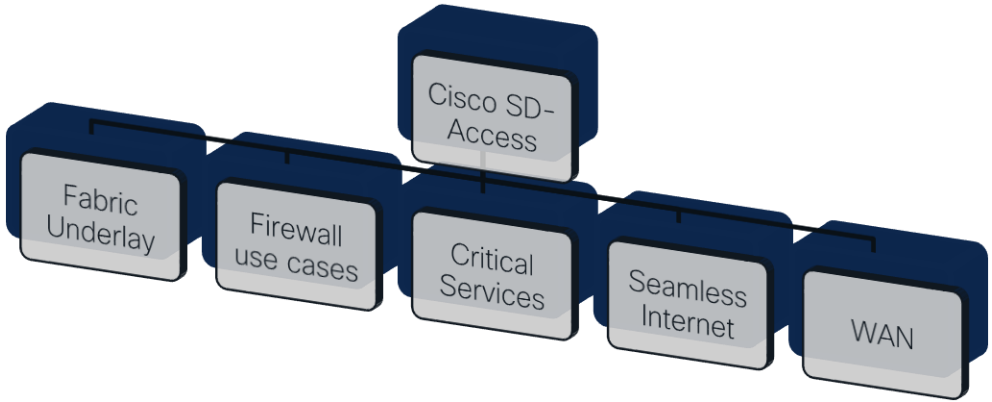
The bridge to possible

Connecting Cisco SD-Access to External World

Devi Bellamkonda
Technical Marketing Engineering, Technical Leader
BRKENS-2811

Agenda



In this Session ….

✓ Expect to learn about new capabilities through use cases.

✗ We will not be covering the basics of Cisco SD-Access and its various components.

✗ The scenarios discussed may not exactly match your challenges, but they can give you insights on how to approach them.

Explore Ideas with ..

- Cisco Partners
- Cisco CX services
- Cisco SE or AM
- Cisco Communities
- Cisco Live meet the expert
- Cisco Live On-Demand Library

Networking

SD-Access

Learn about Cisco's Software Defined Access (SD-Access) solution that provides a secure, dynamic, and automated solution to meet the security and operational challenges faced by an ever-changing environment. The Cisco SD-Access sessions provide a comprehensive overview regarding best practices, design, deployment, migration and monitoring of a Cisco SD-Access architecture.

START

Feb 5 | 19:45
LABENS-2302
SD-Access Troubleshooting

Feb 6 | 08:45
TECOPS-2001
Transforming Network Operations by Migrating from Prime Infrastructure to Cisco DNA Center

Feb 7 | 10:00
BRKOPS-2035
Real World Use Cases for Deploying and Operating Cisco SD-Access Using Cisco DNA Center

Feb 7 | 17:00
BRKARC-2092
Catalyst 9000 SiliconOne and IOS XE Architecture and Innovation

Feb 8 | 08:30
BRKARC-2035
The Catalyst 9000 Switch Family - An Architectural View

Feb 8 | 08:30
BRKENS-2810
Cisco Software Defined Access - Under the Hood

Feb 8 | 08:30
BRKENS-3096
Migrating Classical Enterprise Campus Networks to VXLAN EVPN Based Networks

Feb 8 | 08:30
BRKOPS-2077
Tips and Tricks for Prime Infrastructure to Cisco DNA Center Migration

Feb 8 | 08:30
LTRENS-2419
SD-Access Wired lab with Endpoint Analytics

Feb 8 | 10:30
BRKENS-2814
Role of Cisco ISE in SD-Access Network

Feb 8 | 12:00
BRKENS-2811
Connecting Cisco SD-Access to the External World

If you are unable to attend a live session, you can watch it On Demand after the event

CISCO Live!

Feb 8 | 16:30

BRKENS-2829

What's New in Cisco SD-Access

Feb 9 | 08:30

BRKENS-2815

SD Access for Distributed Campus Session

Feb 9 | 08:30

BRKENS-2828

LISP Architecture Evolution - New Capabilities Enabling SD-Access

Feb 9 | 10:30

BRKENT-2837

GAME Time ! Will You Be the Networker of the Year?

Feb 9 | 13:45

BRKENS-2502

Cisco SD-Access Best Practices - Design and Deployment

Feb 10 | 09:00

BRKENS-2819

Cisco SD-Access and Multi-Domain Segmentation

Feb 10 | 09:00

BRKENS-3834

1 to 100 - Master all Steps of Deployment, seamless Integration and Migration of large SDA and SD-WAN Networks

Feb 10 | 09:00

BRKTRS-3820

SD Access: Troubleshooting the Fabric

Feb 10 | 11:00

FINISH **BRKENS-2820**

Demystifying IP Multicast in SD-Access

If you are unable to attend a live session, you can watch it On Demand after the event

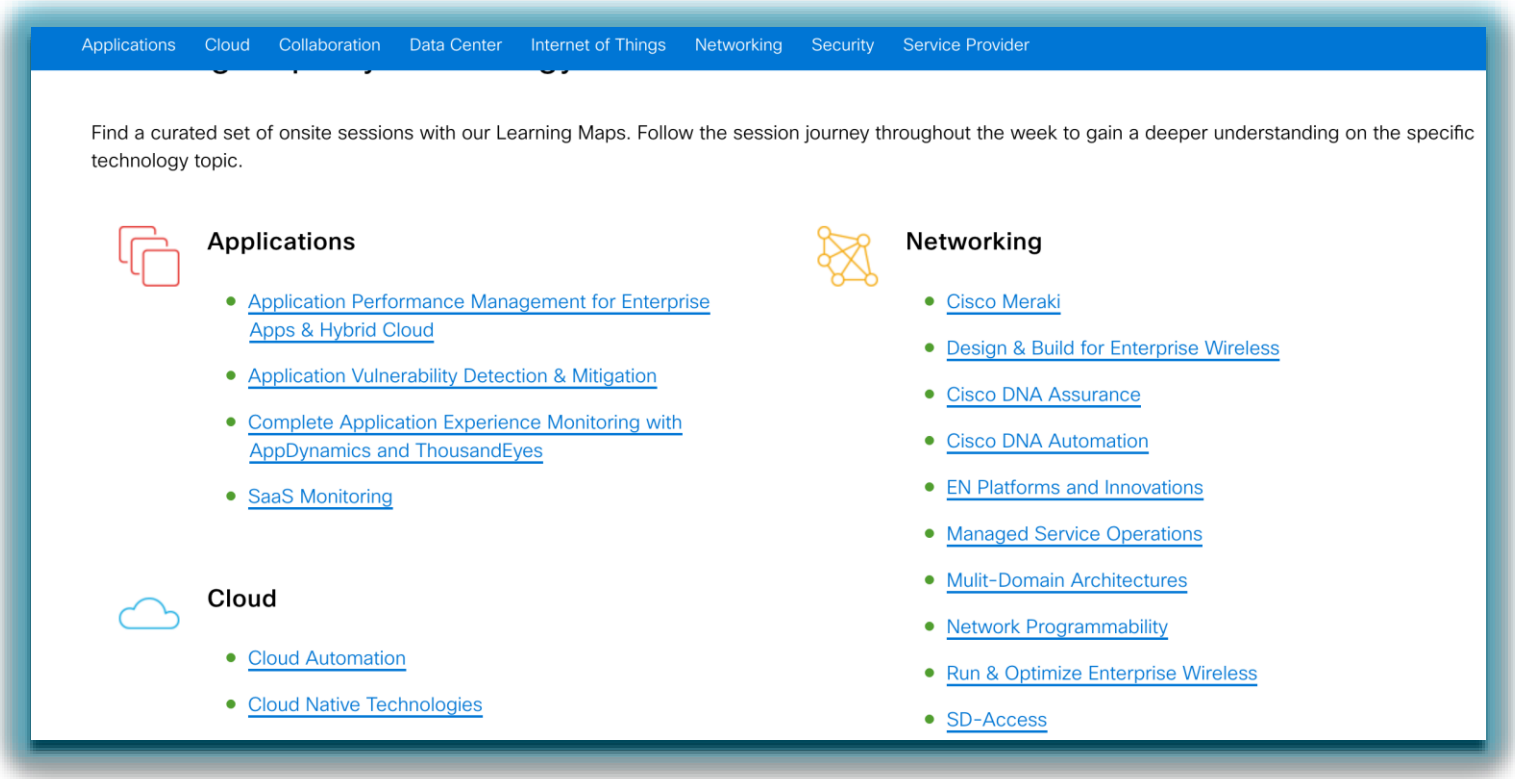
CISCO Live!

For Your Reference

The PDF contains lot more information **“For your Reference”**

Learning Maps by Technology Track

For Your Reference



Learning Maps

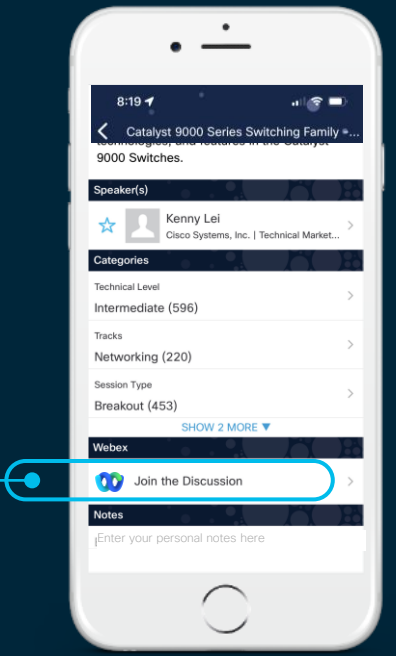
Cisco Webex App

Questions?

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

How

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



Webex spaces will be moderated by the speaker until February 24, 2023.

MTS – Meet The Speaker – MTS- 1059

- Session Title - **Meet the Speaker: BRKENS-2811 – MTS-1059**
- 02/09/23 @ 11:40AM
- In the Sessions Lounge
- Continue the post session discussion/Q&A
- On the session catalog

Customer Challenges and Requirements

Customer Challenges and Requirements

- Fabric ready Underlay
  - Underlay for the fabric should be automated
  - Concurrent Underlay automation for sites
  - Zero-Touch Image Management with device onboarding

Customer Challenges and Requirements

- Firewall
  - Enforcement on Firewall
  - Network access for vendors at Convention Center

Customer Challenges and Requirements

- Critical Services
  - Simplified Critical services access such as Shared Services and Internet with minimum configuration.

Customer Challenges and Requirements

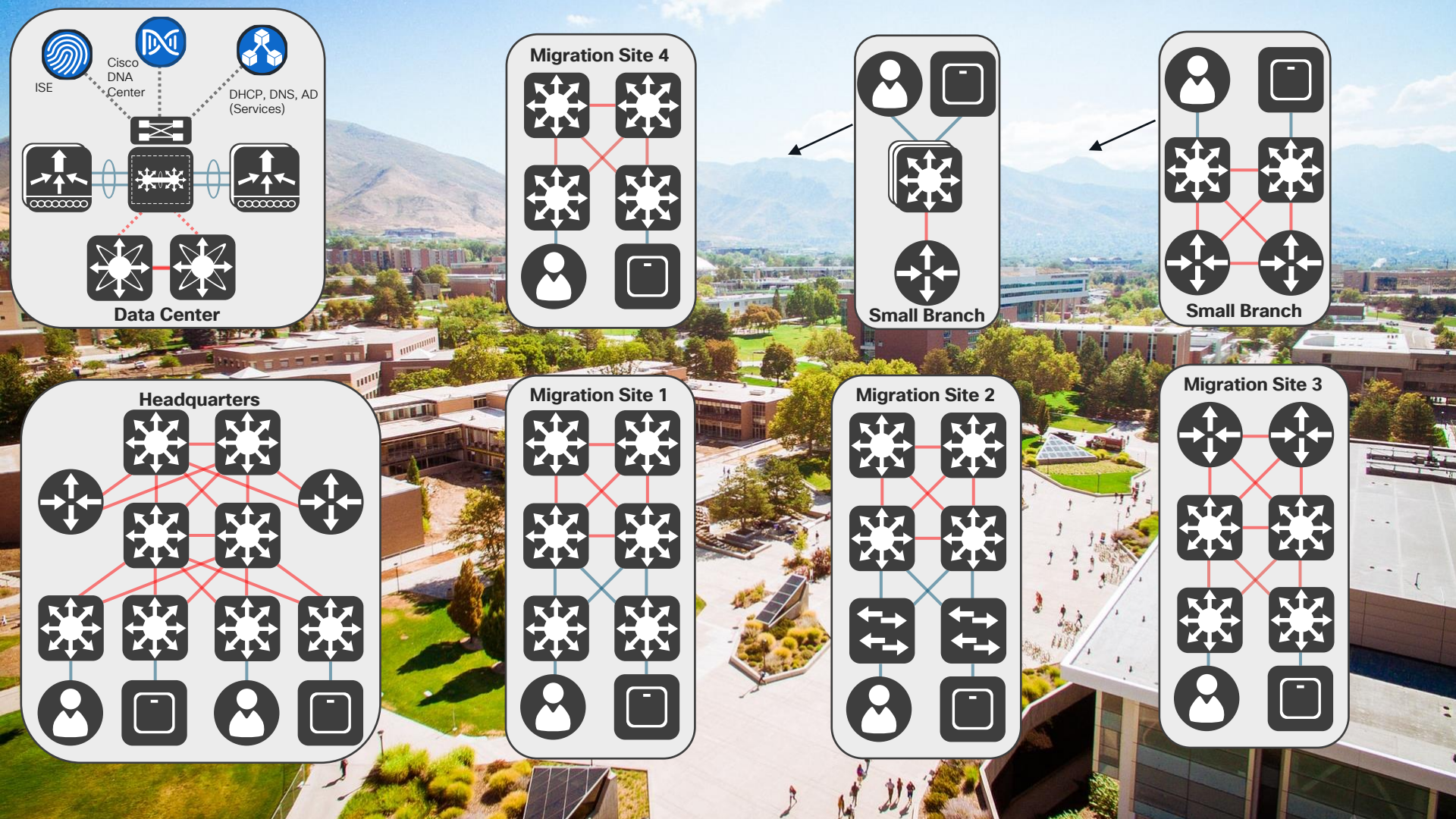
- Seamless Internet Connectivity
  - Consistent Policy across Cisco SD-Access sites.
  - No loss in Internet Connectivity(Active/Backup Internet).

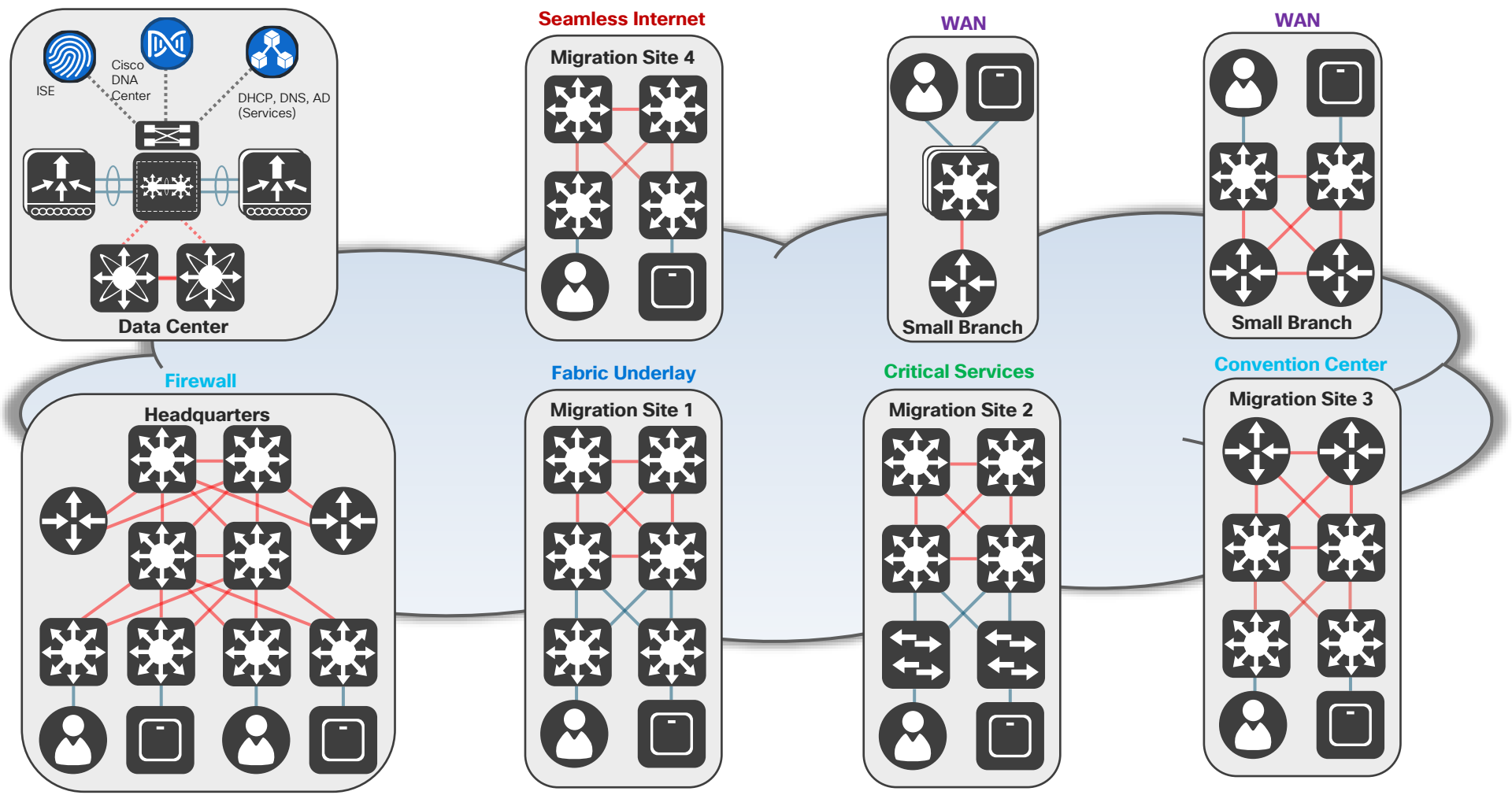
Customer Challenges and Requirements

- Branch and Regional Locations
  - Cisco SD-WAN network is already deployed.
  - This SD-WAN network is used for between Branch locations and regional sites to communicate with the remainder of the network.
  - Consistent policy must be used across the Campus and WAN.
  - Maximize port usage on switches in the Branch locations

Customer Challenges and Requirements

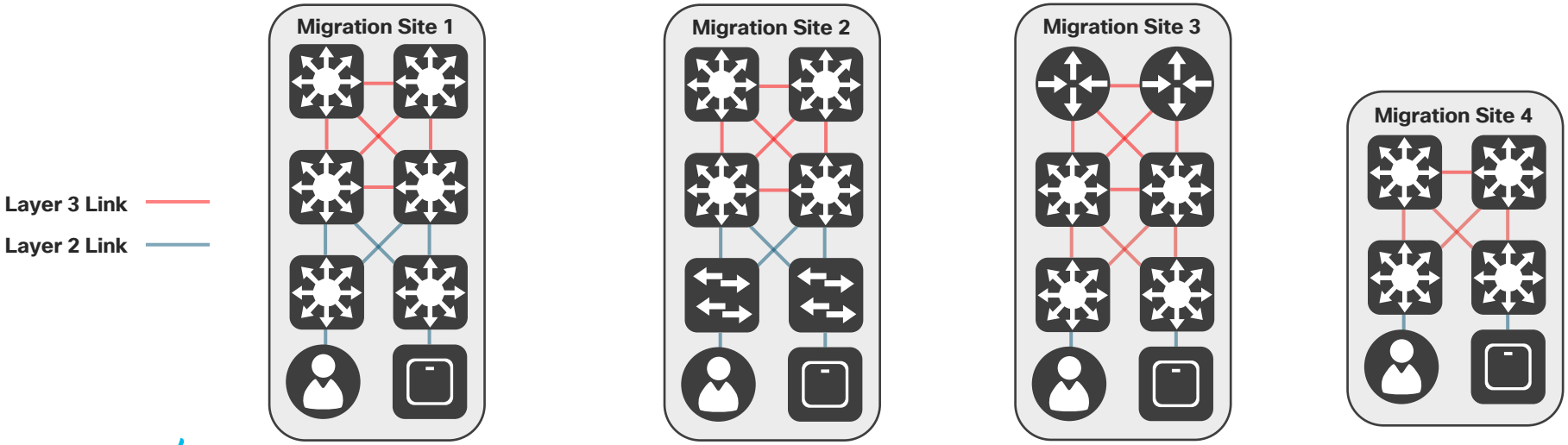
- Fabric ready Underlay
  - Underlay for the fabric should be automated
  - Concurrent Underlay automation for sites
  - Zero-Touch Image Management with device onboarding
- Firewall
  - Enforcement on Firewall.
  - Network access for vendors at Convention Center
- Critical Services
  - Simplified Critical Services such as Shared Services and Internet with minimum configuration
- Seamless Internet Connectivity
  - Consistent Policy across Cisco SD-Access sites.
  - No loss in Internet Connectivity(Active/Backup Internet).
- Branch and Regional Locations
  - Cisco SD-WAN network is already deployed.
  - This SD-WAN network is used for between Branch locations and regional sites to communicate with the remainder of the network.
  - Consistent policy must be used across the Campus and WAN.
  - Maximize port usage on switches in the Branch locations


ISE
Cisco DNA Center
DHCP, DNS, AD (Services)
Data Center
Migration Site 4
Small Branch
Small Branch
Headquarters
Migration Site 1
Migration Site 2
Migration Site 3



*** WLCs for each site not shown**

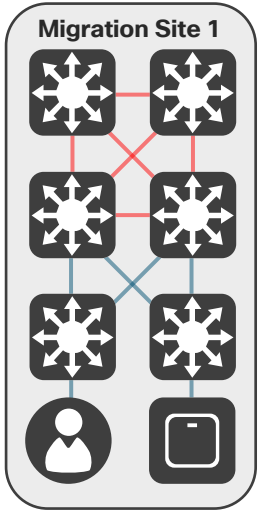
LAN Automation Enhancements



Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation

RECAP



Layer 3 Switch

- Zero-Touch Image Management with device onboarding.
- Automated underlay buildout with validated best practice configuration.
- L3 routed access network with IS-IS routing protocol.
- Higher MTU to accommodate VXLAN encapsulation
- (optional) enable Multicast option to support Broadcast, Unknown-Unicast and Link-local Multicast (BUM).

Automated underlay

Turnkey solution to dynamically discover, onboard and provision switches to simplify network operations.

Fabric Network Infrastructure

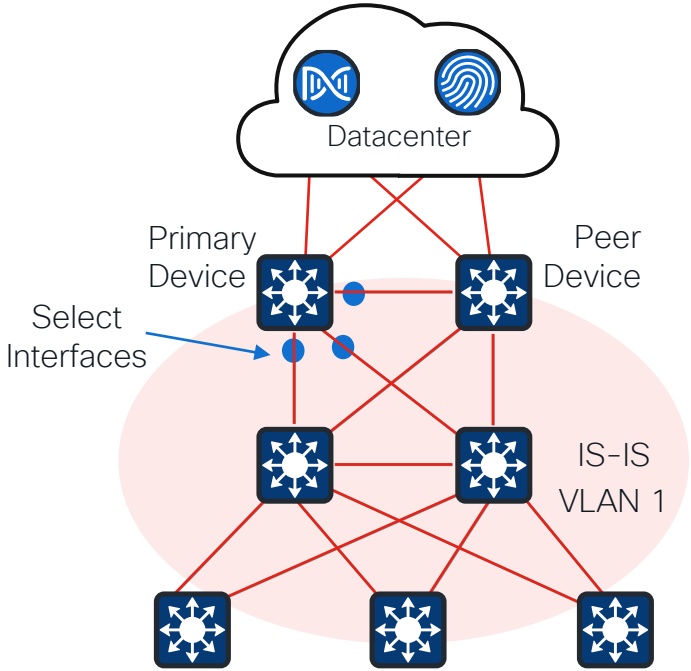
RECAP

- Underlay Infrastructure: LAN Automation Procedure

- Define Network Settings
  - Network - Network Hierarchy
  - Device Credentials – CLI, SNMP, HTTP(s)Credentials
  - IP Address Pools – IP Pool to build underlay infrastructure

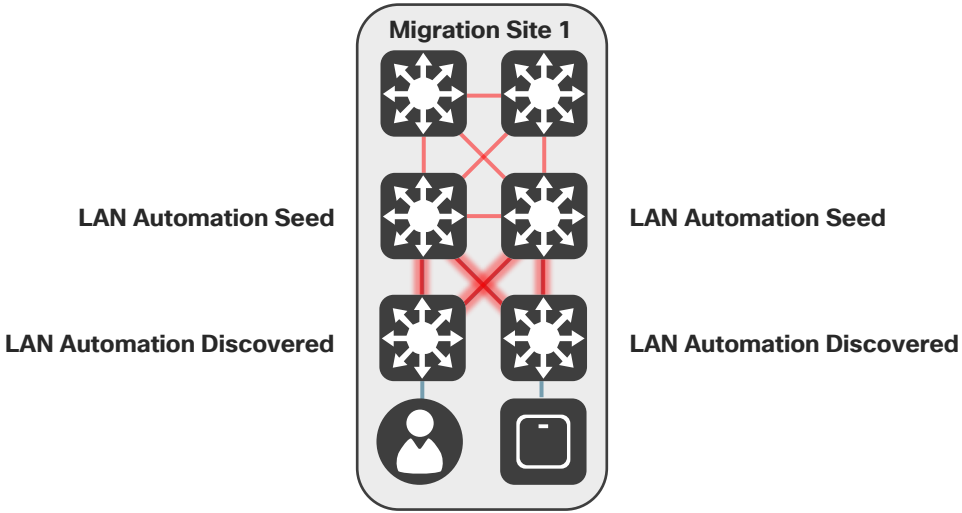
- Provision network devices
  - Select Seed devices – Primary/Peer Device and Interfaces
  - Start LAN Automation – Discover network devices, image management and assigned to site.
  - Stop LAN Automation – configure routed-access

[Cisco DNA Center User Guide, Release 2.3.5]
[Cisco DNA Center SD-Access LAN Automation Deployment Guide]



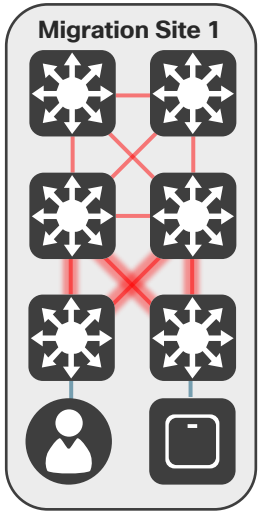
Fabric Network Infrastructure

Underlay Infrastructure: After LAN Automation



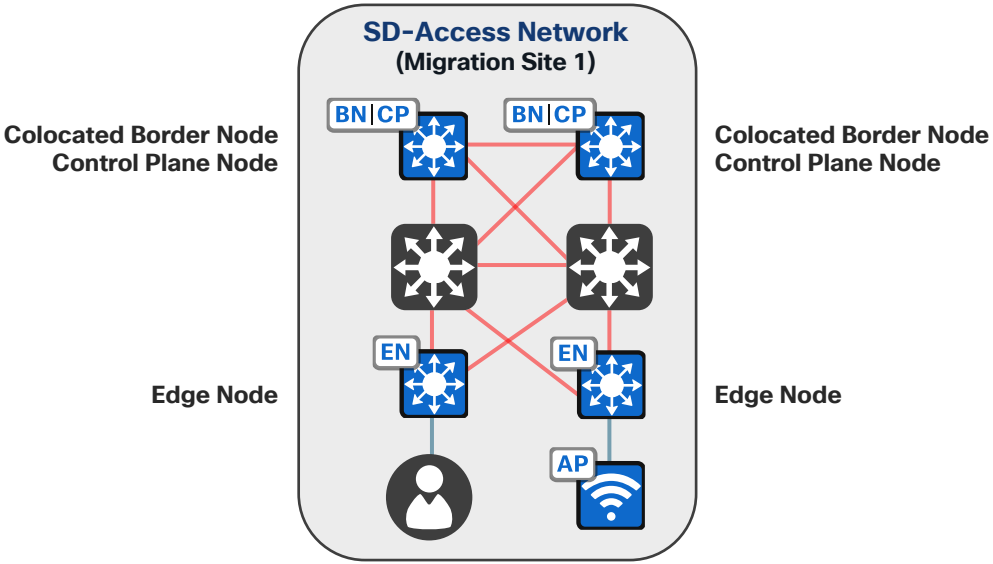
Fabric Network Infrastructure

Underlay Infrastructure: After LAN Automation



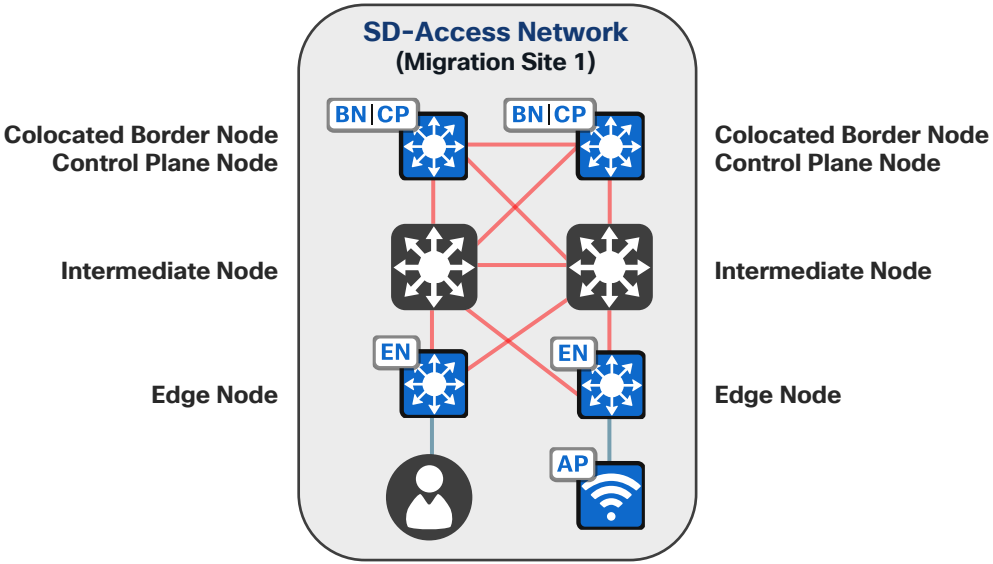
Fabric Network Infrastructure

Underlay Infrastructure: Site after Migration



Fabric Network Infrastructure

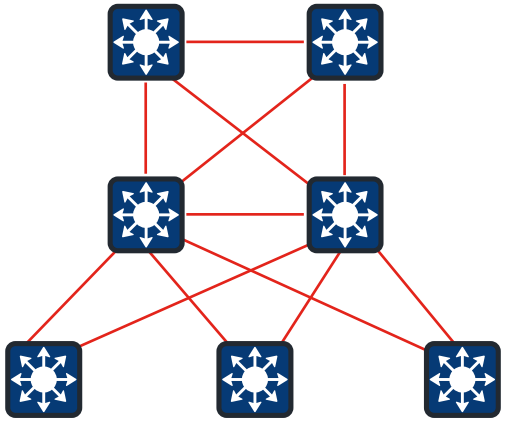
Underlay Infrastructure: Site after Migration



Fabric Network Infrastructure

Robust Underlay Infrastructure deployment

- L3 Routed Access Network
- Any routing protocol
- Resilient and Redundant fast-converged connectivity with ECMP, BFD, NSF enabled.
- Loopback 0 with /32 host prefix.
- Higher MTU to accommodate VXLAN encapsulation
- Underlay multicast to optimize overlay subnet multicast/broadcast distribution



Manual Underlay

Device-by-Device onboarding and configuration either manually or through Cisco DNA Center Plug-and-Play.

Automated Underlay

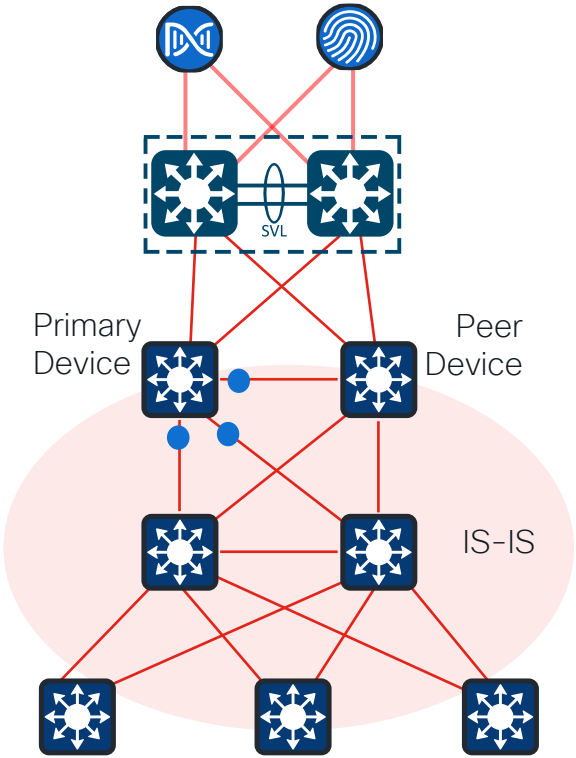
Turnkey solution to onboard multiple switches with image management and best-practices configuration.

Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation Considerations

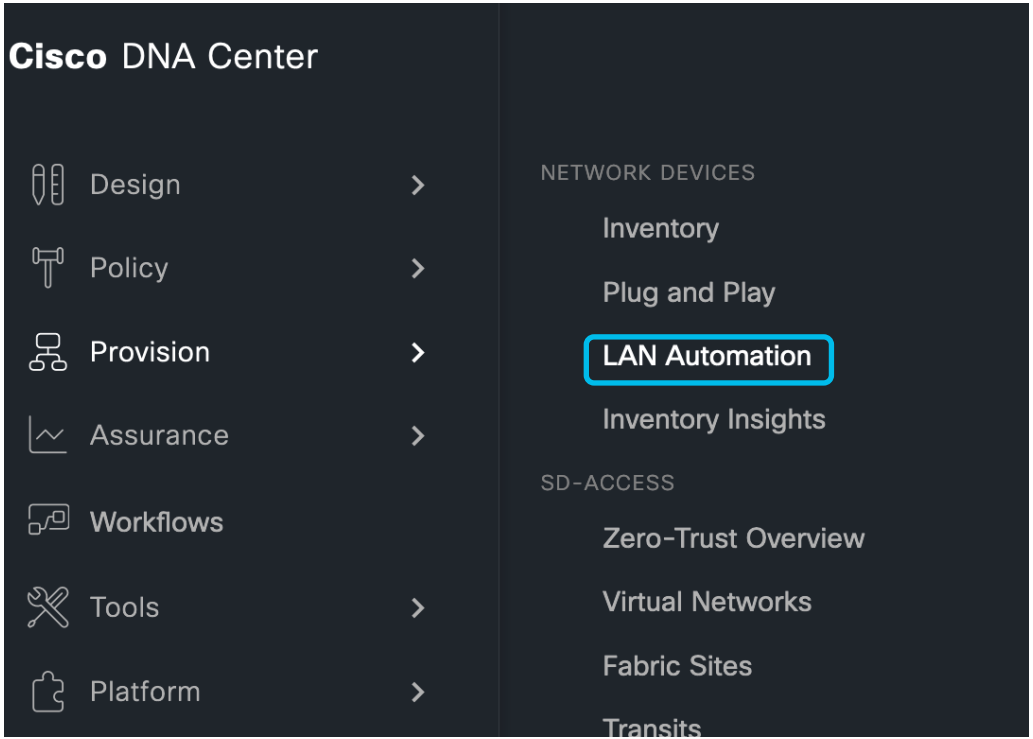
For Your Reference

- Primary and Peer Device should be discovered and managed in Cisco DNA Center.
- Network Devices must be running DNA Advantage license.
- Redistribute IS-IS routing protocol into routing protocol used, ensuring the LAN Automation ip address pool has reachability to Cisco DNA Center.
- LAN Automation IP Address Pool should be reserved as type ‘LAN’.
- LAN IP Address Pool is split into 3 sub-pool to reserve:
  - Temporary DHCP Pool on the Primary Device.
  - Configure Pt-to-Pt link subnet (/31 prefix)
  - Configure Loopback 0 interface with host (/32) prefix address



Fabric Network Infrastructure

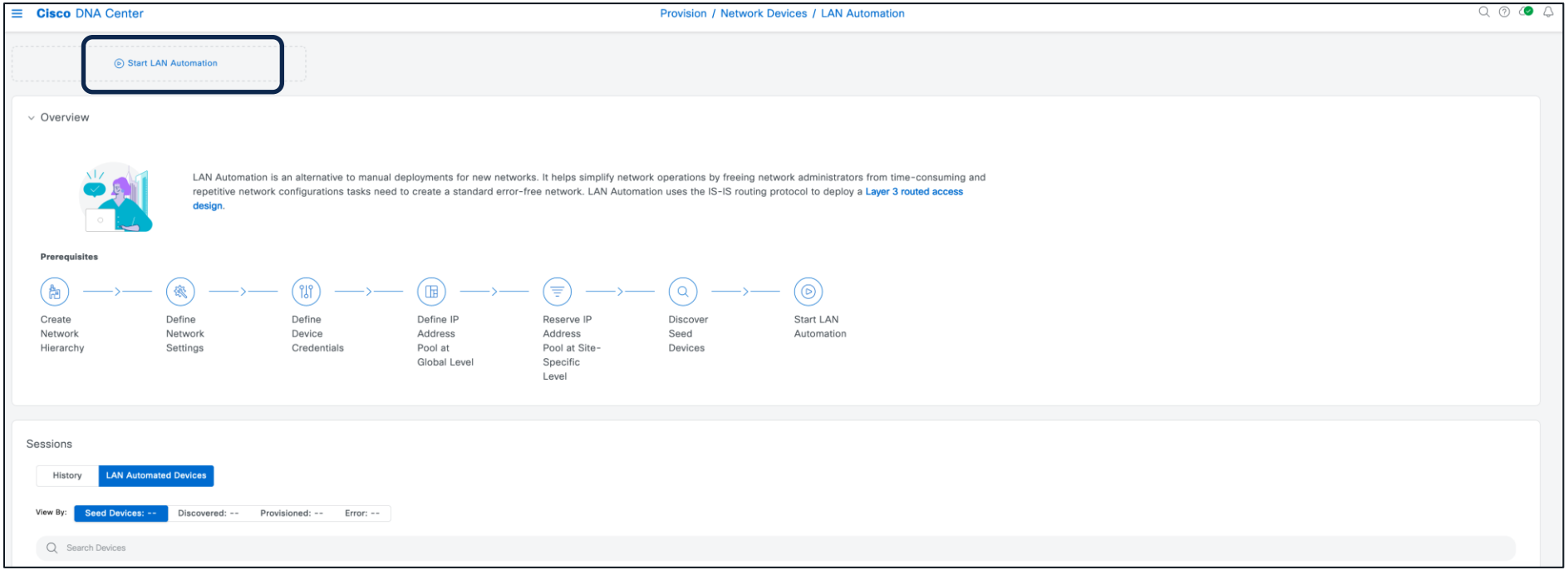
Underlay Infrastructure: LAN Automation Automation



LAN Automation has a new home

Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation Automation

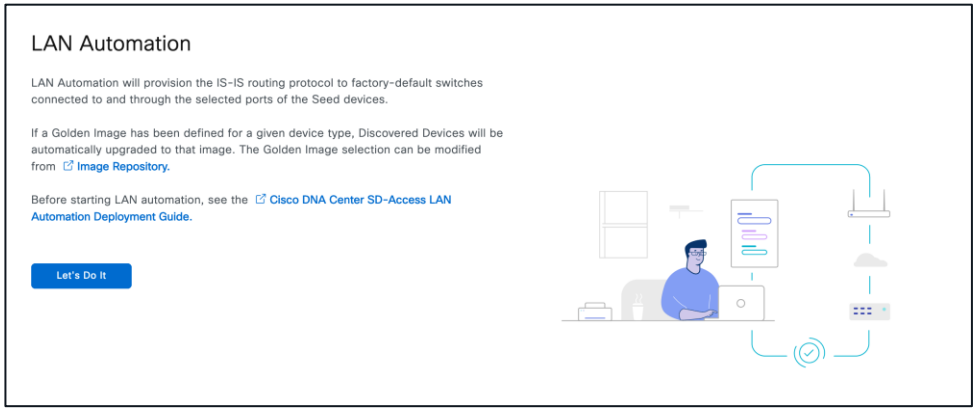


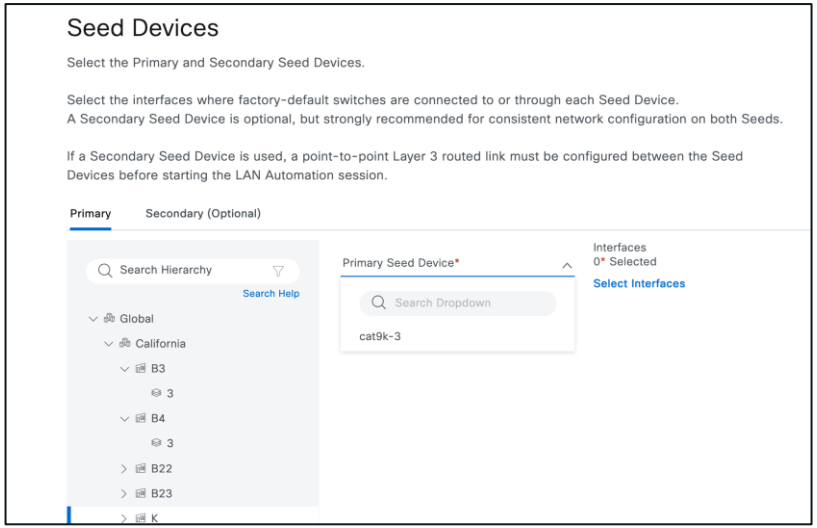
New LAN Automation Landing page

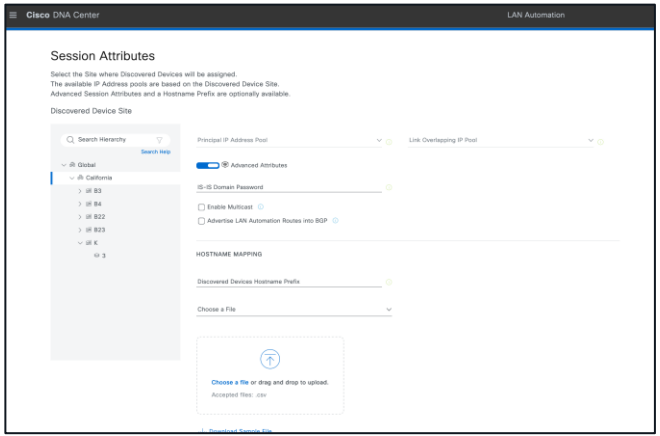
Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation Automation

For Your Reference

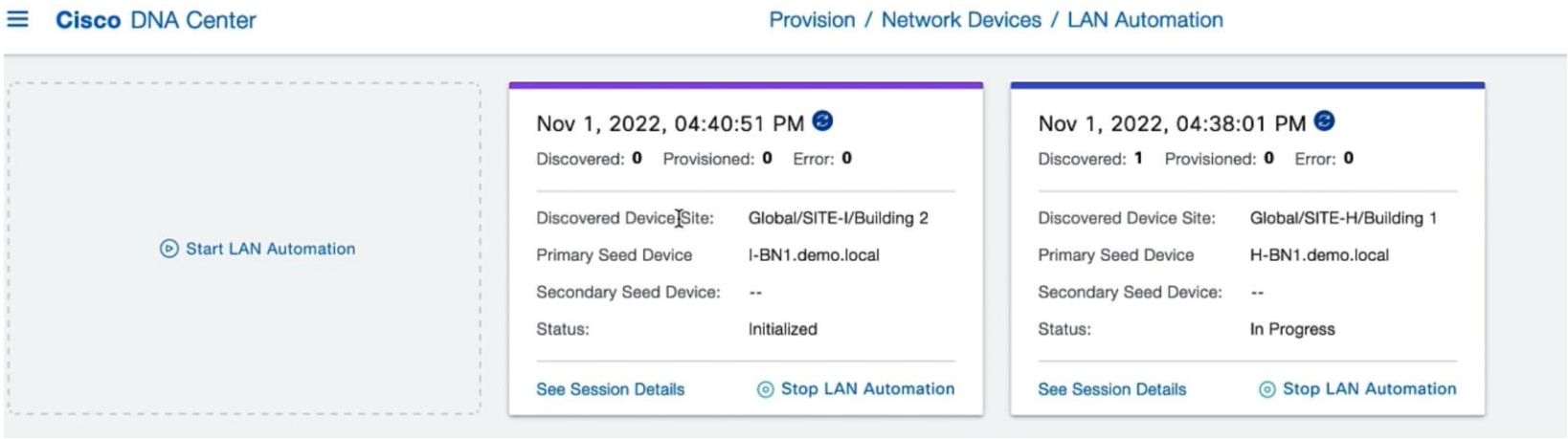






Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation Automation

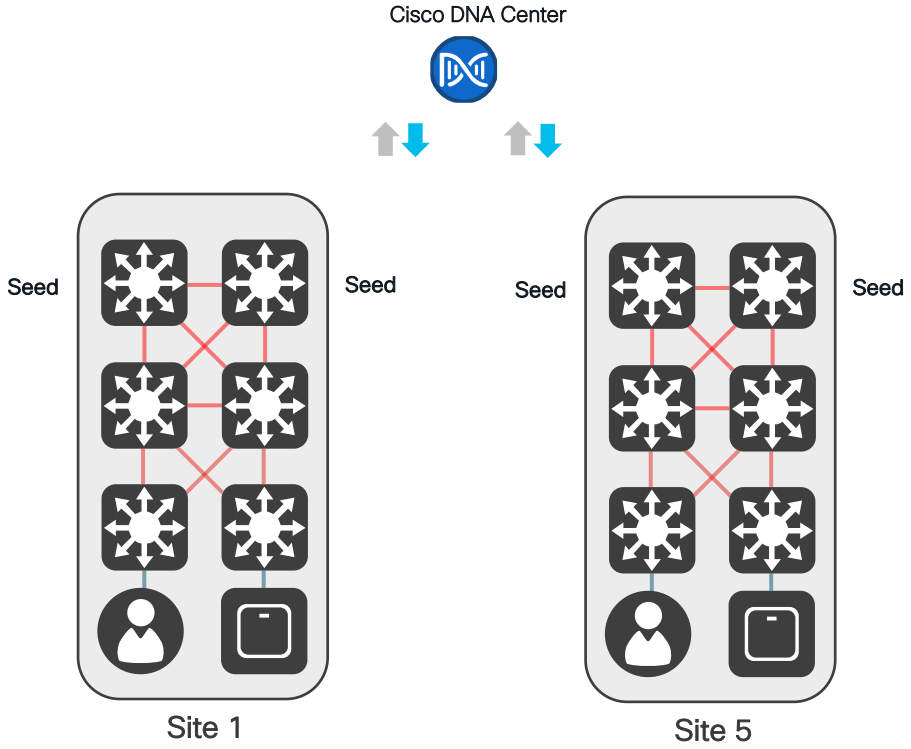


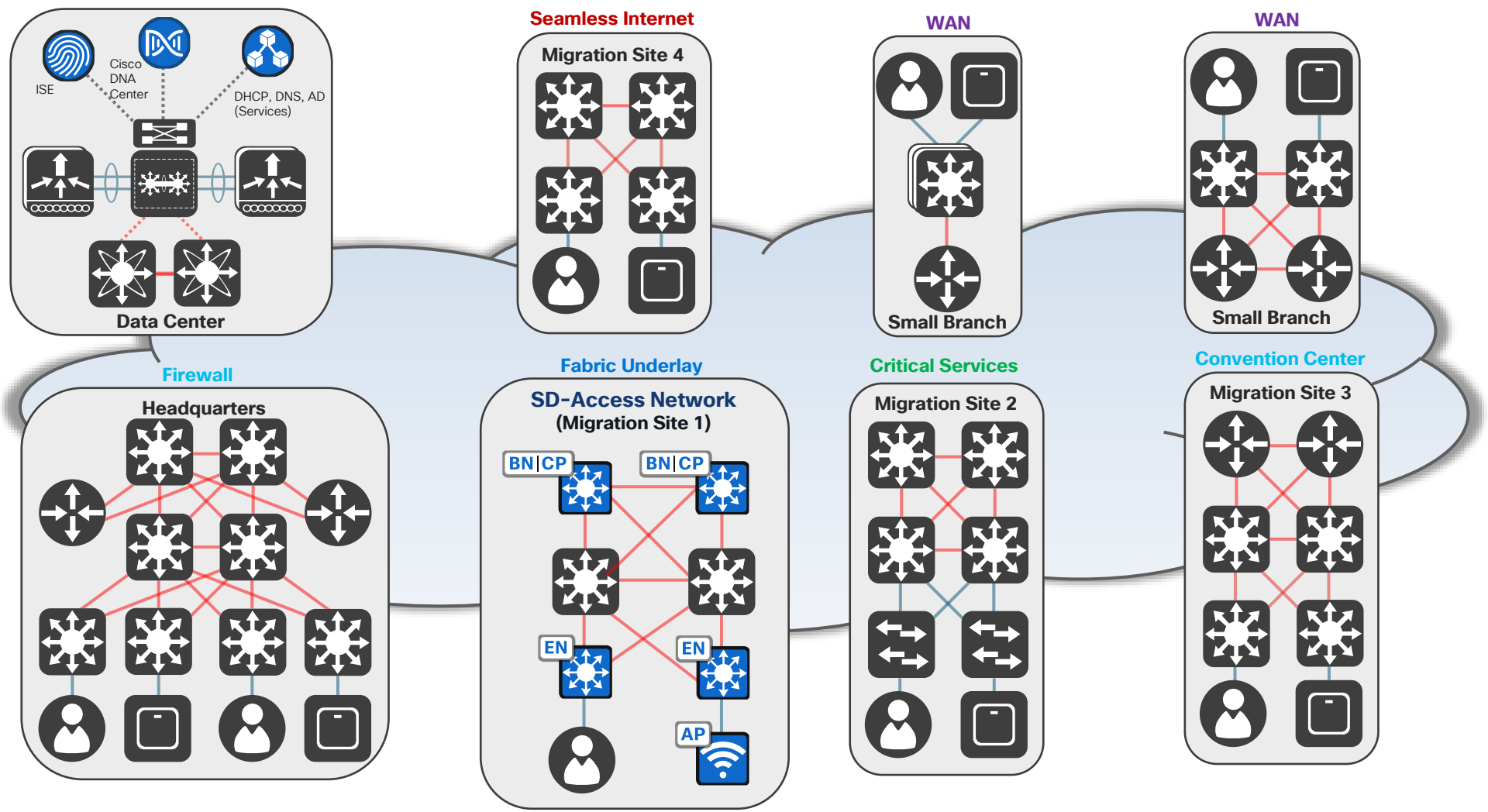
We can have 5 simultaneous Lan automation sessions with one session per site.

