leaking / consolidation preferably on Firewalls connected upstream**

# BLACKBIRD (PE/FE): Interface Configuration

Option #2

## Access-facing Interfaces

```
interface Vlan2
 vrf forwarding v1
 ip address 172.16.18.254 255.255.255.0
!
interface Vlan3
 mac-address 0000.0c9f.f708
 vrf forwarding x1
 ip address 172.16.19.254 255.255.255.0
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility x1-pool-1
!
interface TenGigabitEthernet1/0/2
 description Connects to Ixia C3P12
 switchport mode trunk
 device-tracking attach-policy ipdt
 spanning-tree portfast trunk
```

## Core-facing Interface

```
interface TenGigabitEthernet1/1/1
 no switchport
 ip address 10.1.8.253 255.255.255.0
 mpls ip
```

# PE MPLS VPN: BGP Configuration

Option #2

```
router bgp 1
 bgp router-id interface Loopback1
 bgp log-neighbor-changes
 neighbor 10.1.10.3 remote-as 1
 neighbor 10.1.10.3 update-source Loopback1
 !
 address-family vpnv4
  neighbor 10.1.10.3 activate
  neighbor 10.1.10.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf v1
  redistribute connected
 exit-address-family
```

```
router bgp 1
 bgp router-id interface Loopback1
 bgp log-neighbor-changes
 neighbor 10.1.10.5 remote-as 1
 neighbor 10.1.10.5 update-source Loopback1
 !
 address-family vpnv4
  neighbor 10.1.10.5 activate
  neighbor 10.1.10.5 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf v1
  redistribute connected
 exit-address-family
```

# CEF Programming on PE/FE and PE/Border-CP node

Option #2

```
BLACKBIRD#sh ip cef vrf v1 192.168.1.0
192.168.1.0/24
  nexthop 10.1.8.254 TenGigabitEthernet1/1/1 label 21-(local:20) 22

BLACKBIRD#sh ip cef vrf x1 192.168.2.0
0.0.0.0/0
  nexthop 10.1.20.3 LISP0.4120
```

```
CRUSADER#sh ip cef vrf v1 172.16.18.1
172.16.18.0/24
  nexthop 10.1.9.253 TenGigabitEthernet1/0/1 label 24-(local:25) 21

CRUSADER#sh ip cef vrf x1 172.16.19.1
172.16.19.1/32
  nexthop 10.1.20.5 LISP0.4120
```

Option #2

# MPLS VPN Packet Capture on P node

```
VIGILANTE#sh mon cap file flash:b.pcap det
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on
   [Protocols in frame: eth:ethertype:mpls:ip:tcp]
Ethernet II, Src: 50:61:bf:bf:85:46 Dst: 50:61:bf:28:d9:56
   Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header, Label: 21, Exp: 1, S: 0, TTL: 63
   0000 0000 0000 0001 0101 .... .... .... = MPLS Label: 21
   .... .... .... .... .... 001. .... .... = MPLS Experimental Bits: 1
   .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
   .... .... .... .... .... .... 0011 1111 = MPLS TTL: 63
MultiProtocol Label Switching Header, Label: 22, Exp: 1, S: 1, TTL: 63
   0000 0000 0000 0001 0110 .... .... .... = MPLS Label: 22
   .... .... .... .... .... 001. .... .... = MPLS Experimental Bits: 1
   .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
   .... .... .... .... .... .... 0011 1111 = MPLS TTL: 63
Internet Protocol Version 4, Src: 172.16.18.1, Dst: 192.168.1.1
   0100 .... = Version: 4
Transmission Control Protocol, Src Port: 24000, Dst Port: 80, Seq: 1, Len: 6
   Source Port: 24000
   Destination Port: 80
```

# BLACKBIRD: LISP FE Configuration

Option #2

```
router lisp
 domain-id 10
 locator-table default
 locator-set RLOC_BB
  IPv4-interface Loopback0 priority 10 weight 10
  exit-locator-set
 !
 locator default-set RLOC_BB
 service ipv4
  encapsulation vxlan
  itr map-resolver 10.1.20.3
  etr map-server 10.1.20.3 key 7 14141B180F0B
  etr map-server 10.1.20.3 proxy-reply
  etr
  sgt distribution
  sgt
  proxy-itr 10.1.20.5
  exit-service-ipv4
 !
 service ethernet
  itr map-resolver 10.1.20.3
  itr
  etr map-server 10.1.20.3 key 7 05080F1C2243
  etr map-server 10.1.20.3 proxy-reply
  etr
  exit-service-ethernet
 !
 instance-id 4120
  remote-rloc-probe on-route-change
  dynamic-eid x1-pool-1
   database-mapping 172.16.19.0/24 locator-set RLOC_BB
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf x1
   map-cache 0.0.0.0/0 map-request
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 8120
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 3
   database-mapping mac locator-set RLOC_BB
   exit-service-ethernet
  !
  exit-instance-id
 !
 ipv4 locator reachability minimum-mask-length 32
 ipv4 source-locator Loopback0
 exit-router-lisp
```

# CRUSADER: LISP Border Configuration

Option #2

```
CRUSADER#srl
router lisp
 domain-id 10
 multihoming-id 10
 locator-table default
 locator-set Defaultetrset
  IPv4-interface Loopback0 priority 10 weight 10
  exit-locator-set
 !
 locator-set RLOC_CR
  IPv4-interface Loopback0 priority 10 weight 10
  auto-discover-rlocs
  exit-locator-set
 !
 locator default-set RLOC_CR
 service ipv4
  encapsulation vxlan
  map-cache publications
  import publication publisher 10.1.20.3
  itr map-resolver 10.1.20.3
  etr map-server 10.1.20.3 key 7 070C285F4D06 domain-id 10
  etr map-server 10.1.20.3 proxy-reply
  etr
  sgt distribution
  sgt
  route-export publications
  distance publications 250
  import database publication locator-set RLOC_CR
  proxy-itr 10.1.20.3
  map-server
  map-resolver
  exit-service-ipv4
 !
 instance-id 4120
  remote-rloc-probe on-route-change
  service ipv4
   eid-table vrf x1
   database-mapping 0.0.0.0/0 locator-set Defaultetrset default-etr
   map-cache publications
   import publication publisher 10.1.20.3
   itr map-resolver 10.1.20.3
   etr map-server 10.1.20.3 key 7 01100F175804 domain-id 10
   etr map-server 10.1.20.3 proxy-reply
   etr
   sgt distribution
   sgt
   route-export publications
   distance publications 250
   import database publication locator-set RLOC_CR
   no proxy-etr
   proxy-itr 10.1.20.3
   exit-service-ipv4
  !
  exit-instance-id
 map-server session passive-open Defaultetrset
 ipv4 locator reachability exclude-default
 ipv4 source-locator Loopback0
 exit-router-lisp
```

# CRUSADER: LISP Control Plane Configuration

Option #2

```
CRUSADER#srl
router lisp
 site VPN
  authentication-key 7 13061E010803
  eid-record instance-id 4120 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 8120 any-mac
  allow-locator-default-etr instance-id 4120 ipv4
  exit-site
```

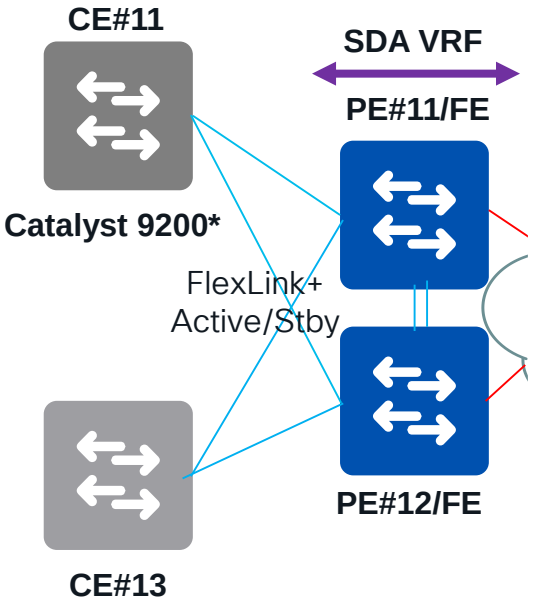
# Provider Edge/Fabric Edge – Packet Capture on P-node

Option #2

```
VIGILANTE#sh mon cap file flash:b.pcap det
Starting the packet display ..... Press Ctrl + Shift + 6 to exit
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
   [Protocols in frame: eth:ethertype:ip:udp:vxlan:eth:ethertype:ip:tcp]
Ethernet II, Src: 50:61:bf:bf:85:46, Dst: 50:61:bf:28:d9:56
Internet Protocol Version 4, Src: 10.1.20.5, Dst: 10.1.20.3
   0100 .... = Version: 4
User Datagram Protocol, Src Port: 65473, Dst Port: 4789
   Source Port: 65473
   Destination Port: 4789
Virtual eXtensible Local Area Network
   Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
      1... .... .... .... = GBP Extension: Defined
   Group Policy ID: 0
   VXLAN Network Identifier (VNI): 4120
Ethernet II, Src: 50:61:bf:bf:00:00, Dst: ba:25:cd:f4:ad:38
Internet Protocol Version 4, Src: 172.16.19.1, Dst: 192.168.2.1
   0100 .... = Version: 4
Transmission Control Protocol, Src Port: 24000, Dst Port: 80, Seq: 1, Len: 6
   Source Port: 24000
   Destination Port: 80
```

