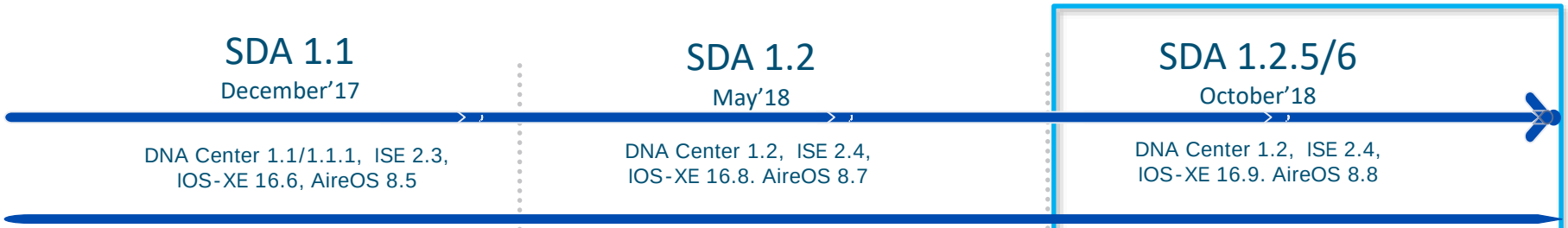
SD-Access 1.2.5/6 TDM Deck

Satish Kondalam
Version 1.0
Technical marketing Engineer
09/19/2018

Introduction

SD-Access Roadmap

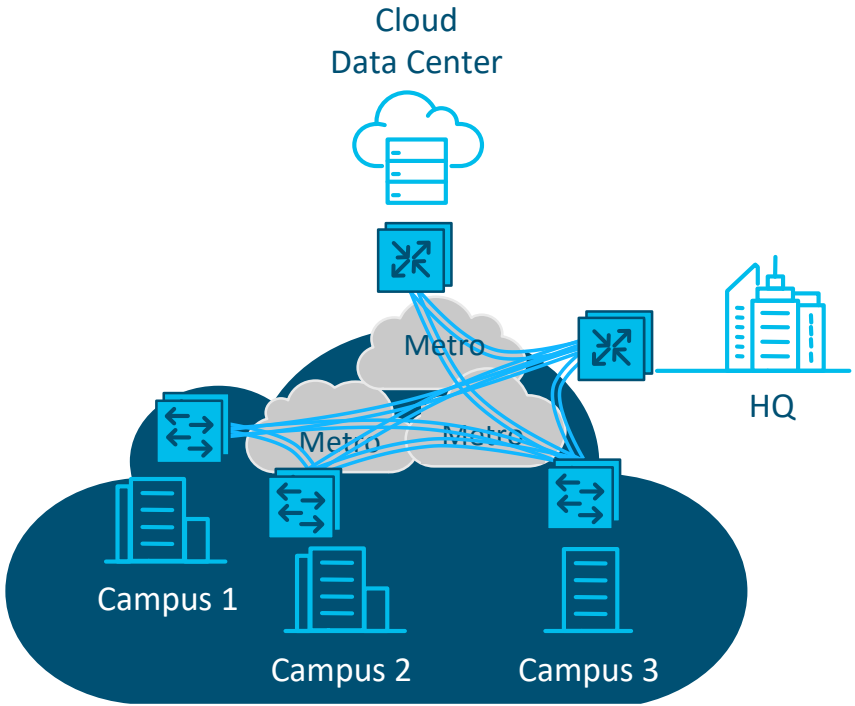


- **Identity-based Policy & Segmentation**
- **Automated Network Fabric**
- **Fabric-Enabled Wireless**
- **Wireless Assurance** (DNAC 1.1.1)
- **Network Health Monitoring**

- **SD-Access for Distributed Campus** (Beta)
- **SD-Access Extension for IoT** (Beta)
- **IBNS 2.0**
- **Usability Enhancements**
- **Fabric Enabled Wireless Enhancements**

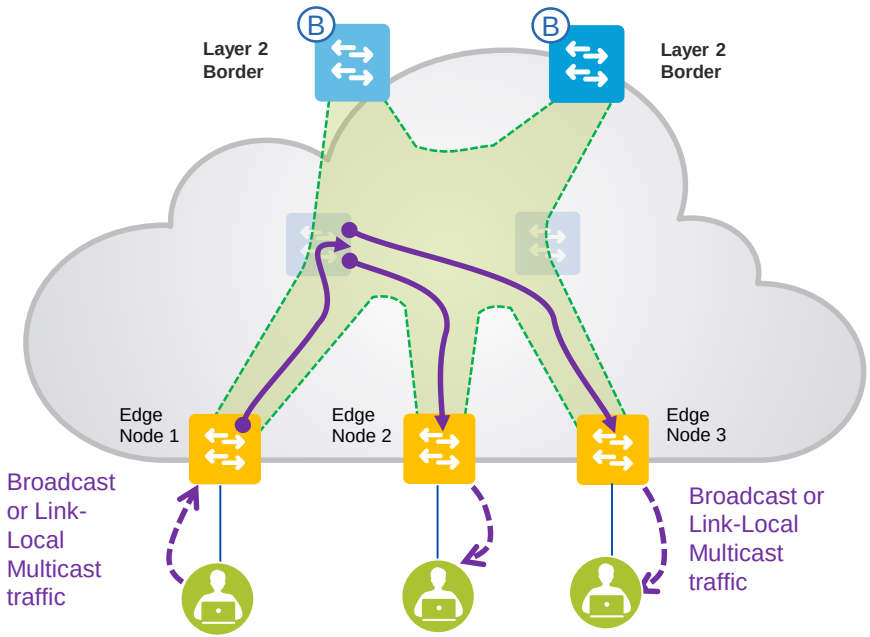
- **SD-Access for Distributed Campus** (FCS)
- **Layer 2 Flooding**
- **Layer 2 Hand off for Migration purposes**
- **Native Multicast**
- **Fabric in a Box**
- **LAN Automation & Host On-boarding Enhancements**
- **Fabric Control Plane Resiliency (six control plane nodes)**
- **DNAC CLI Templates**

SD-Access for Distributed Campus



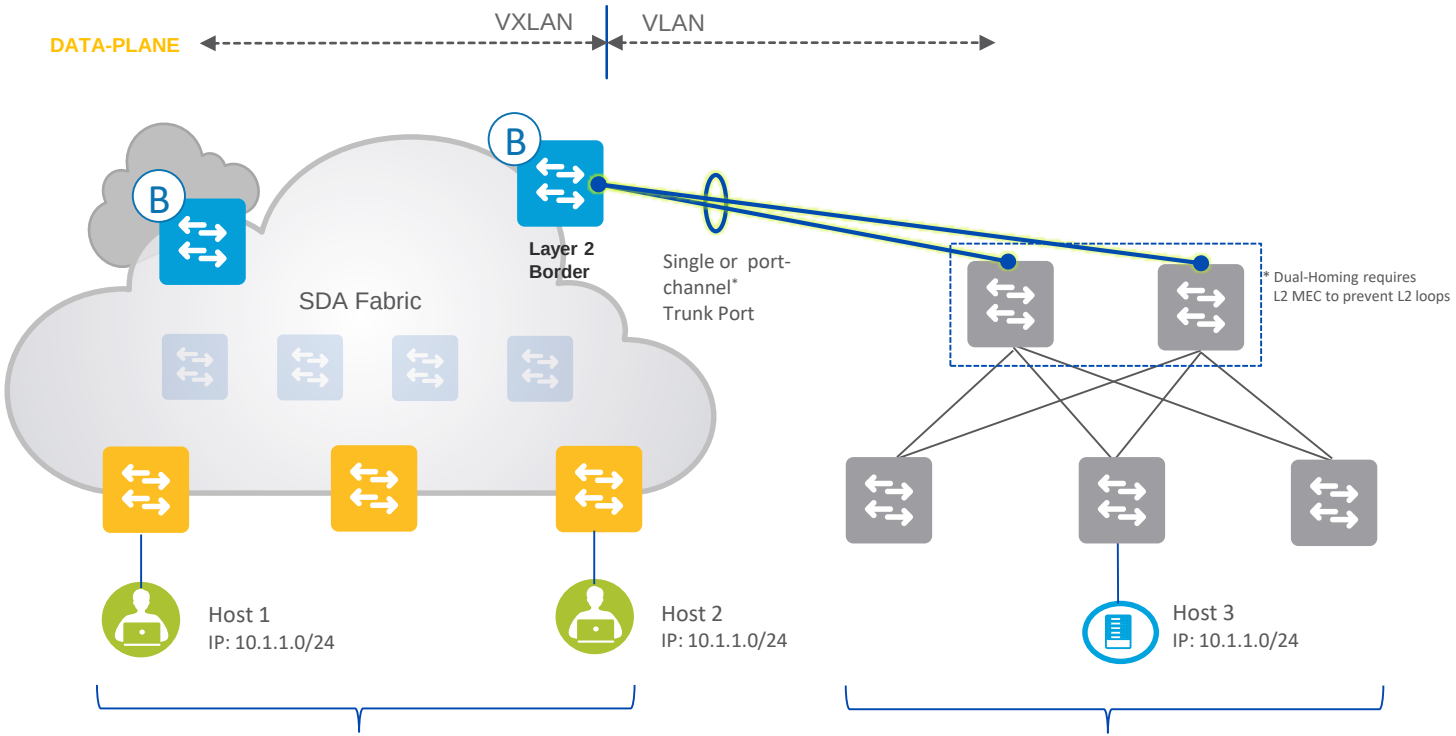
- End-to-end segmentation
- Centralized Automation & Assurance
- Future Proof for SD-WAN
  (Viptela SD-WAN Integration on Roadmap)

Layer 2 Flooding in SD-Access



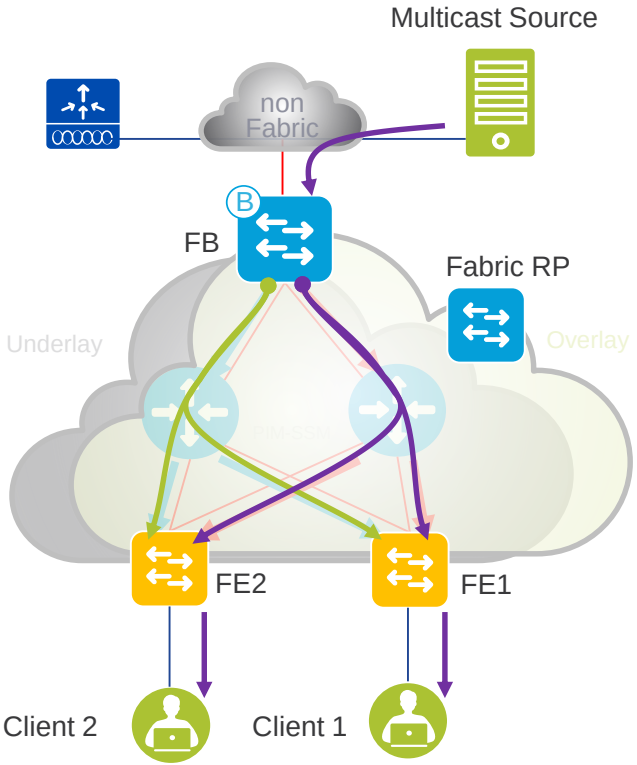
- Allows Layer 2 flooding within an IP Subnet/vlan
- Silent Host Support
- Broadcast , Link Local Multicast and ARP flooding support

Layer 2 Hand off for Migration in SD-Access



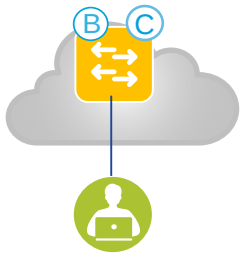
Native Multicast in SD-Access

* DNAC 1.2.6



- Significantly reduces replication load at the Head-End
- Significantly improves overall scale and reduces latency

Fabric in a Box in SD-Access



FABRIC IN A BOX

- FE+FB+CP on C9K
- Reduces the cost to deploy SDA for “mini” sites

SD-Access 1.2 Software Compatibility

DNA Center	DNAC 1.2.5/6
ISE	ISE 2.4 Patch 2
Catalyst 3K/9K	IOS-XE 16.9.1s
Catalyst 4500	IOS 3.10.1 es
Catalyst 6800	15.5(1)SY2
Nexus 7700	8.2(2) SMU's, CSCvg39911, CSCvh87828, CSCvg09282, CSCvh32898
ASR1K/ISR4K/CSR	IOS-XE 16.9.1s
Wireless LAN	AireOS 8.8

* **Minimum SW version needed for new features in SDA 1.2**

SD-Access 1.2.X Backward Compatibility

DNA Center	DNAC 1.2.x	
ISE	ISE 2.3 Patch 4	ISE 2.3 Patch 2
Catalyst 3K/9K	IOS-XE 16.8.1s	IOS-XE 16.6.4
Catalyst 4500	IOS 3.10.1es	
Catalyst 6800	15.5(1)SY1	
Nexus 7700	8.2(1) SMU	
ASR1K/ISR4K/CSR	IOS-XE 16.8.1s	IOS-XE 16.6.4
Wireless LAN	AireOS 8.7	AireOS 8.5 MR3

* **DNAC's releases will support backward compatibility In terms of device code versions**

SD-Access 1.2 Scale

SD-Access1.2 Scale

Fabric Constructs	Maximum Supported on Single DNAC Cluster
No of Fabric Domains per DNA Cluster	10
No of Fabric Sites across the Fabric Domains*	200
Total Endpoints (including APs) per DNA Cluster* APs (Counted as Endpoints) per DNA Cluster *	25K 4000
Number of Virtual Networks	64
Fabric Nodes (Edge, Border, WLC) per DNA cluster *	500**
Non-Fabric Nodes(Intermediate, Subtended, Routers) per DNA Cluster *	1000
Control Plane Nodes Per Fabric Site	2
Default Border Nodes Per Fabric Site	4

- Above scale is split across all the configurable fabric domains (10) or can be in one fabric domain

** A Stack of switches is considered as one Fabric Node

Single DNAC cluster = 3 DNAC appliances (2+1 in HA)

SD-Access 1.2 Scale

Fabric Constructs	Maximum Supported on Single DNAC Cluster
IP Pools *	500
Groups (SGTs) per DNA Cluster *	4K
Number of Access Control Policies per DNA Cluster *	1K
Number of Traffic Copy Policies per DNA Cluster *	10
Number of Contracts per DNA Cluster *	500

- Above scale is split across all the configurable fabric domains (10) or can be in one fabric domain

** A Stack of switches is considered as one Fabric Node

Single DNAC cluster = 3 DNAC appliances (2+1 in HA)

*** These are 1D Platform numbers**

SD-Access 1.2 – Edge Scale

Fabric Constructs	Catalyst 3650	Catalyst 3850	Catalyst 9300	Catalyst 4K (Sup8E)	Catalyst 9400	Catalyst 9500
Virtual Networks	64	64	256	64	256	256
Local End Points/Hosts	2K	4K	4K	4K	4K	4K
SGT/DGT Table	4K	4K	8K	2K	8K	8K
SGACLs (Security ACEs)	1350	1350	5K	1350	18K	18K

*** These are 1D Platform numbers**

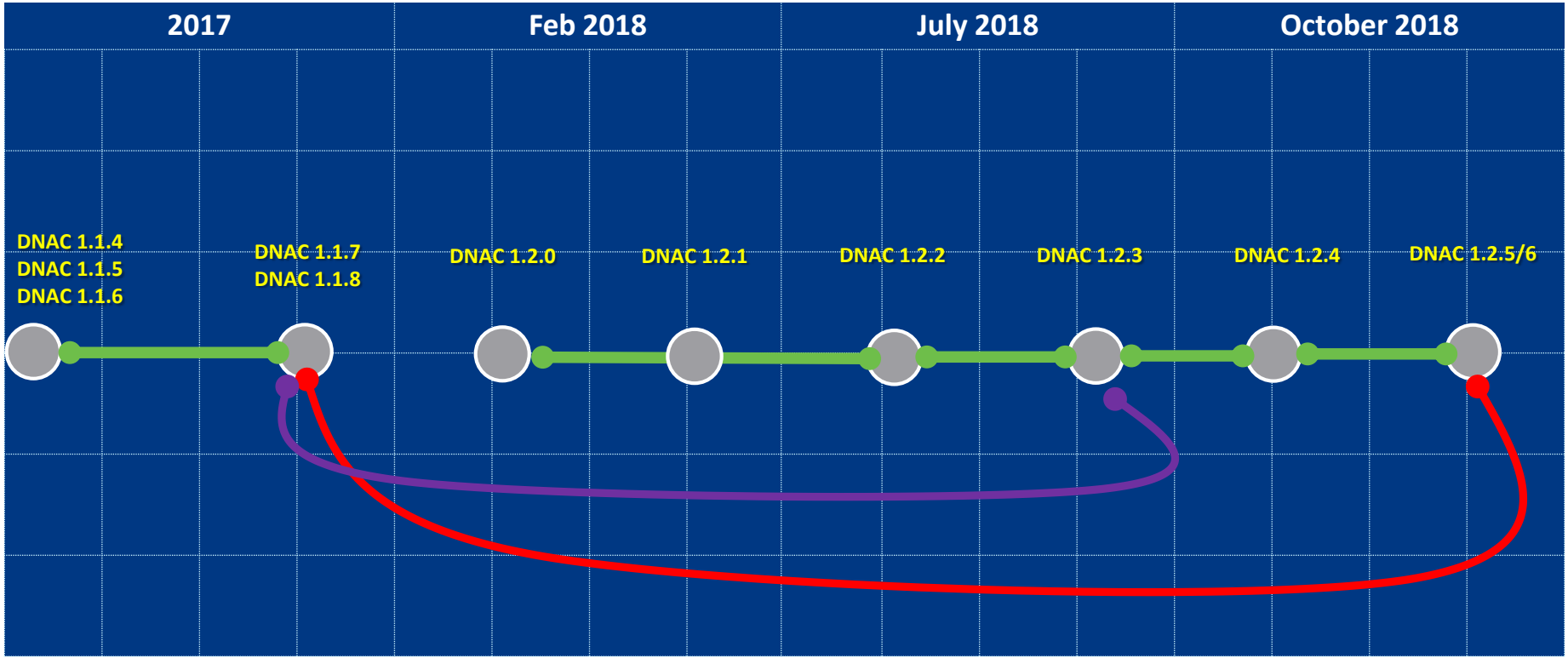
SD-Access – Border Scale

Scale	Catalyst 3850(XS)	Catalyst 9300	Catalyst 9400 (*SUP1 XL)	Catalyst 9500	Catalyst 9500H	Catalyst 6800	Nexus N7700	ASR1K/ ISR4K	CSR1Kv
Virtual Networks	64	256	256	256	256	500	500	4K	n.a.
SGT/DGT Table	4K	8K	8K	8K	8K	30K	16K	62K	n.a.
SGACLs (Security ACEs)	1500	5K	18K	18K	18K	30K(XL) 12K(non XL)	16K	64K	n.a.
Fabric Control Plane Entries with Border Co-Located on Same Device	3K	16K	80K	80K	80K	25K	Not Supported	200K/100K (16GB) 100K/50K (8GB)	200K
IPv4 Fabric Routes	8K	4K	20K	48K	48K	1M (XL)/ 256K	500K	4M (16GB) 1M (8GB)	n.a.
IPv4 Fabric Host Entries	16K	16K	80K	96K	96K		32K		

* SUP1 XL is only supported as Border node

SD-Access 1.1x to 1.2.5 Migration

SD-Access 1.2 Migration Matrix



SD-Access 1.2.5/6 Features

SDA 1.2.5/6 Features

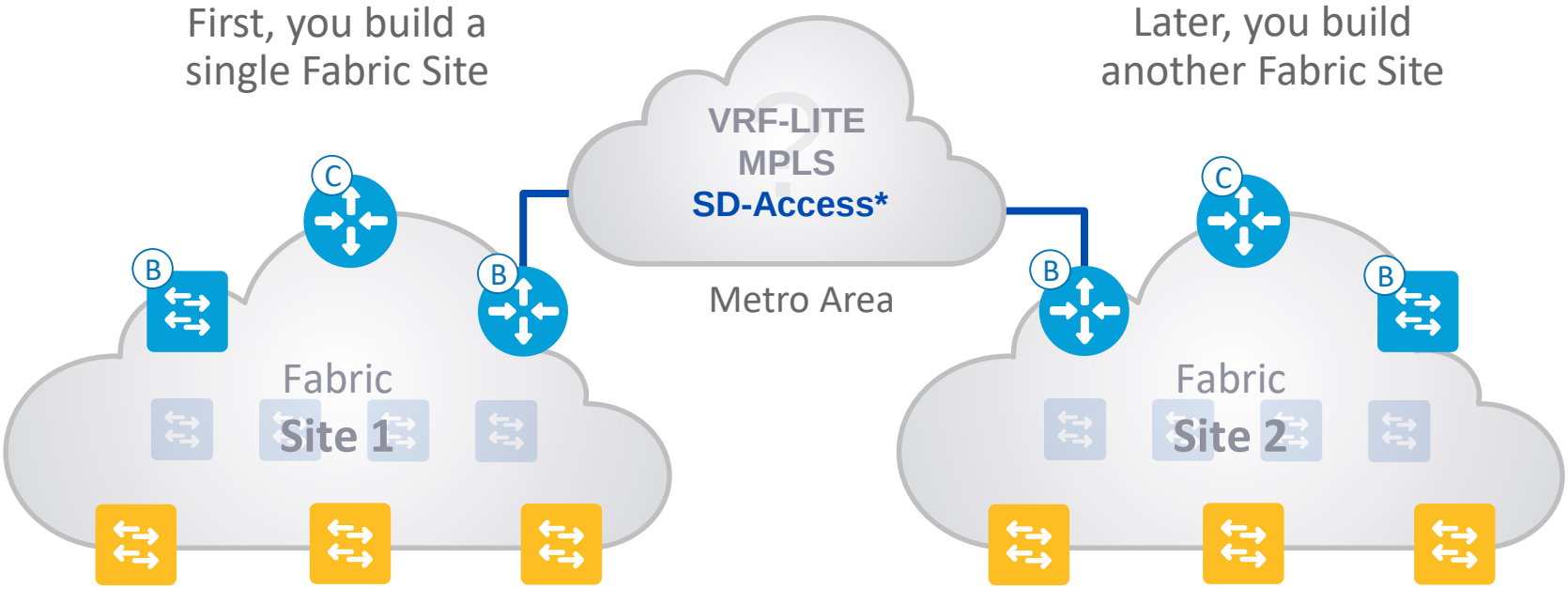
Below are the new features that are being introduced with DNAC/SD-Access 1.2.5/6

- SD-Access for Distributed Campus
- Layer 2 Flooding
- Fabric in a Box
- Native Multicast
- LAN Automation Enhancements
- Host On-Boarding Enhancements
- Fabric Control Plane Resiliency
- DNAC CLI Templates

SD-Access for Distributed Campus

Fabric Sites & Domains

Connecting Multiple Fabrics



How do you connect them together?

SD-Access Distributed campus

Fabric Border Support Matrix

SDA Border Node	SD-Access Distributed campus (SD-Access Transit)	SD-Access Distributed Campus (IP Transit)
C9K	YES	YES
ASR1K/ISR4K	YES	YES
C6K	No	YES
N7K	NO	YES

SD-Access for Distributed Campus

Fabric Sites and Domains

* RECAP

A **Fabric Site** is an independent fabric area of a with a unique set of network devices: Control Plane, Border, Edge, WLC, ISE PSN

Different levels of redundancy and scale can be designed per Site by including local resources: DHCP, AAA, DNS, Internet, etc.

A Fabric Site may cover a single **physical location**, **multiple locations**, or just a **subset of a location**

- Single Location ➔ Branch, Campus or Metro Campus
- Multiple Locations ➔ Metro Campus + Multiple Branches
- Subset of a Location ➔ Building or Area within a Campus

SD-Access for Distributed Campus

Fabric Sites and Domains

* RECAP

A **Fabric Domain** may consist of one or more Fabric Sites + Transit

Multiple Fabric Sites are connected to each other using a **Transit Site**

There are two types of Transit:

- **SD-Access Transit** - Enables a native SD-Access (LISP,VXLAN,CTS) fabric, with a domain-wide Control Plane node for inter-site communication

- **IP-Based Transit** - Leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites

SD-Access for Distributed Campus

Transit site types

* RECAP

❖ SD-Access Transit :

- Inter-site traffic uses VXLAN-GPO encapsulation, driven by a LISP-based control-plane lookup.
- Border nodes will do a LISP lookup with the domain Control Plane node (in the Transit site).
- Border nodes perform a VXLAN encapsulation to deliver the traffic directly to remote sites.
- End to End policy-plane is maintained using SGT group tags.
- No performance-based routing is available in the Transit site.
- End to end automation by DNAC

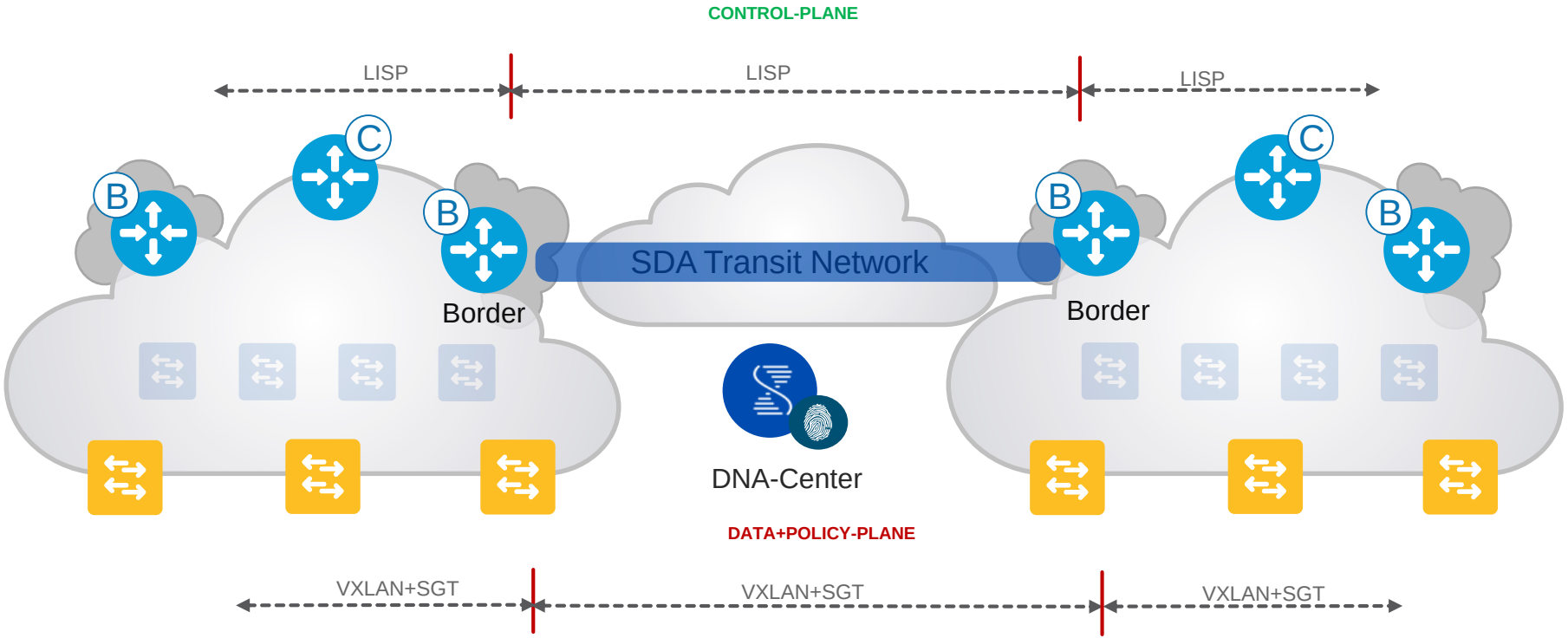
❖ IP-Based Transit :

- Traffic between sites will use the existing control and data-plane of the IP Transit site
- Border nodes hand off the traffic to the directly connected External domain (VRF-LITE with BGP).
- Traffic is delivered via traditional (IP-based) method across the External domain to remote sites.
- End to End policy can only be maintained by Manual configuration.
- If SD-WAN is deployed in IP Transit, then performance-based routing, encryption, etc. is possible.

SD-Access for Distributed Campus

SD-Access Transit

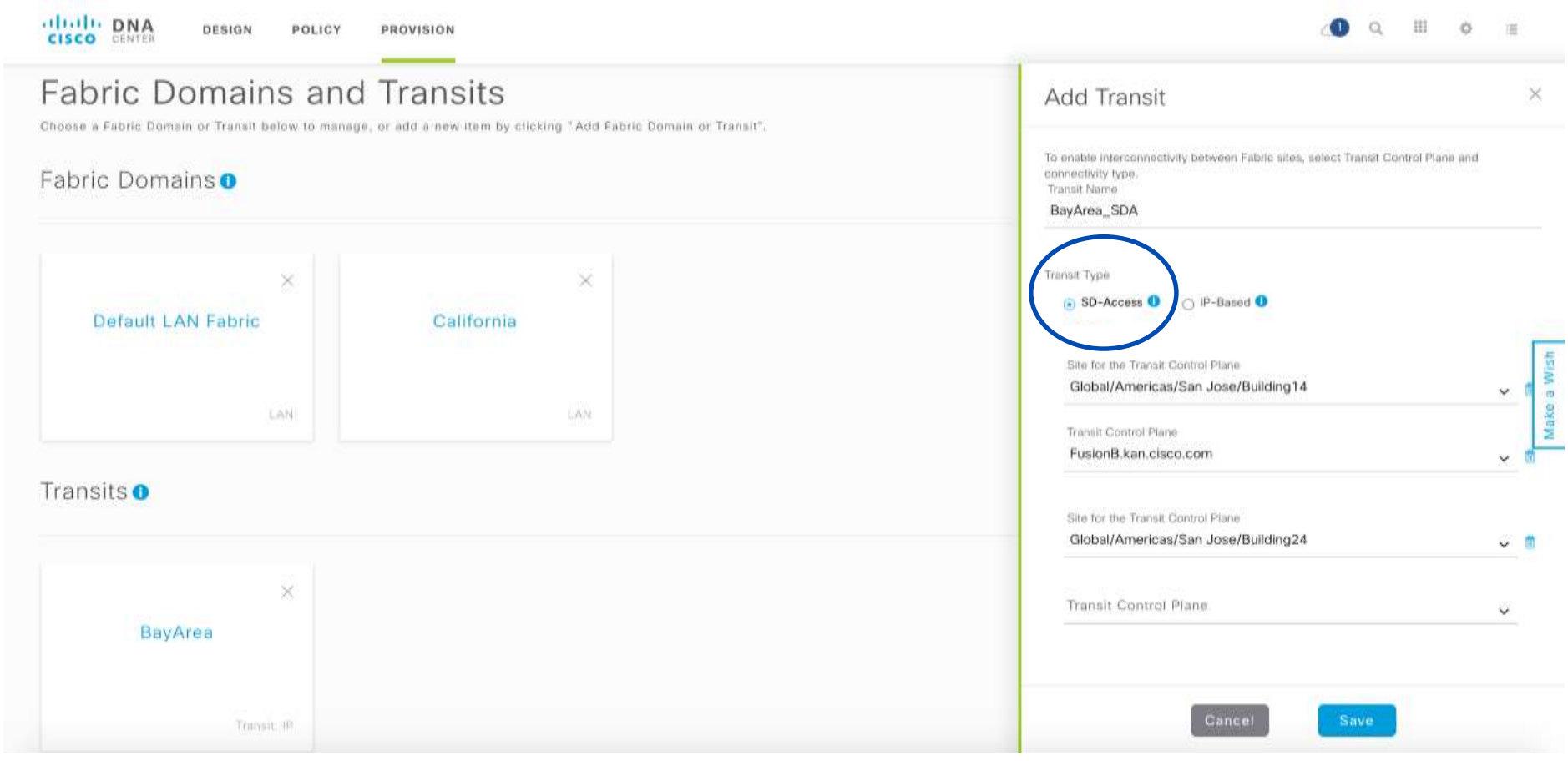
* RECAP



SD-Access for Distributed Campus

SD-Access Transit

* RECAP

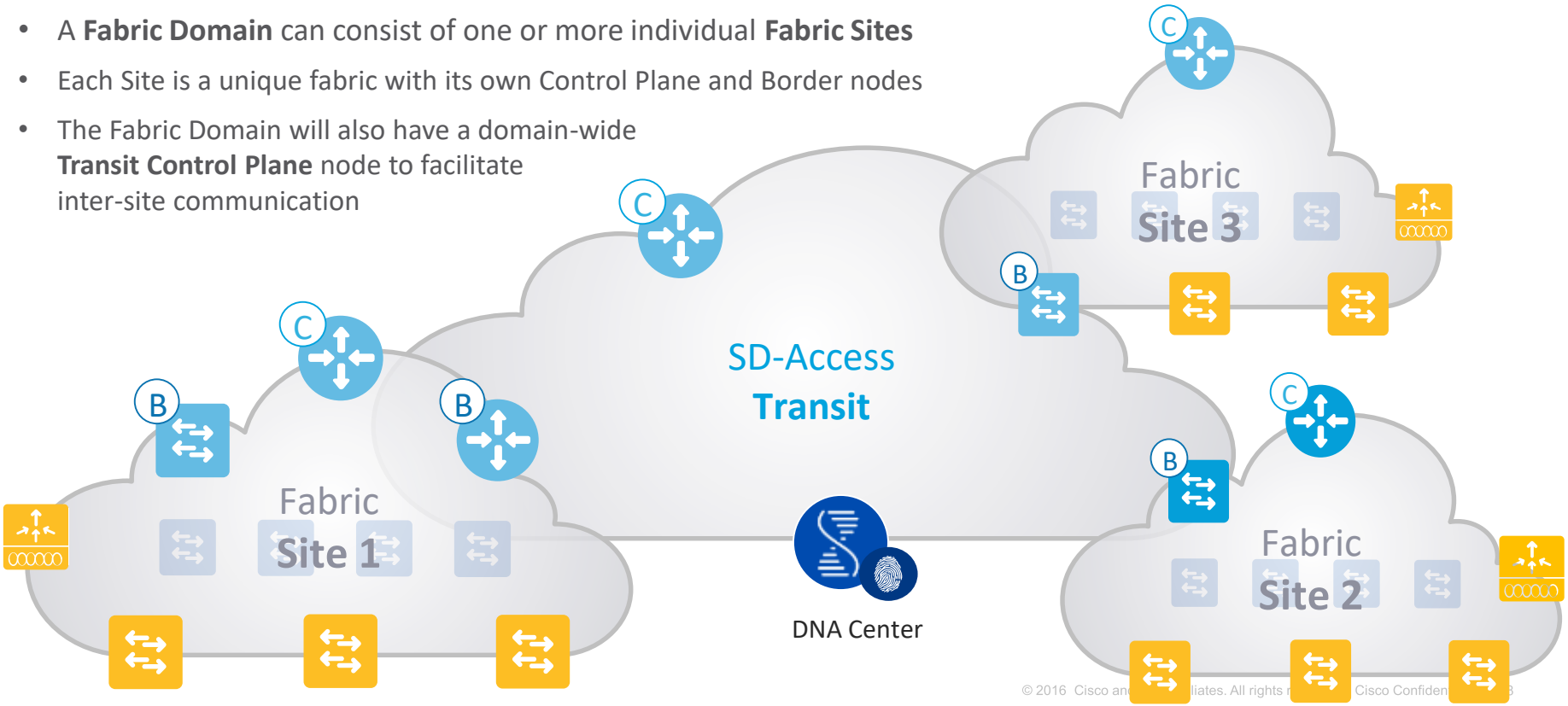


SD-Access for Distributed Campus

SD-Access Transit

* RECAP

- A **Fabric Domain** can consist of one or more individual **Fabric Sites**
- Each Site is a unique fabric with its own Control Plane and Border nodes
- The Fabric Domain will also have a domain-wide **Transit Control Plane** node to facilitate inter-site communication