Fabric Network Infrastructure

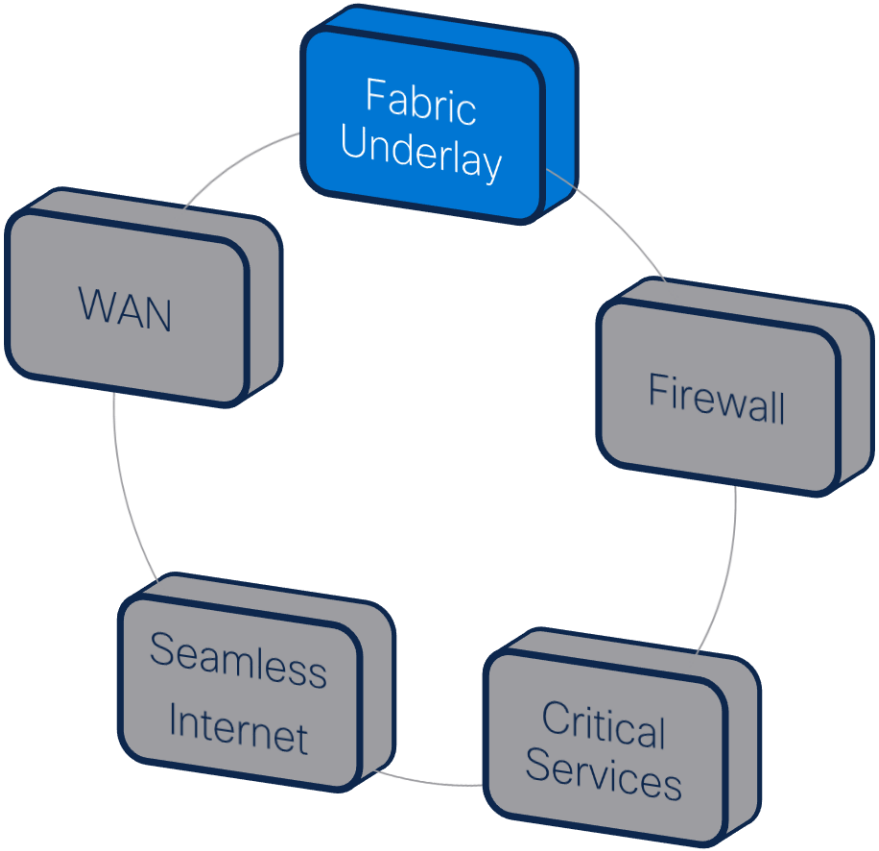
Underlay Infrastructure: LAN Automation Enhancements

- Simultaneous LAN Automation sessions is supported from Cisco DNA Center release 2.3.5.x .
- Simultaneous LAN Automation sessions:
  - This feature will allow customers to initiate up to 5 multiple LAN Automation sessions with one session per site.
  - Zero Touch onboarding of PNP ready switches at 5 different sites.
  - Dedicated LAN Automation landing page with a new workflow to initiate LAN Automation.
- As part of LAN Automation enhancements, user can Add or Delete L3 links which helps customers to better manage links through customization.
- Deleting is permitted on an existing link that have previously been configured by LAN Automation.





Progress Chart



Fabric Constructs

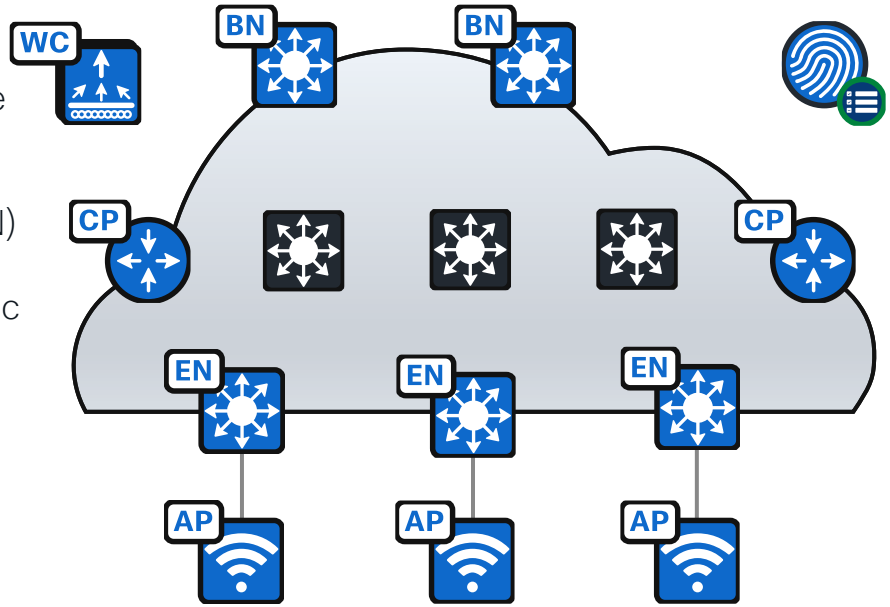
Fabric Constructs

Fabric Sites – A Closer Look

For Your Reference

Fabric Sites are an independent fabric area with a unique set of network device.

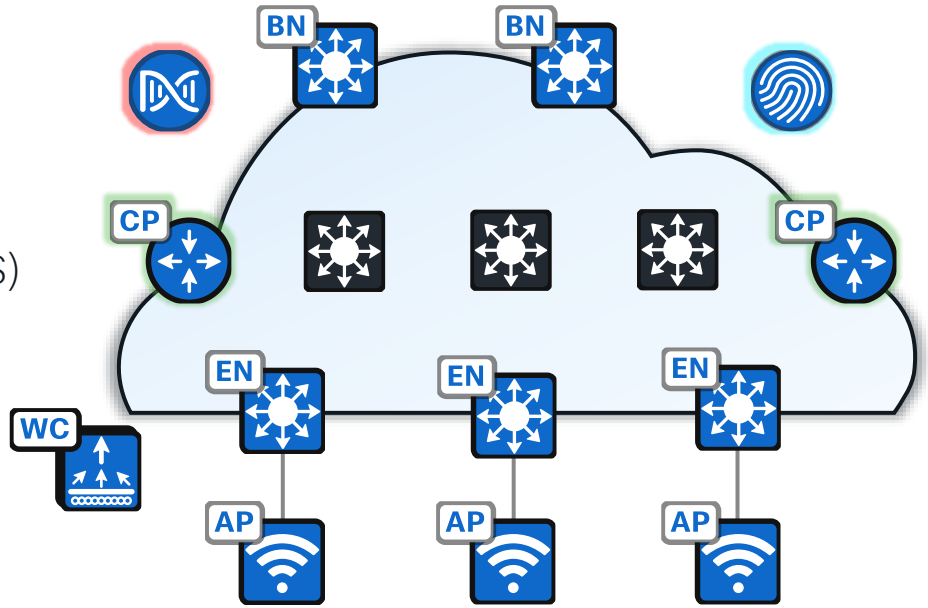
- Contains Control Plane Nodes, Border Nodes, and Edge Nodes.
- Contains Fabric WLC and ISE Policy Service Node (PSN)
- The Border Node is the ingress and egress for the Fabric Site.
- May cover a single location, multiple locations, or a subset of a location (floor of a building)



For Your Reference

SD-Access Fabric
Planes of Operation

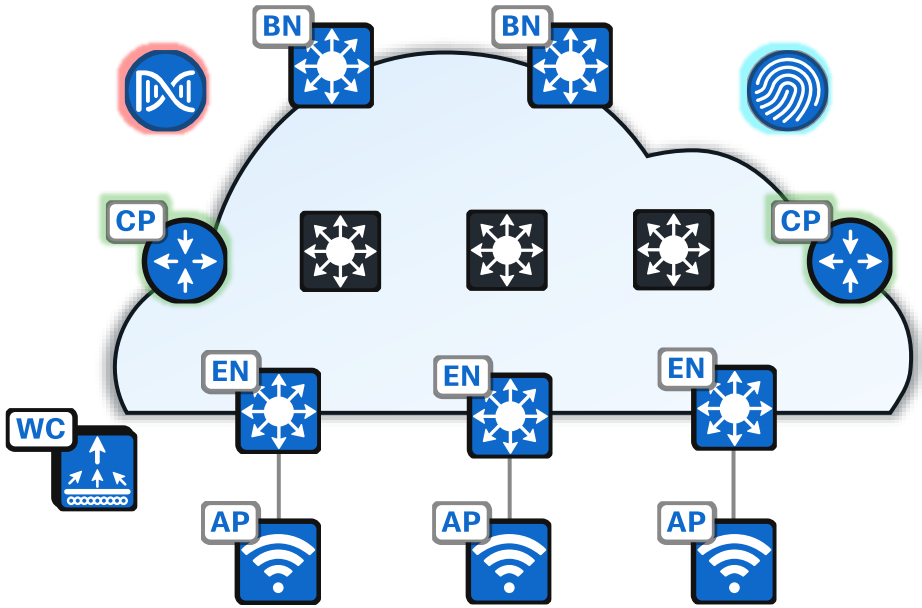
1. Management Plane with Cisco DNA Center
2. Control Plane based on LISP
3. Data Plane based on VXLAN
4. Policy Plane based on Cisco Trustsec (CTS)



For Your Reference

SD-Access Fabric
LISP Control Plane

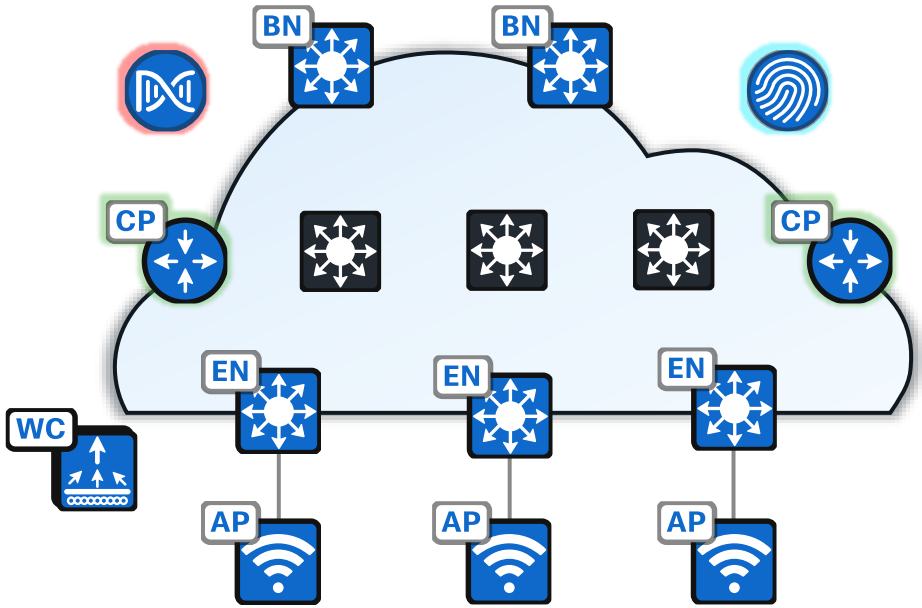
- Fabric Nodes use LISP as a control plane protocol for Endpoint Identifier (EID) and Routing locator (RLOC) information.
- Control Plane Node acts as a LISP Map-Server and LISP Map-Resolver for EID-to-RLOC mappings
- Edge Nodes and Internal Border Node devices register EIDs to the Map Server.
- External Border Node acts as PXTR (LISP Proxy Tunnel Router) to provide a default gateway when no mapping exists.



For Your Reference

SD-Access Fabric
VXLAN Data Plane

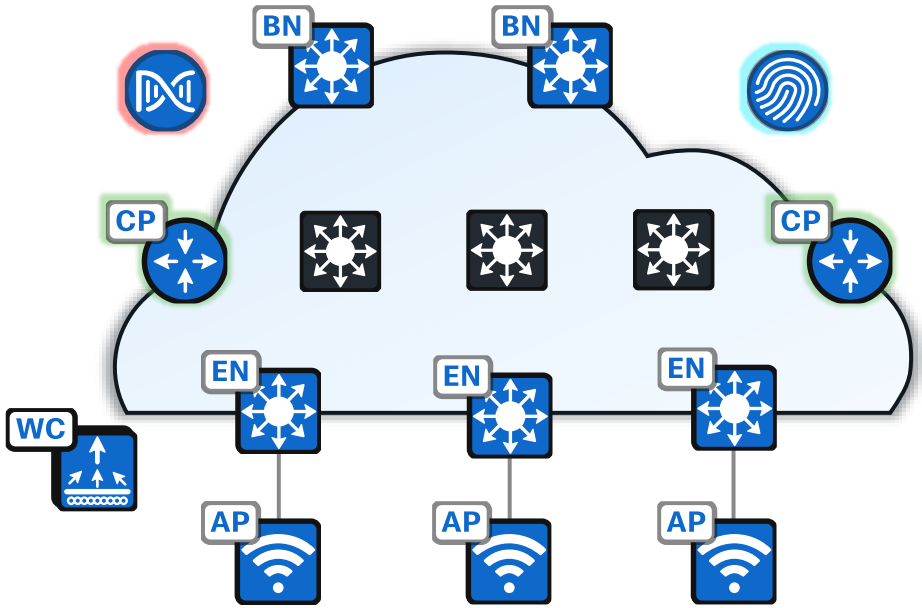
- Fabric Nodes use VXLAN as the data plane protocol which supports both Layer 2 and Layer 3 overlays.
- This because VXLAN encapsulation preservers the original Ethernet header.
- VXLAN header contains VNID (VXLAN Network Identifier) field which allows up to 16 million VNIs.
- VXLAN header also has Group Policy ID for Scalable Group Tags (SGTs) allowing 64,000 SGTs.



For Your Reference

SD-Access Fabric
Cisco TrustSec Policy Plane

- Security Group Tags (SGT) are a logical construct based on the user and device context.
- ISE dynamically assign SGTs to the users and devices connecting to the network Fabric.
- Fabric Nodes add SGTs to the encapsulation of data communication between users and devices.
- Edge Nodes enforce the SG-ACL policies and contracts for the SGTs they protect locally.



Cisco SD-Access Borders

Cisco SD-Access Border

Border Nodes – A Closer Look

- There are three (3) ways to configure a Border Node.

Rest of the Company (Internal-Only)

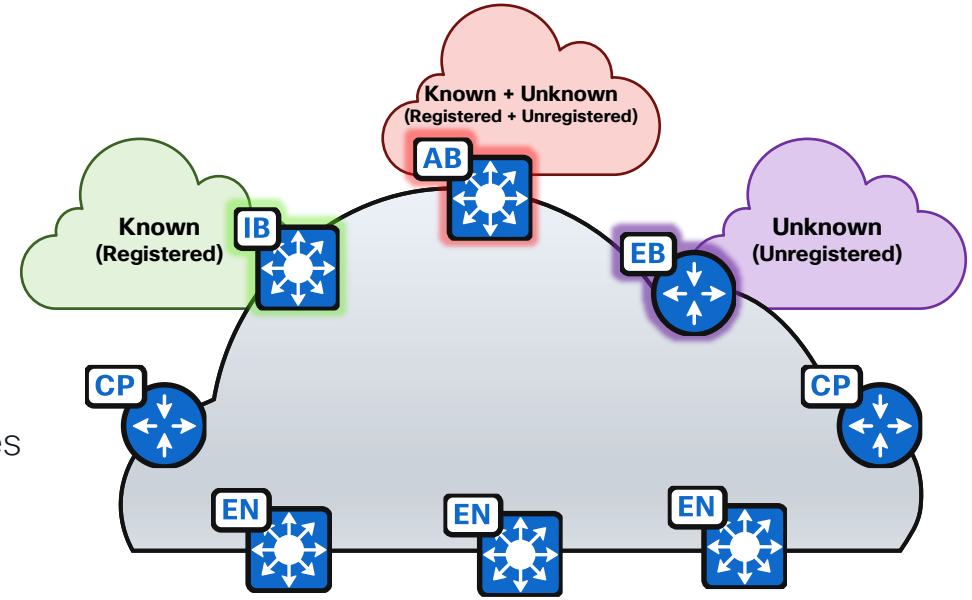
- Used for *Known* (registered) routes

Outside World (External-Only)

- Used for *Unknown* (unregistered) routes

Anywhere (Internal & External)

- Used to access *Known* and *Unknown* routes
  - Registered and unregistered

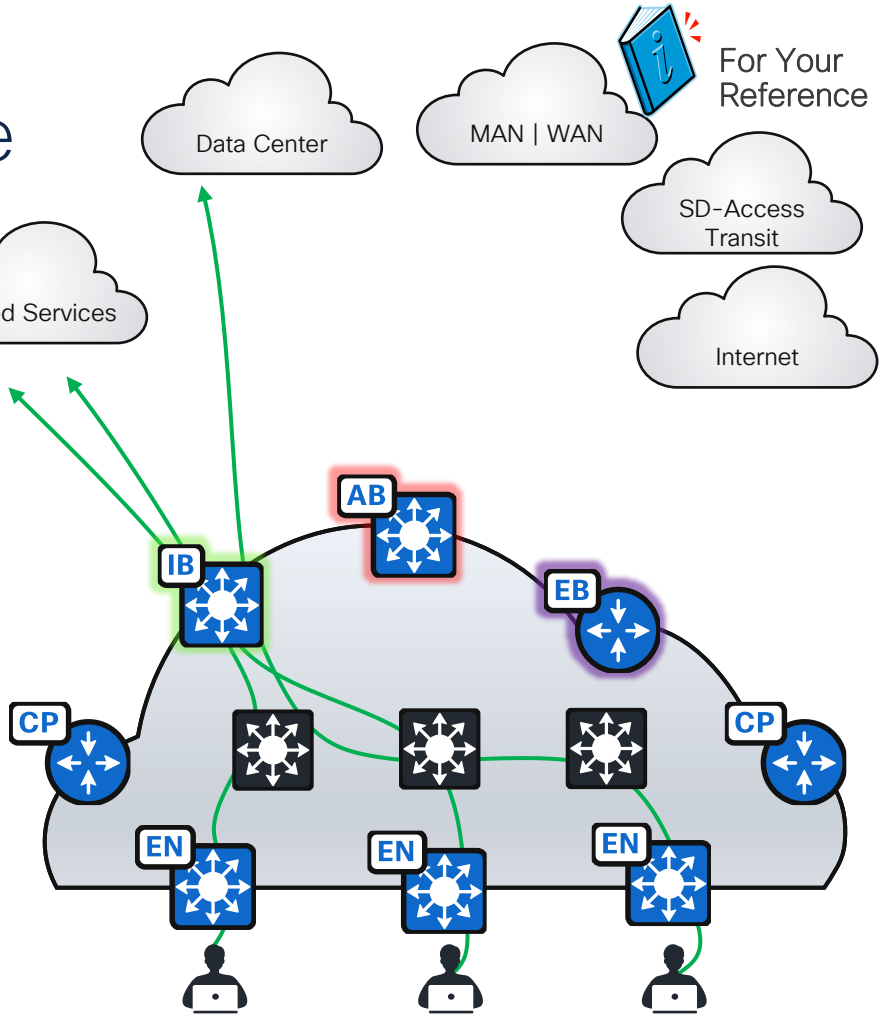


Internal Border

Internal-Only Border Node

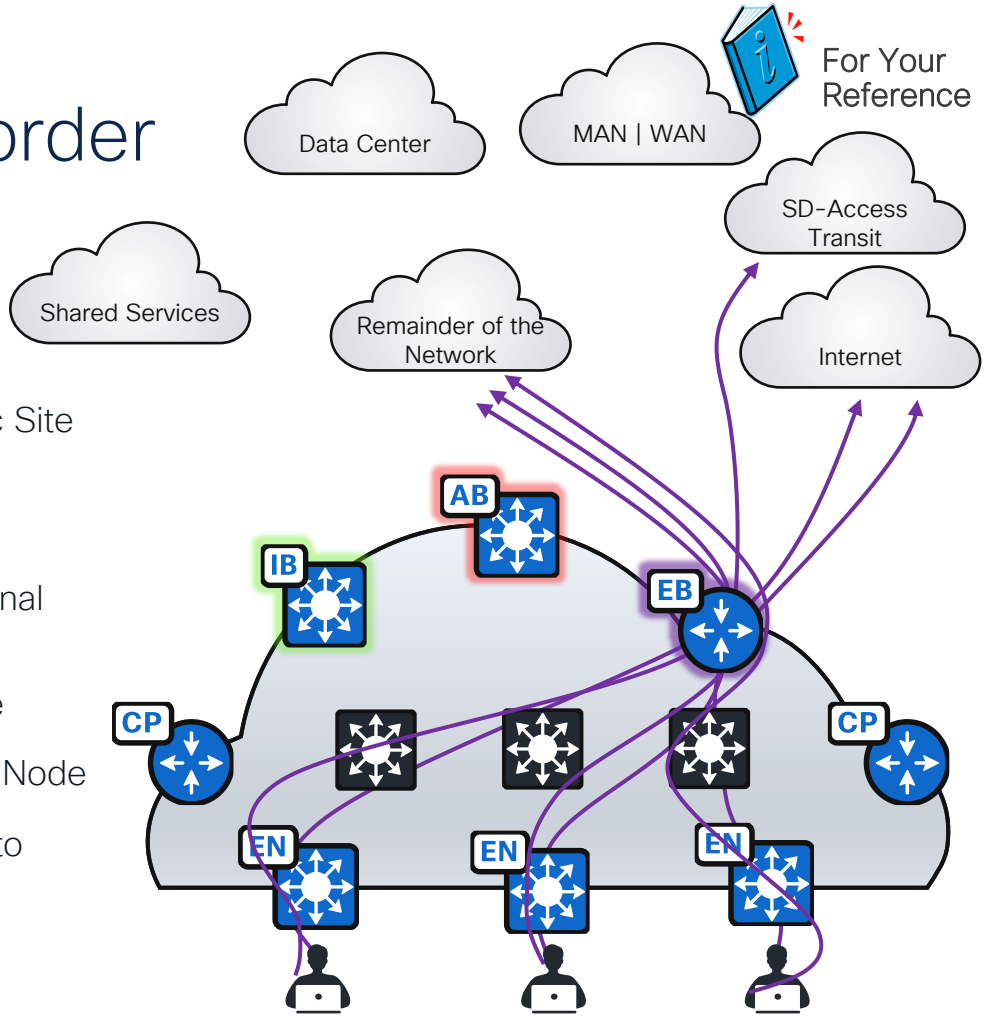
Internal-Only Border

- Connects the Fabric to *known (registered)* networks
- **Registered** networks generally include WAN, Data Center, Shared Services, etc.
- Advertises (exports) Fabric prefixes to the external domains
- **Imports** external prefixes into Fabric Site and registers them with the Control Plane Node



External Border

SD-Access External Border



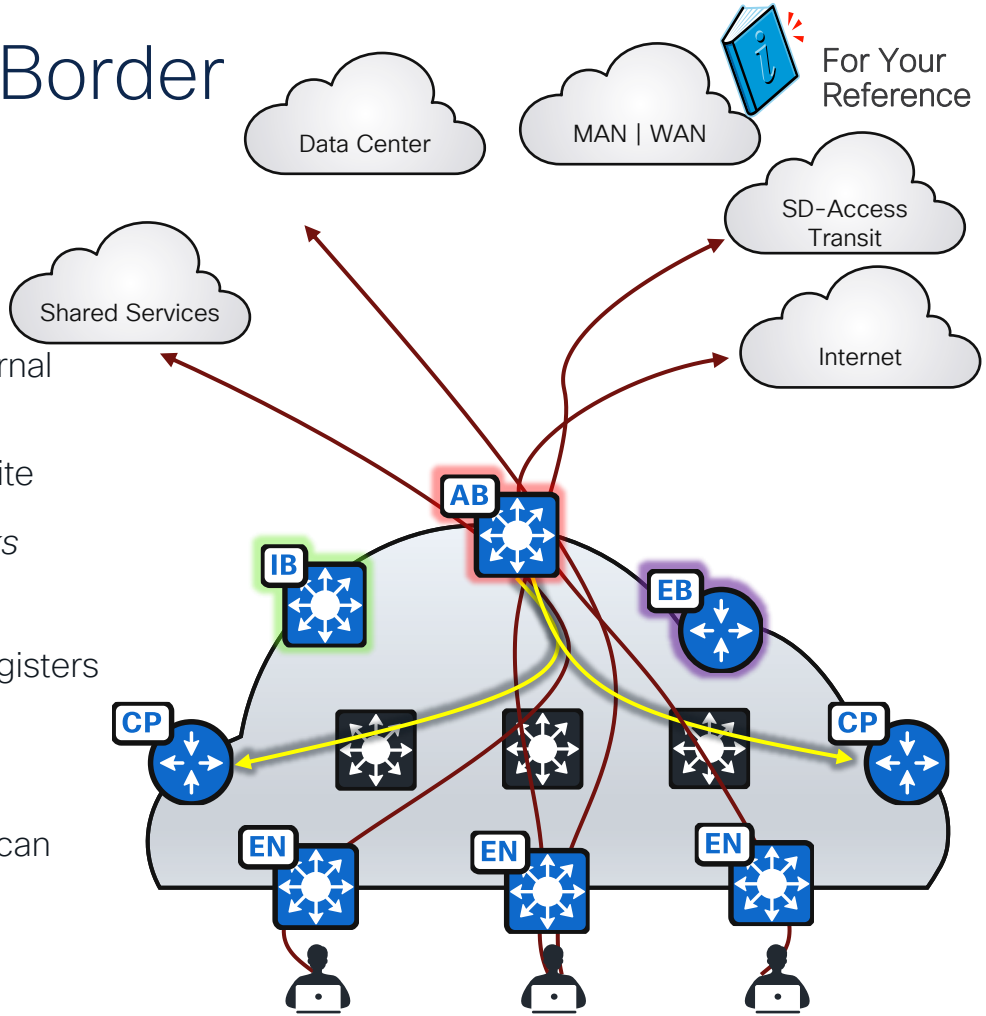
External-Only Border

- Fabric *Gateway of Last Resort*
  - Provides a default egress point for the Fabric Site
- Connects the Fabric to *unknown (unregistered)* networks
- Advertises (exports) fabric prefixes to the external domains
- Does not import external prefixes into Fabric Site
- Does not register prefixes with the Control Plane Node
- Border Nodes must have *External* functionality to connect to an SD-Access Transit.

Anywhere Border

cisco Live!

SD-Access Anywhere Border



Anywhere Border

- Advertises (exports) Fabric prefixes to the external domains
- Provides a default egress point for the Fabric Site
- Connects to both *known* and *unknown networks*
  - *Registered and unregistered networks*
- Imports external prefixes into Fabric Site and registers them with the Control Plane Node

- As a Border Node with *External* functionality, it can connect to an SD-Access Transit.

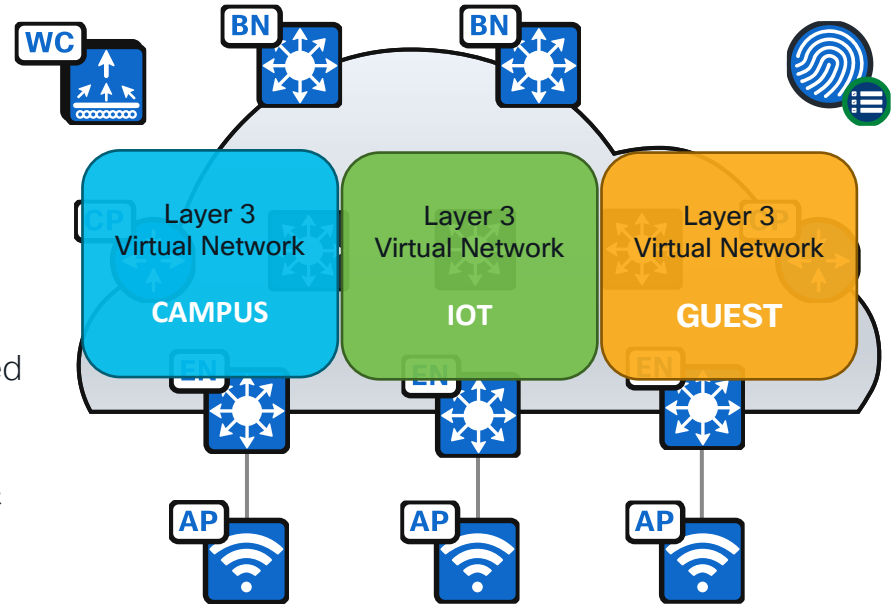
Fabric Constructs

Layer 3 Virtual Network – A Closer Look

For Your Reference

Layer 3 Virtual Networks maintain a separate Routing Table for each instance.

- Provides macro-segmentation (Routing Table Separation)
- Control Plane Node uses Instance ID to maintain separate VRF topologies
- Fabric Nodes add a VNID to the Fabric encapsulation
- Endpoint ID prefixes (Host Pools) are routed and advertised within a Virtual Network
- Uses standard *vrf definition* configuration, along with RD & RT for remote advertisement on the Border Node



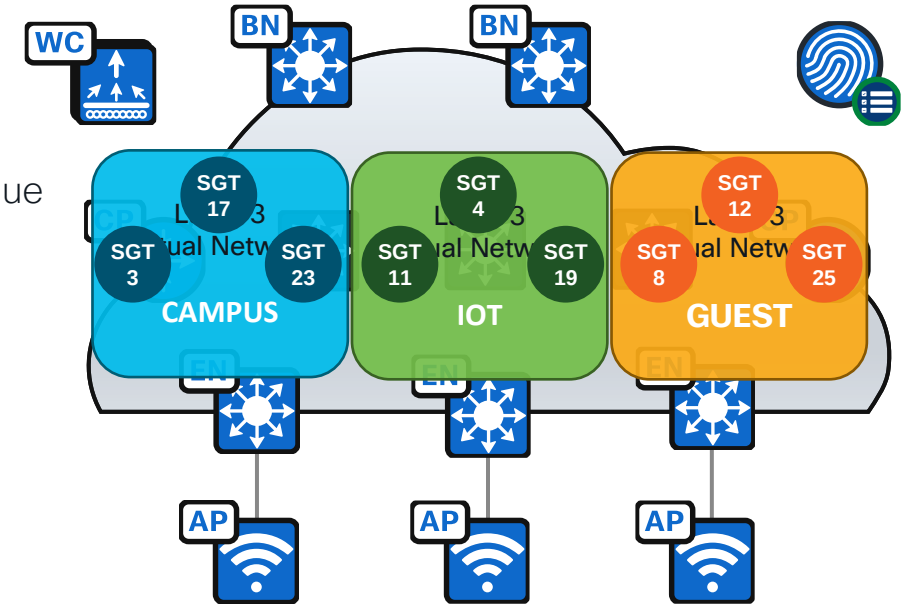
Fabric Constructs

Security Group Tags (SGTs) – A Closer Look

For Your Reference

Security Group Tag is a policy object to group users, devices, and endpoints

- Provides micro-segmentation (Segmentation within a Virtual Network)
- Nodes use Security Groups to ID and assign a unique Security Group Tag (SGT) to Endpoints
- Nodes add an SGT to the Fabric encapsulation
- SGTs are used to manage address-independent Group-Based Policies
- Edge Nodes use SGT to enforce local Scalable Group ACLs (SGACLs)



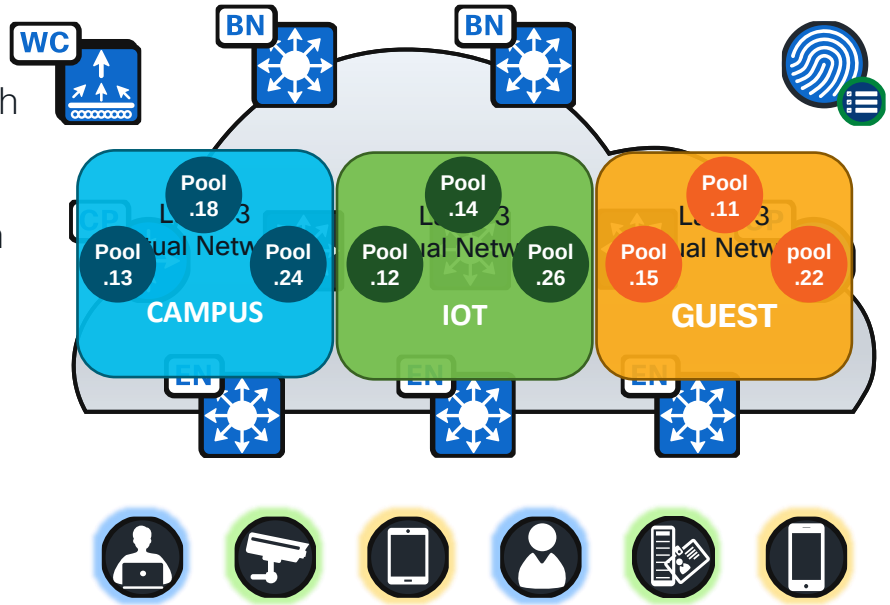
Fabric Constructs

Host Pools – A Closer Look

For Your Reference

Host Pools provide basic IP functions necessary for attached Endpoints

- Edge Nodes use a Switch Virtual Interface (SVI), with IP Address /Mask, etc. per Host Pool
- Fabric uses Dynamic EID mapping to advertise each Host Pool (per Instance ID)
- Fabric Dynamic EID allows Host-specific (/32, /128 or MAC) advertisement and mobility
- Host Pools can be assigned Dynamically (via Host Authentication) and/or Statically (per port)



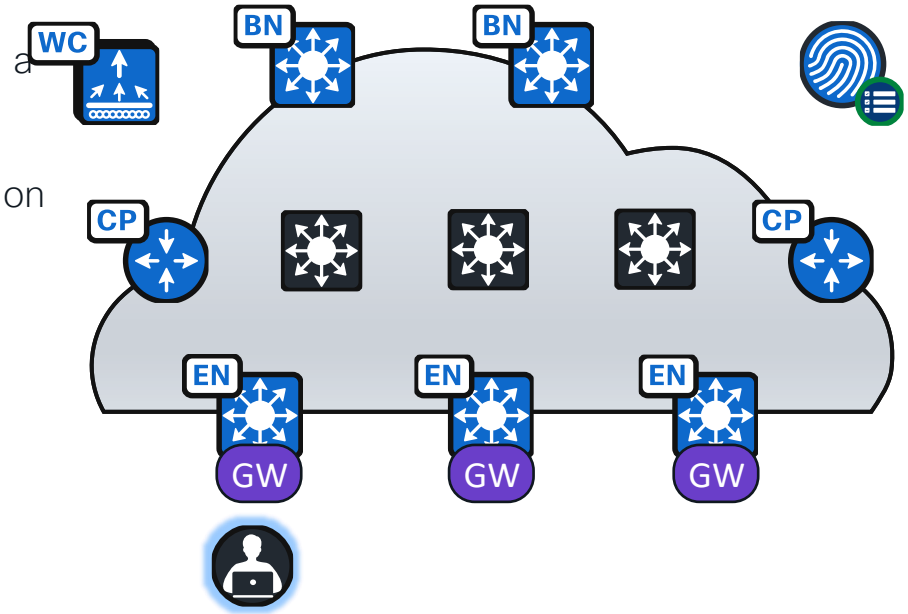
Fabric Constructs

Anycast Gateway – A Closer Look

For Your Reference

Anycast Gateway provides a Layer 3 Default Gateway for IP capable endpoints.

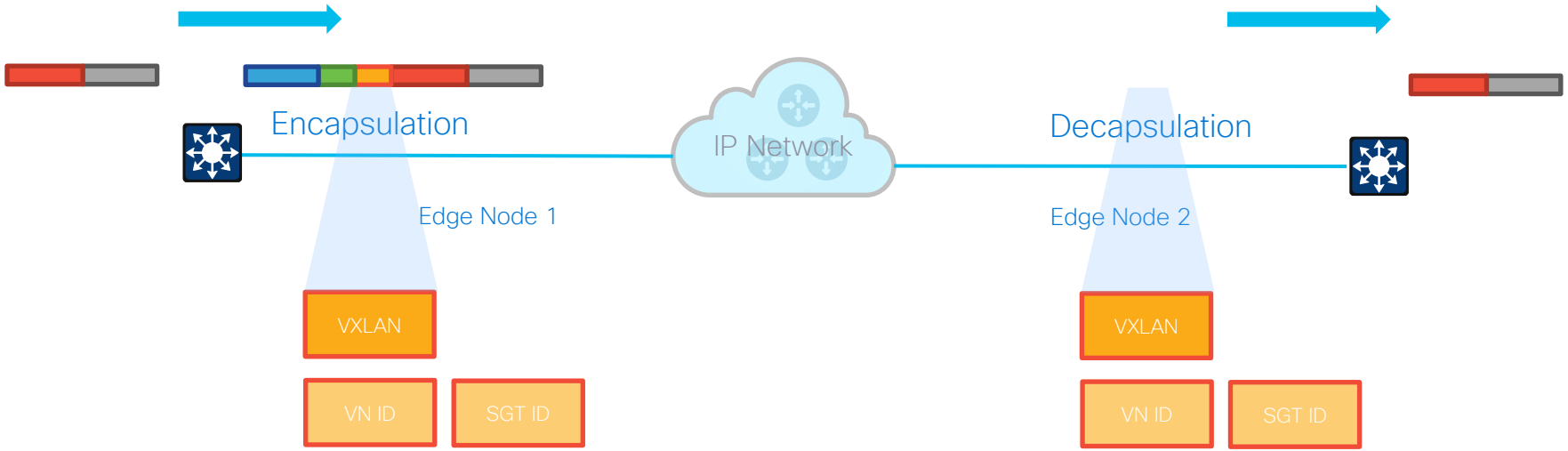
- Similar principle and behavior to HSRP / VRRP with a shared “Virtual” IP and MAC address.
- The same Switch Virtual Interface (SVI) is present on EVERY Edge Node and uses the the SAME IP and MAC address.
- Control-Plane with Fabric Dynamic-EID mapping maintains the Host-to-Edge-Node relationship.
- When a Host moves from Edge Node 1 to Edge Node 2, it does not need to change its Default Gateway. ☺



Propagation using VXLAN

VN and SGT in VXLAN-GPO Encapsulation

For Your Reference



Classification
Static or Dynamic VN and SGT assignments

Propagation
Carry VN and Group context across the network

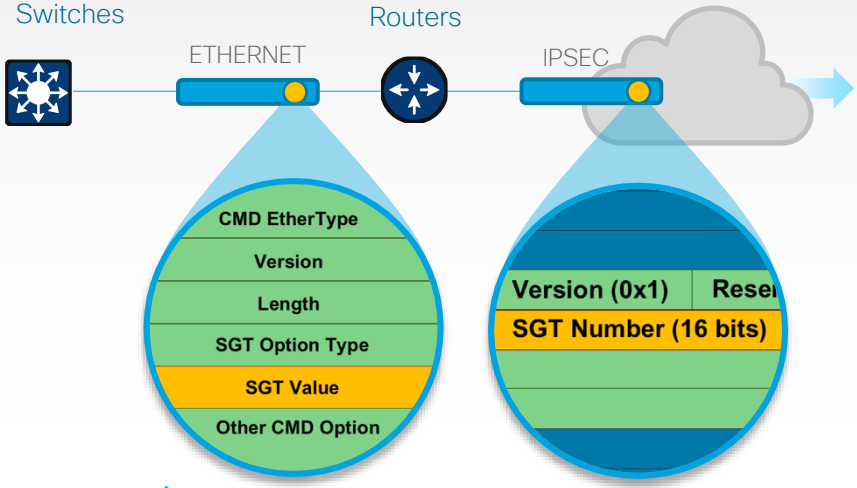
Enforcement
Group Based Policies ACLs, Firewall Rules

Propagation Methods

For Your Reference

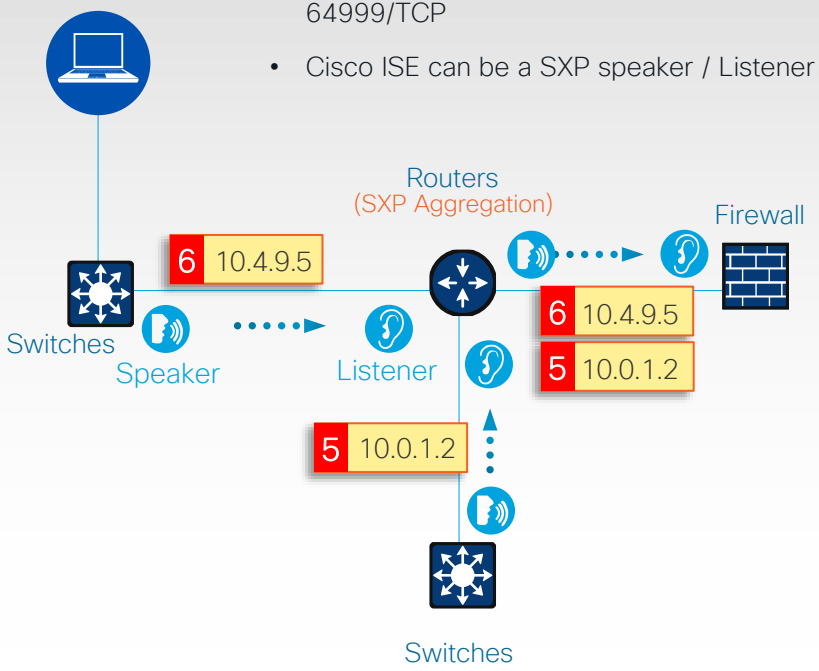
Inline Methods

- **Ethernet Inline Tagging:** (EtherType:0x8909) 16-Bit SGT encapsulated within Cisco Meta Data (CMD) payload.
- **IPSec / L3 Crypto:** Cisco Meta Data (CMD) uses protocol 99, and is inserted to the beginning of the ESP/AH payload.
- **VXLAN:** SGT (16 bit) inserted into Segment ID of VXLAN Header



SGT Exchange Protocol (SXP)

- IP-to-SGT binding exchange over 64999/TCP
- Cisco ISE can be a SXP speaker / Listener



Policy Enforcement on Firewall

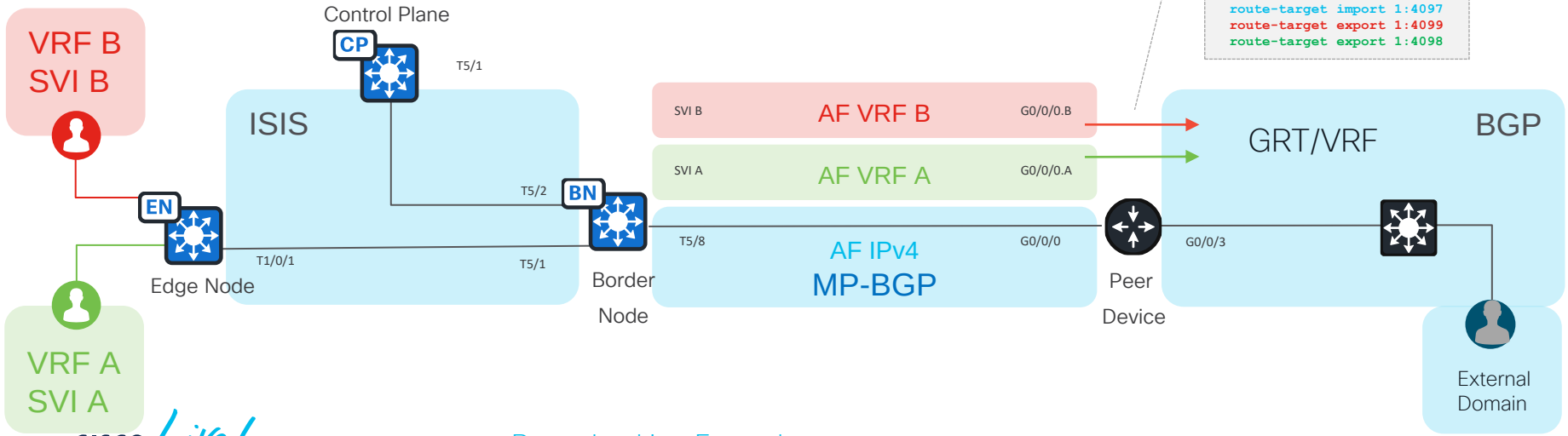
RECAP

Border Deployment Options

Shared Services (DHCP, AAA, etc..) with Border

Cisco SD-Access Border connecting External Domain with existing Global Routing Table should use a Peer Device with MP-BGP & VRF import/export.

```
ip vrf USERS
 rd 1:4099
 route-target export 1:4099
 route-target import 1:4099
 route-target import 1:4097
!
ip vrf DEFAULT_VN
 rd 1:4098
 route-target export 1:4098
 route-target import 1:4098
 route-target import 1:4097

ip vrf GLOBAL
 rd 1:4097
 route-target export 1:4097
 route-target import 1:4097
 route-target export 1:4099
 route-target export 1:4098
```