# Rollover migration of Fabric Edge on existing PEs

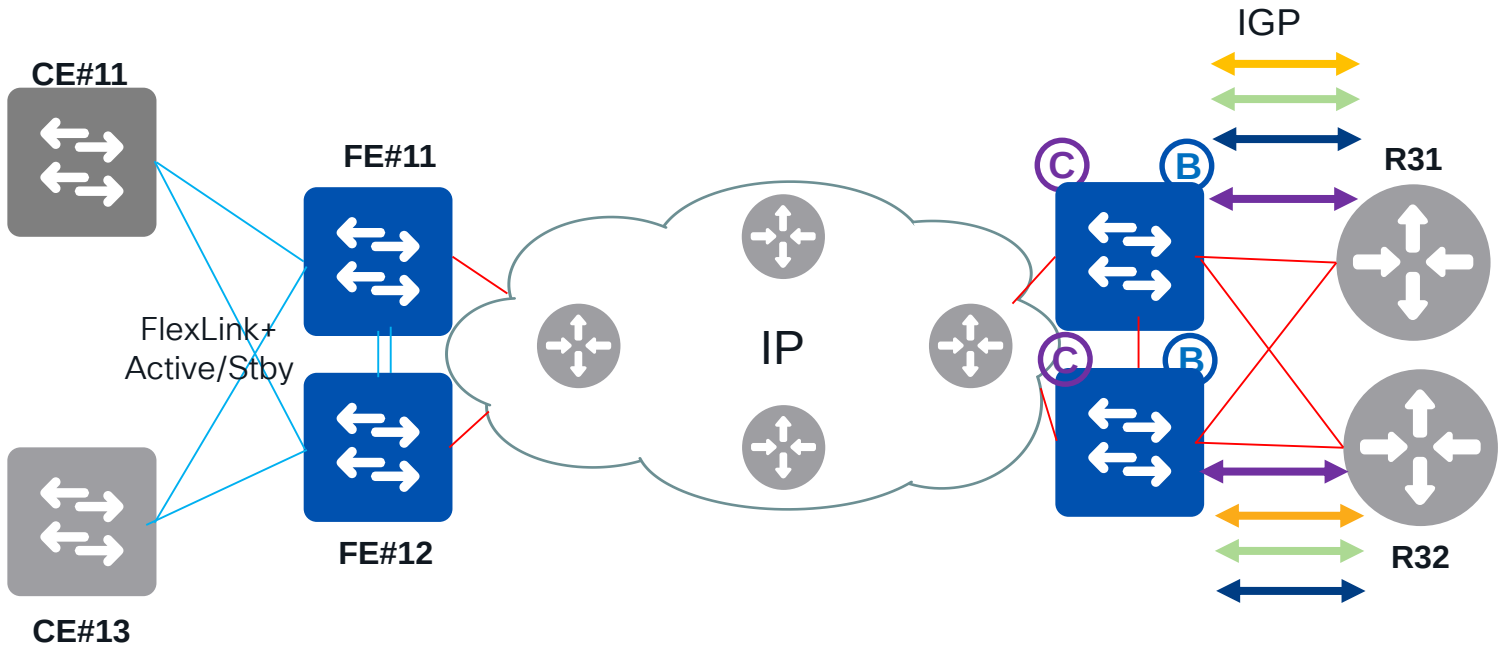
Option #2



# Recommendations for Border/CP Design Choice

## Co-existing Border/CP along with MPLS PE functionality

Option #2

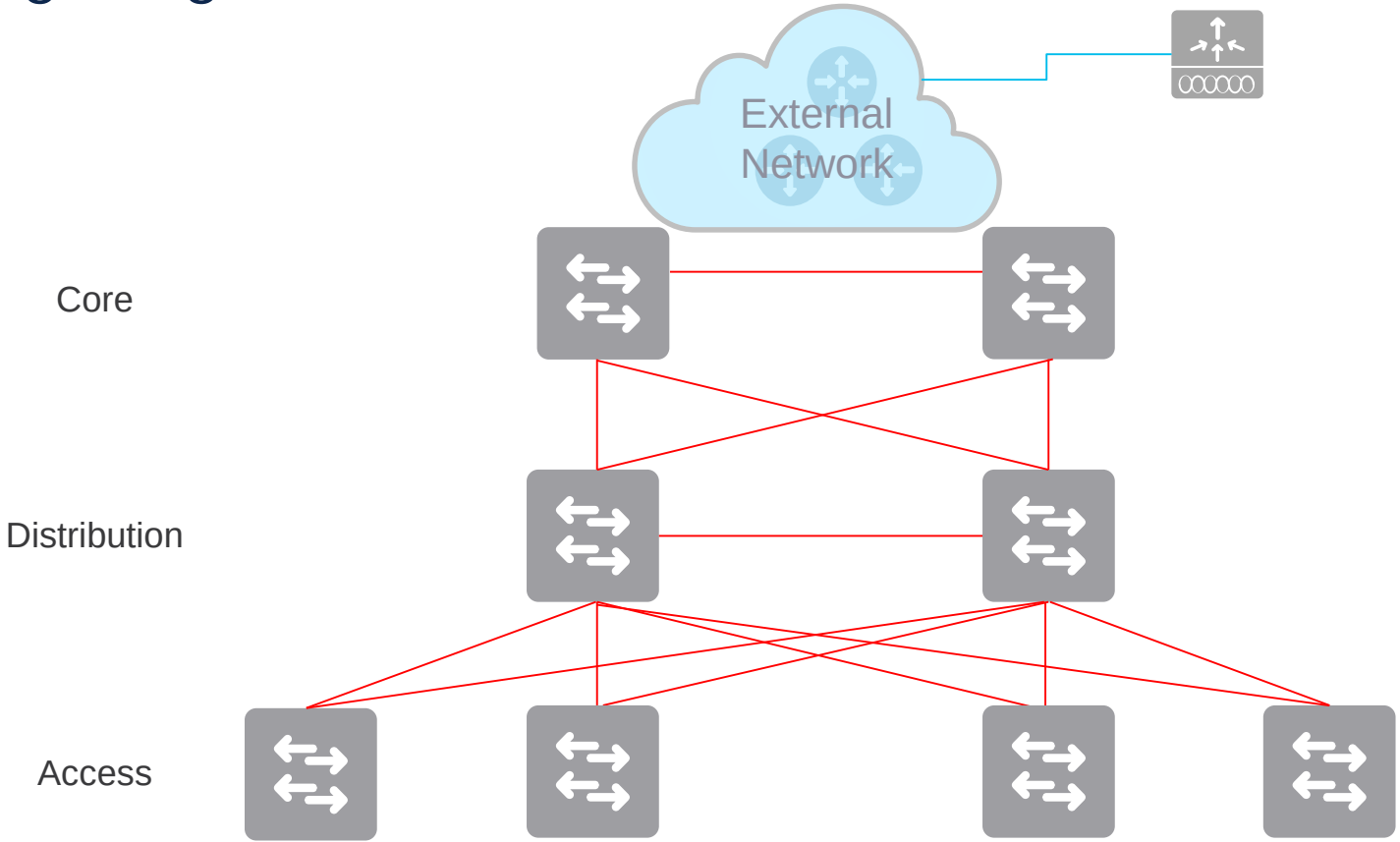


# Migrating Routed Access Designs

Hop, and maybe a skip, and you are done!!

cisco Live!