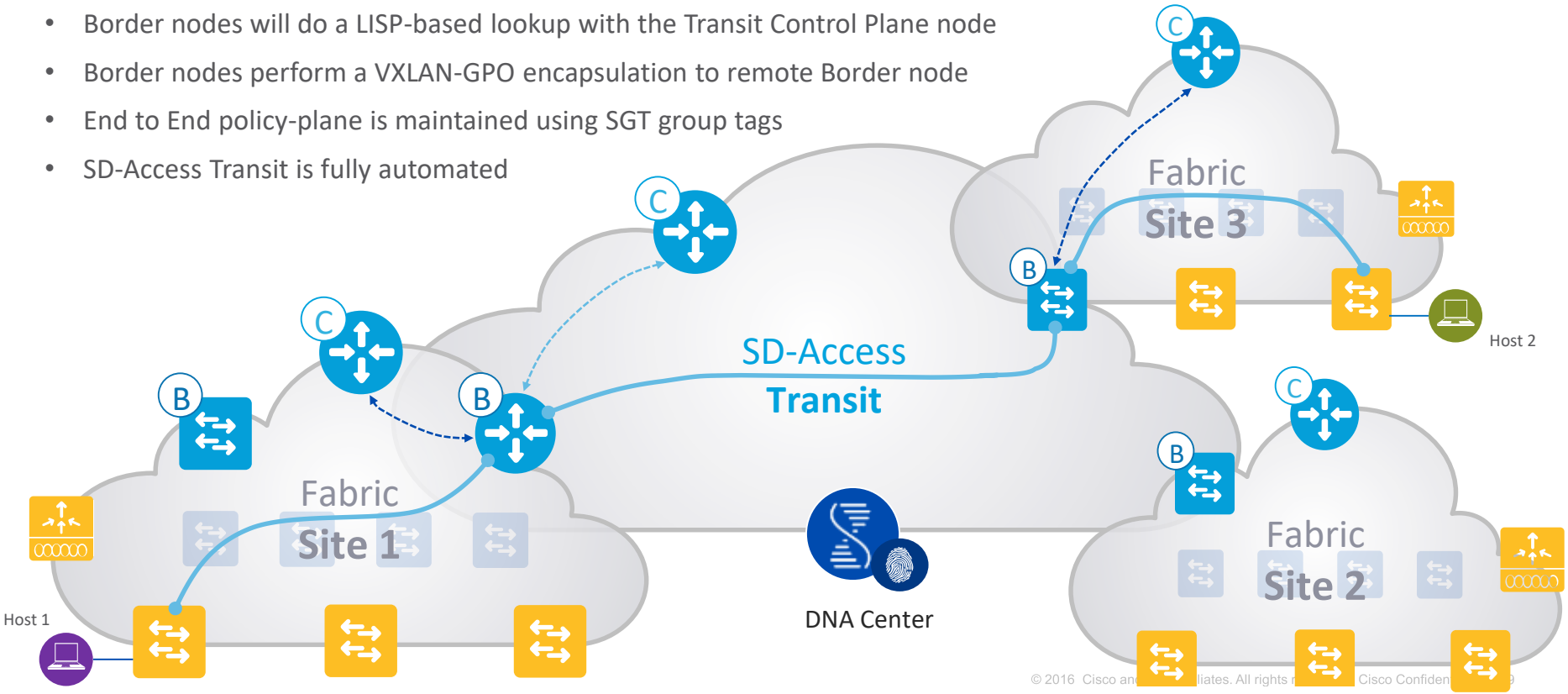


SD-Access for Distributed Campus

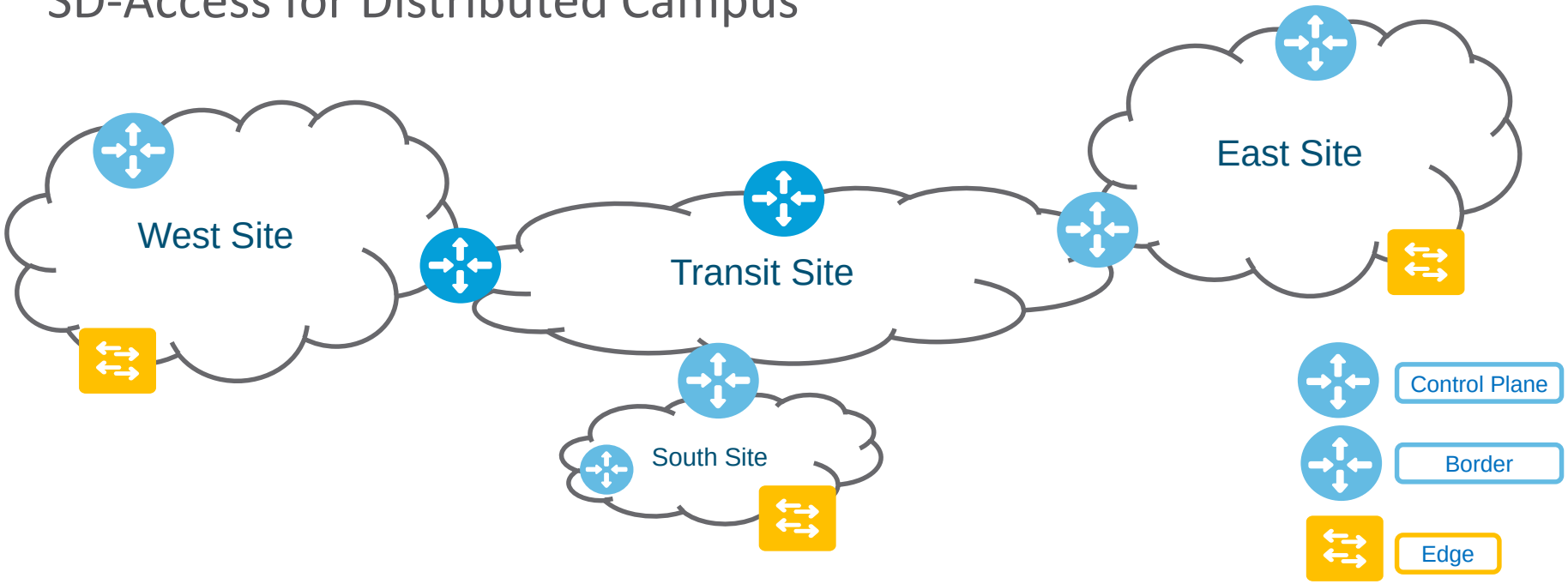
SD-Access Transit

* RECAP

- Border nodes will do a LISP-based lookup with the Transit Control Plane node
- Border nodes perform a VXLAN-GPO encapsulation to remote Border node
- End to End policy-plane is maintained using SGT group tags
- SD-Access Transit is fully automated

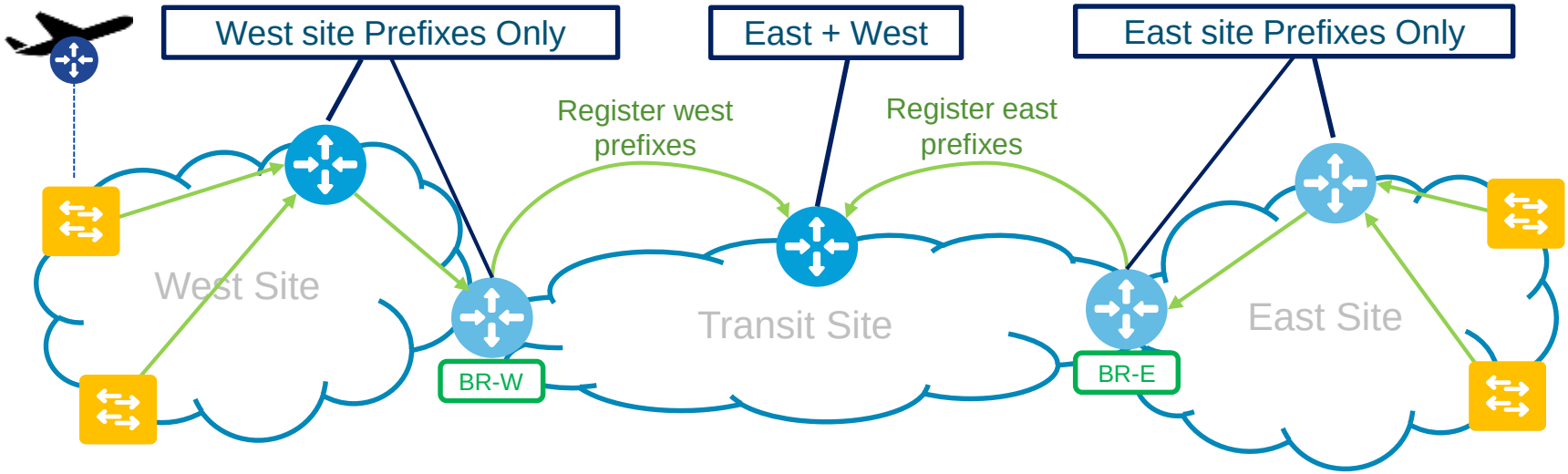


SD-Access for Distributed Campus

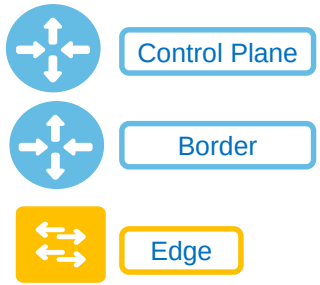


- Each site only maintains state for in-site end-points.
- Off site traffic follows default to transit.
- Survivability, each site is a fully autonomous resiliency domain
- Each site has its own unique subnets

SD-Access Transit Control Plane for Scale



- Border Routers hold Soft state for local site prefixes only
- Hard/Forwarding state instantiated on Border Routers strictly on demand
- Control Plane of the Stub sites holds only local host mappings. No remote mappings
- Cross site summary mappings registered in Transit Control Plane



SD-Access for Distributed Campus

SD-Access + IP Transit

- When Outside world(External) border needs to be used ?
  - This type of Border is picked when we want to connect to SD-access transit or the internet.
- When Anywhere(Internal +External) border needs to be used ?
  - This type of Border is picked when we want to connect to SD-access transit or internet and known part of the company like DC, WAN etc.
- When Rest of Company (Internal) border needs to be used ?
  - This type of Border is picked when we want to connect a site to the known part of the company like DC, WAN etc.

SD-Access for Distributed Campus

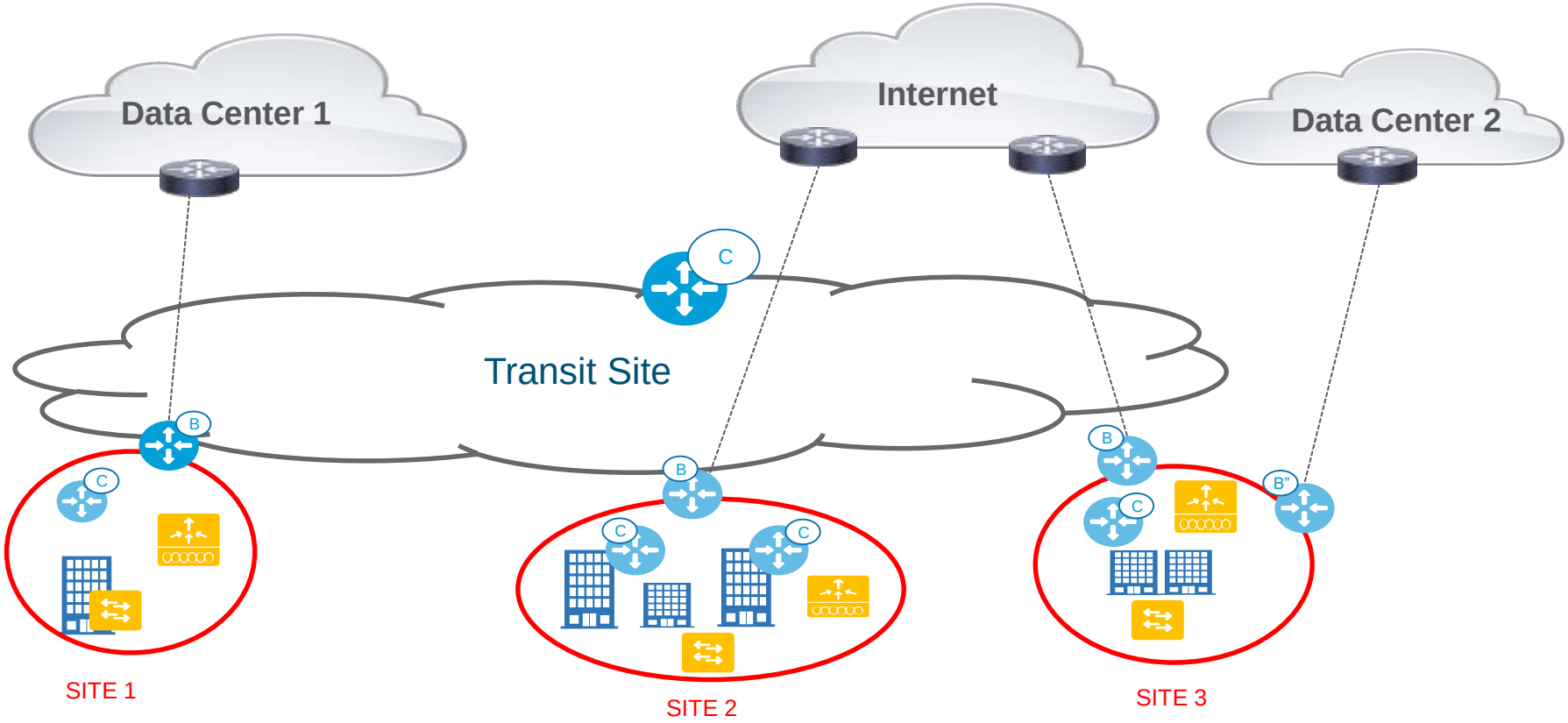
SD-Access + IP Transit

* RECAP

- When using DNAC to configure SD-Access Distributed campus with SD-Access transit we need to choose Outside world(external border) or Anywhere(internal +external) border when connecting to SD-Access transit.

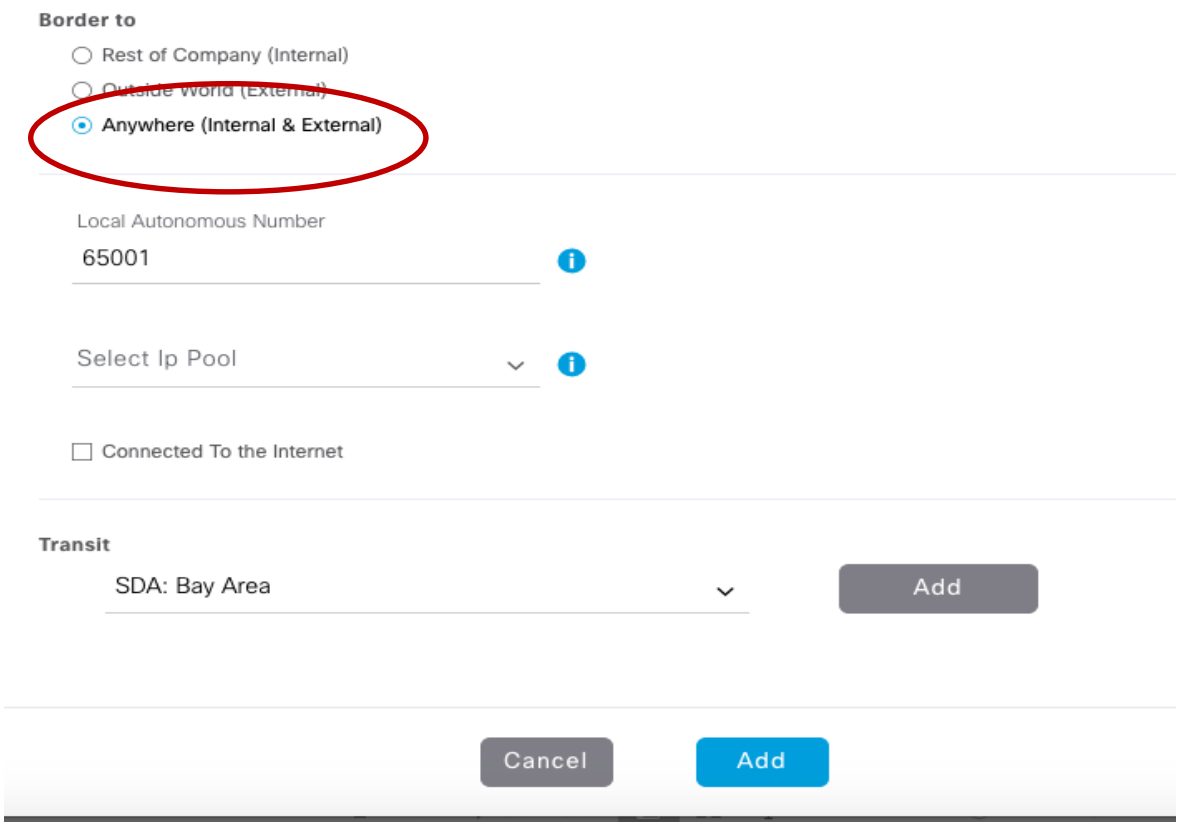
- In any given site when other external domain's like DC , WAN are being connected then we need to choose Rest of company (Internal) border.

SD-Access for Distributed Campus



SD-Access for Distributed Campus

DC/Internet/SD-Access Transit in Site 1



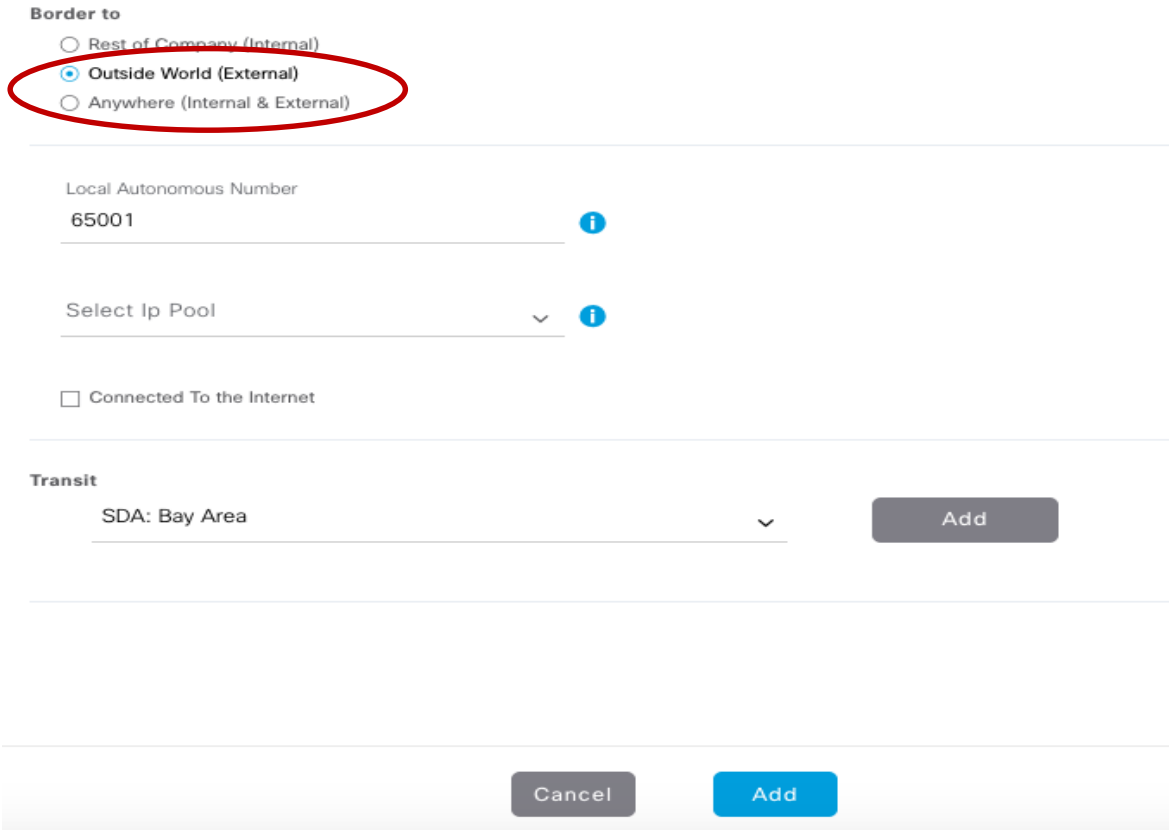
Pick Internal + External border

This is needed to ensure that the borders import the routes from DC 1 and register to the transit control plane node.

From above slide this needs to enabled on site 1 border so that site 2 and 3 border can use it to talk to Data center 1.

SD-Access for Distributed Campus

Internet/SD-Access Transit in site 2 and 3



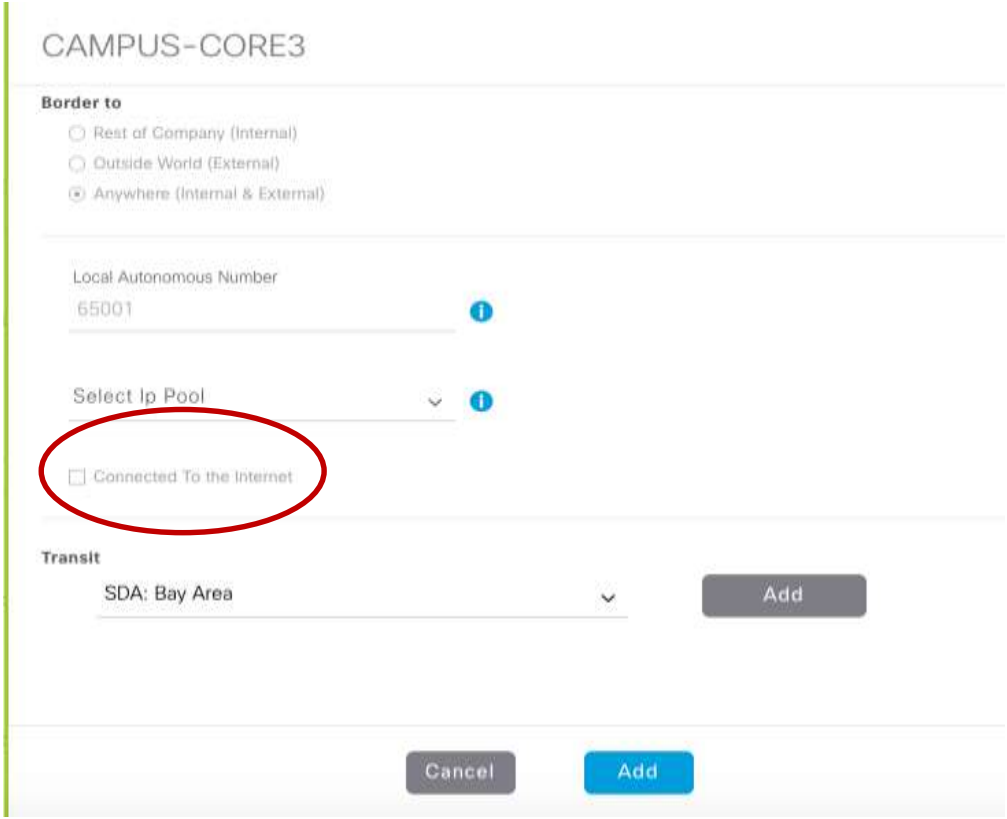
Pick External border

This is needed to ensure that the borders connect to the SD-Access transit and the Internet.

From above slide this needs to enabled on site 2 and 3 border that connect to SD-Access Transit.

SD-Access for Distributed Campus

Internet Access



Connected to Internet – Check Box

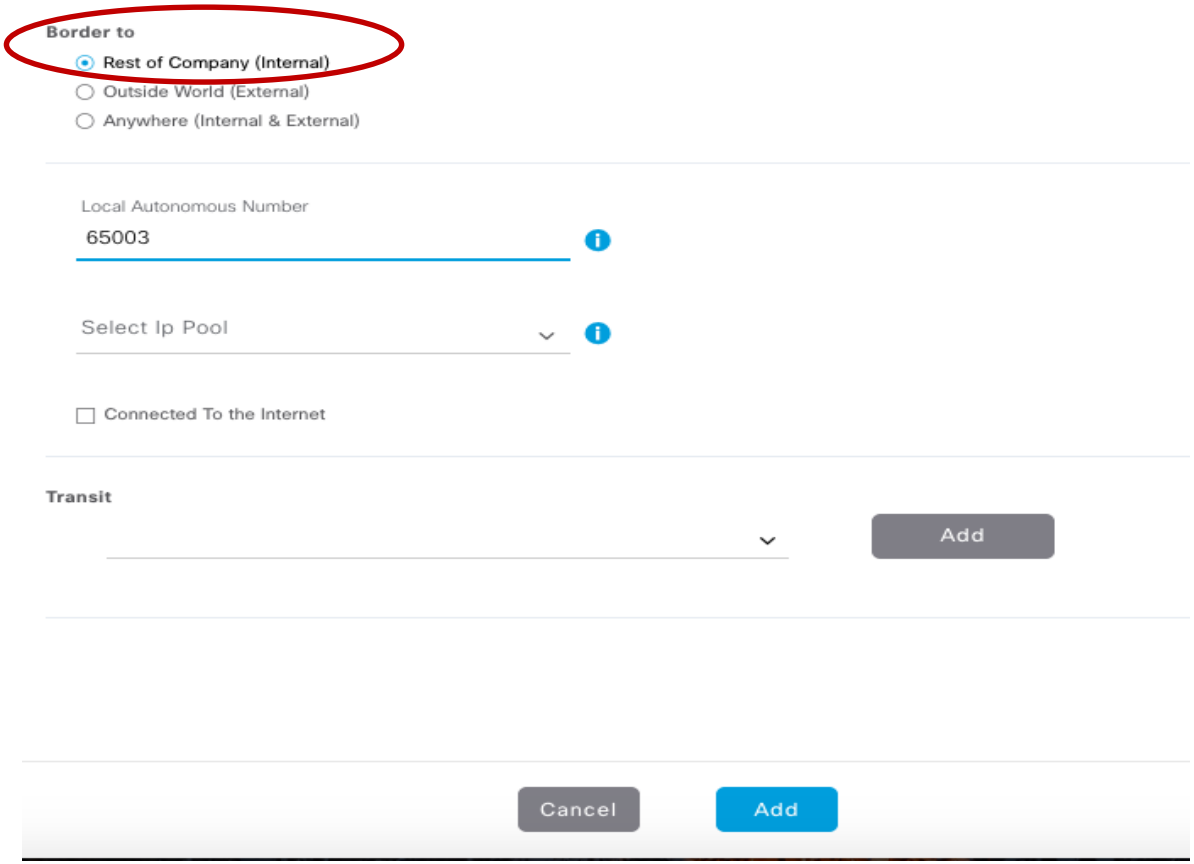
This checkbox needs to be mandatorily enabled on all borders that connect to internet when SD-Access is used as the transit.

This is needed to ensure that the borders/sites that don't have access to internet will use the borders/sites that do have access to internet to talk to it.

From above slide the check box needs to be marked on site 2 and 3 border (that connect to SD-Access transit so that site 1 border can use them to talk to internet

SD-Access for Distributed Campus

Data Center 2 in Site 3



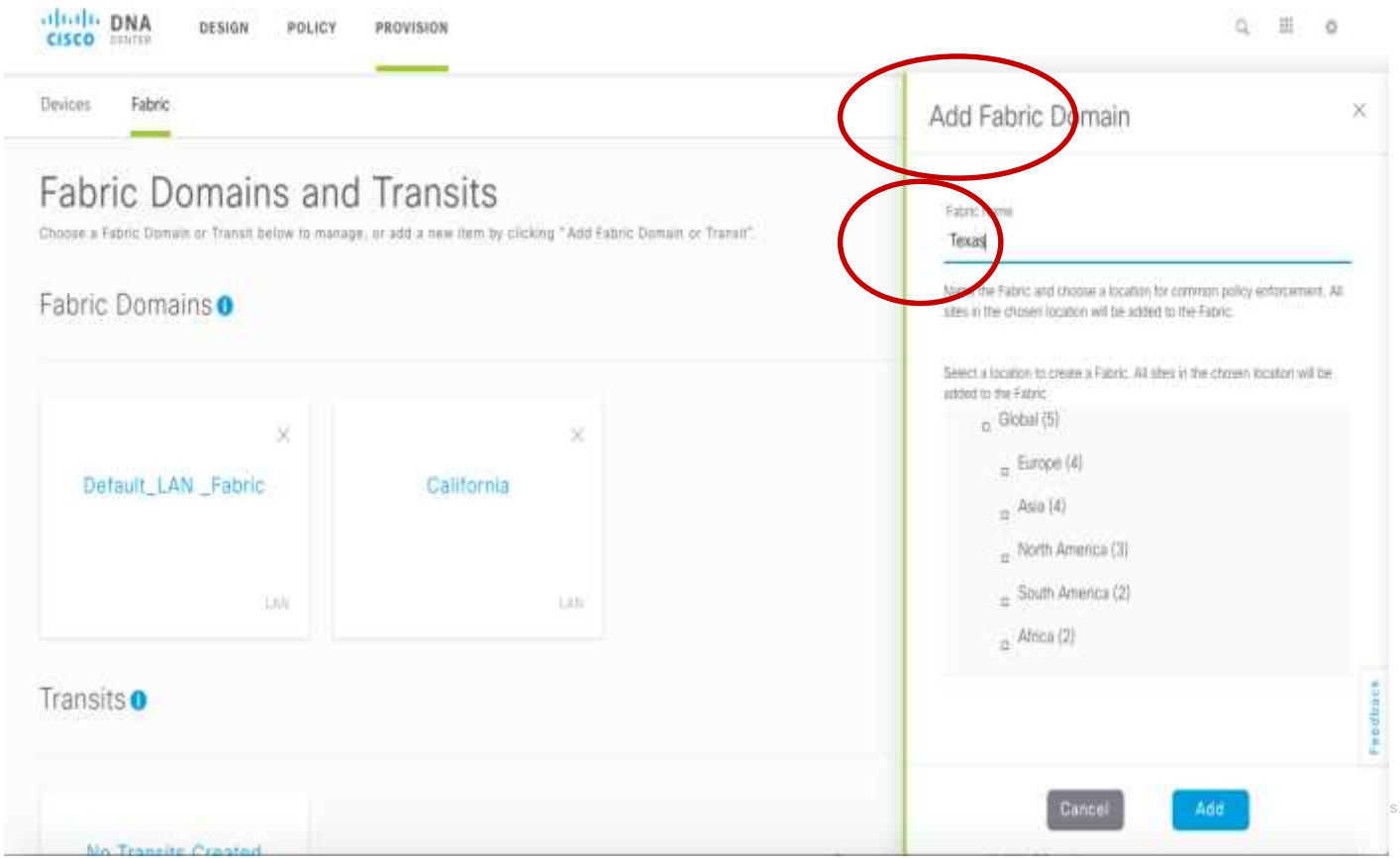
Pick Internal border

This is needed to ensure that the borders import the routes from DC 2 and register to the site control plane node.

From above slide this needs to enabled on site 3 border (B") so that we can use it to talk to Data center 2.