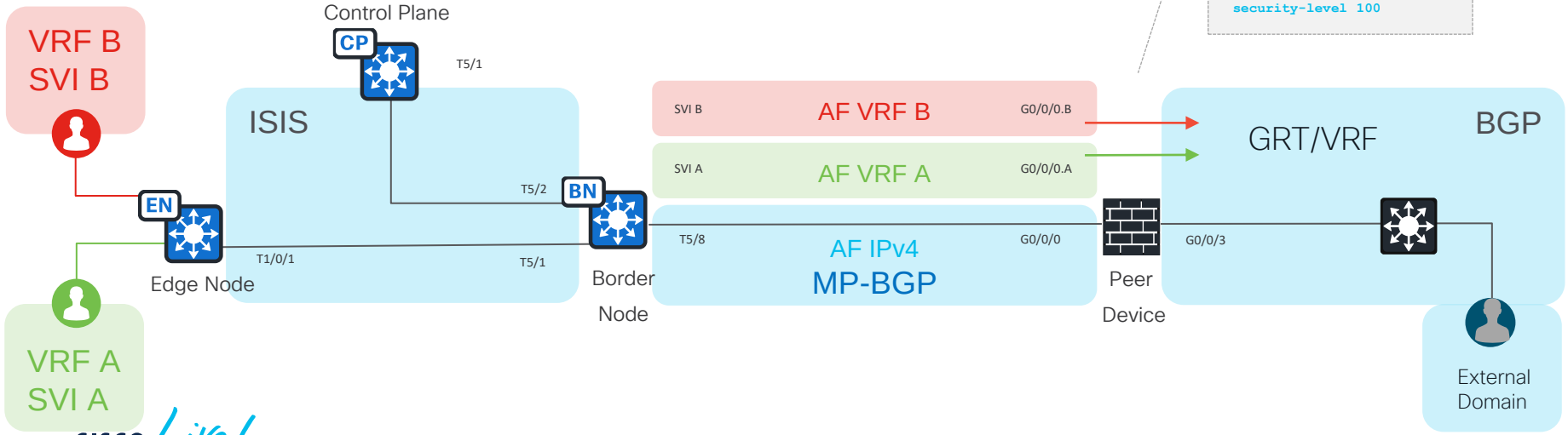
Route Leaking Example

Border Deployment Options (Peer Device Firewall)

Shared Services (DHCP, AAA, etc..) with Border

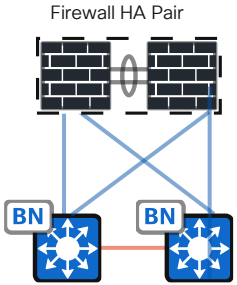
Cisco SD-Access Border connecting External Domain with existing Global Routing Table could use a “Peer Device Firewall” with multiple Zones/Sub-Interfaces

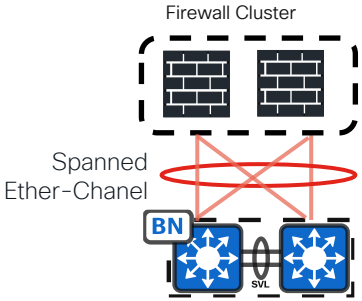
```
int gi0/0/0.A
 vlan 101
 nameif A
 security-level 100
!
int gi0/0/0.B
 vlan 102
 nameif B
 security-level 100
!
int gi0/0/0
 nameif inside
 security-level 100
```

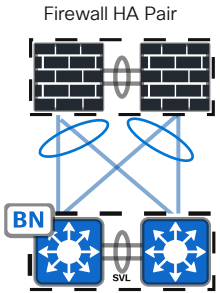


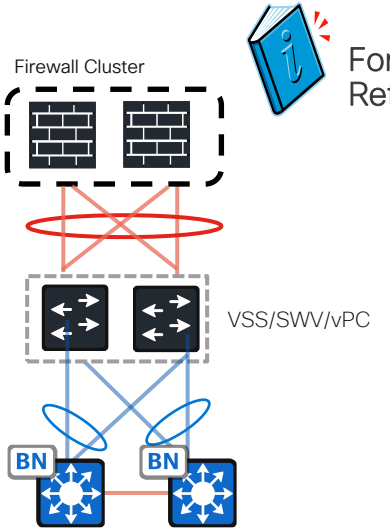
Border Deployment Options (Peer Device Firewall)

Sample Scenarios

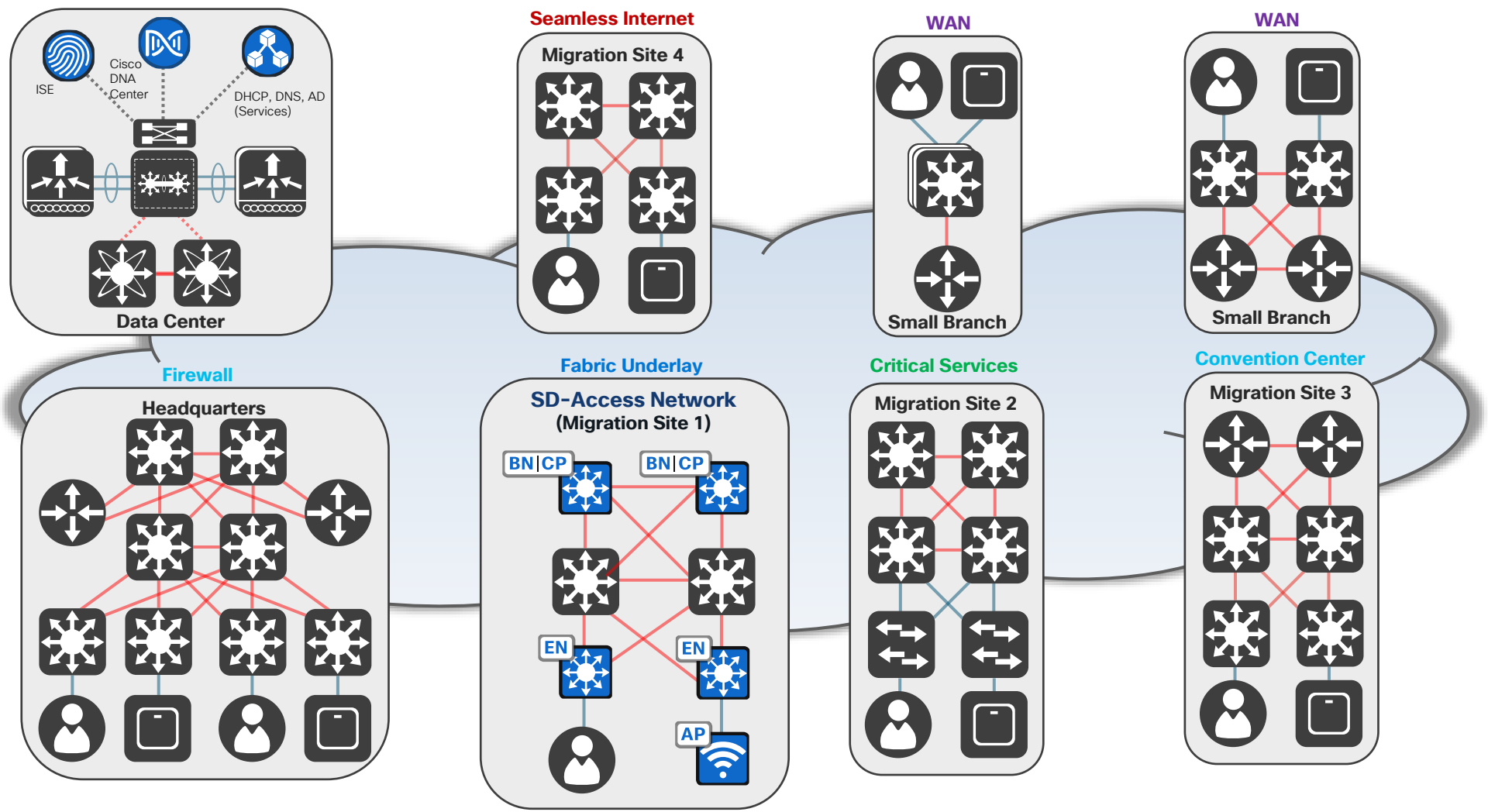








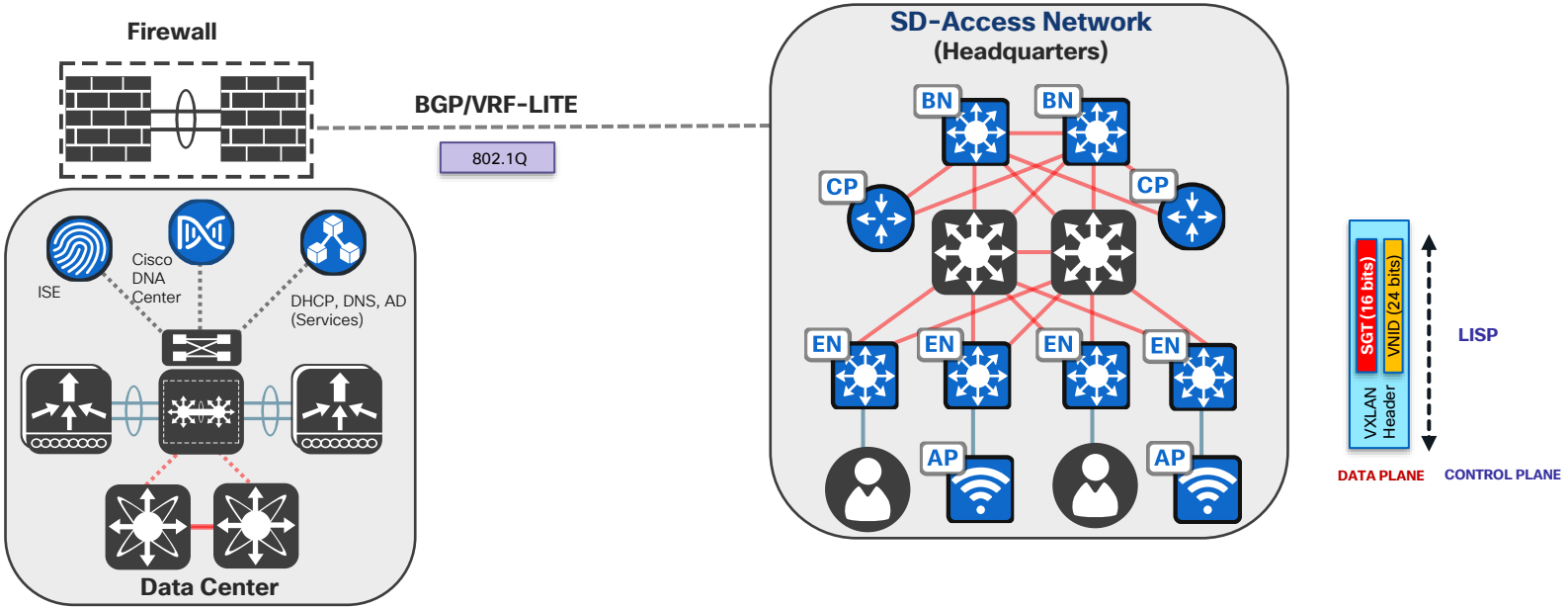
For More Information:
Cisco Secure Firewall and SDA Integration Deep Dive - BRKSEC-2845



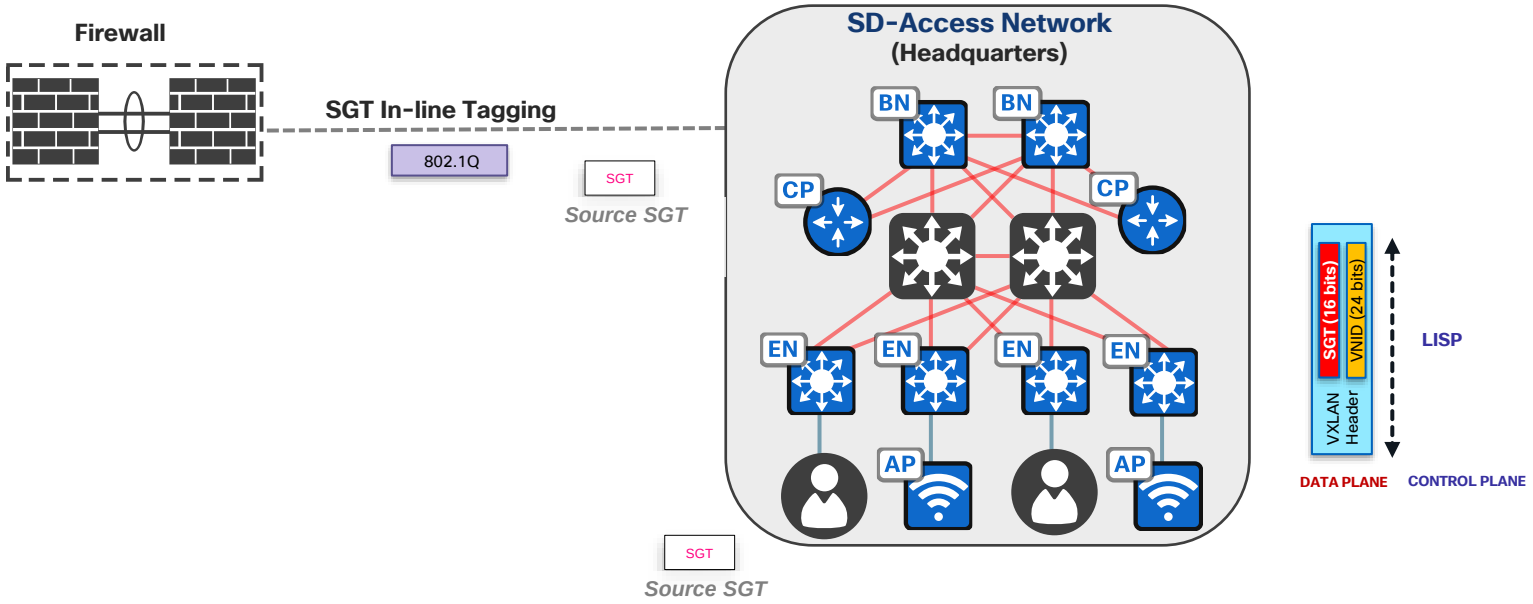
Cisco SD-Access

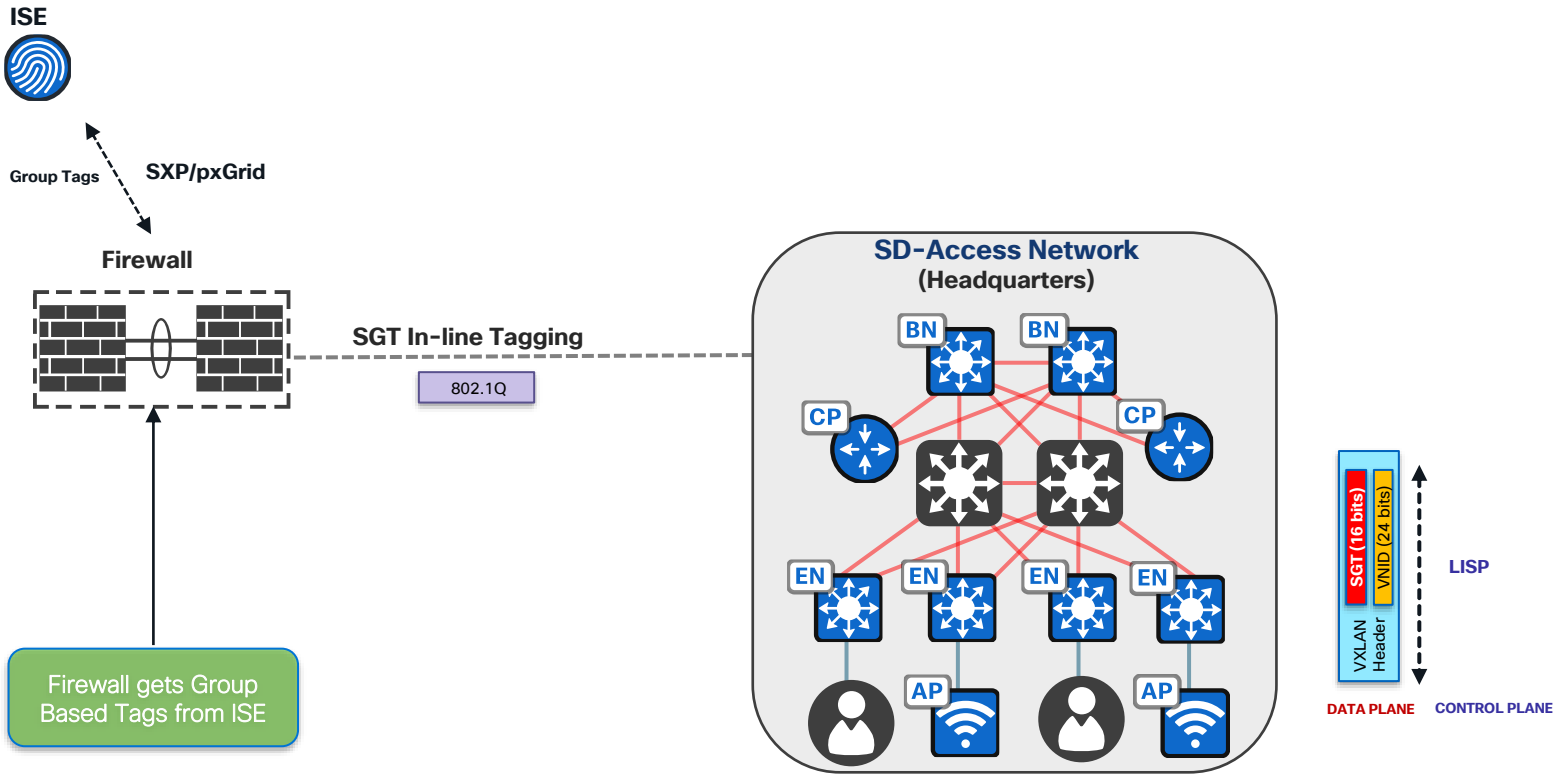
Firewall

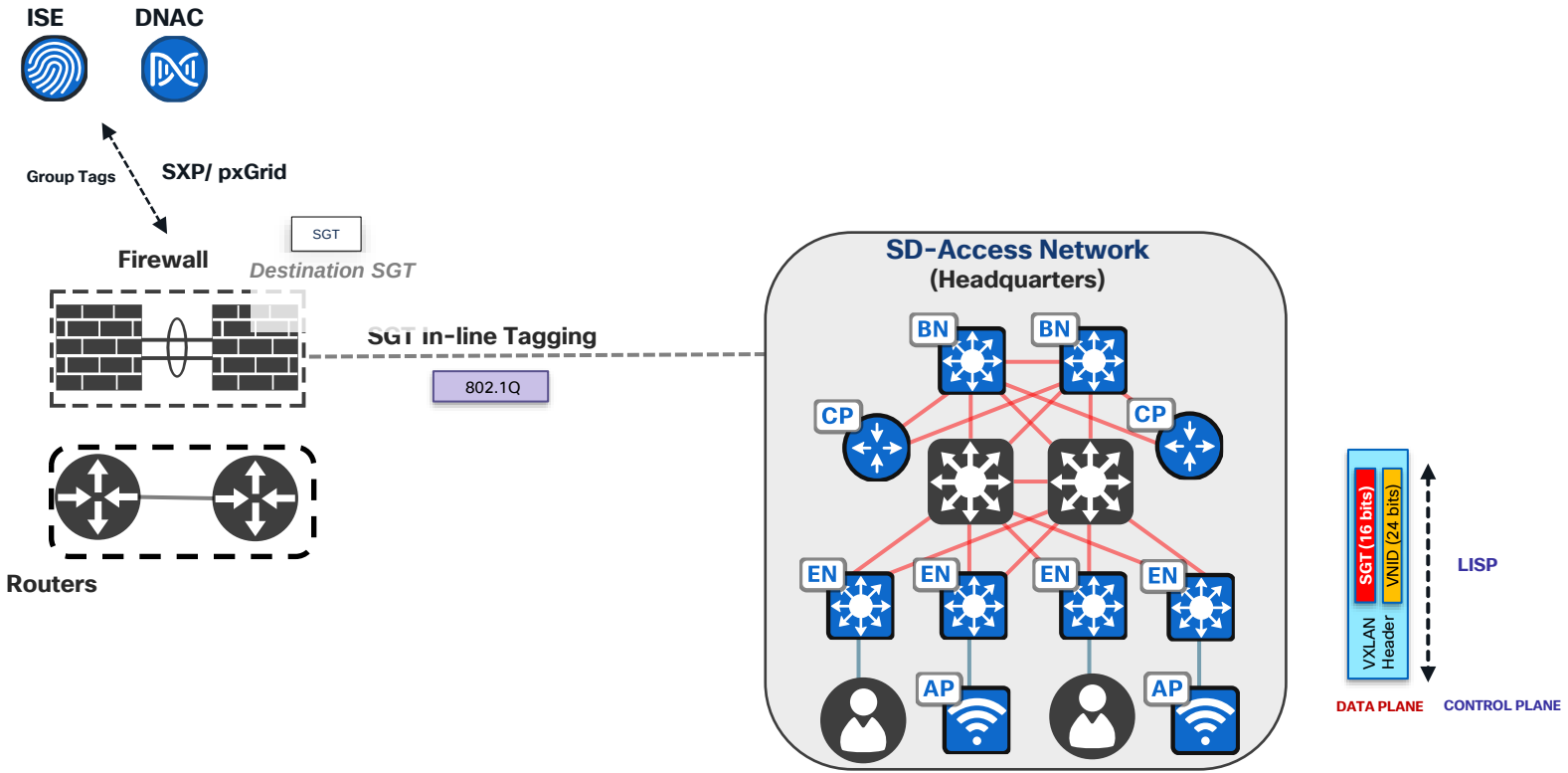
- Enforcement on Firewall
- Network access for vendors at Convention Center



- Recommended for designs requiring Stateful Inspection and Inter-VN policy
- Ideal for designs requiring audits adding logging capabilities.



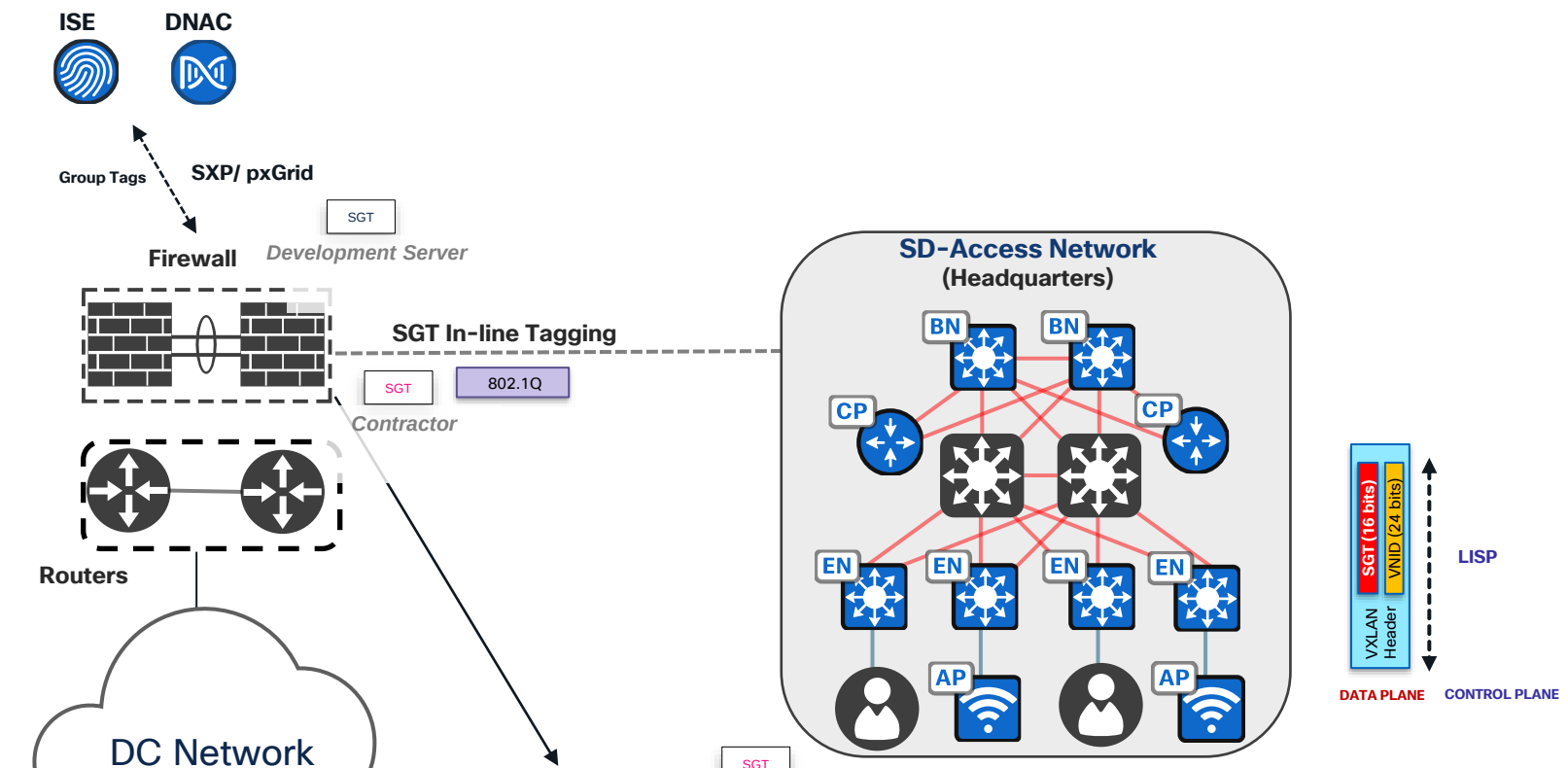




Cisco SD-Access

Policy Enforcement on Firewall

- Peer device may learn mappings from ISE via pxGrid (NGFW for e.g.) and SXP if the peer device is Router/Switch/ASA.
- If Destination Mappings Known by Peer device, then Enforce.
- Inter VN policy enforcement can be done on a Peer device such as a router/switch or a firewall like ASA/FTD
- SGT In-line tagging needs to enable on physical trunk on switches and sub-interfaces on Routers/Firewalls



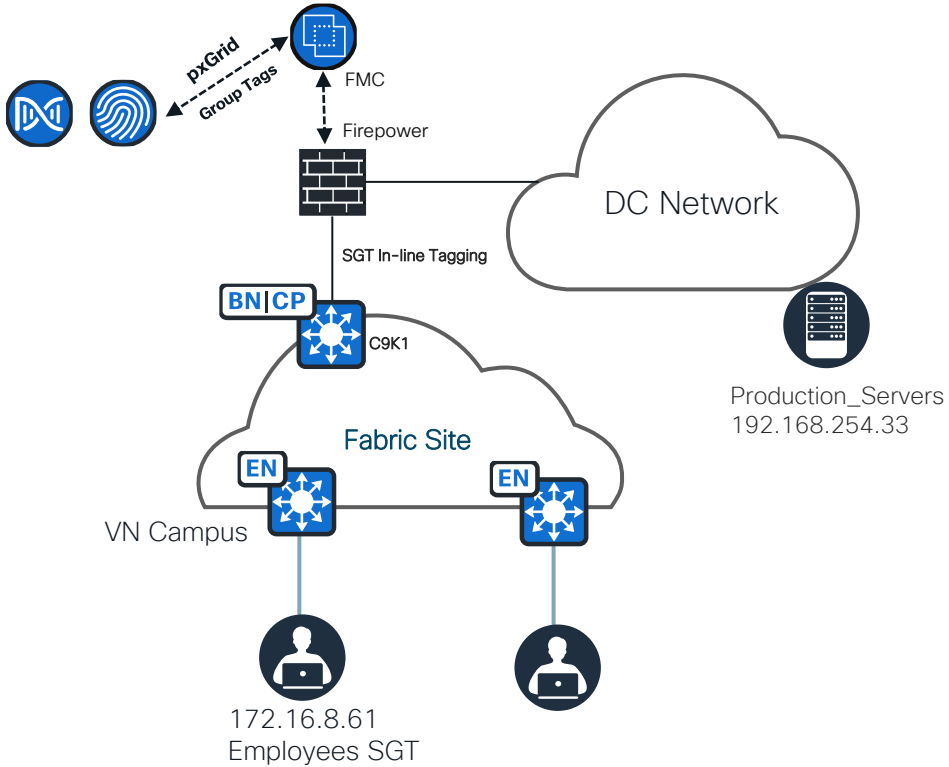
SGT

Contractor

SGT	DGT	Contract
Contractor	Development Server	Deny
Developer	Development Server	Permit
Employee	Development Server	Allow Web

Policy Enforcement on Firewall Demo

Policy Enforcement on Firewall Demo



FW SGT Propagation Use-Cases

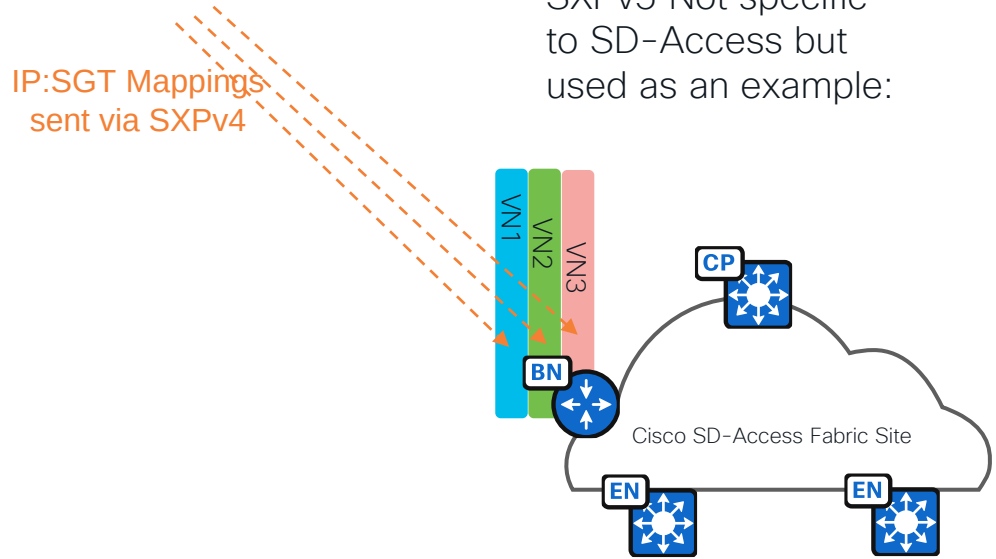
Key Take Away

Inline Tagging	Control Plane Propagation	Control Plane Propagation & Inline Tagging – Recommended
• Scalable Inter-VN policies with source SGT criteria only • Appropriate for firewall as a Cisco SD-Access peer device • If enforcing using Source SGTs, Ethernet Inline tagging can be implemented as it offers better scalability.	• Flexible Attribute-Based Inter-VN policy • Source and Destination SGT can be propagated via Control Plane propagation using pxGrid or SXP. • If enforcing using destination SGT , Control plane propagation methods such as pxGrid and SXP can be used. • Memory limits on the enforcement device needs to be considered	• A combination of both is scalable approach where user sends source SGTs via Inline and Destination SGT via pxGrid. • Minimal utilization of Firewall memory.

If SXP is your only choice ? - SXPv5

SXP Version 1	Initial SXP version supporting IPv4 binding propagation.
SXP Version 2	Includes support for IPv6 binding propagation and version negotiation.
SXP Version 3	Adds support for Subnet-SGT binding propagation. If speaking to a lower version, then the subnet will be expanded to individual IP-SGT entries.
SXP Version 4	Loop detection and prevention, capability exchange and built-in keep-alive mechanism.

SXPv5 Not specific to SD-Access but used as an example:

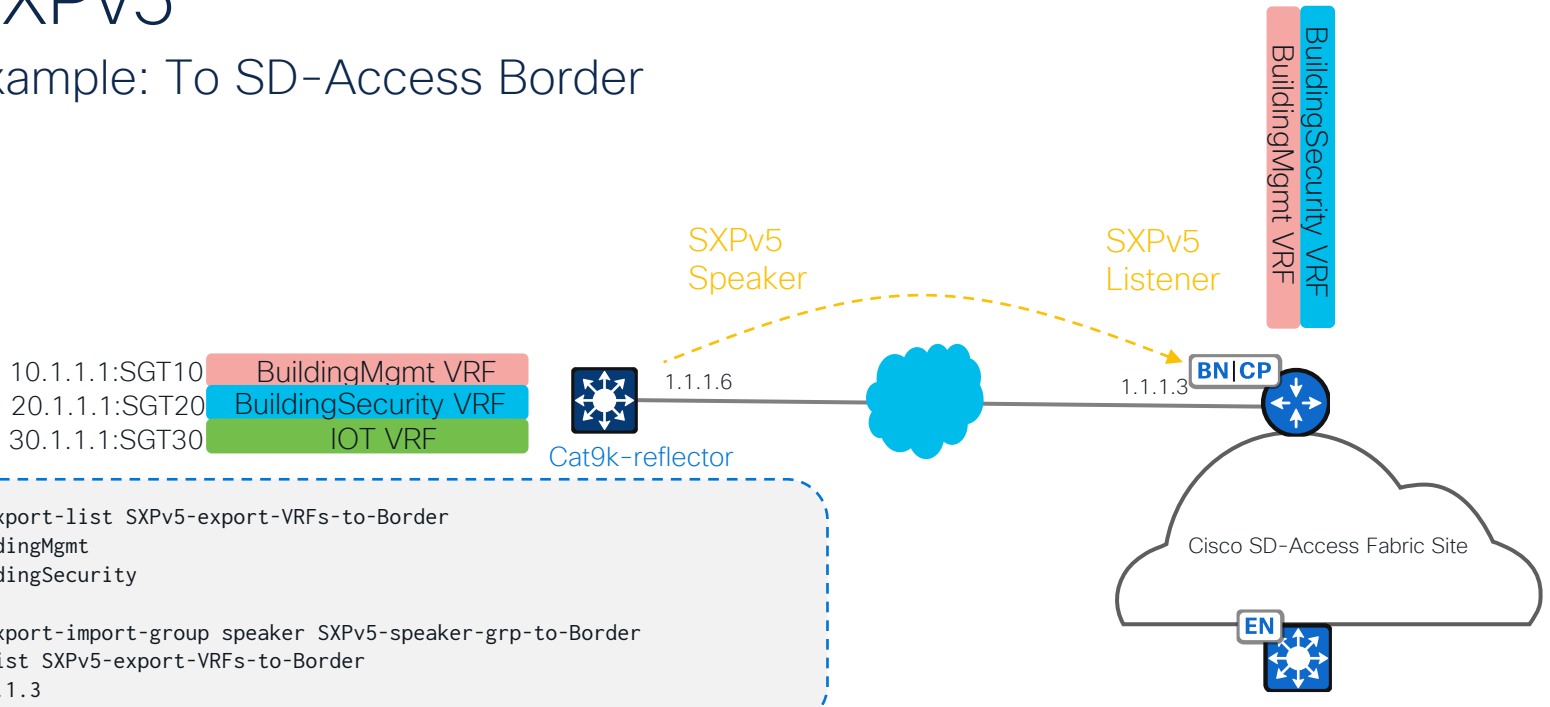


Latest SXP version before 17.9.1 is SXPv4 (not VRF aware)

IOS-XE 17.9.1

SXPv5

Example: To SD-Access Border




```
cts sxp export-list SXPv5-export-VRFs-to-Border
 vrf BuildingMgmt
 vrf BuildingSecurity
!
cts sxp export-import-group speaker SXPv5-speaker-grp-to-Border
 export-list SXPv5-export-VRFs-to-Border
 peer 1.1.1.3
```

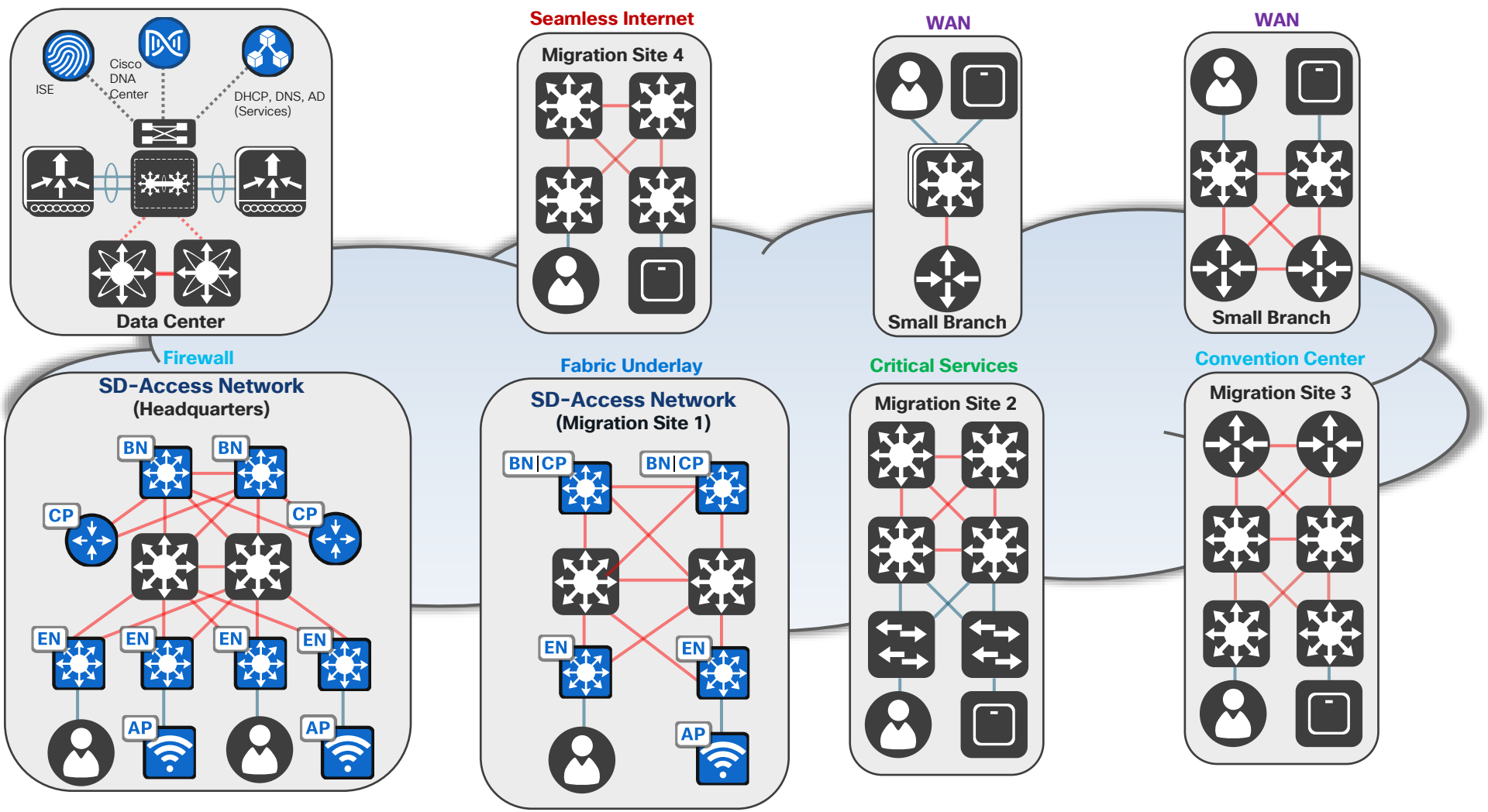
```
cts sxp import-list SXPv5-import-from-Reflector
 vrf
!
cts sxp export-import-group listener SXPv5-import-grp-from-Reflector
 import-list SXPv5-import-from-Reflector
 peer 1.1.1.6
```

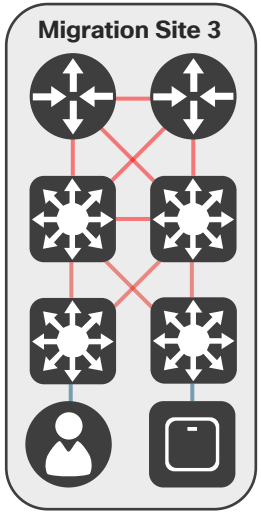
Group-Based Policy SXPv5 Guide

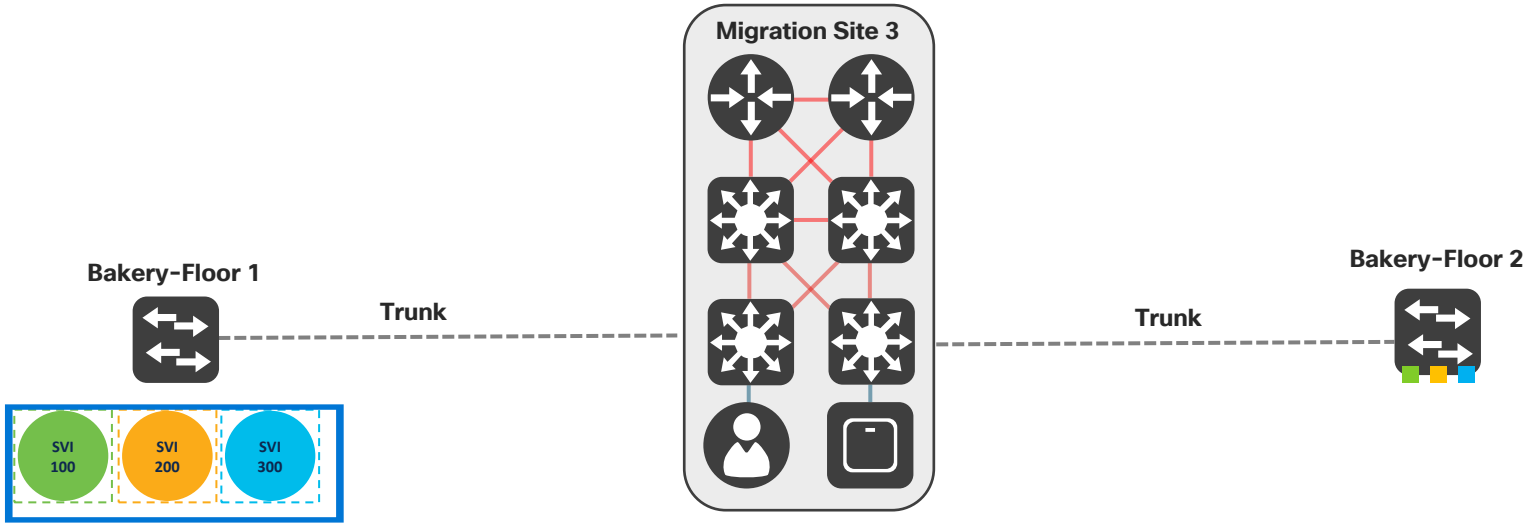
VLAN-Based L2VNI

Convention Center Use case

cisco Live!

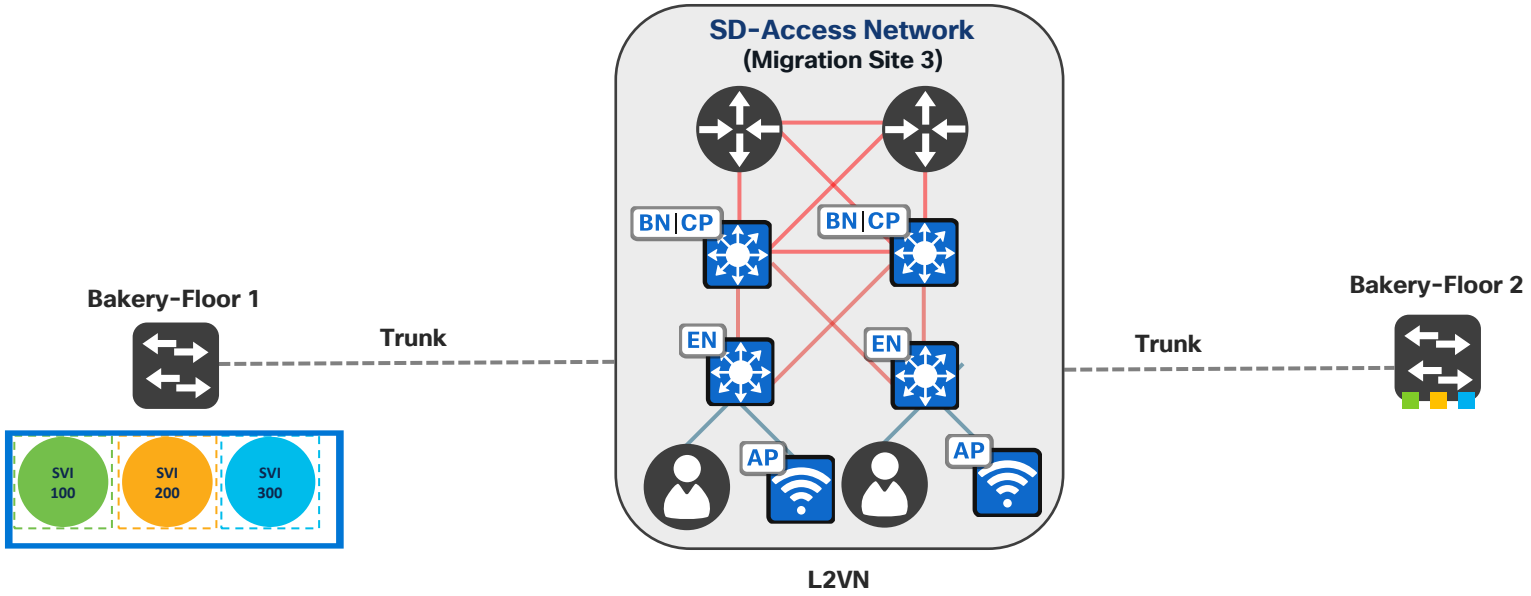






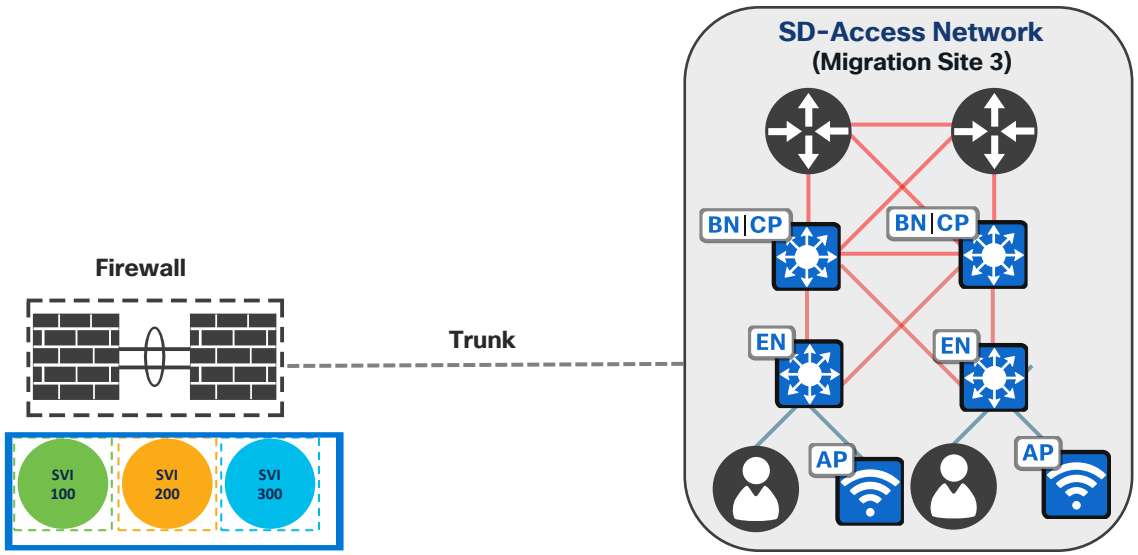
Cisco SD-Access

VLAN-BASED L2VNI After Migration



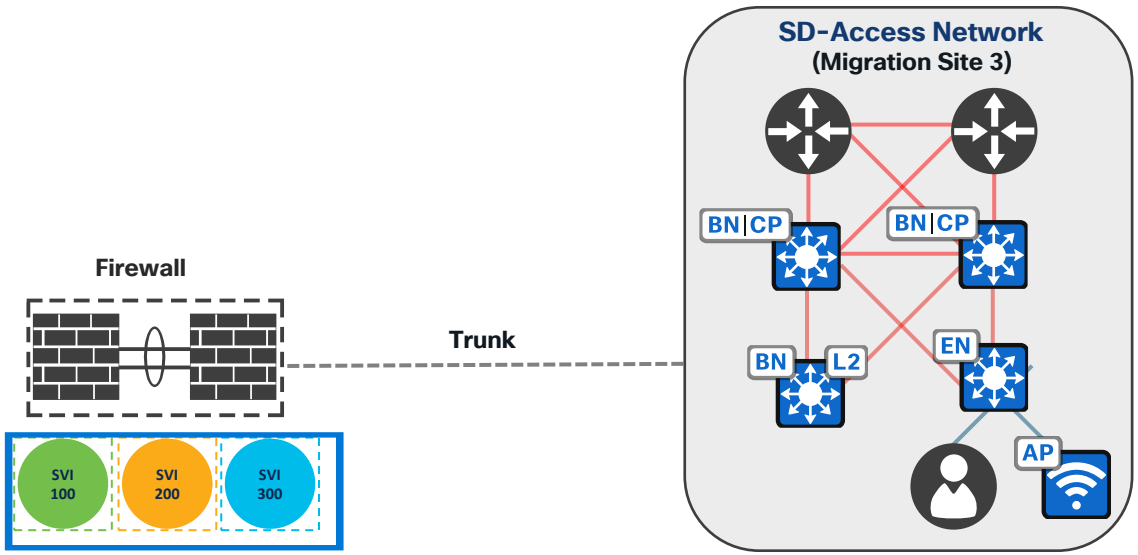
Cisco SD-Access

VLAN-BASED L2VNI



Cisco SD-Access

VLAN-BASED L2VNI



Cisco SD-Access

VLAN-BASED L2VNI

Overview

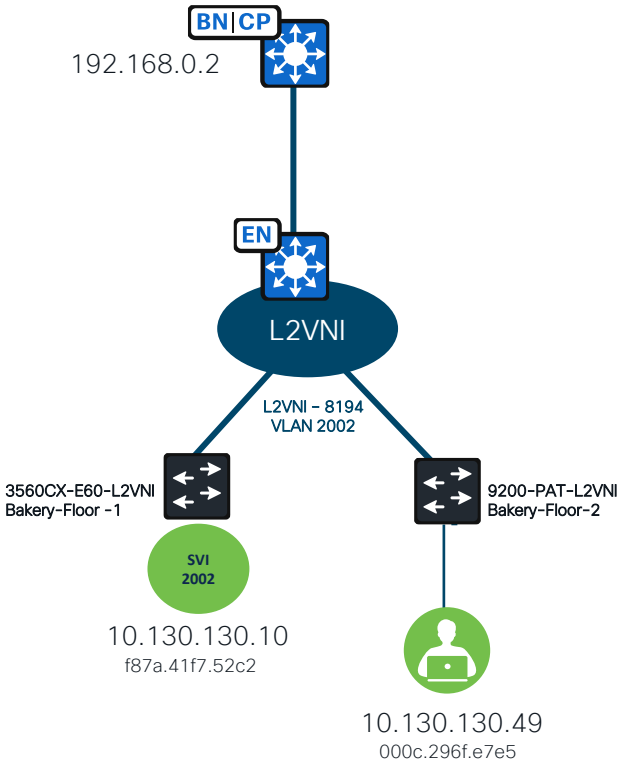
- Traditionally endpoints send non-local traffic (traffic destined for a remote subnet) to a Distributed Anycast Gateway which is present on all Edge Nodes for a given fabric site.
- The Edge Node is then responsible for forwarding traffic to the appropriate routed destination after performing a destination lookup via LISP.
- VLAN-based L2VNI service enables Cisco SD-Access to provide pure Layer 2 connectivity between endpoints with no Anycast Gateway present in the fabric site.