# Migrating Routed Access to Cisco SD-Access-LISP

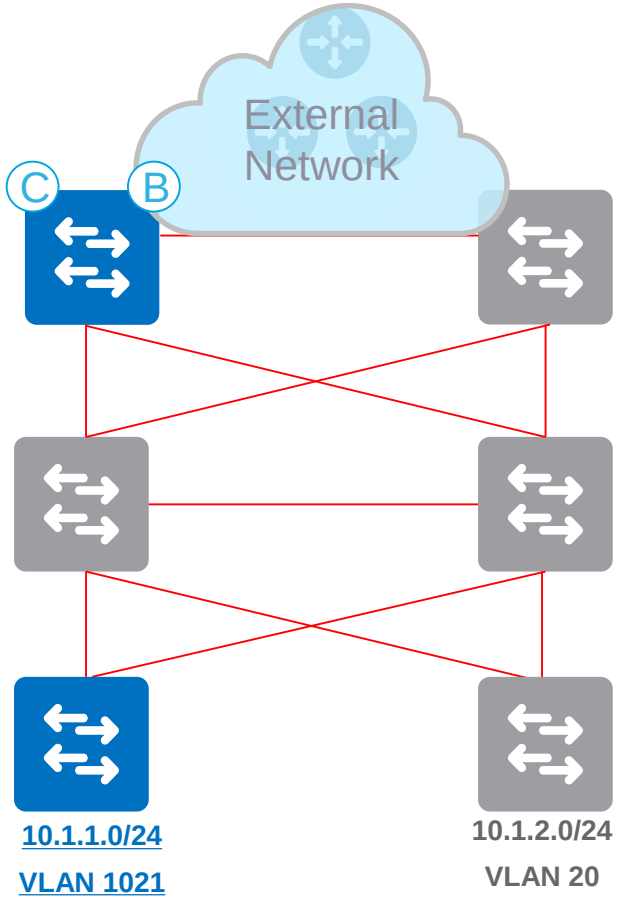


# Routed Access Design Considerations

- Can re-use the existing subnets to migrate into Cisco SD-Access-LISP
- No changes to existing DHCP scope and subnet size
- No changes to existing firewall or other policies that are based on IP-ACL
- Old network design is retained for familiarity
- Cannot realize the advantages of bigger subnets, but lesser subnets that are optimized for Cisco SD-Access-LISP

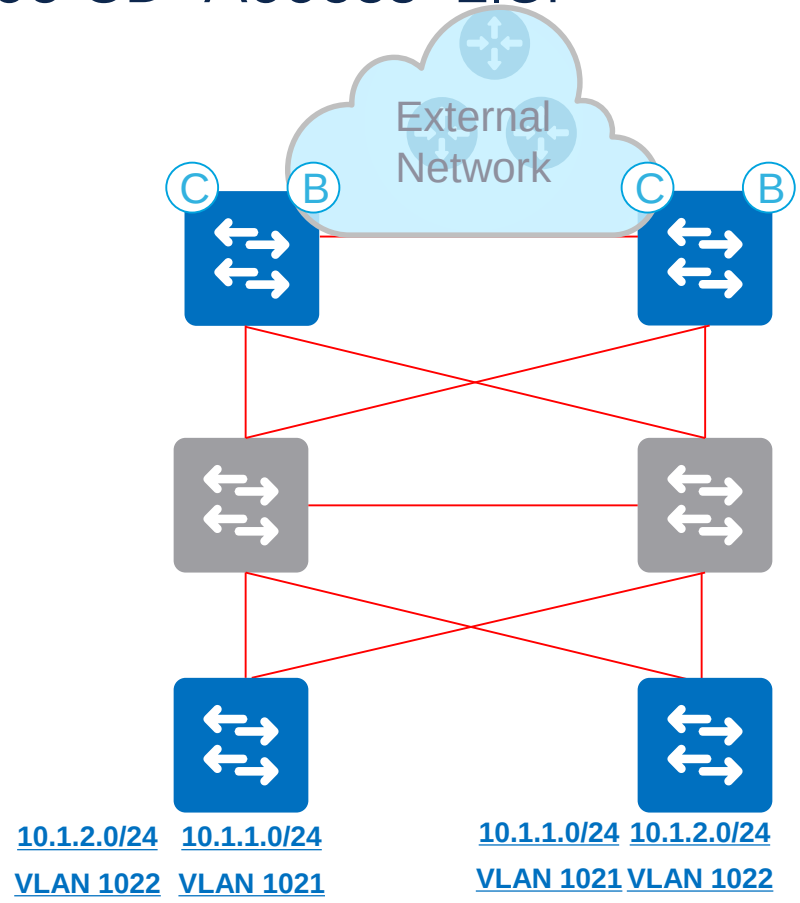
# Routed Access Migration to Cisco SD-Access-LISP

- Shutdown existing SVI (Vlan10 in this case)
- Provision existing subnet from Cisco DNA-Center (10.1.1.0/24 in this case)
- Cisco DNA-Center will provision Vlan1021 with 10.1.1.0/24
- Move hosts to fabric-enabled IP Pool
- Verify connectivity



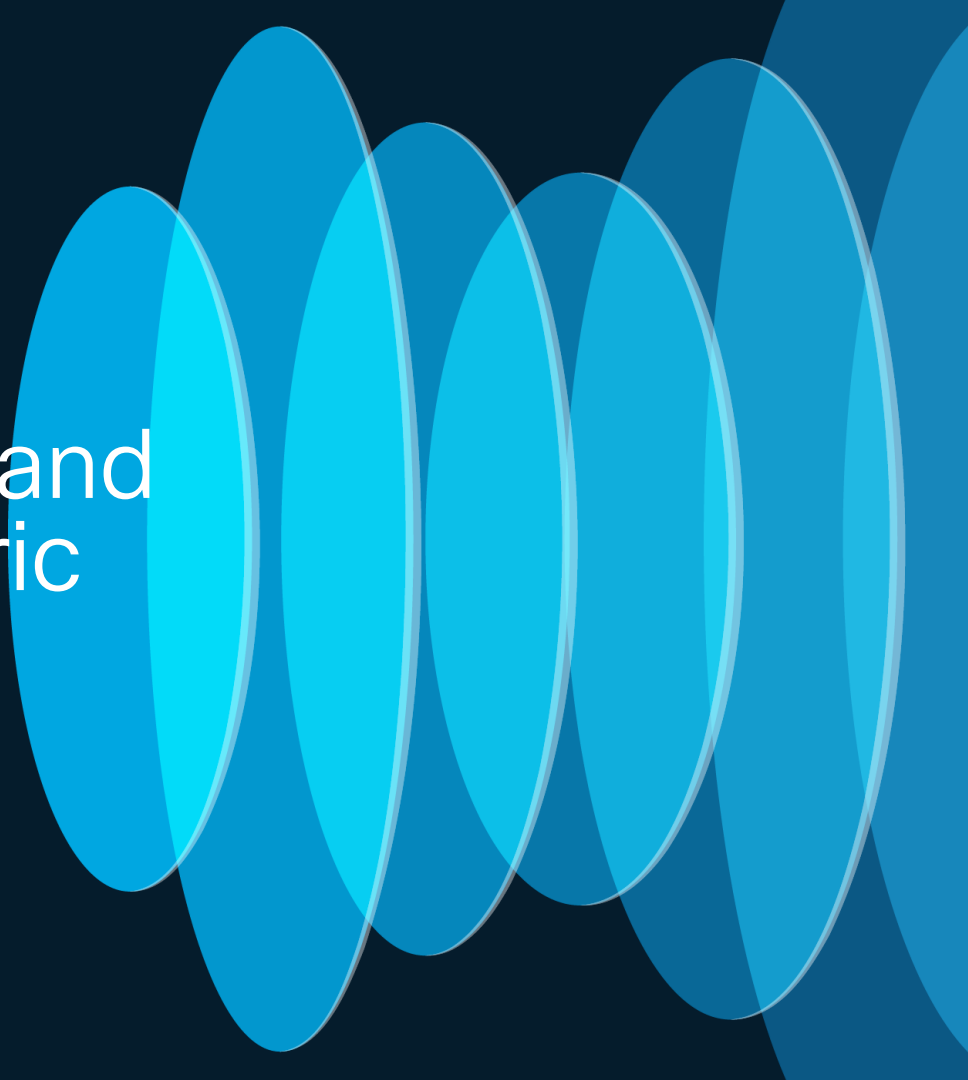
# Routed Access Migration to Cisco SD-Access-LISP

- Repeat the process for other VLANs on the Fabric Edge
- Repeat the same process on other access switches in converting them to Fabric Edge
- Migration is One-Switch—At-A-Time – **NOT** – One-Vlan-At-A-Time



# Migrating Wireless and Integrating into fabric

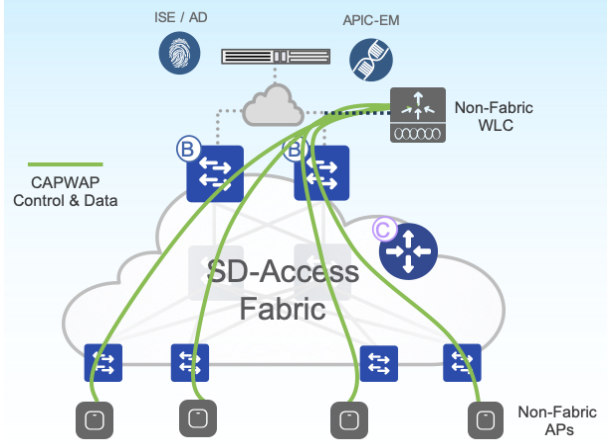
Almost there!!



cisco Live!