SD-Access @ DNA Center

Enabling SD-Access Distributed Campus

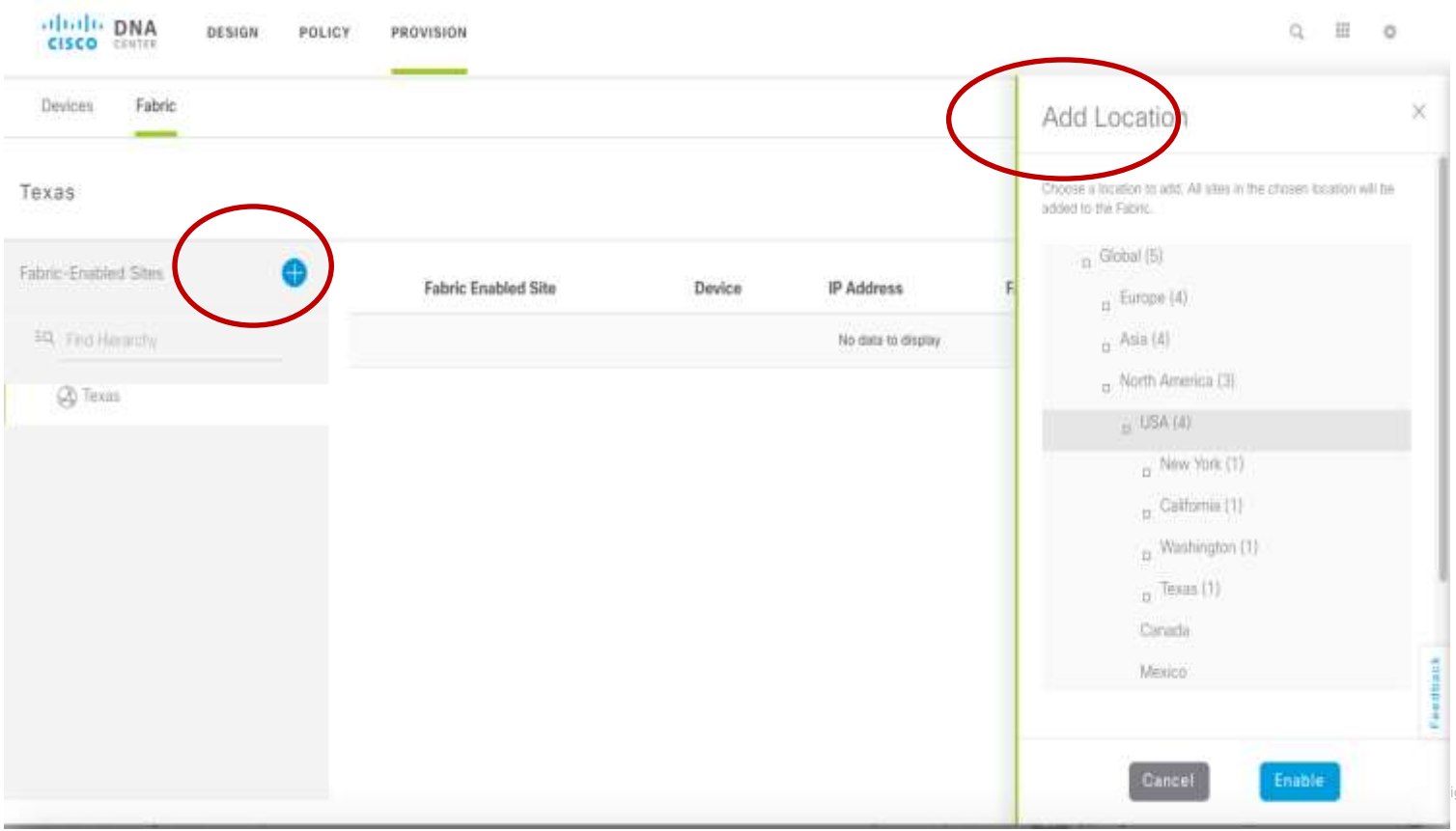


Create a Fabric Domain

This will create the fabric domain. You can now add fabric sites to this fabric domain

SD-Access @ DNA Center

Enabling SD-Access Distributed Campus



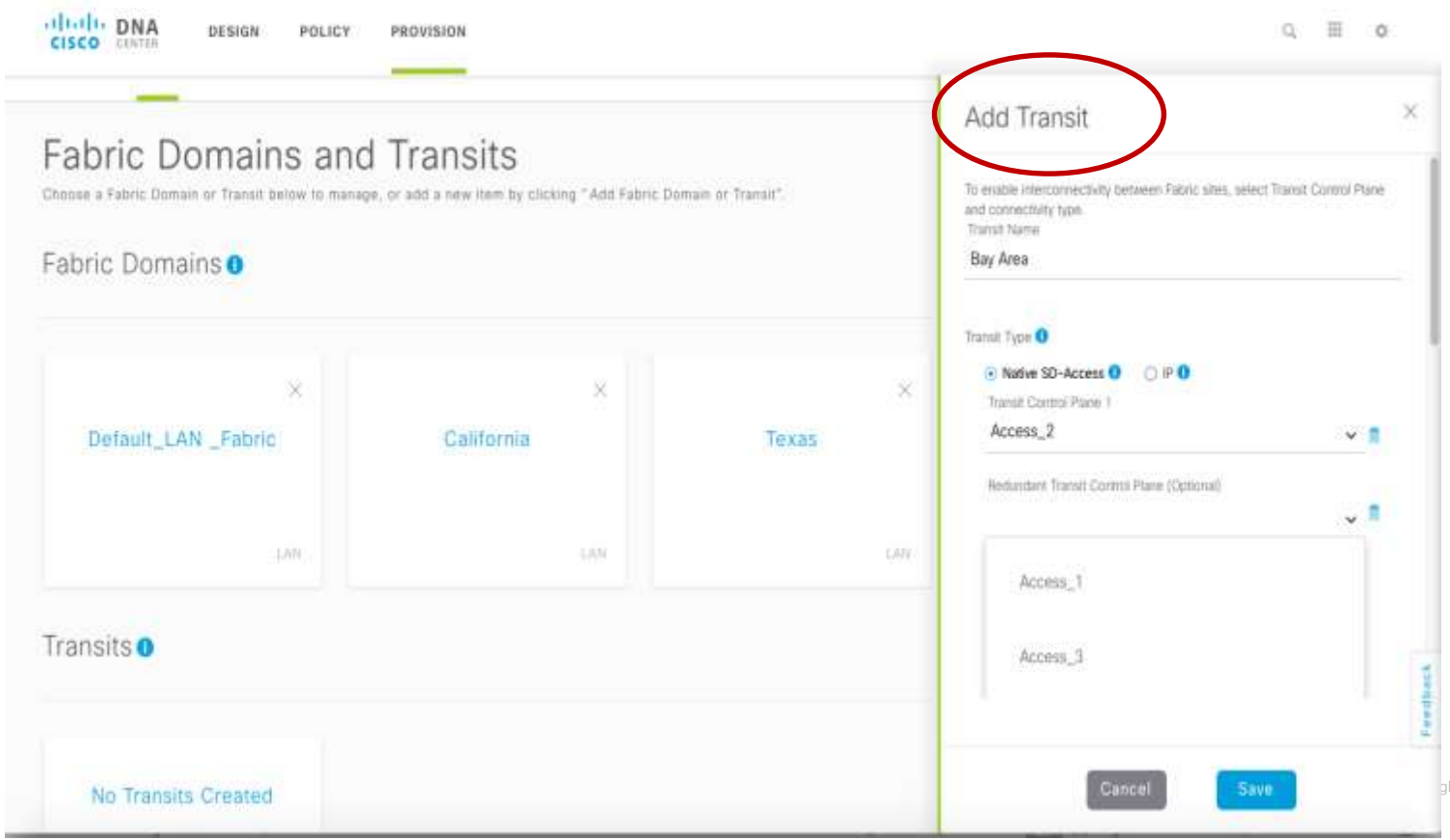
Add a Fabric Site under a Fabric Domain,

This will add fabric sites to this fabric domain.

We follow a hierarchical model where if you select , lets say USA then every location like Ney work , California , Texas etc. are added to the fabric site

SD-Access @ DNA Center

Enabling SD-Access Distributed Campus

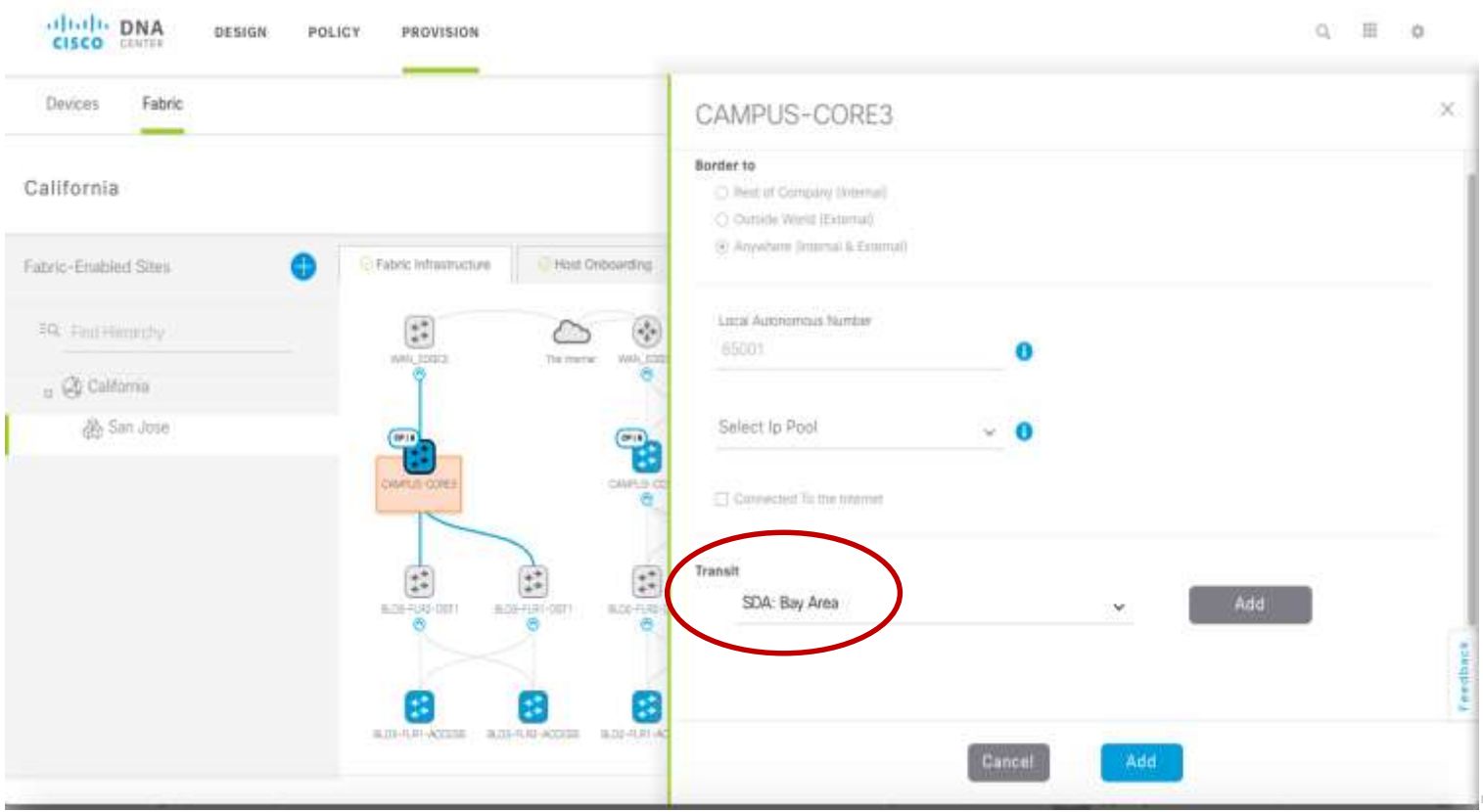


Create a Transit

Add Transit CP nodes to Transit

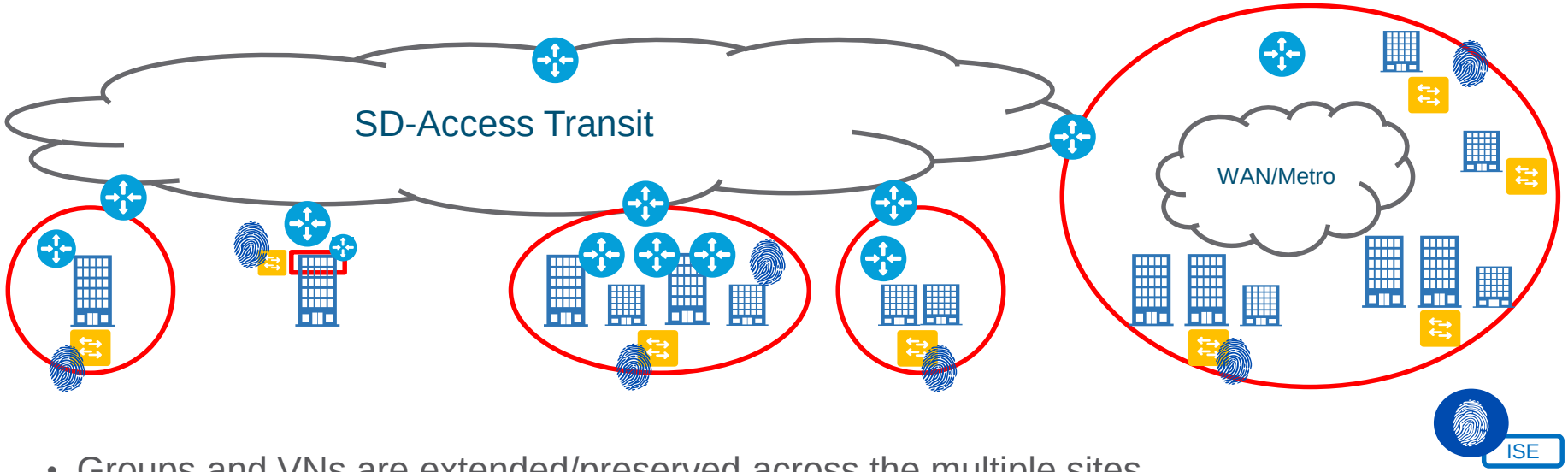
SD-Access @ DNA Center

Enabling SD-Access Distributed Campus



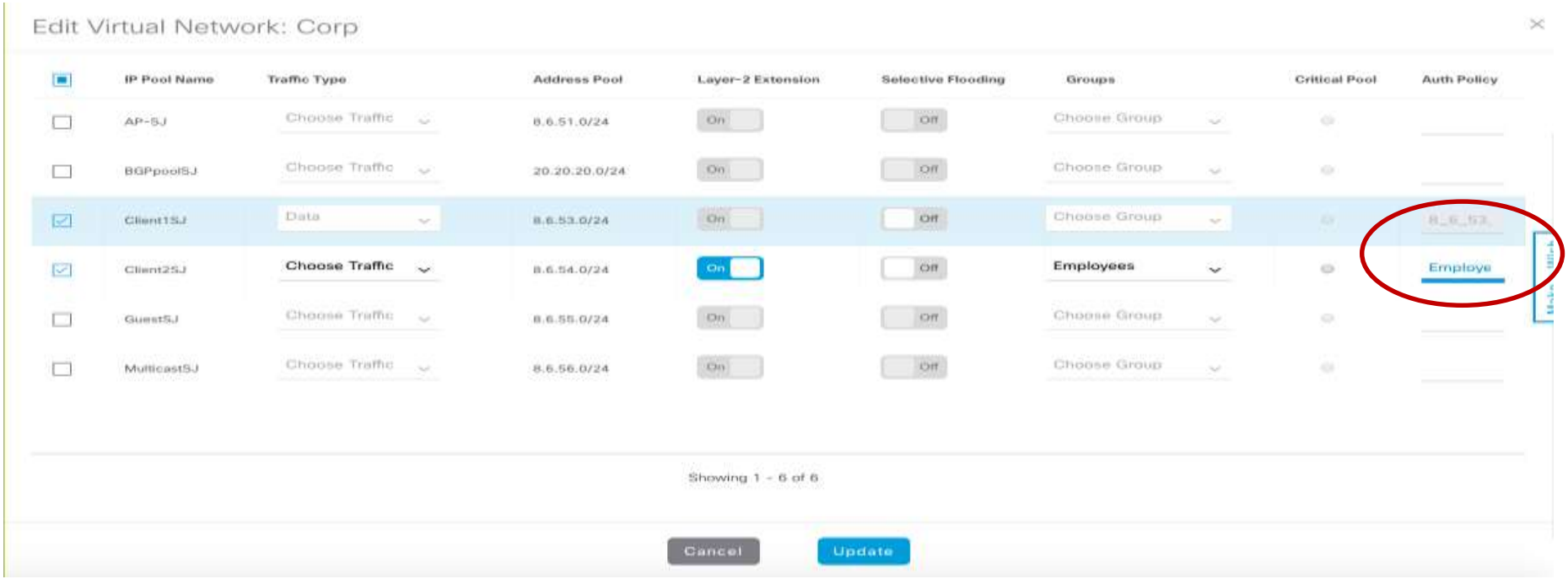
Add Borders to the Transit as needed.

SD-Access for Distributed Campus- Policy



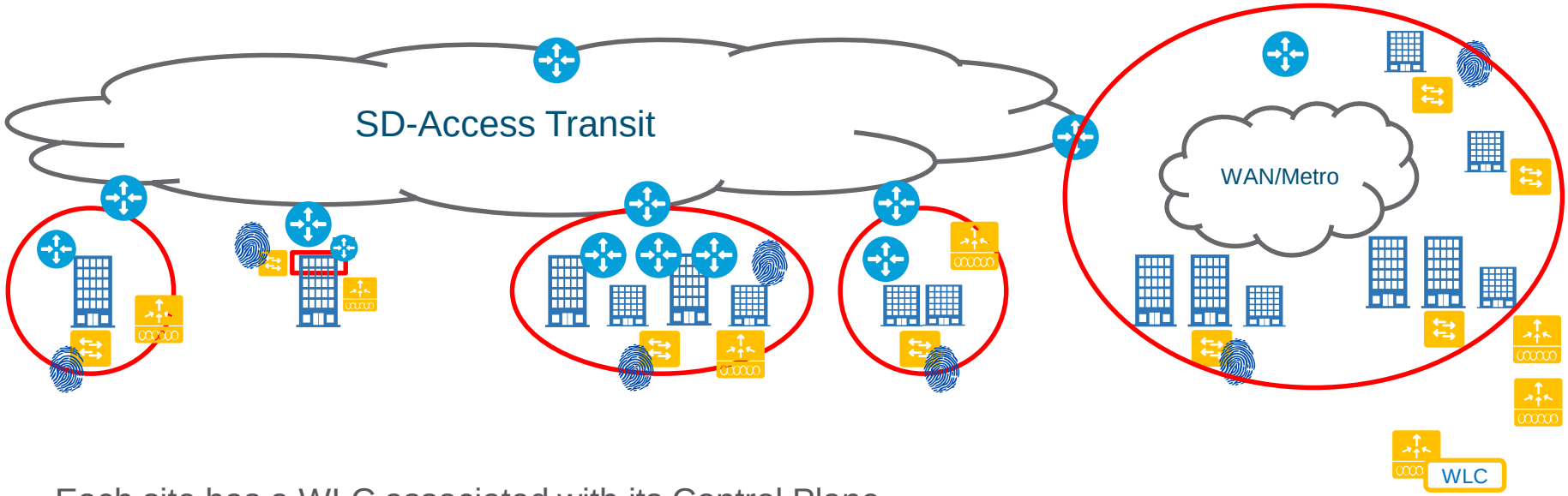
- Groups and VNs are extended/preserved across the multiple sites
- End to end policy enforcement using Group tags (SGT's)
- Across sites we don't have the same IP subnets

SD-Access for Distributed Campus- Policy



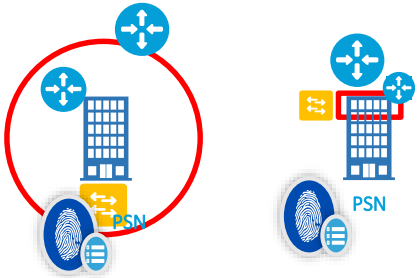
- Different subnets across the sites can have the same Auth Policy/Vlan name
- Same policy maintained across sites for the same set of users

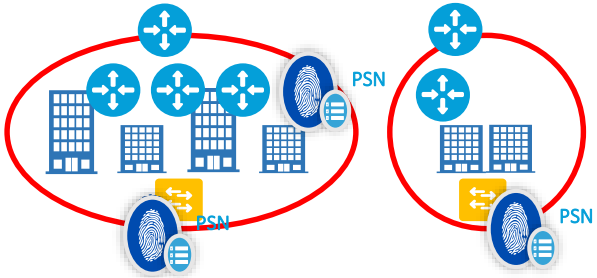
SD-Access for Distributed Campus- Wireless

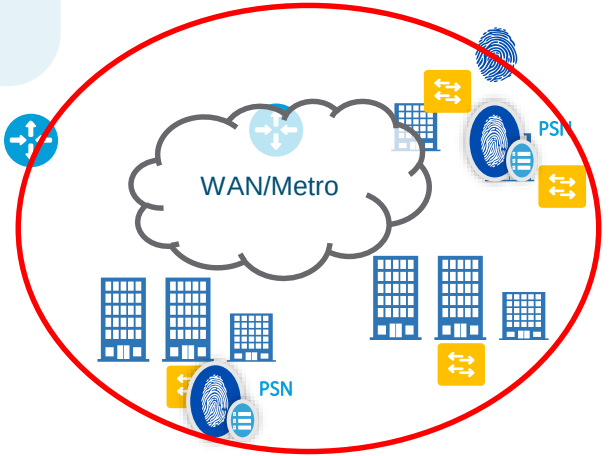


- Each site has a WLC associated with its Control Plane
- Smaller locations in the same metro site may share a WLC

ISE distributed deployment – Model 1

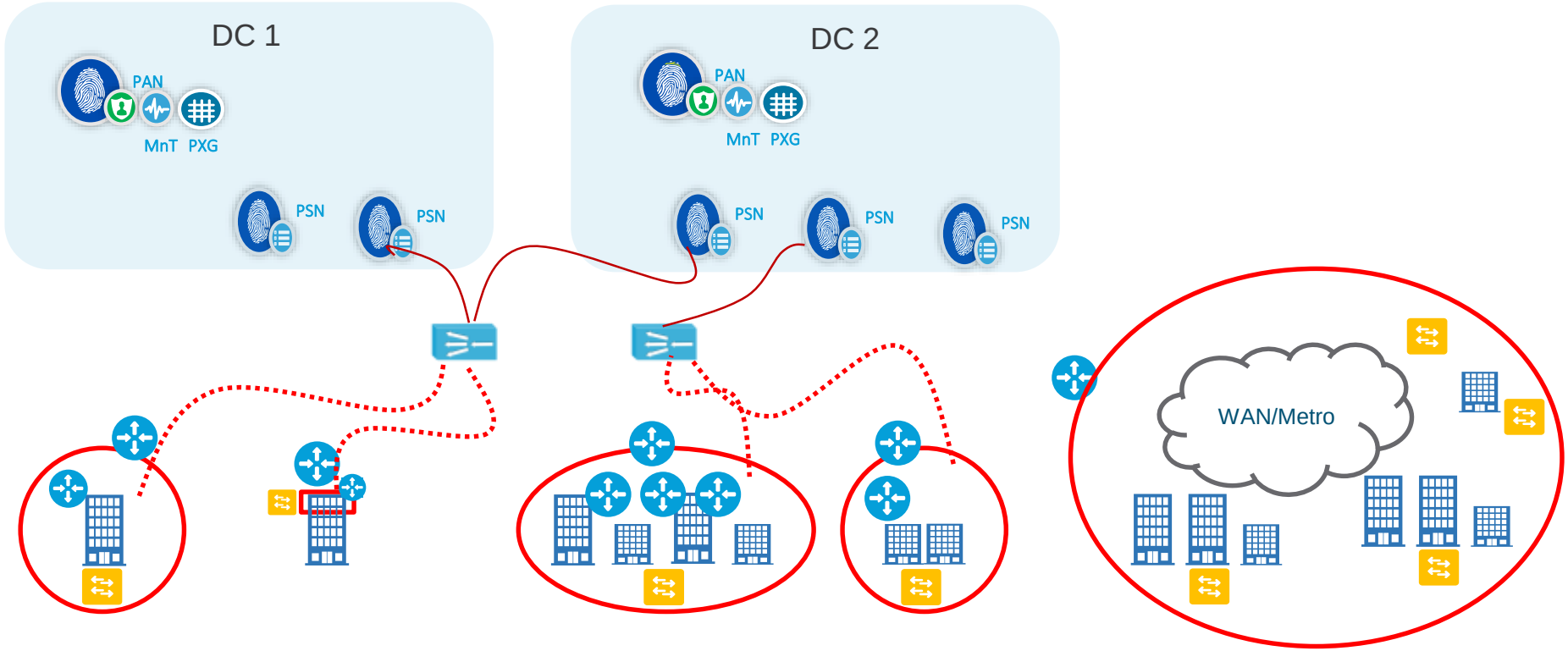






- PSN Nodes in Every Site
- Max of 2 PSN's per site
- PAN's are Centralized in Data Center

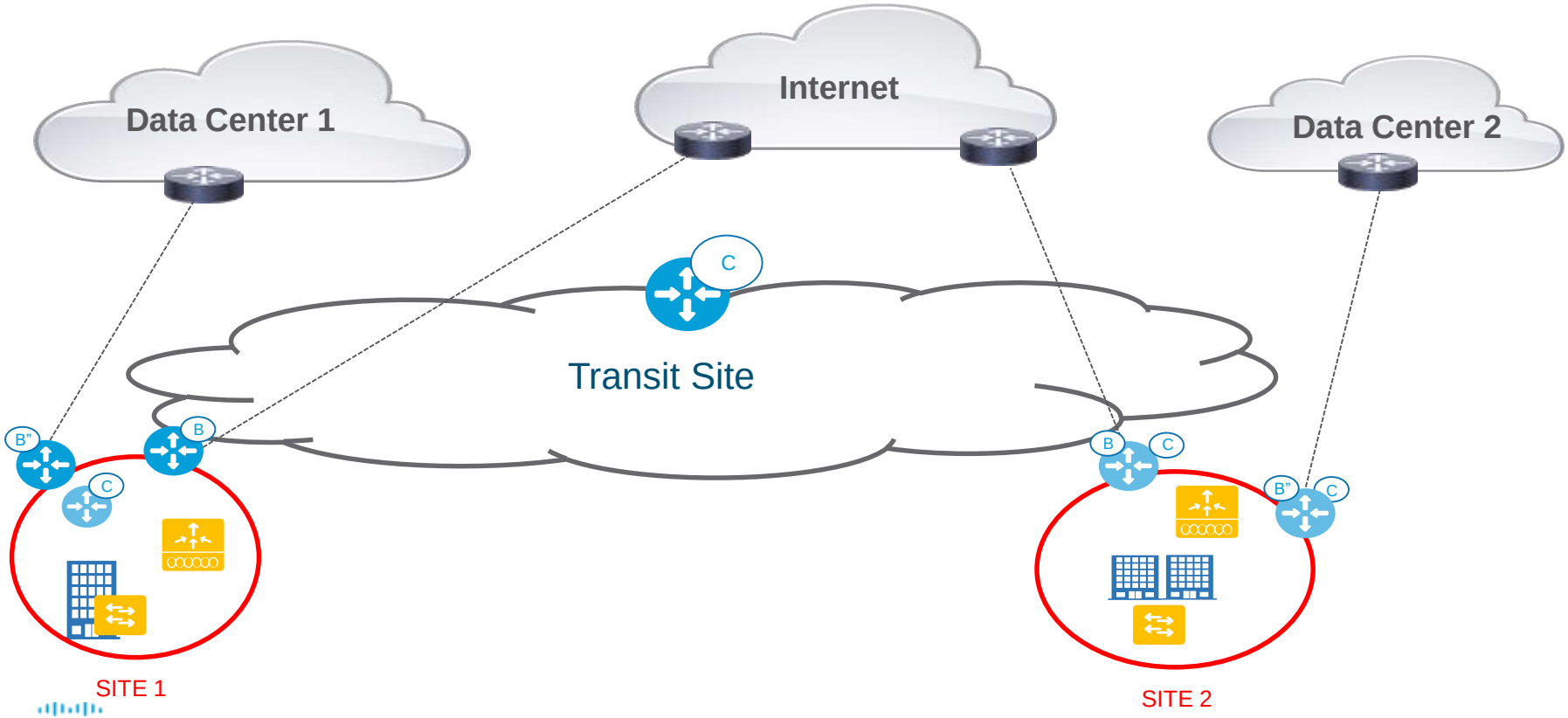
ISE distributed deployment – Model 2



- PSN's are Behind an Load Balancer
- Text box provided in DNAC to input Load Balancer IP

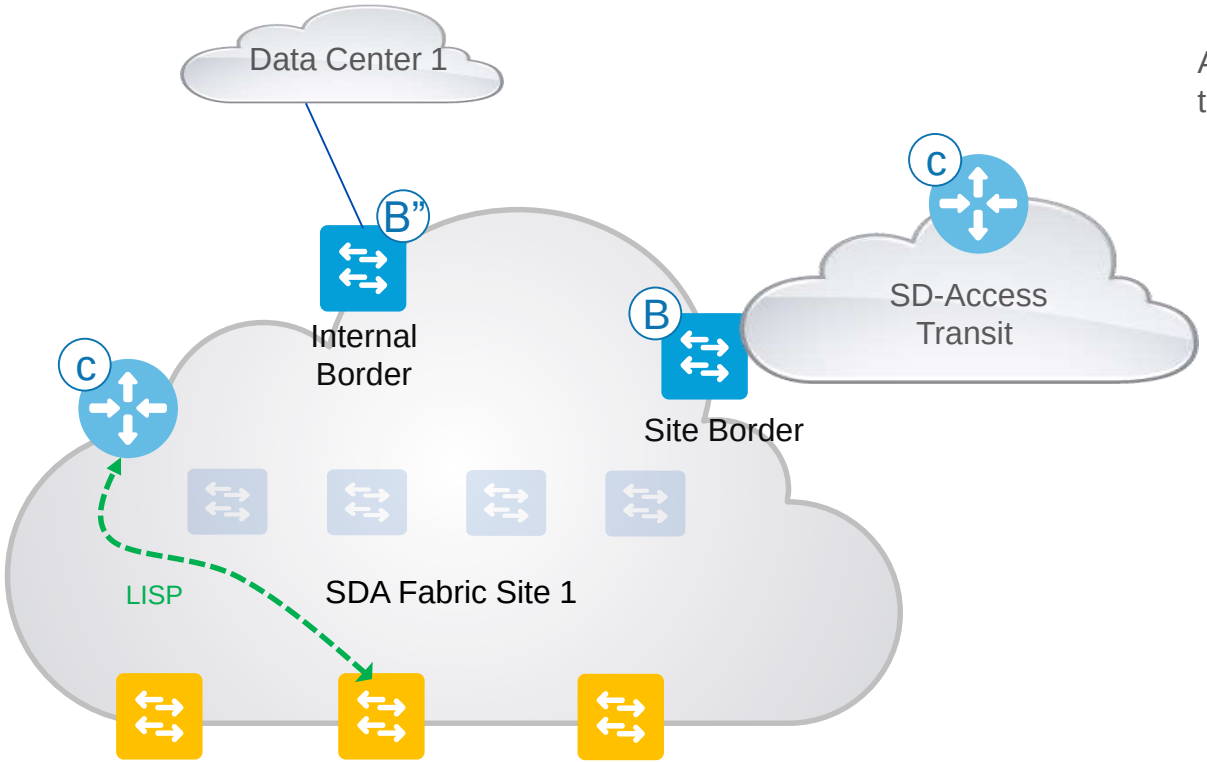
SD-Access Distributed Campus Deployment Models

SD-Access for Distributed Campus



SD-Access for Distributed Campus

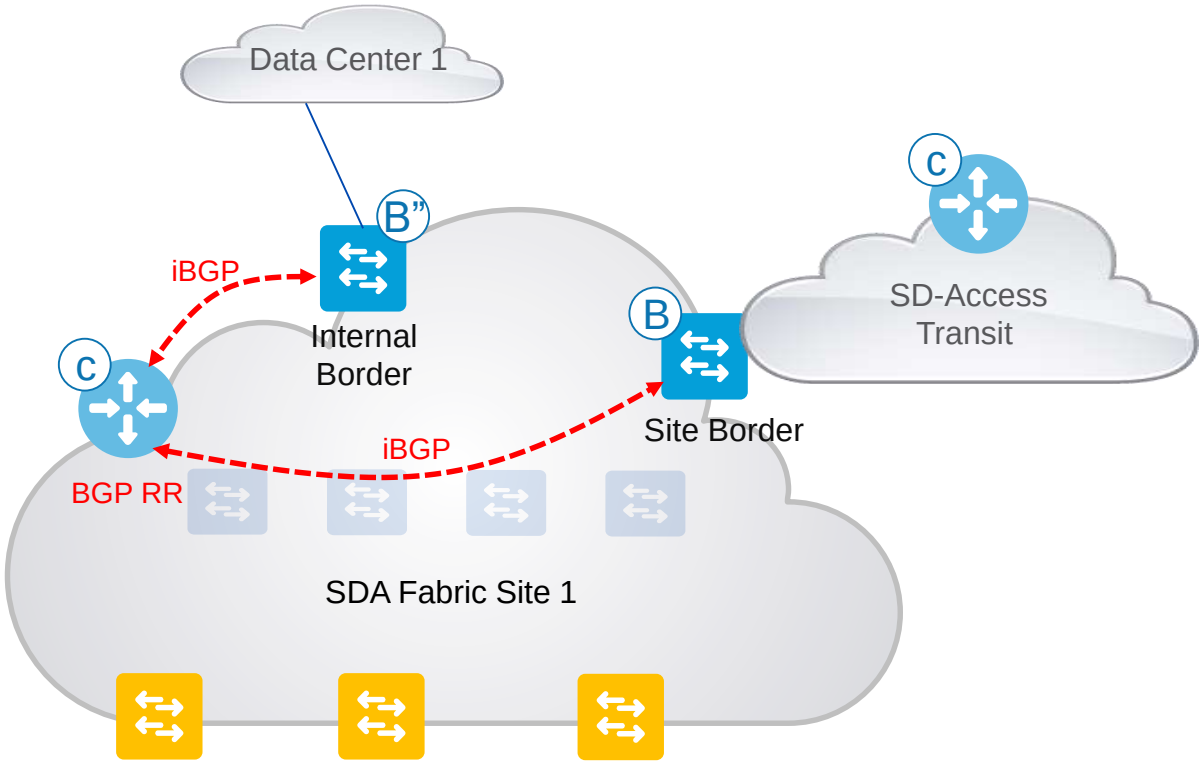
Non Co-Located Border and Control Plane node- Site 1



All edge nodes register their IP/MAC mappings to the control plane node.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



The Control plane node advertises these mappings via iBGP to all the border nodes in that site. These advertisements are based on aggregate routes from the control plane node.

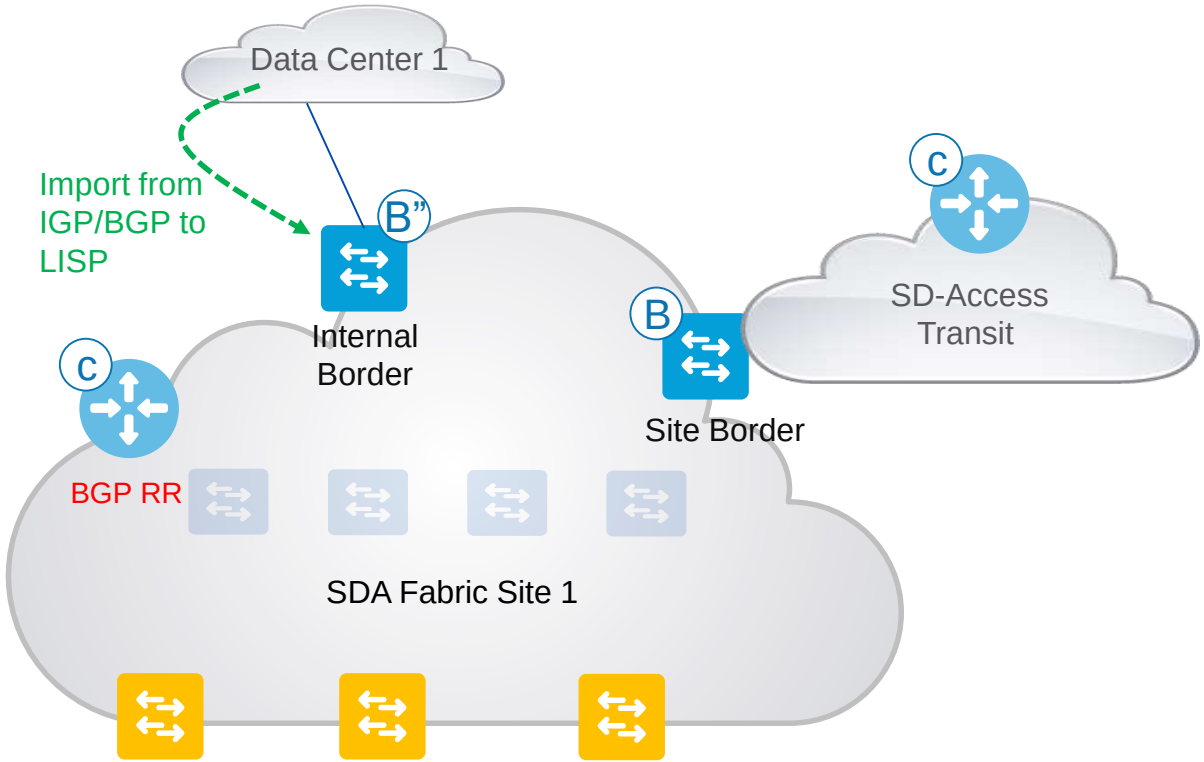
On the control Plane node we add a route-map (TAG_LOCAL_EIDS) outbound for all the neighborship's to the border nodes in that site.

This route-map sets the community for all the routes advertised to ”65370”.

The Control plane node in also a BGP route reflector meaning it reflects the routes learned from one border to others within that site.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



The Internal Border imports the routes from IGP/BGP into LISP so that we can register it to the control plane node. When performing this route import we attach a route-map (DENY_ALL_EIDS) to that function.

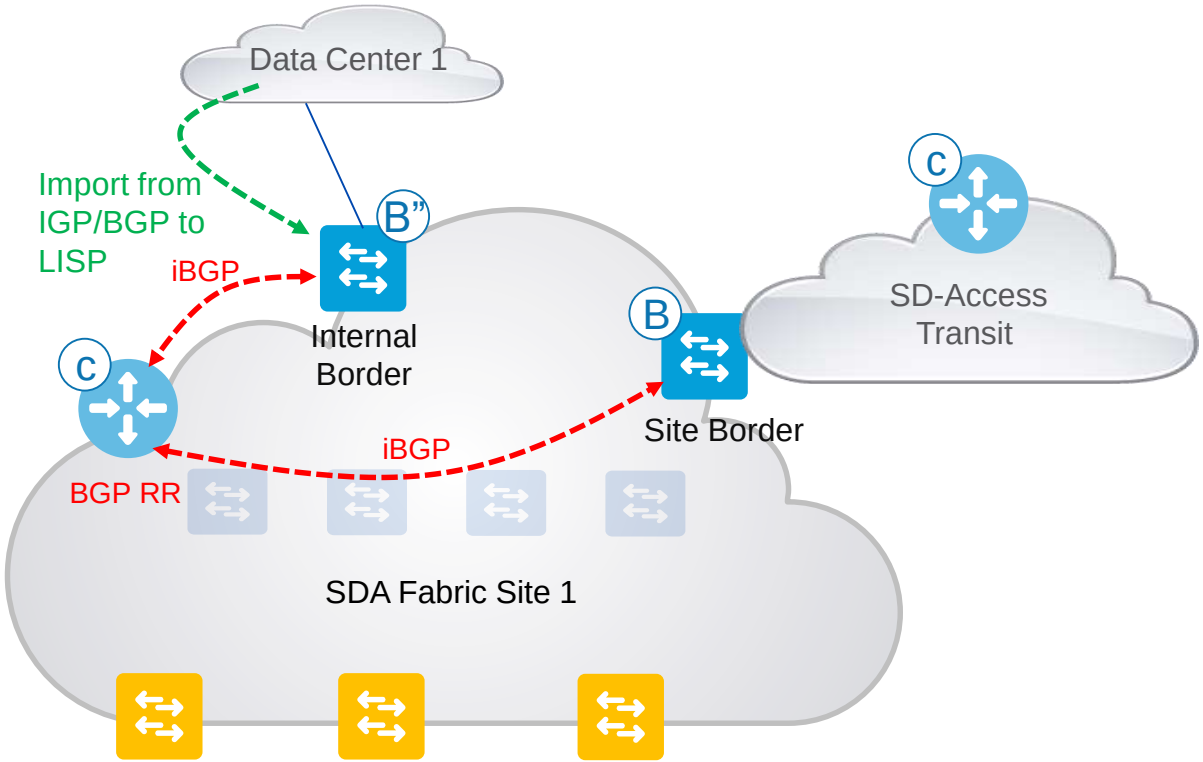
This route-map tags the routes we are importing with community value”65370” .This is done in the BGP neighborship using the rote-map (TAG_LOCAL_EIDS)

The route-map also denies all the EID prefixes from being imported. The EID prefixes that are denied are not only from from local site but also from other sites via the transit CP.

* For above we use the community lisp of transit CP which is explained in later slides.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1

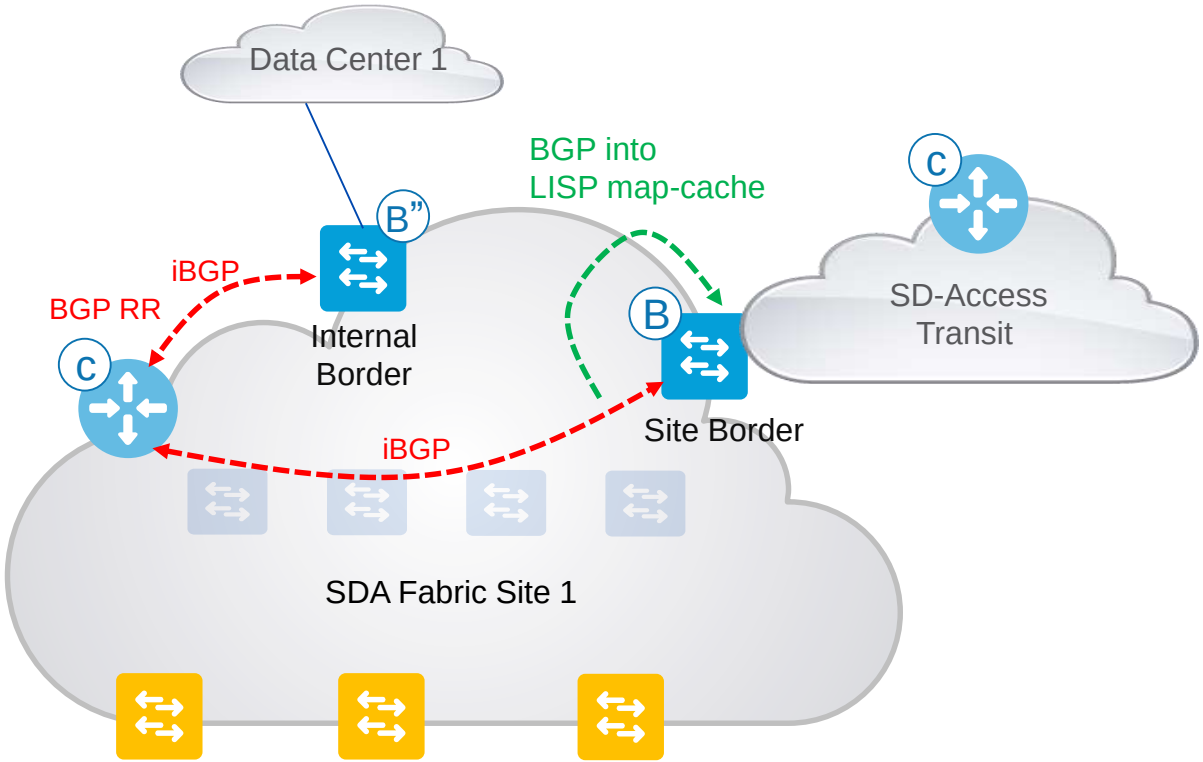


The prefixes imported from the DC to the internal border are sent to the site border since the CP node is a BGP RR and will reflect all the routes.

Since the BGP RR cannot tag any routes in transit (it can only reflect routes and not modify any attributes) we are tagging the routes with the needed community attribute on the internal border.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



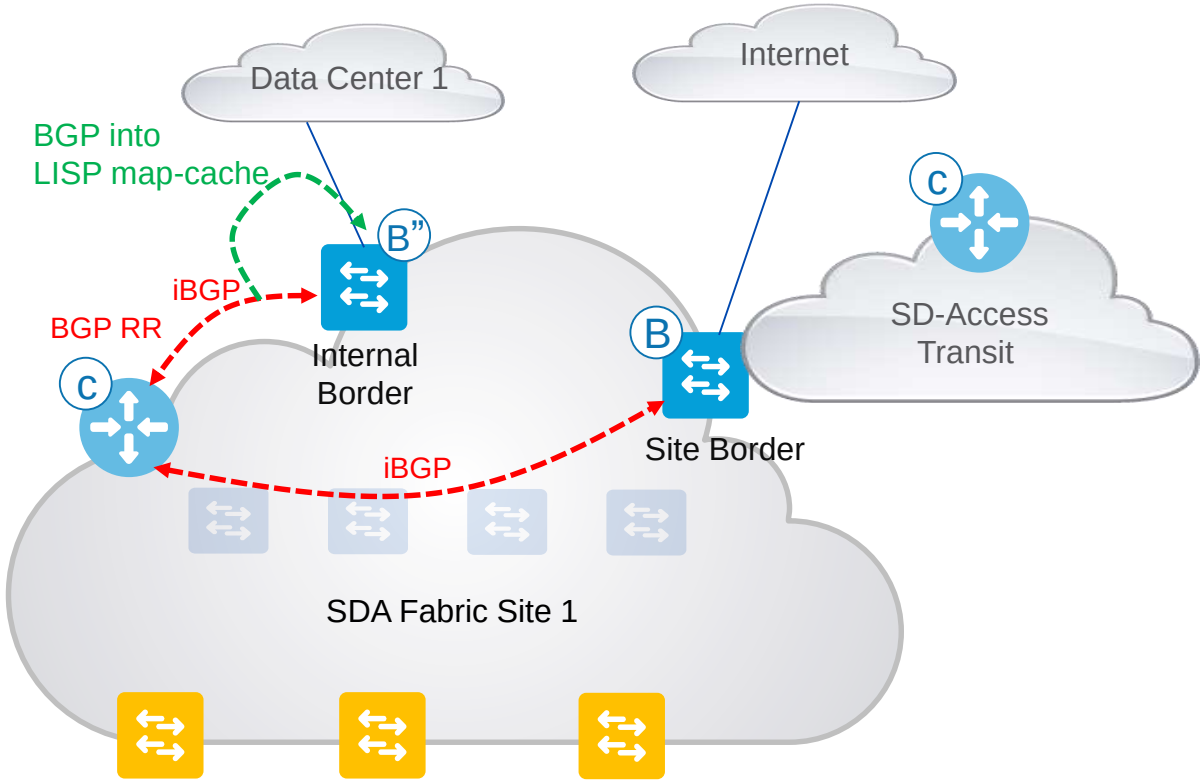
At the Site Border all the prefixes tagged with community “65370” needs to imported into LISP map-cache . This is done with a route-map (PERMIT_ALL_EIDS) where all the EID’s will be imported as map-cache entries.

These entries that are originating in the site are either through the LISP CP tagged with the community attribute and also from the internal border tagged with the same community attribute.

The local site border also imports the other site prefixes coming from transit CP into map-cache entry. This will be explained in later slides.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



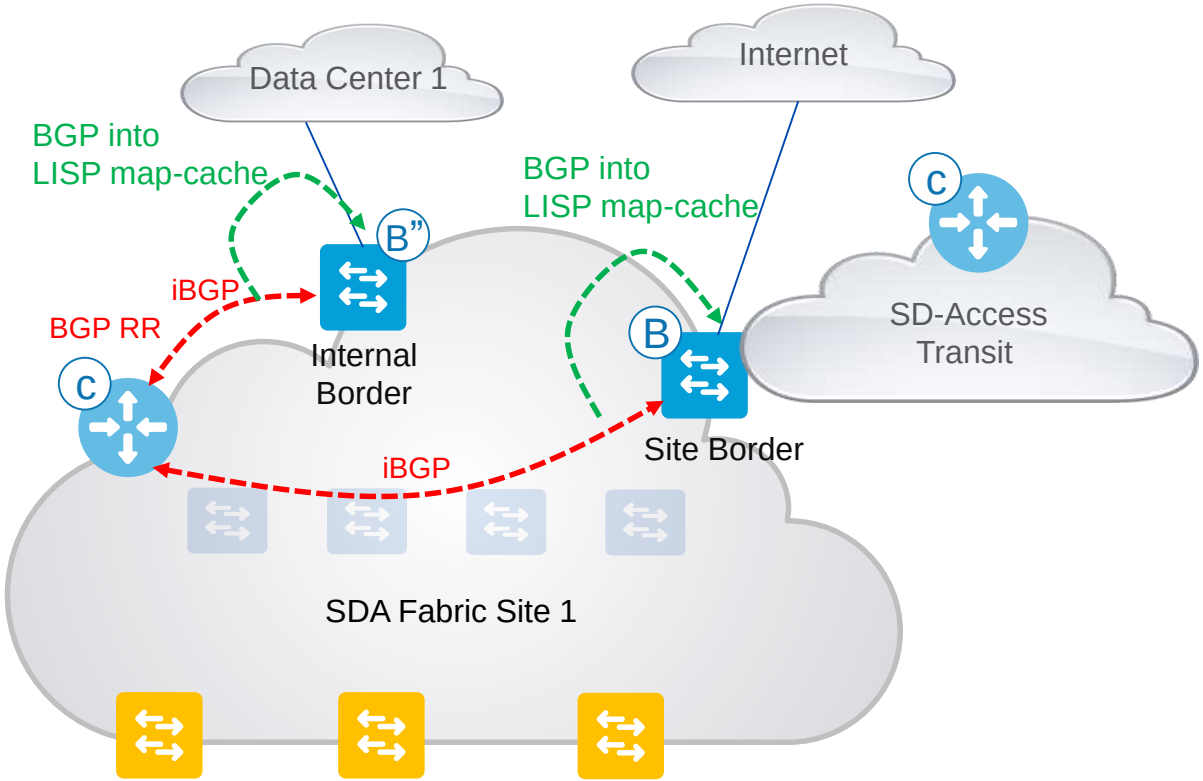
At the Internal Border as well all the prefixes tagged with community “65370” needs to imported into LISP map-cache . This is done with a route-map (PERMIT_ALL_EIDS) where all the EID’s will be imported as map-cache entries.

These entries that are originating in the site are either through the LISP CP tagged with the community attribute and also from the site border tagged with the same community attribute.

The internal border also imports the other site prefixes coming from transit CP into map-cache entry. This will be explained in later slides.

SD-Access for Distributed Campus

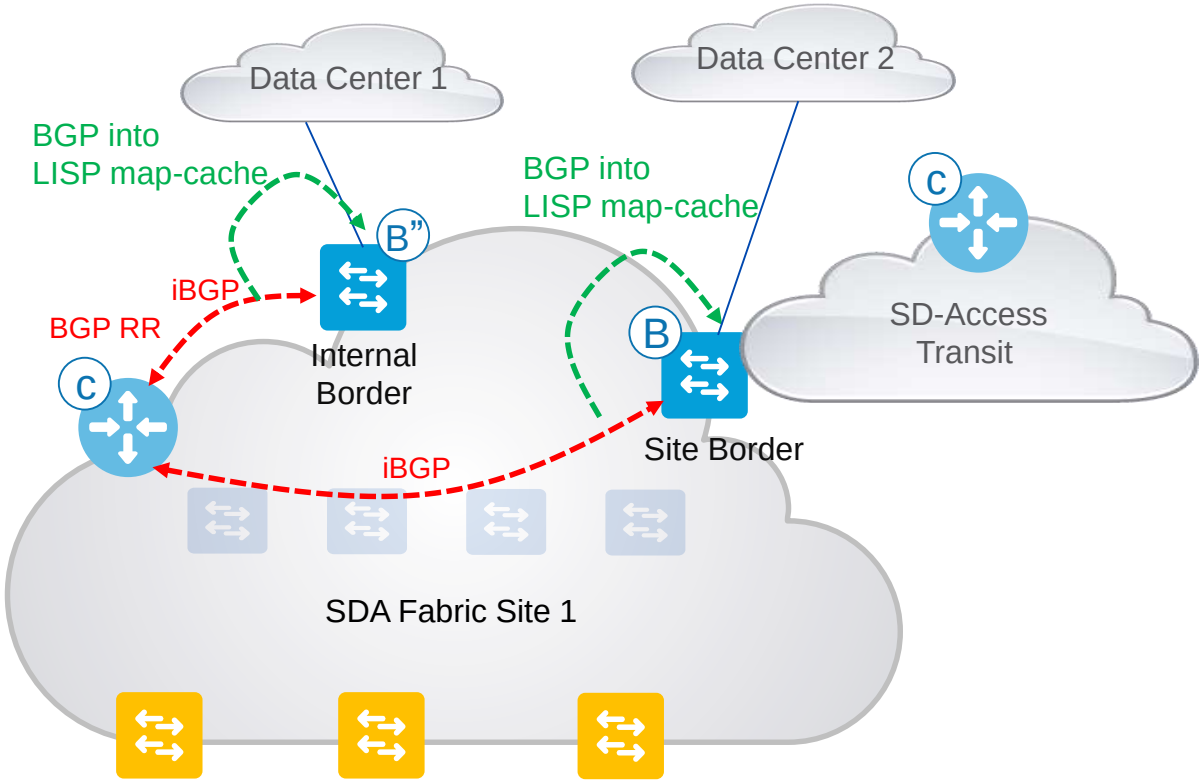
Transit Use case - Site 1



The site 1 fabric is acting as a transit network between Internet and Data Center.

SD-Access for Distributed Campus

Transit Use case - Site 1



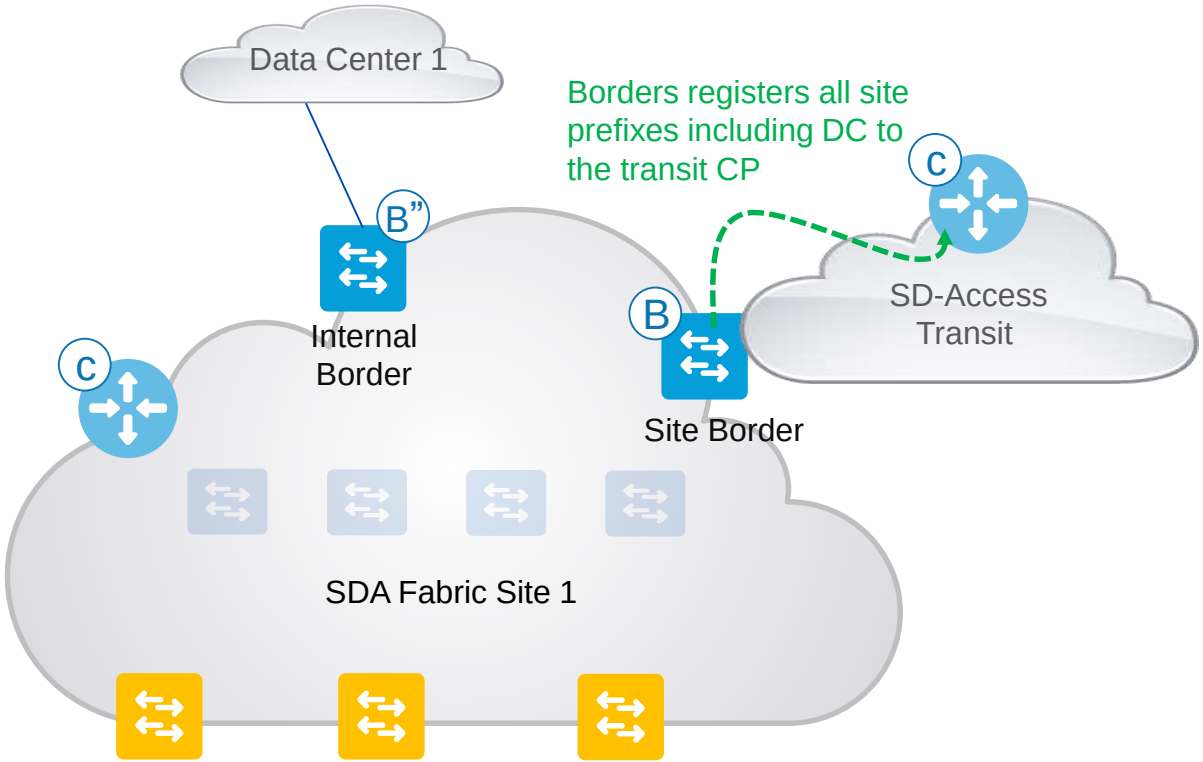
If the Site I fabric was connecting to Data center 1 via Internal border and Data Center 2 via site border then Data center 1 and 2 can talk to each other using the site 1 fabric.

This transit use case is being enabled in DNAC 1.2.5.

In this case the site border is an Internal+ external border.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1

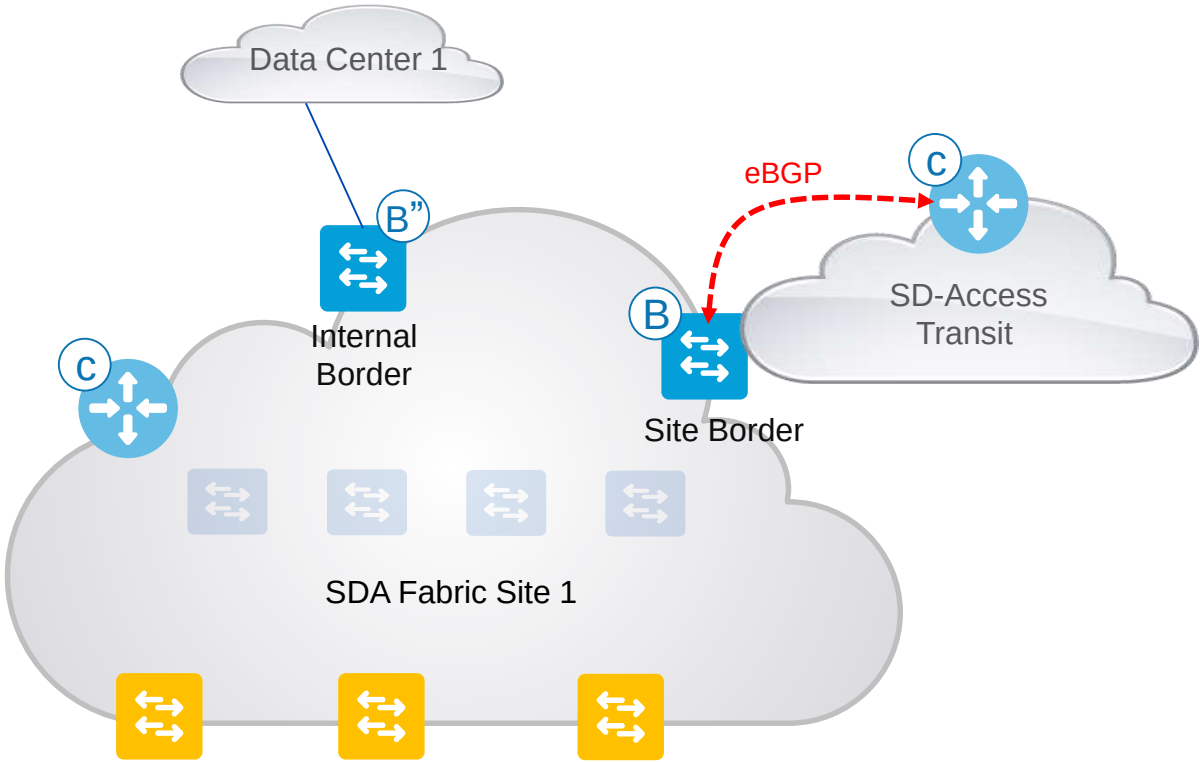


At the Site Border all the prefixes tagged with community “65370” needs to be registered with the transit CP. This needs to be done to ensure that the other sites can use the site border of site 1 to reach data center 1 and also site 1 prefixes. The route-map (SITE_LOCAL_EIDS) is used to ensure that only the site 1 prefixes are registered to the transit CP.

These prefixes are already aggregated from the site CP and hence the transit CP will only have subnet entries and not /32 entries.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



Since all site borders registers their local sites prefixes to the transit CP it has the entire information of the fabric domain.

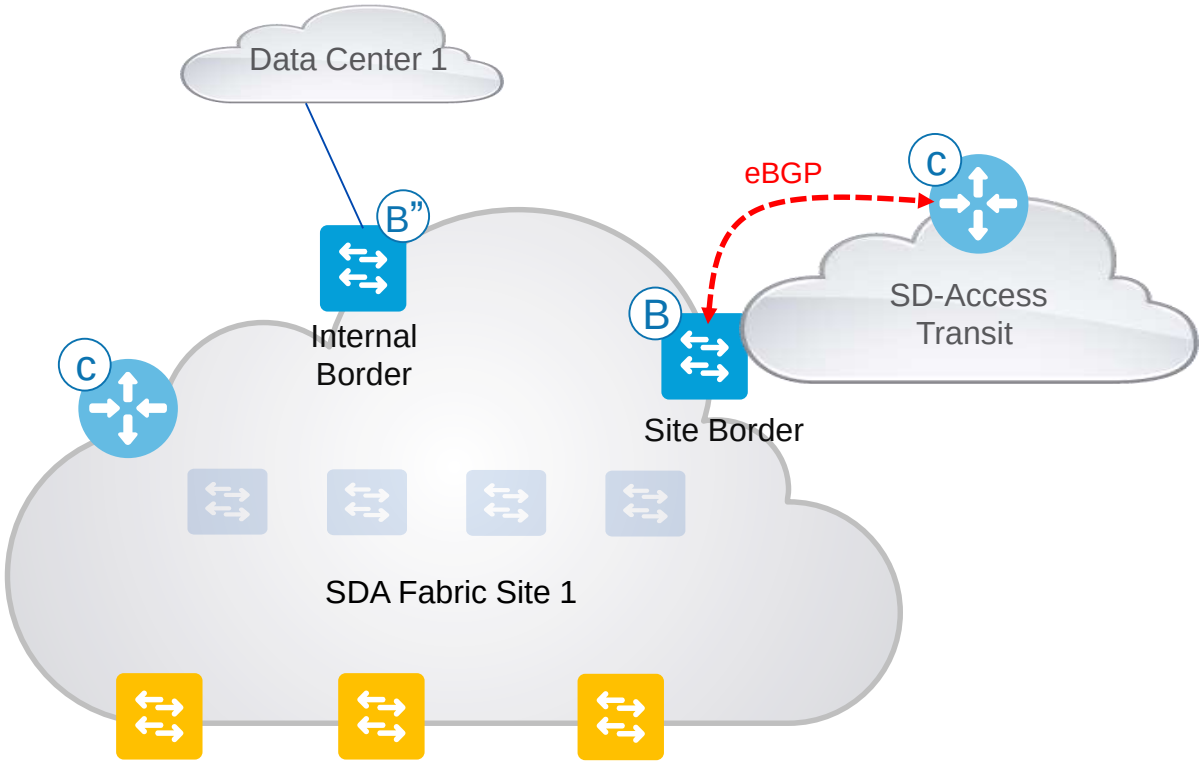
The Transit CP is auto configured from DNAC to use AS 64512 and form eBGP relationship to all the site borders. The AS number is auto picked by DNAC is always constant (no user provided options).

If the Transit CP has BGP already configured we check if its with AS 64512 and if it is we will accept it. If not we will throw an error and ask user to change the AS number or remove BGP.

This also means that the site borders can never be configured with AS 64512 and we will ensure that from the UI this is blocked.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



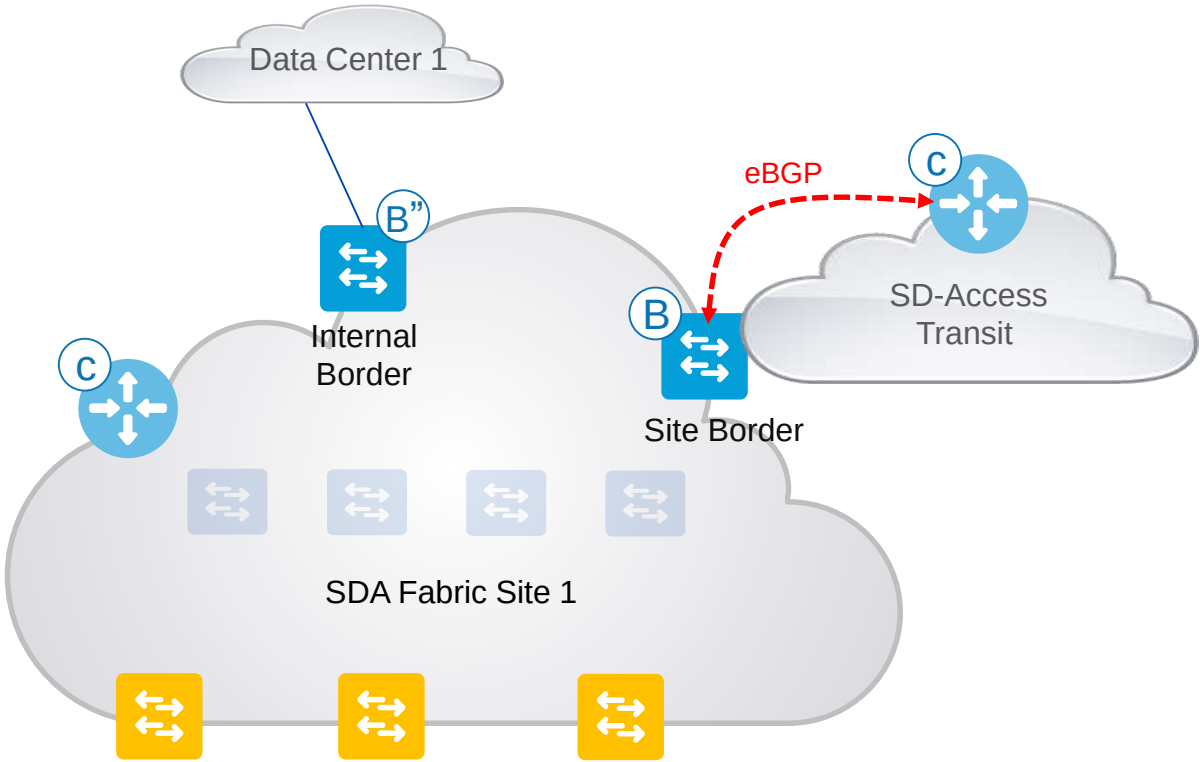
At the Transit CP we have a route-map (DENY_ALL) configured in the inbound direction for all the eBGP neighborship's from all the site borders to ensure that BGP does not accepts any routes.

The reason this is done is to ensure that the transit CP has the routes from the LISP registration only from all Site borders for its respective prefixes.

If BGP would advertise the routes than since its admin distance is 20 and in LISP we configure the admin distance to 250 BGP will be preferred. If transit CP prefers the BGP value then there is no way to distinguish routes based on community attributes anymore. This is explained in later slides.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



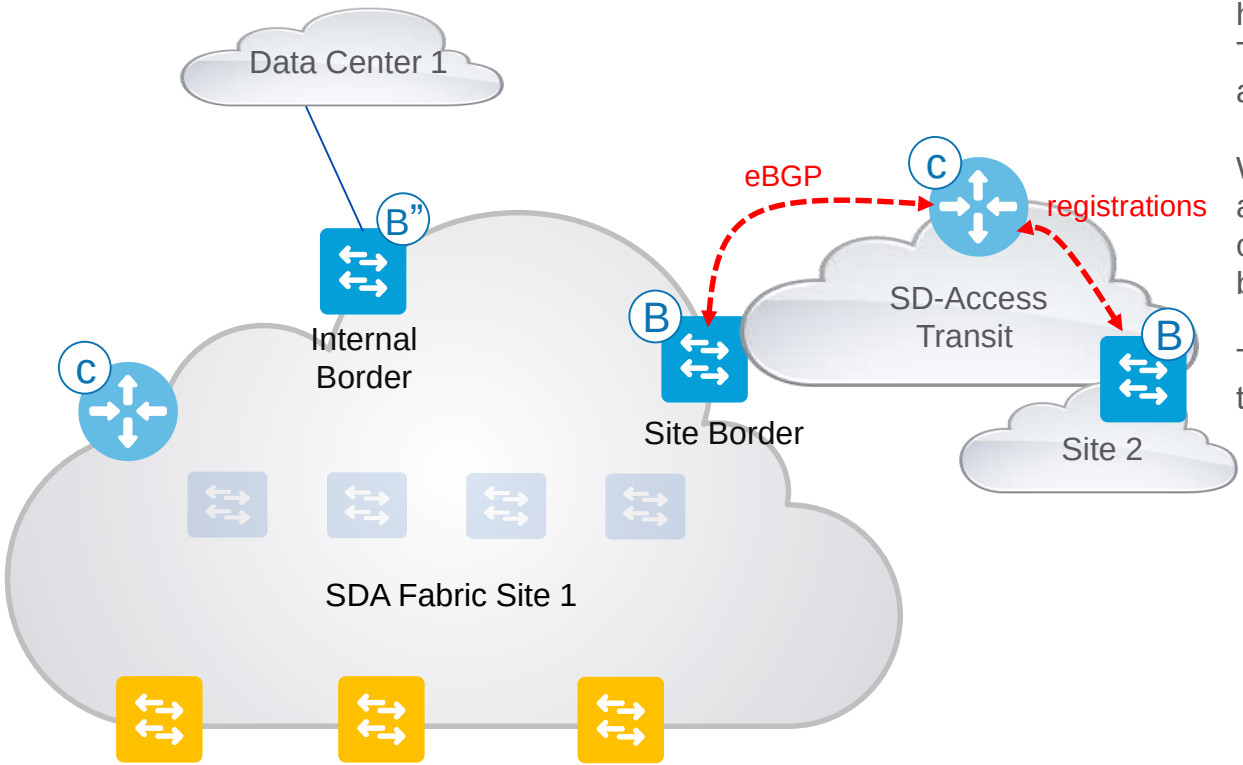
At the Transit CP we have a route-map (DENY_ALL) configured in the inbound direction for all the eBGP neighborship's from all the site borders to ensure that BGP does not accepts any routes.

The reason this is done is to ensure that the transit CP has the routes from the LISP registration only from all Site borders for its respective prefixes.

If BGP would advertise the routes than since its admin distance is 20 and in LISP we configure the admin distance to 250 BGP will be preferred. If transit CP prefers the BGP value then there is no way to distinguish routes based on community attributes anymore. This is explained in later slides.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



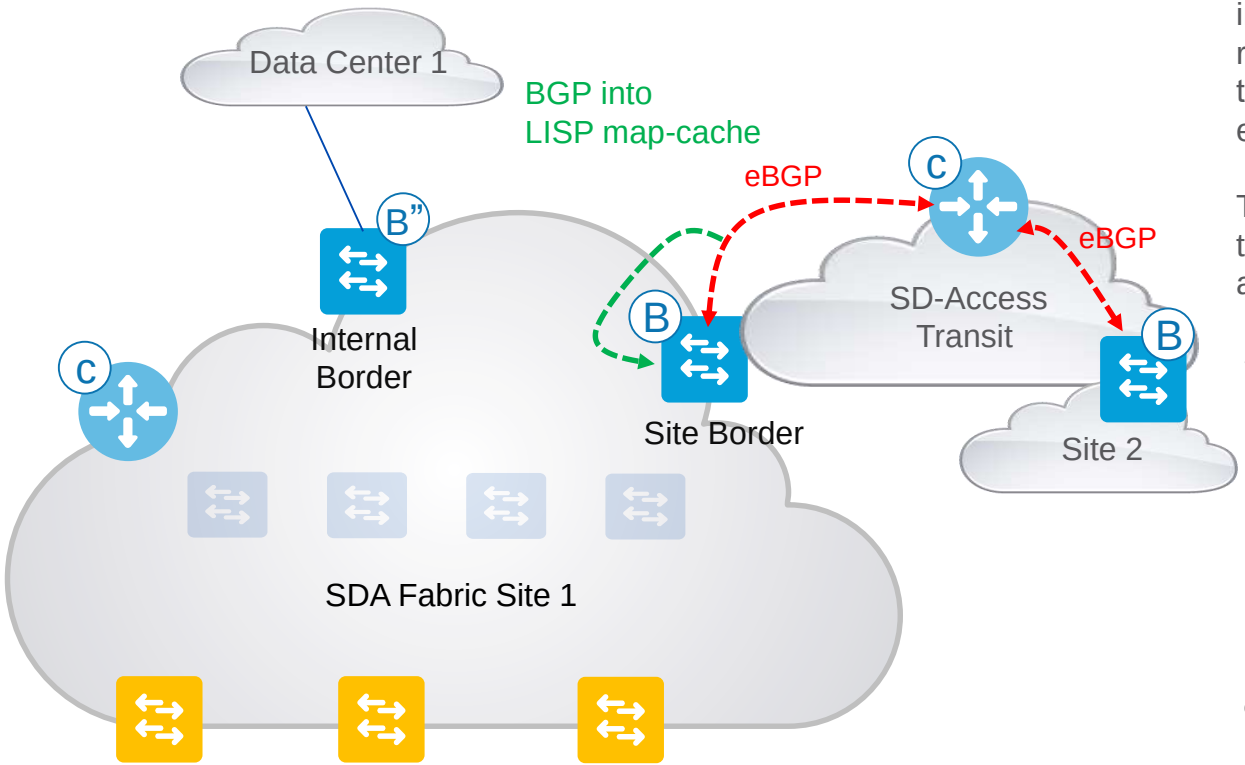
The Transit CP gets all the site prefix registrations from all sites borders and hence is has the information from all sites. This information is advertised via eBGP to all the sites borders.

When we create this neighborship we add a route-map (TAG_TRANSIT_EIDS) outbound for all the neighborship's to the border nodes in that site.

This route-map sets the community for all the routes advertised to ”65371”.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



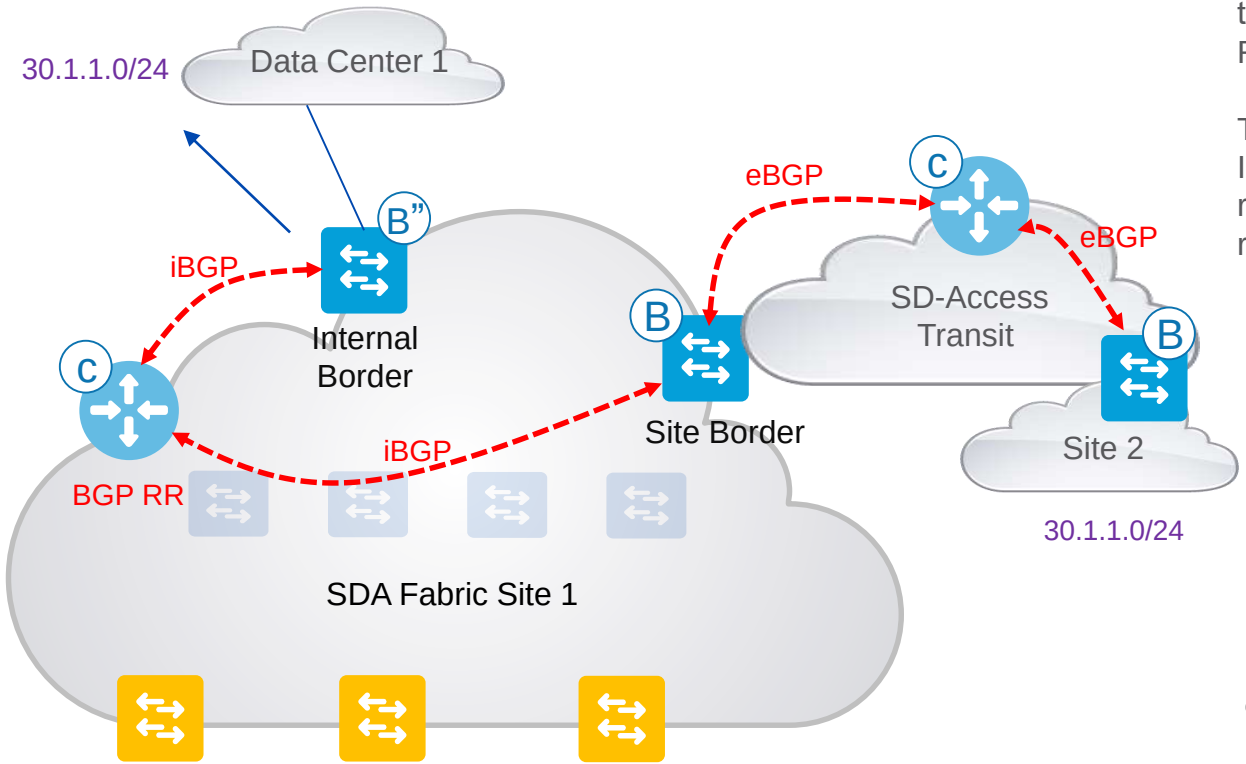
At the Site Border all the prefixes tagged with community “65371” needs to imported into LISP map-cache . This is done with a route-map (PERMIT_ALL_EIDS) where all the EID’s will be imported as map-cache entries.

These entries that are originating from the transit CP that go in the LISP map-cache are for all the subnet routes for all the sites.

Slide 38 earlier also talks about this.

SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1

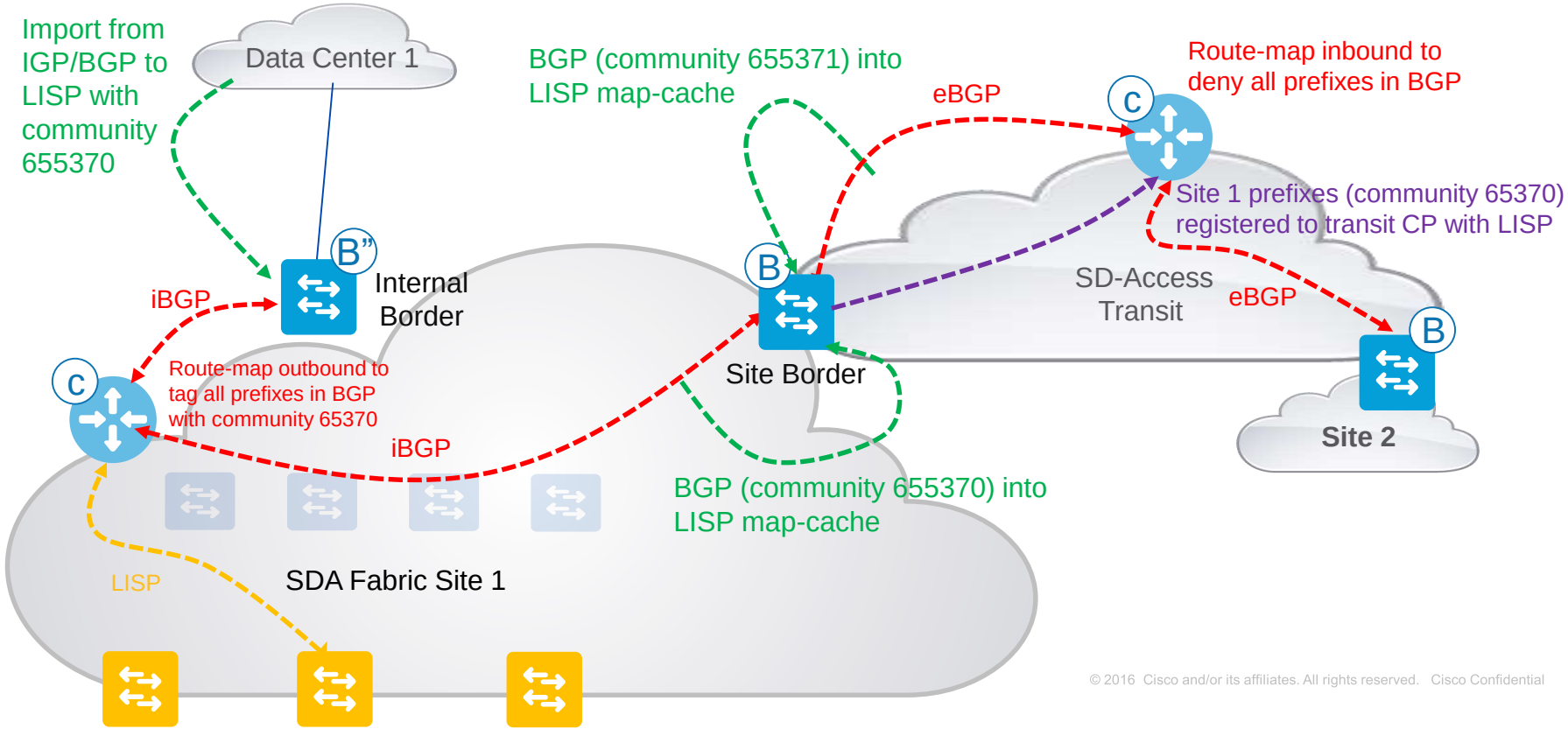


The routes coming from the Transit CP to the site border through eBGP are sent to the site CP via iBGP and since it’s a BGP RR its advertised to other border as well.

This is done for transit purposes so that Internal border can advertise other sites routes to Data center 1 so that DC 1 can reach users in site 2.

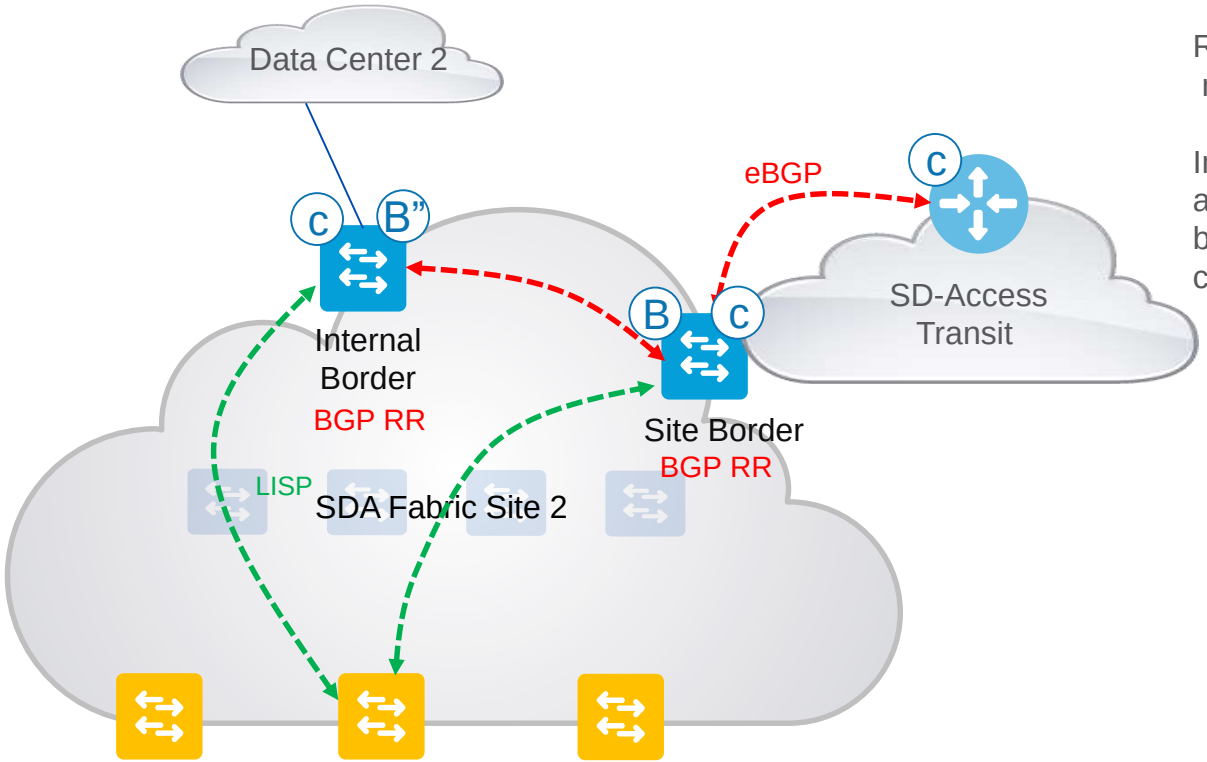
SD-Access for Distributed Campus

Non Co-Located Border and Control Plane node- Site 1



SD-Access for Distributed Campus

Co-Located Border and Control Plane node- Site 2



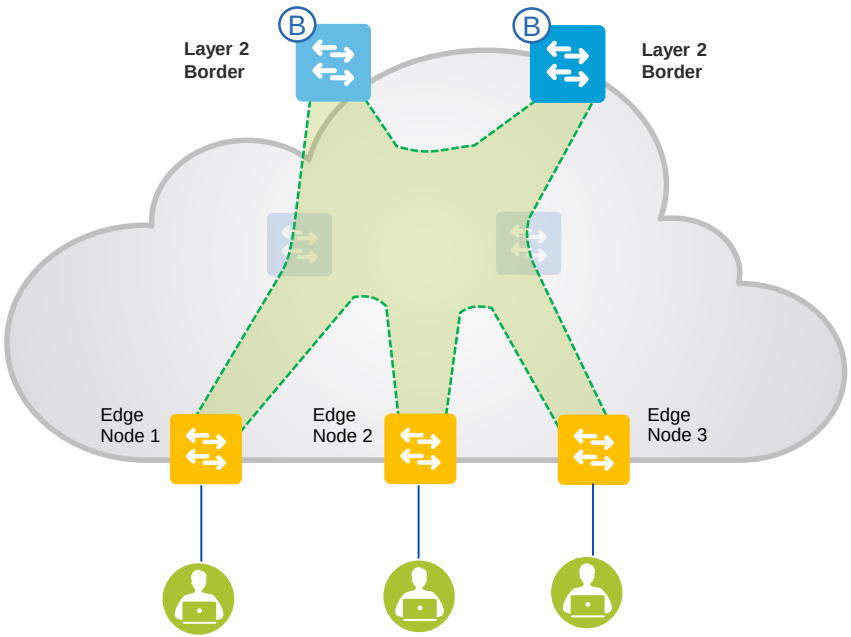
In the Co-located use case both the CP’s are route-reflector clients to each other.

Rest of the configuration models are similar to the non co-located use case.

In the non co-located use case the prefix aggregation is done at the CP node through BGP but for the co-located use case its driven via configurations on the site border.

Layer 2 Flooding

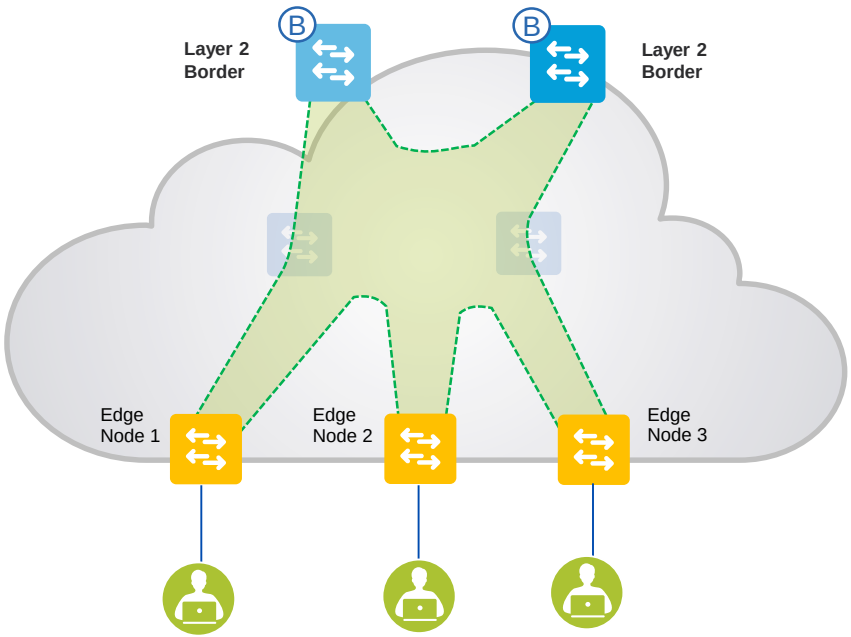
Layer 2 Flooding in SD-Access



- All Edge and layer 2 hand off enabled Border nodes are joined to a single shared “Broadcast” multicast group in the Underlay. This shared channel is where all Broadcast / Link-Local Multicast / ARP traffic will be sent between the fabric nodes.
- Incoming Broadcast / Link-Local Multicast/ARP traffic for a given VN is encapsulated in VXLAN, and then sent with {Source IP = FE node RLOC, Destination IP = Underlay Multicast Group} as the outer IP addresses.
- PIM ASM is used in the Underlay for multicast transport of the Layer 2 frames.

.

Layer 2 Flooding in SD-Access



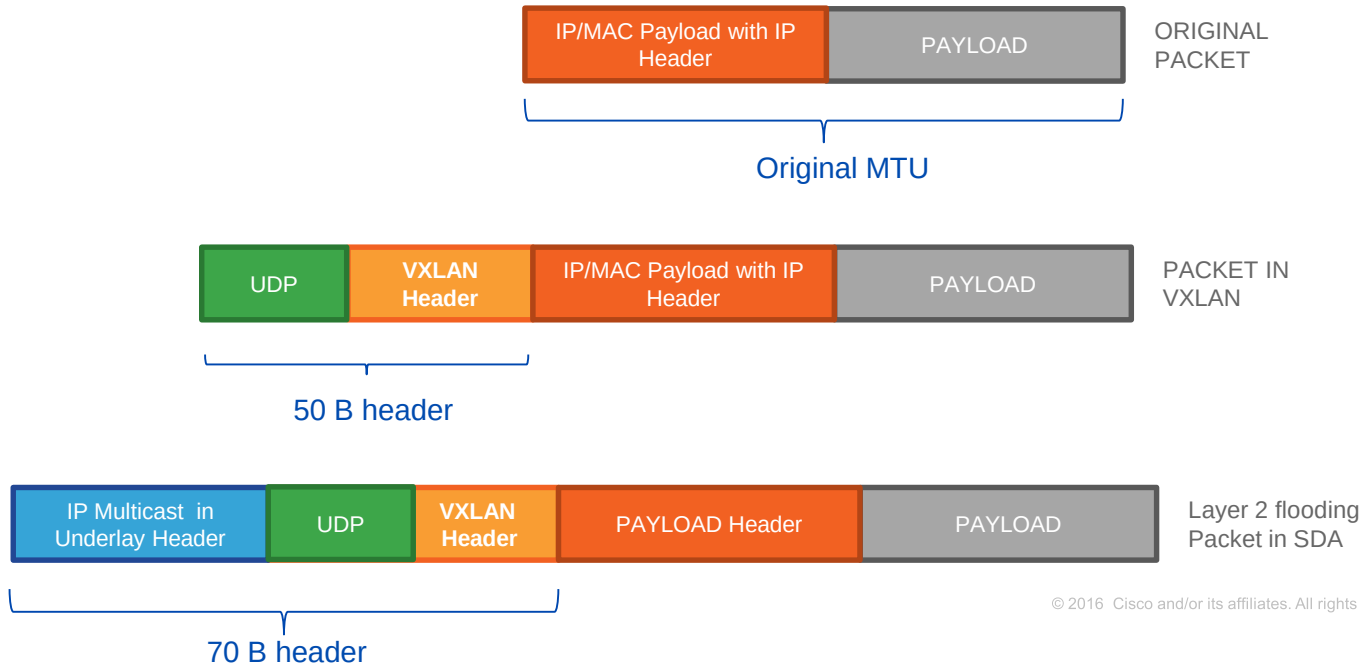
- This feature also helps with Silent Host as when ARP is flooded in fabric the silent host becomes un-silent since it will respond to the ARP reply.
- Once the ARP reply is sent from the silent host it is registered in fabric and the fabric IPDT (IP device tracking) configuration will ensure that the host remains alive in fabric.

.

Layer 2 Flooding in SD-Access

Header Format

- Total header size for Layer 2 flooding is 70 Bytes. This needs to be accounted for when designing the underlay MTU size.



Layer 2 Flooding in SD-Access

RP Selection

- When using Lan Automation in DNAC 1.2.5 the underlay is configured with PIM ASM and the “seed” devices are selected as the RP.
- The Primary Seed and the secondary seed are selected as Anycast RP’s and there is MSDP running between them.
- When incremental Lan automation is preformed to add additional edge nodes into the underlay on Day N provisioning by using distribution layer as Seed nodes the DNAC remembers the first seed device and provisions the edges nodes to use those as the “RP’s”.
- If underlay is configured manually or LAN automation was performed in a earlier DNAC version then PIM ASM with RP’s and MSDP sessions needs to be configured manually as per above.

Layer 2 Flooding in SD-Access

Forwarding

- In the fabric today we support 500 IP subnets and each subnet is mapped individually to a VLAN/Layer 2 VNI in fabric.
- Each Layer 2 VNI aka IP Subnet is mapped to an individual underlay multicast group and this multicast group is used to transmit broadcast, link local multicast and ARP frames between the fabric nodes within the Layer 2 VNI/IP Subnet.
- Every Fabric node for a given IP subnet registers with the RP on the designated multicast group and hence when one fabric nodes sends traffic on that group all other fabric nodes also receive it.

Layer 2 Flooding in SD-Access

Forwarding

- In the fabric today as noted earlier we support 500 IP subnets starting from vlan range 1021 to 1521.
- The associated multicast group range associated for The layer 2 flooding is in the range of 239.0.0.1 to 239.0.1.246.
- Vlan 1021 is assigned 239.0.0.1, vlan 1022 is assigned 239.0.0.2, vlan 1023 is assigned 239.0.0.3 and so on till vlan 1521 which is assigned 239.0.1.246.

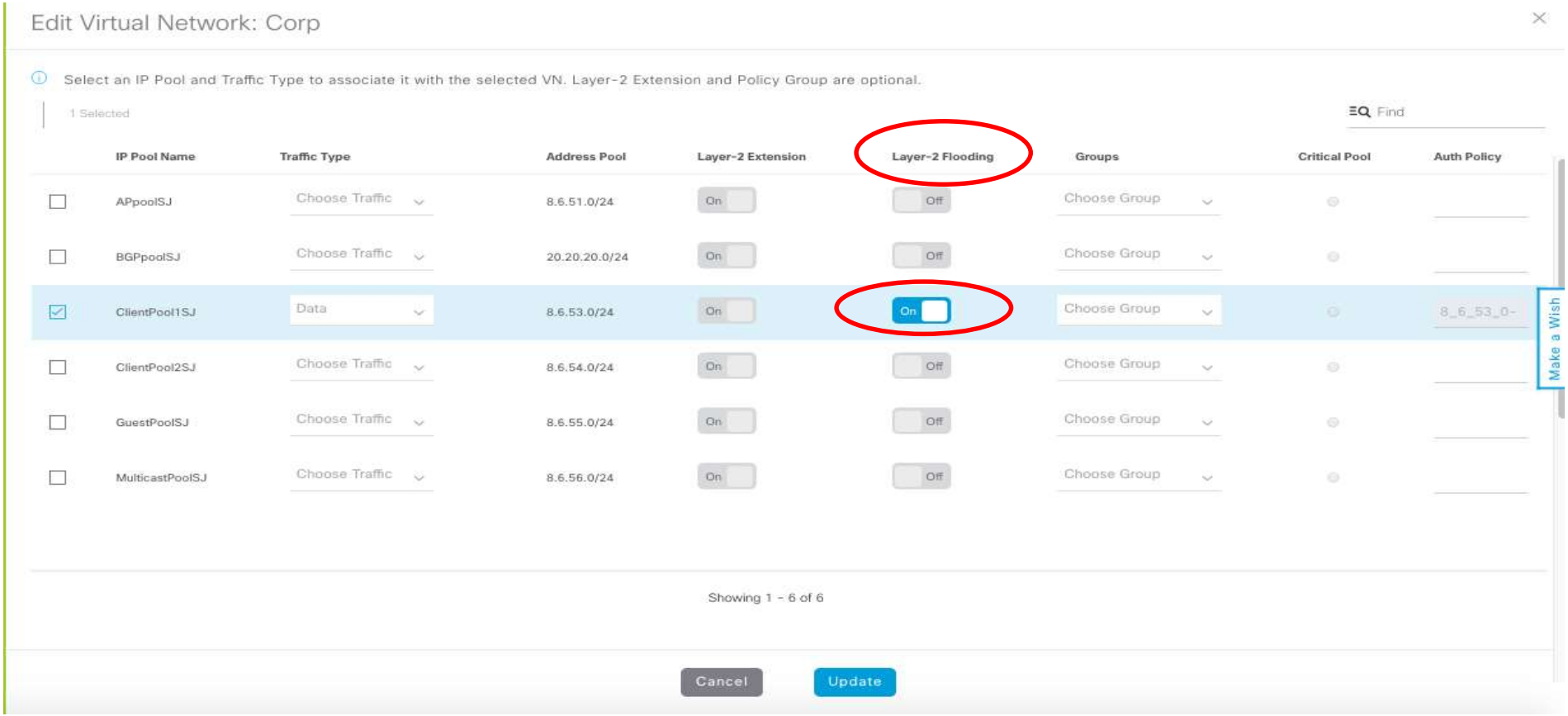
Layer 2 Flooding in SD-Access

Configuration

- The Layer 2 flooding is enabled on a per IP Subnet/vlan basis in the host on-boarding section.
- When the knob is enabled all the Fabric edge nodes which have the IP subnet configured will be mapped to the multicast group in the underlay as well the Layer 2 hand off border which maps the internal fabric vlan to the external (discussed in later slides in the layer 2 hand off for migration section).
- Once the knob is turned on immediately all Broadcast / Link-Local Multicast / ARP traffic is flooded on that respective multicast group for that given IP subnet.

Layer 2 Flooding in SD-Access

Configuration



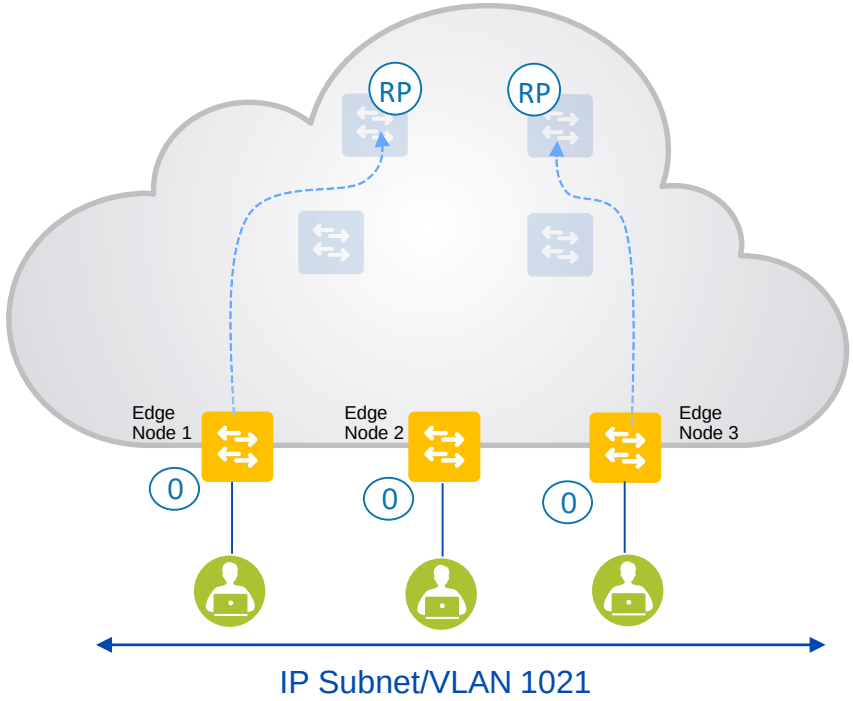
Layer 2 Flooding in SD-Access

Support Matrix

SD-Access Fabric Role	Device Supported	Software Release
Edge	C3K, C9K	16.9.1s
Layer 2 Hand off @ Border	C9K,C3K C6K	16.9.1s 15.5(1) SY2

Layer 2 Flooding in SD-Access

Forwarding

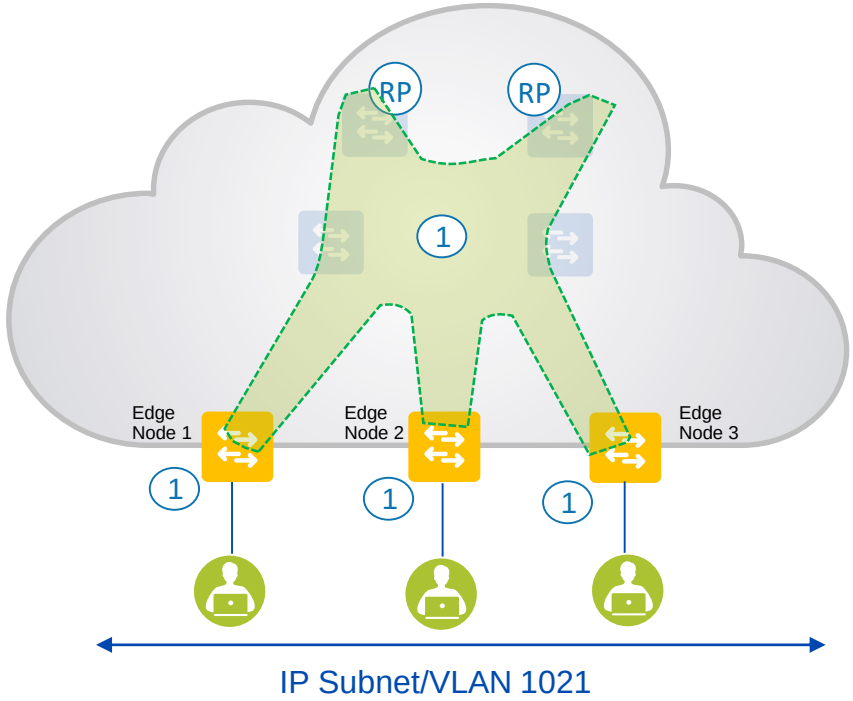


0 A Given IP Subnet is mapped to a dedicated multicast address in the Underlay. The group is a ASM group and hence all the PIM joins are sent to the RP in the underlay.

```
instance-id 8188
  remote-rloc-probe on-route-change
  service ethernet
    eid-table vlan 1021
    broadcast-underlay 239.0.0.1
    database-mapping mac locator-set xxx
  exit-service-ethernet
exit-instance-id
```

Layer 2 Flooding in SD-Access

Forwarding

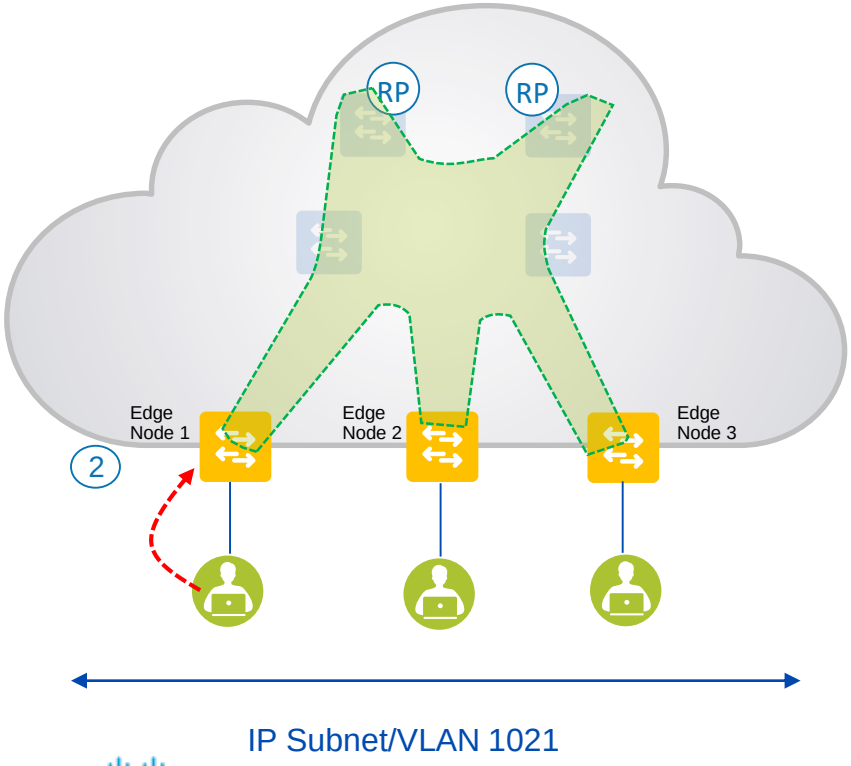


1 Since all the Fabric nodes that have the IP subnet configured have sent the PIM joins on their respective multicast group , a multicast tree is pre built for that particular IP subnet.

The traffic is flooded on this pre built multicast tree.

Layer 2 Flooding in SD-Access

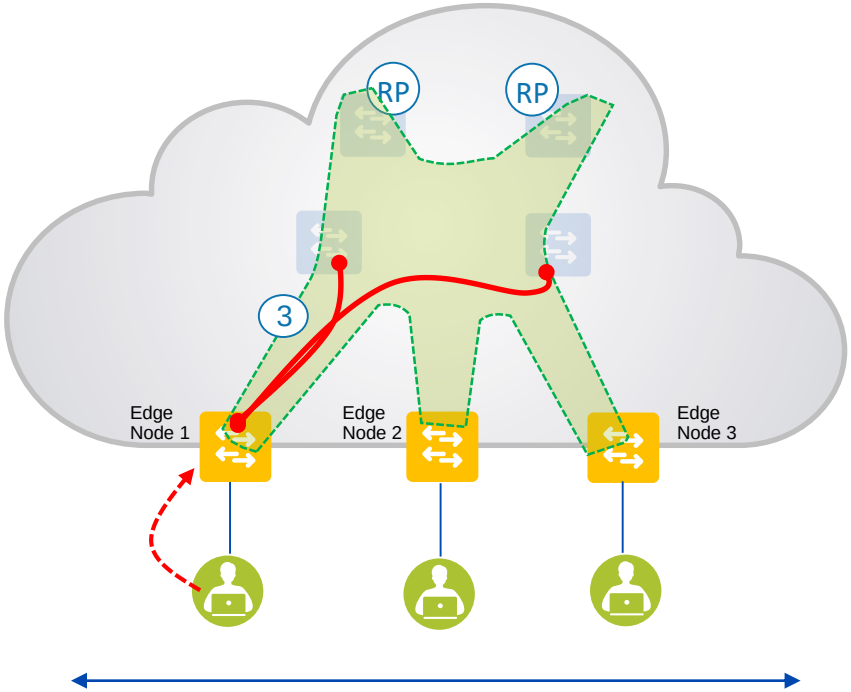
Forwarding



2 ARP/Broadcast/Link Local Multicast traffic is coming from the end host to the fabric edge node.

Layer 2 Flooding in SD-Access

Forwarding



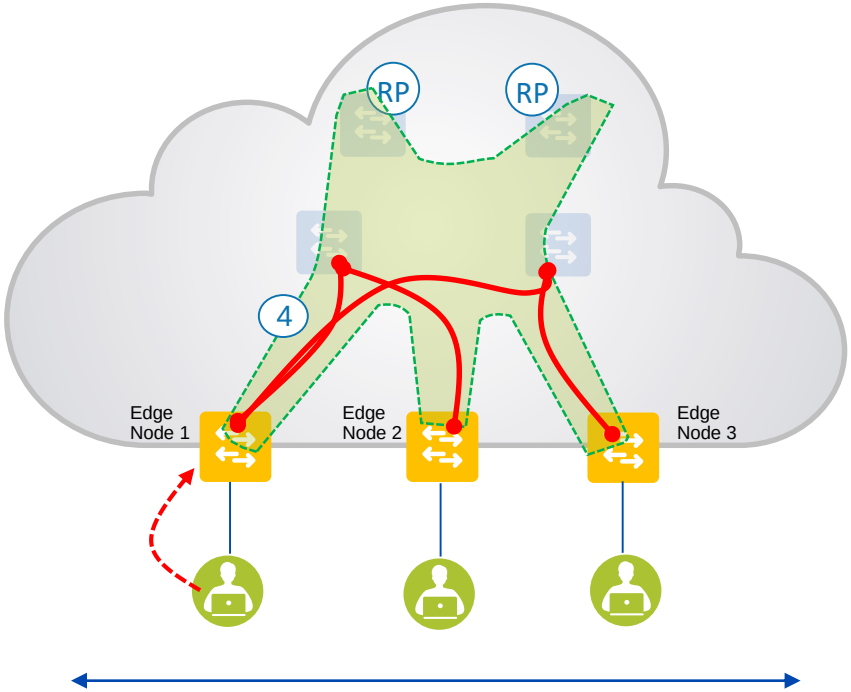
3 The fabric edge node intercepts the traffic and is sent over the dedicated multicast group in the underlay.

The Underlay based on normal multicast functionality is responsible for replicating the traffic as needed.

The Source tree failover also happens based on regular multicast working.

Layer 2 Flooding in SD-Access

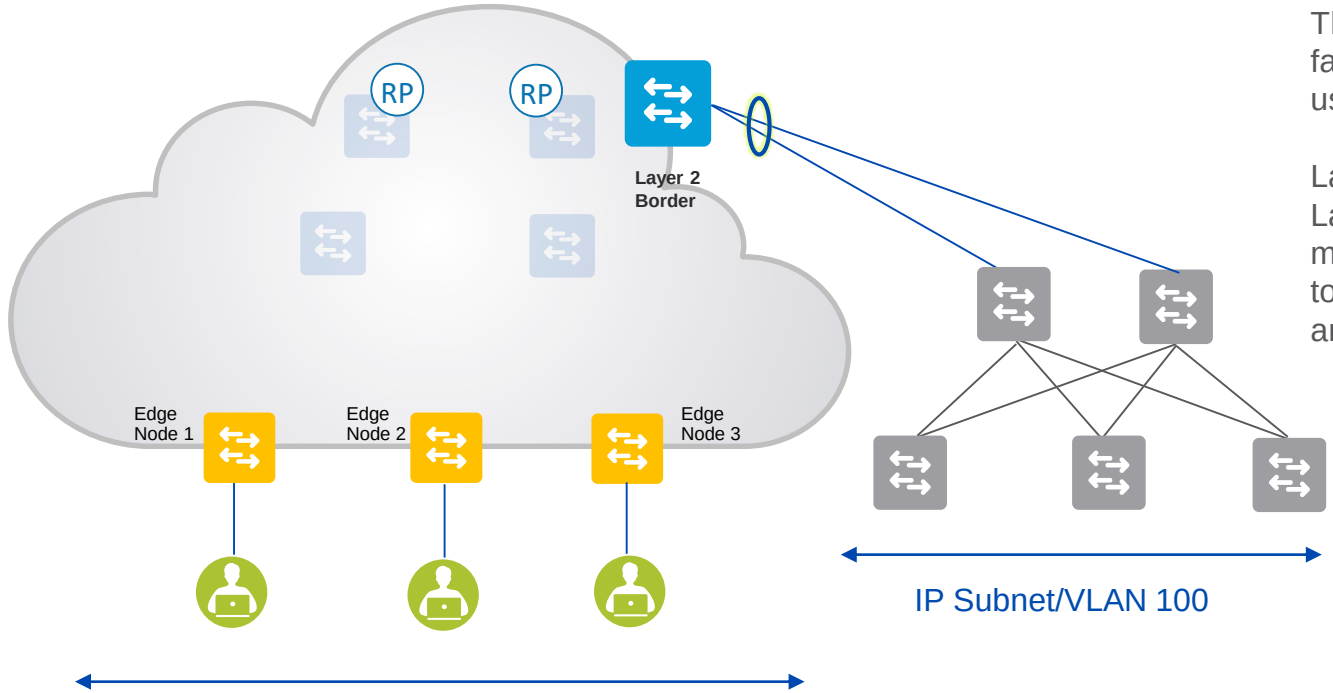
Forwarding



4 All the FE nodes get the traffic sent by edge node 1.

Layer 2 Flooding in SD-Access

Forwarding



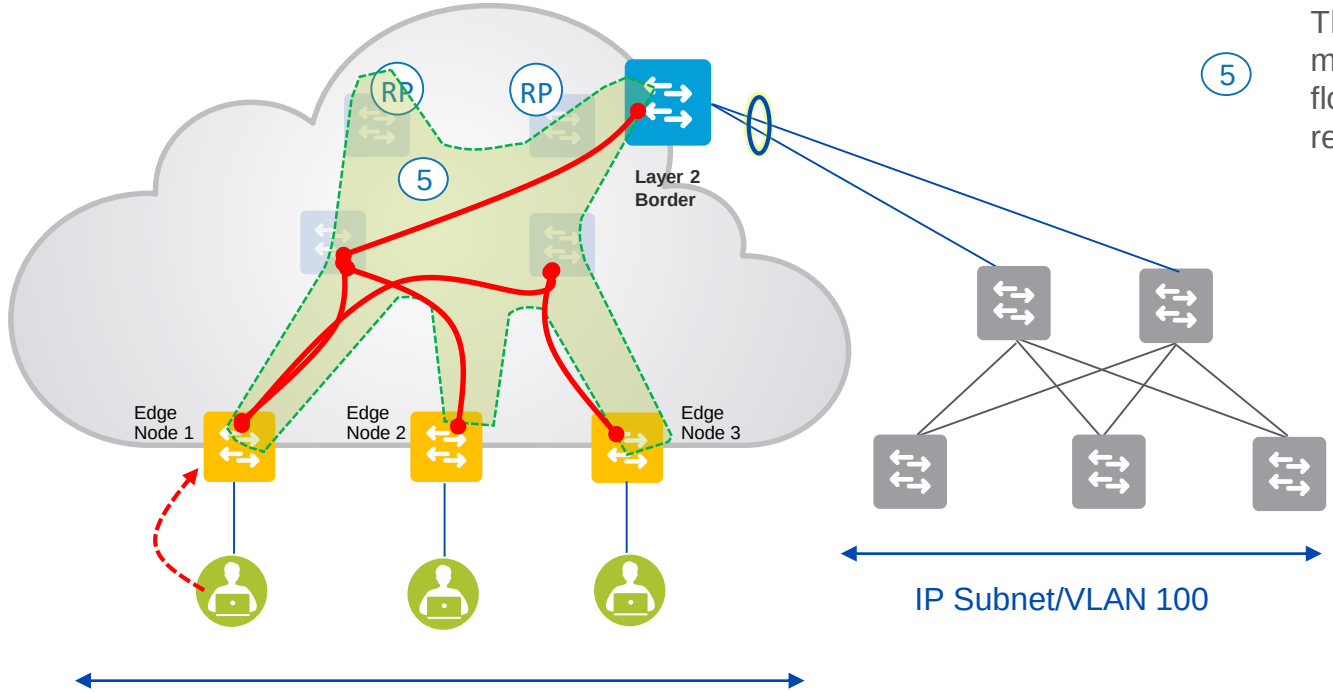
The Layer 2 Border maps vlan 1021 in fabric to vlan 100 in non fabric. They use the same IP subnet.

Layer 2 flooding ensures that the Layer 2 Border has also the same multicast group configured in Underlay to ensure that traffic across vlan 1021 and vlan 100 is flooded.

The Layer 2 Border functionality is explained in the next section.

Layer 2 Flooding in SD-Access

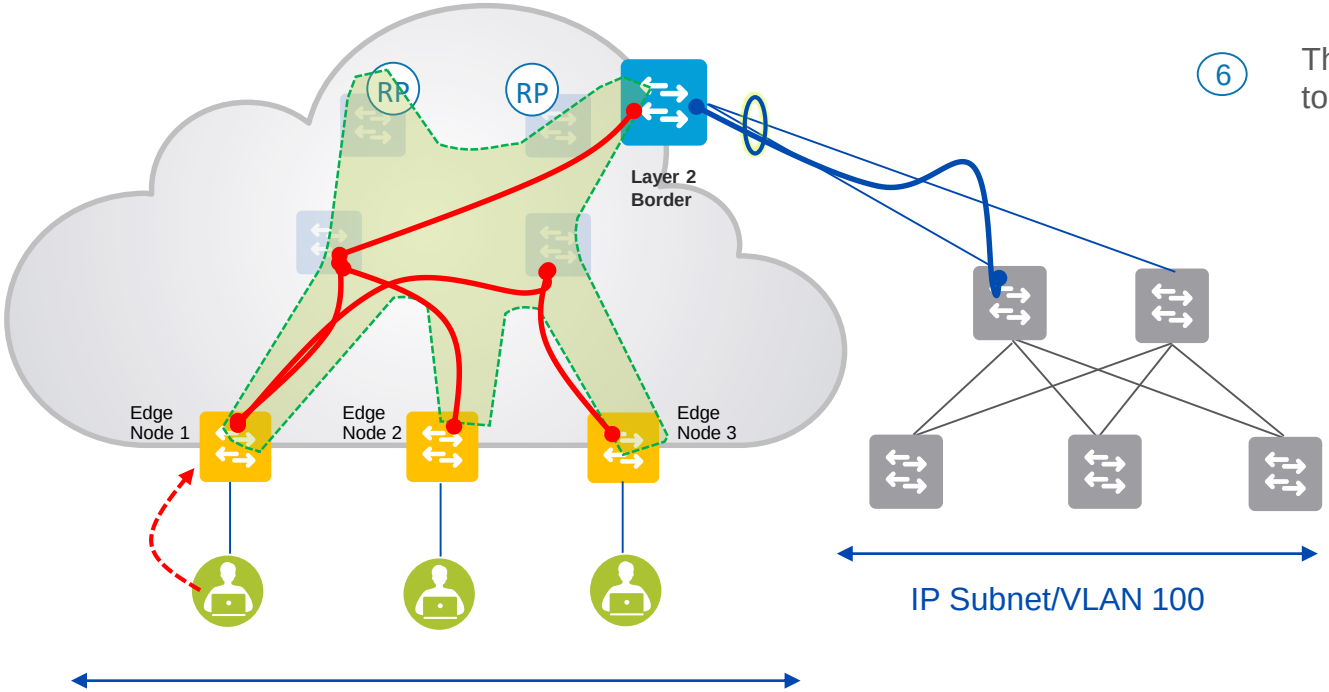
Forwarding



The Layer 2 Border is also part of the multicast traffic and hence traffic is flooded in the multicast group it reaches the layer 2 border as well.

Layer 2 Flooding in SD-Access

Forwarding

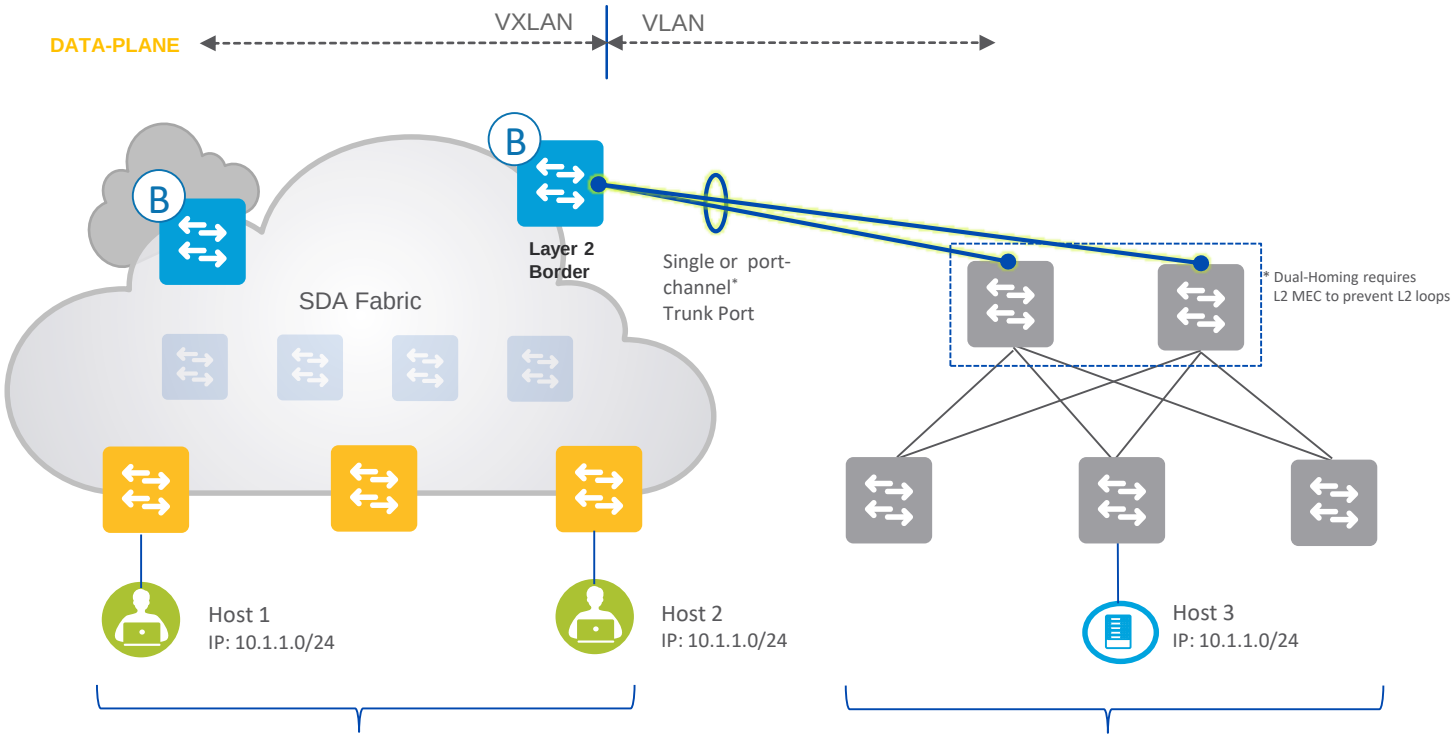


6

The Layer 2 Border floods on vlan 100 to the external world.

Layer 2 Hand off for Migration

Layer 2 Hand off for Migration in SD-Access



Layer 2 Hand off for Migration in SD-Access

Forwarding

- The layer 2 Border maps vlan 1024 in fabric to vlan 300 in non fabric. Both the vlan's have the same IP subnet which helps in migration.
- The layer 2 Border will have the same configuration as the edge nodes expect that vlan 1021 is replaced by vlan 300.
- The SVI for the vlan 300 will be hosted on the layer 2 border by the DNAC configuration. If the SVI exists for that vlan in any other device then that has to deleted and be moved to the layer 2 border.
- All the end points from the non fabric side is registered to the CP node by the Layer 2 Border.

The vlan numbers are just an example to understand the concept

Layer 2 Hand off for Migration in SD-Access

Forwarding

- **Fabric Edge:**

```
service ethernet
 encapsulation vxlan
 database-mapping limit dynamic 5000
 itr map-resolver x.x.x.x
 etr map-server x.x.x.x key 7 09594D00
 etr map-server x.x.x.x proxy-reply
exit-service-ethernet
!
instance-id 8188
  remote-rloc-probe on-route-change
  service ethernet
    eid-table vlan 1024
    broadcast-underlay 239.0.0.1
    database-mapping mac locator-set xxx
  exit-service-ethernet
exit-instance-id
!
interface Vlan1024
 description Configured from apic-em
 mac-address 0000.0c9f.f45c
 vrf forwarding Corp
 ip address 8.6.53.0 255.255.255.0
 ip helper-address 10.121.128.101
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 8_6_53_0-Corp
```

- **Layer 2 Border:**

```
service ethernet
 encapsulation vxlan
 database-mapping limit dynamic 5000
 itr map-resolver x.x.x.x
 etr map-server x.x.x.x key 7 09594D00
 etr map-server x.x.x.x proxy-reply
exit-service-ethernet
!
instance-id 8188
  remote-rloc-probe on-route-change
  service ethernet
    eid-table vlan 300
    broadcast-underlay 239.0.0.1
    database-mapping mac locator-set xxx
  exit-service-ethernet
exit-instance-id
!
interface Vlan300
 description Configured from apic-em
 mac-address 0000.0c9f.f45c
 vrf forwarding Corp
 ip address 8.6.53.0 255.255.255.0
 ip helper-address 10.121.128.101
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 8_6_53_0-Corp
```

Layer 2 Hand off for Migration in SD-Access

Caveats

- The layer 2 Border supports only 4K host registrations across all the external vlan's. What this means is that when Layer 2 hand off for migration is configured on a border node for vlan 10 , 20 and 300 then across that vlan's we support only 4K end points connected to it.

- The Layer 2 Border does not support any multi-homing which means that we can connect the non fabric network to an access port or a trunk port but to only one device on the fabric side. The non fabric side can be in a stack wise virtual(SVL) configuration but on fabric side its one device only. The device can be a regular stack(not SVL).

Layer 2 Hand off for Migration in SD-Access

Support Matrix

SD-Access Border Node	Supported	Software Release
C3K	YES	16.9.1s
C9K	YES	16.9.1s
C6K	NO	N/A
N7K	NO	N/A
ASR1K/ISR4K	NO	N/A

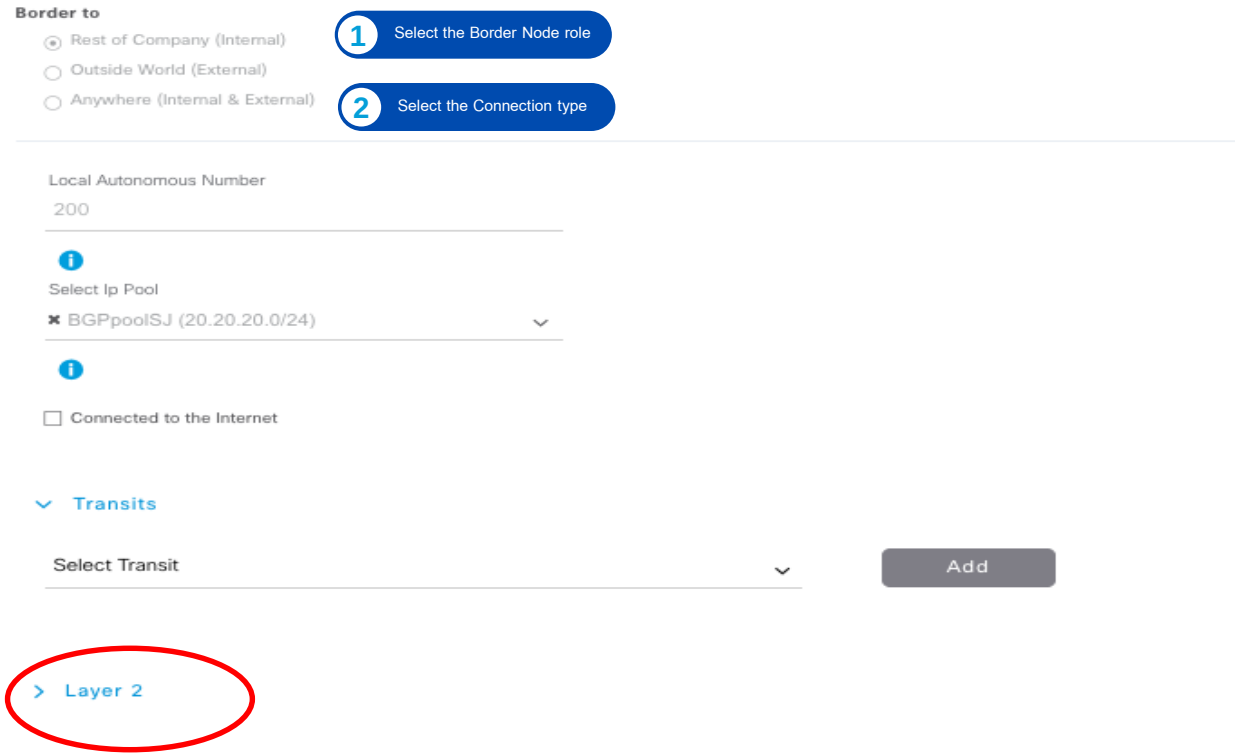
Layer 2 Hand off for Migration in SD-Access

Scale

Fabric Constructs	Catalyst 3850	Catalyst 9300	Catalyst 9400	Catalyst 9500	Catalyst 9500H
Local End Points/Hosts	4K	4K	4K	4K	4K

Layer 2 Hand off for Migration in SD-Access

Configuration



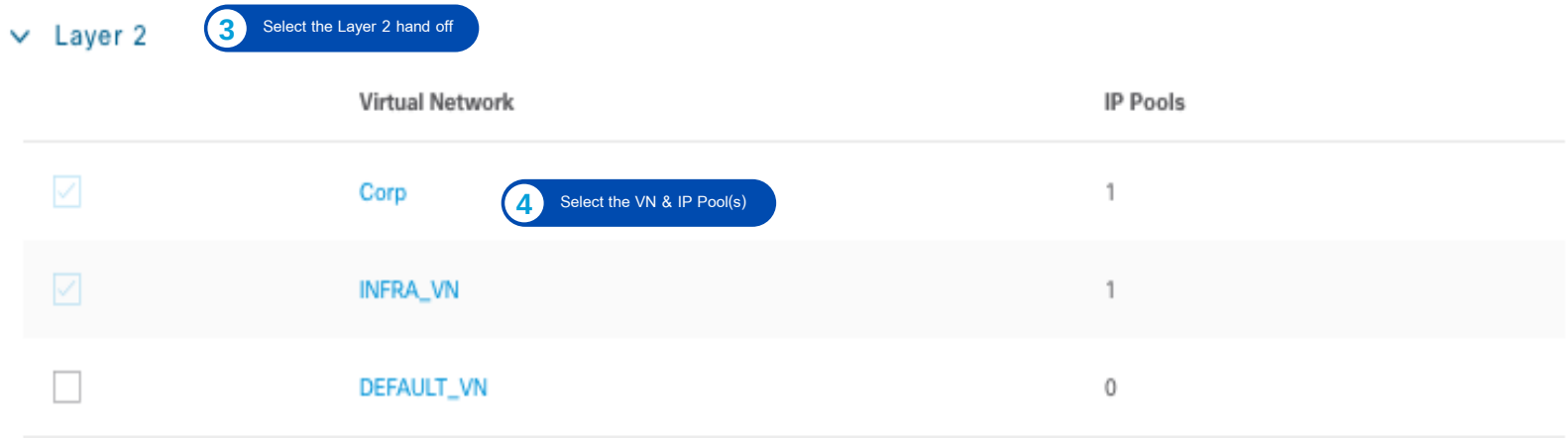
Layer 2 Hand off for Migration in SD-Access

Configuration

- The Type of Border node that needs to be picked depends on what the border node connects to.
- Slide 32 explains what type of border node needs to be selected for a respective connectivity type.

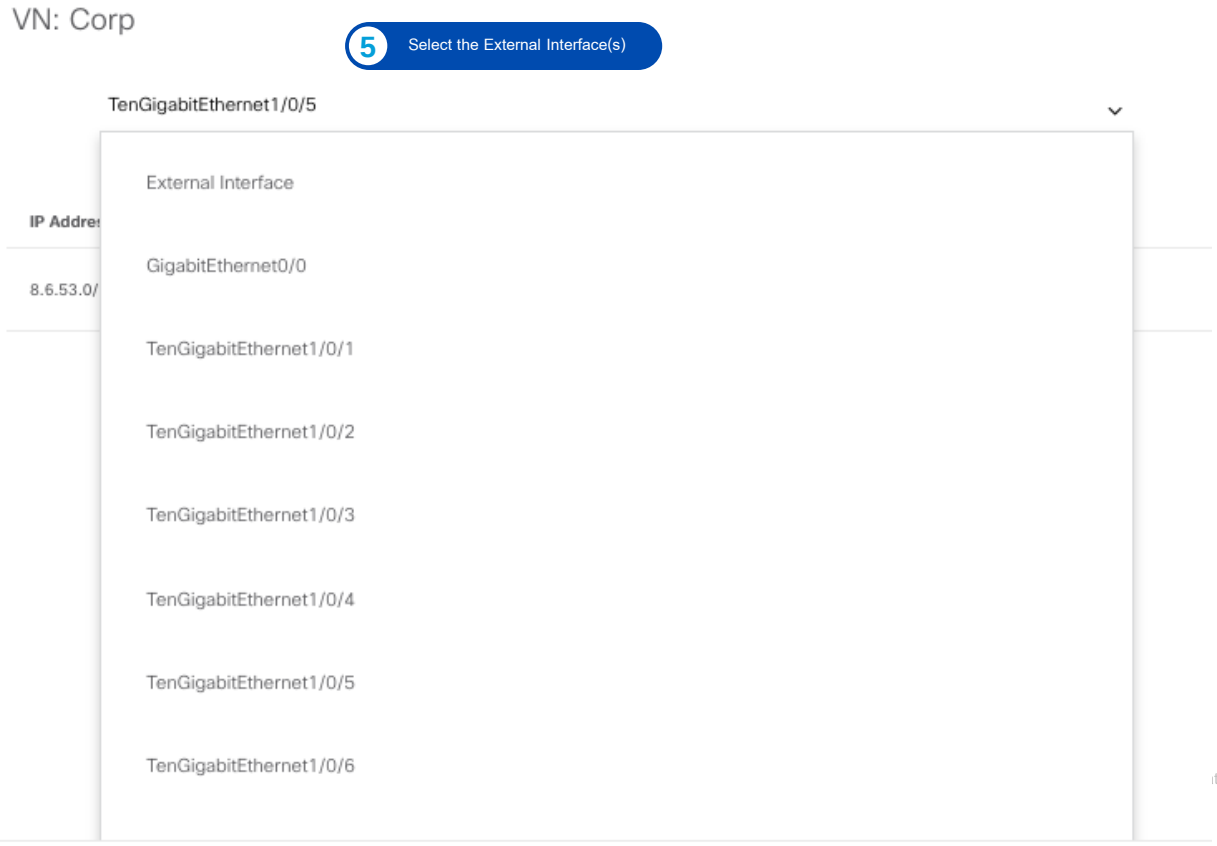
Layer 2 Hand off for Migration in SD-Access

Configuration



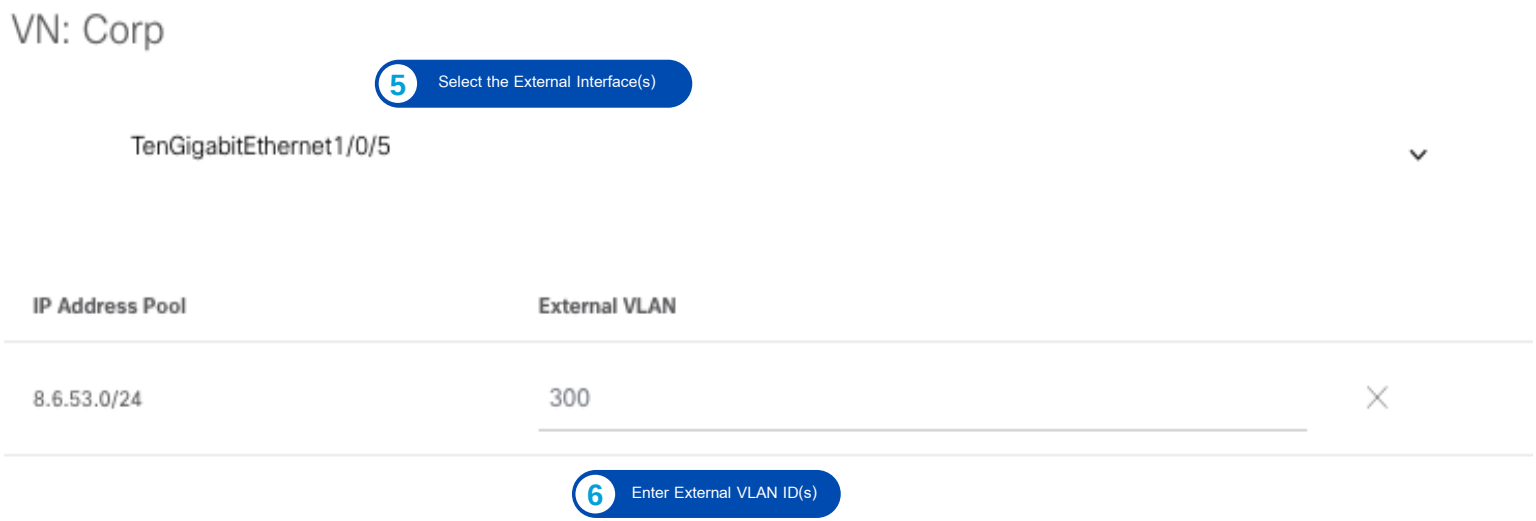
Layer 2 Hand off for Migration in SD-Access

Configuration



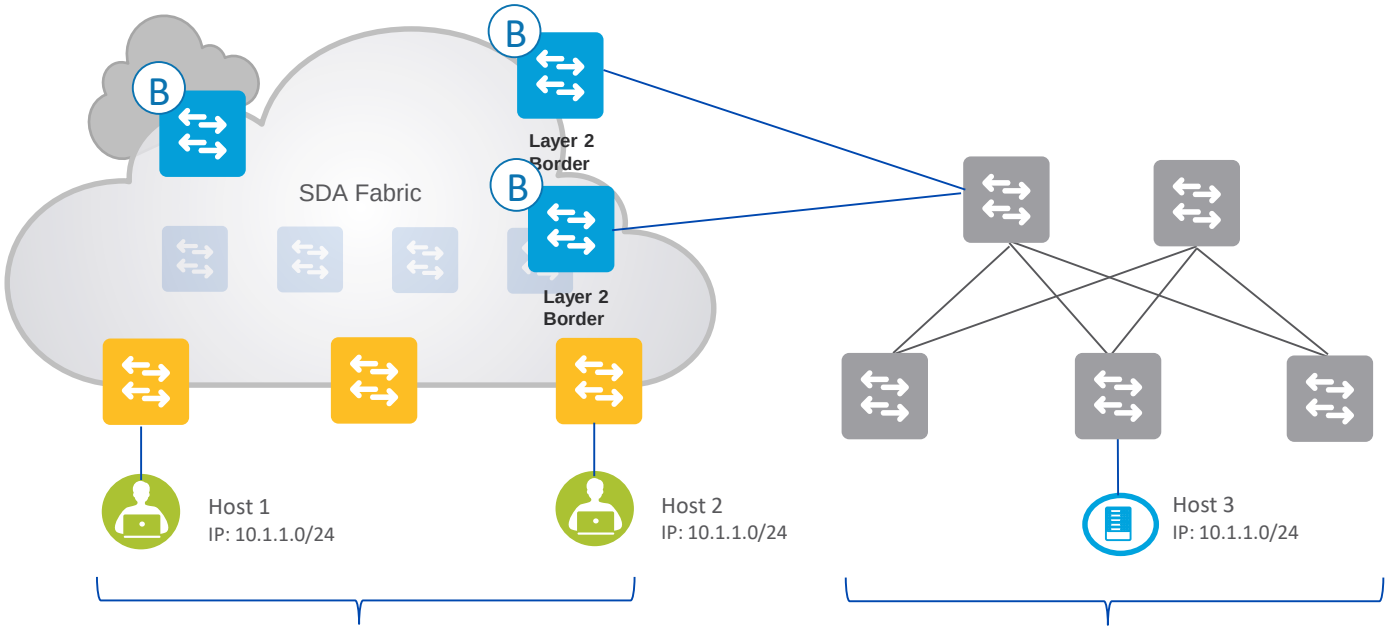
Layer 2 Hand off for Migration in SD-Access

Configuration



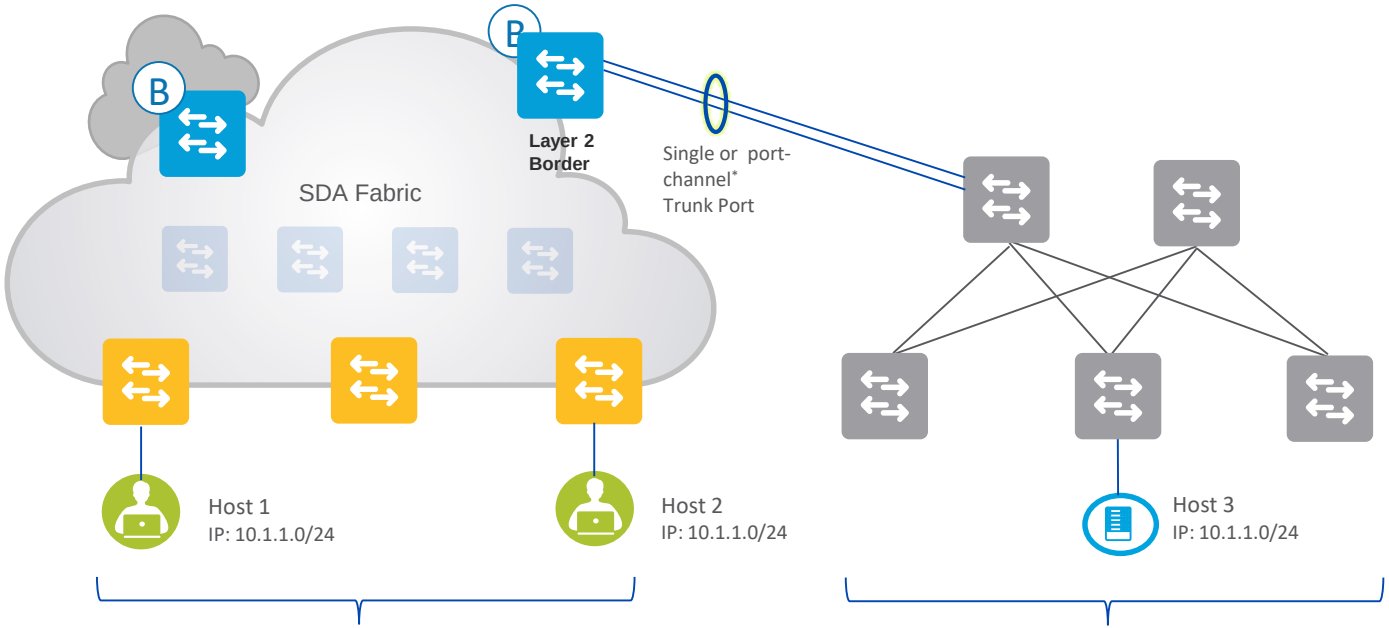
Layer 2 Hand off for Migration in SD-Access

Deployment Models – **Not supported**



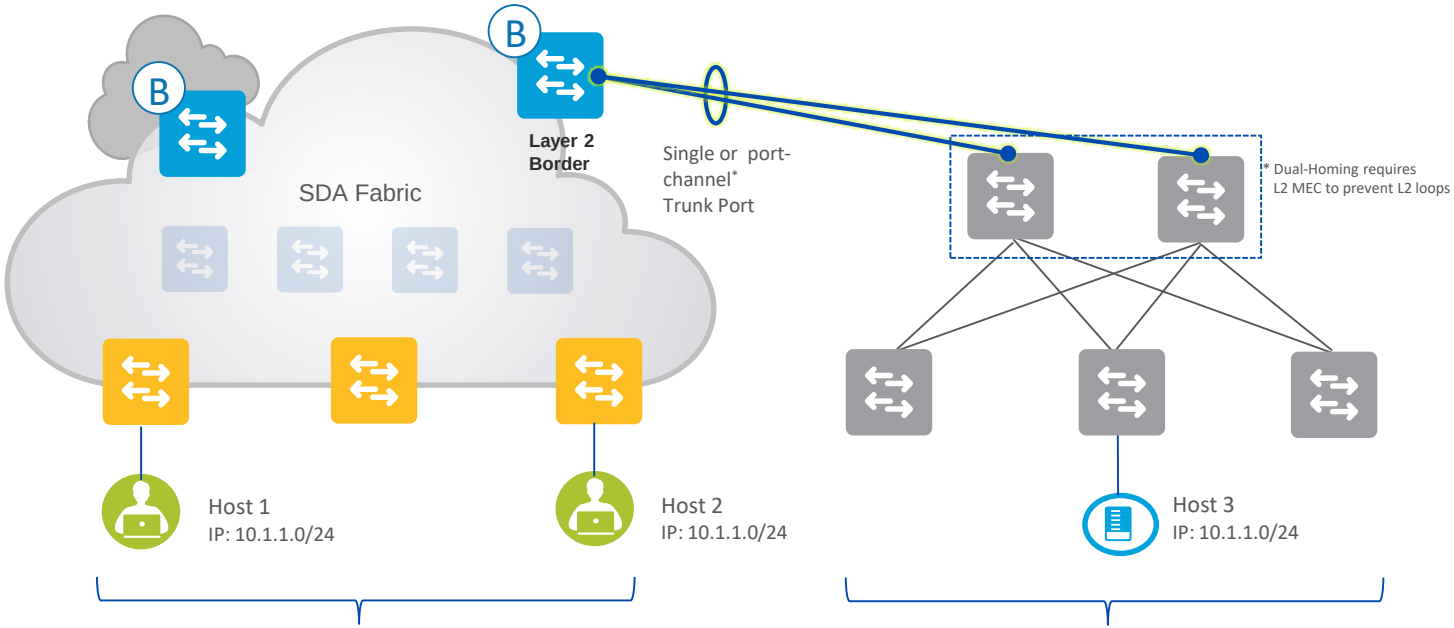
Layer 2 Hand off for Migration in SD-Access

Deployment Models – **Supported**



Layer 2 Hand off for Migration in SD-Access

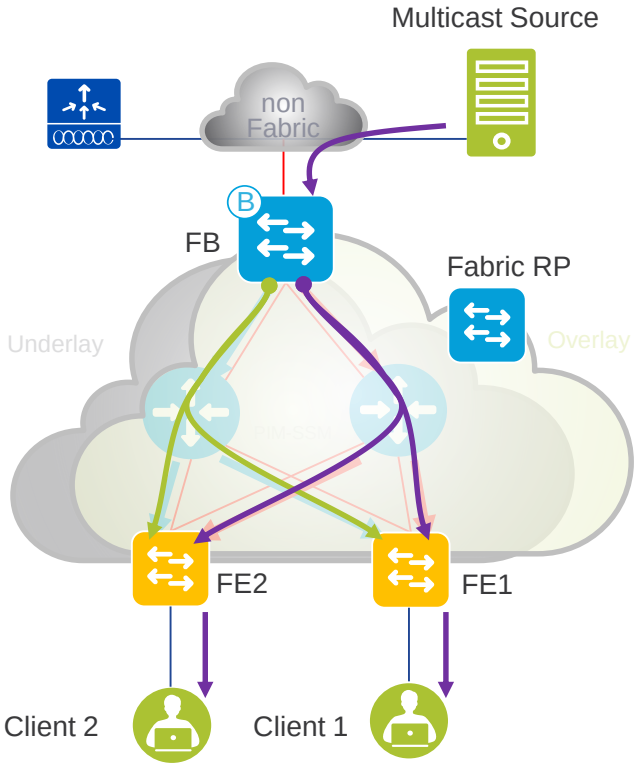
Deployment Models – **Supported**



Native Multicast

Native Multicast in SD-Access

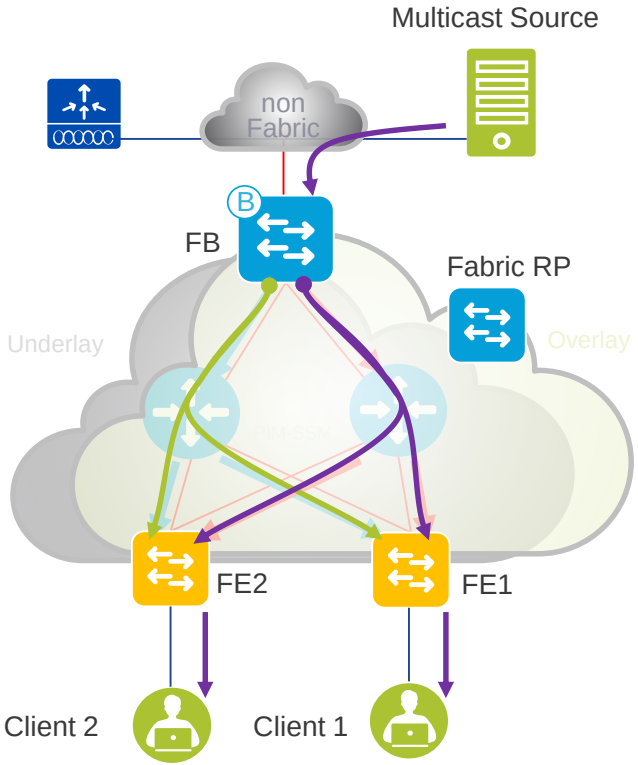
* DNAC 1.2.6



- All existing Multicast Overlay behavior is the same
- PIM ASM and SSM can be used in the Overlay as before.
- Each multicast group in the Overlay is mapped to a corresponding (PIM SSM) Multicast Underlay Group
- Multicast distribution (replication) occurs natively within the Underlay network (e.g. intermediate nodes)
- Incoming Multicast traffic for a given VN is encapsulated in VXLAN, and then sent with {Source IP = FE node RLOC, Destination IP = Underlay Multicast Group} as the outer IP addresses.
- PIM SSM is used in the underlay for multicast transport

Native Multicast in SD-Access

* DNAC 1.2.6

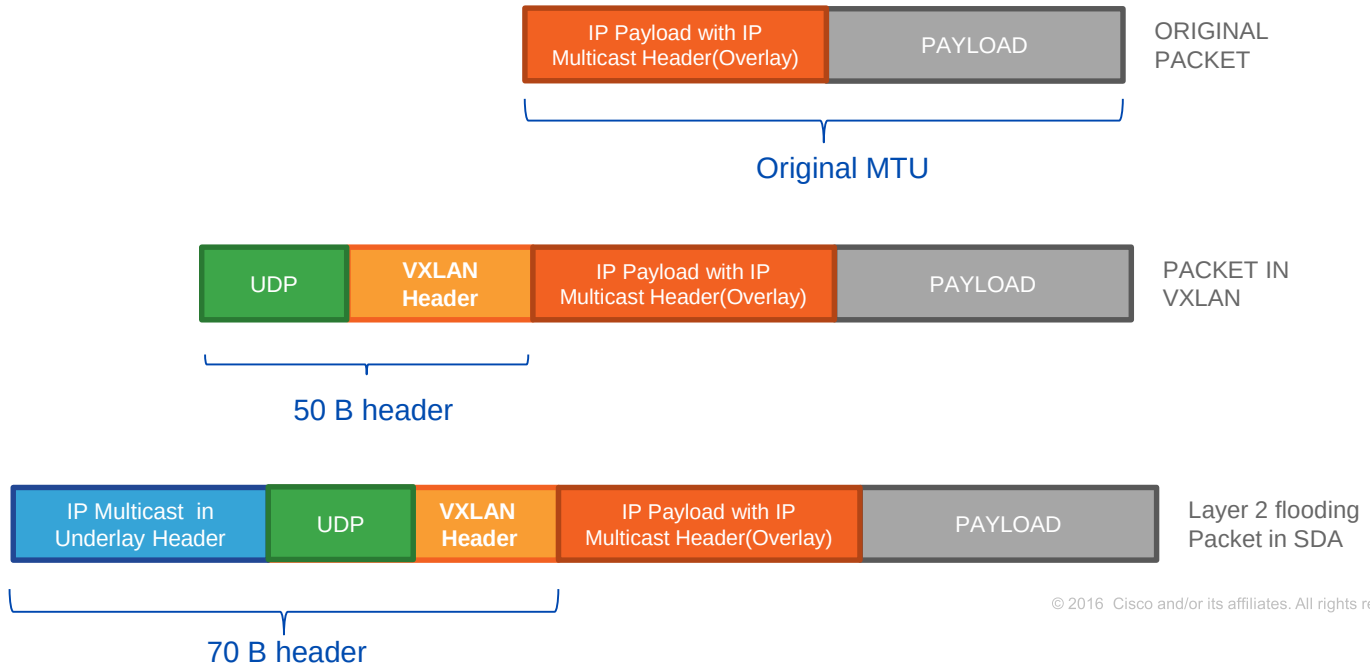


- In given fabric site we can either have head end replication or native multicast , meaning this is not a per device configuration rather a per site configuration.
- Since we are using SSM in the underlay all the PIM joins will need a source address unlike when using ASM. To achieve this the source address used for all the joins is the RLOC address of the fabric node which is Loopback 0.
- Hence the state created in the Underlay will include (S, G) entries for all the groups , in essence (RLOC,G) entries.

Native Multicast in SD-Access

Header Format

- Total header size for Native Multicast is 70 Bytes. This needs to be accounted for when designing the underlay MTU size.



Native Multicast in SD-Access

Forwarding

- Native multicast uses SSM in the underlay and hence no RP's are needed. The SSM group used in the underlay is the 232.0.0.x range.
- If Lan automation is used with DNAC 1.2.5 then the necessary configuration in the underlay is performed.
- If Lan automation was done with earlier DNAC version or manually then above configuration (PIM SSM with 232.0.x group range) must be done manually to support native multicast in fabric.

Native Multicast in SD-Access

Forwarding

- With Native multicast the control plane messaging in the Overlay does not change where we use a combination of LISP and PIM to ensure that the PIM joins from source and receivers make it across the network.
    - Above is documented clearly in the Multicast TDM deck.
- Depending on whether PIM ASM or SSM used in overlay we make use of a RP to ensure control plane messaging is taken care of in the overlay.
- When head end replication for multicast is used then the data plane uses the overlay where the fabric node closest to source will replicate or create an unicast stream for each receiver fabric node. When switched over to native multicast the data plane does not use the overlay but uses the designated SSM multicast group in the underlay and the underlay replicates the traffic.

Native Multicast in SD-Access

Forwarding

- In fabric today we support 1000 multicast groups across all configured VN's in the Overlay and these1000 groups will be mapped to 1000 groups in the underlay when native multicast is used.
- The underlay groups range starts with 232.0.0.1 and goes to 100 groups from that. So the group ranges starts from 232.0.0.1 and ends with 232.0.3.232 .
- Even if the Overlay has the same group range for the multicast traffic there are no issues as the Overlay group are in a VRF and underlay group is in Global routing table.
- The Overlay to Underlay group mapping is based on the same algorithm across all supported devices and hence there will be no mis-match of mapping.

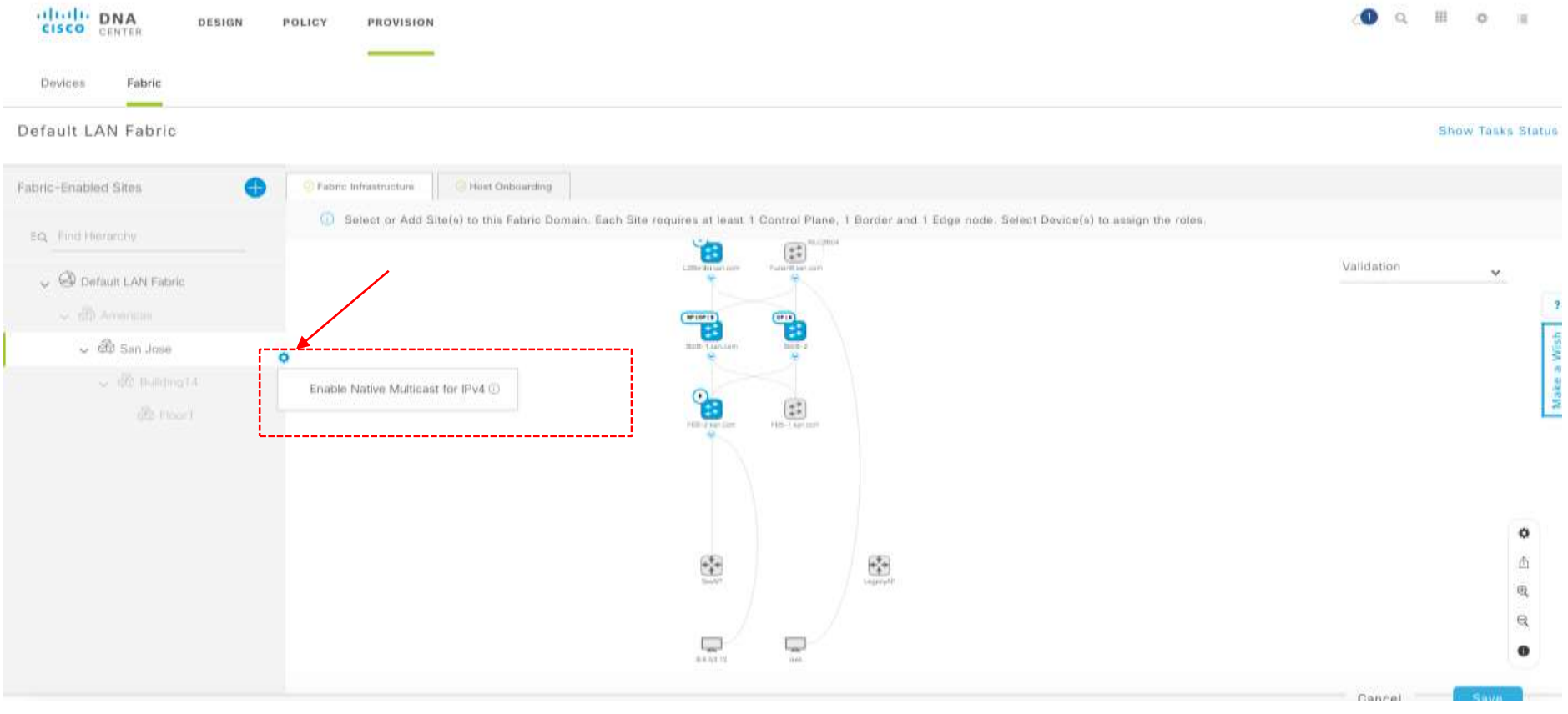
Native Multicast in SD-Access

Configuration

- The Multicast configuration for a given fabric site is done as earlier by starting with an RP and then picking the needed VN and an IP subnet. That does not change with native multicast.
- A knob is provided at a fabric site level to enable or disable native multicast.
- Once the knob is turned on immediately the traffic is moved over from head end replication to native multicast.
- This will incur a small outage in multicast traffic and hence recommended to do in a maintenance window.

Native Multicast in SD-Access

Configuration



Native Multicast in SD-Access

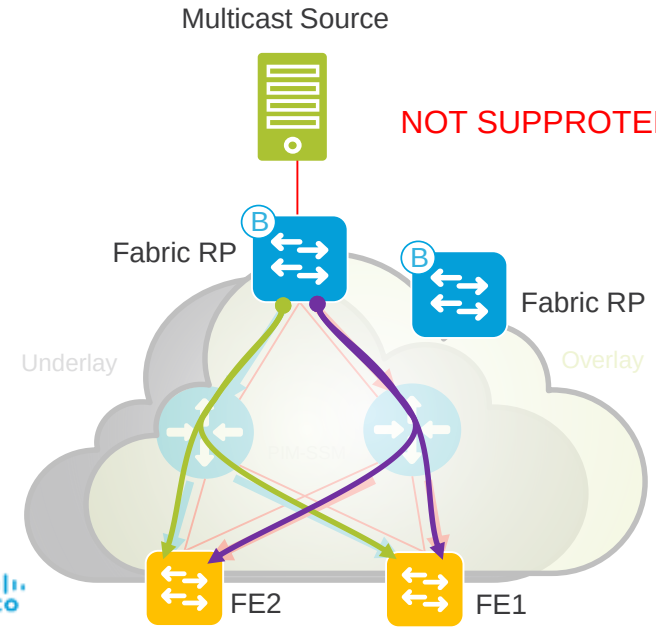
Support Matrix

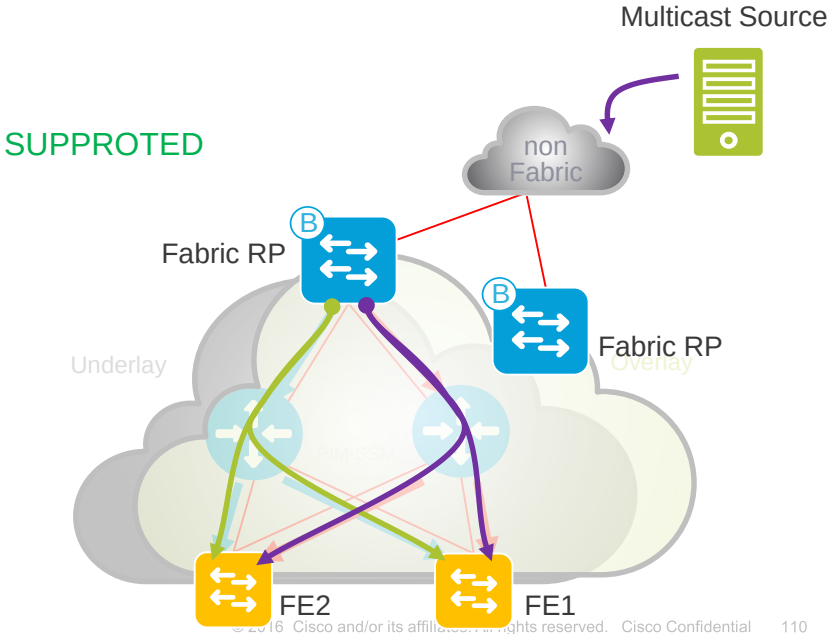
SD-Access Fabric Device	Supported	Software Release
C3K	YES	16.9.1s
C9K	YES	16.9.1s
C6K	YES	15.5(1) SY2
N7K	NO	N/A
ASR1K/ISR4K	YES	16.9.1s

Native Multicast in SD-Access

Caveat

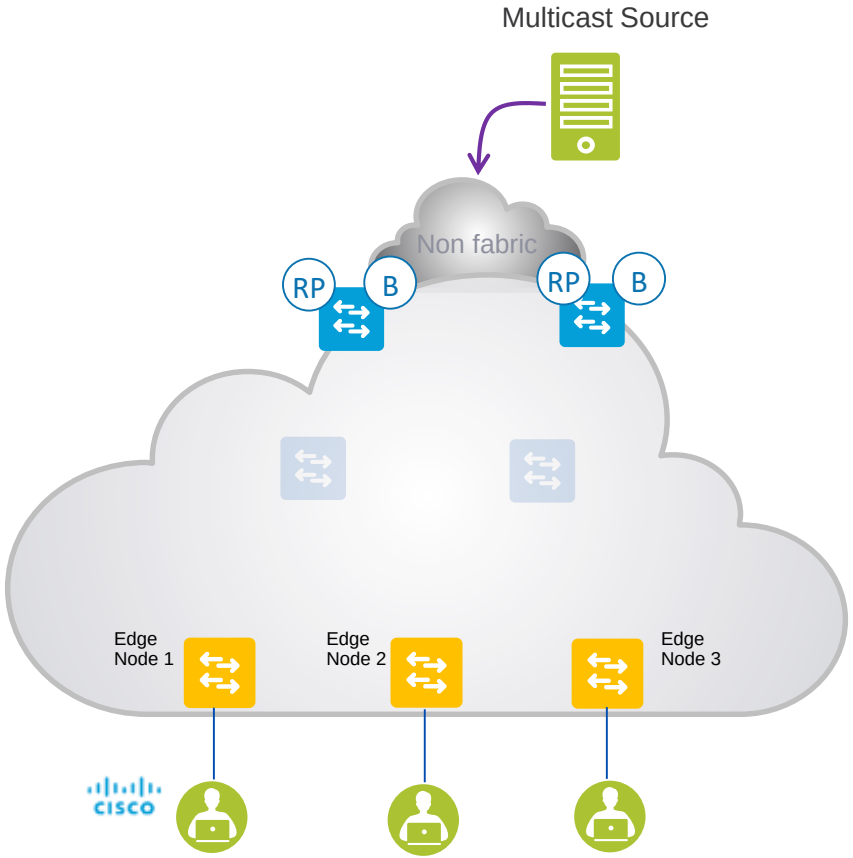
- In both Native and Head end replication we don't support a source directly connected to only one RP in the Overlay if there is a dual RP configured in the network.





Native Multicast in SD-Access

Forwarding



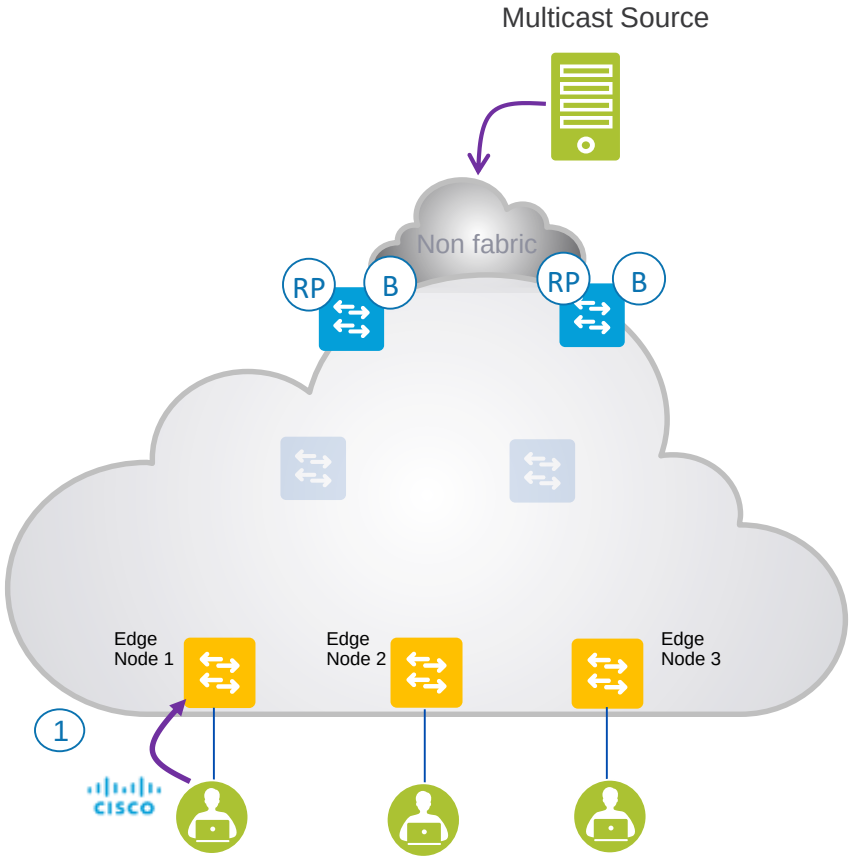
0 When the native multicast knob is turned on for a given fabric site the VN's where multicast is turned on will be instructed to move over to native multicast for the data path.

The Configuration is pushed under the LISP interface for the respective VN's and the multicast groups in that VN will be mapped to underlay SSM groups for data transport.

Interface LISP0.4096
ip pim lisp transport multicast
ip pim lisp core-group-range 232.0.0.1 1000

Native Multicast in SD-Access

Forwarding



1. Host , which is a receiver sends an IGMP join to the group 238.0.0.1 to the fabric edge node

In this example we assume that ASM is used in the overlay and the group address is 238.0.0.1.

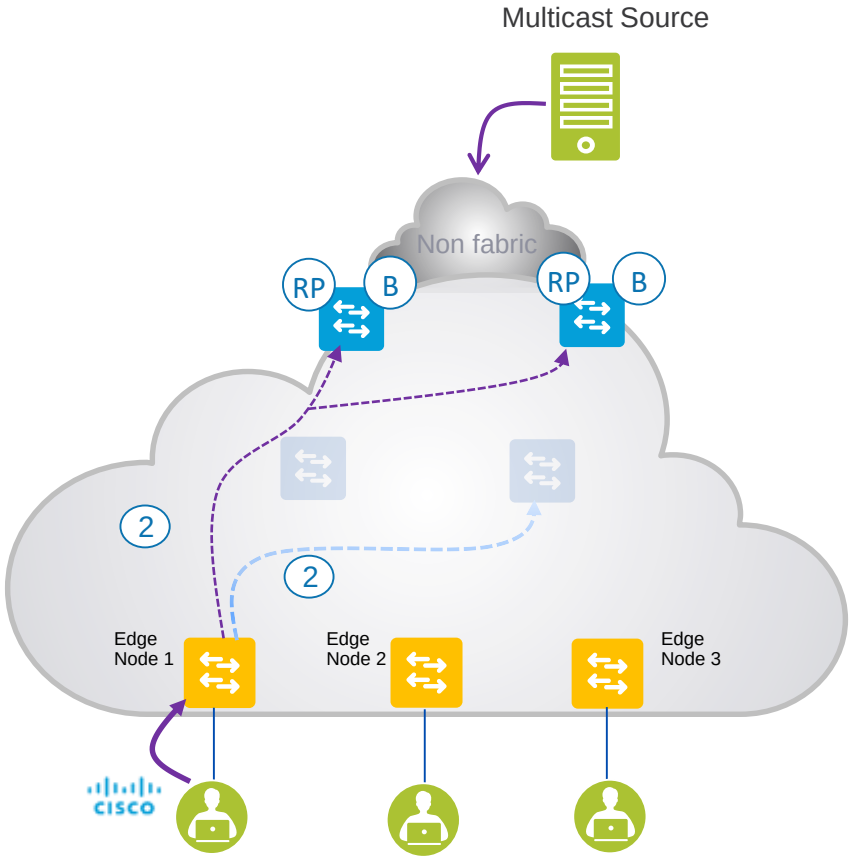
The SSM mapping for that group in the underlay is 232.0.0.9.

This is derived based on the configuration.

Since we are using SSM in the Underlay for native multicast there is no pre built multicast tree for any given group in Overlay.

Native Multicast in SD-Access

Forwarding



2 When the fabric edge node receives the IGMP join for group 238.0.0.1 the fabric edge node coverts that to PIM joins.

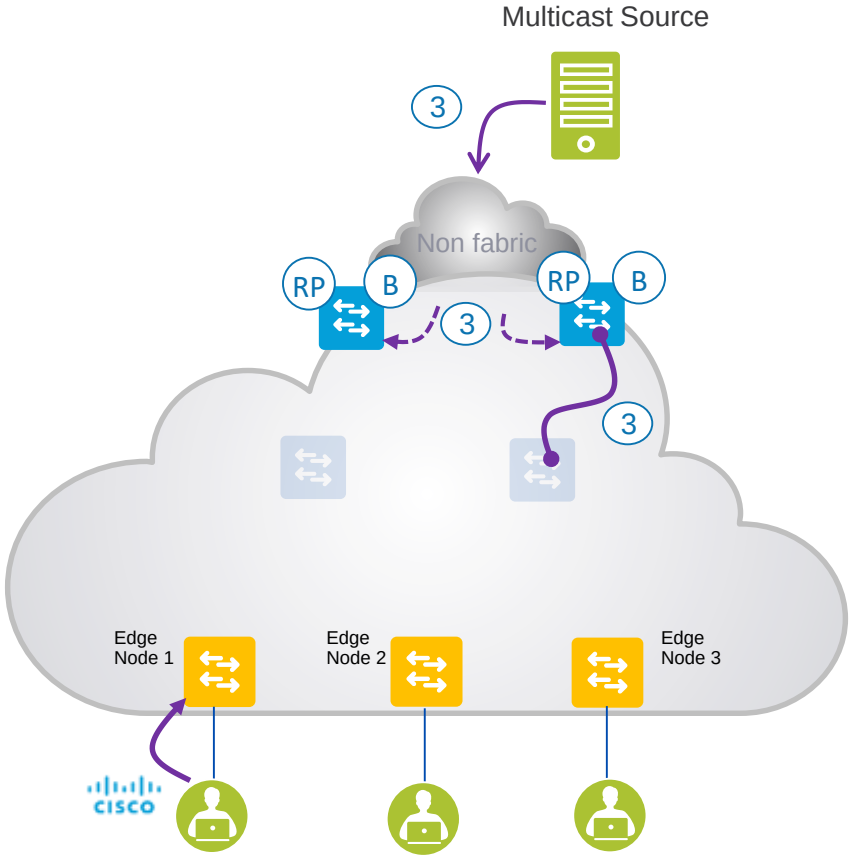
It sends one join in the Overlay to the RP for the group address 238.0.0.1 and it also sends one in the underlay for 232.0.0.9 (SSM group). The source address in the underlay join will be RLOC address as SSM always needs a source IP.

This is due to the fact that native multicast maps an overlay group to an SSM underlay multicast group.

The *,G joins in the Overlay and S,G/RLOC,G joins in the Underlay are formed because of this.

Native Multicast in SD-Access

Forwarding



3 The multicast source starts sending traffic and the closest fabric node , In our case the fabric border + RP will send a source registration message in the overlay on the group address 238.0.0.1 to the RP and also send the traffic in the overlay on the group address 238.0.0.1 .

With above the same fabric node also sends the traffic in the underlay on the mapped group 232.0.0.9 to the RP.

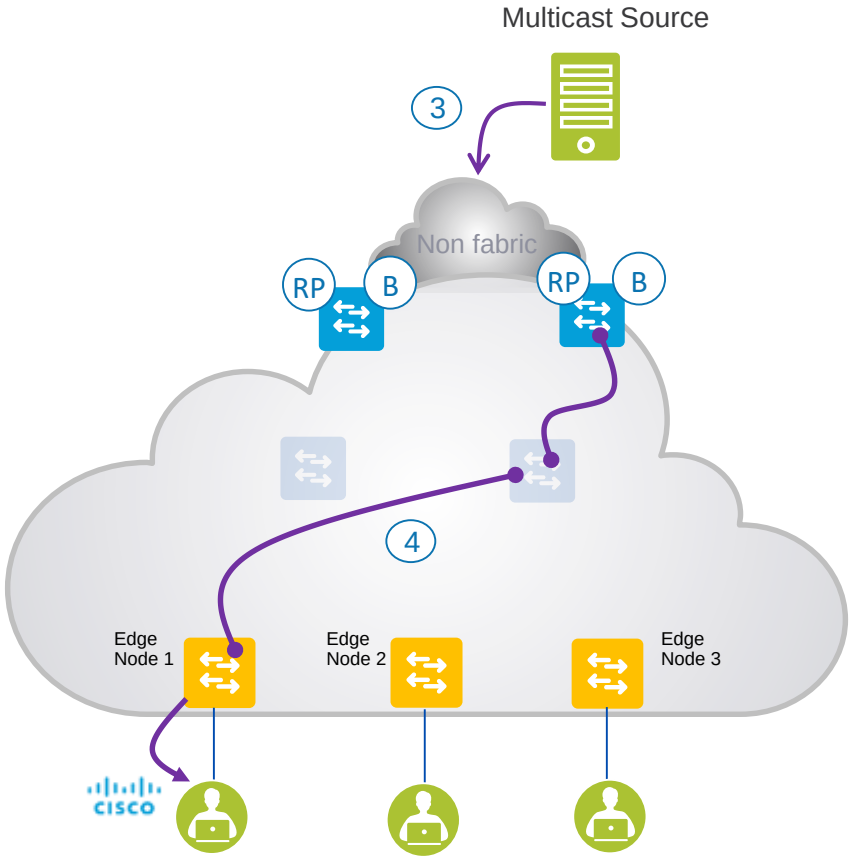
The traffic is sent to the RP because the Overlay group is still ASM.

This creates the S,G state in the underlay for the Overlay group.

If SSM was used in the Overlay then the RP would have no role.

Native Multicast in SD-Access

Forwarding



4 The Underlay now has enough information to replicate the traffic to the needed devices.

Fabric in a Box

Fabric in a Box in SD-Access

- The fabric in a box is supported on C9K switches only.
- It is only supported on a single device but that device can be a stack , not Stack wise virtual though but back stacking.
- Any given fabric site will support only one fabric in a box and no other fabric devices can be in that site.(this restriction will be removed soon)
- The scale for fabric in a box will go to the fabric edge scale for the given C9K device.
- Currently on that device embedded wireless is not supported.

Fabric in a Box in SD-Access

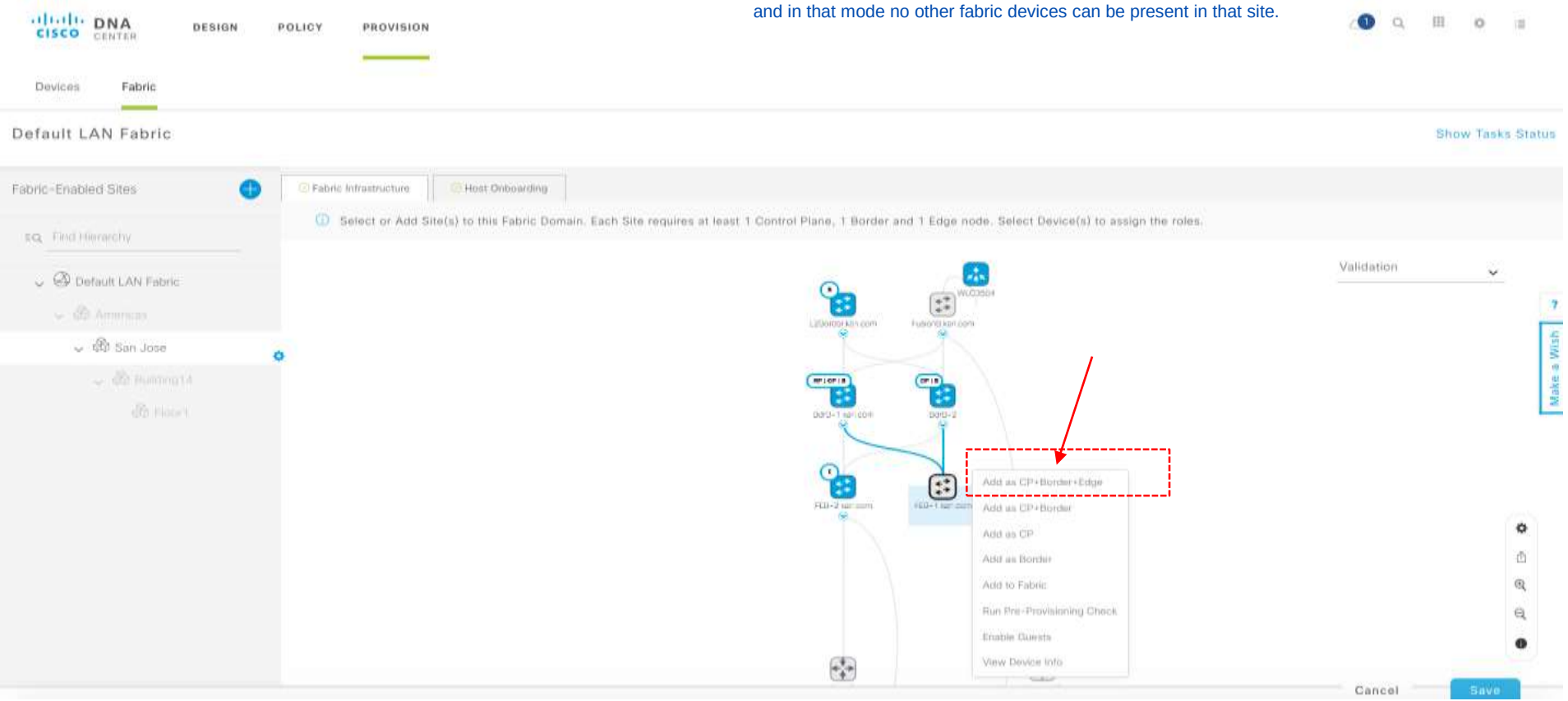
Scale

Fabric Constructs	Catalyst 9300	Catalyst 9400	Catalyst 9500	Catalyst 9500 H
Virtual Networks	256	256	256	256
Local End Points/Hosts	4K	4K	4K	4K
SGT/DGT Table	8K	8K	8K	8K
SGACLs (Security ACEs)	5K	18K	18K	18K

Fabric in a Box in SD-Access

Configuration

In this example we already have devices configured with other roles in the site and hence below Configuration would not be accepted. As stated earlier we can have one fabric in a box in a given site and in that mode no other fabric devices can be present in that site.



Six Control Plane nodes in a Fabric Site

Fabric Resiliency in SD-Access

- Starting from DNAC 1.2.5 we will support up to six CP nodes in a given fabric site.
- If fabric enabled wireless is implemented in that site then the CP nodes will remain as two with an Aire OS controller.
- When eWLC controllers will be supported in fabric then those controllers will support up to six CP nodes.
- When using SDA Transit for hand off only two Transit CP nodes are still supported in fabric.

Lan Automation Enhancements

DNAC 1.2.5 Lan Automation Enhancements

- Multicast support in underlay for Layer 2 flooding and Native multicast

Multicast support in Underlay

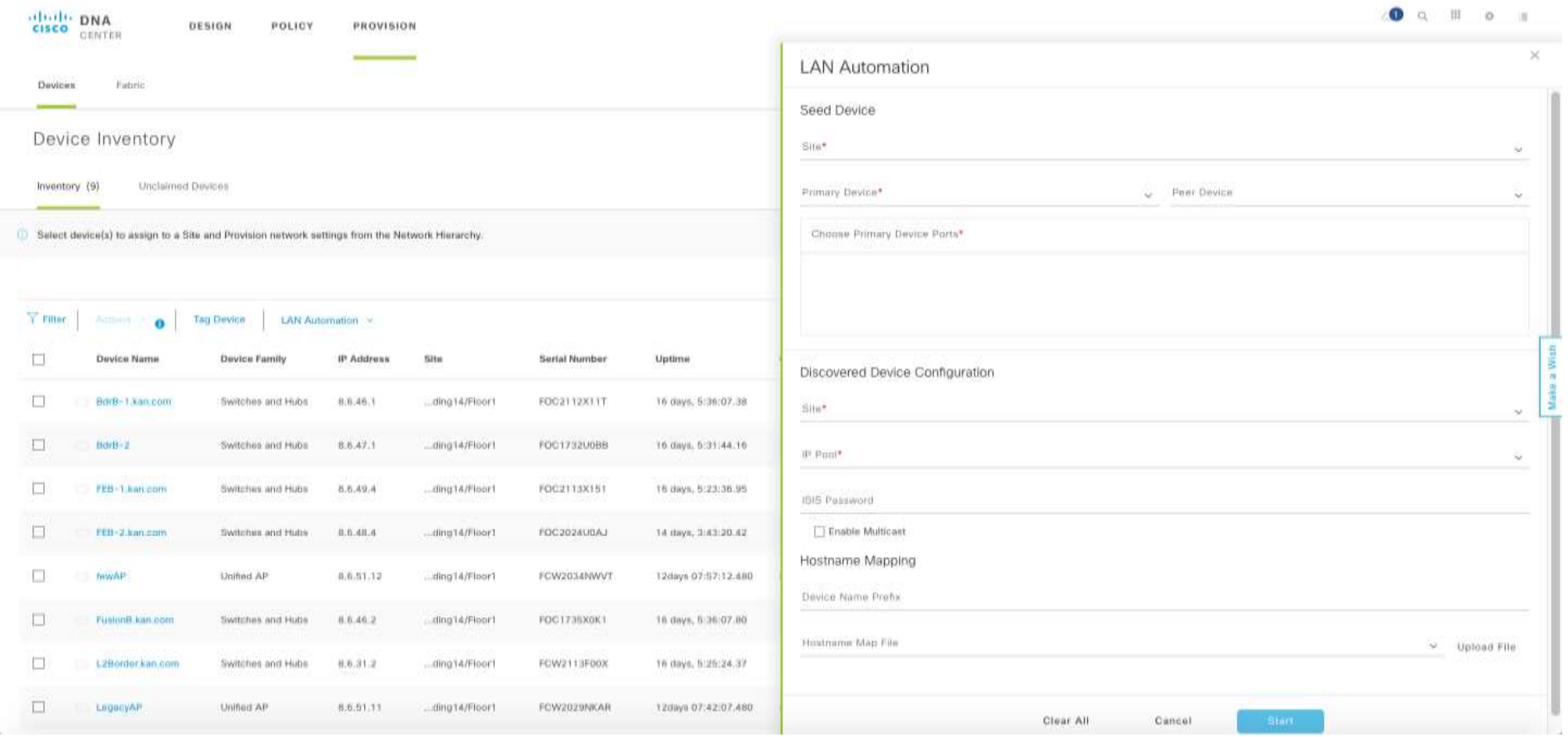
- Starting from DNAC 1.2.5 we have the option to selectively enable multicast in the underlay in the global routing table.
- When this option is selected both PIM ASM and SSM is enabled in the underlay.
- For PIM ASM the seed nodes are chosen as the RP's using Anycast configuration. To achieve this MSDP between the RP's are also configured in the underlay.
- For PIM SSM the default group of 232.0.0.0/8 is used.
- All the needed uplink interfaces and loopbacks are configured with the needed PIM configurations.

Multicast support in Underlay

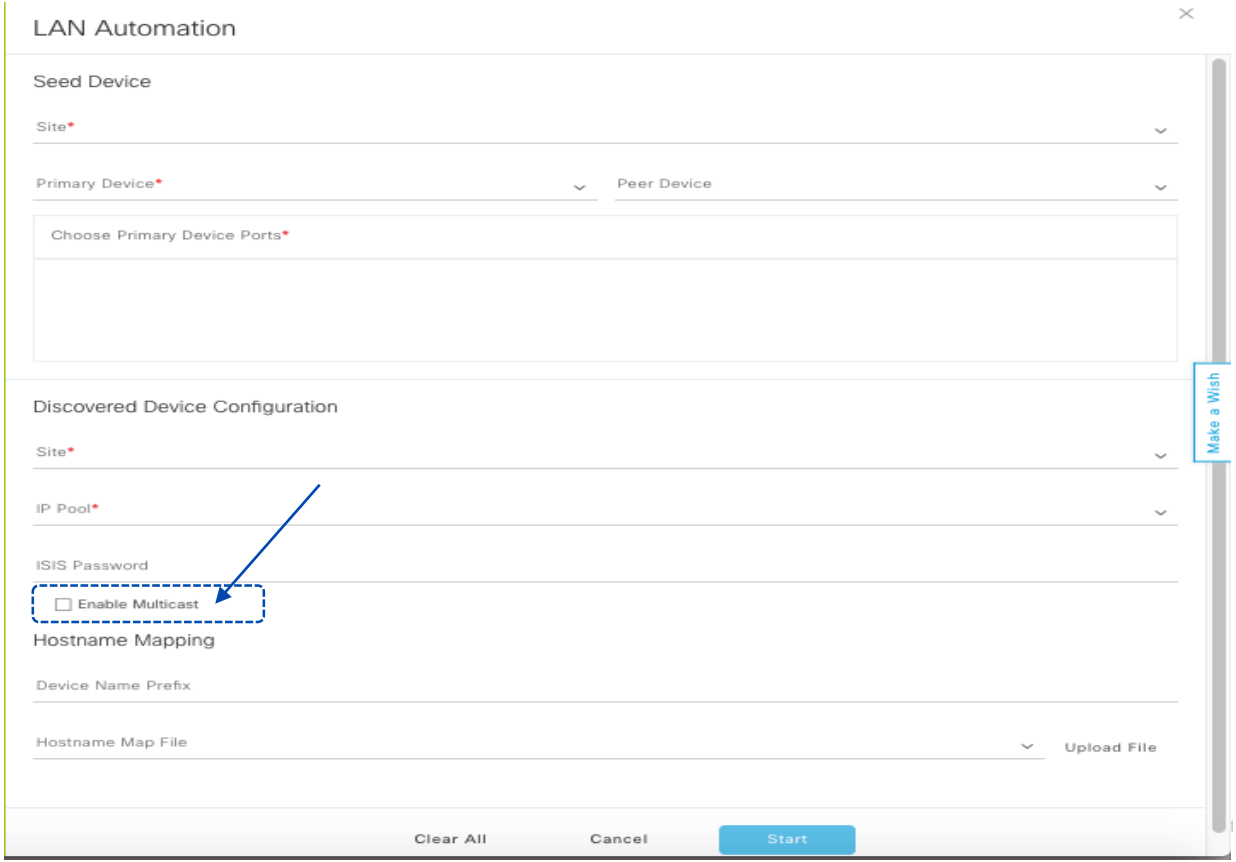
- The IP address for the RP nodes and MSDP peers are picked from the IP pool given for Lan automation. Hence ensure that a big enough pool is chosen during Lan automation that caters to these extra IP's.

- Because of multicast in the underlay we consume an extra three IP address from the given IP pool for Lan automation.

Multicast support in Underlay



Multicast support in Underlay



Host On-Boarding Enhancements

DNAC 1.2.5 Host On-boarding Enhancements

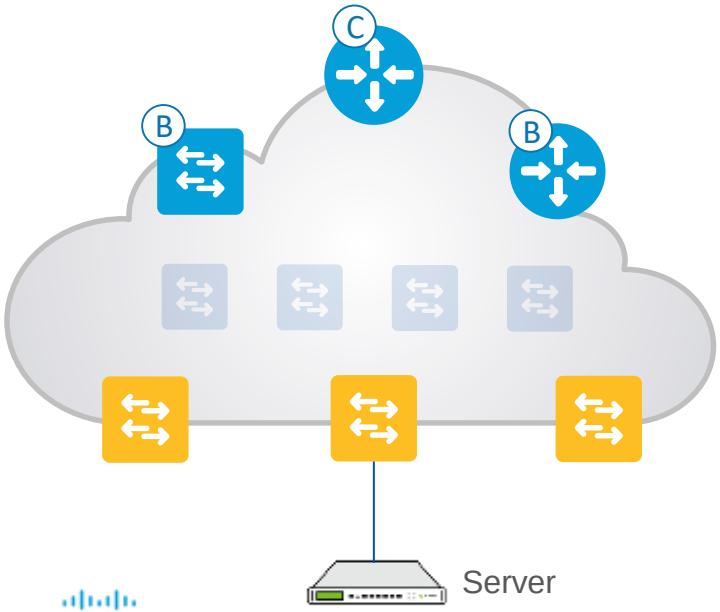
- Trunk Support on fabric edge nodes for Server connectivity.
- Device Profiling in SD-Access
- Custom VLAN information sent to ISE through API's for easier policy creation.

Trunk Support on fabric edge

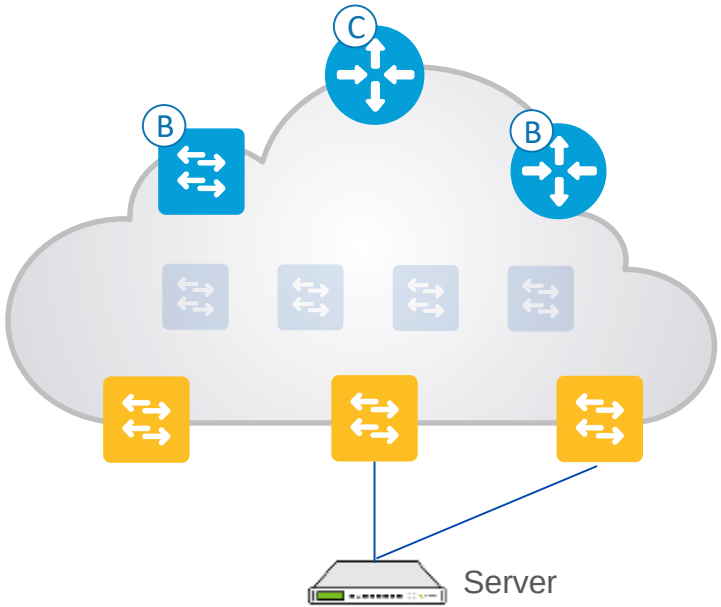
- Starting with DNAC 1.2.5 we support Trunk port on a edge node for server connectivity only.
- The port cannot be connected to any third party switches ,Flex AP's or non supported extended nodes.
- We will support upto 50 end points on that trunk port meaning we lock down the trunk port to only accept 50 mac-address.
- Dual homing of the server to multiple fabric edge nodes is not supported.

Trunk Support on fabric edge

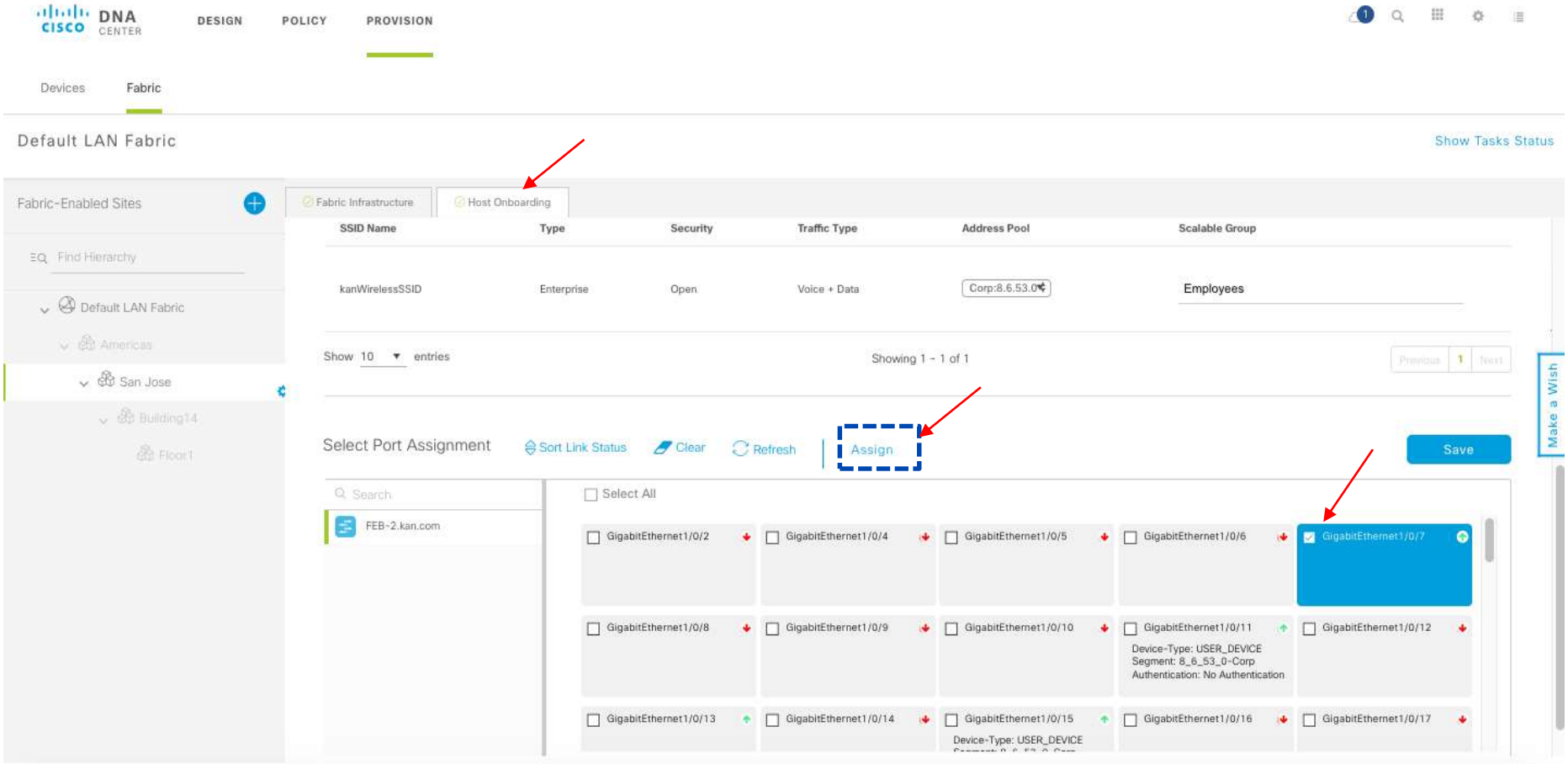
SUPPORTED



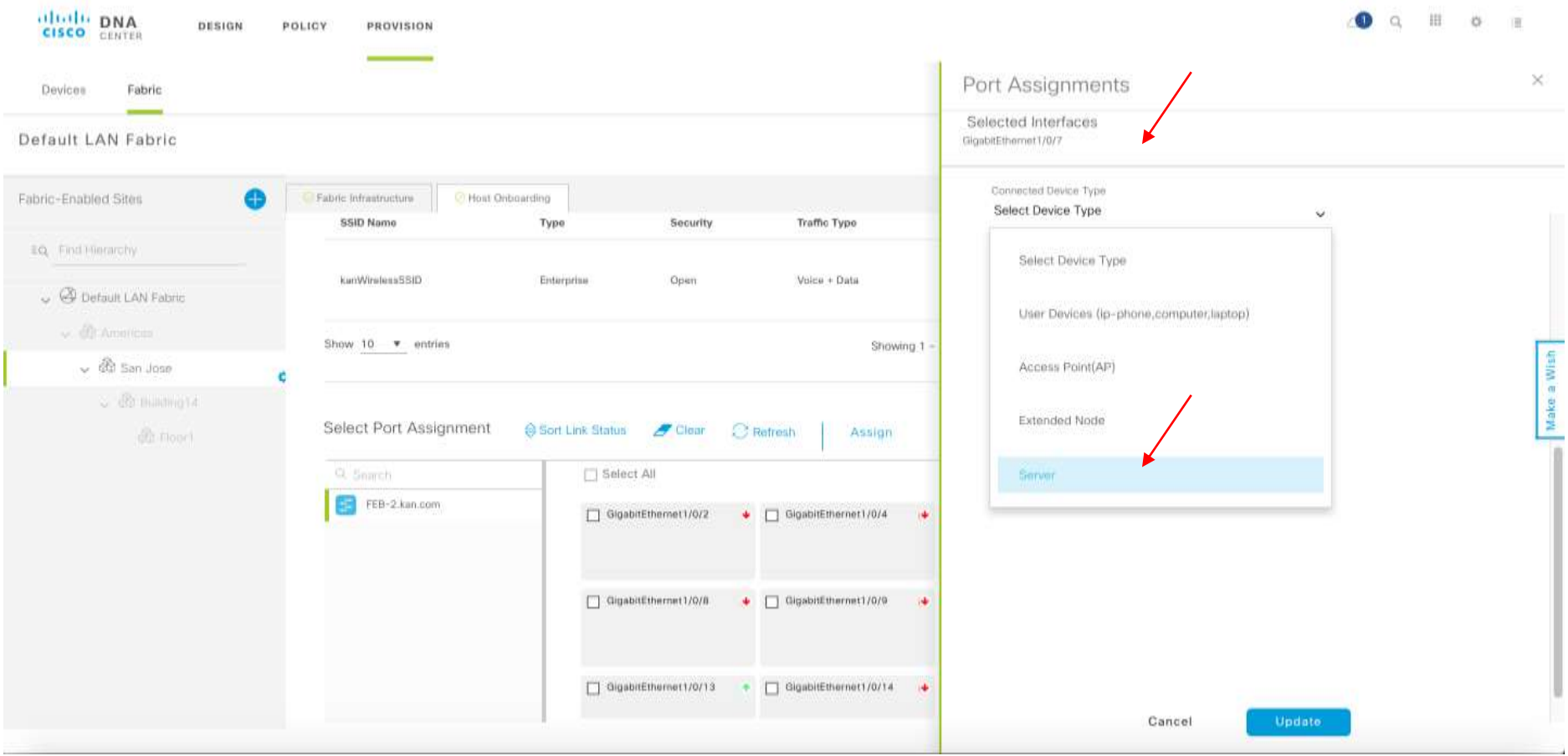
NOT-SUPPORTED



Trunk Support on fabric edge



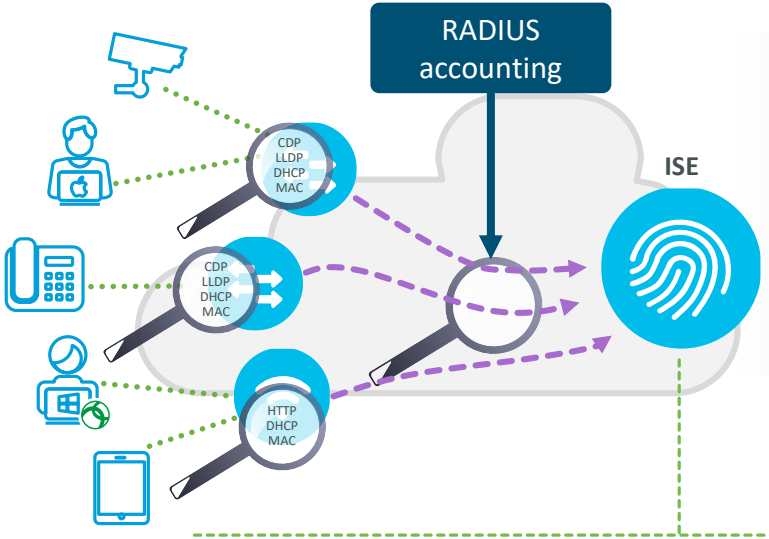
Trunk Support on fabric edge



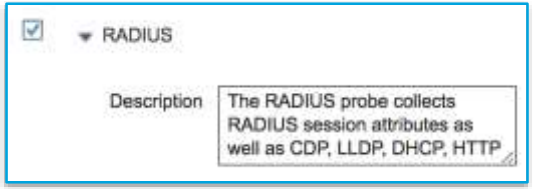
Device Profiling in SD-Access

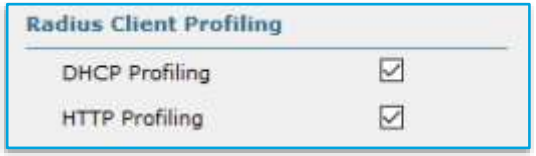
- Starting with DNAC 1.2.5 we will configure device sensor CLI's to enable device profiling on the fabric edge nodes.
- With above we will collect the needed information from end points and send data to ISE so that it can classify them into the right device groups and also use its MAC address for MAB authentication.

Device Profiling in SD-Access



- MAC OUI
- CDP/LLDP
- DHCP
- HTTP (WLC only)
- mDNS,
- H323,
- MSI-Proxy (4k only)



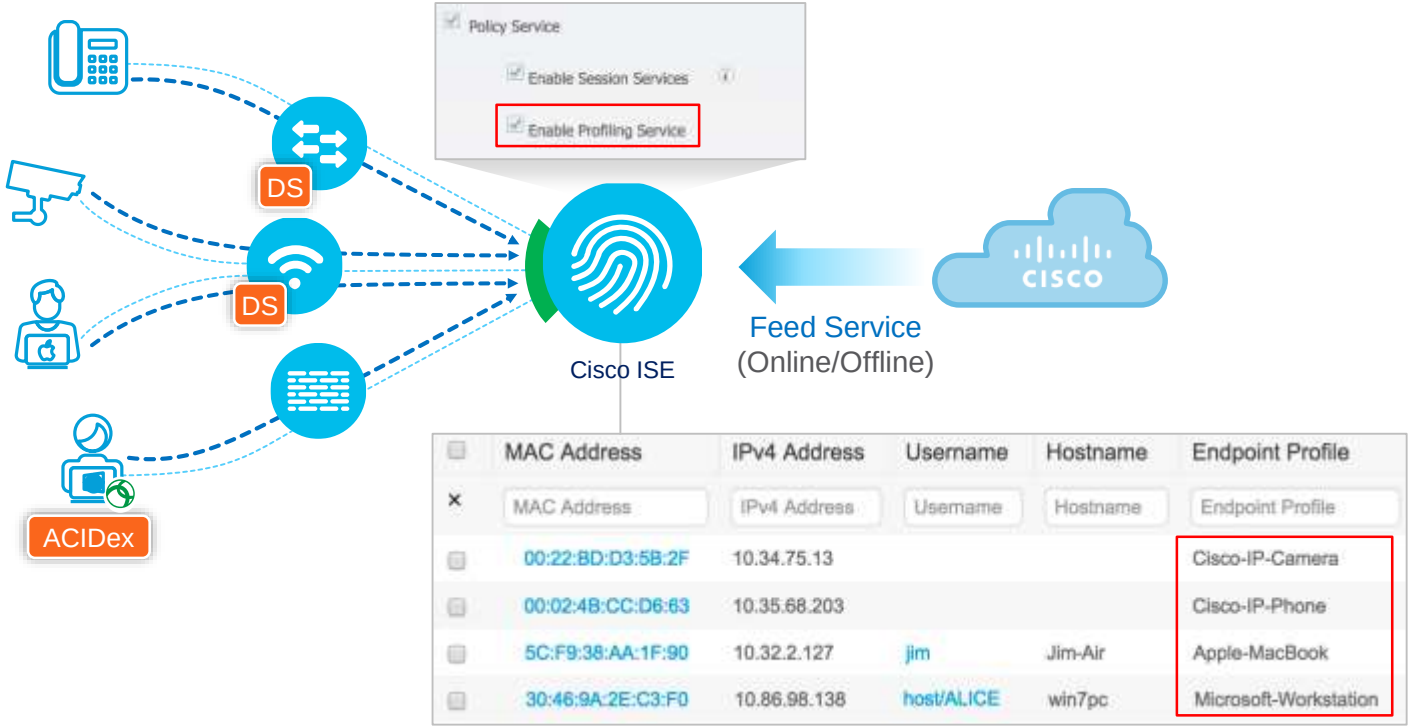


Data From Device Sensor	+	Profile Conditions	=	PROFILED
Example: **MAC OUI + Lexmark**		If DHCP Class ID Contains **E260dn**		It's a Lexmark **E260n Printer**

Device Profiling in SD-Access

The profiling service in Cisco ISE identifies the devices that connect to your network

Endpoints send interesting data, that reveal their device identity



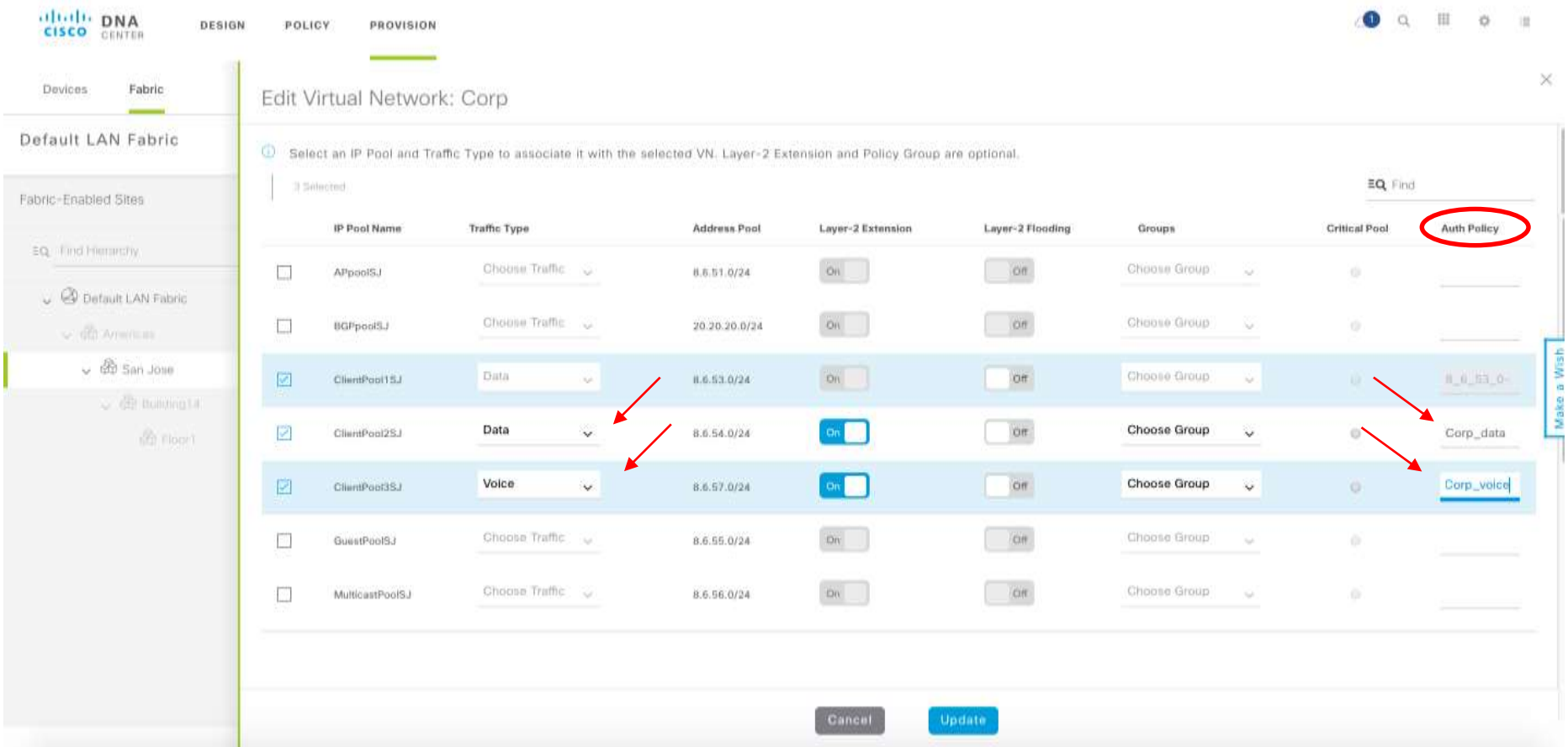
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

Vlan information sent to ISE via API’s

- Starting with DNAC 1.2.5 the vlan name created in DNAC for a given IP subnet is auto populated into ISE. This helps with ease of policy creation in ISE.
- The vlan names are configured in DNAC and are pushed to ISE via API’s.
- The respective traffic type needs to picked so that it is reflected in ISE correctly.

See next slide

Vlan information sent to ISE via API's

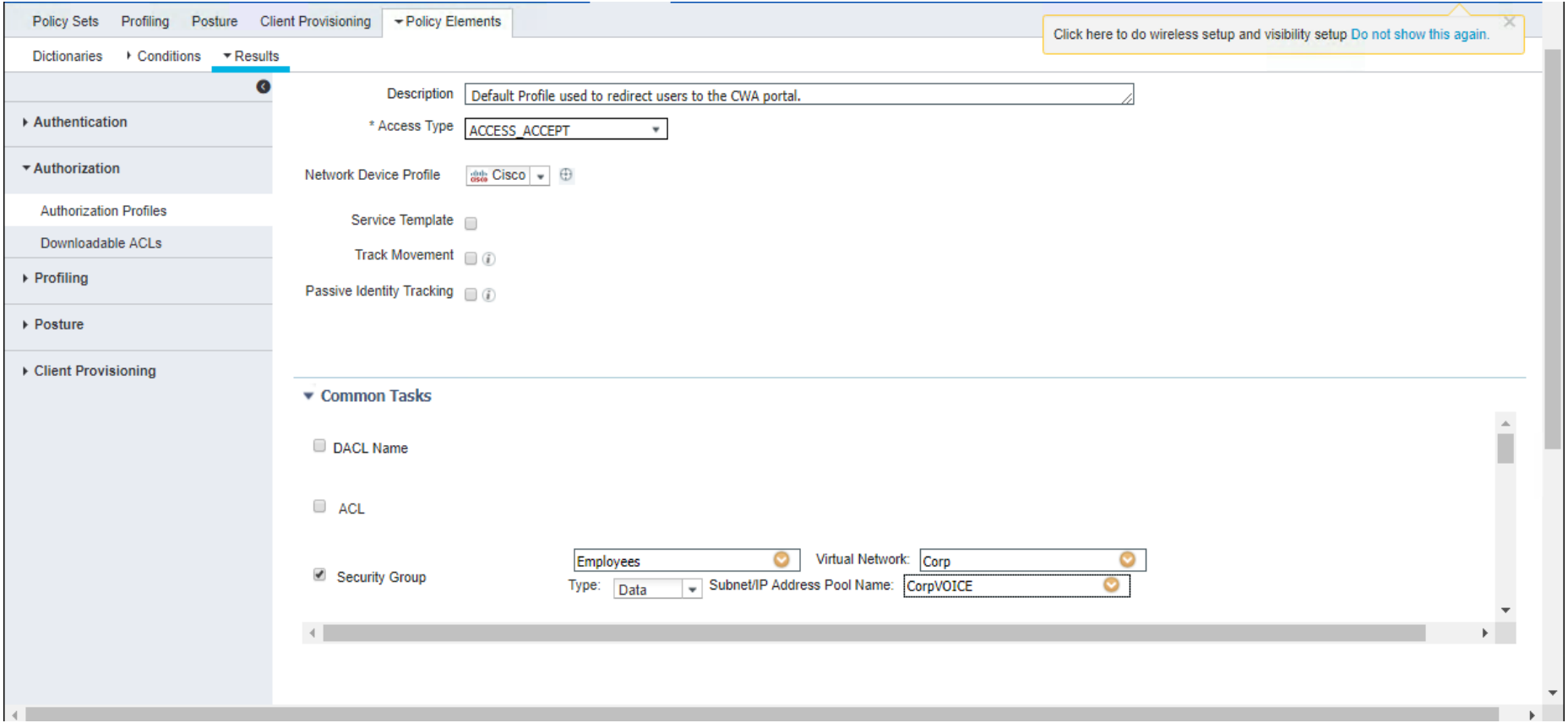


Vlan information sent to ISE via API’s

- In ISE , under the Authorization profile page in ISE user can pick the VNs and pools from drop down already as that is now being shared from DNAC via API’s.

See next slide

Vlan information sent to ISE via API's



DNAC CLI Templates

DNAC CLI Templates

- In DNAC 1.2.5 to enable faster SD-Access customer deployments there are a certain sent of configurations that will be permitted in the fabric through DNAC templates.

- These configurations are yet pushed through the SDA App workflows yet.

DNAC CLI Templates

No.	Configuration
1.	Switch Hardening : • CoPP, SSH ACL, Line VTY, BPDU Guard, Root Guard
2.	Border Handoff: • Port channel for Border handoff • iBGP, OSPF
3.	Transparent Firewall at Border
4.	Variable MTU in Fabric

DNAC CLI Templates

No.	Configuration
5.	Services: • FNF Templates • ETA Templates • QoS Configs
6.	Multi-ISE for Guest Wireless
7.	SGT Inline tagging and propagation at border node (bi-directionally)
8.	Multicast RP outside fabric
9.	SXP to Border


CISCO