Details

- Supported from Cisco DNA Center 2.3.3.x. Fabric Wireless is supported from Cisco DNA Center 2.3.5.x
- A firewall as a default gateway can be used for East-West traffic security compliance.
- L2 flooding will automatically be enabled for any VLAN-based L2VNI.
- L2 flooding in overlay requires ASM (Any-source multicast) in underlay.
- If VLAN-Based L2VNI requires connectivity to endpoints external to fabric, then use Layer 2 Border handoff automation or use an Edge Node “Trunk” port.

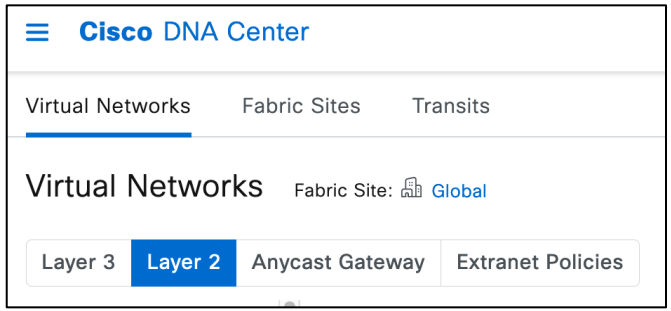
VLAN-BASED L2VNI Demo

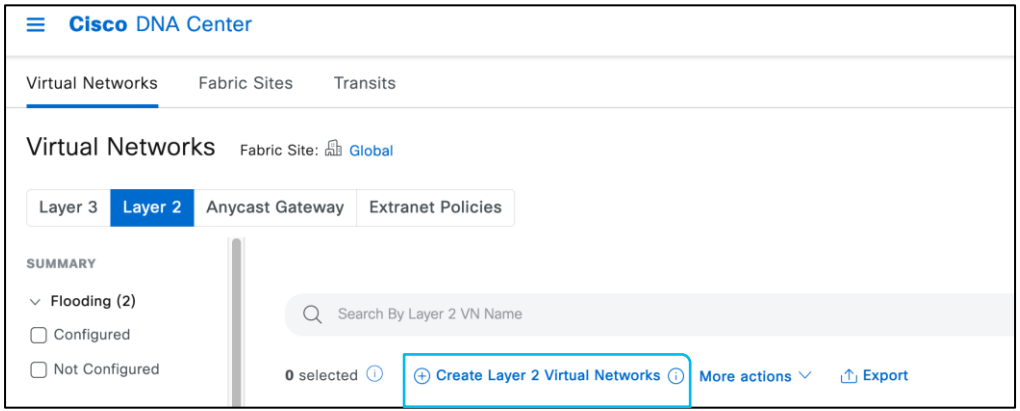
VLAN-BASED L2VNI Demo

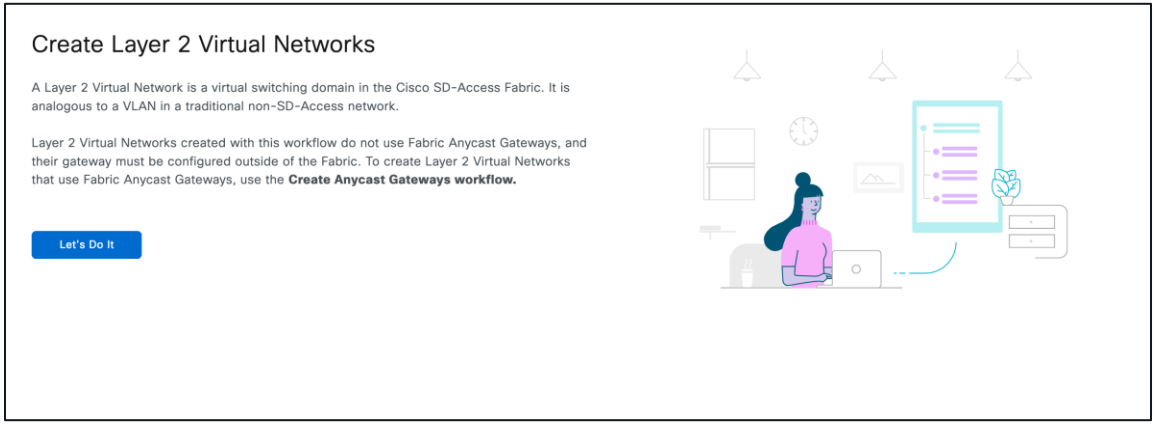


VLAN-BASED L2VNI Automation

For Your Reference



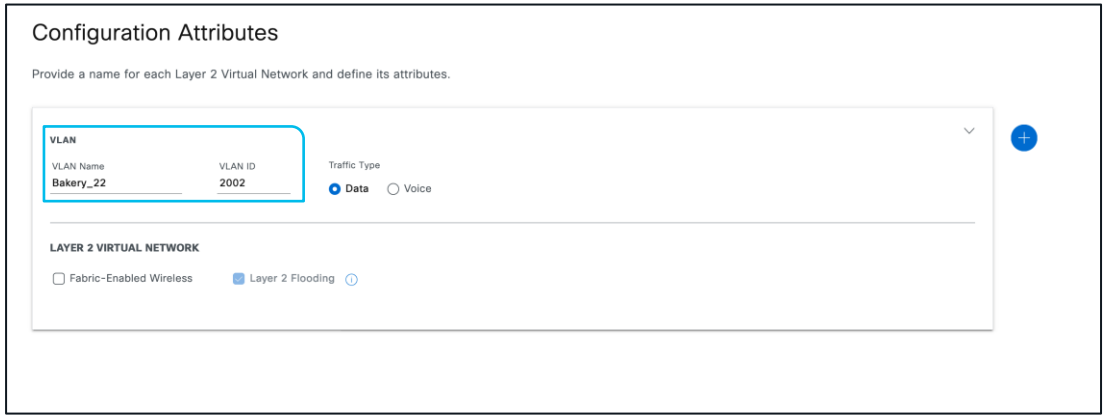


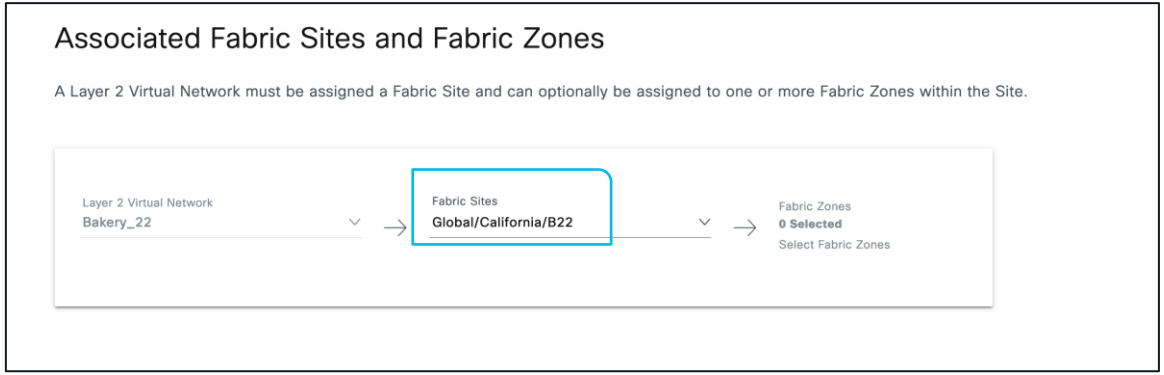


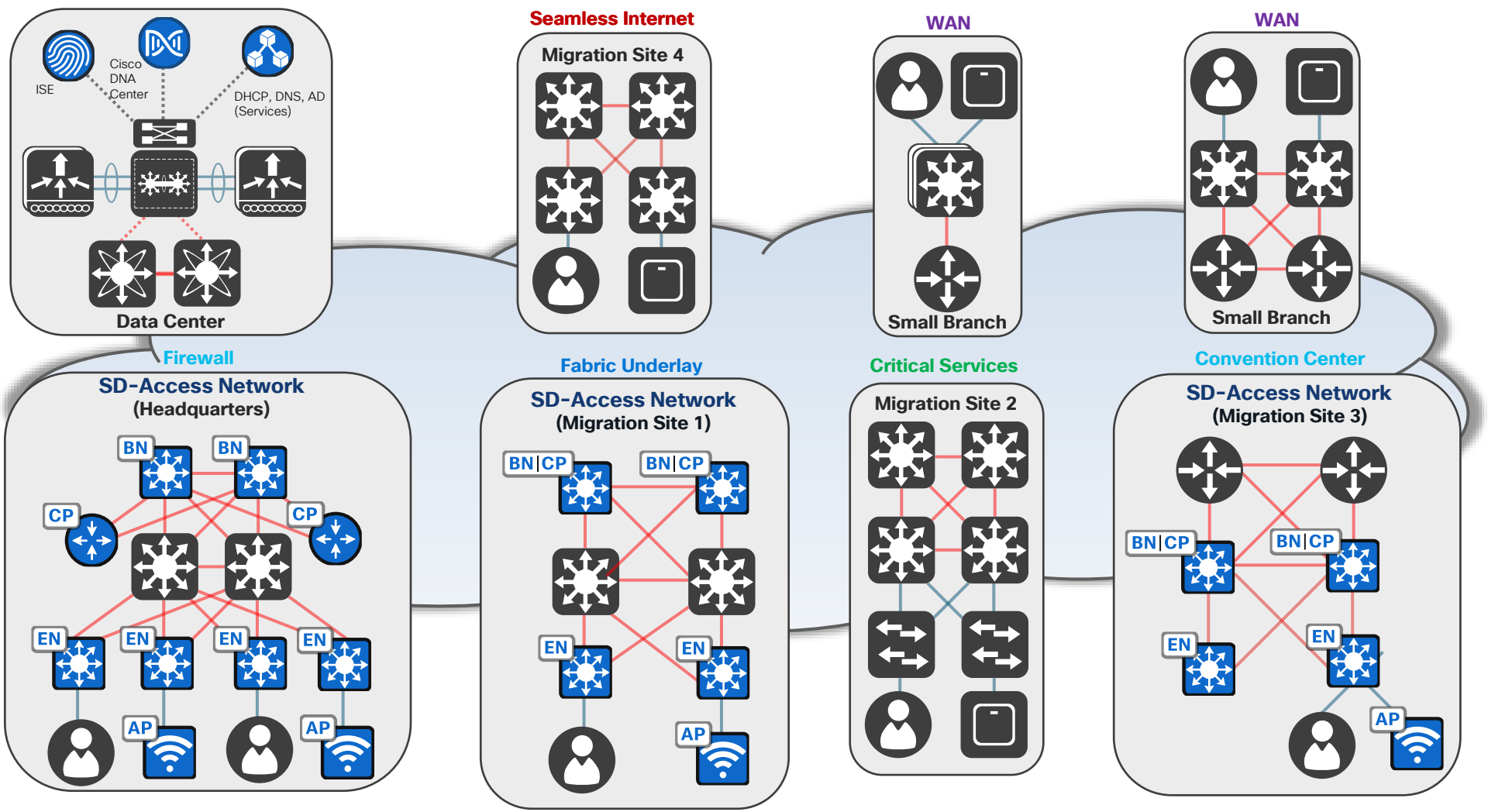
cisco Live!

VLAN-BASED L2VNI Automation

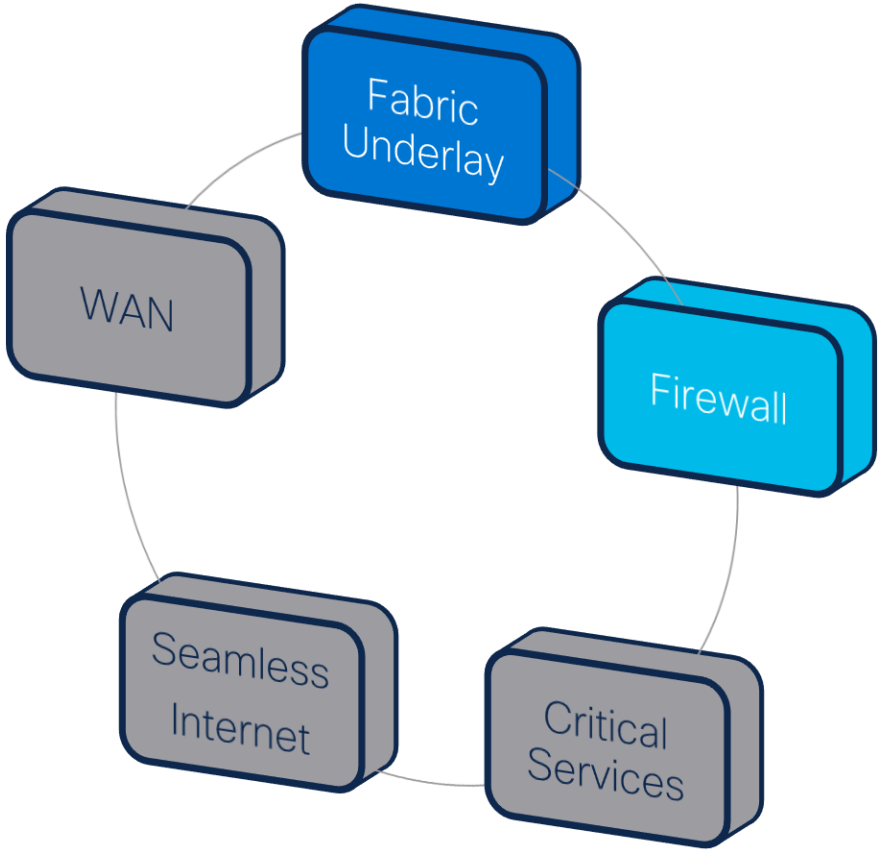
For Your Reference







Progress Chart



Simplified Critical Services access

SD-Access Extranet

Peer Network Configuration

Layer 3 Handoff to External IP Domain

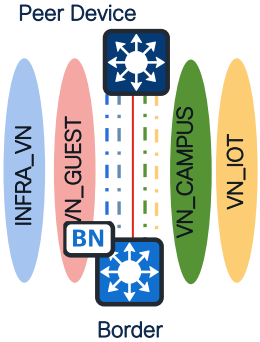
For Your Reference

Extend

- Configure VRF
- Interfaces for each VN matching Border configuration

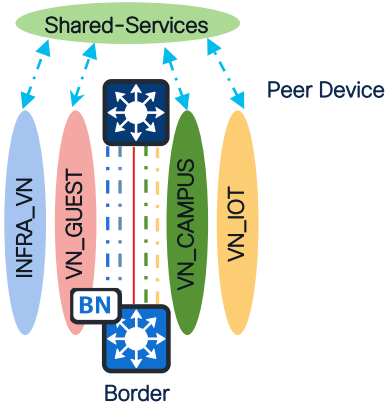
eBGP

- eBGP neighbors for each VN between Peer and Border node



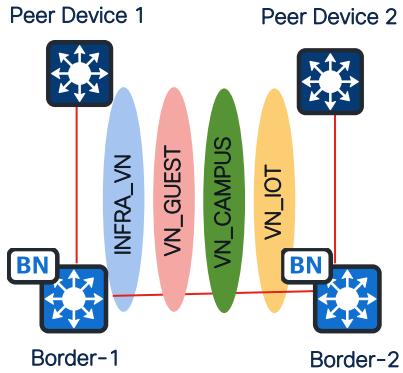
Route Leak

- Route-leak shared-services subnets to each VN
- Route-leak VN subnets into Global



iBGP

- iBGP neighbors for each VN between Border nodes



Not required at Fabric Site LISP Pub-Sub deployments.

Cisco SD-Access

Critical Services

- Simplified Critical Services such as Shared Services and Internet with minimum configuration

Cisco SD-Access

Current Network Challenges

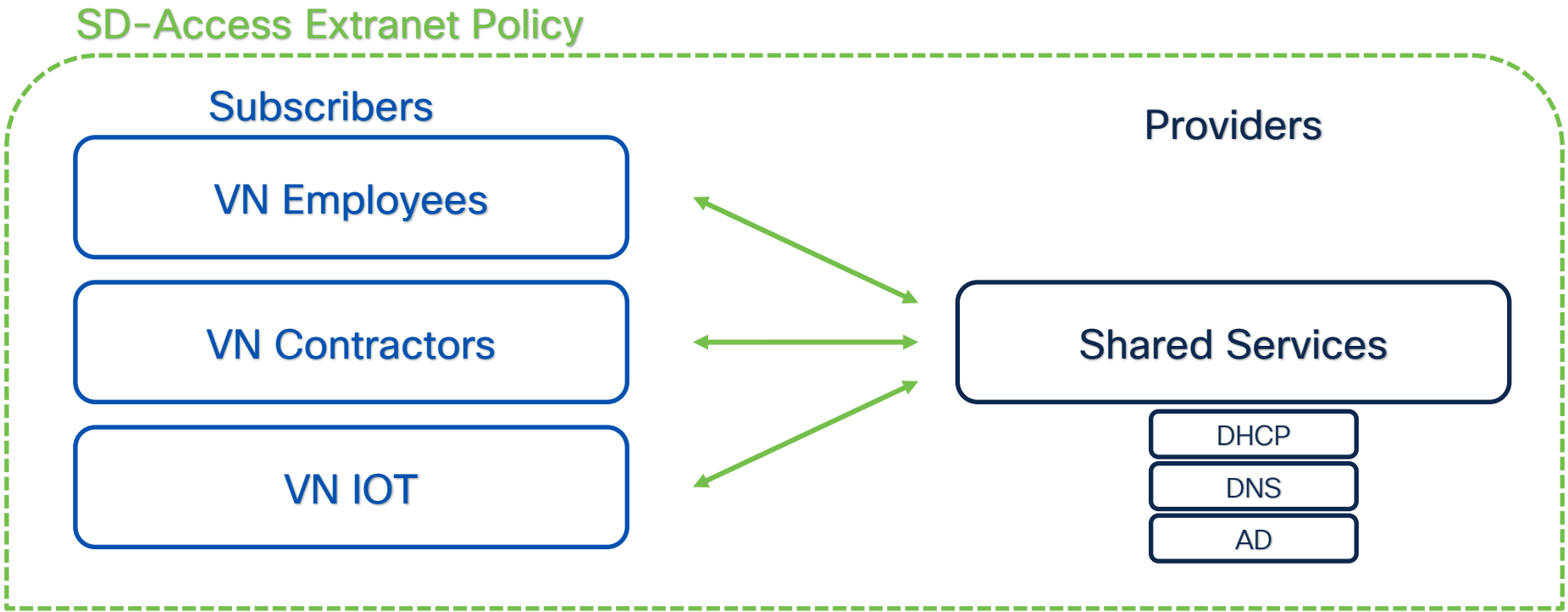
- Endpoints in an SD-Access Fabric Site are in an overlay Virtual Network (VRF Routing Table)
  - Endpoints need access to Internet and critical Shared Services such as DHCP, DNS, and AD.
- Shared Services are located outside the Fabric Site, usually in a Data Center.
  - Shared Services are generally in the GRT although may be in a dedicated Shared Services VRF.
- VRF route leaking is needed to leak Fabric Virtual Networks to the Shared Services routing table.
- This configuration is done manually outside of the Fabric (think "*fusion router*").

Cisco SD-Access Extranet

Solution Introduction

- LISP Extranet provides flexible, and scalable method for providing access to Shared Services and access to the Internet to endpoints inside the Fabric.
- This simplifies SD-Access Fabric deployments by providing a policy-based method of VRF leaking.
- LISP Extranet helps avoiding route-leaking outside Fabric Site by addressing the leaking natively in LISP.

Cisco SD-Access Extranet



Cisco SD-Access Extranet

Definition of Terms

Provider Virtual Network

- Contains a shared services resources such as DHCP, DNS, or even Internet.

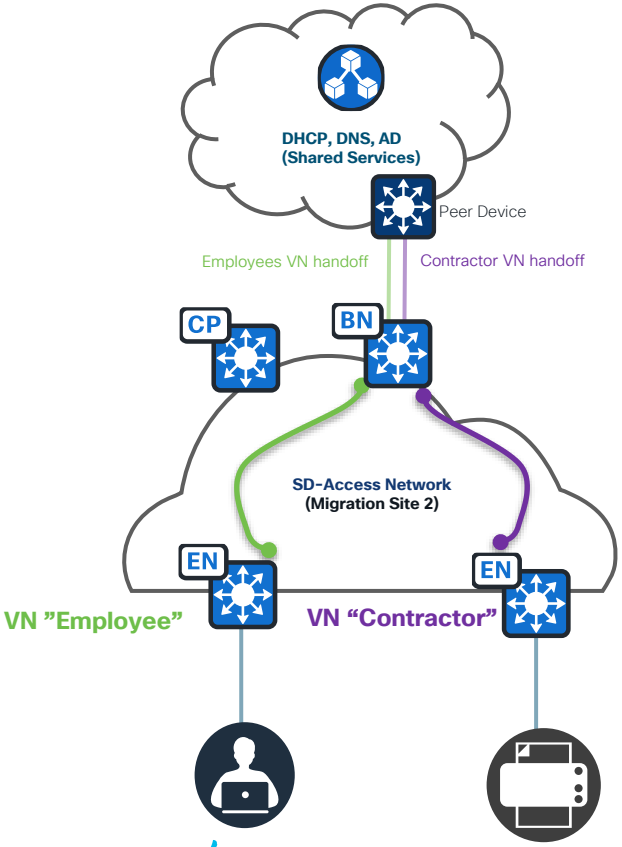
Subscriber Virtual Network

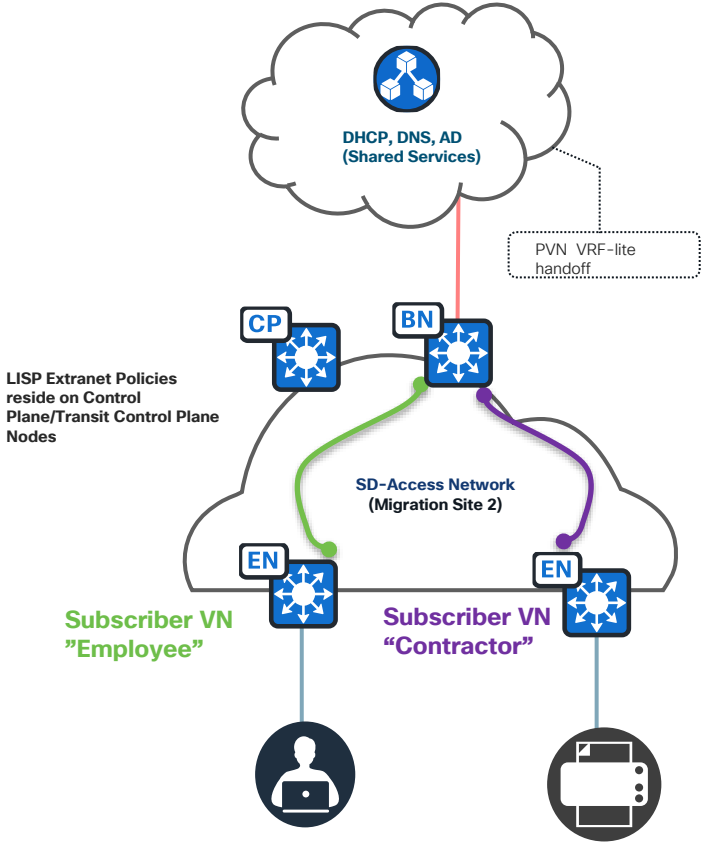
- Contain endpoints, hosts, and users that need to access shared services resources.
- Fabric Layer 3 Virtual Network

Extranet Policy

- Describes the relationship between a Provider Virtual Network and one or more Subscriber Virtual Networks.

Cisco SD-Access Extranet





Cisco SD-Access Extranet

Extranet Policy Details

- Extranet policy is orchestrated and maintained via Cisco DNA Center.
- Supported from Cisco IOS_XE 17.9 and Cisco DNA Center 2.3.4.x
- Extranet Policy can be associated to one or more Fabric Sites connected via IP transit/SD-Access transit.
- With Extranet, user only need to perform layer 3 handoff for Provider VNs from Border nodes.
- Allows communication from the Subscriber Virtual Networks to the Provider Virtual Network.
- Allows communication from the Provider Virtual Network to the Subscriber Virtual Networks.
- Contains a single Provider Virtual Network
- Contains one or more Subscriber Virtual Networks
- Denies Subscriber to Subscriber communication

SD-Access Extranet policy:

Extranet Policy	Provider VN	Subscriber VN
Provider VN	NO	YES
Subscriber VN	YES	NO

Cisco SD-Access Extranet

Considerations

- Extranet policies are supported with Lisp Pub/Sub fabric only
- A Provider Virtual Network in one Policy cannot be a Subscriber Virtual Network in another Policy.
- A Subscriber Virtual Network in one Policy cannot be a Provider Virtual network in another Policy.
- Provider VN can be a dedicated VN or INFRA_VN (INFRA_VN cannot be a subscriber VN).
- A Virtual Network can be a Provider in only one Policy.
- Virtual Networks can be a Subscriber in one or more Policies.
- Provider to Provider communication is not supported.
- Subscriber to Subscriber communication is not supported.
  - Extranet is not meant to leak Fabric VRF to Fabric VRF.
  - If two devices inside the Fabric need to communicate with one another, put them in the same Virtual Network.
- Multicast leveraging Extranet functionality is not supported (If Multicast traffic stays within a VN, then it is supported. E.g., RP,Source,Receiver within a VN)

Cisco SD-Access Extranet

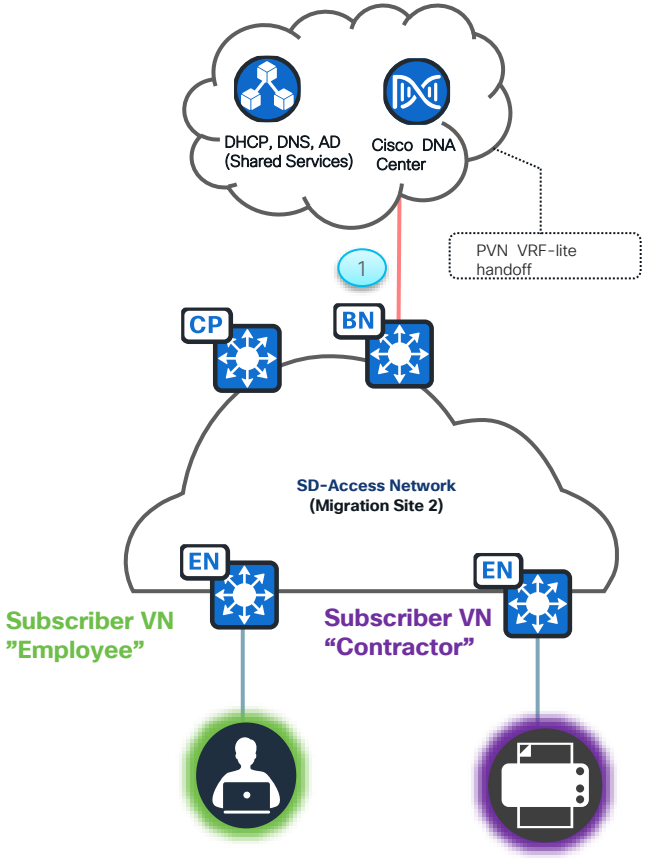
Packet Flows

cisco Live!

SD-Access Extranet – Shared Services

1

- All virtual networks (VNs) within the fabric require connectivity to shared services, which are connected to the fabric border through a Provider VRF called "Shared Services." These routes are imported into the Provider VRF "Shared Services" in LISP.



SD-Access Extranet – Shared Services

2

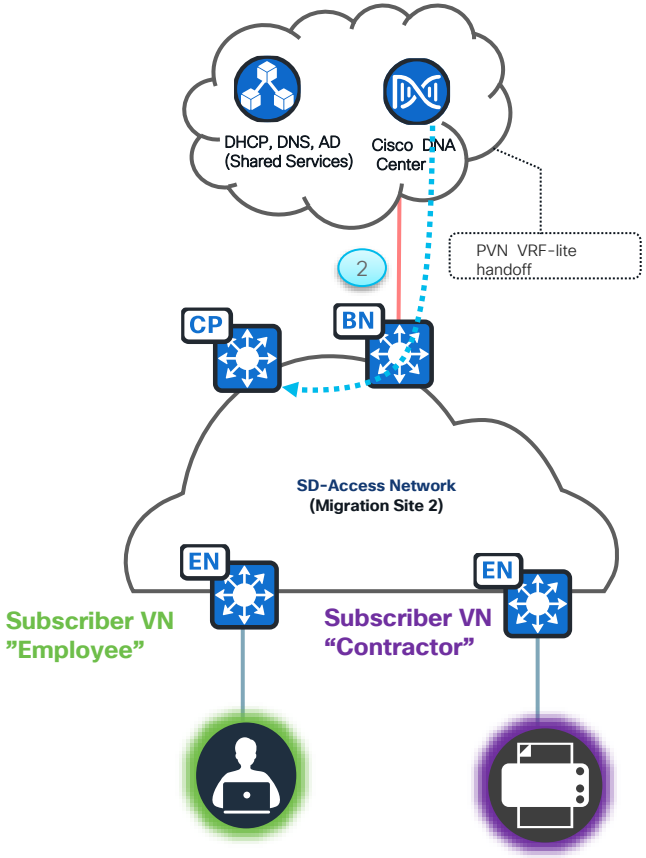
- Admin creates SD-Access Extranet policy via Cisco DNA Center workflow which is configured in Control Plane node.

Extranet Policy :

- Provider VN is " Shared Services"
- Subscriber VN is "Employee"
- Subscriber VN is "Contractor"

* Only 1 Provider VRF is allowed per extranet policy instance.

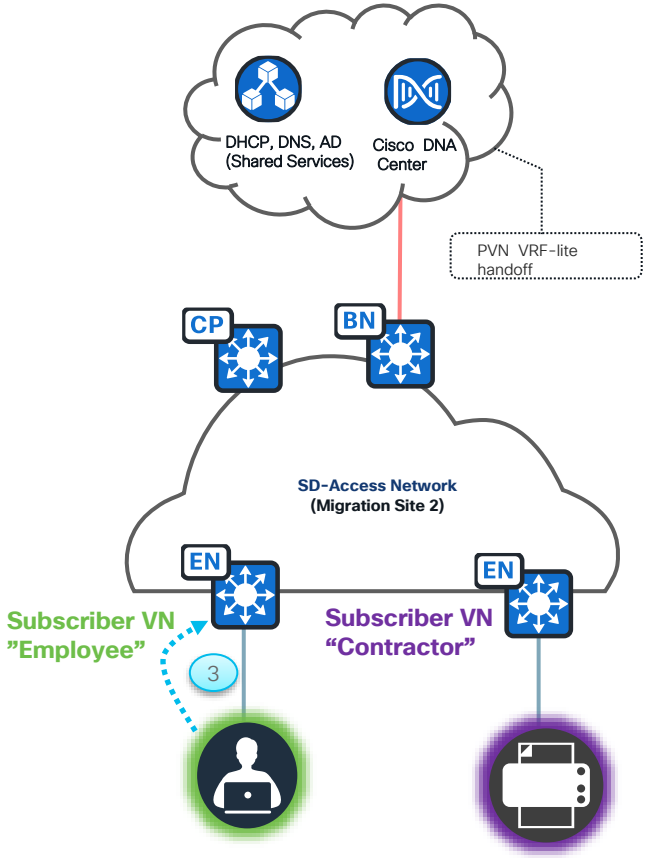
- Multiple subscribers are allowed.
- At this stage, CP knows about users (host entries) in respective virtual networks and their location(Edge node).
- CP also knows about shared service prefixes via Border (Border is either Internal or Anywhere)



SD-Access Extranet – Shared Services

3

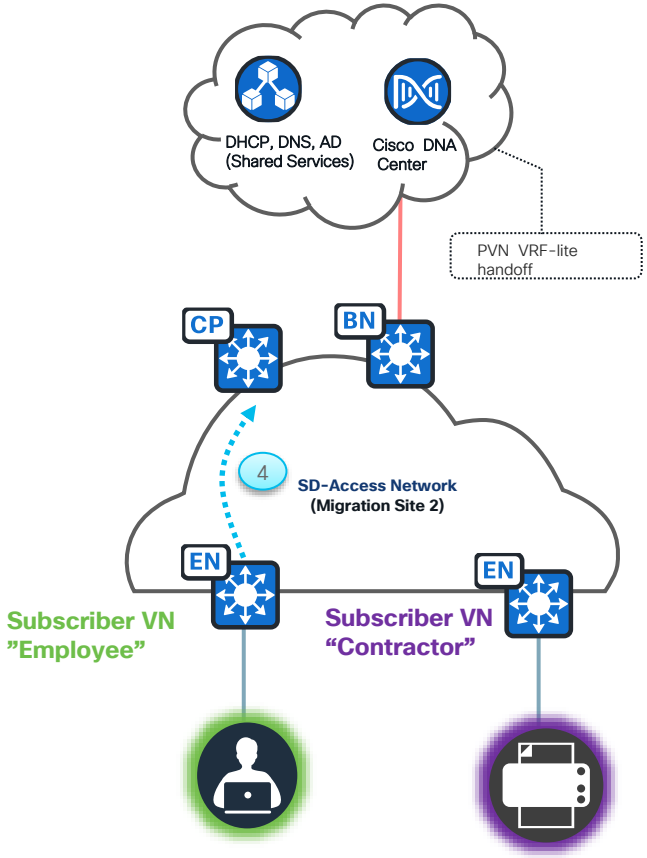
- Host in Virtual Network Subscriber VN Employee on Edge node wants to communicate with server in Shared Services (Shared Services VN)



SD-Access Extranet – Shared Services

4

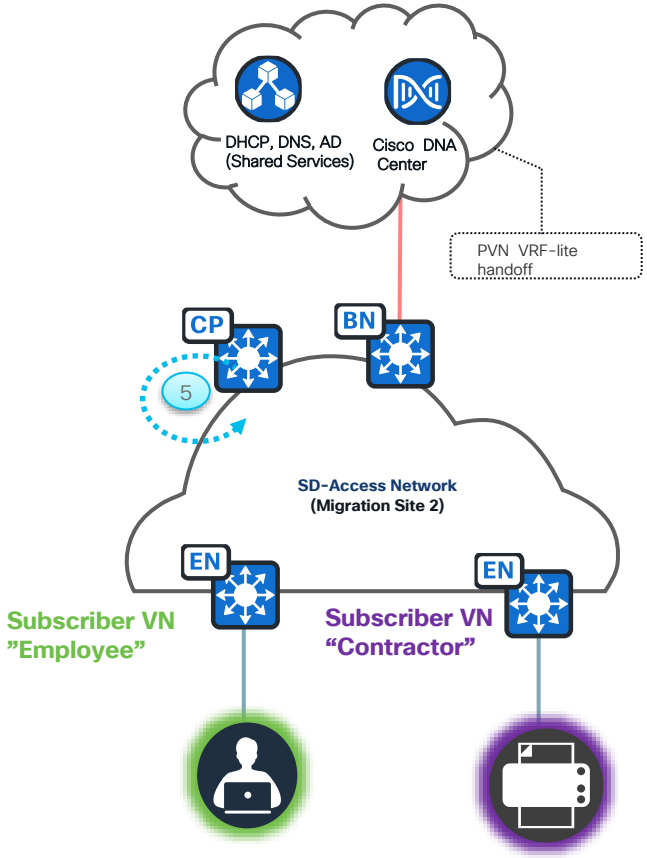
- Edge node with Virtual Network Employees sends a map-request to the control plane node requesting to reach Server in Shared Services



SD-Access Extranet – Shared Services

5

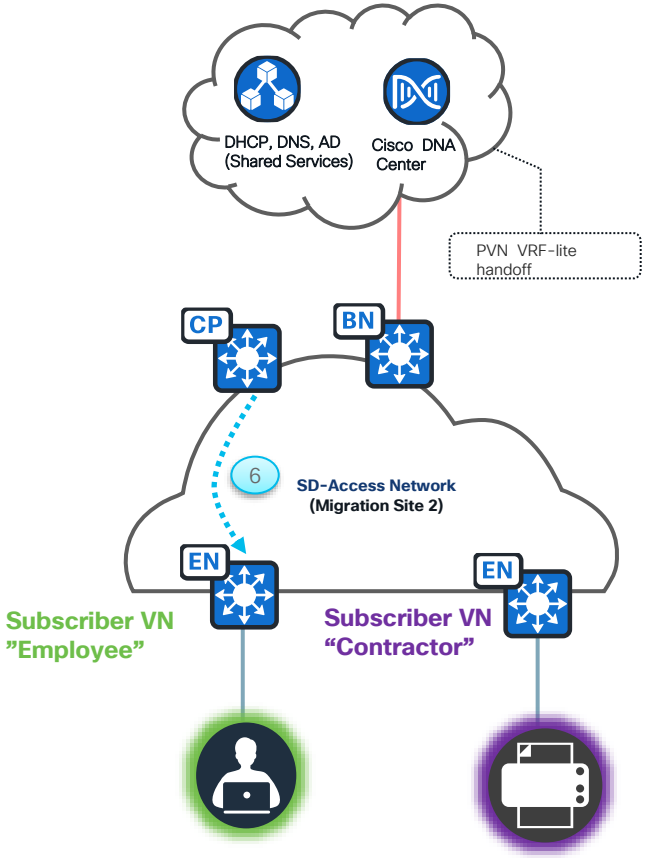
- Control Plane node is going to first look at the source VN which is Subscriber VN Employee for shared service subnet which will be absent.
- Second lookup would be in Provider VN Shared Services as Employee is part of an extranet policy where the prefix will be present.



SD-Access Extranet – Shared Services

6

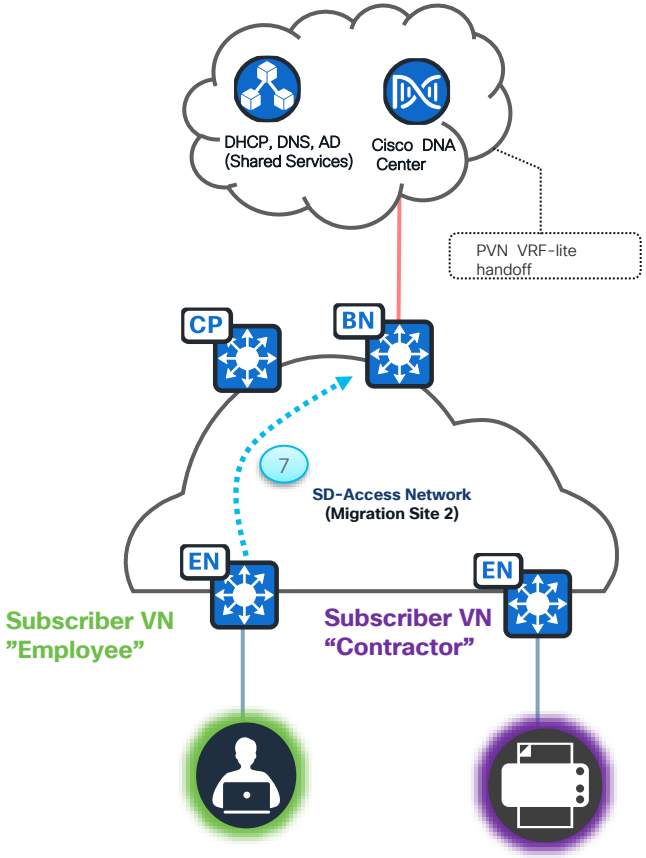
- Control Plane node will respond with map-reply with Provider VN Shared Services information to the Edge node



SD-Access Extranet – Shared Services

7

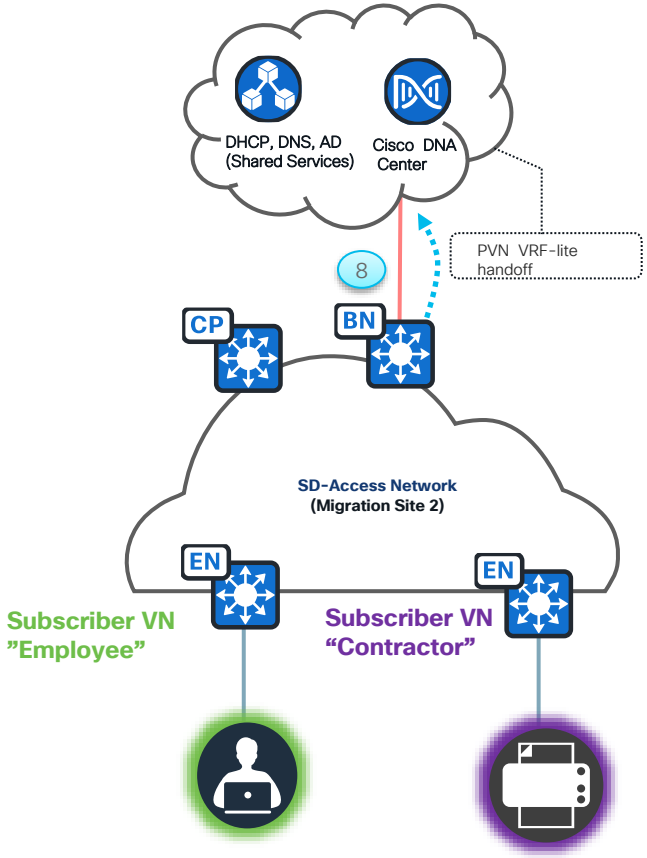
- Edge node will send the data plane traffic (VXLAN encapsulated) to the Border node in Provider VN Shared Services.



SD-Access Extranet – Shared Services

8

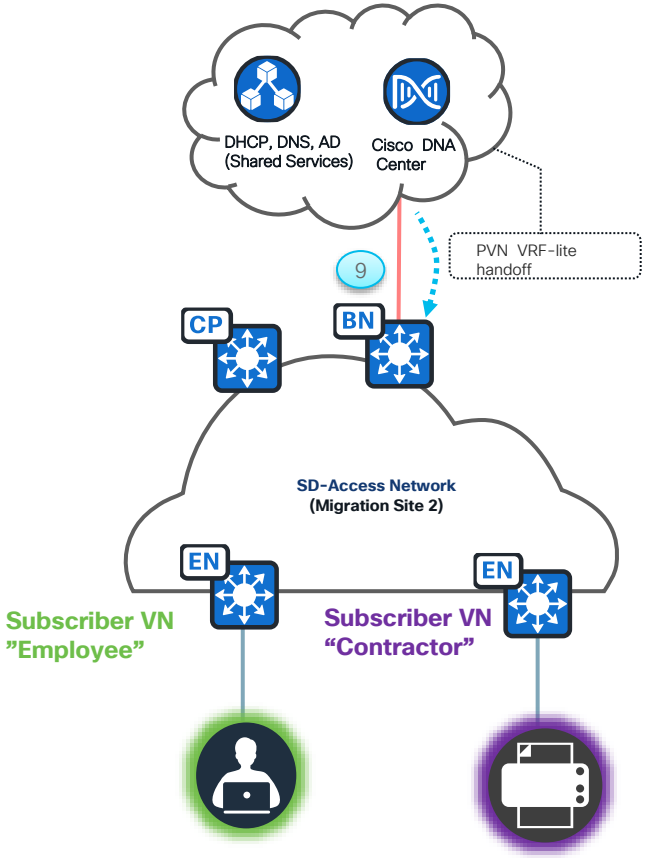
- Border node will de encapsulate the VXLAN traffic and send the IP traffic to external world (Shared Services)



SD-Access Extranet – Shared Services

9

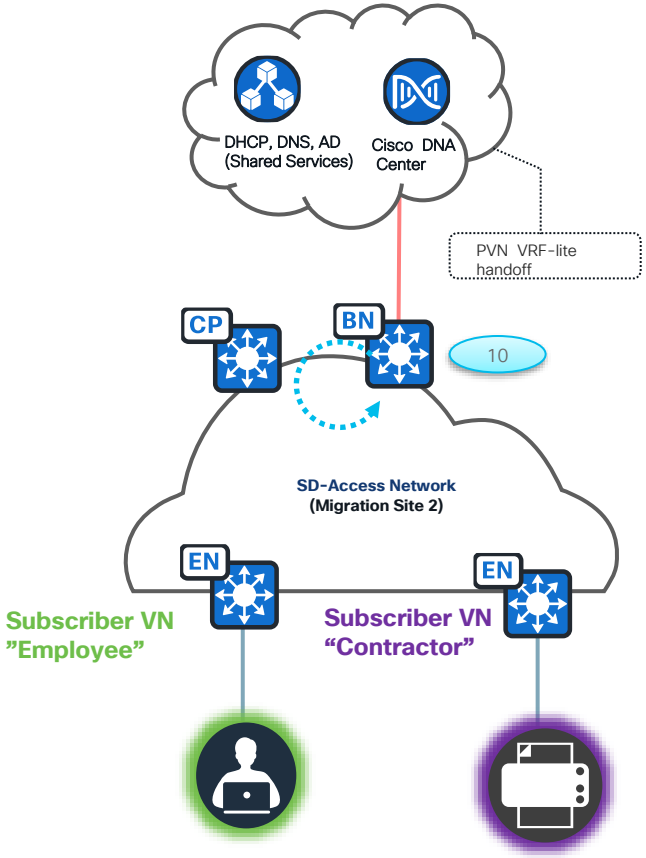
- Return traffic from shared services is going to ingress at the Border node in Provider VN Shared Services.