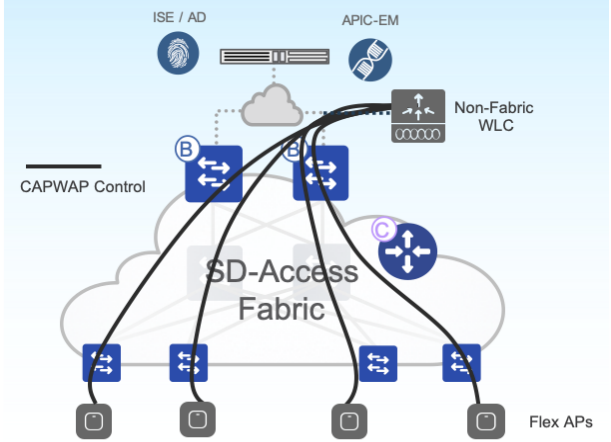
# Wireless options in LISP Fabric

## CUWN wireless Over The Top (OTT)



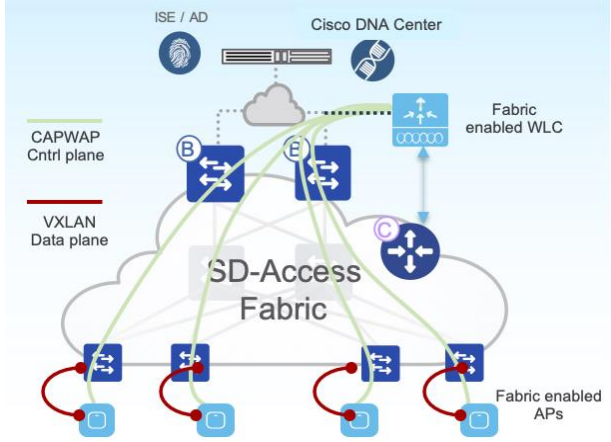

- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport
- Supported on any WLC/AP software and hardware

## FlexConnect Over The Top (OTT)



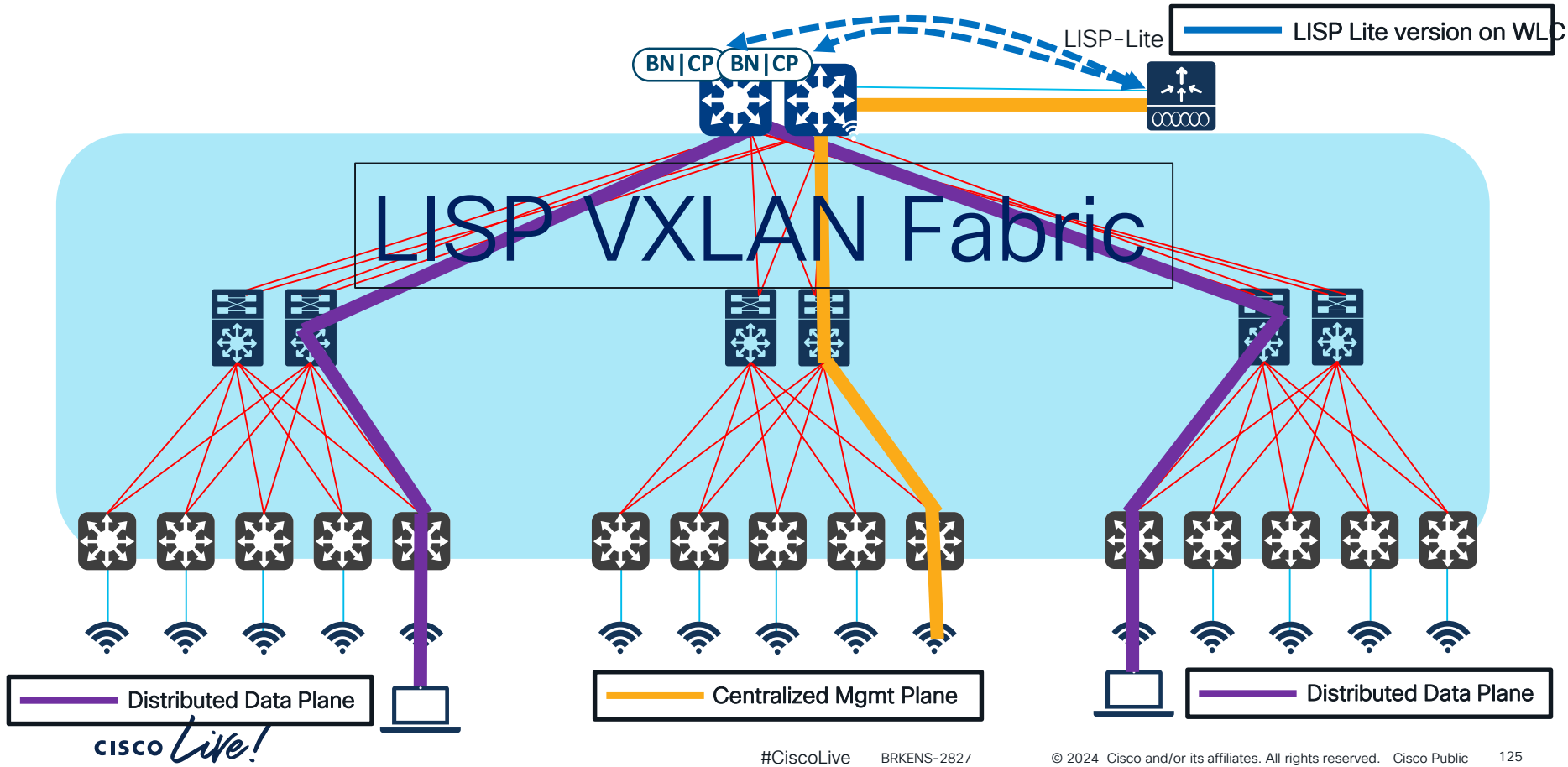

- CAPWAP for Control Plane
- Data plane is locally switched. Wireless traffic is treated like wired traffic.
- **NEW in IOS-XE 17.6.1**

## Fabric Enabled Wireless

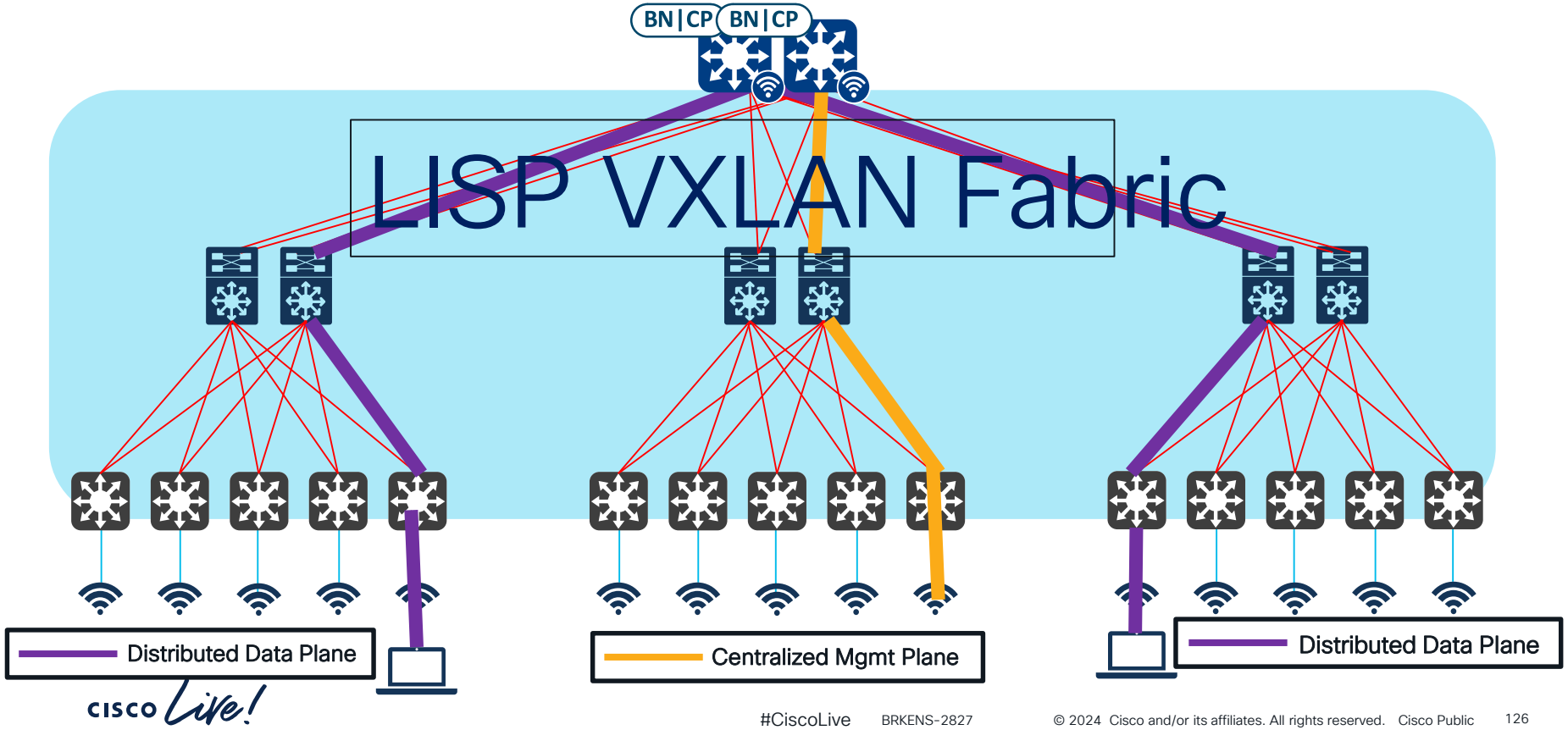



- CAPWAP Control Plane, VXLAN Data plane
- WLC/APs integrated in Fabric, LISP advantages
- Optimized for 802.11ac & 802.11ax APs