SD-Access Extranet – Shared Services

10

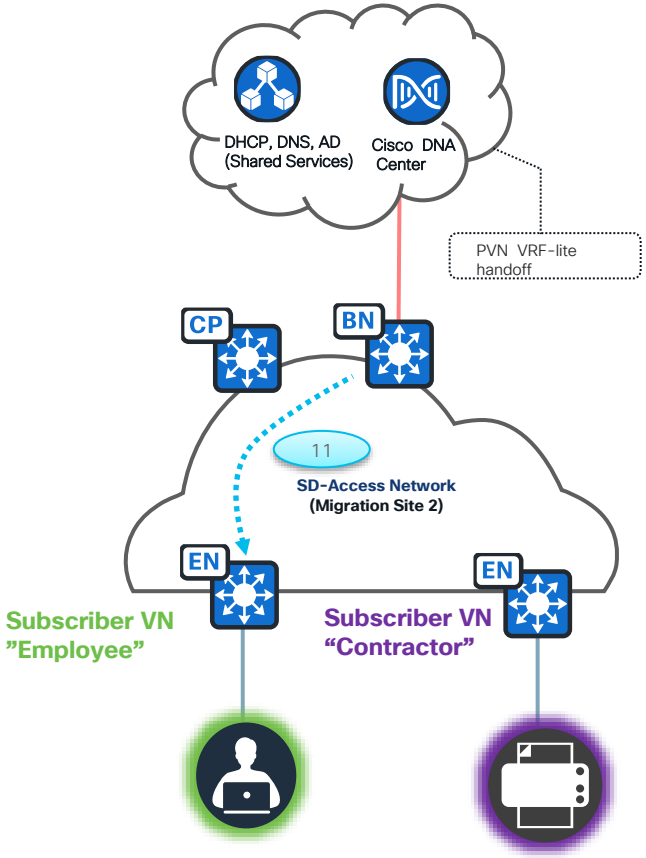
- Border node will not have destination host information in the Provider VN Shared Services. A policy is defined on the border where the ingress packet is always looked up in the respective subscriber VN.



SD-Access Extranet – Shared Services

11

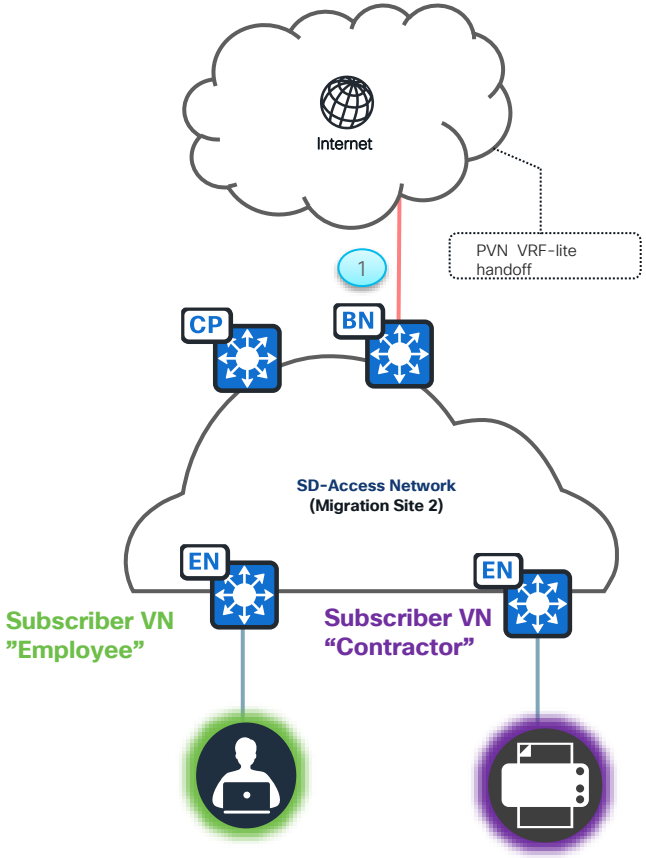
- Border node will send the data plane traffic (VXLAN encapsulated) to the Edge node in Subscriber VN Employee.



SD-Access Extranet – Internet

1

- Border connects to Internet
- All user VN's in fabric needs connectivity to Internet
- Internet will connect to a Provider VRF named as "Internet" that is only present on the fabric border.
- Internet prefixes are not known to the Border nodes.



SD-Access Extranet – Internet

2

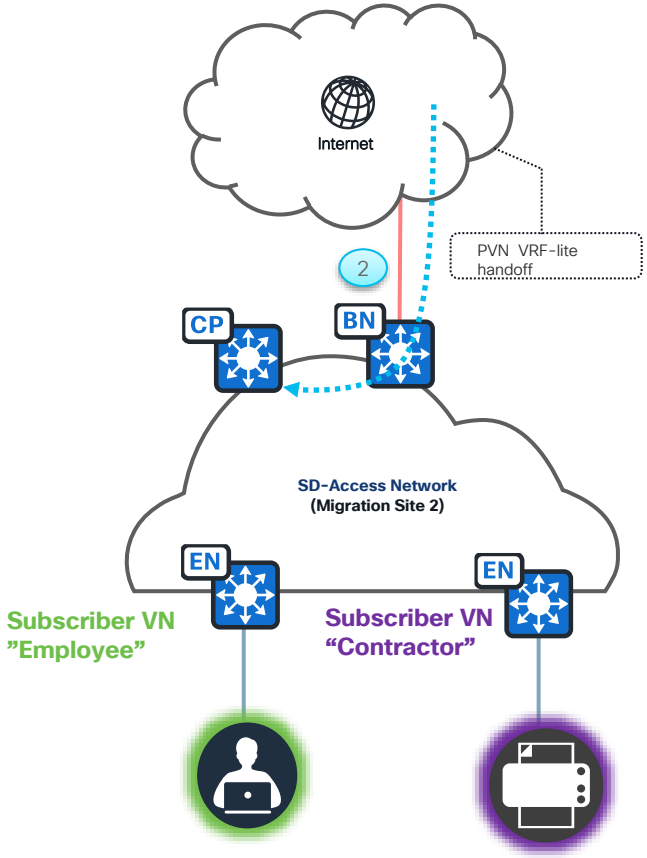
- Admin creates SD-Access Extranet policy via Cisco DNA Center workflow which is configured in Control Plane node.

Extranet Policy :

- Provider VN is " Internet"
- Subscriber VN is "Employee"
- Subscriber VN is "Contractor"

* Only 1 Provider VRF is allowed per extranet policy instance.

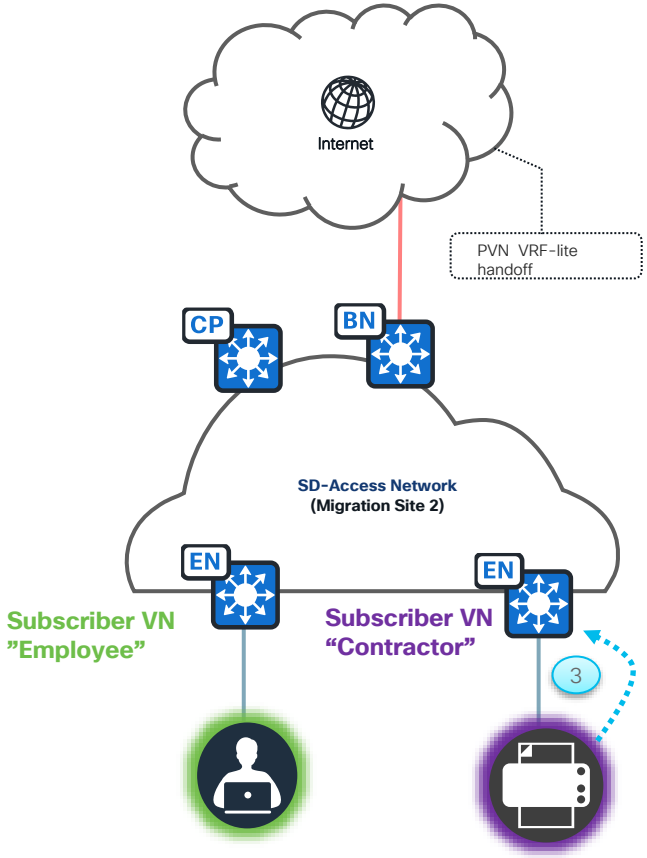
- Multiple subscribers are allowed.
- At this stage, CP knows about users (host entries) in respective virtual networks and their location(Edge node).



SD-Access Extranet – Internet

3

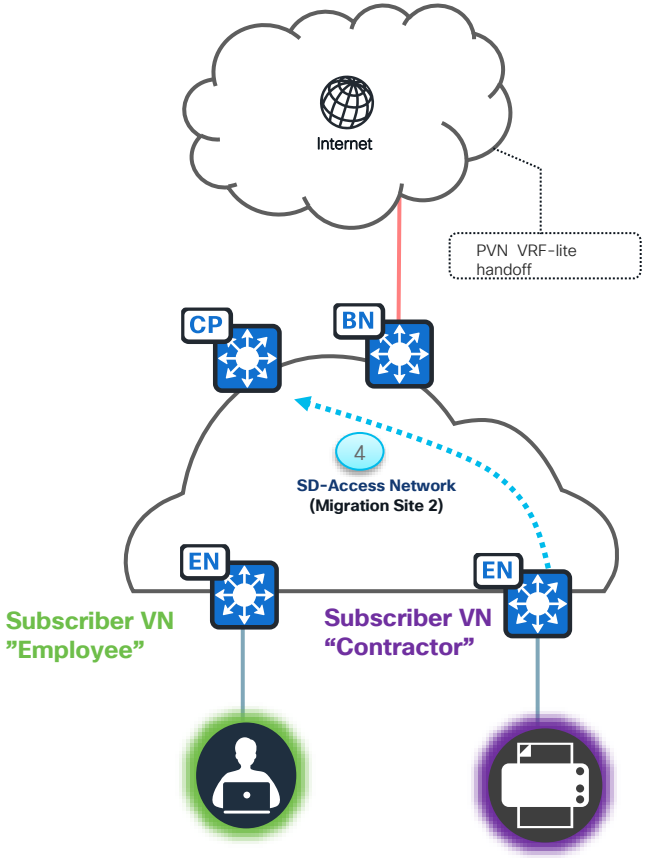
- Host in Virtual Network Subscriber VN Contractor on Edge node wants to reach a prefix on the Internet which is reachable via default route in Provider VN Internet



SD-Access Extranet – Internet

4

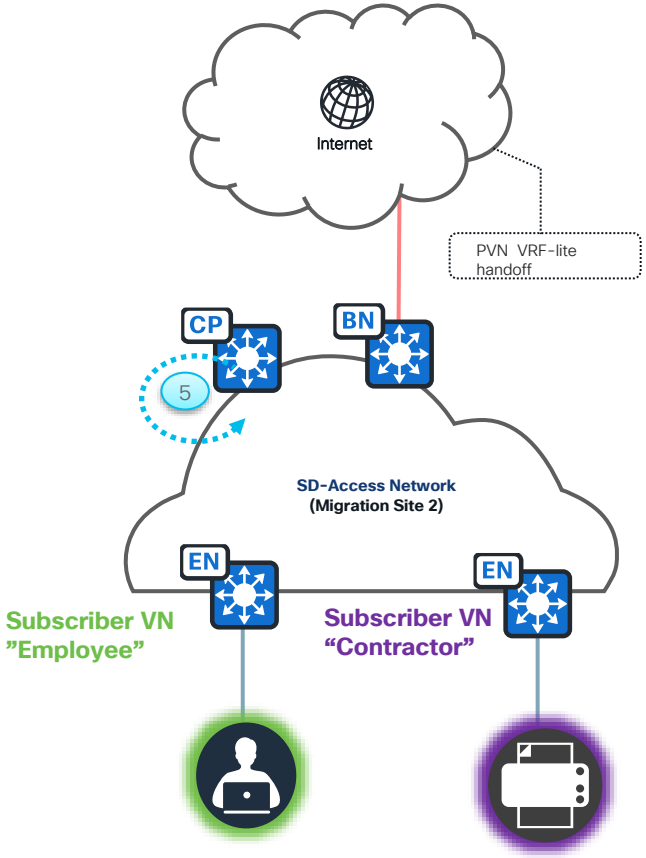
- Edge node with Virtual Network Subscriber VN Contractor sends a map-request to the control plane node requesting to reach prefix in Internet.



SD-Access Extranet – Internet

5

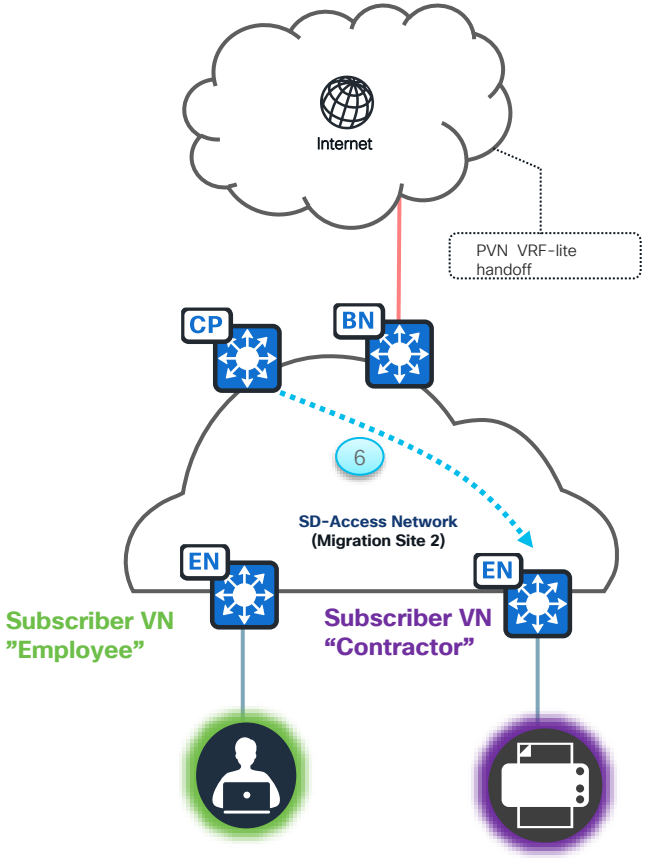
- Control Plane node is going to first look at the source VN which is Subscriber VN Contractor for internet prefix which will be absent.
- Second lookup would be in Provider VN Internet as Contractor is part of an extranet policy where the prefix will be absent.



SD-Access Extranet – Internet

6

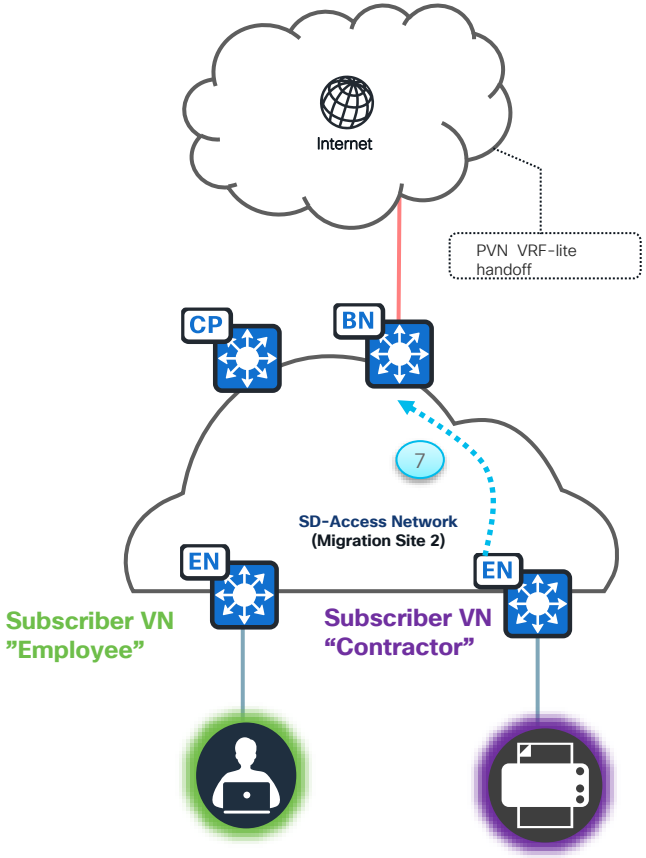
- If no registration is found for the prefix in both source VN Subscriber VN Contractor and Provider VN Provider VN Internet then, Control Plane node will respond to Edge node with a map-reply informing edge node to send the traffic to Border using Provider VN Internet which has default route present



SD-Access Extranet – Internet

7

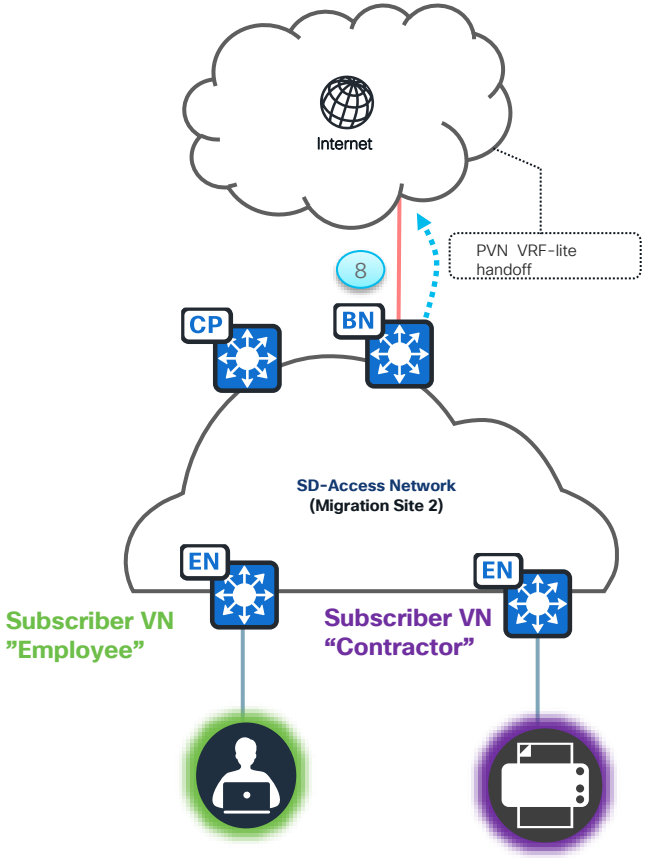
- Edge node will send the data plane traffic (VXLAN encapsulated) to the Border node in Provider VN Internet.



SD-Access Extranet – Internet

8

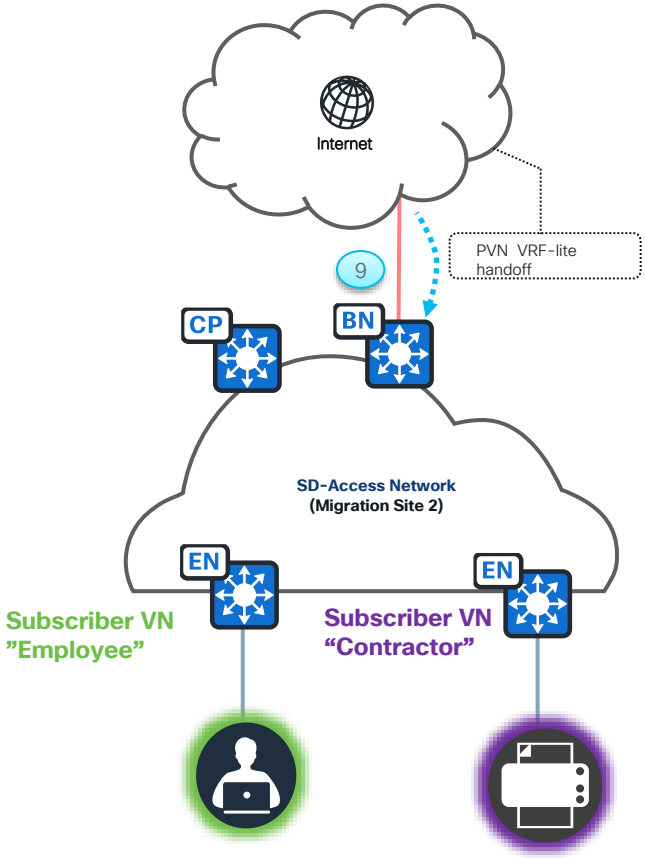
- Border node will de encapsulate the VXLAN traffic and send the IP traffic to external world (Internet)



SD-Access Extranet – Internet

9

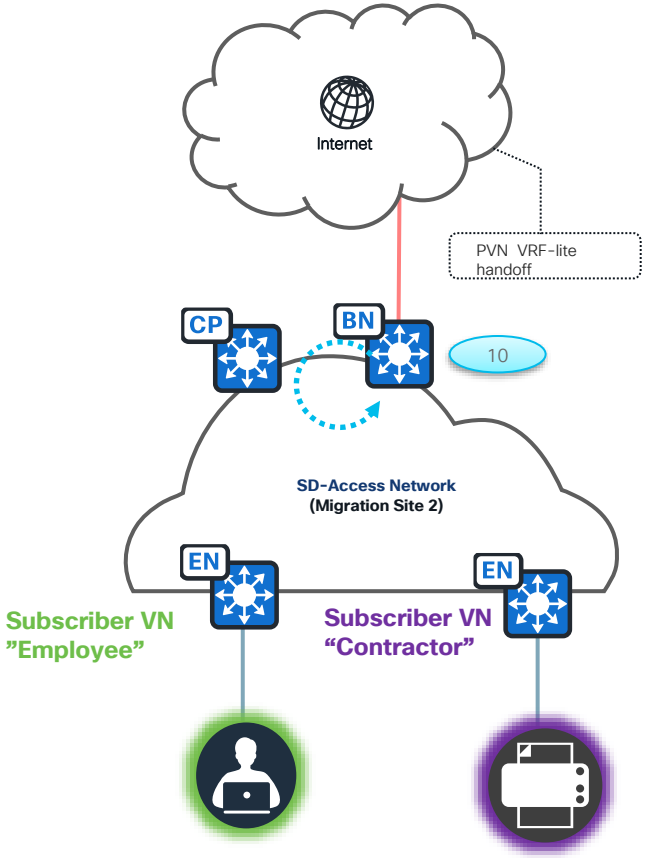
- Internet traffic is going to ingress at the Border node in Provider VN Internet



SD-Access Extranet – Internet

10

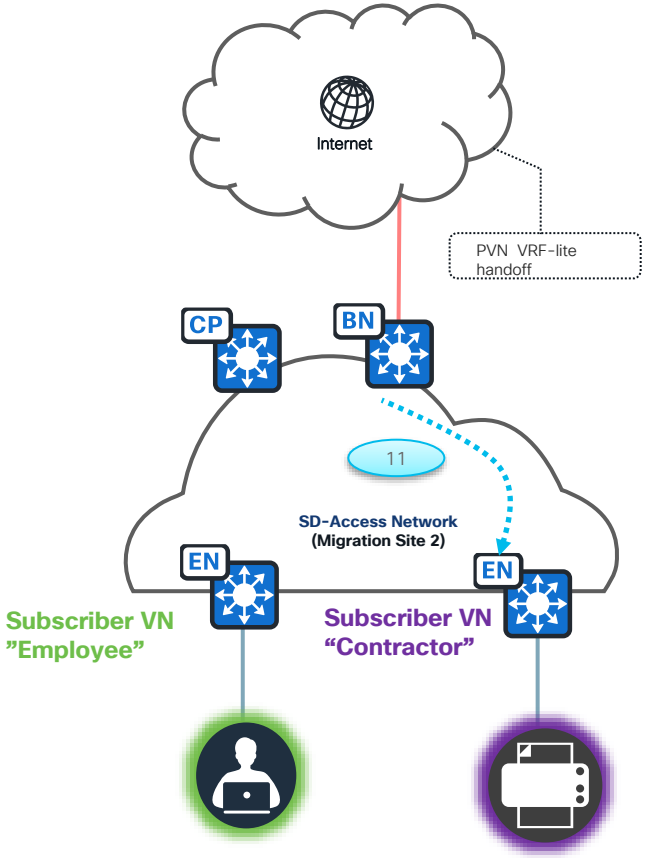
- Border node will not have destination host information in the Provider VN Internet. A policy is defined on the border where the ingress packet is always looked up in the respective subscriber VN.



SD-Access Extranet – Internet

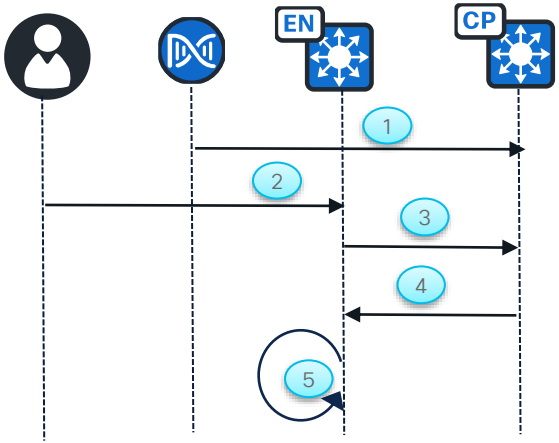
11

- Border node will send the data plane traffic (VXLAN encapsulated) to the Edge node in Subscriber VN Contractor.



SD-Access Extranet – Subscriber to Subscriber policy

How Subscriber to Subscriber policy is denied ?



- Fabric edge installs entry in map-cache and CEF to drop traffic between Subscribers

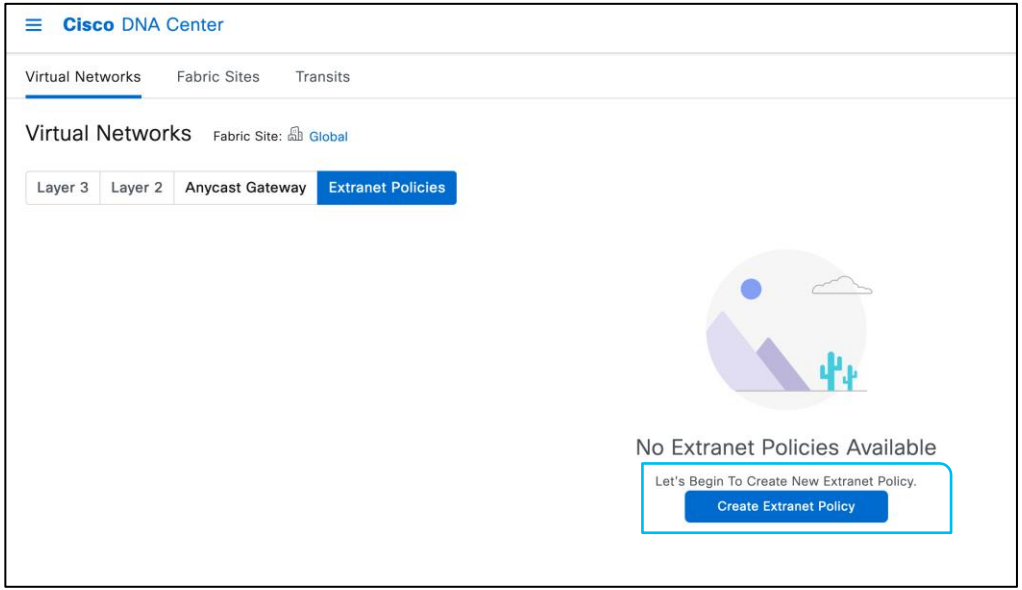
```
Fabric_edge#show ip lisp instance-id 4105 map-cache 9.10.61.0
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf corp (IID 4105),
7 entries

9.10.61.0/24, uptime: 00:00:04, expires: 00:14:55, via map-reply,
drop
  Sources: map-reply
  State: drop, last modified: 00:00:04, map-source: 9.254.254.66
  Active, Packets out: 0(0 bytes), counters are not accurate
```

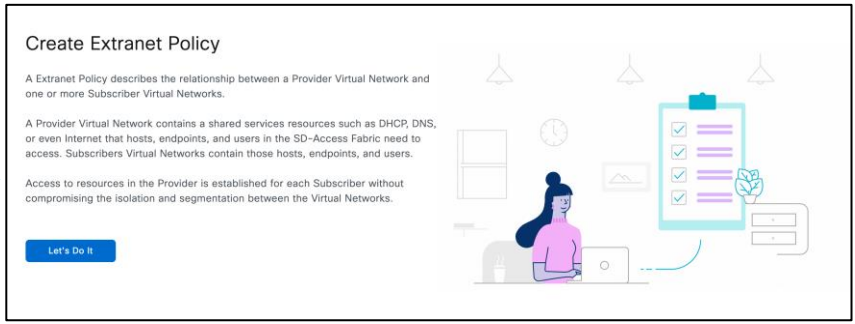
Flow	Event
1	• Admin creates SD-Access Extranet policy via Cisco DNA Center workflow which is configured in Control Plane node. Extranet Policy : ▪ Provider VN is " Shared Services" ▪ Subscriber VN is "Employee" ▪ Subscriber VN is "Contractor"
2	• Host on a subscriber VN (Employee) tries to initiate a communication to another host in the subscriber VN(Contractor)
3	• The respective edge node generates a map request to the control plane.
4	• Map server responds back with a map-reply with the action set to drop the frame
5	• Edge node installs the entry in map-cache and CEF to drop the frame, thus blocking subscriber to subscriber communication

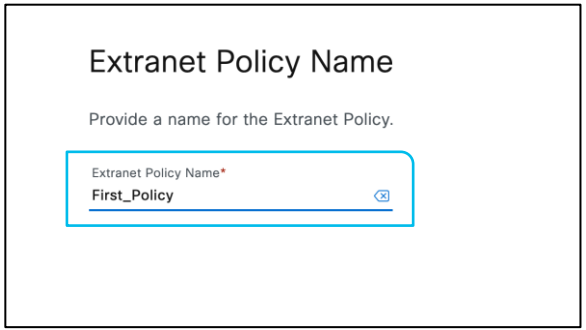
```
▷ Frame 70: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
▷ Ethernet II, Src: Cisco_01:f5:67 (70:1f:53:01:f5:67), Dst: Cisco_81:85:67 (70:0b:4f:81:85:67)
▷ Internet Protocol Version 4, Src: 9.254.254.66, Dst: 9.254.254.68
▷ User Datagram Protocol, Src Port: 4342, Dst Port: 4342
◢ Locator/ID Separation Protocol
    0010 .... .... .... .... .... = Type: Map-Reply (2)
    .... 0... .... .... .... .... = P bit (Probe): Not set
    .... .0.. .... .... .... .... = E bit (Echo-Nonce locator reachability algorithm enabled): Not set
    .... ..0. .... .... .... .... = S bit (LISP-SEC capable): Not set
    .... ...0 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0x663a7c310b21d1c2
  ◢ Mapping Record 1, EID Prefix: [4105] 9.10.61.0/24, TTL: 15, Action: Drop/Policy-Denied, Authoritative
      Record TTL: 15
      Locator Count: 0
      EID Mask Length: 24
      100. .... .... .... = Action: Drop/Policy-Denied (4)
      ...1 .... .... .... = Authoritative bit: Set
      .... .000 0000 0000 = Reserved: 0x000
      0000 .... .... .... = Reserved: 0x0
      .... 0000 0000 0000 = Mapping Version: 0
      EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    ▷ EID Prefix: [4105] 9.10.61.0
```

SD-Access Extranet Automation Workflow

For Your Reference

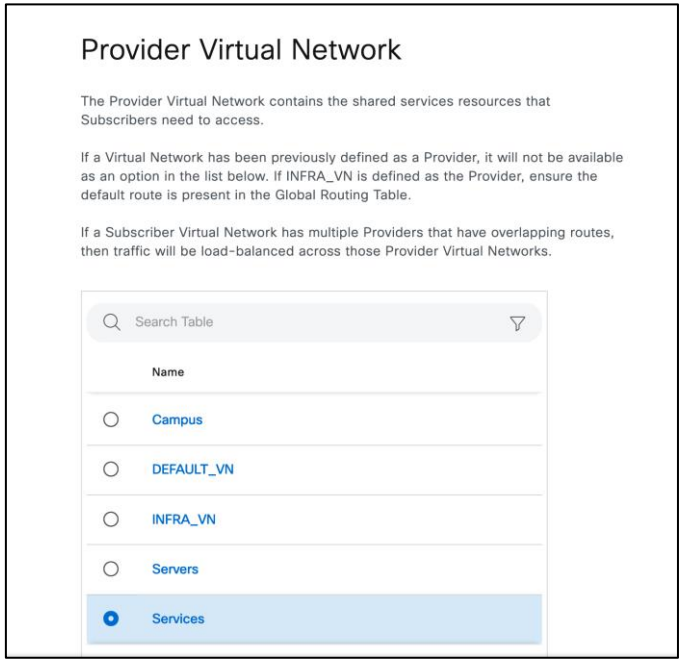


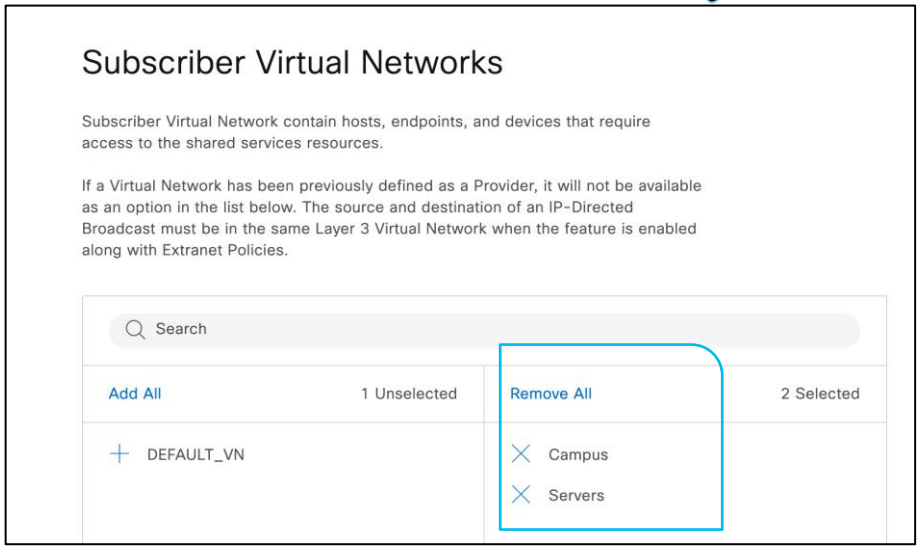




SD-Access Extranet Automation Workflow

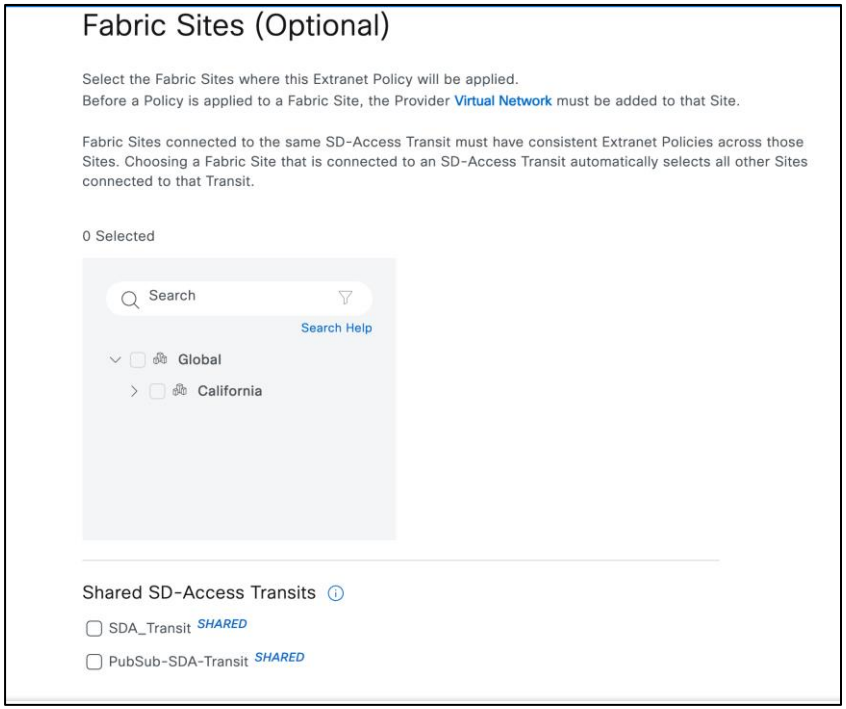
For Your Reference

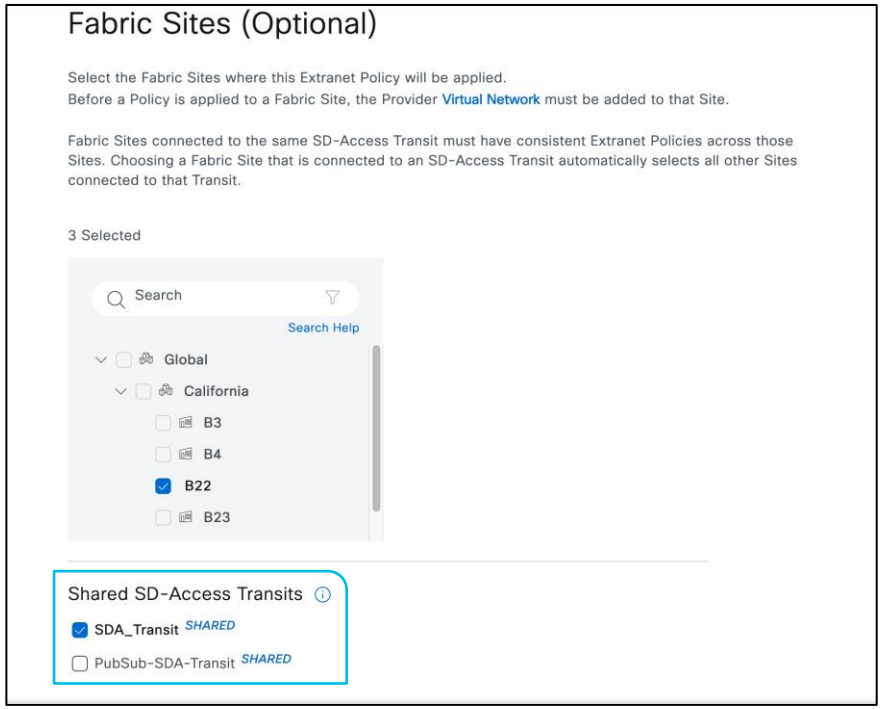




SD-Access Extranet Automation Workflow

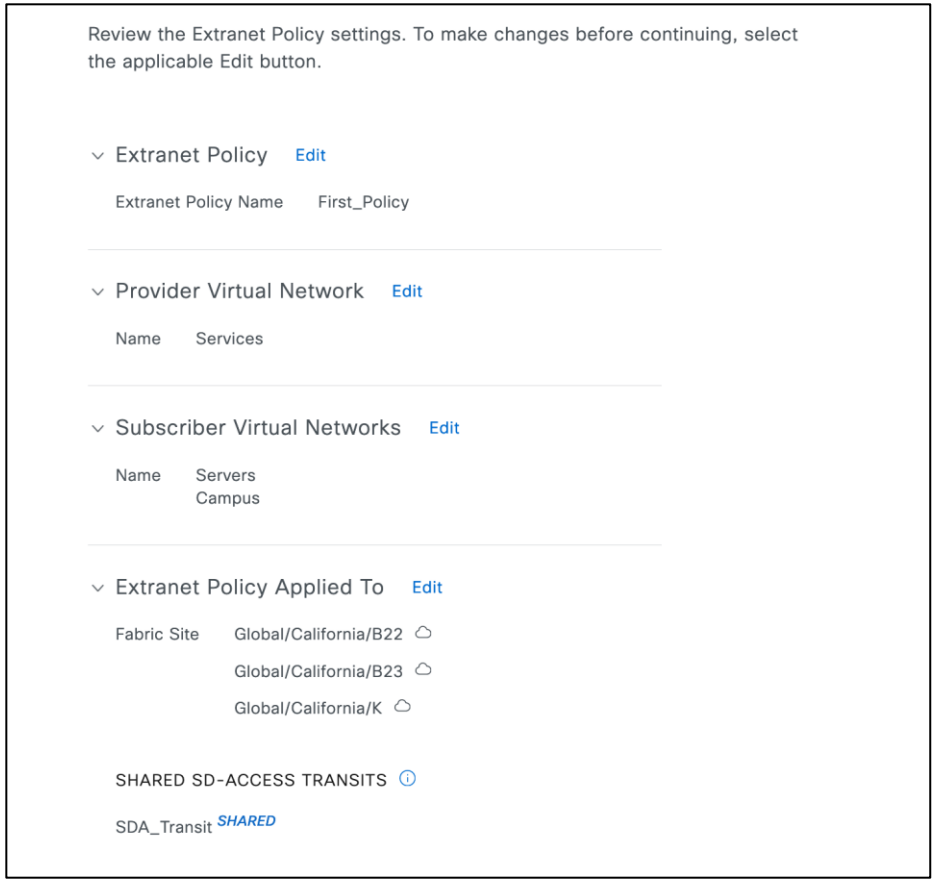
For Your Reference





SD-Access Extranet Automation Workflow

For Your Reference



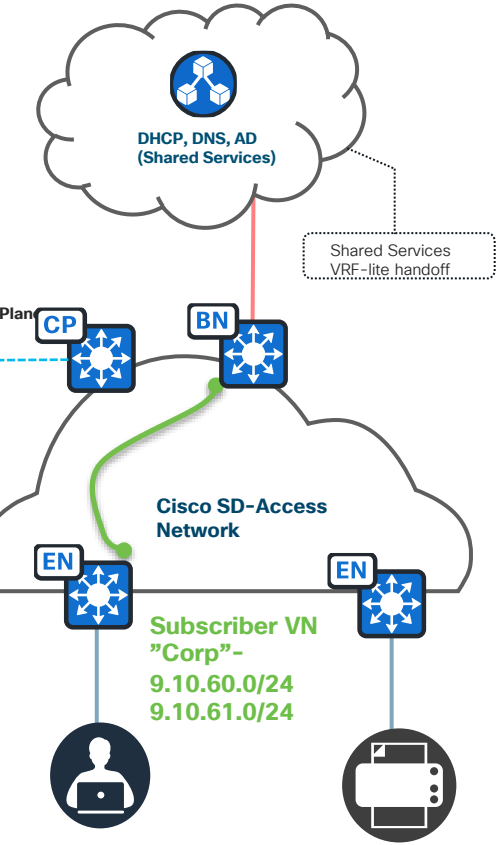
Cisco SD-Access Extranet

Single Site Example

For Your Reference

Extranet Policy created on Cisco DNA Center:

VN Policy Name	Provider VN	Subscriber VN
P1	Shared Services	Corp



Configuration

```
extranet p1
 eid-record-provider instance-id 4104
  ip-any
  exit-eid-record-provider
 !
 eid-record-subscriber instance-id 4105
  9.10.60.0/24
  9.10.61.0/24
  ip-any
  exit-eid-record-subscriber
 !
 exit-extranet
```

Extranet Policy

```
show lisp extranet p1 instance-id 4104
LISP Extranet policy table
Home Instance ID: 4104
Prov/Sub    Source             InstID     EID prefix
Provider    Default ETR Reg V4 4104
Subscriber  Config             4105       9.10.60.0/24
Subscriber  Config             4105       9.10.61.0/24
Total entries: 3
```

Cisco SD-Access Extranet

Multi-site Site Example

For Your Reference

Extranet policy configuration on Transit Control Plane Node:

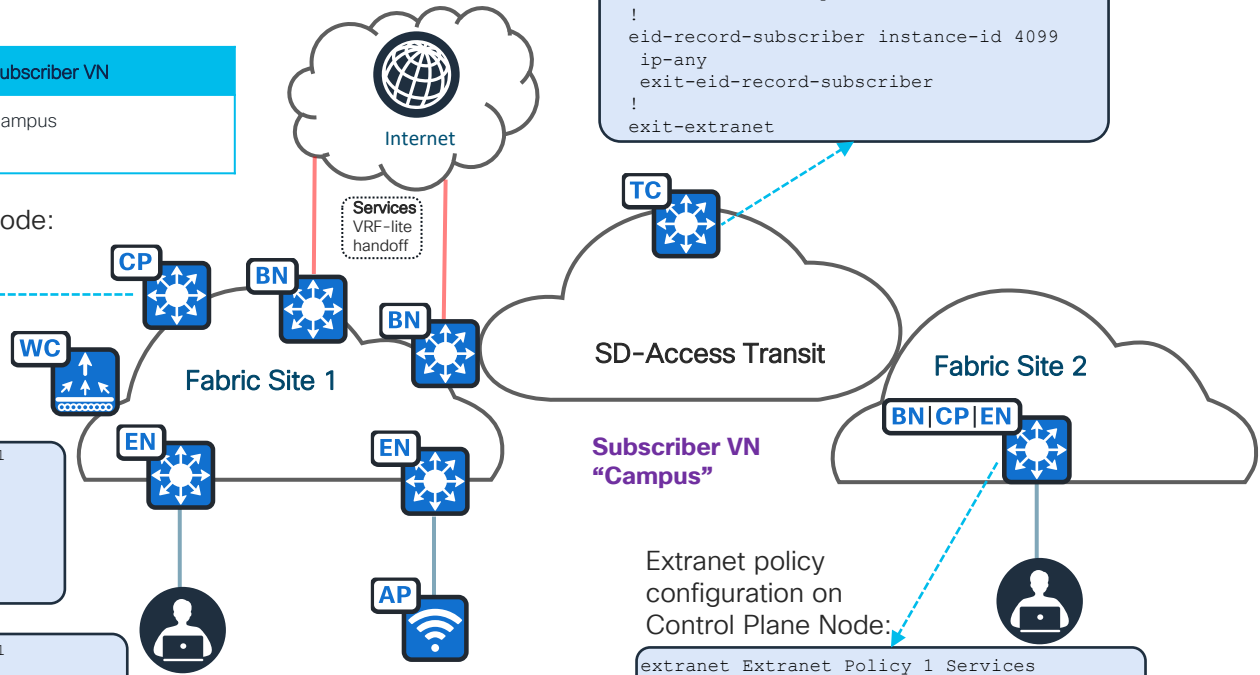
```
extranet Extranet_Policy_1_Services
  eid-record-provider instance-id 4101
   ip-any
   exit-eid-record-provider
  !
  eid-record-subscriber instance-id 4099
   ip-any
   exit-eid-record-subscriber
  !
  exit-extranet
```

Extranet Policy created on Cisco DNA Center:

VN Policy Name	Provider VN	Subscriber VN
Extranet_Policy_1_Services	Services	Campus

Extranet policy configuration on Control Plane Node:

```
extranet Extranet_Policy_1_Services
  extranet-config-from-transit
  eid-record-provider instance-id 4101
   exit-eid-record-provider
  !
  exit-extranet
```



Extranet Policy on Local CP :

```
show lisp extranet Extranet_Policy_1_Services instance-id 4101
LISP Extranet policy table
Home Instance ID: 4101
Prov/Sub     Source              InstID     EID prefix
Provider     Default ETR Reg V4  4101
Subscriber   Config-Propagation  4099       172.16.8.0/24
Subscriber   Config-Propagation  4099       172.16.42.0/24
Total entries: 3
```

Extranet Policy on TCP nodes :

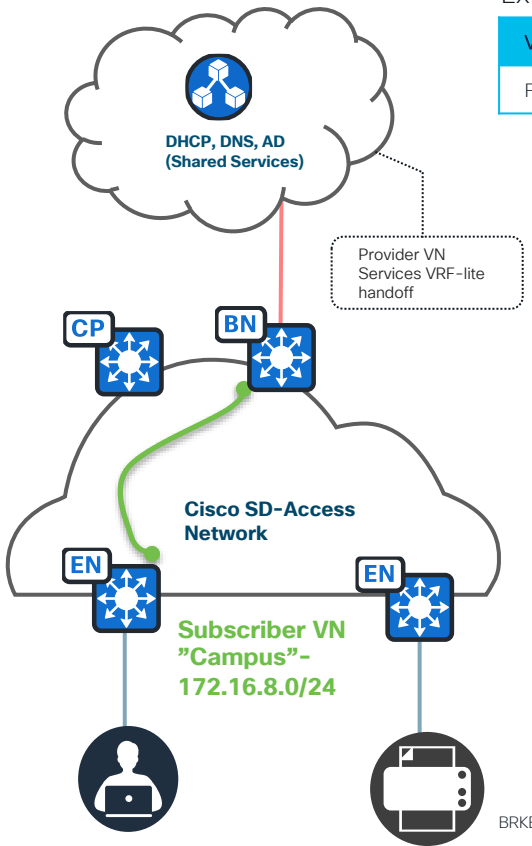
```
show lisp extranet Extranet_Policy_1_Services instance-id 4101
LISP Extranet policy table
Home Instance ID: 4101
Prov/Sub     Source              InstID     EID prefix
Provider     Default ETR Reg V4  4101
Subscriber   Dynamic             4099       172.16.8.0/24
Subscriber   Dynamic             4099       172.16.42.0/24
Total entries: 3
```

Extranet policy configuration on Control Plane Node:

```
extranet Extranet_Policy_1_Services
  extranet-config-from-transit
  eid-record-provider instance-id 4101
   exit-eid-record-provider
  !
  exit-extranet
```

Cisco SD-Access Extranet Demo

Cisco SD-Access Extranet Demo



Extranet Policy created on Cisco DNA Center:

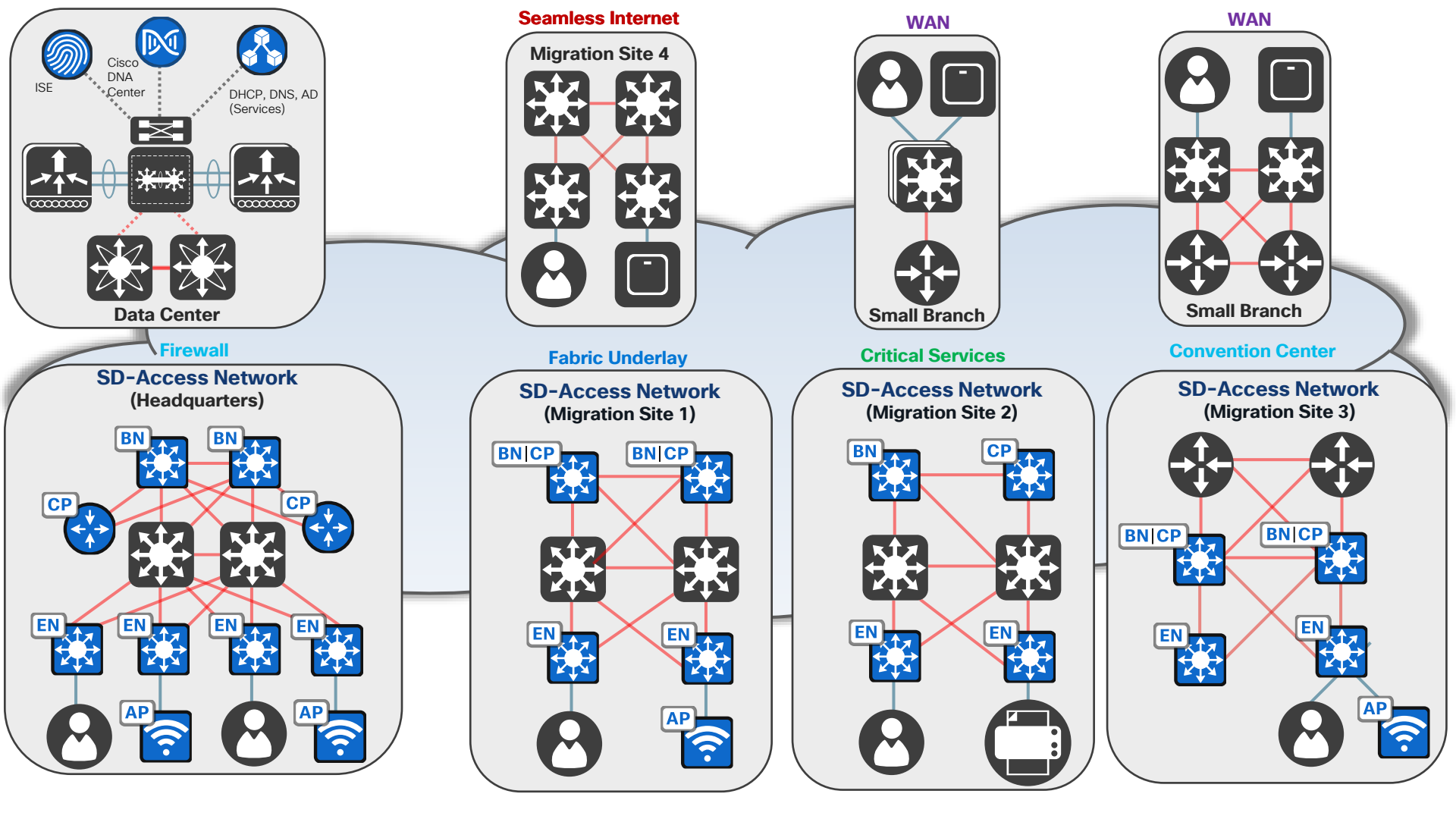
VN Policy Name	Provider VN	Subscriber VN
First_Policy	Services	Campus

Cisco SD-Access Extranet

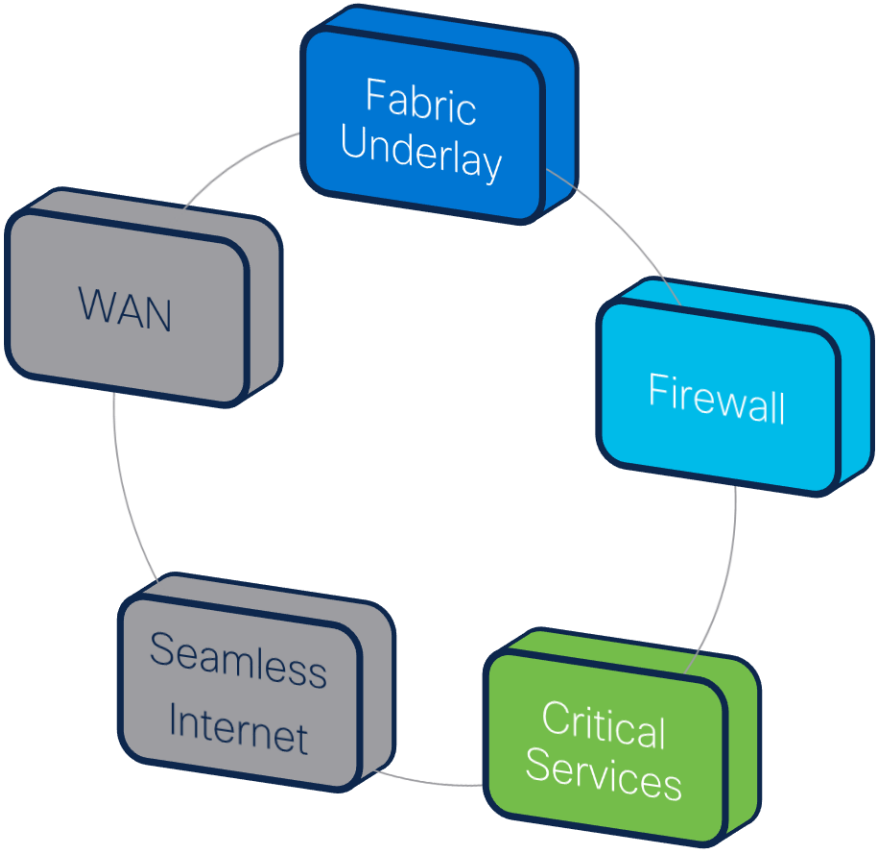
Key Take Away

Overview

- Automated Route Leaking Configuration via Cisco DNA Center.
- Subscriber to Subscriber communication is not supported.
  - Extranet is not meant to leak Fabric VRF to Fabric VRF.
  - If two devices inside the Fabric need to communicate with one another, put them in the same Virtual Network.
- If Inter-VN policy enforcement is desired on devices such as firewalls, then use traditional route leaking.


ISE
Cisco DNA Center
DHCP, DNS, AD (Services)
Data Center
Seamless Internet
Migration Site 4
WAN
Small Branch
WAN
Small Branch
Firewall
SD-Access Network
(Headquarters)
BN
CP
EN
AP
Fabric Underlay
SD-Access Network
(Migration Site 1)
BN|CP
Critical Services
SD-Access Network
(Migration Site 2)
Convention Center
SD-Access Network
(Migration Site 3)

Progress Chart



Seamless Internet Connectivity

LISP Pub/Sub

Cisco SD-Access

Seamless Internet Connectivity

- Consistent Policy across Cisco SD-Access sites.
- No loss in Internet Connectivity(Active/Backup Internet).

Cisco SD-Access

Seamless Internet Connectivity

- Cisco SD-Access Transit
- LISP Publisher/Subscriber

SD-Access Transits

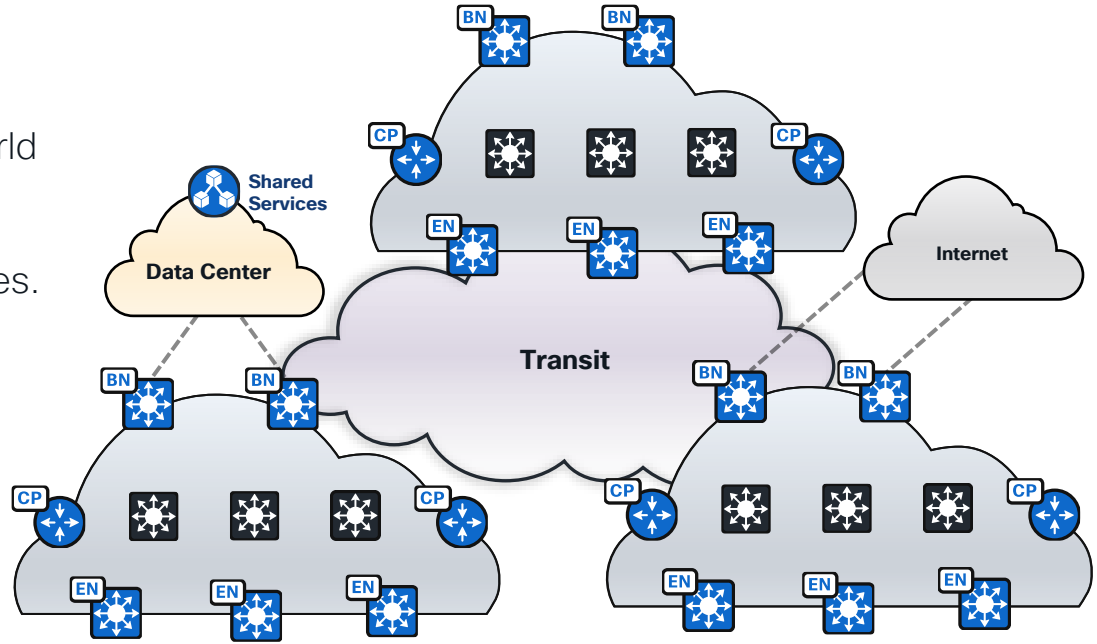
Fabric Constructs

Transits – A Closer Look

RECAP

Transits connect a Fabric Site to another network or another Fabric Site.

- Connect a Fabric Site to the external world and the Data Center.
- Connects Fabric Site to other Fabric Sites.



Fabric Constructs

Transits – A Closer Look

SD-Access Transit

- Maintains Cisco SD-Access constructs (LISP,VXLAN,CTS) natively between sites.
- End-to-end policy maintained using Fabric encapsulation
- End-to-end automated by Cisco DNA Center
- Uses domain-wide Control Plane Nodes for inter-site control plane communication
- Requires WAN / MAN to support a large enough MTU for 50-byte VXLAN header

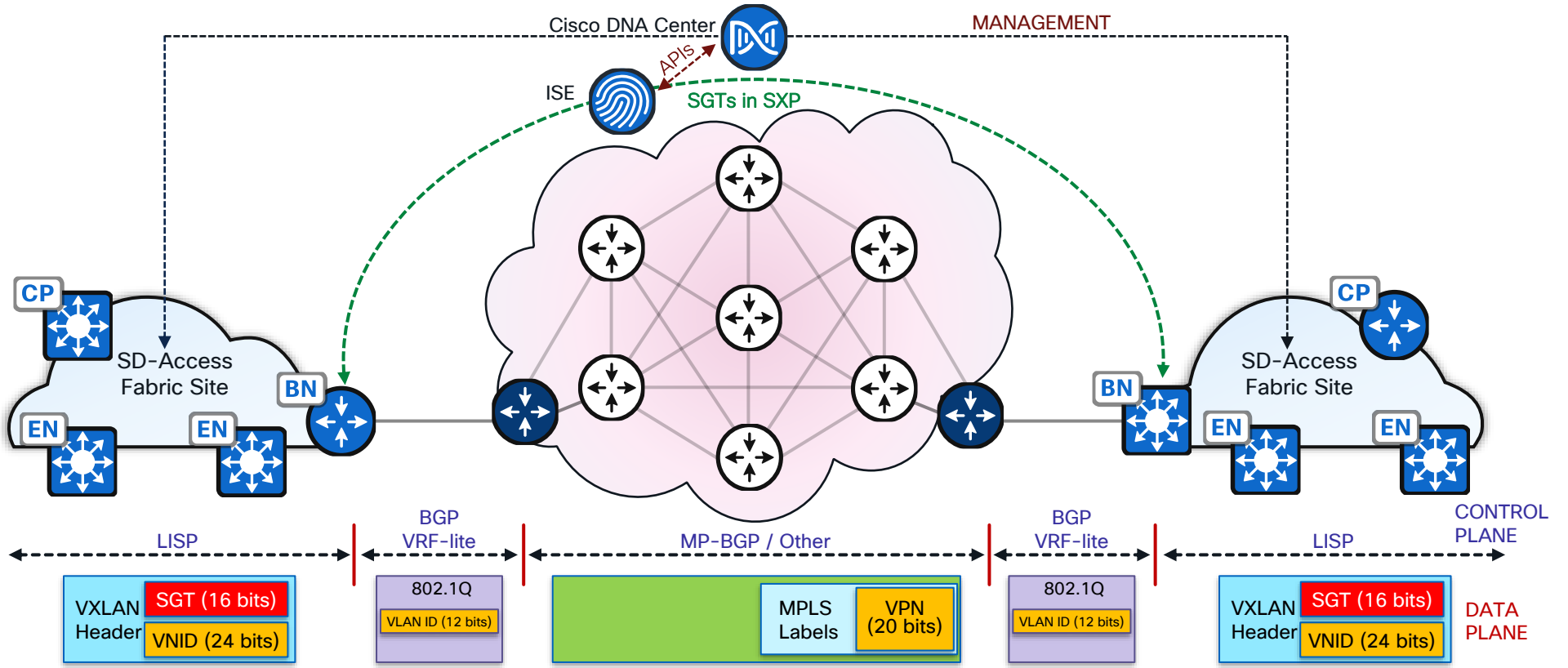
IP-Based Transit

- Borders hand off traffic direct to external domain with VRF-lite and BGP
- End-to-end policy maintained using manual configuration
- Requires remapping of VRFs and SGTs to maintain policy and segmentation between Sites
- Traffic between sites use external networks' control plane and data plane protocols

For More Information: Cisco SD-Access – Connecting Multiple Sites in a Single Fabric Domain - BRKENS-2815

Generic IP-Based WAN Transit Between Fabric Sites

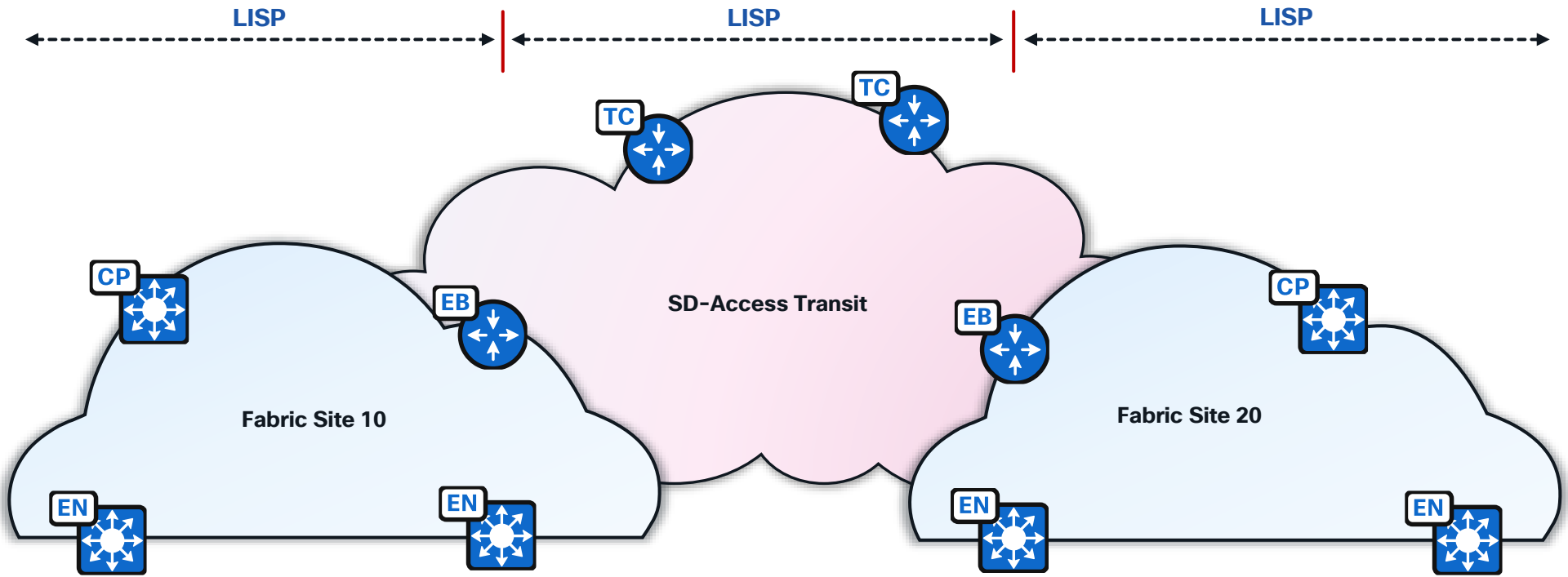
RECAP



Cisco SD-Access Transit

Control Plane

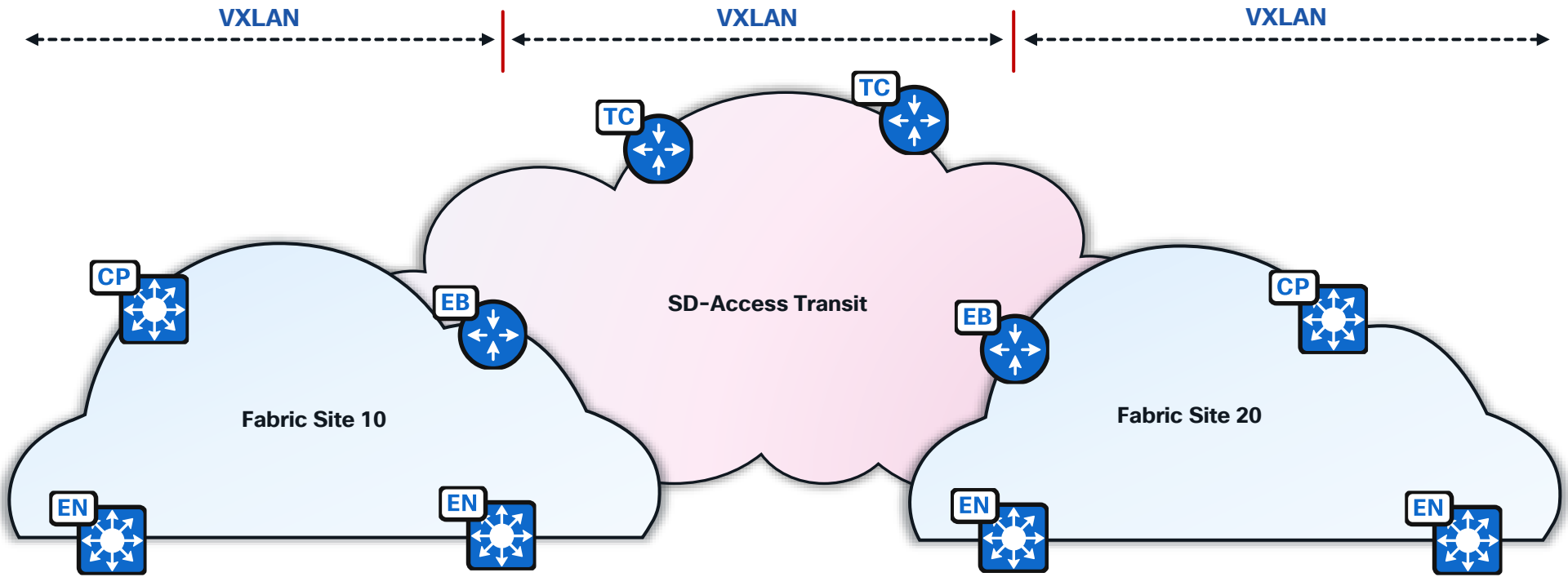
RECAP



Cisco SD-Access Transit

Data Plane

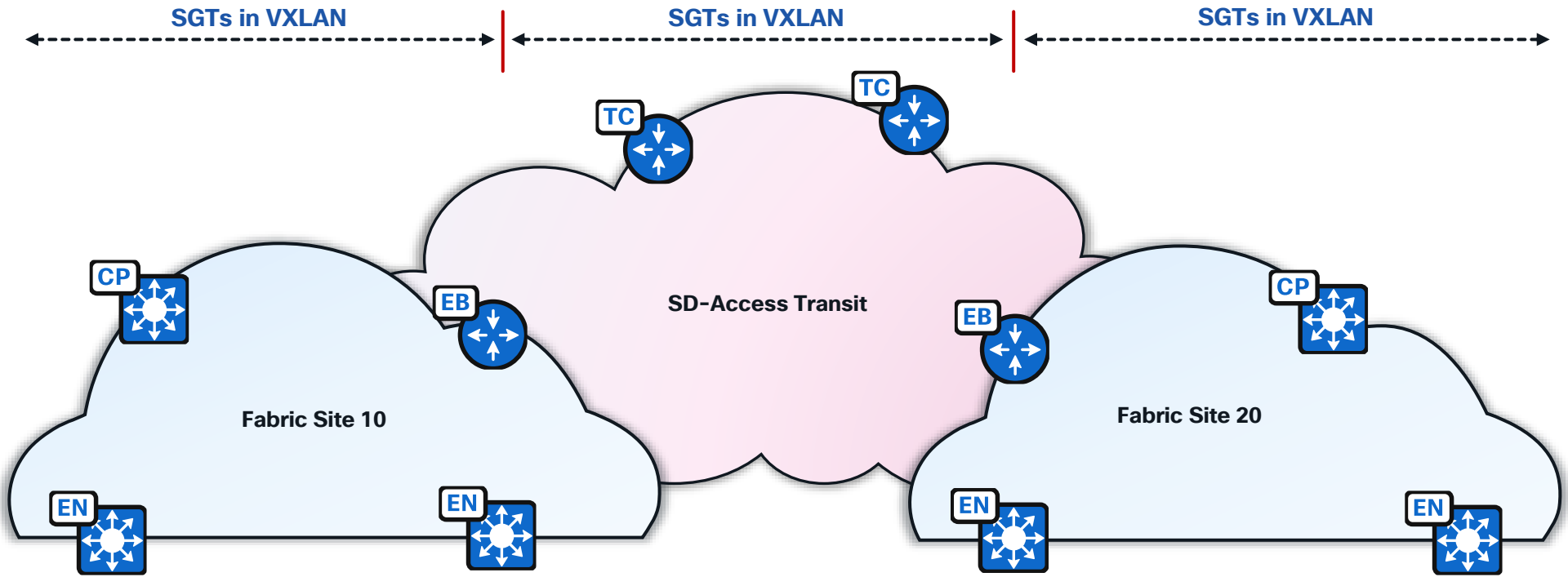
RECAP



Cisco SD-Access Transit

Policy Plane

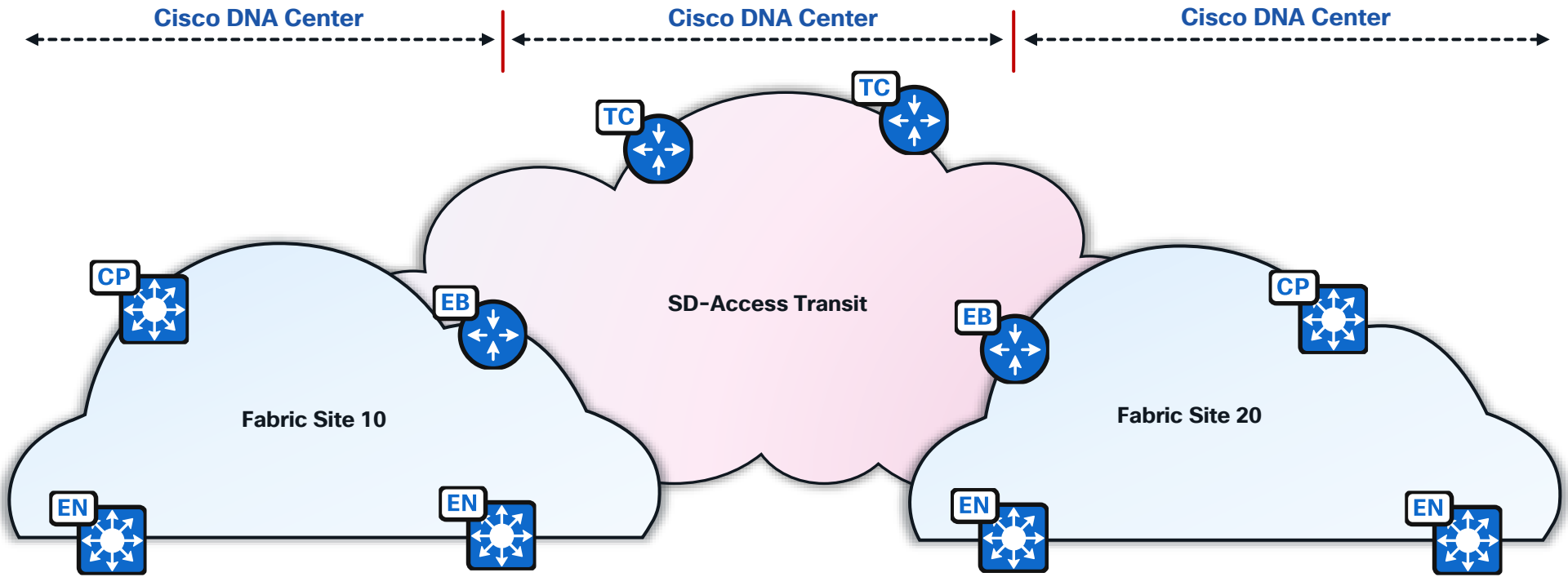
RECAP



Cisco SD-Access Transit

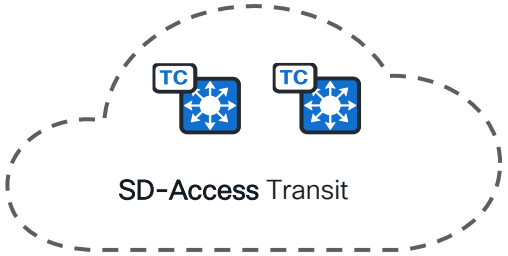
Management Plane

RECAP



Cisco SD-Access Deployment

Multisite Deployment with SD-Access Transit



SD-Access Transit is a native solution carrying VN and SGT between Fabric sites.

Key Considerations:

- Higher MTU support

- Transit Control Plane nodes are **dedicated devices** with IP reachability to every fabric site's Border nodes
- Transit Control Plane nodes is **not required to be in data forwarding path**
- Transit Control Plane nodes maintains aggregate prefixes of all Fabric sites
- Fabric site Border node should be either External or Anywhere border type to connect to SD-Access Transit.
- SD-Access Transit can be deployed with LISP-BGP or **LISP Pub/Sub**

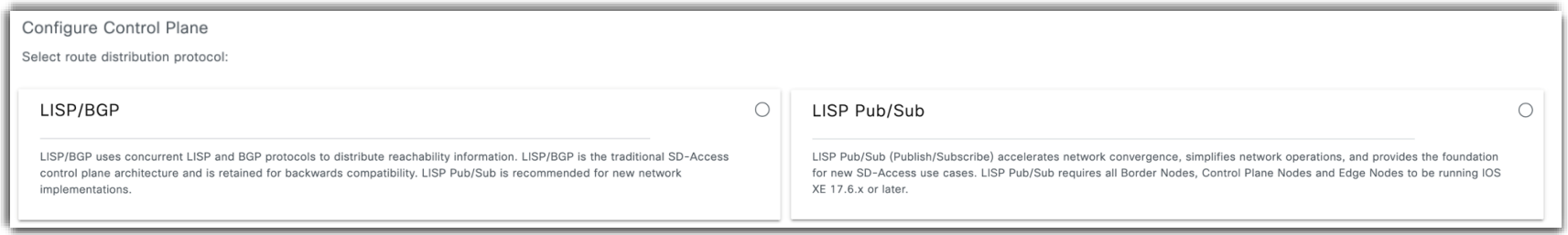
For Your Reference

SD-Access Control Plane Protocols

An Introduction to LISP Pub/Sub

cisco Live!

SD-Access Control Plane Protocol
Cisco DNA Center 2.2.3.x



LISP/BGP

- Released circa 2017
- An instant classic
- Reliable and Stable
- BGP Transport

LISP Pub/Sub

- Released in 2021
- An instant masterpiece
- Reliable and Stable
- Native LISP Transport
- Highly Extensible

LISP Pub/Sub

What Challenges are We Solving?

Extensibility

- LISP Pub/Sub builds a new framework for LISP infrastructure.
- LISP Pub/Sub architecture is a building block for other features and capabilities:
  - Dynamic Default Border Node
  - LISP Backup Internet
  - SD-Access Extranet

LISP Pub/Sub

Architecture Introduction

- LISP Pub/Sub is new control plane protocol for SD-Access.
- It is a signaling protocol to carry information such as as prefixes, mappings, and other data.
- LISP Pub/Sub provides the capability to selectively push information.

Architecture Use Cases

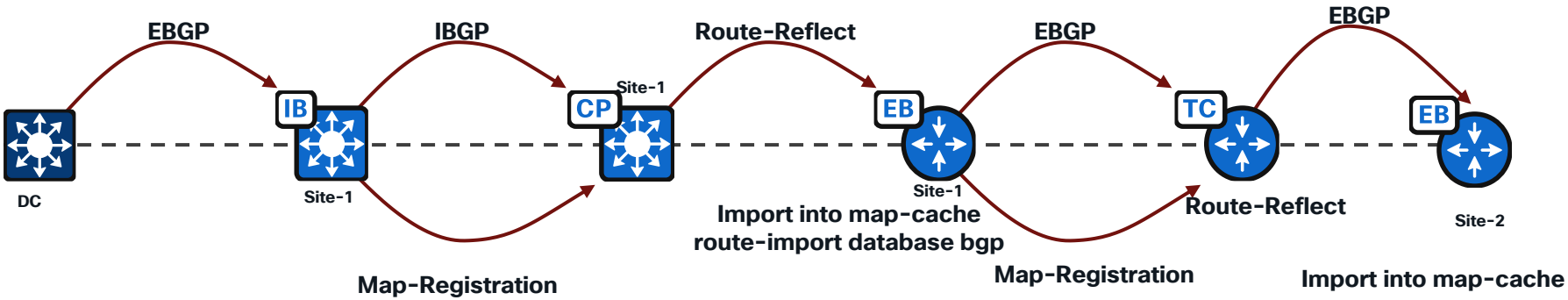
- LISP Pub/Sub removes the dependency of BGP to propagate information within the Fabric Site.
- LISP Pub/Sub adds new features and capabilities because of the information it can carry.

LISP/BGP Control Plane

Before LISP Pub/Sub

Reliance on BGP

- To push LISP Site-Registration table to another device, another protocol was needed.
- BGP was used as that transport
- This created an underlying reliance on BGP.



LISP/BGP Control Plane

Before LISP Pub/Sub

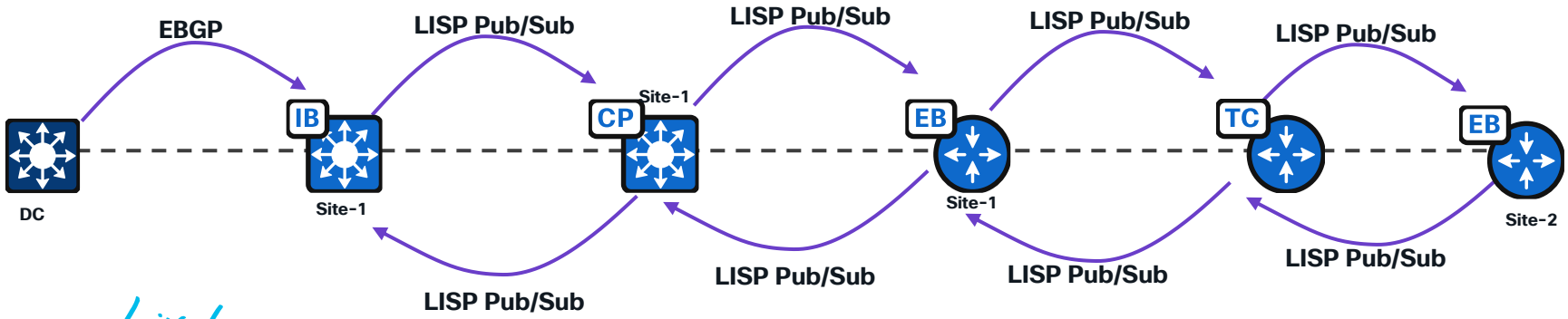
Reliance on BGP

- With BGP, LISP only knows the prefixes, not full EID-to-RLOC mappings.
  - BGP populates map-cache with an incomplete entry
- Map-cache is fully resolved through map-requests
  - This mean additional control plane protocol messages.
- When BGP reconverges, map-cache needs to updated.
  - This means further control plane messages

LISP Pub/Sub Control Plane

The Architecture Evolution

- LISP Pub/Sub introduces the capability within the control plane signaling of LISP to selectively push information.
- The mapping system (Control Plane Node) notifies PITRs (Border Nodes) about mapping changes along with additional details associated with those mappings.
- LISP Pub/Sub uses native LISP, devoid of external protocol such as BGP, to propagate the prefixes and full mapping information.



LISP Pub/Sub Control Plane

Basic Definitions – Part 1

Subscription

- The process LISP devices use to express interest for a certain portion of information within the mapping system.

Publication

- The information that the mapping system sends to the Subscriber (the LISP device).

LISP Pub/Sub Control Plane

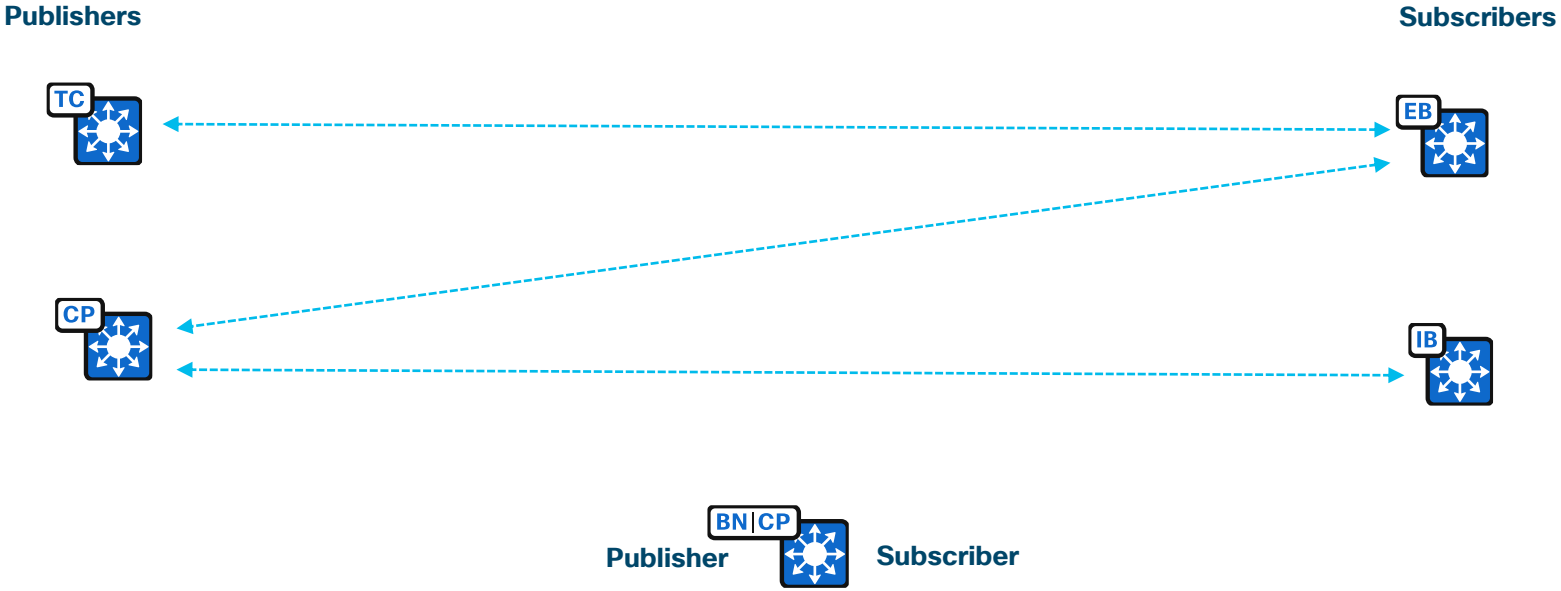
Basic Definitions – Part 2

Subscribers

- Border Nodes

Publishers

- Control Plane Nodes/Transit Control Plane Nodes



LISP Pub/Sub

Details

- In release 2.2.3.x, LISP Pub/Sub is supported only for newly created fabric sites with devices running IOS XE software ≥17.6.x
- Migration from LISP/BGP to LISP Pub/Sub is not currently available.
- When we upgrade DNAC release to DNAC 2.2.3.x fabric sites created prior to this will continue to operate with LISP BGP based fabric.
- Transit Control Plane Nodes can support LISP/BGP fabric sites or LISP Pub/Sub-based fabric sites, not both simultaneously.

LISP Dynamic Default Border Node

LISP Pub/Sub – Dynamic Default Border

Current Network Challenges

Loss of Default Route

- If a Border Node's losses the default route, it can take minutes for the network to converge (BGP).
  - Note: This a common routing challenge that is not specific to SD-Access LISP Fabric.

Potential Ways to Solve For Loss of Default Route

- Bidirectional Forwarding Detection (BFD)
- Per-VRF IBGP between redundant Border Nodes
- EEM scripts tracking state of EBGP Peers

Note: Convergence of the network after a Border Node reload is the responsibility of the IGP in the underlay.

Fabric Gateway of Last Resort

LISP BGP

LISP BGP

Problem Statement

- Configure an Edge Node to use one or Border Nodes as the Fabric Gateway of Last Resort.
  - Configure an xTR to use one or more PeTRs as the gateway of last resort in the Fabric Site.

LISP BGP

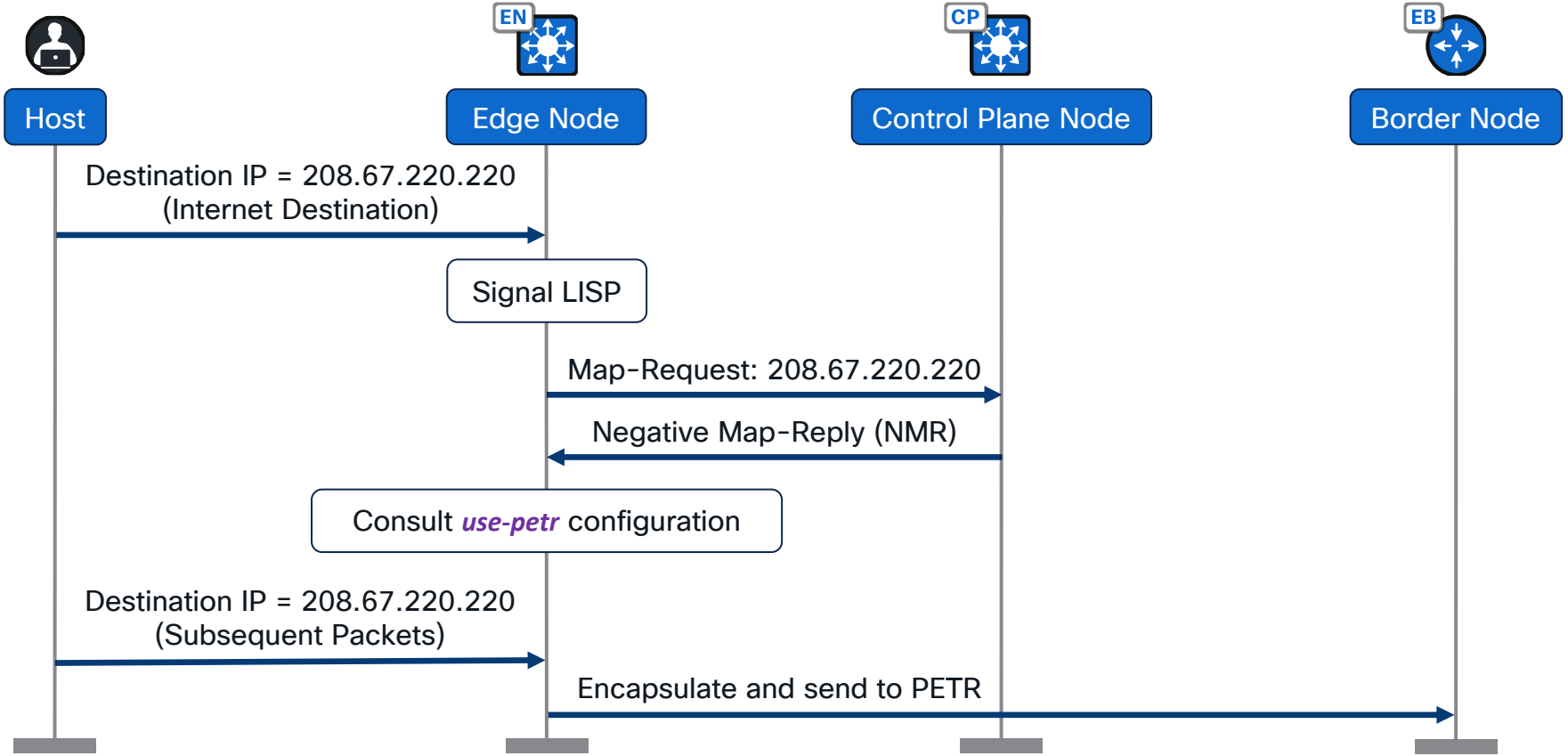
Static Solution

- Static use-petr configuration is used on all the xTRs to configure the proxy-ETR.
- When the xTR receives NMR from map server, xTRs forward traffic to this configured proxy-ETR.
- Configured proxy-ETRs cannot be changed dynamically if external connectivity at the proxy-ETR changes.

```
router lisp
! Output omitted for brevity

 service ipv4
  itr map-resolver 192.168.10.1
  etr map-server 192.168.10.1
  etr
  use-petr 192.168.30.7
  use-petr 192.168.30.8
  proxy-itr 192.168.30.5
  exit-service-ipv4
```

Static use-petr configuration

LISP BGP Forwarding Logic



Fabric Gateway of Last Resort

LISP Pub/Sub

cisco Live!

LISP Pub/Sub – Dynamic Default Border

Problem Statement

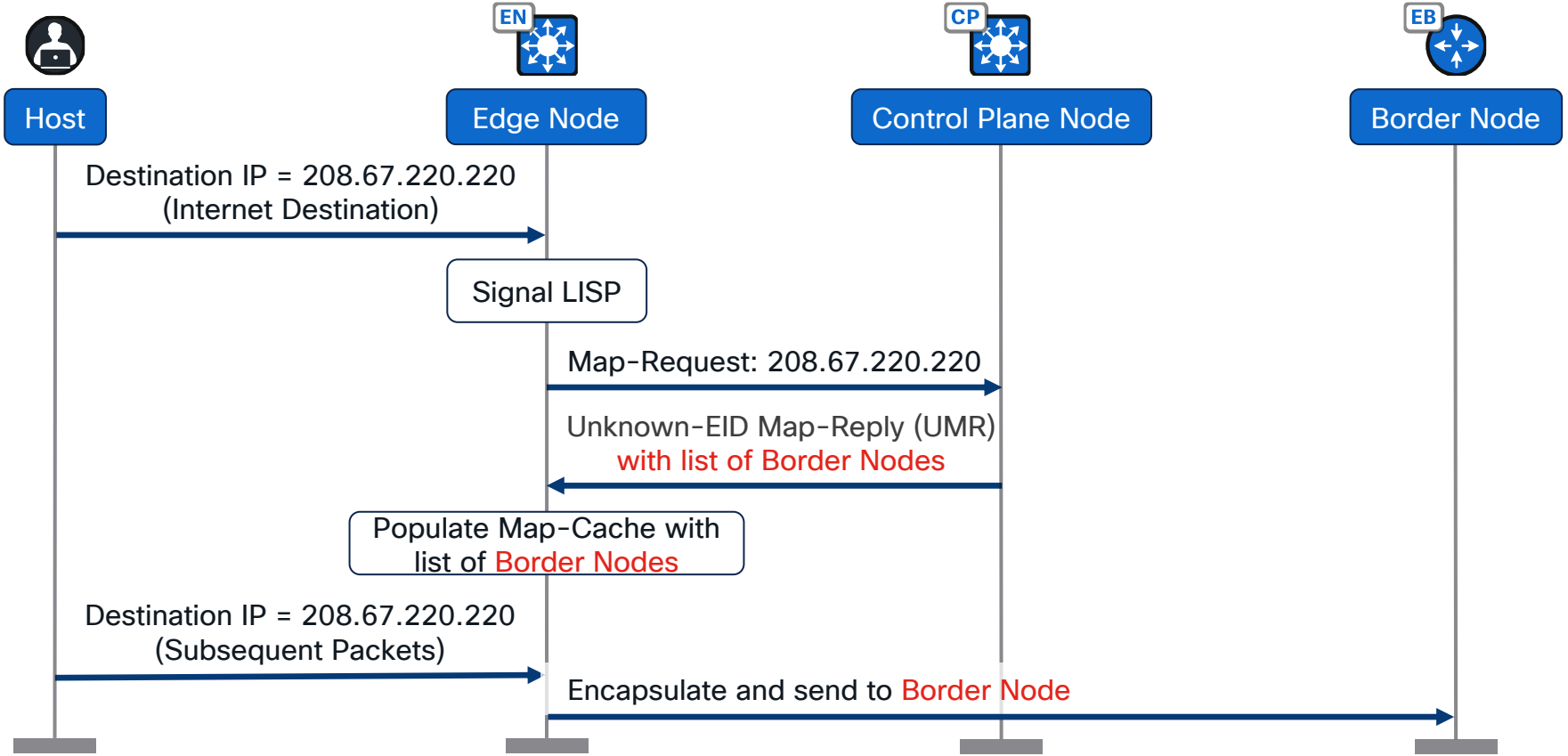
- Configure an Edge Node to use one or Border Nodes as the Fabric Gateway of Last Resort.
  - Configure an xTR to use one or more PeTRs as the gateway of last resort in the Fabric Site.