# Fabric-enabled Wireless – Best of Both!!



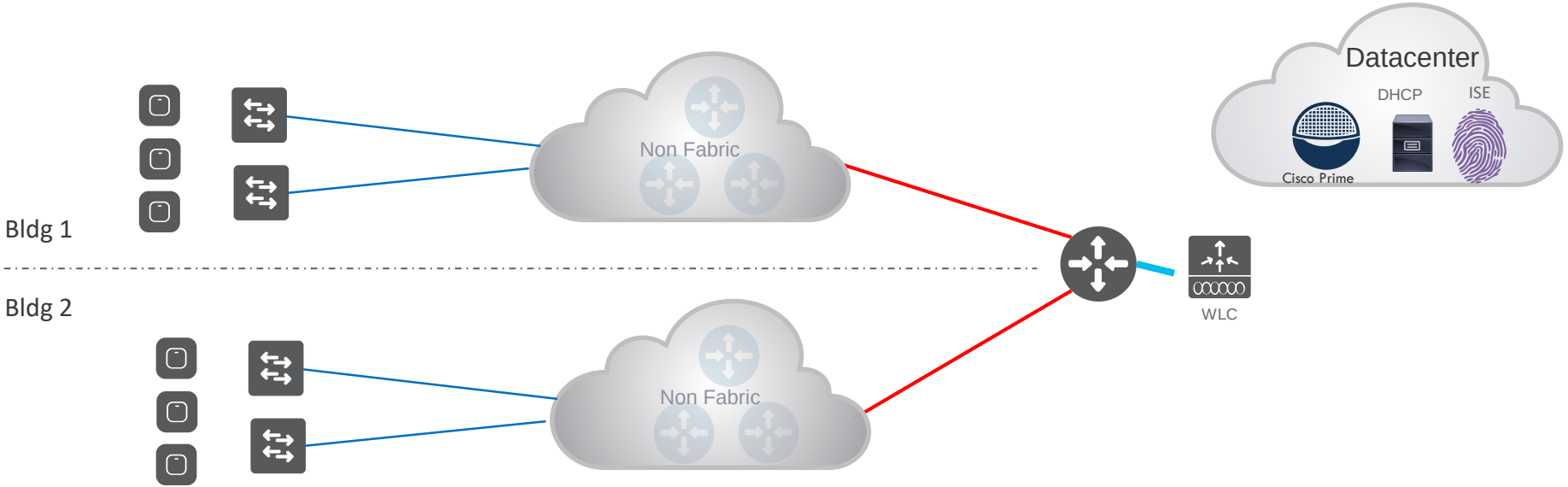
# Fabric-enabled Wireless – Embedded WLC Option



# Benefits of Fabric-enabled Wireless

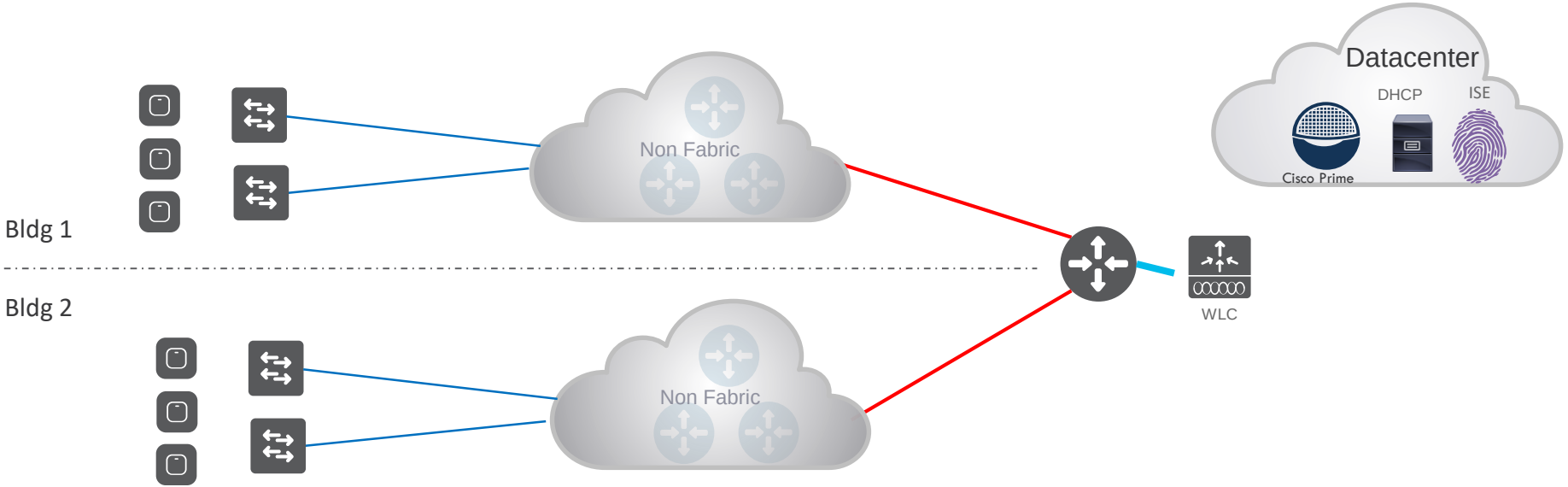
- Provides a Centralized Control and Management Plane
- Provides a Distributed Data Plane
- Best of BOTH Worlds
- Scales wireless in all the above aspects
- Consistency in forwarding traffic across Wired/Wireless
- Consistency in applying policy across Wired/Wireless
- Consistency in troubleshooting across Wired/Wireless

# Migrating to Cisco SD-Access-LISP Wireless from CUWN




- Customer has a site with Centralized wireless
- Assumptions:
  - Migration to Fabric happens in a single area (e.g. building) at the time and migration is in one shot
  - No need for seamless roaming between new SDA area and the existing wireless deployment

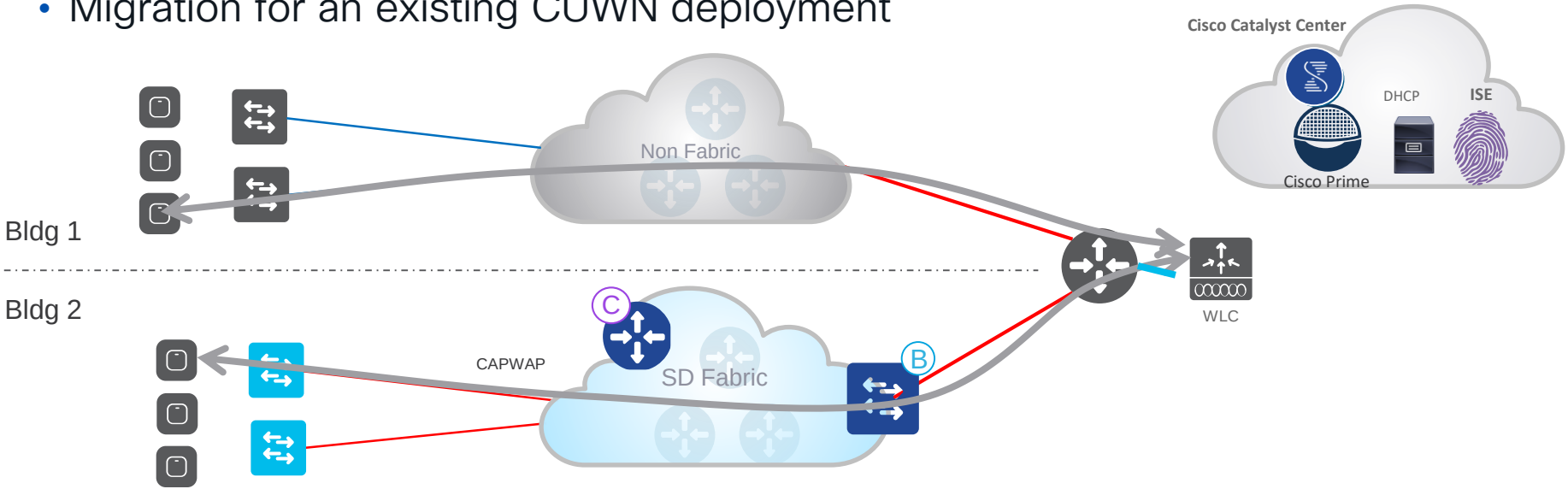
# Migrating to Cisco SD-Access-LISP Wireless from CUWN




- Customer has a site with Centralized wireless
- Assumptions:
  - Migration to Fabric happens in a single area (e.g. building) at the time and migration is in one shot
  - No need for seamless roaming between new SDA area and the existing wireless deployment

# Cisco SD-Access-LISP Wireless Migration

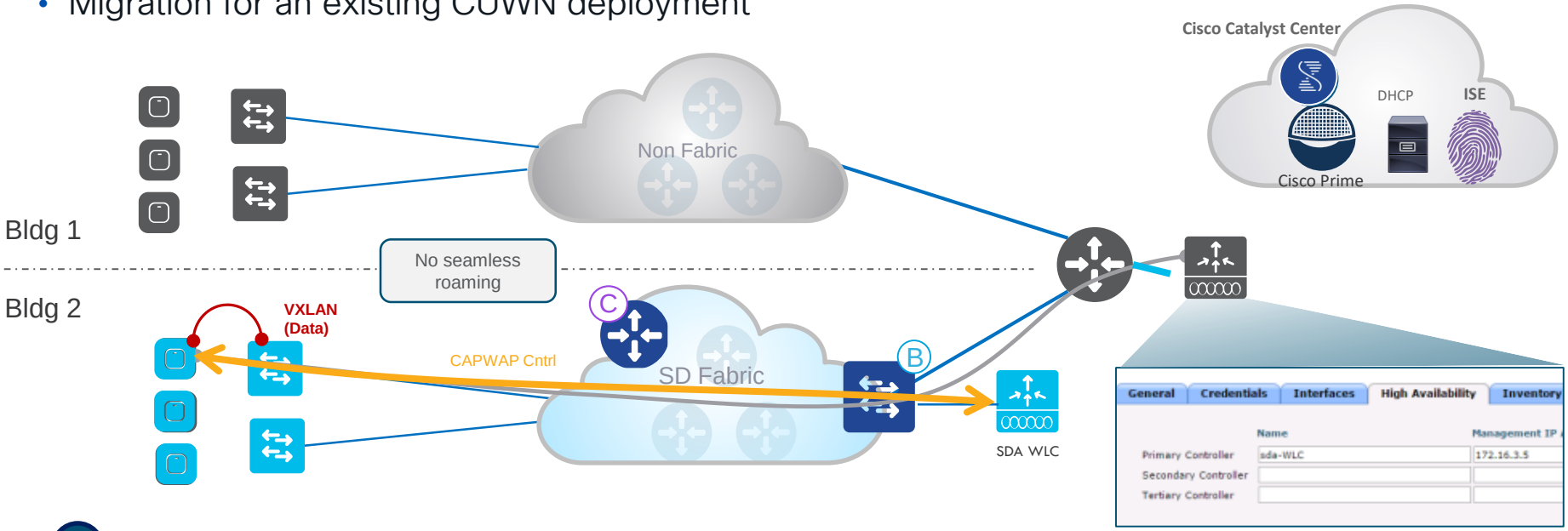
- Migration for an existing CUWN deployment




1. Add Cisco Catalyst Center and ISE (if not present already)
2. Migrate wired network to Fabric first
3. Wireless is over the top

# Cisco SD-Access-LISP Wireless Migration

- Migration for an existing CUWN deployment

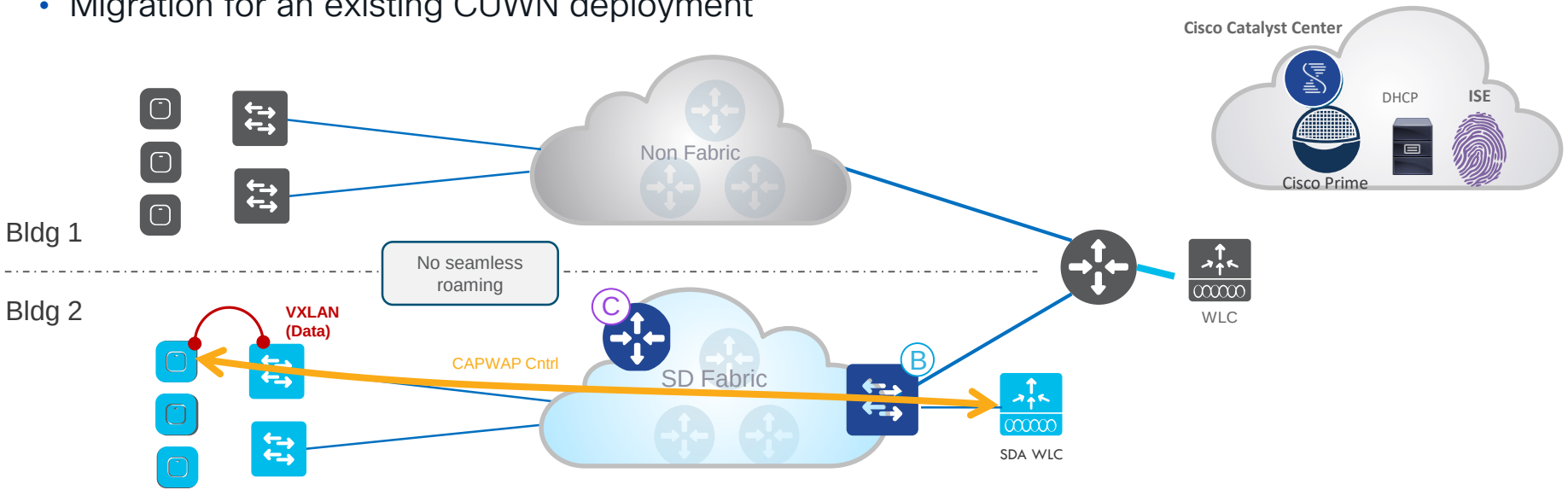



1. Add a dedicated WLC for Cisco SD-Access-LISP and configure it with same SSIDs
2. on CUWN WLC, configure the APs in the area to join the new Fabric WLC
3. Traffic now goes through the Fabric

CAPWAP Control
VXLAN

# Cisco SD-Access-LISP Wireless Migration

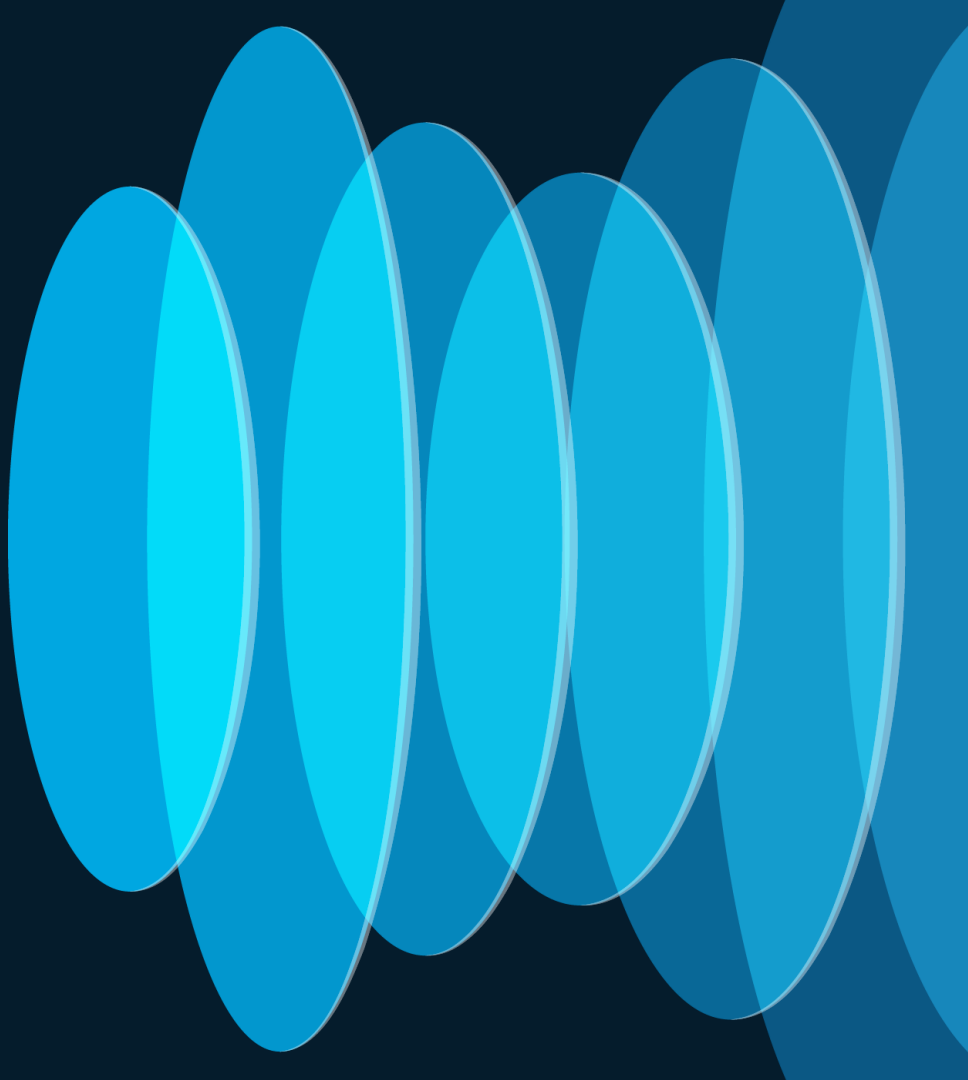
- Migration for an existing CUWN deployment




## Recommendations

- Cisco Catalyst Center/Prime for CUWN areas, Cisco Catalyst Center for SDA areas
- Dedicated WLC for Cisco SD-Access Wireless
- Same SSIDs on Fabric and non-Fabric
- Same RF Groups for CUWN WLC and SDA WLC
- WLCs in different Mobility Group (no seamless roaming between areas)

# What Next??

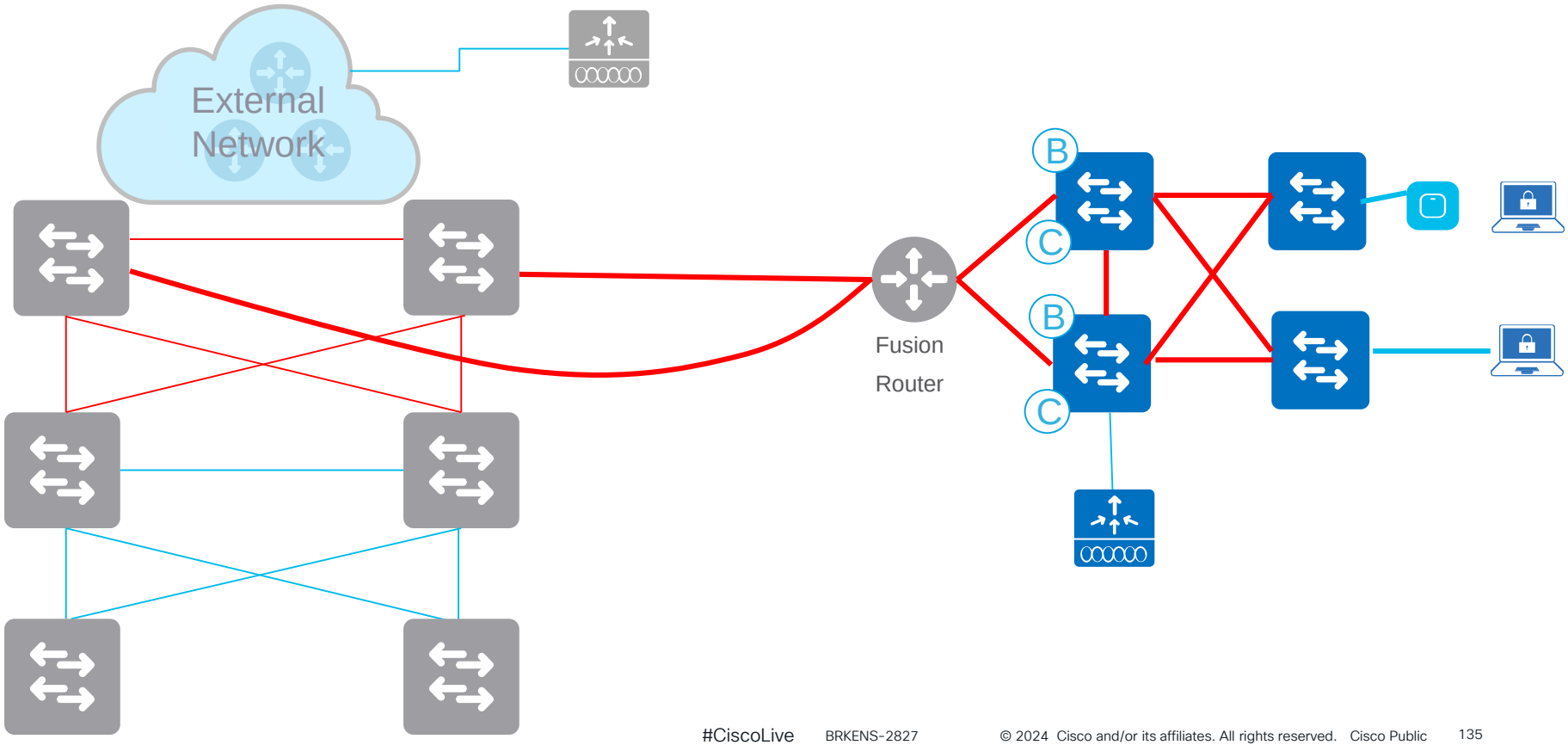


# Build a PoC in a Lab

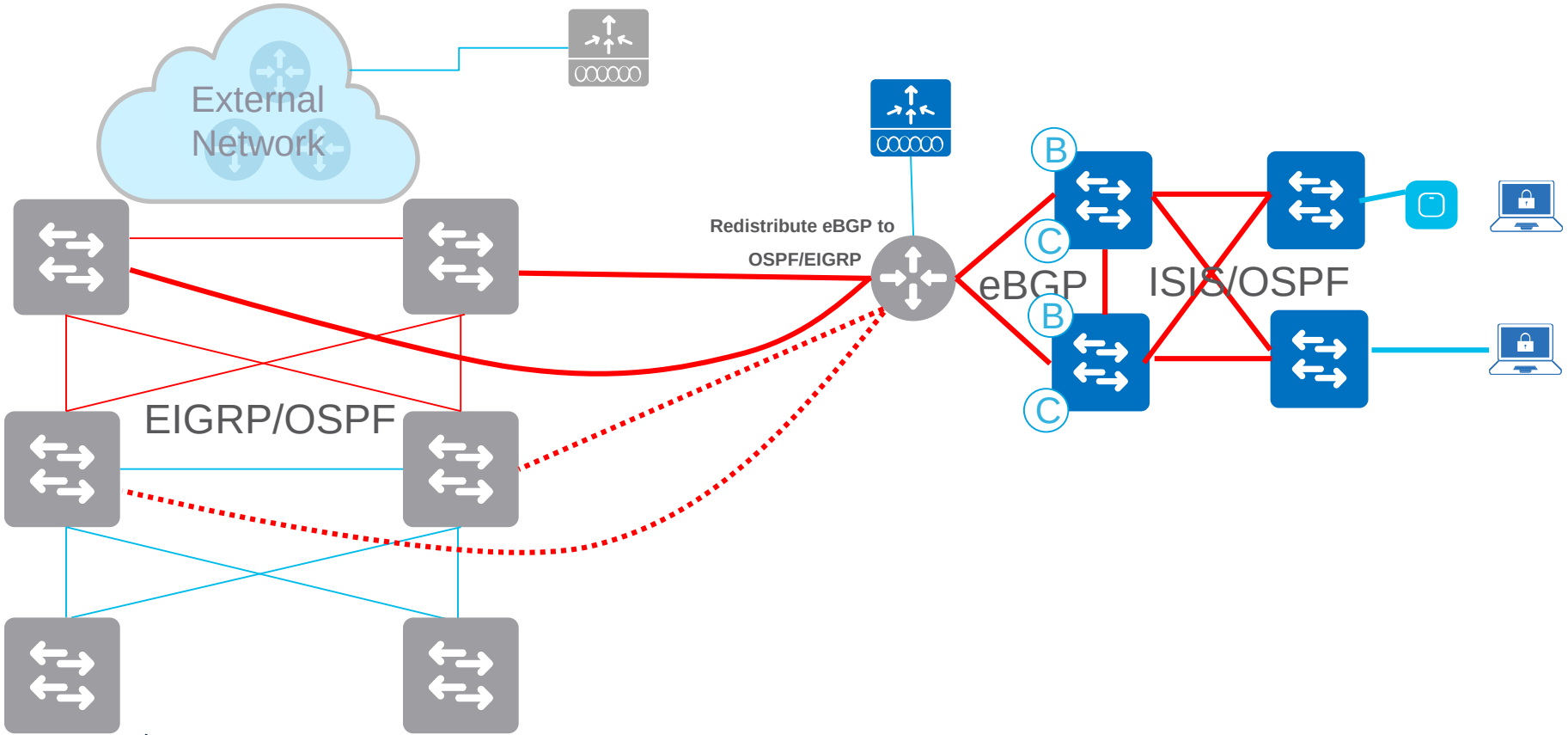
Start in a lab – isolated, controlled environment

How do I connect a lab to the production network if I want to validate use cases

# Connecting PoC Lab to Production



# IGP Normalization



# Plan Production Pilot Roll-out

- Pre-plan and execute Management components installation and configuration
- Plan a maintenance window for the actual network migration
- Start small in non-critical areas, and considerate user groups (towards IT)
- Preferably start with the IT department
- Start with 1 VN – few SGTs
- Migrate same type of endpoints and grow big
- Have backups of network device configurations
- Have a rollback plan so users are not affected

# Key Takeaways

- **Can start with just two switches to build an SDA-LISP fabric**
- **Can migrate existing network topologies / subnets** into SD-Access-LISP
- Supports migration of
  - **Layer-2** as well as,
  - **Routed Access** designs
  - MPLS –VPN designs to an IP Core with SD-Access-LISP
- **Automation** support makes it **easy** for migration
- Considerations in migration
  - **PoC** in labs
  - **Start small**, small/medium Campus/Branch locations

# SD-Access LISP **Industry Leading Campus Architecture**

Deployments

**4050+**

Momentum

**40%**

YoY growth in customers

Key use case

**70%**

Wireless

**+ 66%**

API (YoY)

Usage

**24K+**

Sites

**1.8M+**

Devices


Top verticals: Government, Finance, Professional services, and Manufacturing

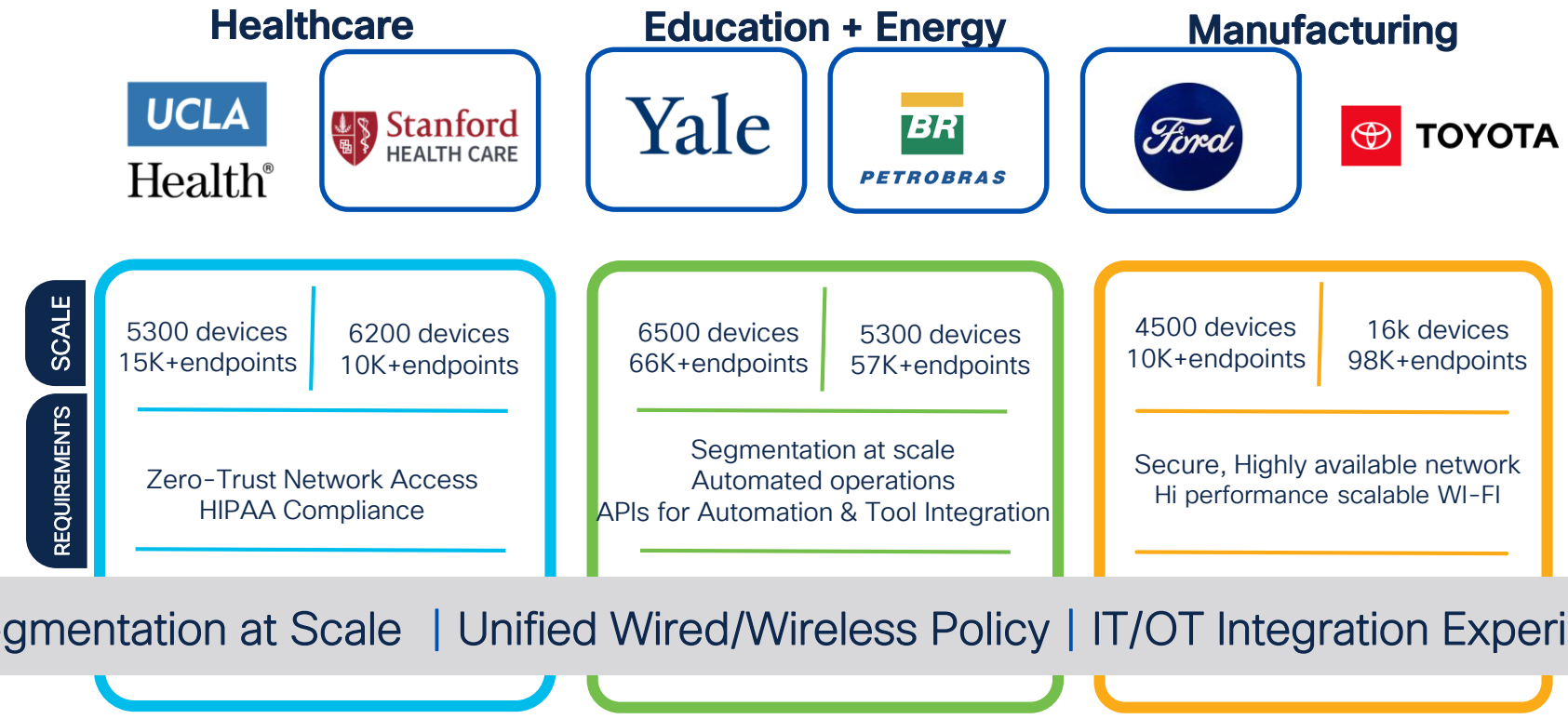
Adopted by 31% of U.S. **Fortune 100** Companies

**EMEA: 52%**

**Americas 29%**

**APJC 19%**

# SD-Access LISP Customer Success




Segmentation at Scale | Unified Wired/Wireless Policy | IT/OT Integration Experience

BRKENS 1801, BRKENS 1802, CIUG-1003

Speaking at this Cisco Live

# Global Partner Solution Advisors

## *NEW* - Fully Virtualized, SD-Access Secure Campus Lab

### Virtualized SD-Access Lab

- Fully Customizable Topology with virtualized 9kv's and 8kv's
- Access on dCloud or build on your existing Data Center
- Fraction of the cost
- GPSA mentored lab buildout support available!

### CTF Mission

- Experience the SD-Access Virtual Lab at Capture the Flag in The World of Solutions
- Use Cases – Fabric Sites and Virtual Network Provisioning, Fusion Automation, Extranet, Micro Segmentation, and more!

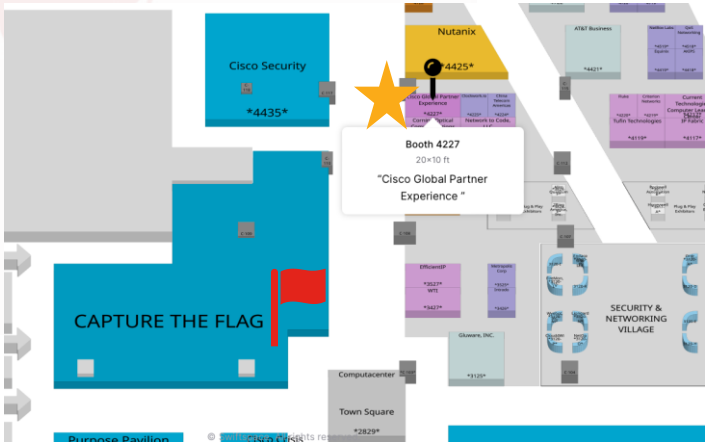
### Contact

- GPSA is your source for no-cost, partner enabment and practice building!
- Visit the Global Partner Experience booth (4227) across from Capture the Flag, for more information.

Virtual SD-Access Lab on dCloud

GPSA Sales Connect Page

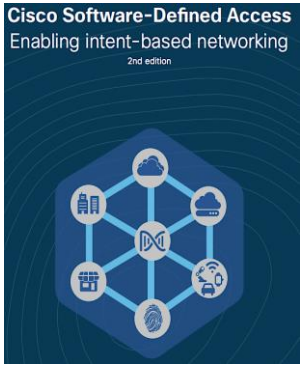
CTF at Cisco Live
Check out Secure Campus Section



# Cisco SD-Access LISP Collaterals

[Cisco Software-Defined Access for Industry Verticals]

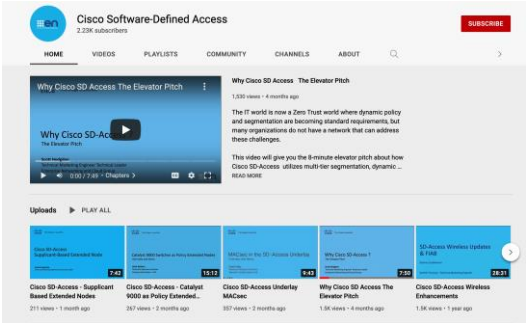

[Cisco Software-Defined Access]
Enabling intent-based networking




[Cisco Solution Validated Profiles (CVPs)]

- [Cisco Large Enterprise and Government Profile]
- [Healthcare Vertical]
- [Financial Vertical]
- [Healthcare Vertical]
- [Manufacturing Vertical]
- [Retail Vertical]
- [University Vertical]

[Cisco SD-Access YouTube Link]




[Cisco SD-Access Design Tool]

[EN&C Validated Designs]

[*The Latest SD-Access Guides*]

New Feature
Enhanced

# Catalyst Leadership in Enterprise Networks

## A Platform based Approach

**Catalyst Center and Meraki Dashboard**

**28M** Network Devices Managed

50% Y/Y

19M APs | 6M Switches | 2.5M Routers | 830M Clients

**13M**
Devices on Catalyst Center

**15.3M**
Devices on Meraki Dashboard

**Catalyst 9000 Family**

100,000+ Customers, Millions of Switches

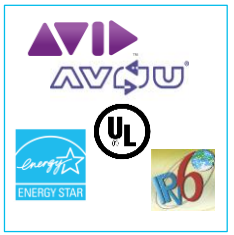
"Catalyst 9K continues to be the fastest ramping product in the company's history"

*- Chuck Robbins, CEO Cisco Systems*

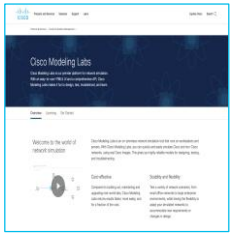
| Secure Networking | Digital Experience | Operational Simplicity |
|---|---|---|
| Common Policy | Campus Automation | Cloud Managed Catalyst |
| Secure Equipment Access | AI Endpoint Analytics | Infrastructure as a Code |
| SD-Access (LISP & EVPN) | Digital Experience ThousandEyes | S3 & CloudWatch Integration |
| High-speed Encryption | AI Ops & Assurance | Visibility, Control & Rollback |


Cisco Validated Profiles (CVP)


Industry Validated Reports




Industry Certifications




Cisco Modeling Labs

# Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.


**Earn 100 points** per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

# 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

# Thank you