LISP Pub/Sub – Dynamic Default Border

Solution

- Implement LISP to monitor for the presence or absence of the default route Border Nodes.
  - Do this on a per-VRF basis.
- Provide a method for the Border Nodes to registered the state of the default route to the Control Plane Nodes.
- Dynamically program this default route state information into map-cache on the Edge Nodes.

LISP Pub/Sub Solution Forwarding Logic



LISP Pub/Sub – Dynamic Default Border

Definition of Terms

Registration

- A Border Node tracks the state of the default route for a given VRF.
- A Border Node then notifies the Control Plane Node of the state of the default route.

De-prioritization

- A Border Node notifies the Control Plane Node of the loss of the default route.
  - The Border Node registers itself with the Control Plane Node with a LISP Priority of 255.
  - A LISP Priority of 255 indicates the Border Node cannot be used as a Fabric Gateway of Last Resort.

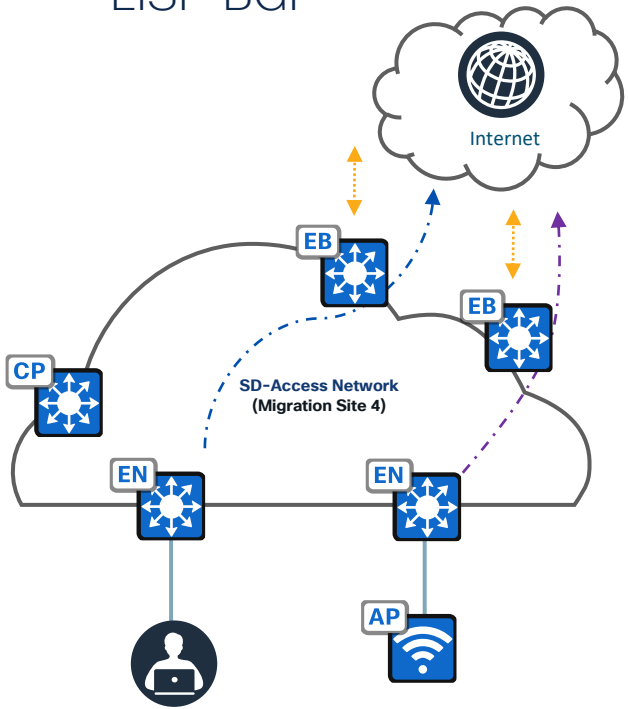
LISP Pub/Sub – Dynamic Default Border

Details

- Dynamic Default Border is enabled by default when we have external borders in the fabric.
- Dynamic Default Border works only with LISP Pub/Sub-based fabrics.
- Dynamic Default Border monitors the default route on External Border/s and registers that with Control Plane node/s
- With Dynamic Default Border, if external border/s loses upstream connectivity, fabric Edge nodes will no longer forward traffic to those external borders, and will dynamically detect and forward the traffic via other available external borders
- With this functionality, traffic within the fabric will quickly converge minimizing traffic loss towards border and traverse traffic through the other border.
- This avoids the need of configuring iBGP manually between external borders.
- With Dynamic Default Border feature fabric edges will not have static “use-petr” anymore instead they will dynamically route the traffic to the border with active default route.
- Depending on the design, Border Node/s are going to register the default route with Local/Transit Control Plane node/s

LISP Pub/Sub – Dynamic Default Border

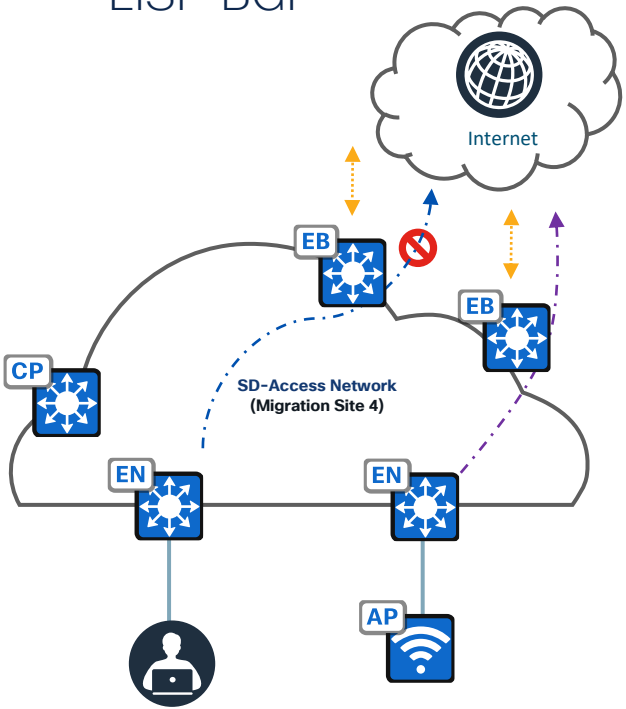
LISP BGP



iBGP- Manual/Templates
eBGP- Automated

LISP Pub/Sub – Dynamic Default Border

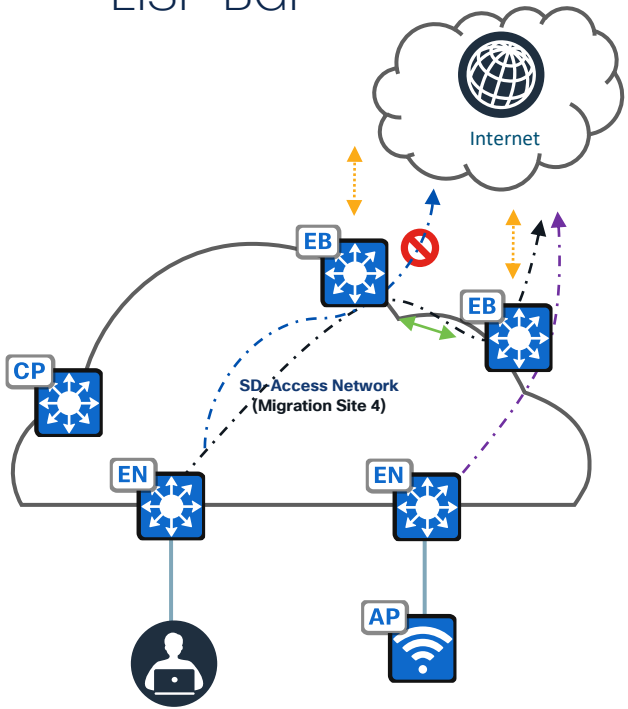
LISP BGP



iBGP- Manual/Templates
eBGP- Automated

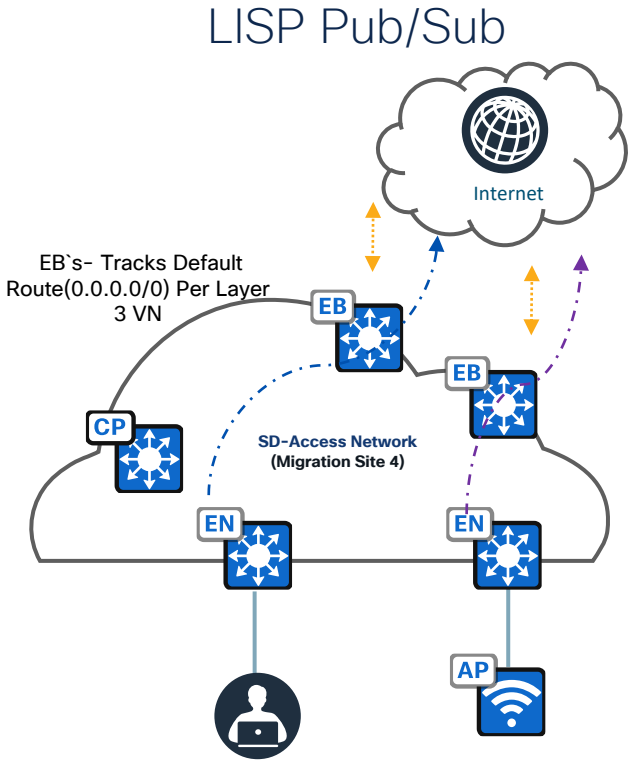
LISP Pub/Sub – Dynamic Default Border

LISP BGP



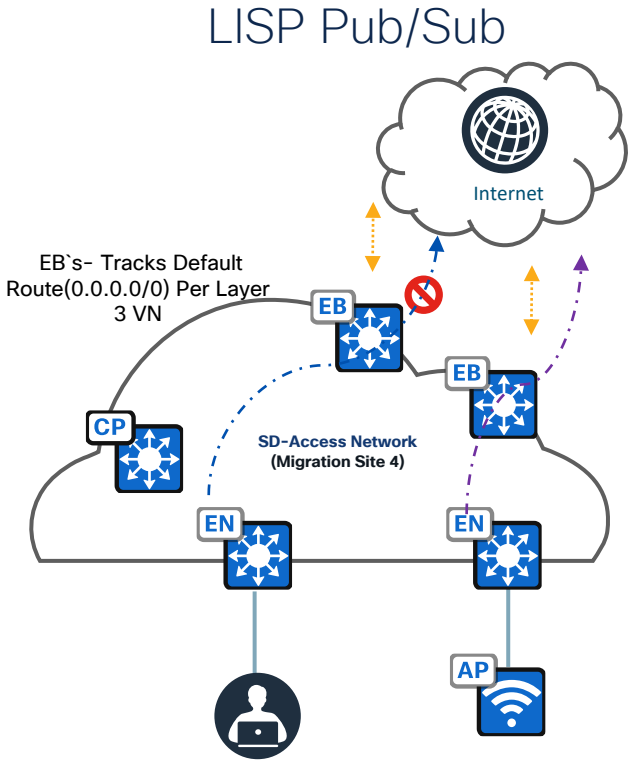
iBGP- Manual/Templates
eBGP- Automated

LISP Pub/Sub – Dynamic Default Border



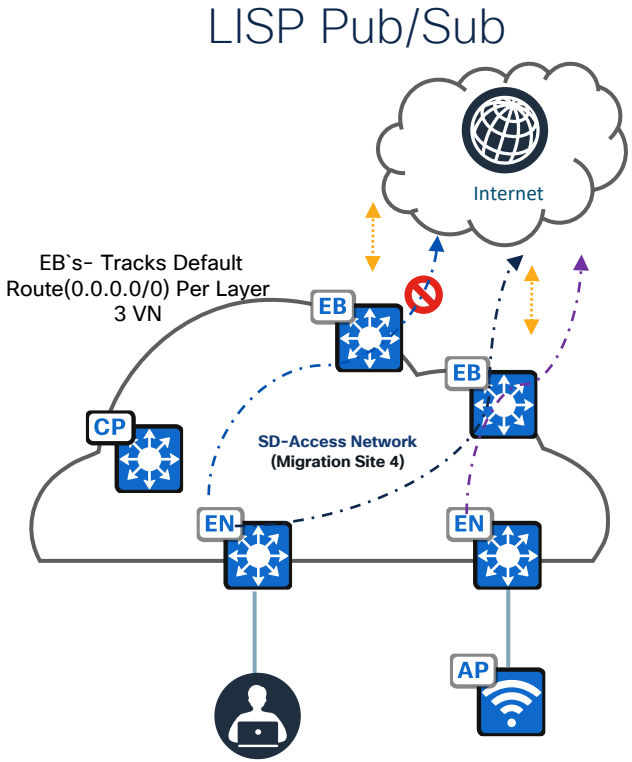
iBGP- Manual/Templates
eBGP- Automated

LISP Pub/Sub – Dynamic Default Border



iBGP- Manual/Templates
eBGP- Automated

LISP Pub/Sub – Dynamic Default Border



iBGP- Manual/Templates
eBGP- Automated

LISP Backup Internet

LISP Backup Internet

Comparison of Functionality

Dynamic Default Border Node

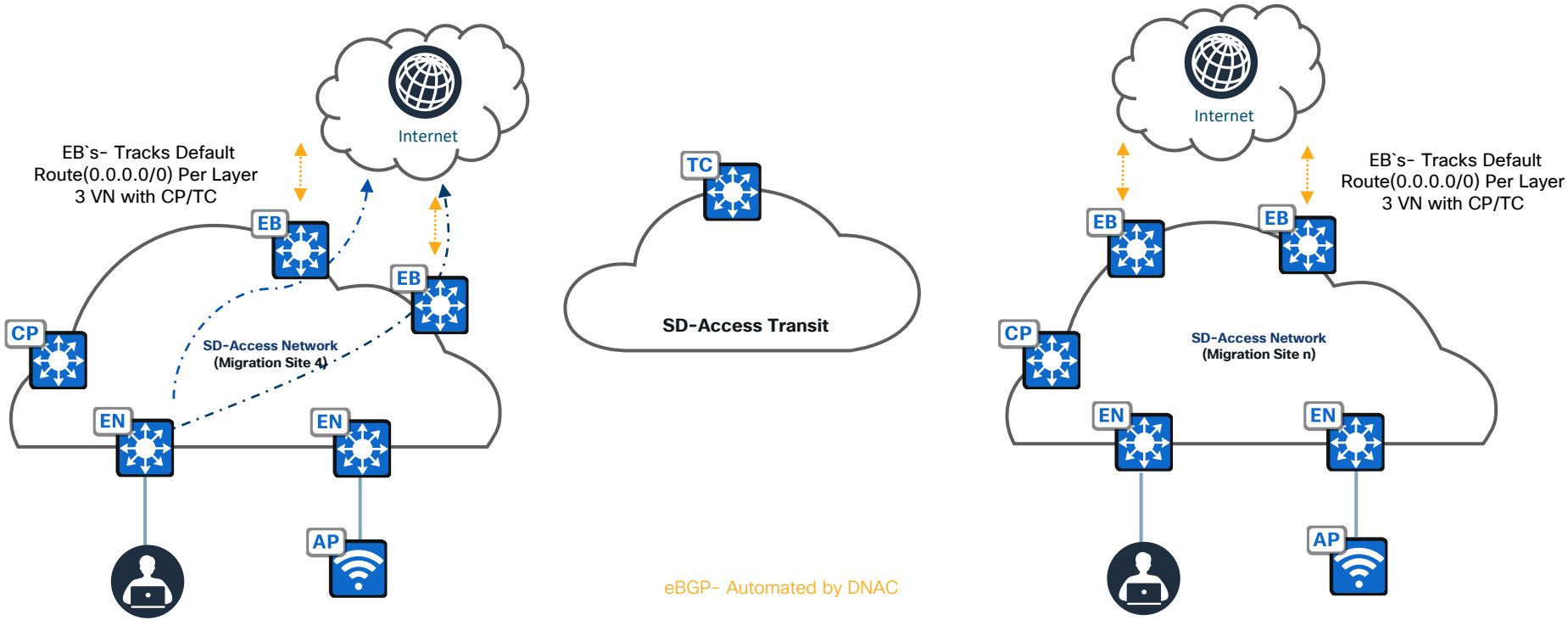
- Border Convergence within a single Fabric Site.
- Results in the removal of using ***use-petr*** within the Fabric Site.

Backup Internet

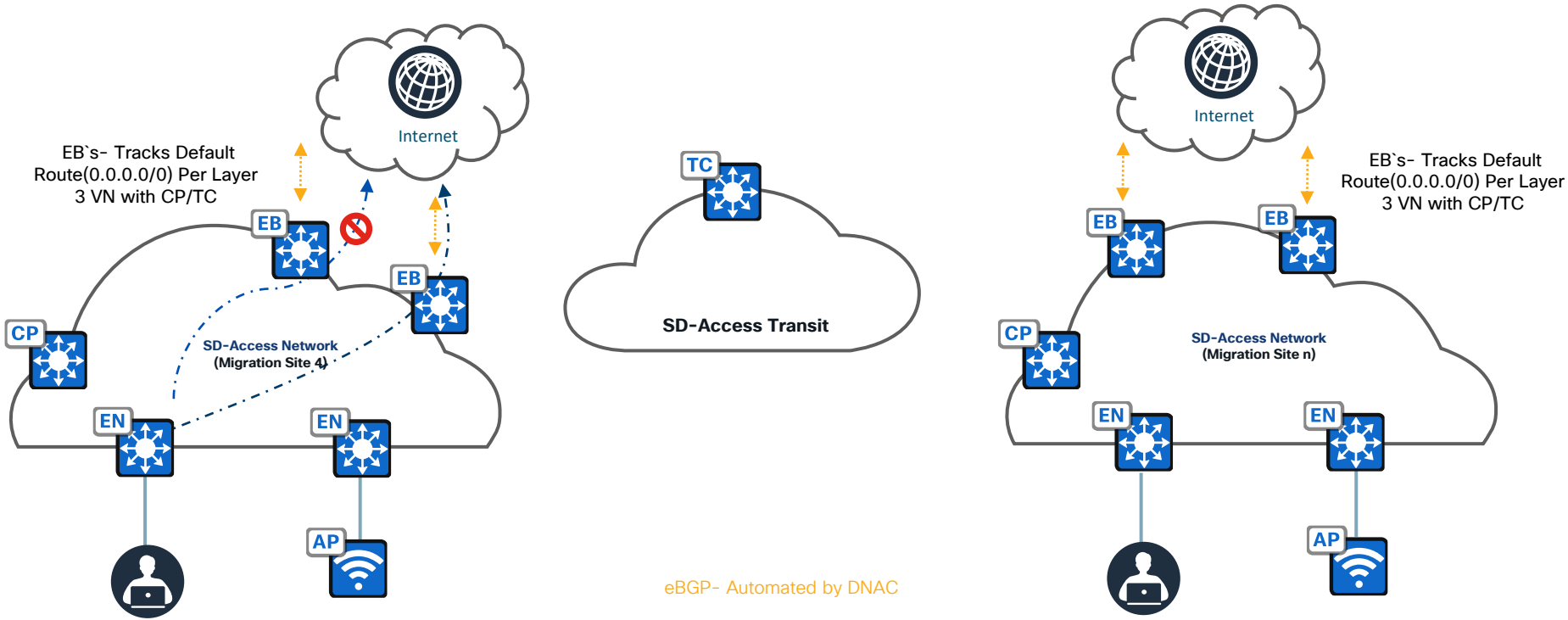
- Essentially Border Convergence across an SD-Access Transit.
- Results in the removal of using ***use-petr*** within the Fabric Domain.

- LISP Backup Internet builds on top of Dynamic Default Border Node feature.

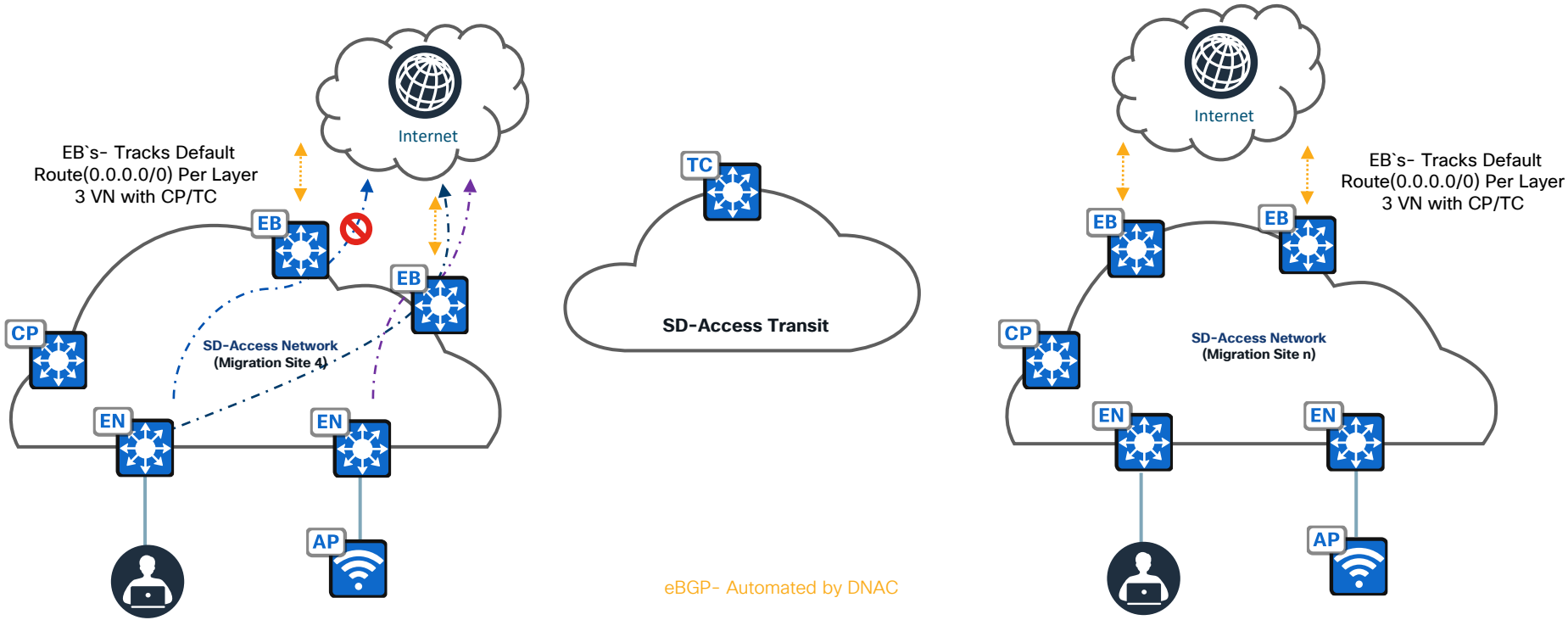
LISP Backup Internet



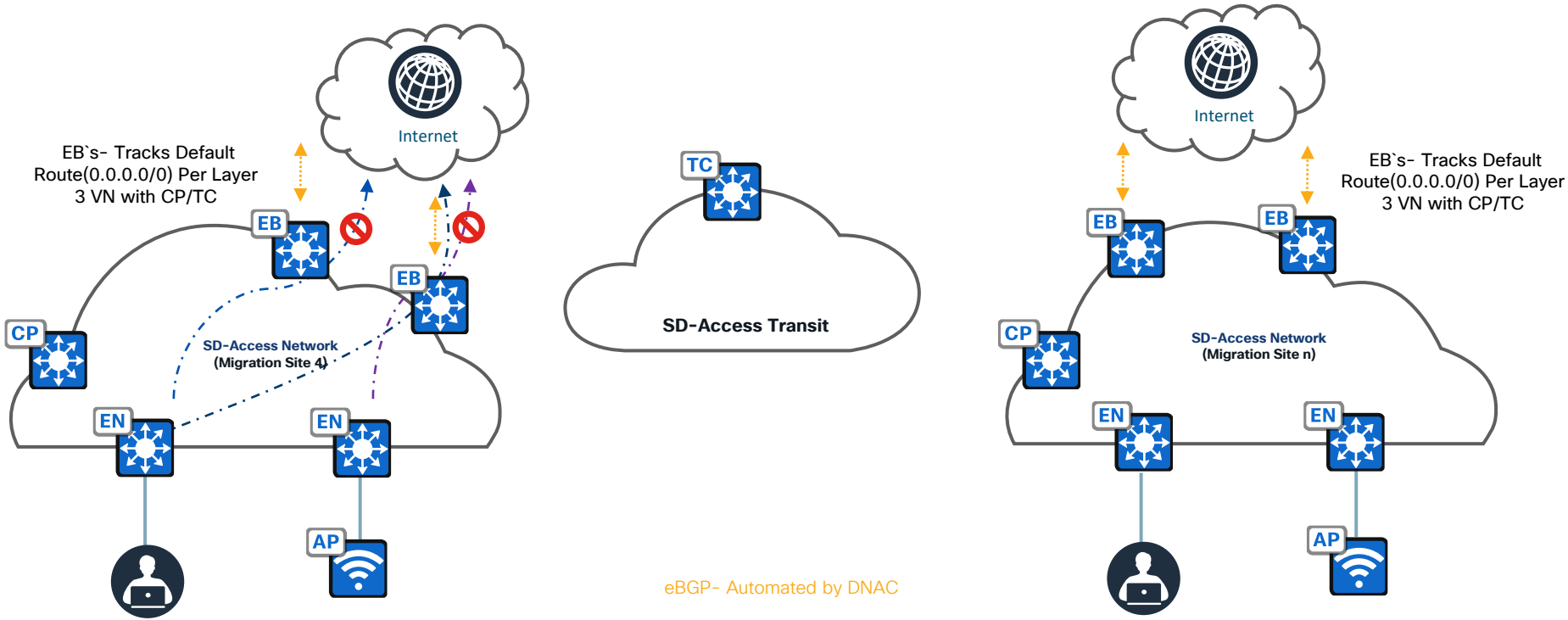
LISP Backup Internet



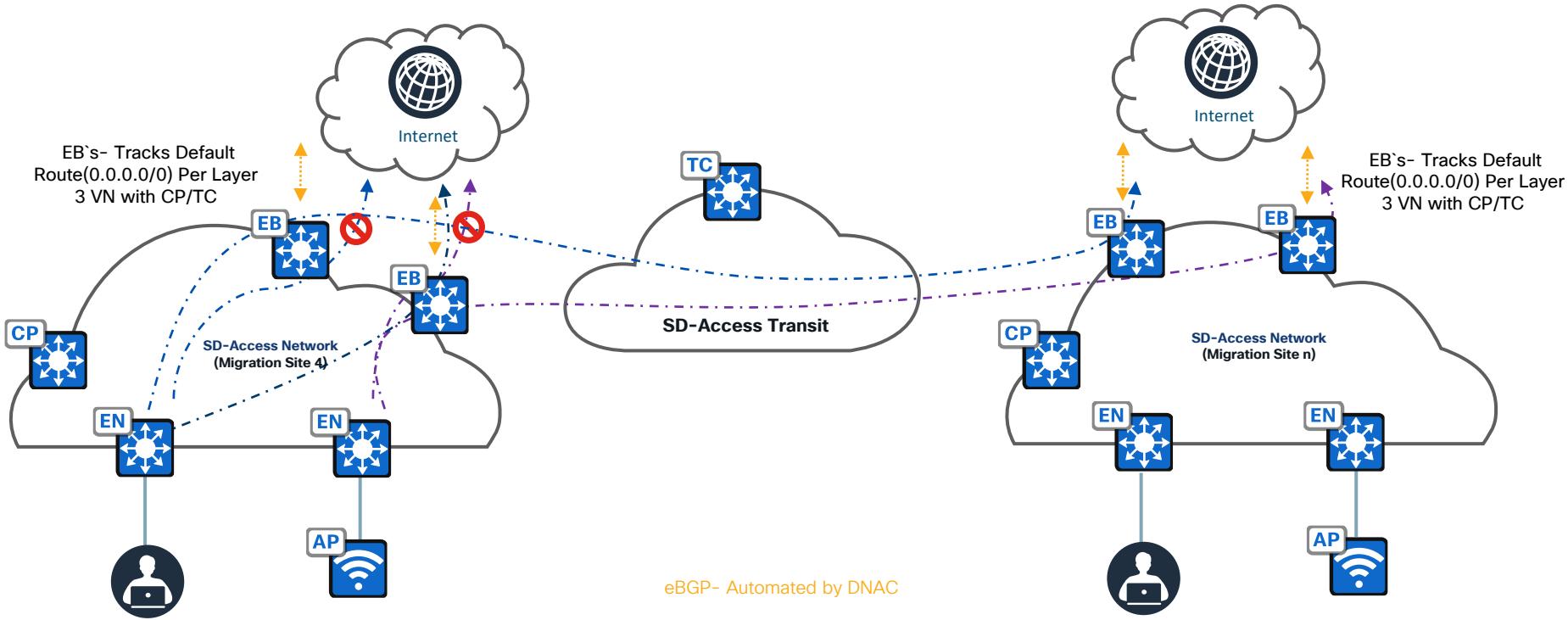
LISP Backup Internet



LISP Backup Internet



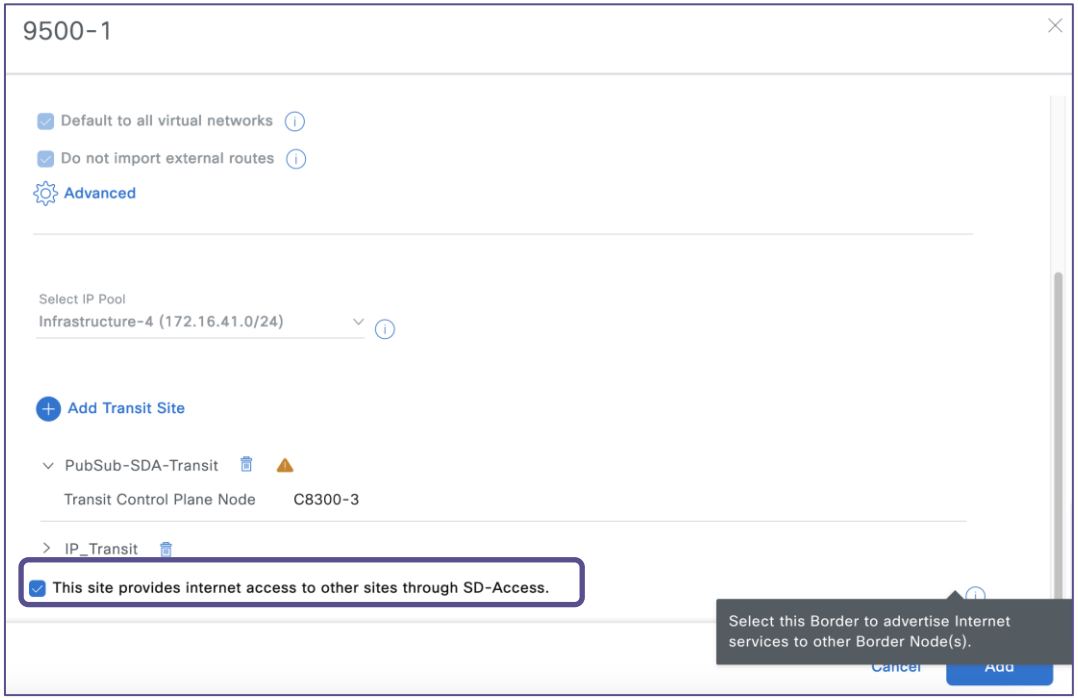
LISP Backup Internet



LISP Backup Internet

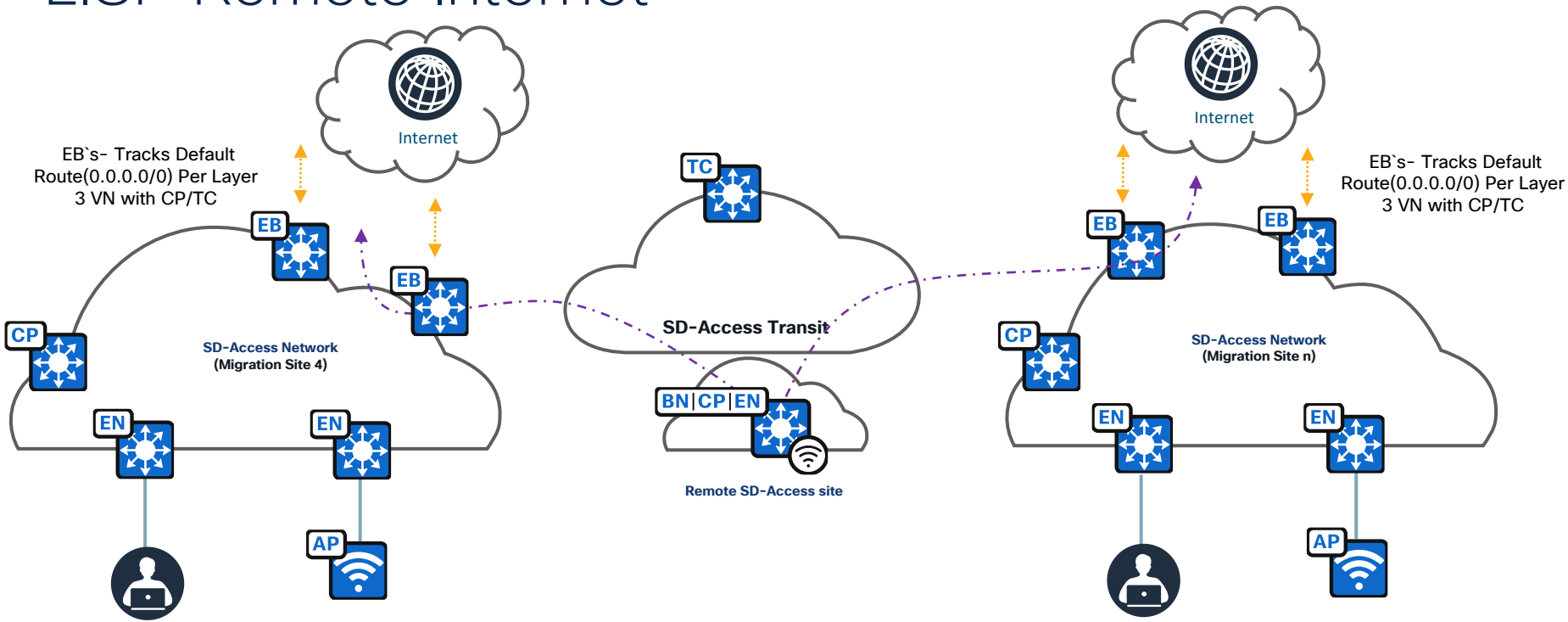
Key Takeaway

- In summary, local Internet is preferred over Backup Internet within the Fabric Site.
- If local Internet is down for the site, then explore other options provided by other fabric sites (Backup Internet).
- Select this box on Border nodes if we want to share internet access.



LISP Remote Internet

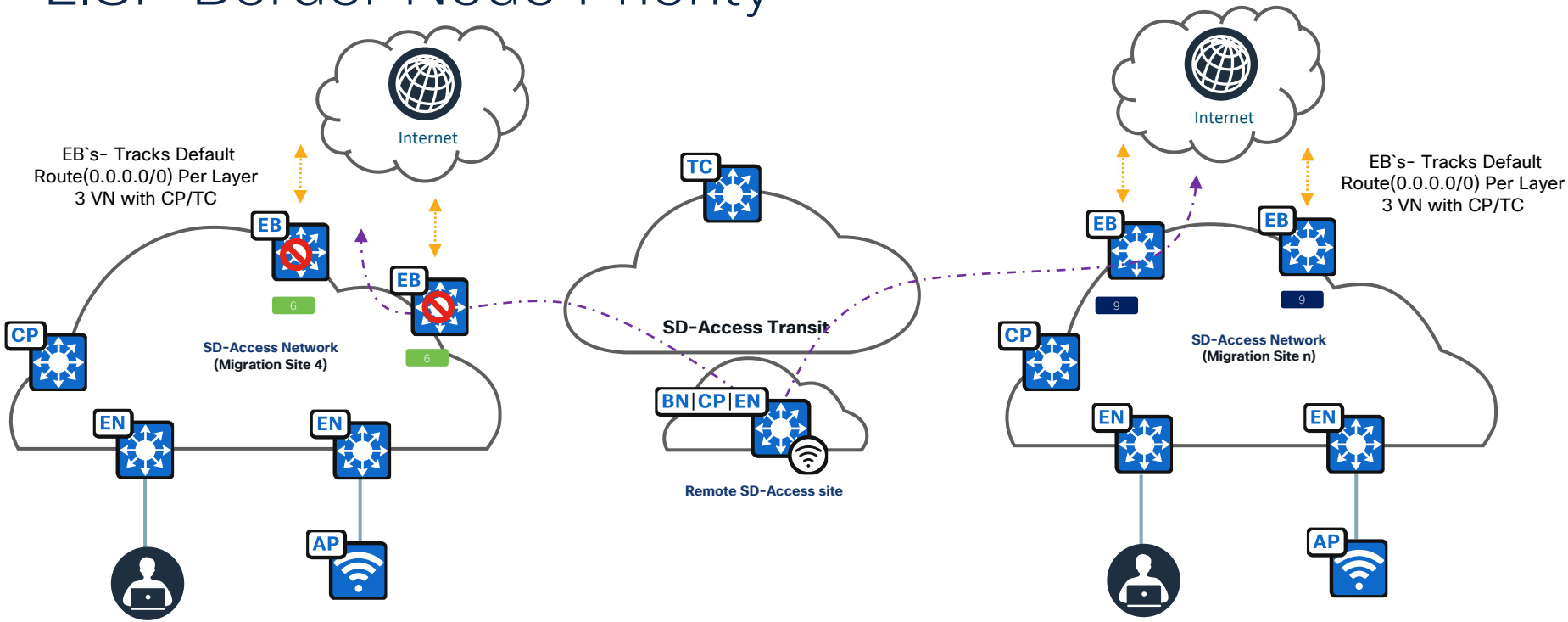
LISP Remote Internet



Remote SD-Access Site uses Internet from either site 4 or site n by default if Internet in those sites is shared

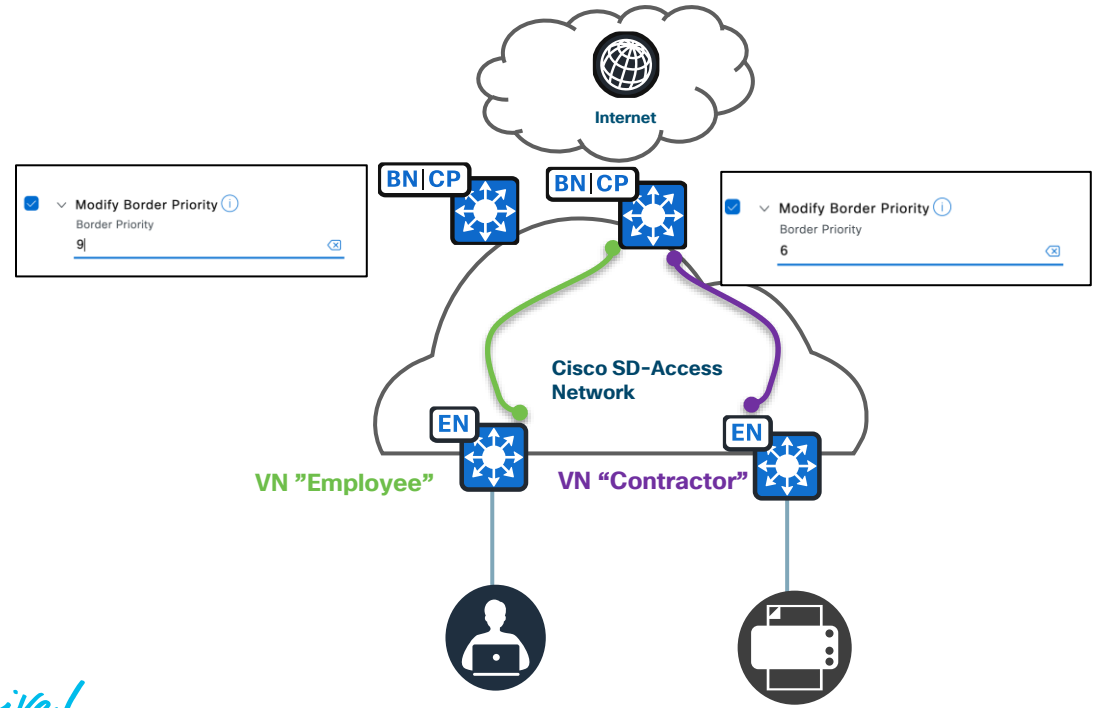
LISP Border Node Priority

LISP Border Node Priority



- Remote SD-Access Site always prefers Migration Site 4 as LISP priority is lower.
- Remote SD-Access Site traffic goes via Migration site n only if Site 4 has no internet(default route available)

Border Node Priority UI Automation



Border Node Priority

Details

- Supported from Cisco DNA Center 2.3.3.x.
- Cisco DNA Center provides users the capability to select a border node to egress the fabric network traffic.
- Users can set the priority values between 1 and 9 (1 is the highest priority and 9 is the lowest. Lower number is the preferred Border).
- By default (if user do not set a priority value), the border is assigned a priority value of 10. If border priorities are not set (or same across Borders), traffic is load balanced across the border nodes.
- User can modify border node priority in Day N without removing devices from fabric.
- The priority value set for a border is applicable to all the virtual networks that are handed-off from that border.
- If an SD-Access Transit interconnects the fabric sites, an external border with the Lowest priority is chosen to send traffic to external networks.
- Supported with both LISP Pub/Sub and LISP BGP fabrics.

Cisco SD-Access

For More Information

- Deep Dive on LISP Architecture: LISP Architecture Evolution – New Capabilities Enabling SD-Access – BRKENS-2828
- Design best Practices: Cisco SD-Access Best Practices – Design and Deployment – BRKENS-2502
- Cisco SD-Access Transits: Cisco SD-Access – Connecting Multiple Sites in a Single Fabric Domain – BRKENS-2815

Transit Control Plane Node
Design Considerations

1. Device must be dedicated to the transit control plane node role.
   - Example: It cannot also be a fabric border node.
2. Ideally, device should not be in the data forwarding (transit path) between sites.
   - Treat this like a BGP route reflector.
3. Deploy a pair of Transit Control Plane Nodes.
   - Always deploy in pairs for fabric domain resiliency

SD-Access Transit
Design Considerations

1. Jumbo Frame Support
   - Must accommodate frame size large enough for 50-byte VXLAN header

2. Commonly Direct or Leased Fiber over a Metro Ethernet (MAN) system
   - Metro-E, DWDM, Owned or Leased Private Circuits, Dark Fiber
   - Designed for MAN, not for WAN unless MTU is sufficient

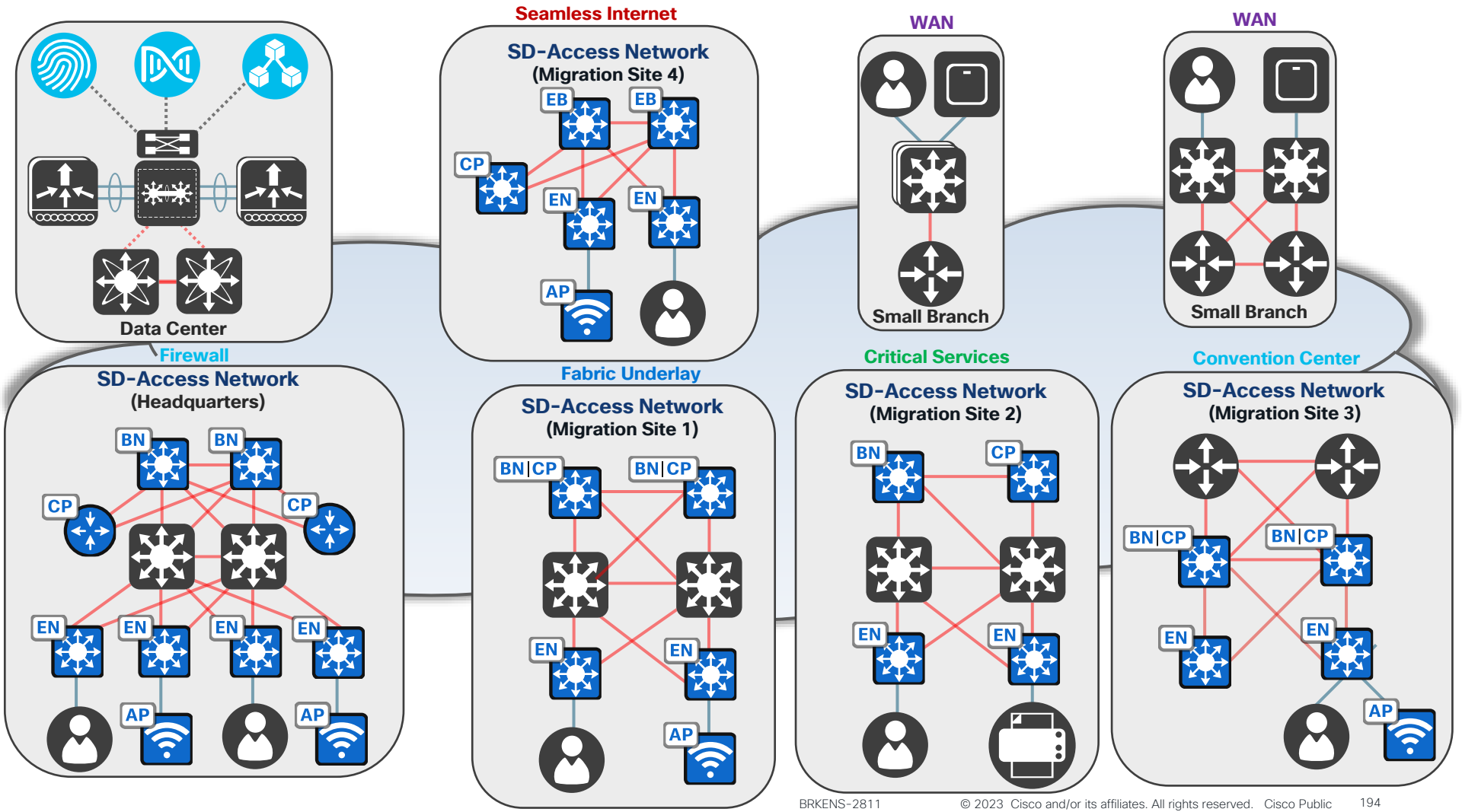
3. IP Reachability
   - Commonly an IGP across the circuit.
   - A full mesh of reachability between Loopback 0 between all Border Nodes connected to an SD-Access Transit as well as the associated Transit Control Plane Node.

4. Choose the LISP mode of operation
   - LISP Pub/Sub
   - LISP/BGP

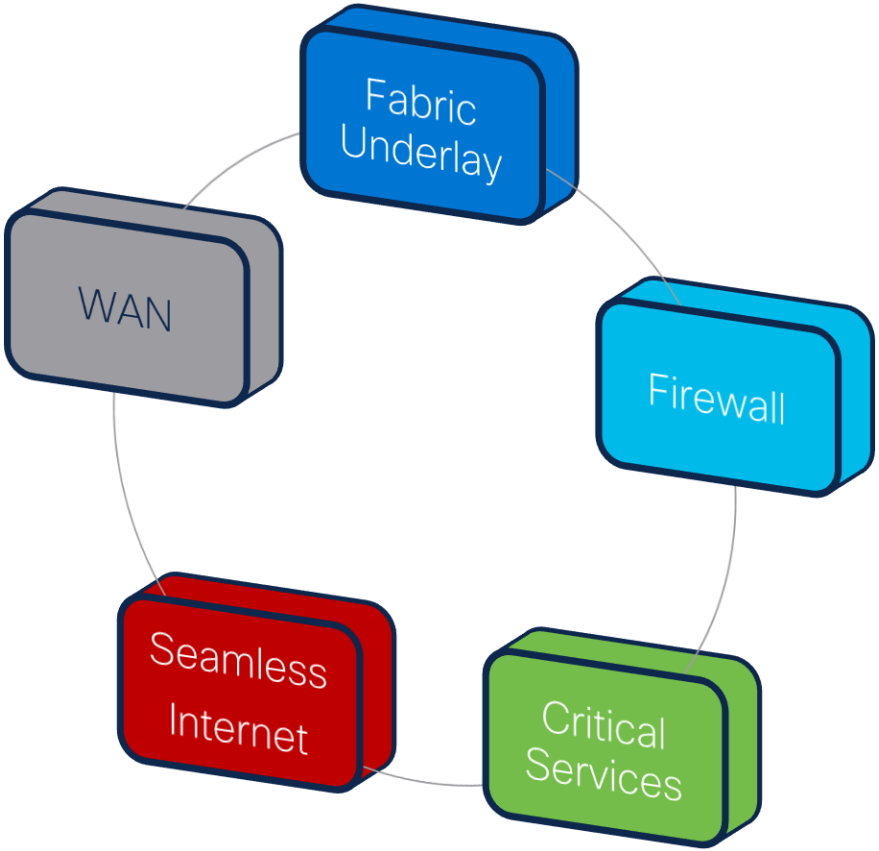
Cisco SD-Access

Seamless Internet Connectivity – Take Away

- Using the SD-Access transit, packets are encapsulated between sites using the fabric VXLAN encapsulation. This natively carries the macro (VRF) and micro (SGT) policy constructs between fabric sites.
- Cisco SD-Access transit built with LISP Pub/Sub has built in functionalities such as :
  - Dynamic Default Border
  - LISP Backup Internet
  - SD-Access Extranet
  - LISP Remote Internet (supported with LISP BGP as well)
  - Border Priority (supported with LISP BGP as well)
- All the above functionalities are automated via Cisco DNA Center



Progress Chart



Consistent Policy Across Geographic Locations

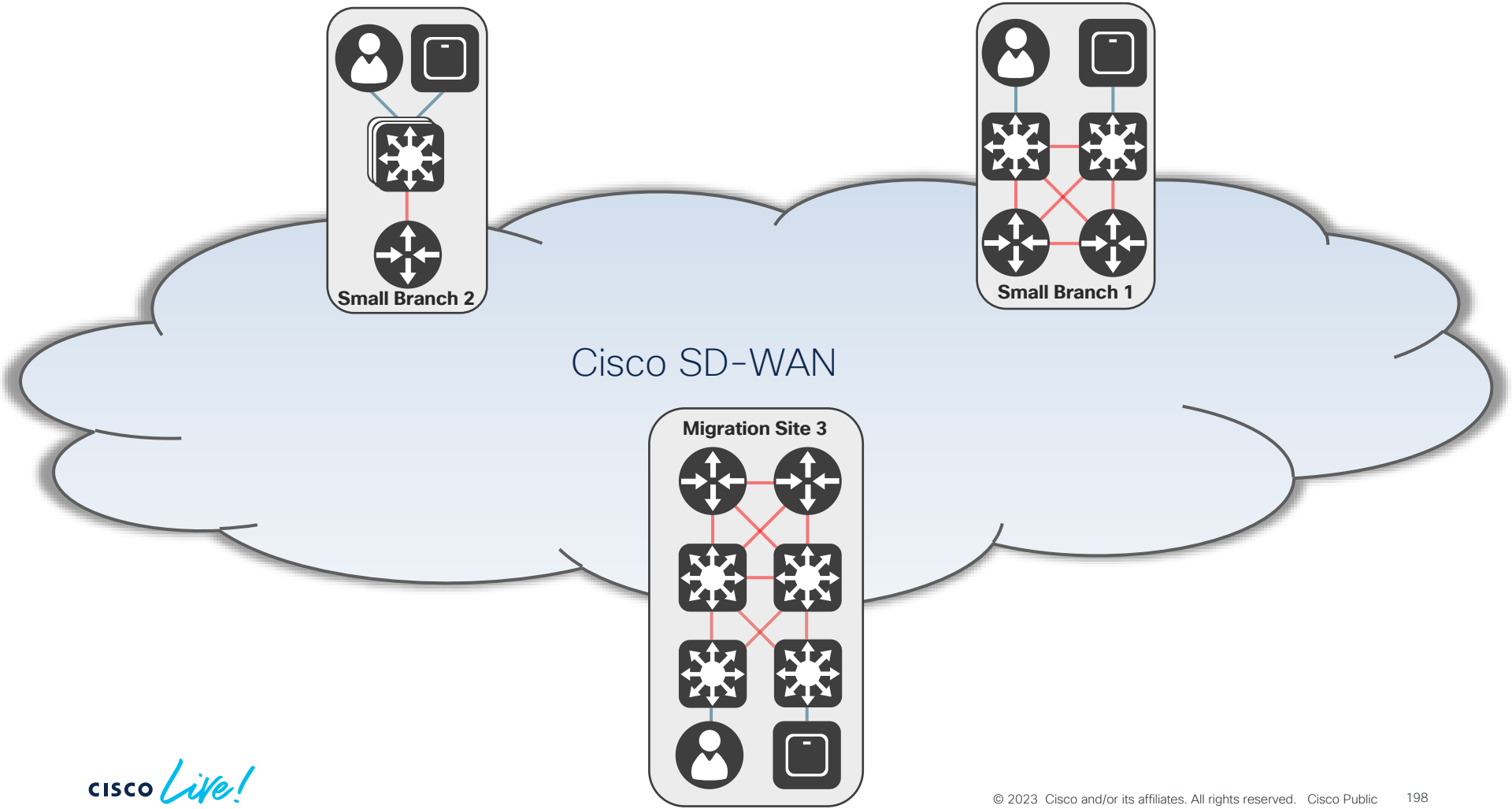
Cisco SD-Access | Cisco SD-WAN

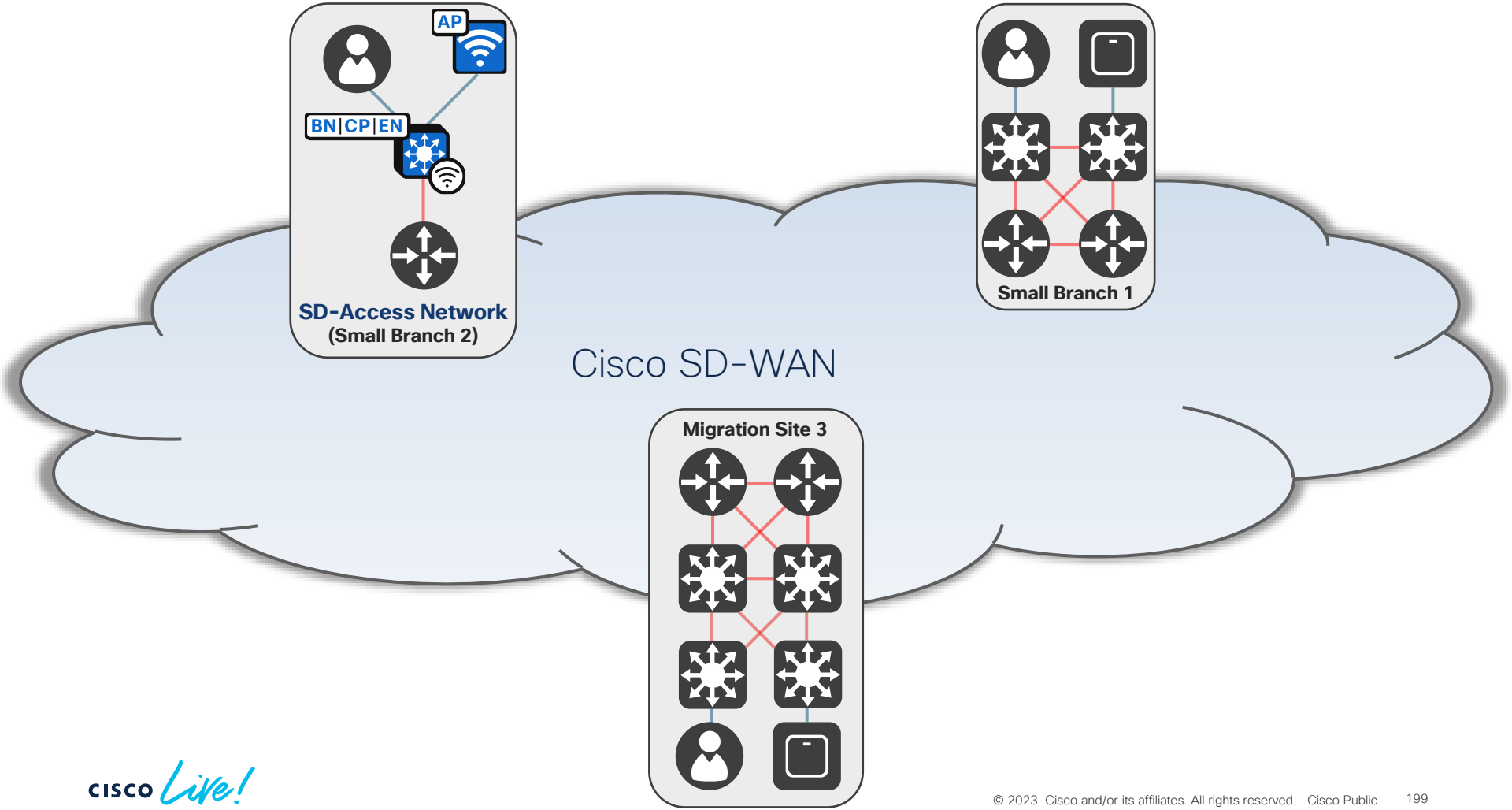
Independent Domains

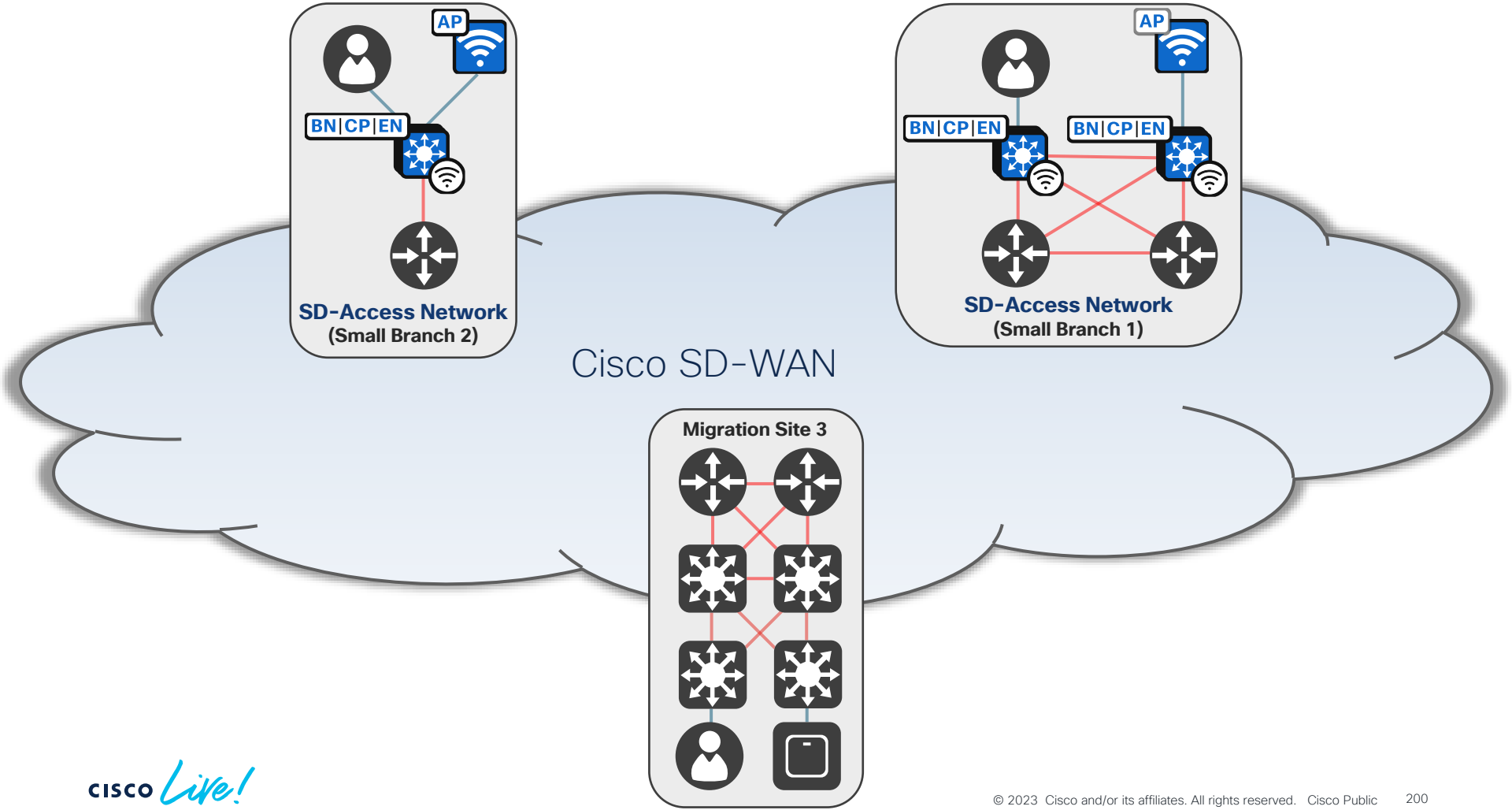
SD-Access	Handoff	SD-WAN
• Control Plane: LISP	• Control Plane: BGP	• Control Plane: OMP
• Data Plane: VXLAN	• Data Plane: VRF-lite	• Data Plane: IPSec | MPLS
• Policy Plane: SGT	• Policy Plane: Inline Tagging	• Policy Plane: CMD in IPSec

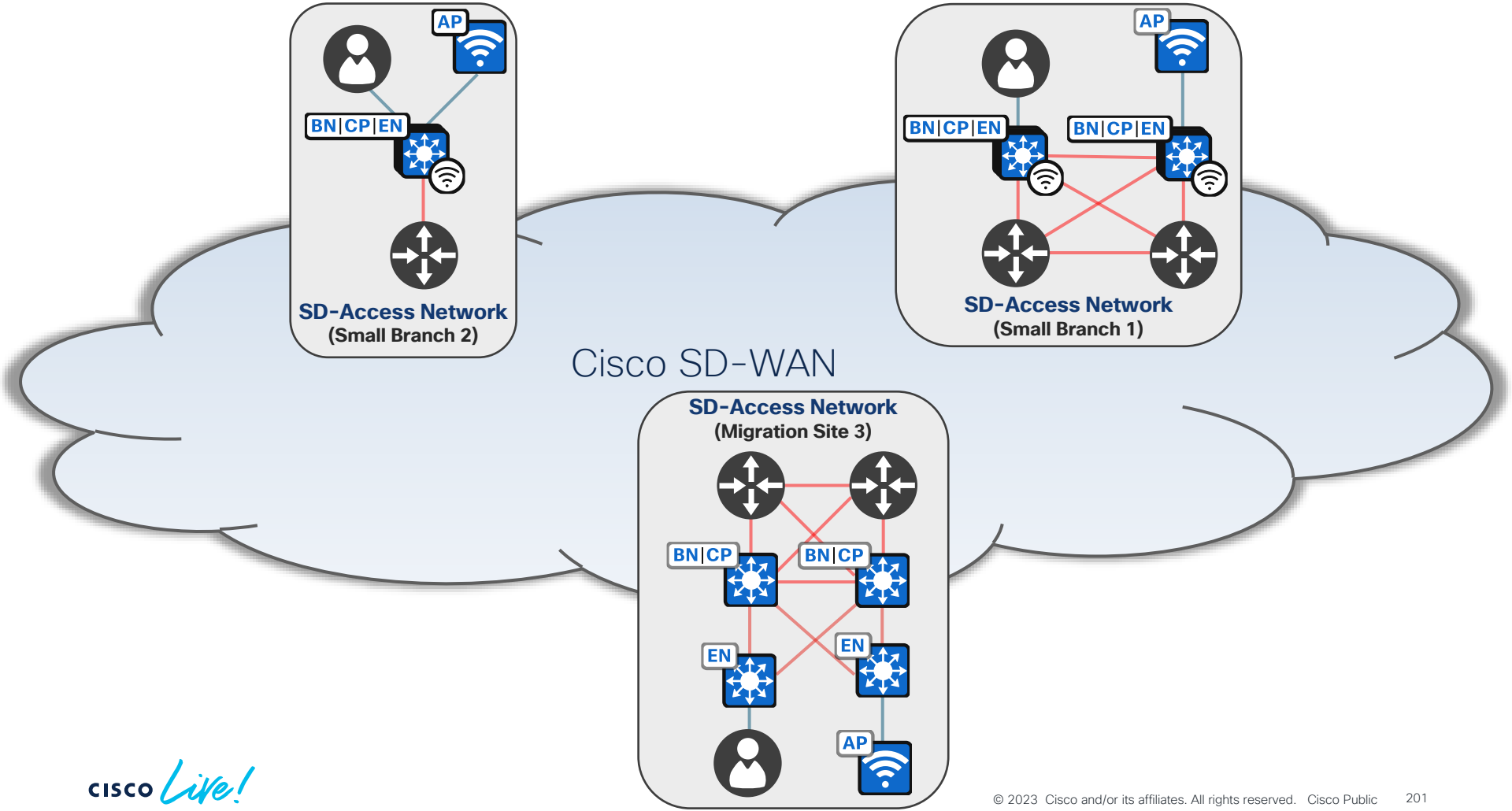
Management Plane
Cisco DNA Center

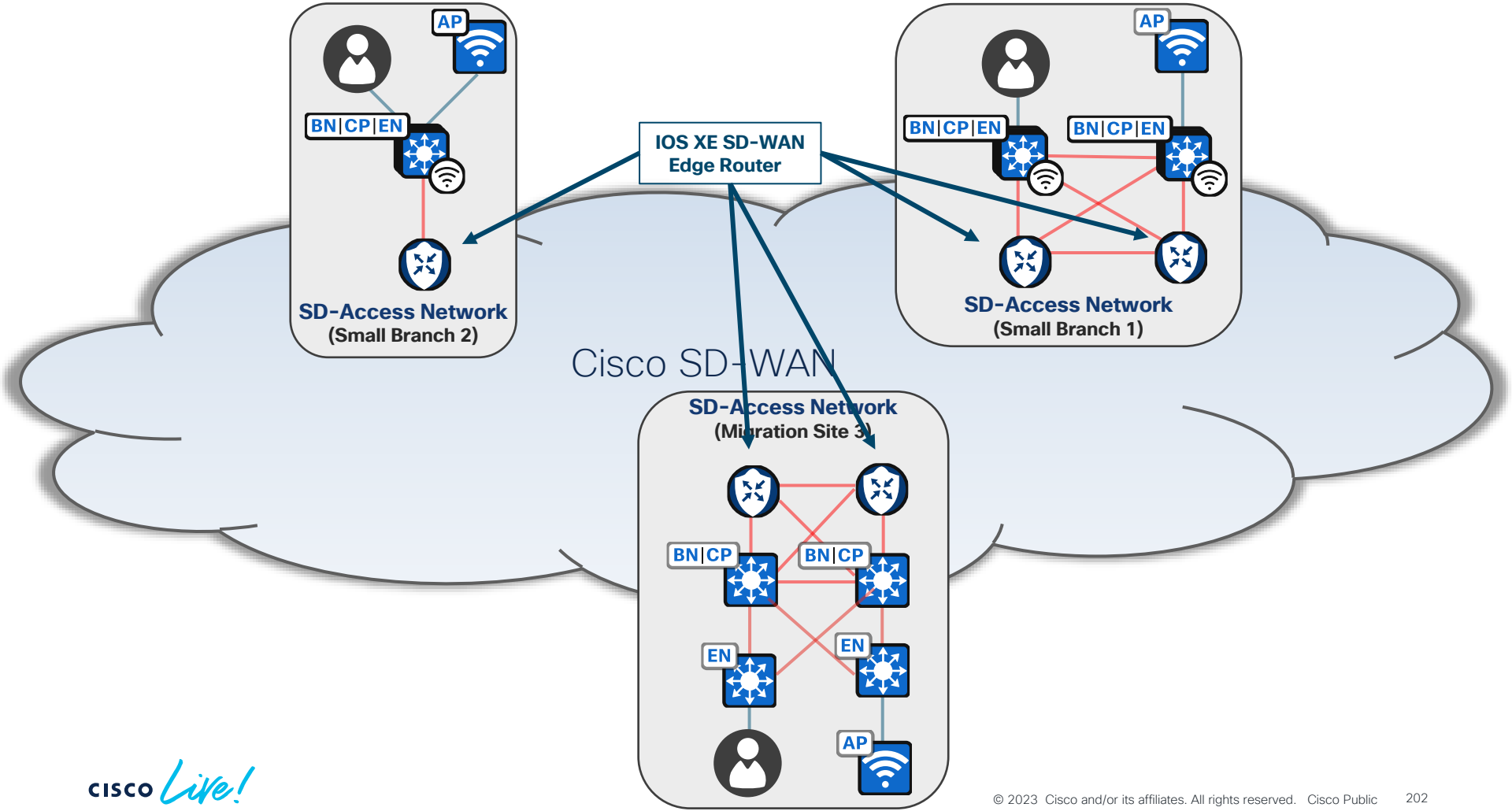
Management Plane
Cisco vManage

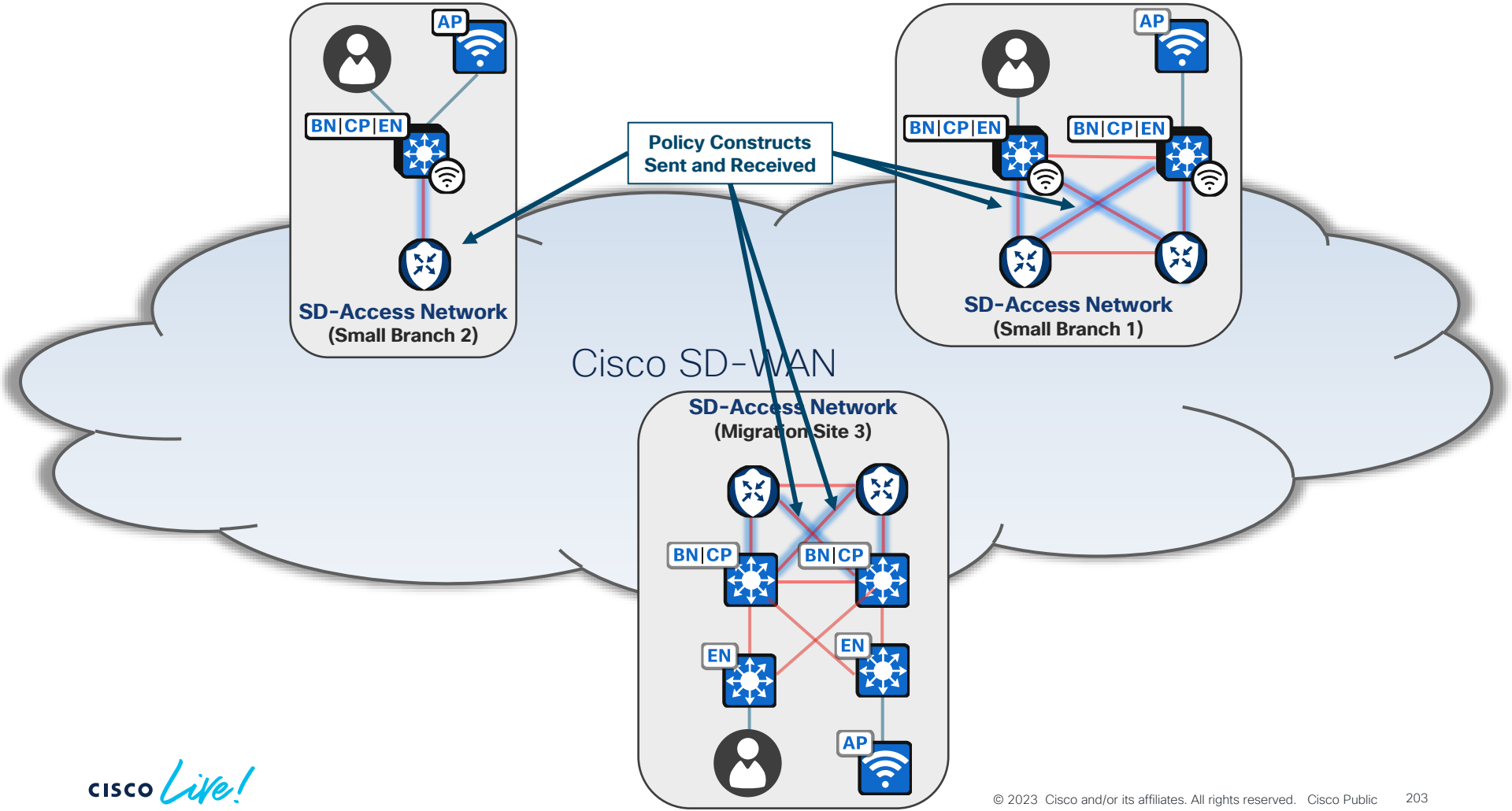


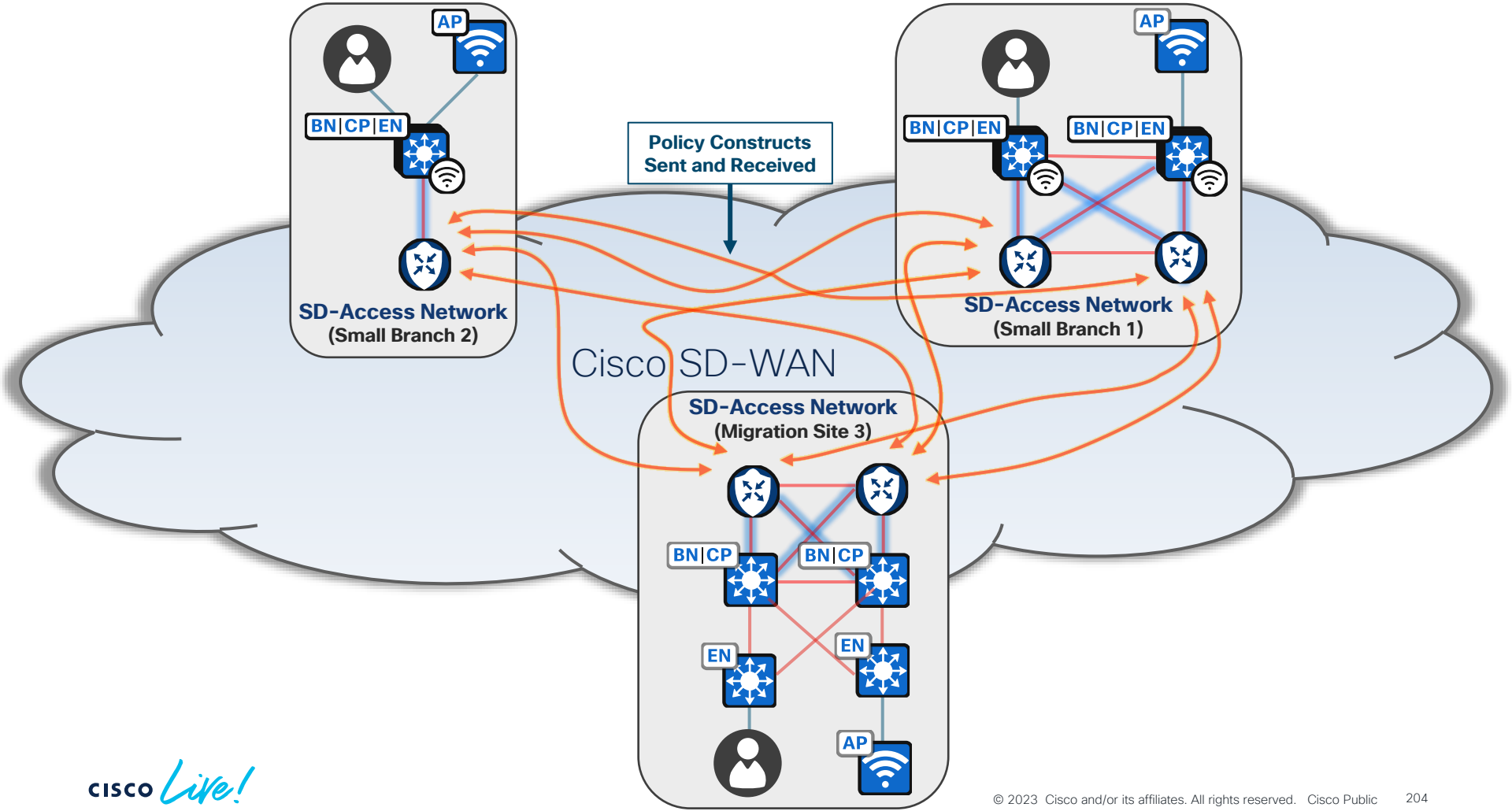






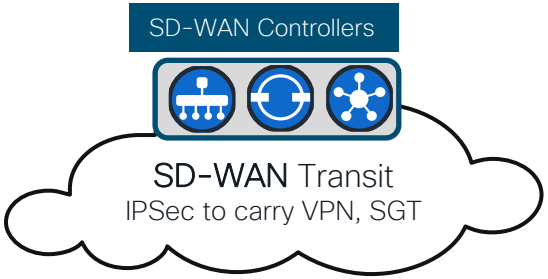






Cisco SD-Access Deployment

Multisite Deployment with SD-WAN Transit



Cisco SD-WAN Transit provides capability to carry VN and SGT across WAN Transport.

Key Considerations:

- Fabric Site network requirements
- Border, WAN Edge platform capabilities.

- Cisco SD-WAN solution, powered by Cisco IOS-XE software provides highly secure and reliable WAN overlay topologies.
- IOS-XE WAN Edge devices provides flexibility to add-on security capabilities as Direct Internet Access (DIA), Application-Aware routing, Firewall, IPS and more..
- Cisco SD-Access provides flexibility to deploy integrated LAN and Wireless with consistent policy at scale.
- Cisco SD-Access and SD-WAN can be deployed with:
  - With **Independent-Domain**: DNA Center are vManage are not integrated.

For Your Reference

Cisco SD-Access Deployment

Cisco SDA|SDWAN Independent Deployment

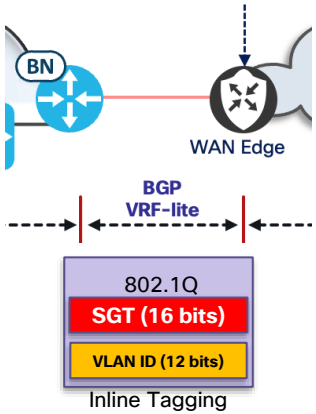
- Cisco SD-WAN WAN Edge and SD-Access Border node are different devices, managed by respective domain controllers.
- Macro-segmentation (VN) is maintained with IP-Handoff between Fabric Border node and WAN Edge device.
- Micro-segmentation (SGT) is shared with Cisco TrustSec Inline tagging. This requires the WAN Edge router and the interface to support TrustSec.

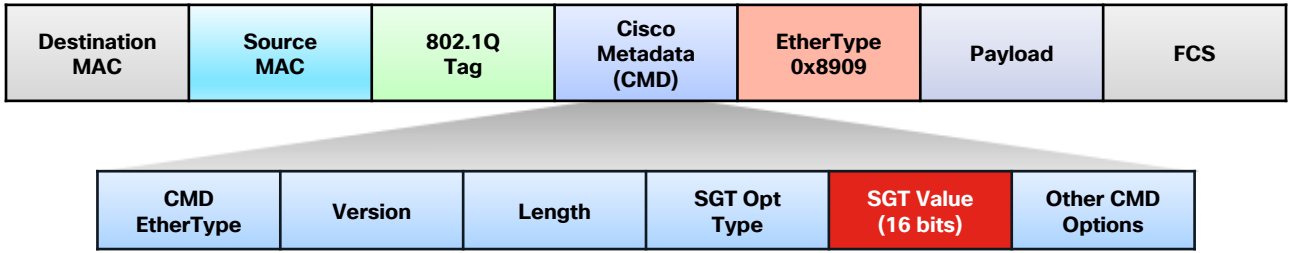
More Details: Cisco Intent Based Cross and Multidomain Integrations for SDA and SD-WAN - BRKXAR-2001

Ethernet Frame with SGT (Inline Tagging)

Independent Domains

For Your Reference



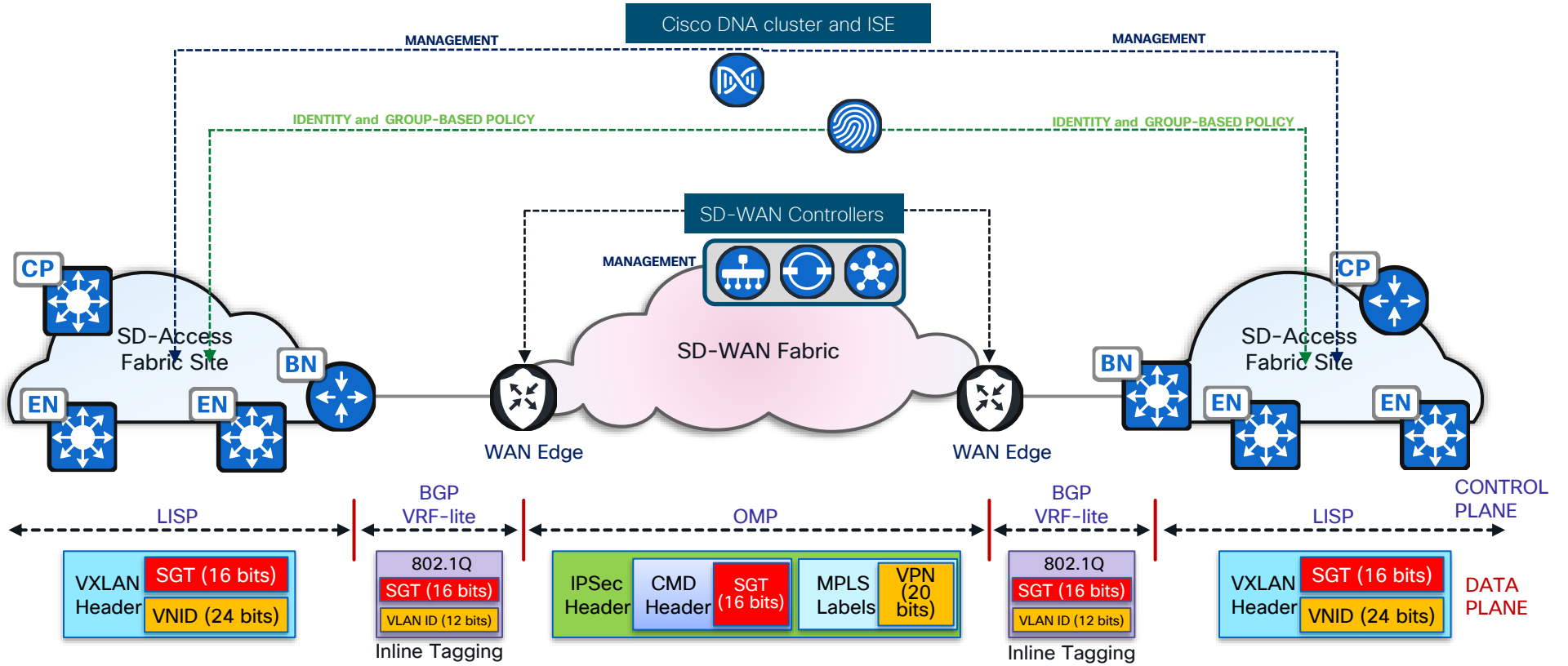


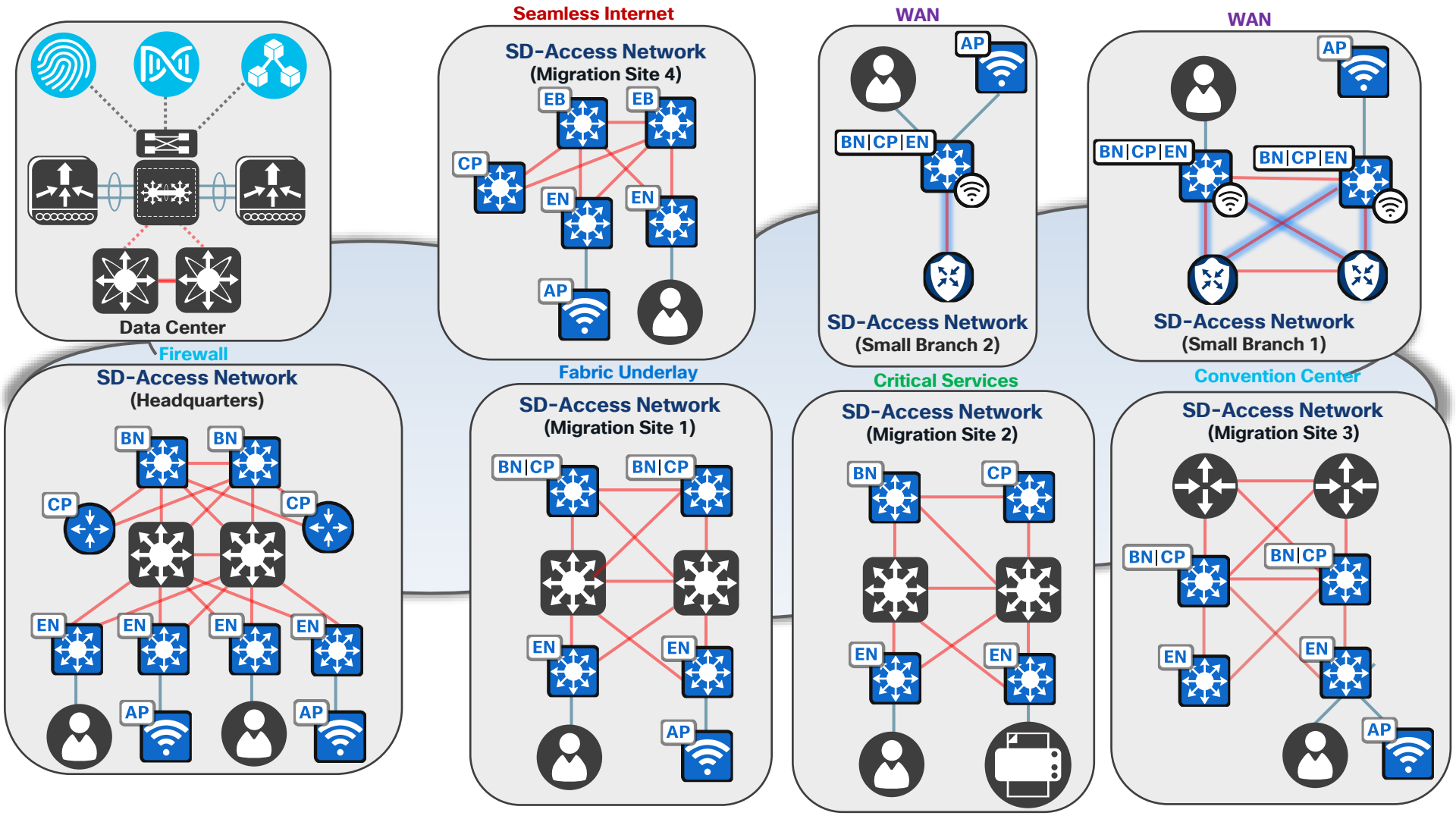
- The SD-Access Border node connects to the IOS XE WAN Edge with 802.1Q trunk.
  - This maps the Fabric VNs (VRFs) into SD-WAN VPNs.
- The SGT is populated in the CMD field of the Ethernet frame by the SD-Access Border Node.
  - It is taken out of the Fabric VXLAN header and put in the frame via inline tagging.
- The IOS XE WAN Edge receives the SGT from this frame and encodes it into the MDATA header.

Note: The LAN interface of the Router needs to support inline SGT Tagging

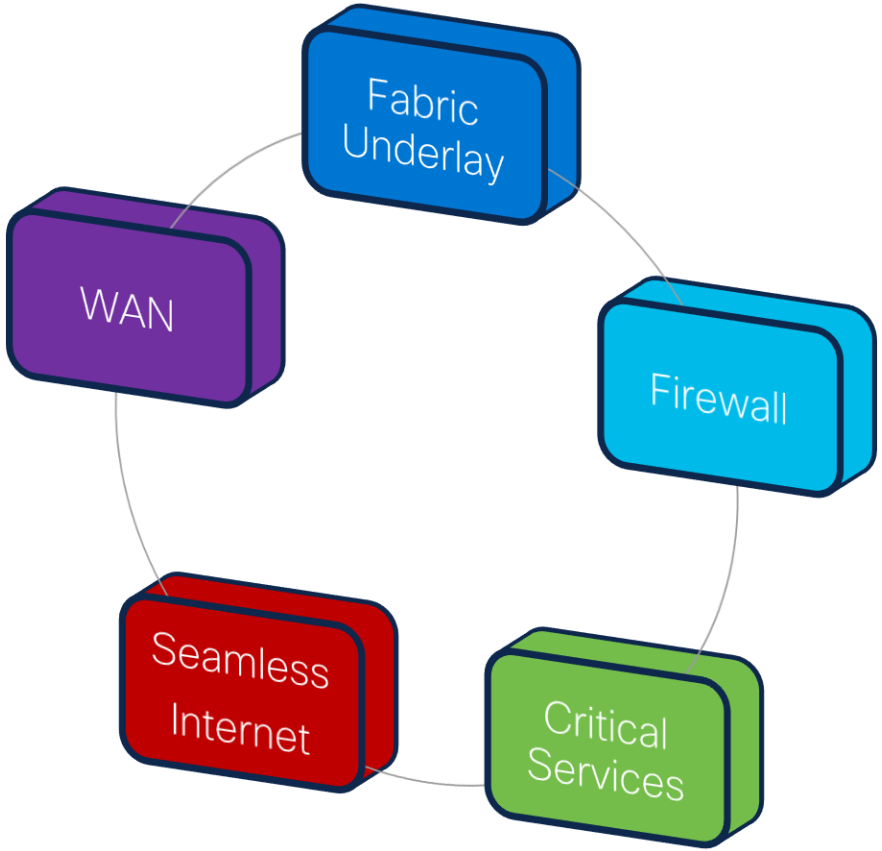
Cisco SD-Access to SD-WAN

Independent Domains




Seamless Internet
WAN
WAN
Data Center
SD-Access Network
(Migration Site 4)
EB
EB
CP
EN
EN
AP
SD-Access Network
(Small Branch 2)
AP
BN|CP|EN
SD-Access Network
(Small Branch 1)
AP
BN|CP|EN
BN|CP|EN
Firewall
SD-Access Network
(Headquarters)
BN
BN
CP
CP
EN
EN
EN
EN
AP
AP
Fabric Underlay
SD-Access Network
(Migration Site 1)
BN|CP
BN|CP
EN
EN
AP
Critical Services
SD-Access Network
(Migration Site 2)
BN
CP
EN
EN
Convention Center
SD-Access Network
(Migration Site 3)
BN|CP
BN|CP
EN
EN
AP

Progress Chart



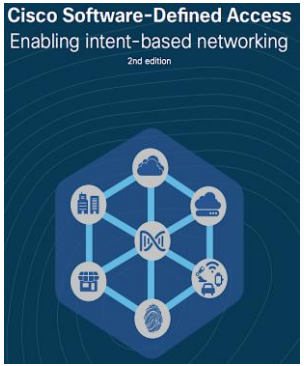
MTS – Meet The Speaker – MTS- 1059

- Session Title - **Meet the Speaker: BRKENS-2811 – MTS-1059**
- 02/09/23 @ 11:40AM
- In the Sessions Lounge
- Continue the post session discussion/Q&A
- On the session catalog

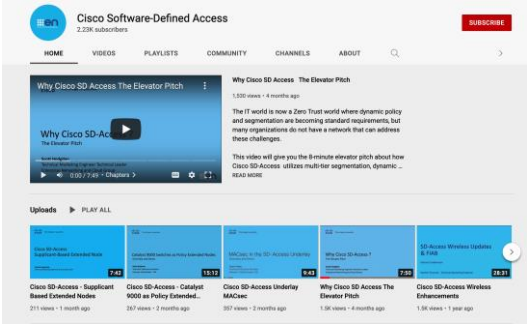
Cisco SD-Access Collaterals

[Cisco Software-Defined Access for Industry Verticals]

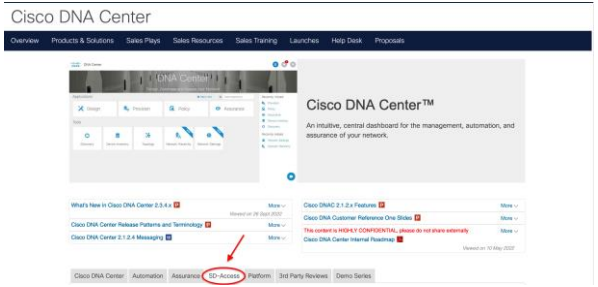
[Cisco Software-Defined Access]
[Enabling intent-based networking]



[Cisco SD-Access YouTube Link]



[Cisco SD-Access SalesConnect Link]



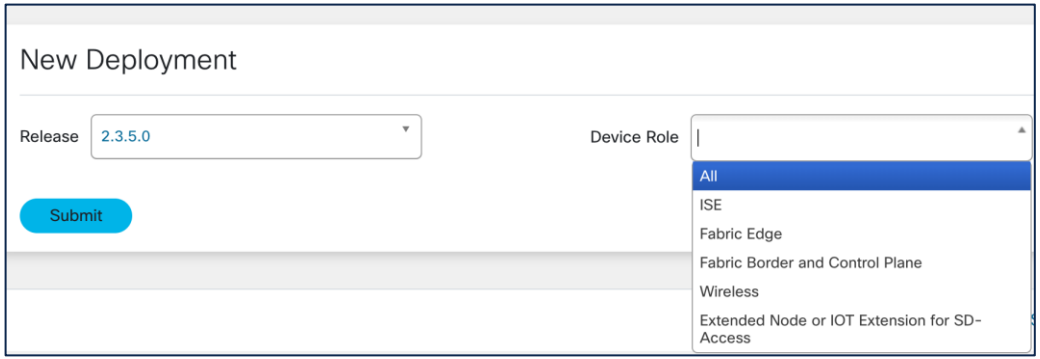
[Cisco SD-Access Design Tool]

[EN&C Validated Designs]

SD-Access Platform Support

Cisco DNA Center Data Sheet

Platform support based on the Fabric Role



For more details: Cisco Software-Defined Access Compatibility Matrix

Supported Hardware and Software Version for all Cisco SD-Access components

cisco Live!

Cisco SD-Access Scale Details

Table 14. Scale and hardware specifications

	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
Hardware description	Cisco UCS C220 M5 Rack Server 44 cores	Cisco UCS C220 M5 Rack Server 56 cores	Cisco UCS C480 M5 Rack Server 112 cores
Cisco DNA Center system scale			
Number of devices[1] (switch, router, wireless controller)	1000	2000	5,000
Number of wireless access points	4000	6000	13,000

For more details: Cisco DNA Center Data Sheet

Summary and What's Next

- Thank you. We can't do this without you! ☺
- Keep sharing the feedback. We are listening.
- Ask the Cisco Sales or CX teams for help.
- Ask questions on the Cisco SD-Access communities: http://cs.co/sda-community
- Go Cisco SD-Access!

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very 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 www.CiscoLive.com/on-demand


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN