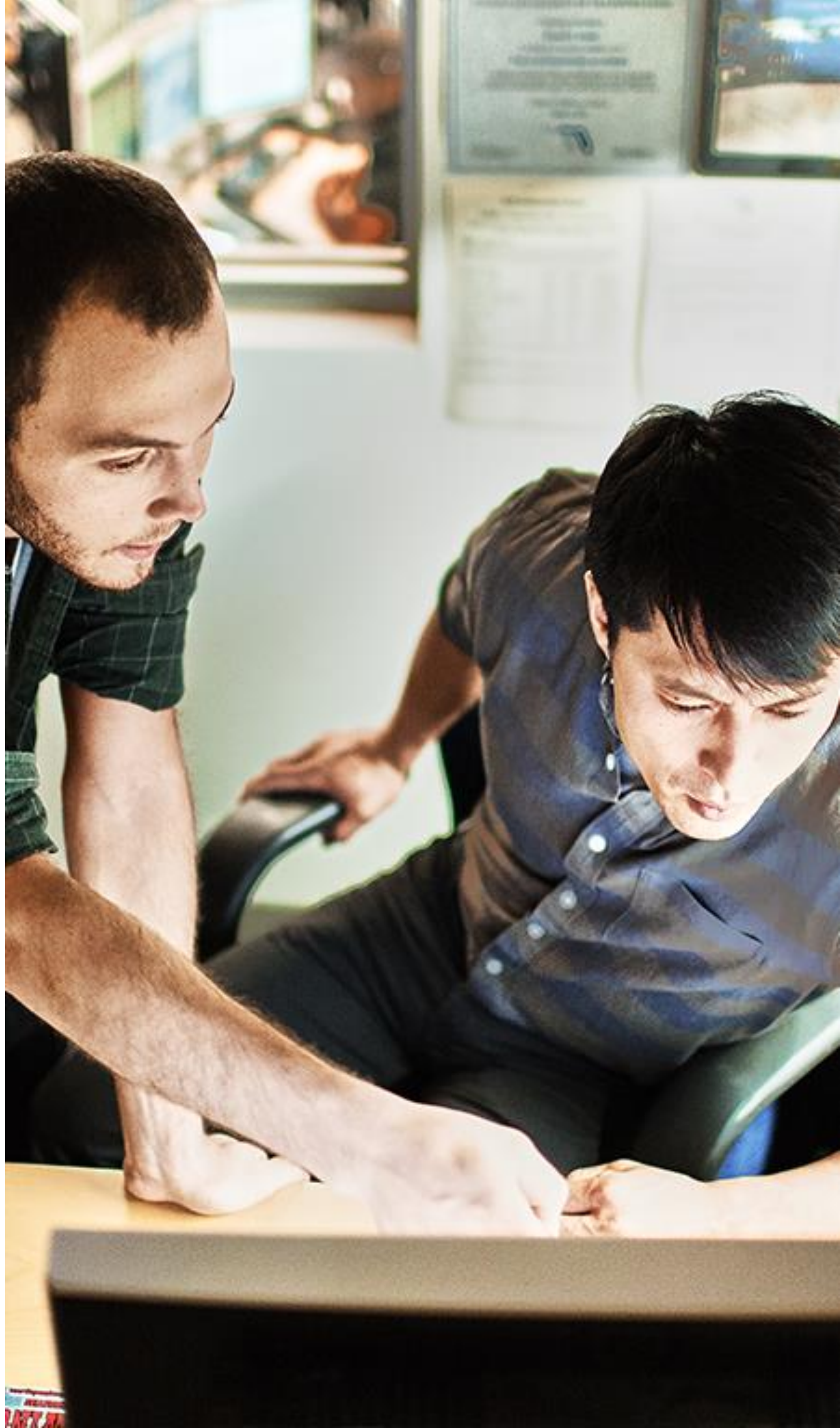
Les Fondamentaux de Cisco SD-Access

Community Live

Jérôme Durand - @JeromeDurand
Technical Solutions Architect – Enterprise Networking

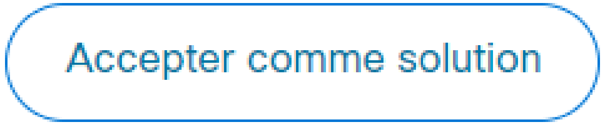
Mercredi 21 juin 2023



Connectez, Engagez, Collaborez !

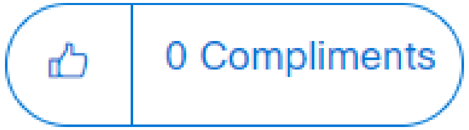
Solutions

Acceptez les solutions qui sont correctes et complimentez ceux qui vous ont aidé ! Aidez autres utilisateurs à trouver les réponses correctes dans la fenêtre de recherche.



Compliments

Mettez en évidence les autres membres. Les votes utiles motivent les membres enthousiastes en leur offrant un signe de reconnaissance !



Spotlight Awards

De nouveaux lauréats tous les mois !

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les Spotlight Awards sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat !
Cliquez ici

Community Spotlight awards

Jérôme DURAND

Technical Solution Architect

Jérôme a intégré le GIP RENATER en 2002, d'abord sur des projets R&D puis comme responsable des opérations en 2006, et enfin en charge de l'équipe services en 2009. Jérôme a rejoint CISCO en 2011 comme expert sur les technologies de routage et commutation. Actuellement, il est très impliqué sur la programmation et l'automatisation des réseaux et notamment les solutions SD-WAN et SD-Access. Il est aussi auteur du RFC 7454 - BGP Operations and Security.

- Accompagnement des clients et partenaires sur Campus sur les projets Catalyst Campus et SD-WAN
- Evangéliste, Blogueur et Youtubeur
- Il a commencé l'aventure SD-Access depuis le tout début
- RFC 7454 – BGP Security BCP (et quelques brouillons sur Internet...)

http://reseauxblog.cisco.fr

Télécharger la présentation

https://bit.ly/WEBsld-jun23

slido

Join at

slido.com

#2460 020

Passcode: **afebum**

Introduction à Cisco SD-Access

The endpoints are changing in the campus... ... Smart buildings are a reality !

Base building services

Access points

Light fixtures

HVAC VAV controllers

Ceiling fans

Smoke alarms

Power meters

Touchscreen PCs

Tenant access and security

Surveillance cameras

Biometric door locks

Facial recognition systems

Entry barriers and turnstiles

Badge readers

IP call towers

Workspace transformation

Meeting room nameplates

PoE displays

Temperature sensors

Status signs

Horns and sirens

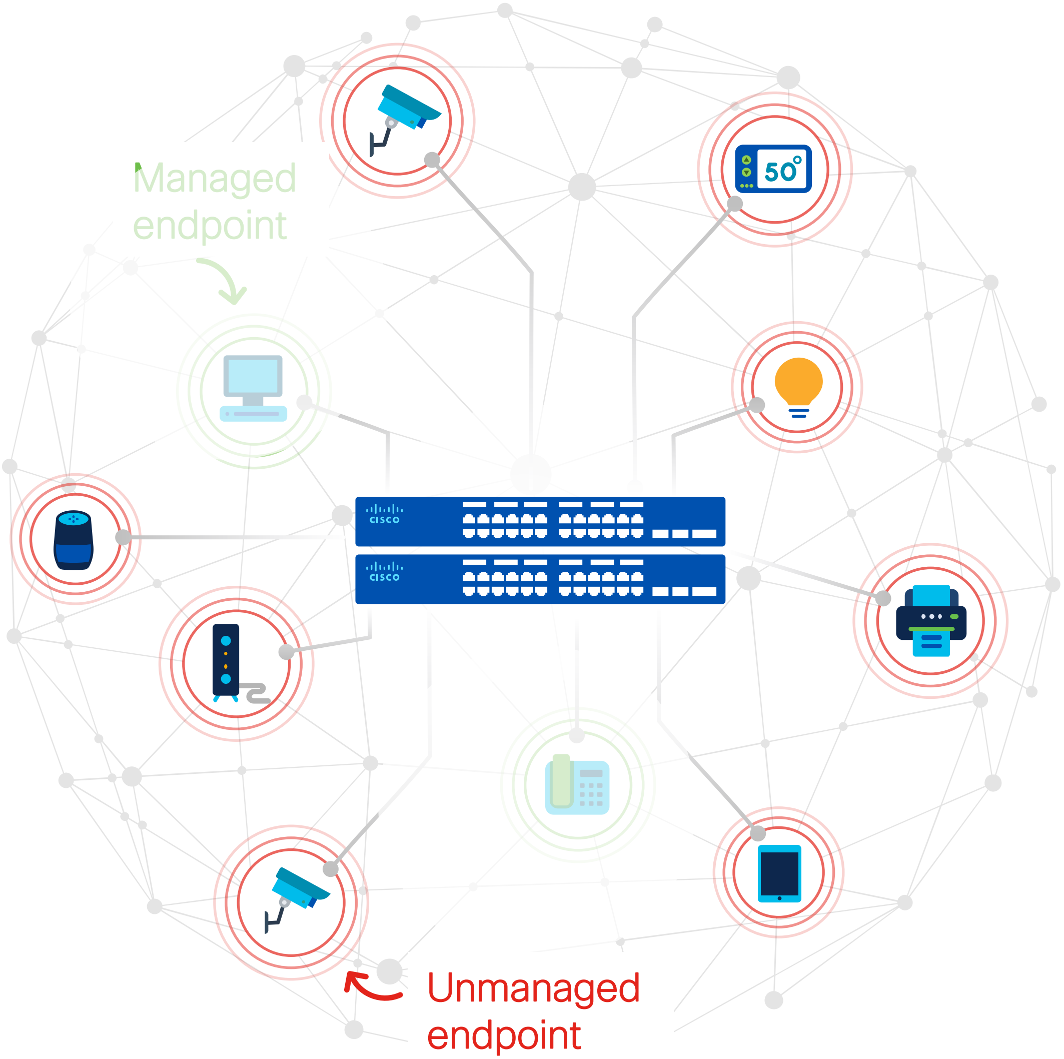
IP call stations

Environmental sensor hubs

Blind motors

Curtain motors

What’s happening in the workplace?



1:5

1:5 managed to **unmanaged endpoint ratio**

Unmanaged endpoints are difficult to patch and **most vulnerable to cyber attacks.**

Secure authentication mechanisms unusable on unmanaged endpoints

Open, unsegmented networks with IOT devices put organizations at risk

Key challenges for traditional networks

Complex to manage

- Many types of users, difficult to configure
- Multiple steps and complex interactions

Slower issue resolution

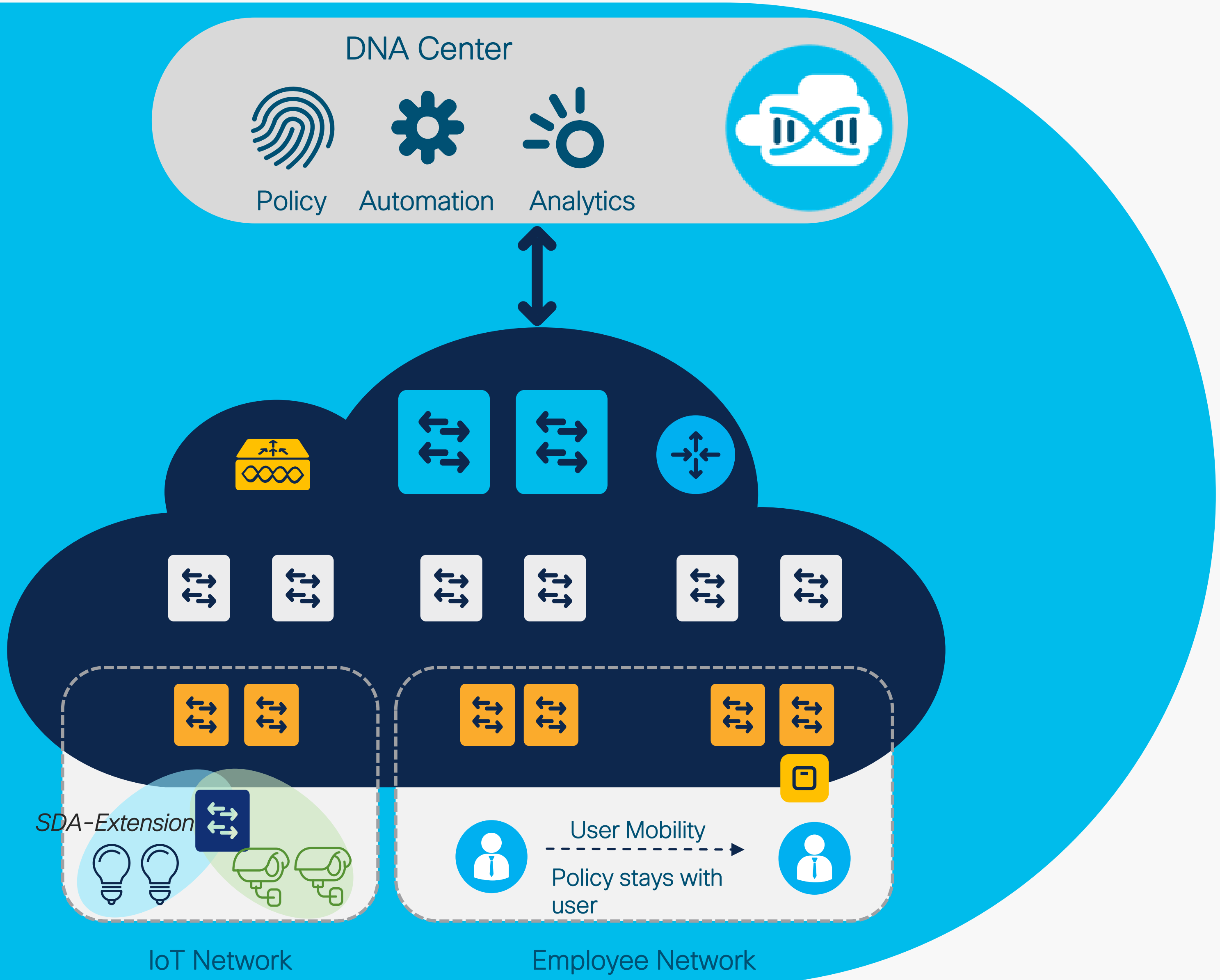
- Separate user policies for wired and wireless networks
- Unable to find users when troubleshooting

Difficult to segment

- Ever-increasing number of users and endpoint types
- Ever-increasing number of VLANs and IP subnets

Today’s networks can’t address the growing needs

Software-Defined Access



Automated Network Fabric

Single Fabric for Wired & Wireless with Workflow-based Automation

Insights & Telemetry

Analytics and insights into user and application behavior

Identity-based Policy & Segmentation

Decoupled security policy definition from VLAN and IP Address

SD-Access Momentum Accelerates

4000+
Customers

20%
Increase in Deployments YoY

101K+ **Devices**
29M+ **Endpoints**
Aggregate

773K Endpoints
2,900 Sites
3,100 Devices

Largest Deployments

Adopted by **28%** of Fortune25 Companies

70%
deployments with Wireless

SDA
Multi-Domain
Architecture

Endpoint Analytics
Unparalleled Visibility

Unified Access Policy
Dynamic Segmentation

Simplified Architecture
Automation at Scale

Healthcare

Financial Services

Government

Professional Services

Education

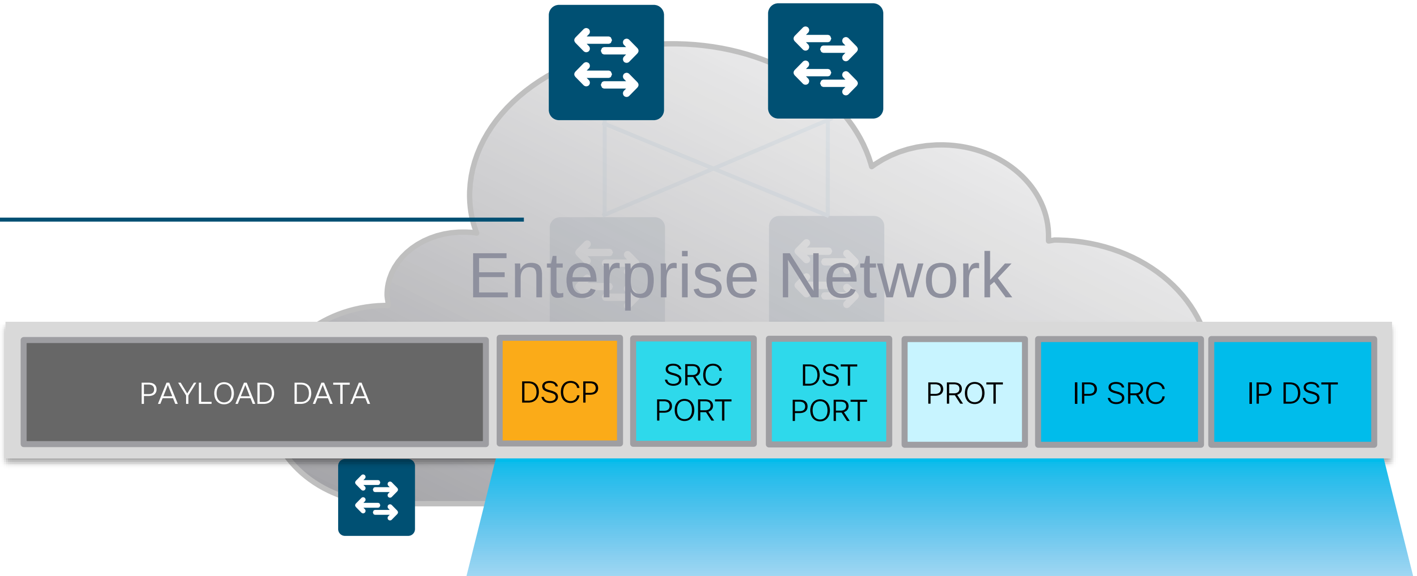
Manufacturing

SD-Access Provides *Industry Leading Campus Architecture*

Policy Model has impact on addressing

Network Policy

- QoS
- Security
- Redirect/copy
- Traffic engineering
- etc.



Policy is based on “5 Tuple”

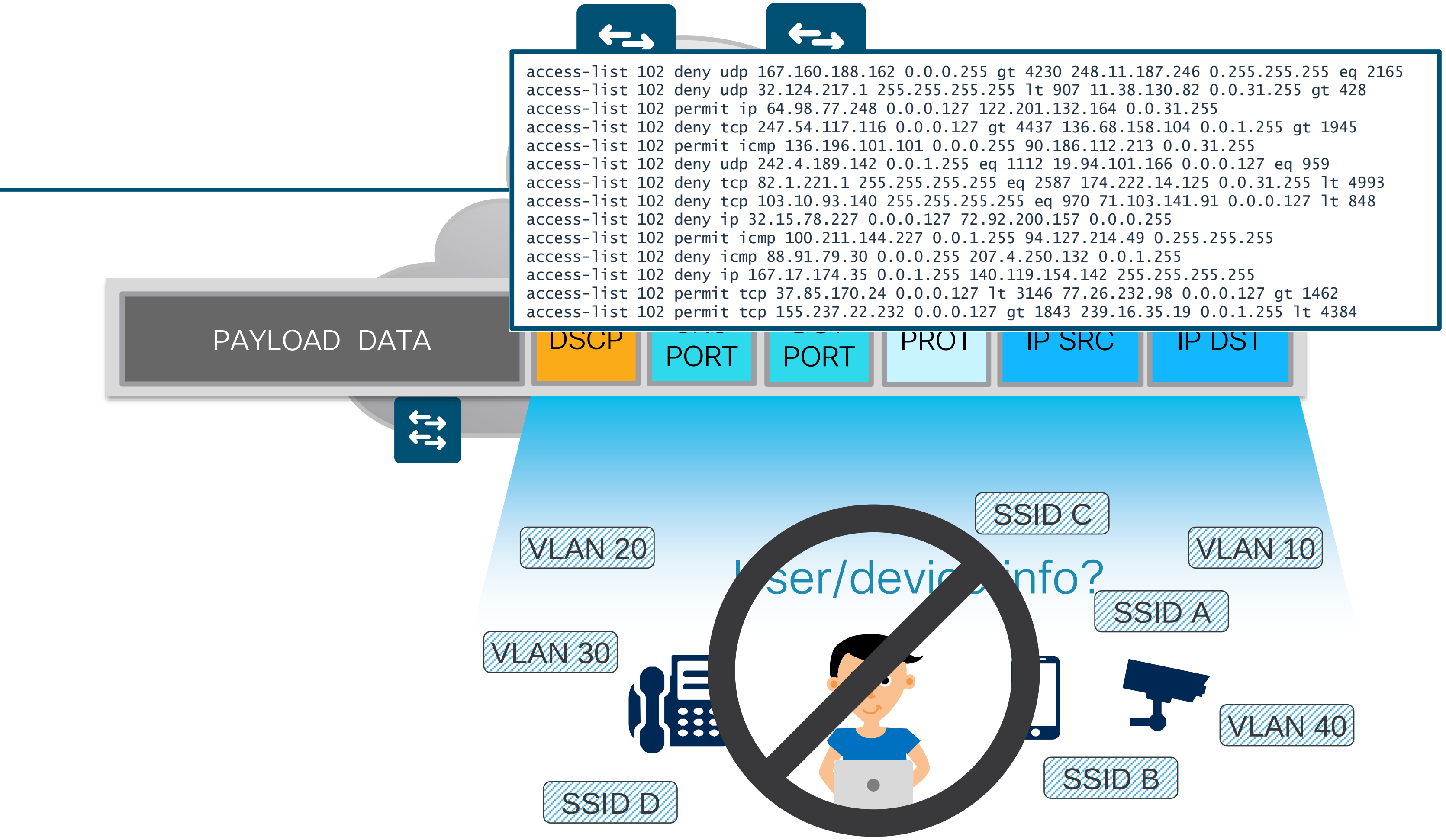
- Only Transitive information
- Survives end to end

Policy Model has impact on addressing

Network Policy

IP
ADDRESSES

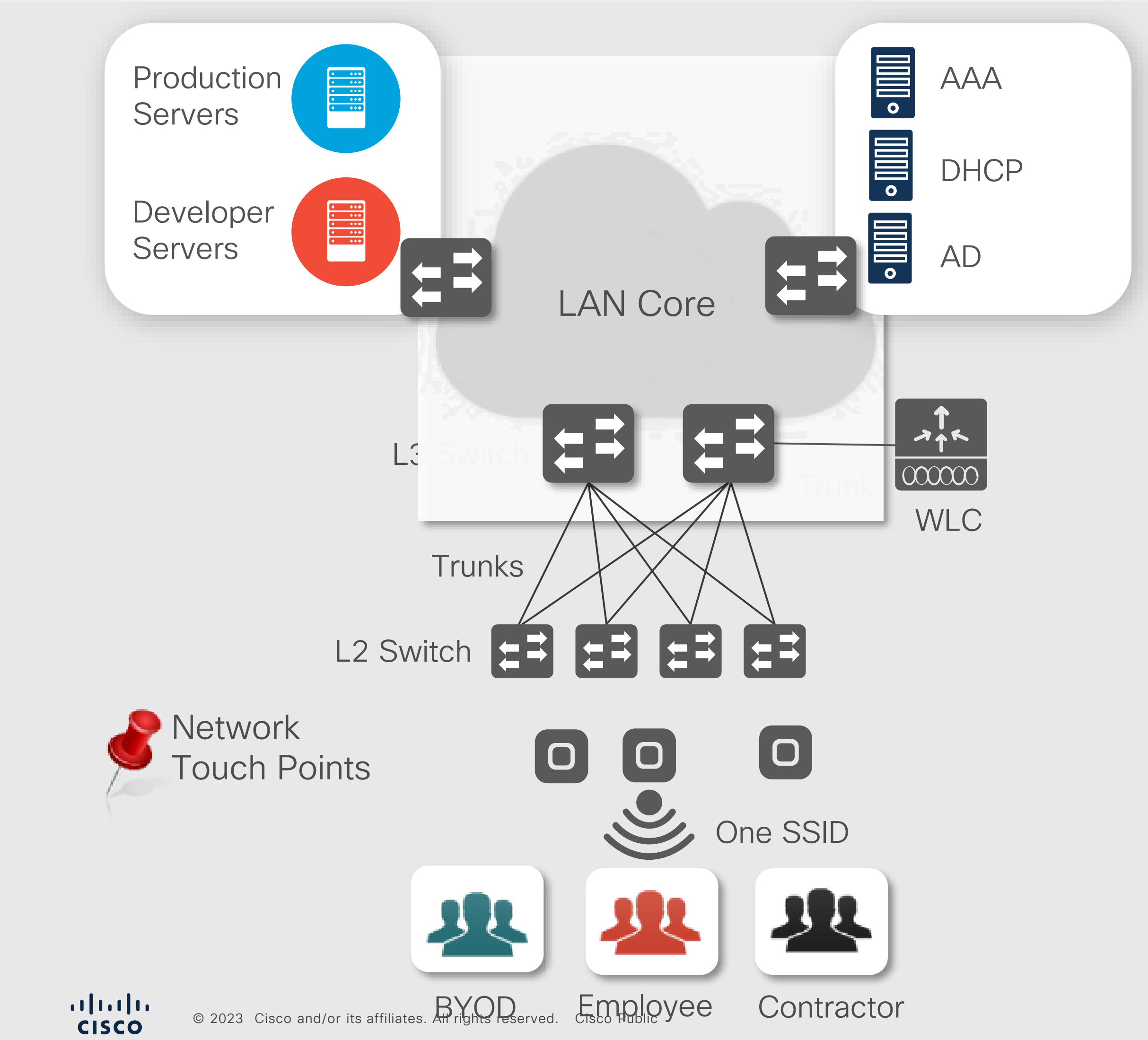
- Locate you
- Identify you
- Drive “treatment”
- Constrain you



```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 122.201.132.164 0.0.31.255
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 90.186.112.213 0.0.31.255
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 72.92.200.157 0.0.0.255
access-list 102 permit icmp 100.211.144.227 0.0.1.255 94.127.214.49 0.255.255.255
access-list 102 deny icmp 88.91.79.30 0.0.0.255 207.4.250.132 0.0.1.255
access-list 102 deny ip 167.17.174.35 0.0.1.255 140.119.154.142 255.255.255.255
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
```

Reference

Creating group based policies is complex



Customer requirements

- Three user Groups
- One single SSID
- Differentiated policies per Group
- Guest segmentation (wired and wireless)

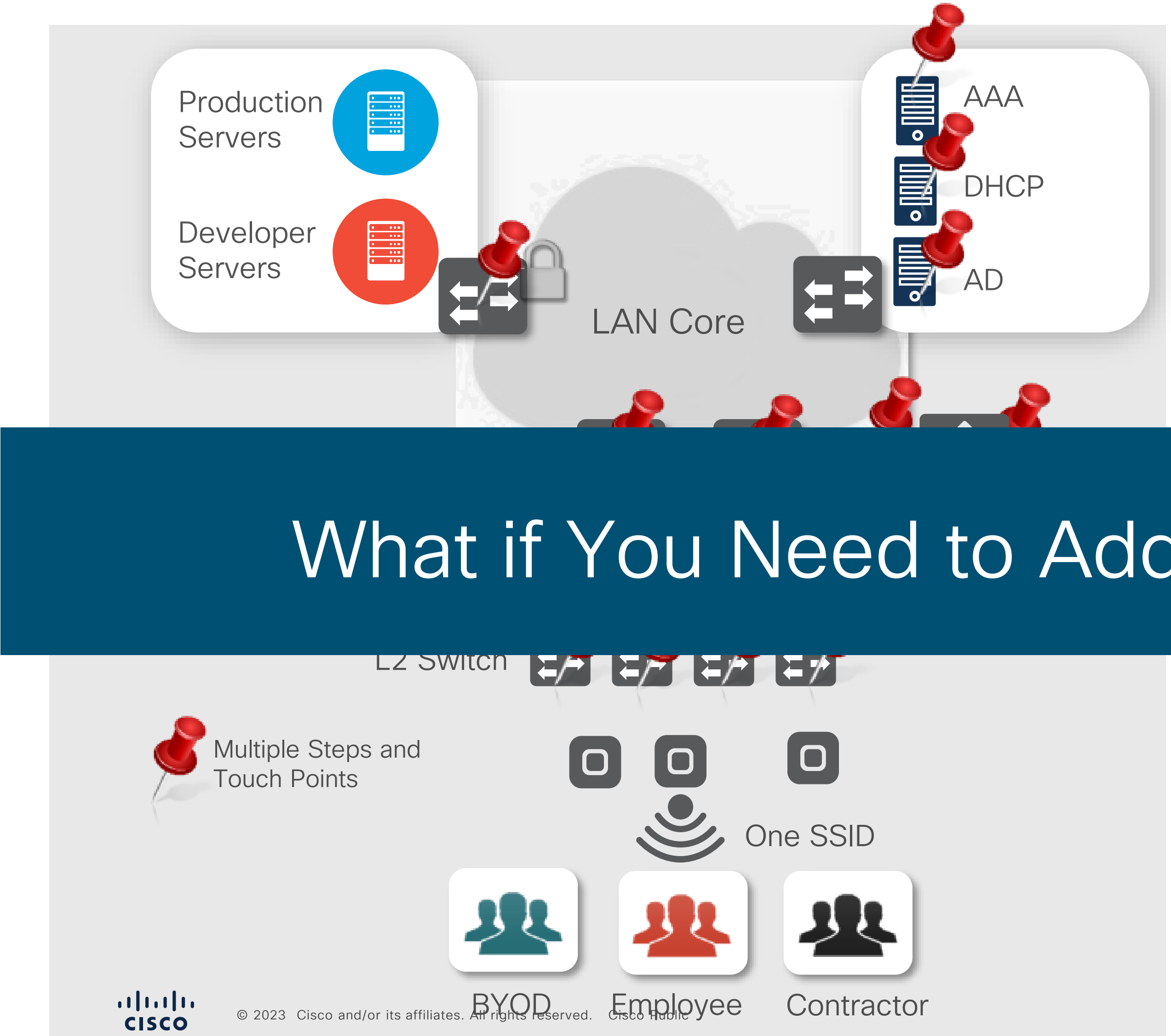
Customer Policy

- Customer Policy requirements:

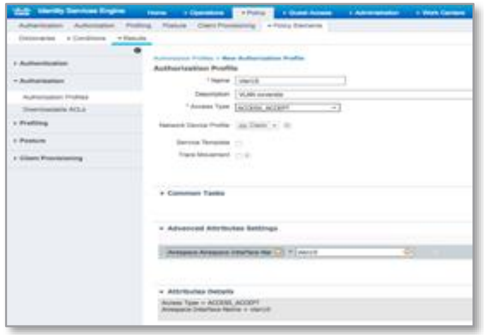
	Production Serv.	Developer Serv.
Employee	🟩	🟥
BYOD	🟩	🟥
Contractor	🟥	🟩

Reference

Creating group based policies is complex

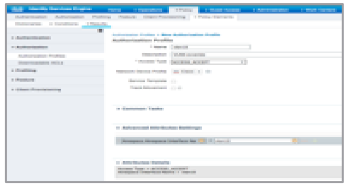


1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

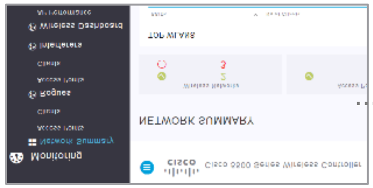


What if You Need to Add Another Group & Policy?

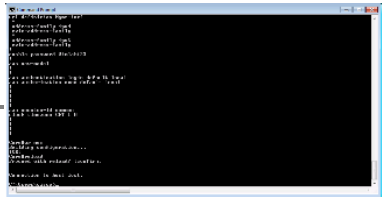
5. Many different User Interfaces



AAA



WLC



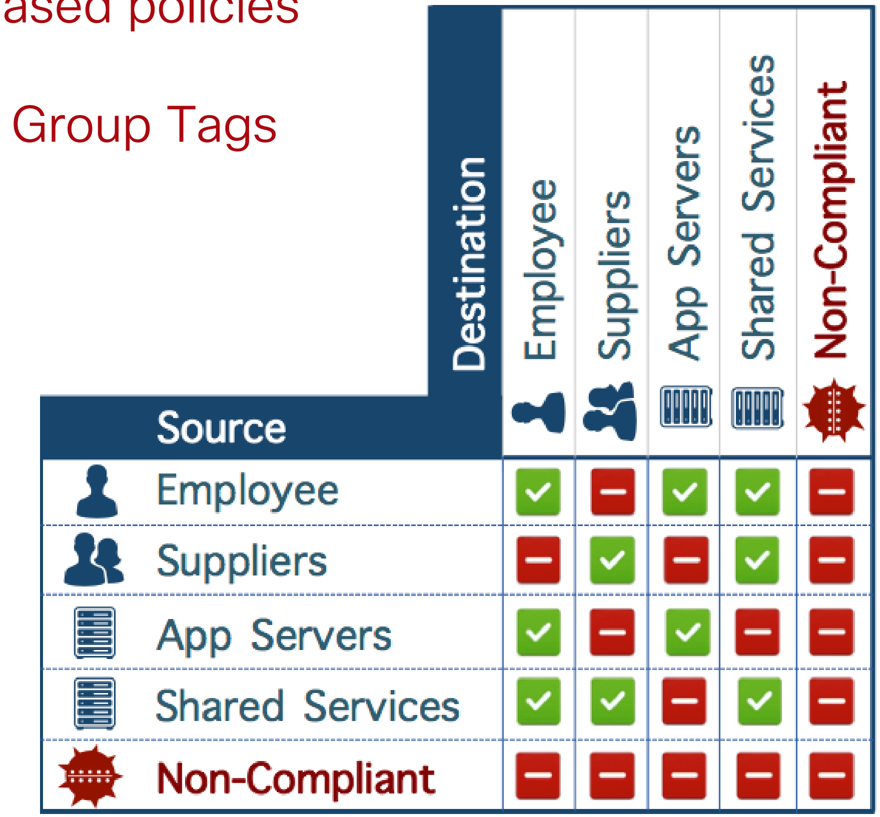
Devices CLI

SD-Access leverages Group-Based policies

Traditional Segmentation

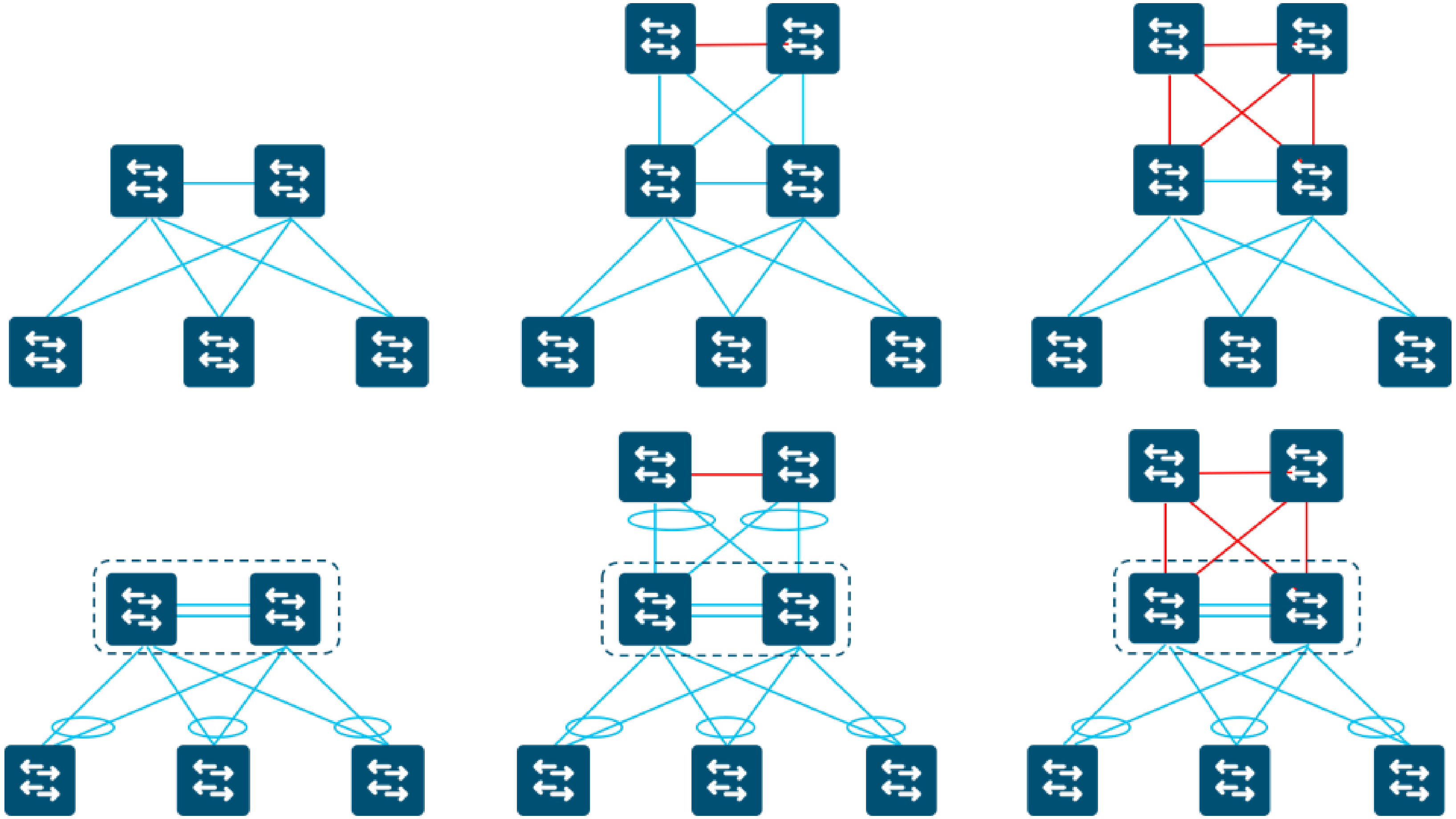
```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
```

Group-Based policies with Scalable Group Tags



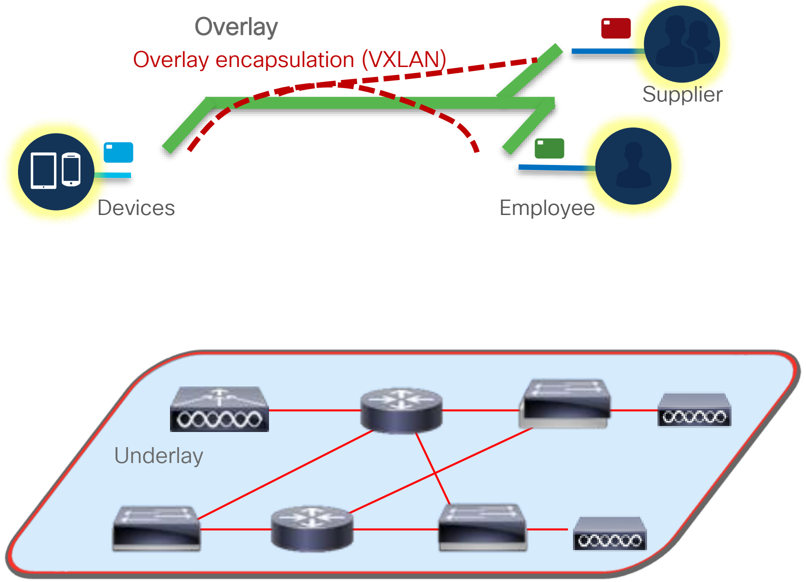
Source \ Destination	Employee	Suppliers	App Servers	Shared Services	Non-Compliant
Employee	✓	−	✓	✓	−
Suppliers	−	✓	−	✓	−
App Servers	✓	−	✓	−	−
Shared Services	✓	✓	−	✓	−
Non-Compliant	−	−	−	−	−

Architecture diversity adds complexity



Solution – Create a fabric to dissociate service and transport planes

Fabric enables Abstraction and Automation



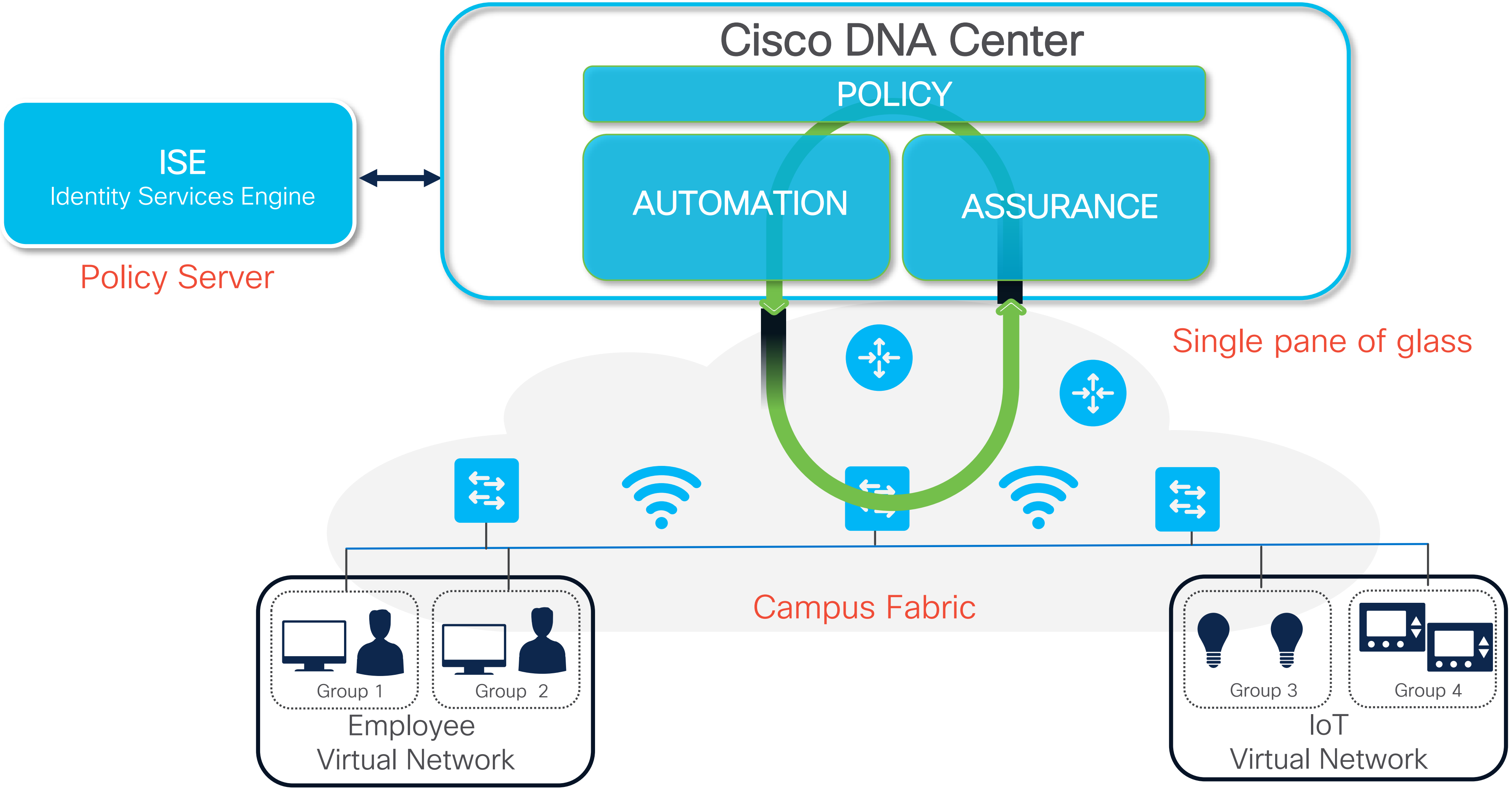
Fabric Overlay – Services plane

- Dynamically connects Users/Devices/Things
- End to End Policies and Segmentation
- Homogeneous – Easy to automate

Fabric Underlay – Forwarding plane

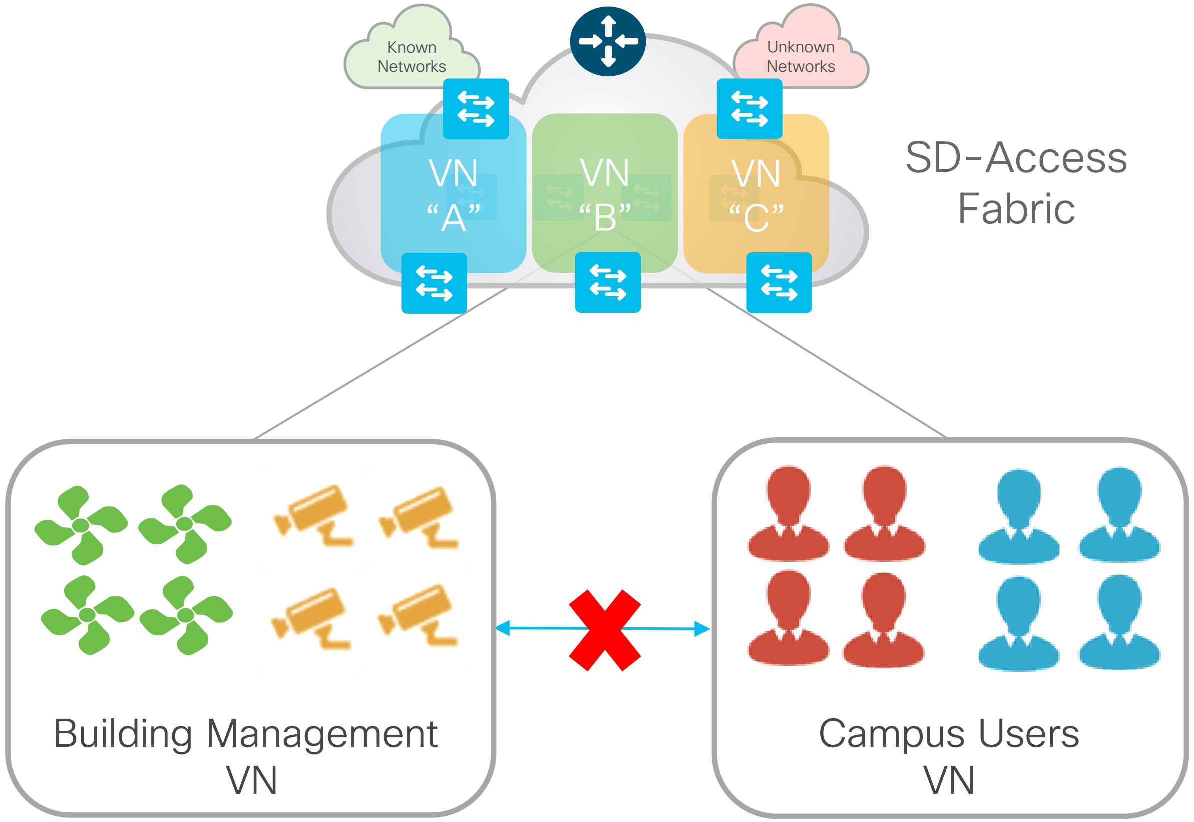
- Connects the network elements to each other
- Optimized for traffic forwarding (resiliency, performance)
- Homogeneous – Easy to automate

Cisco SD-Access architecture



SD-Access Policy – Two Level Hierarchy

Macro Level

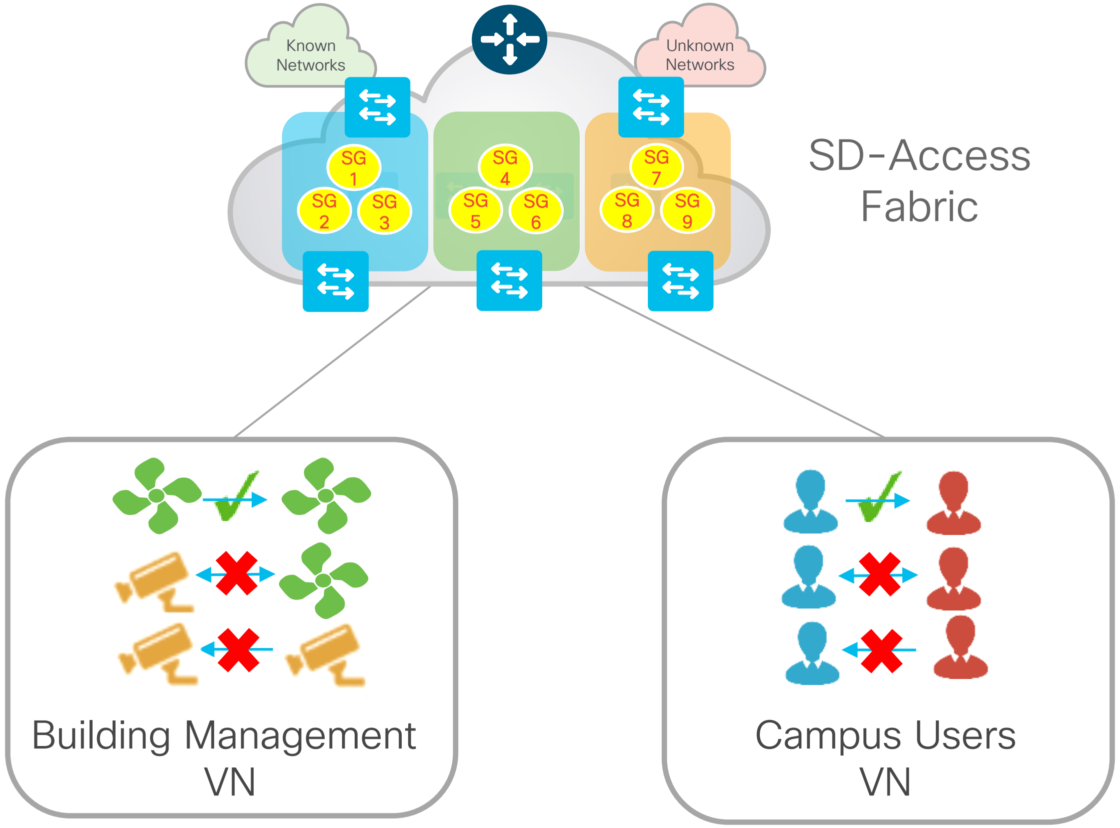


SD-Access Fabric

Building Management VN

Campus Users VN

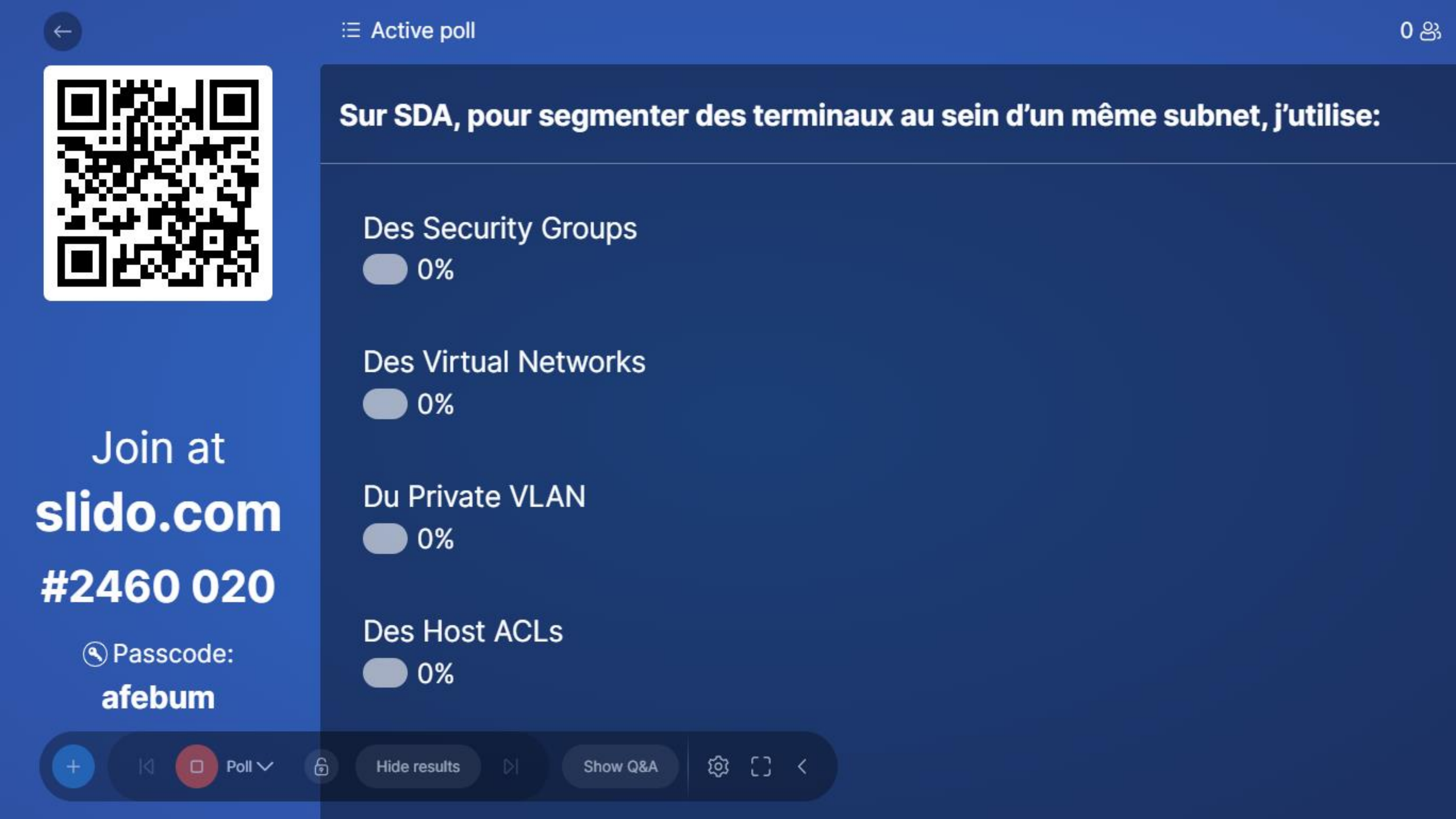
Micro Level



SD-Access Fabric

Building Management VN

Campus Users VN



Sur SDA, pour segmenter des terminaux au sein d'un même subnet, j'utilise:

Des Security Groups
0%

Des Virtual Networks
0%

Du Private VLAN
0%

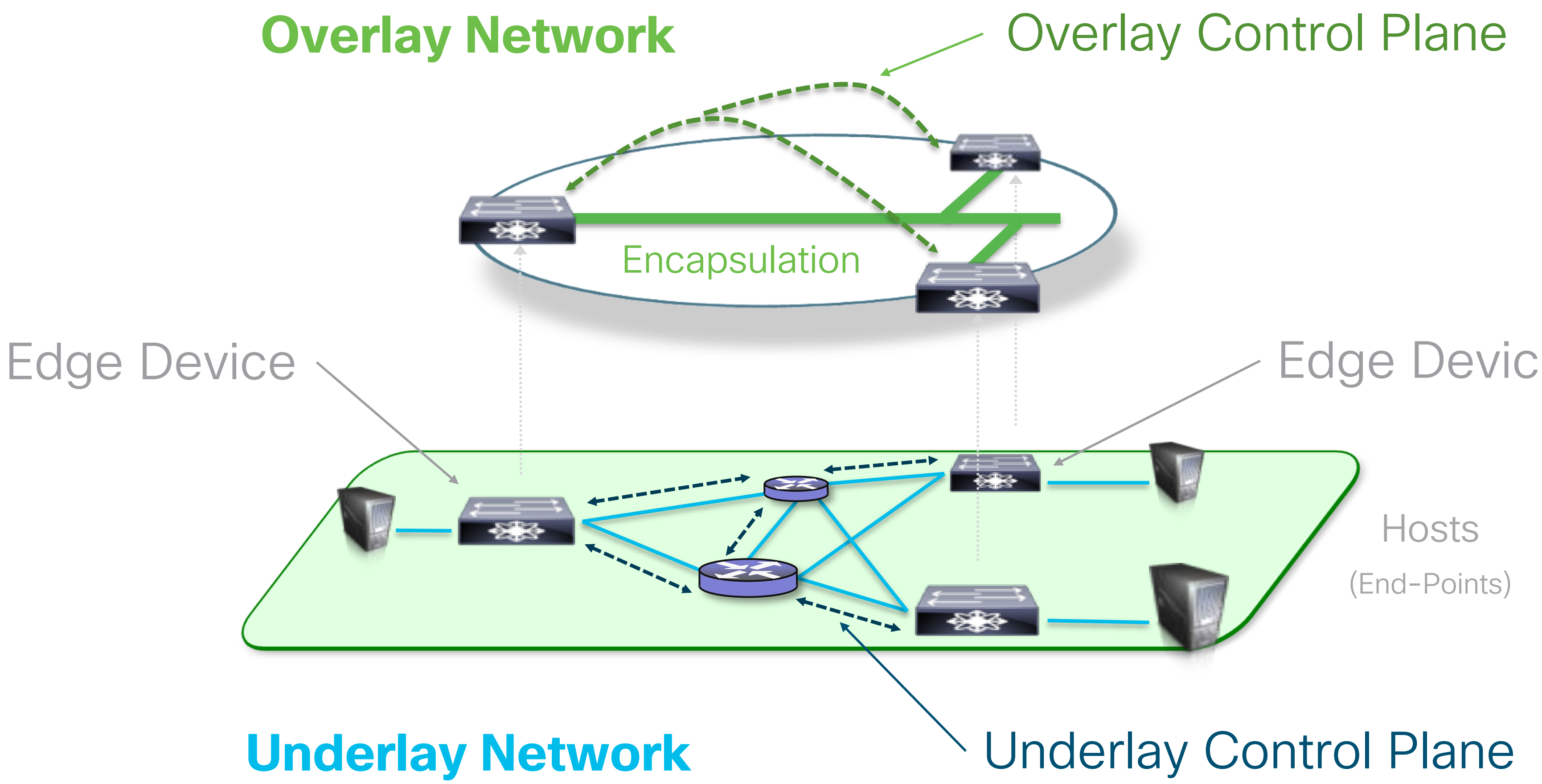
Des Host ACLs
0%

Join at
slido.com
#2460 020

Passcode:
afebum

Fondamentaux techniques

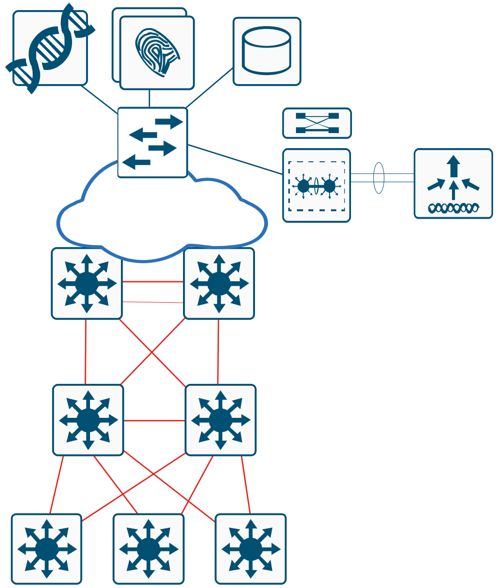
Cisco SD-Access Fundamentals



What are the options to build the Underlay?

Manual Underlay

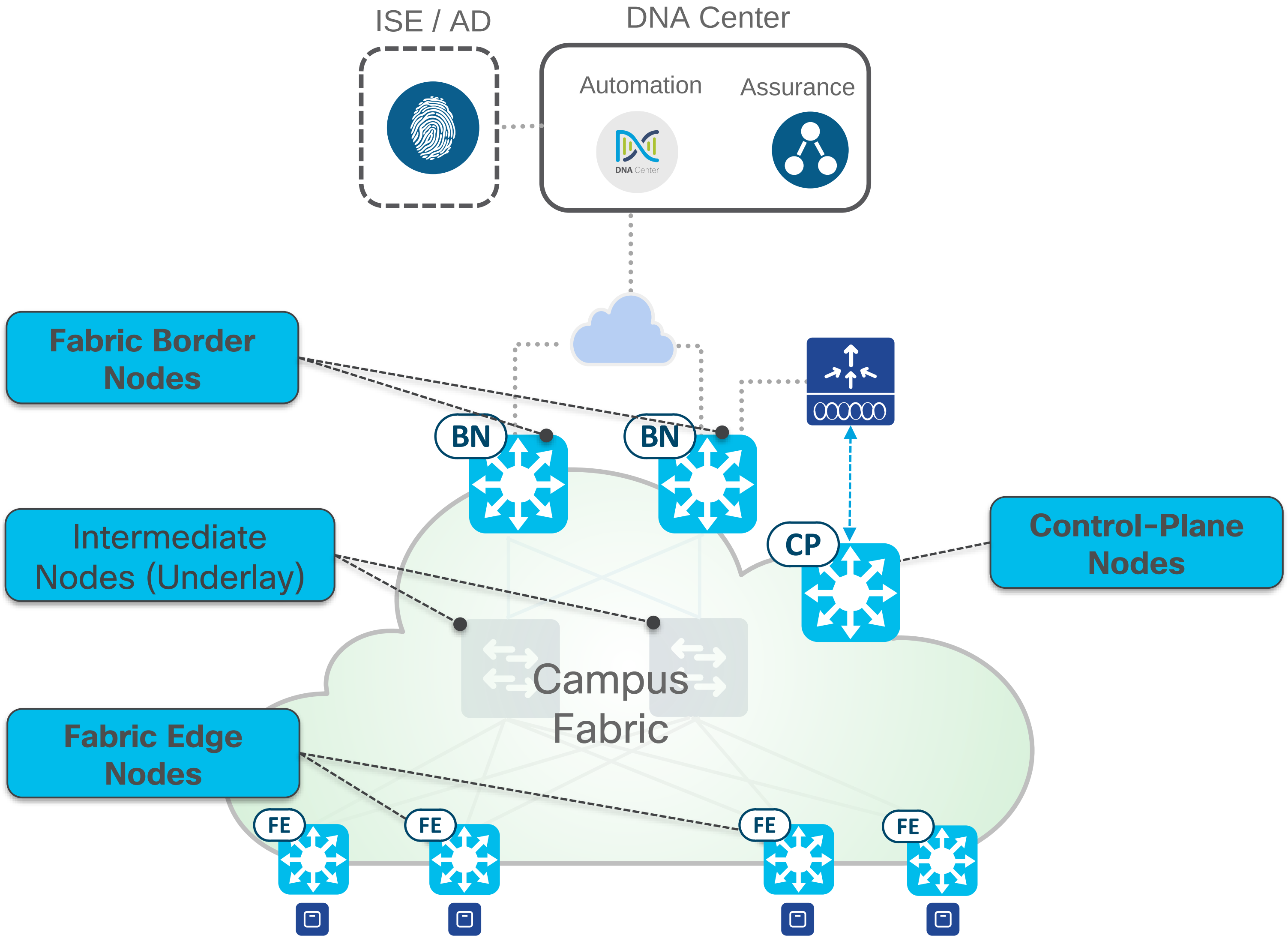
- Any Routed Network
- System MTU: 9100
- Loopback 0 with /32 subnet
- Resiliency – BFD, ECMP, NSF
- Multicast – ASM/SSM, sparse-mode
- CLI, SNMP credentials
- Discover & Manage network device
- Upgrade Software version



Automated Underlay

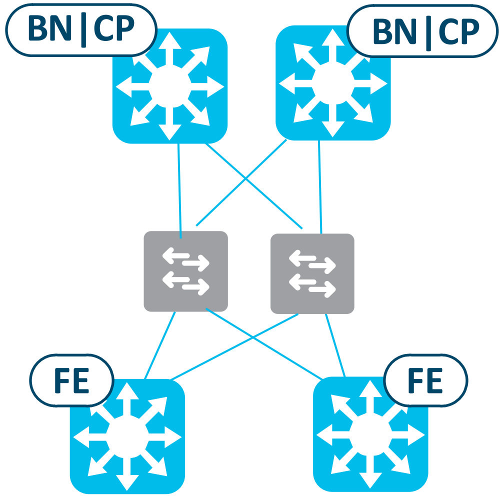
- Discover Seed Device
- Input IP Address Pool
- Start LAN Automation
  - ✓ Discover the network device
  - ✓ Onboard the network device
  - ✓ Upgrade software
- Stop LAN Automation
  - ✓ Complete Configuration (L3 interface, IS-IS)
  - ✓ Manage Device in Cisco DNAC-Center

Cisco SD-Access Fabric Roles

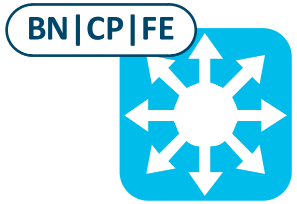


Cisco SD-Access Fabric Roles

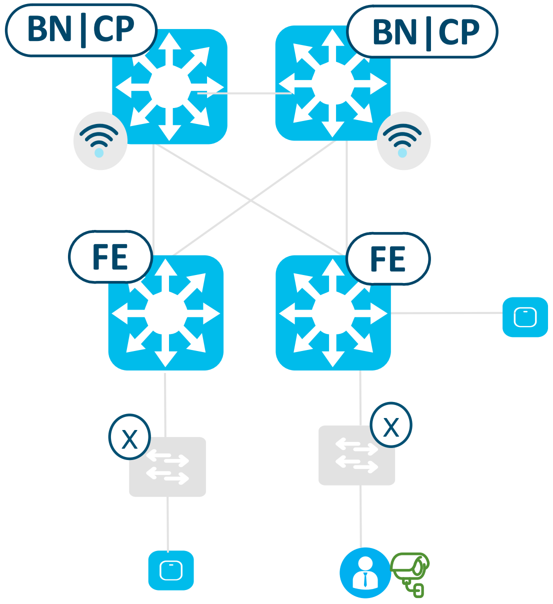
One device can perform more than one function.



Co-located BN/CP



Fabric in a Box (FIAB)

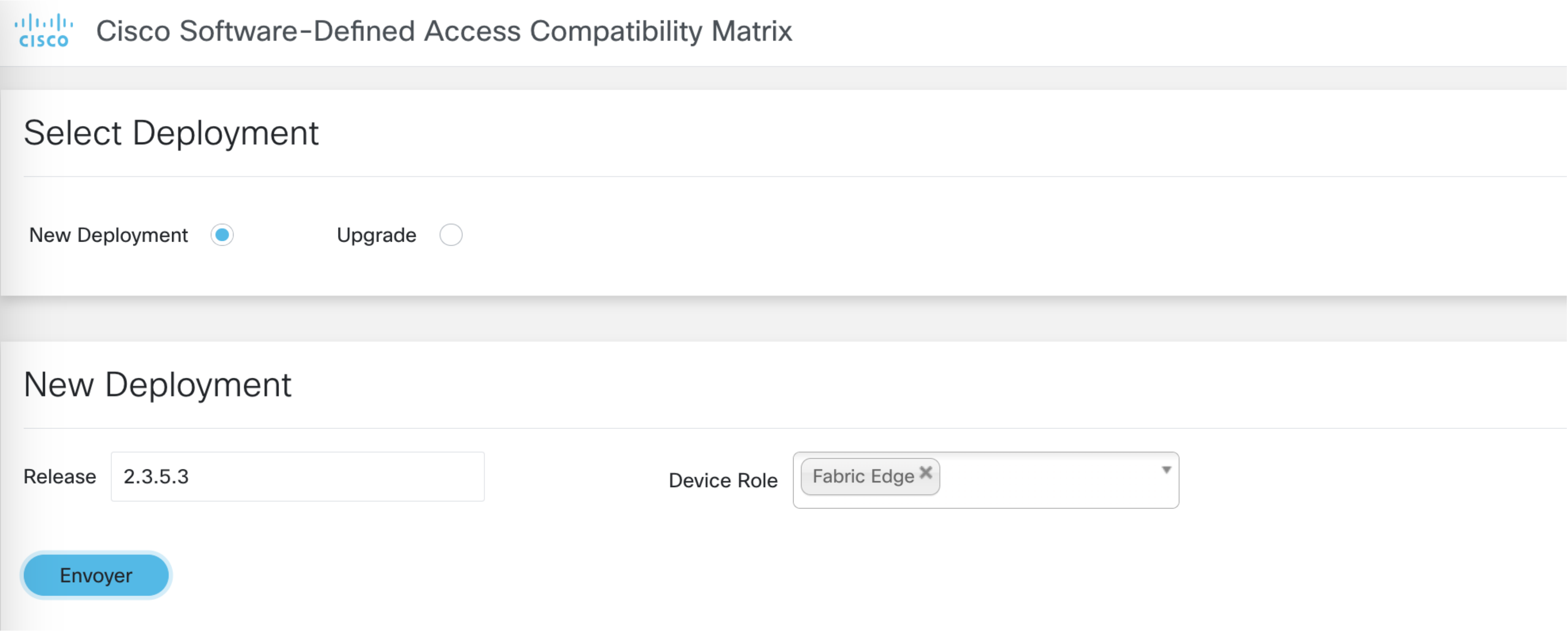


Embedded Wireless

Want to know supported devices ?

Use Compatibility Matrix !

cs.co/sda-compatibility-matrix



Cisco Software-Defined Access Compatibility Matrix

Select Deployment

New Deployment ● Upgrade ○

New Deployment

Release: 2.3.5.3

Device Role: Fabric Edge

SD-Access Fabric technologies

LISP based Control-Plane

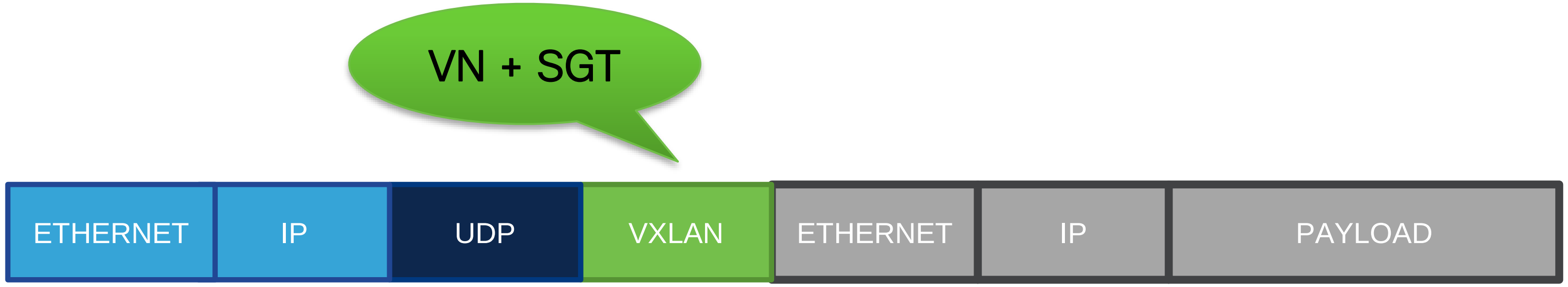
RFC6830 – RFC6831 – RFC6832 – RFC6833 – RFC6834 – RFC6835 – RFC6836 – RFC7052 – RFC 7215
RFC7834 – RFC7835 – RFC7954 – RFC7955 – RFC8060 – RFC8061 – RFC8011 – RFC8013

VXLAN based Data-Plane

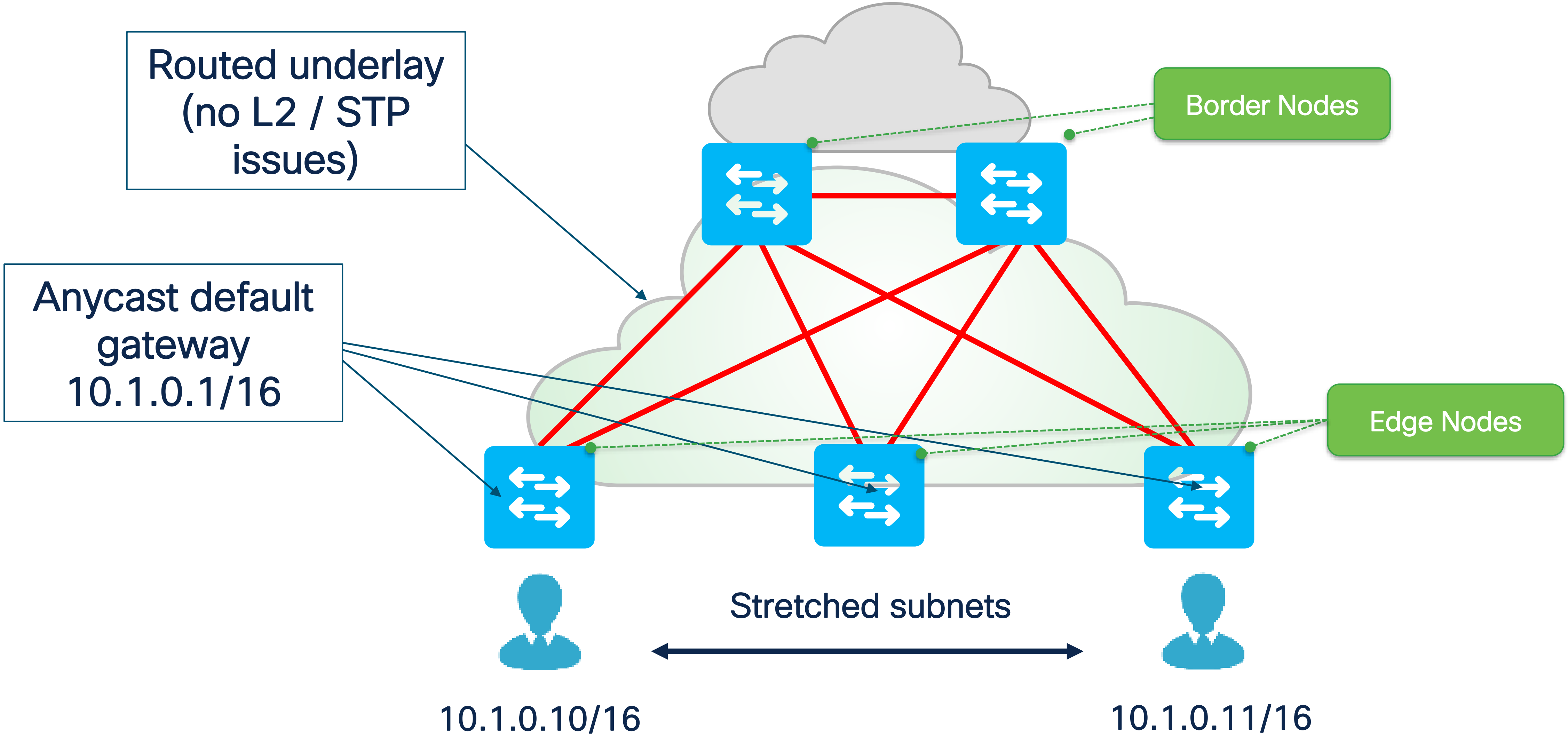
RFC7348

Trustsec based Policy-Plane

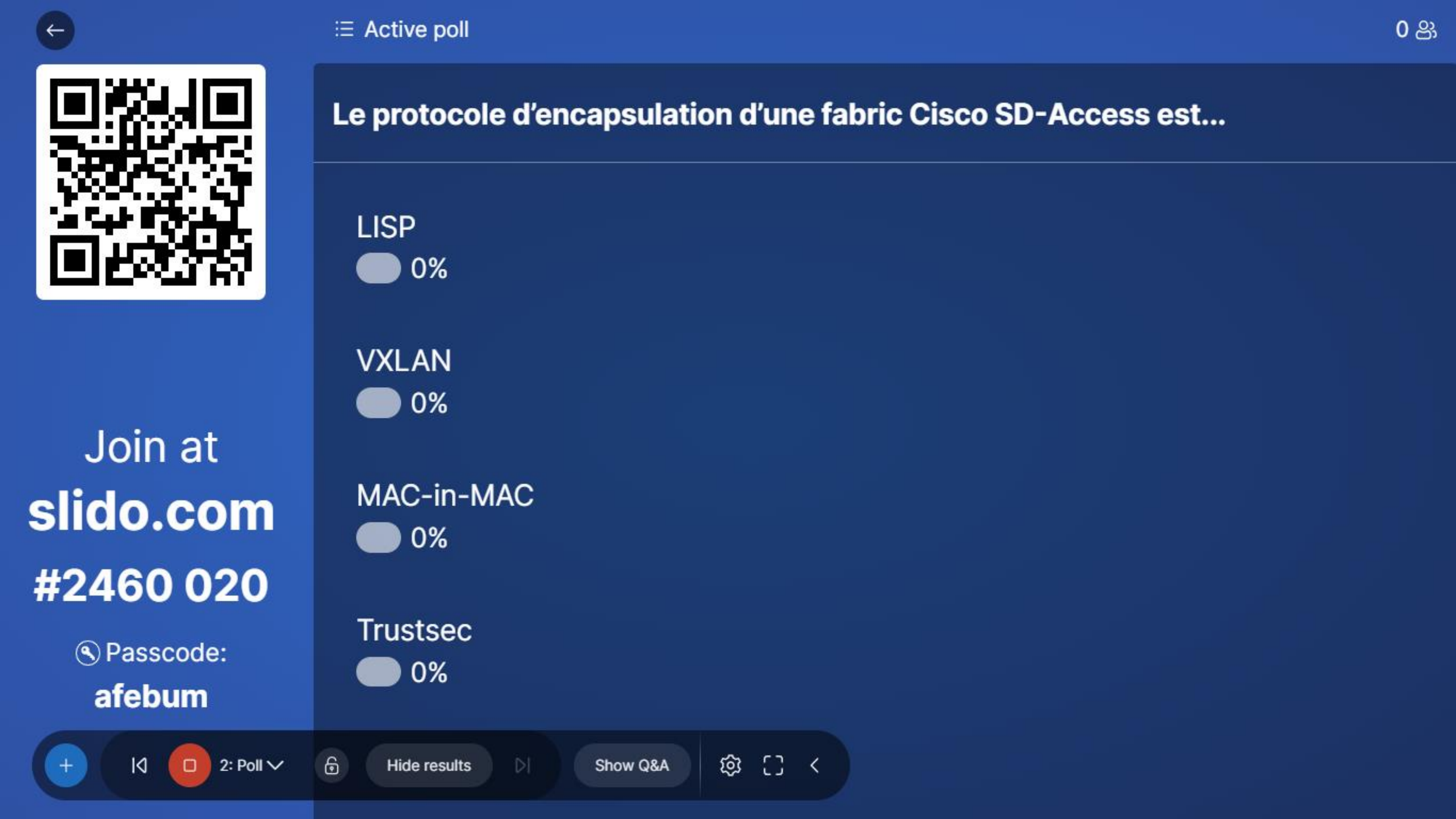
draft-smith-vxlan-group-policy-05 - draft-smith-kandula-sxp-06



Fabric Enables any subnet anywhere



Routed underlay (no L2 / STP issues)
Anycast default gateway 10.1.0.1/16
Border Nodes
Edge Nodes
Stretched subnets
10.1.0.10/16
10.1.0.11/16



Le protocole d’encapsulation d’une fabric Cisco SD-Access est...

LISP
0%

VXLAN
0%

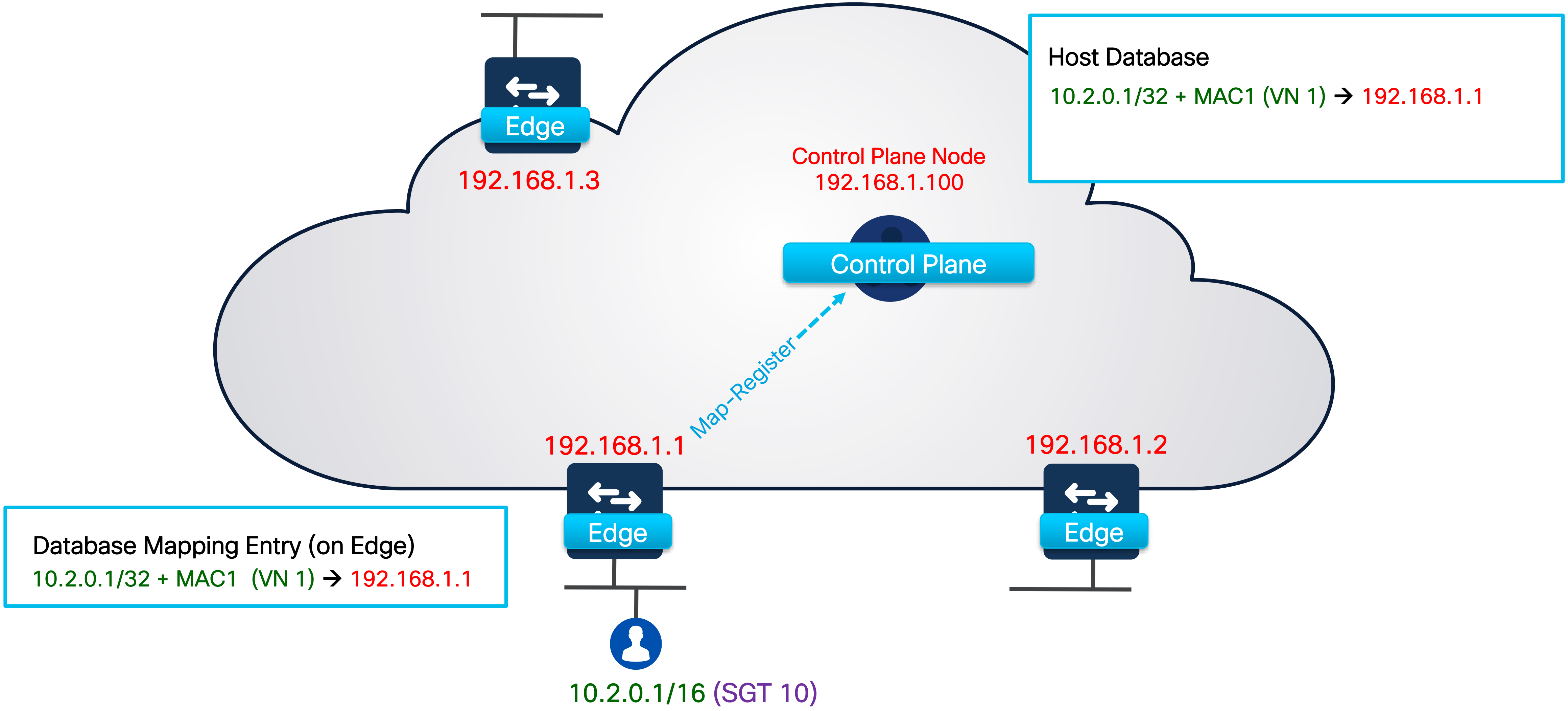
MAC-in-MAC
0%

Trustsec
0%

Join at
slido.com
#2460 020

Passcode:
afebum

Sous le capot d’une fabric SD-Access

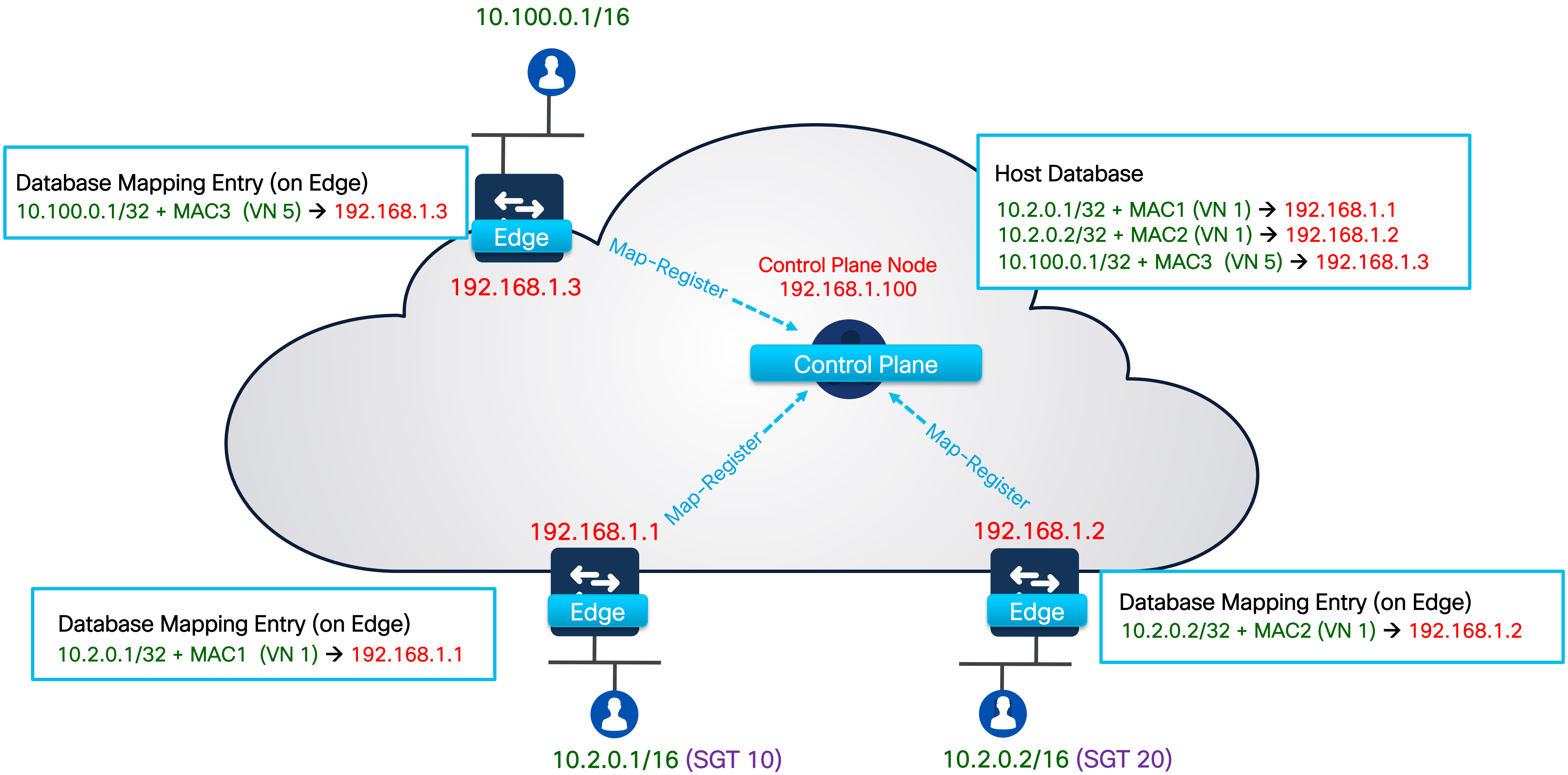


Host Database

10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1

Database Mapping Entry (on Edge)

10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1



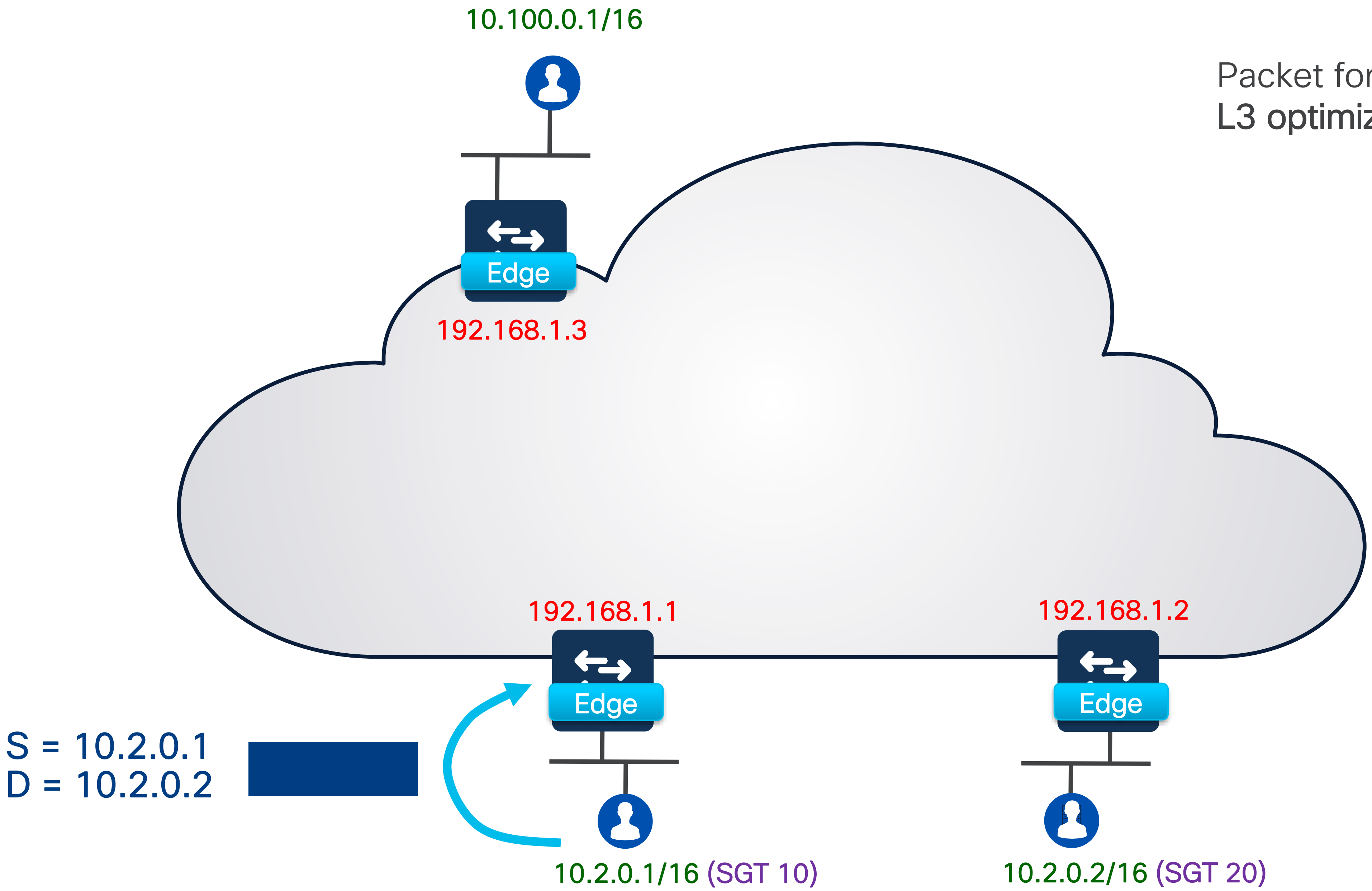
Database Mapping Entry (on Edge)
10.100.0.1/32 + MAC3 (VN 5) → 192.168.1.3

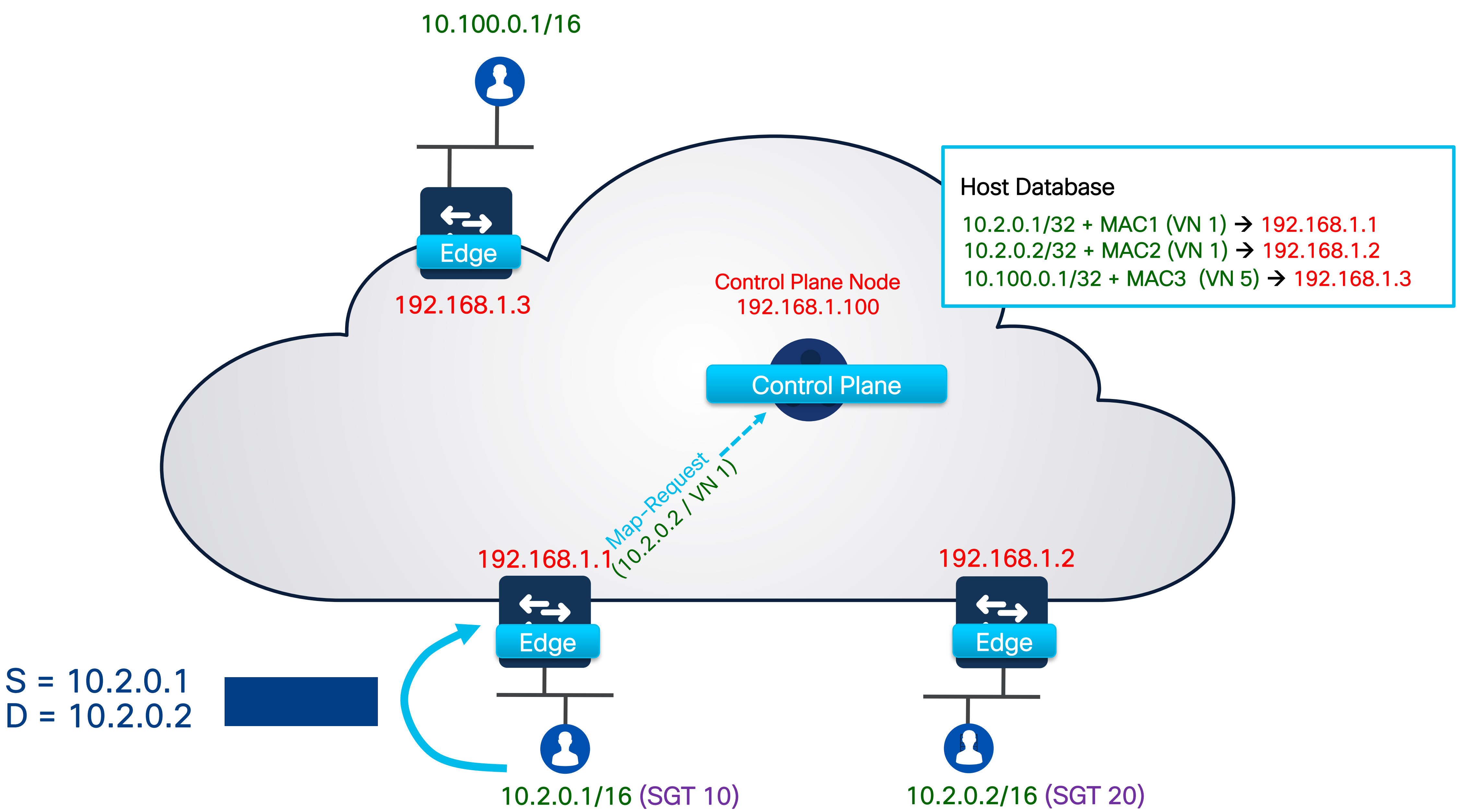
Host Database
10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1
10.2.0.2/32 + MAC2 (VN 1) → 192.168.1.2
10.100.0.1/32 + MAC3 (VN 5) → 192.168.1.3

Database Mapping Entry (on Edge)
10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1

Database Mapping Entry (on Edge)
10.2.0.2/32 + MAC2 (VN 1) → 192.168.1.2

Packet forwarding
L3 optimized





10.100.0.1/16

Edge

192.168.1.3

Control Plane Node
192.168.1.100

Control Plane

Map-Request
(10.2.0.2 / VN 1)

192.168.1.1

Edge

192.168.1.2

Edge

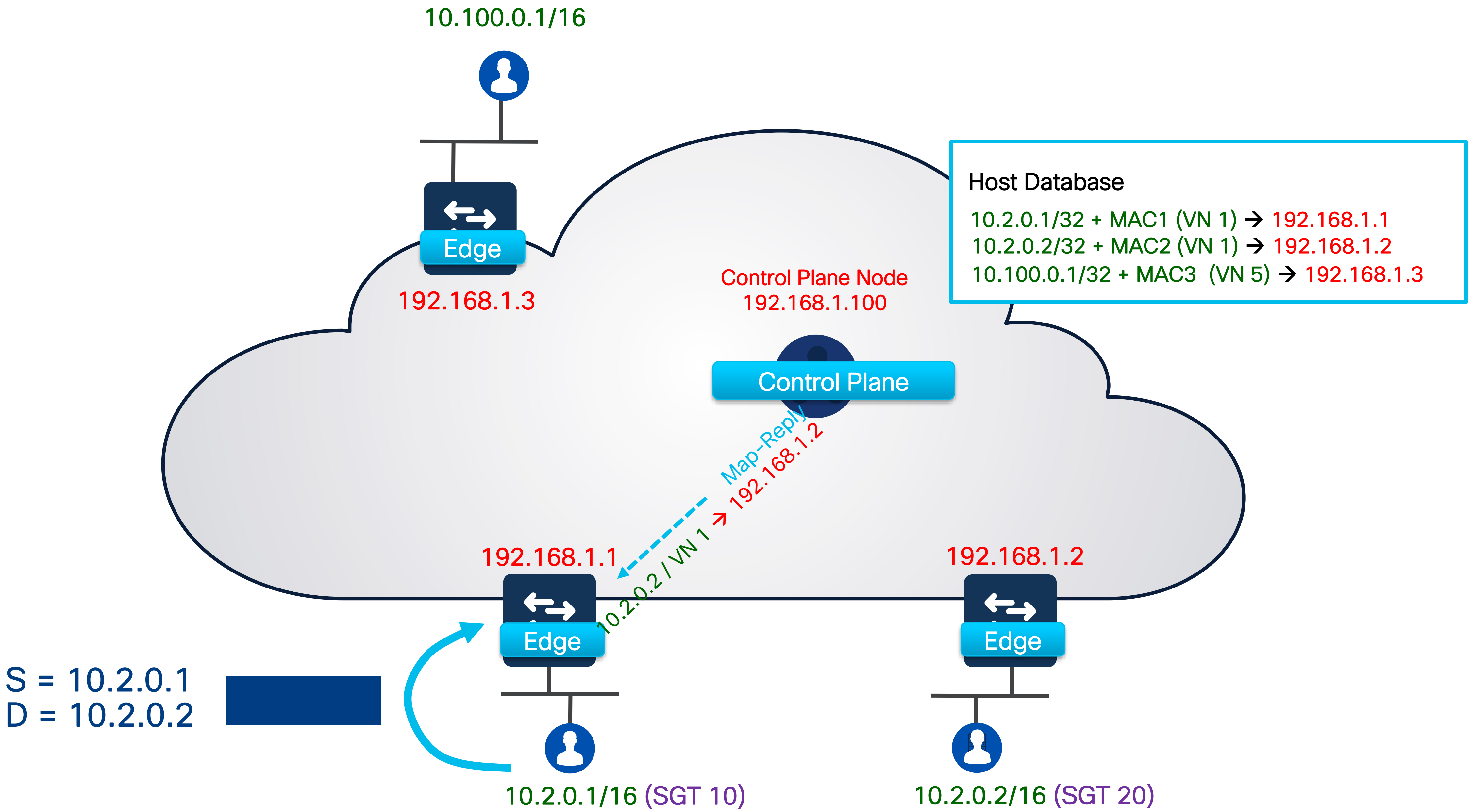
S = 10.2.0.1
D = 10.2.0.2

10.2.0.1/16 (SGT 10)

10.2.0.2/16 (SGT 20)

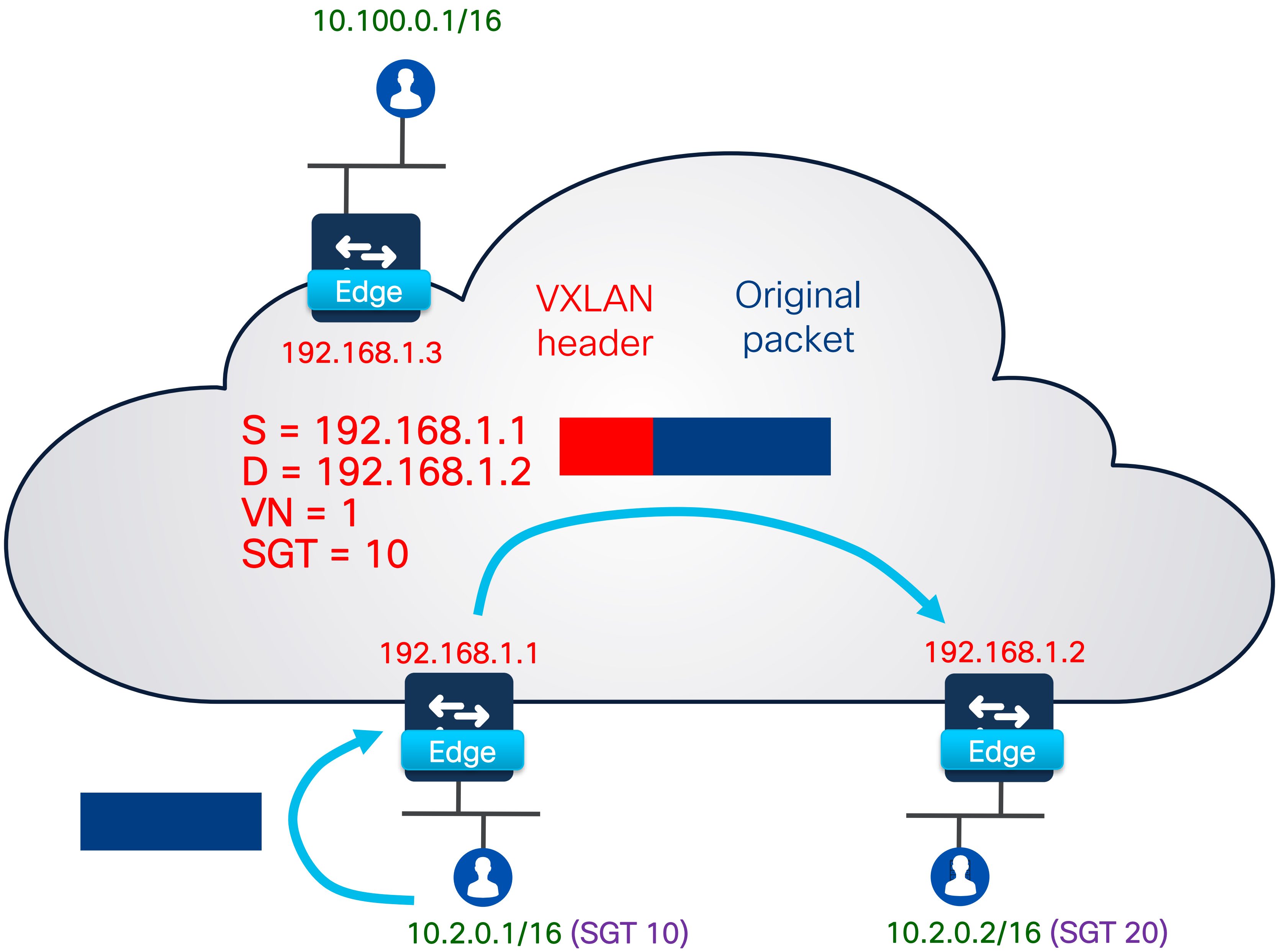
Host Database

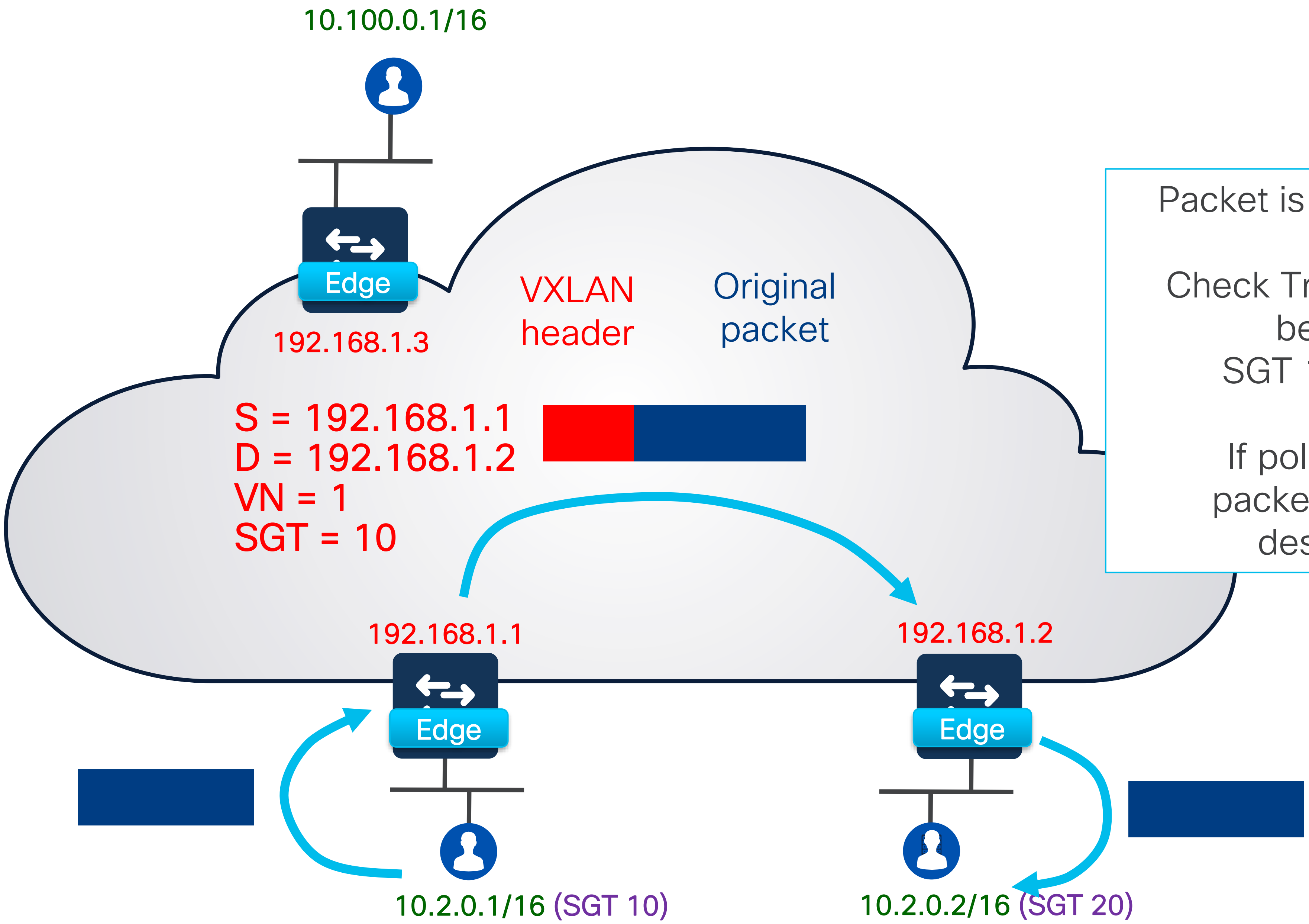
10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1
10.2.0.2/32 + MAC2 (VN 1) → 192.168.1.2
10.100.0.1/32 + MAC3 (VN 5) → 192.168.1.3



Host Database

10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1
10.2.0.2/32 + MAC2 (VN 1) → 192.168.1.2
10.100.0.1/32 + MAC3 (VN 5) → 192.168.1.3


10.100.0.1/16
Edge
192.168.1.3
VXLAN
header
Original
packet
S = 192.168.1.1
D = 192.168.1.2
VN = 1
SGT = 10
192.168.1.1
Edge
192.168.1.2
Edge
10.2.0.1/16 (SGT 10)
10.2.0.2/16 (SGT 20)

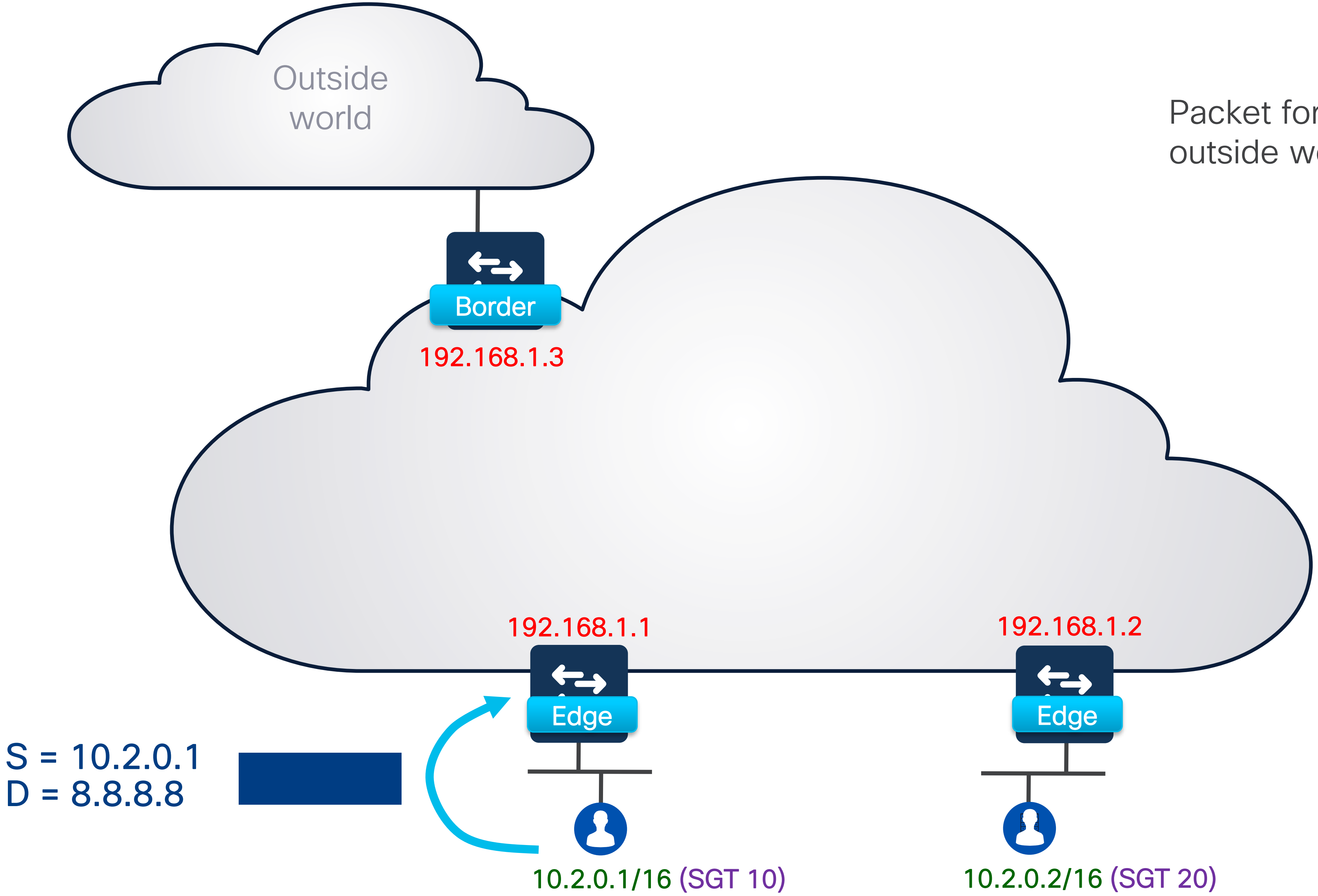


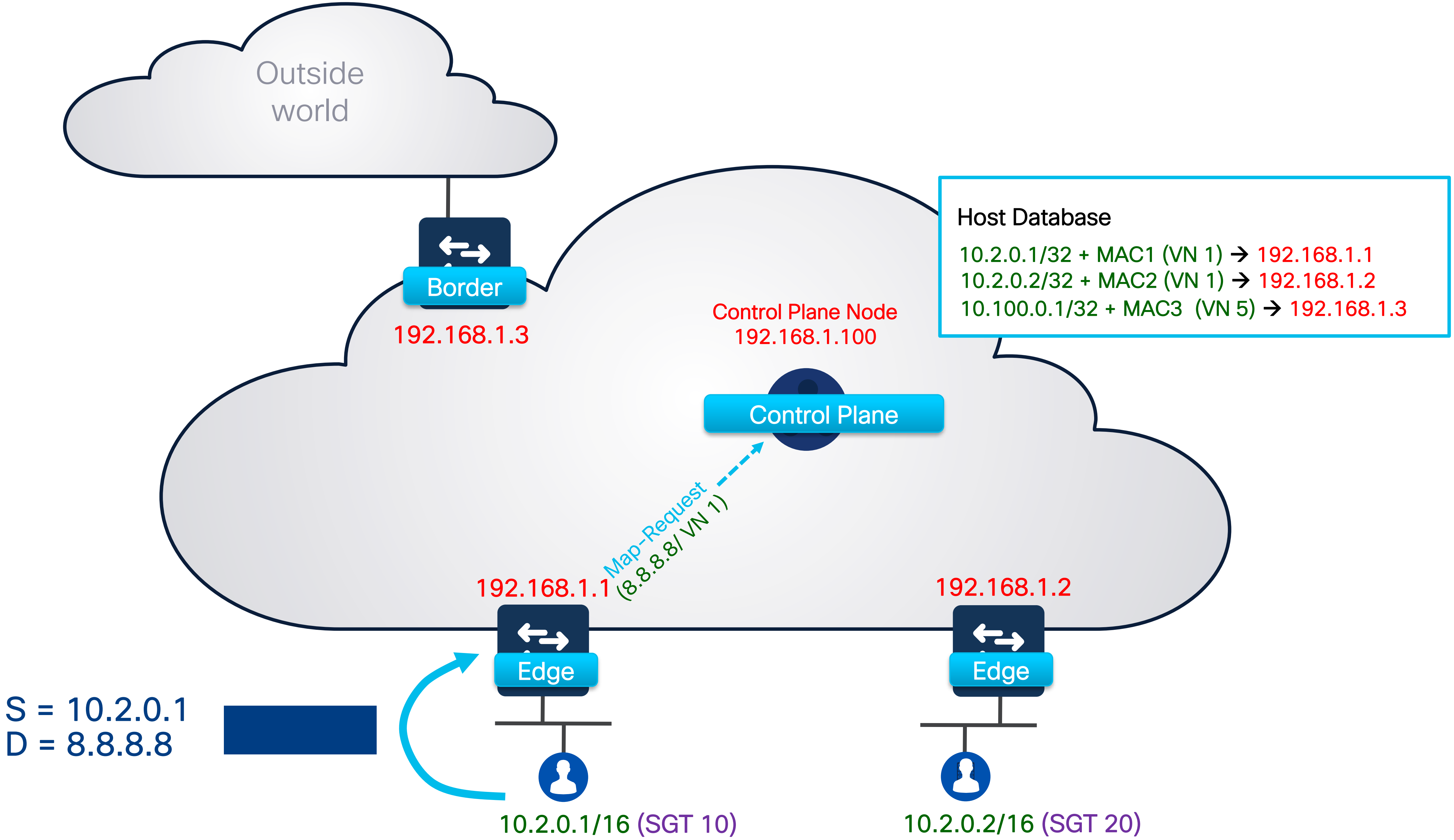
Packet is decapsulated

Check Trustsec policy between SGT 10 and 20

If policy allows packet is sent to destination

Packet forwarding to the outside world

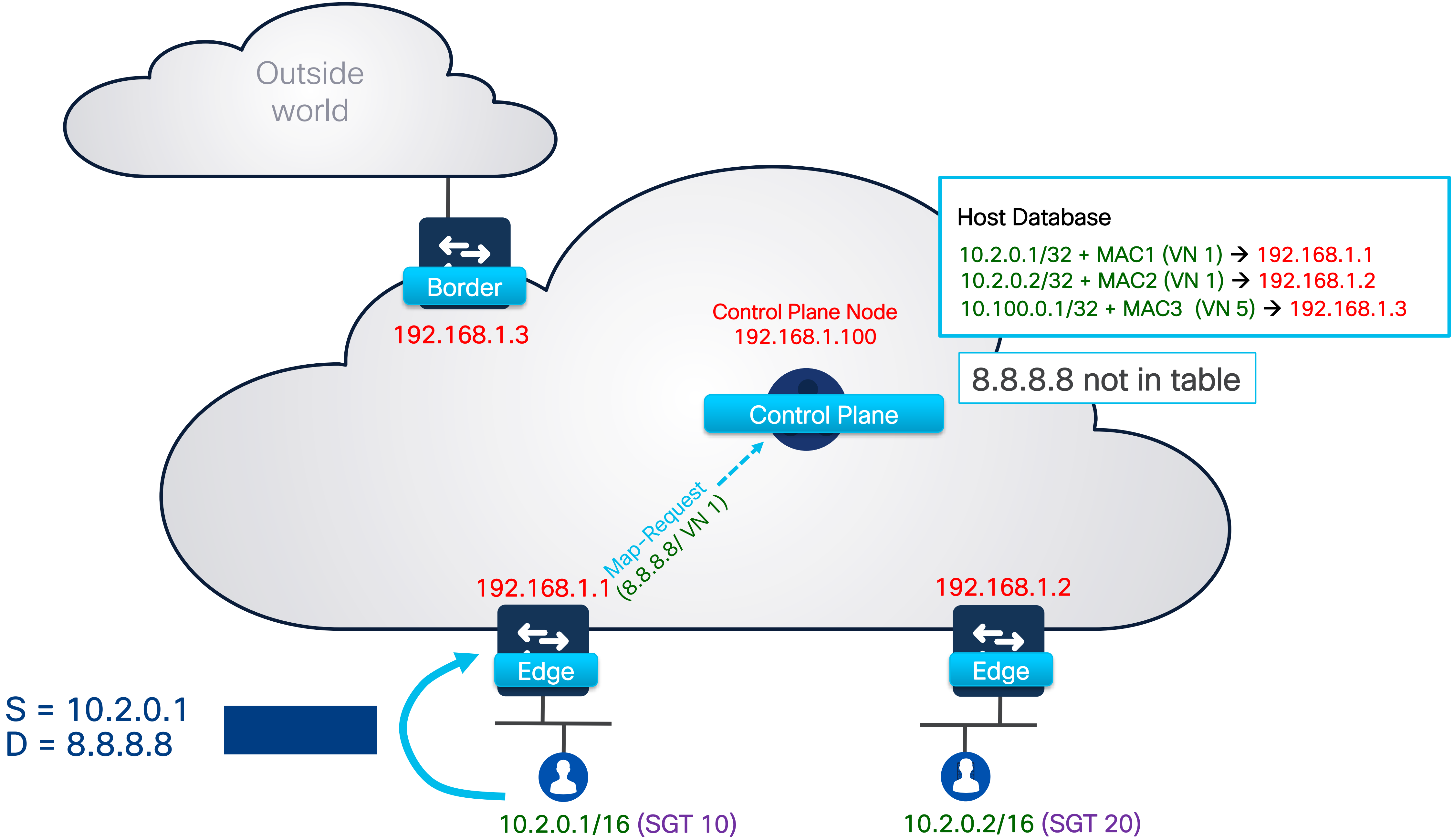




Host Database

10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1
10.2.0.2/32 + MAC2 (VN 1) → 192.168.1.2
10.100.0.1/32 + MAC3 (VN 5) → 192.168.1.3

S = 10.2.0.1
D = 8.8.8.8

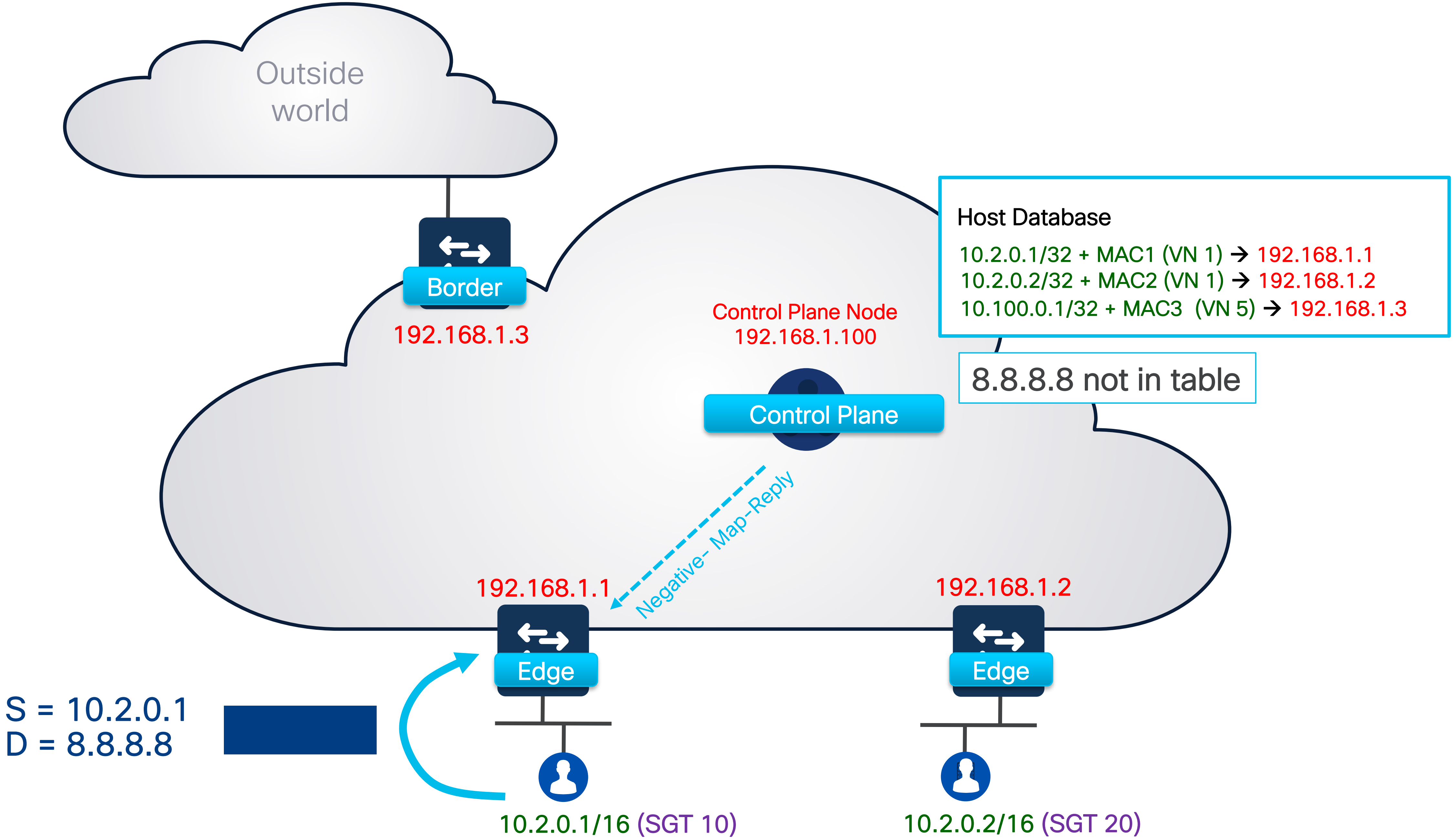


Host Database

10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1
10.2.0.2/32 + MAC2 (VN 1) → 192.168.1.2
10.100.0.1/32 + MAC3 (VN 5) → 192.168.1.3

8.8.8.8 not in table

S = 10.2.0.1
D = 8.8.8.8

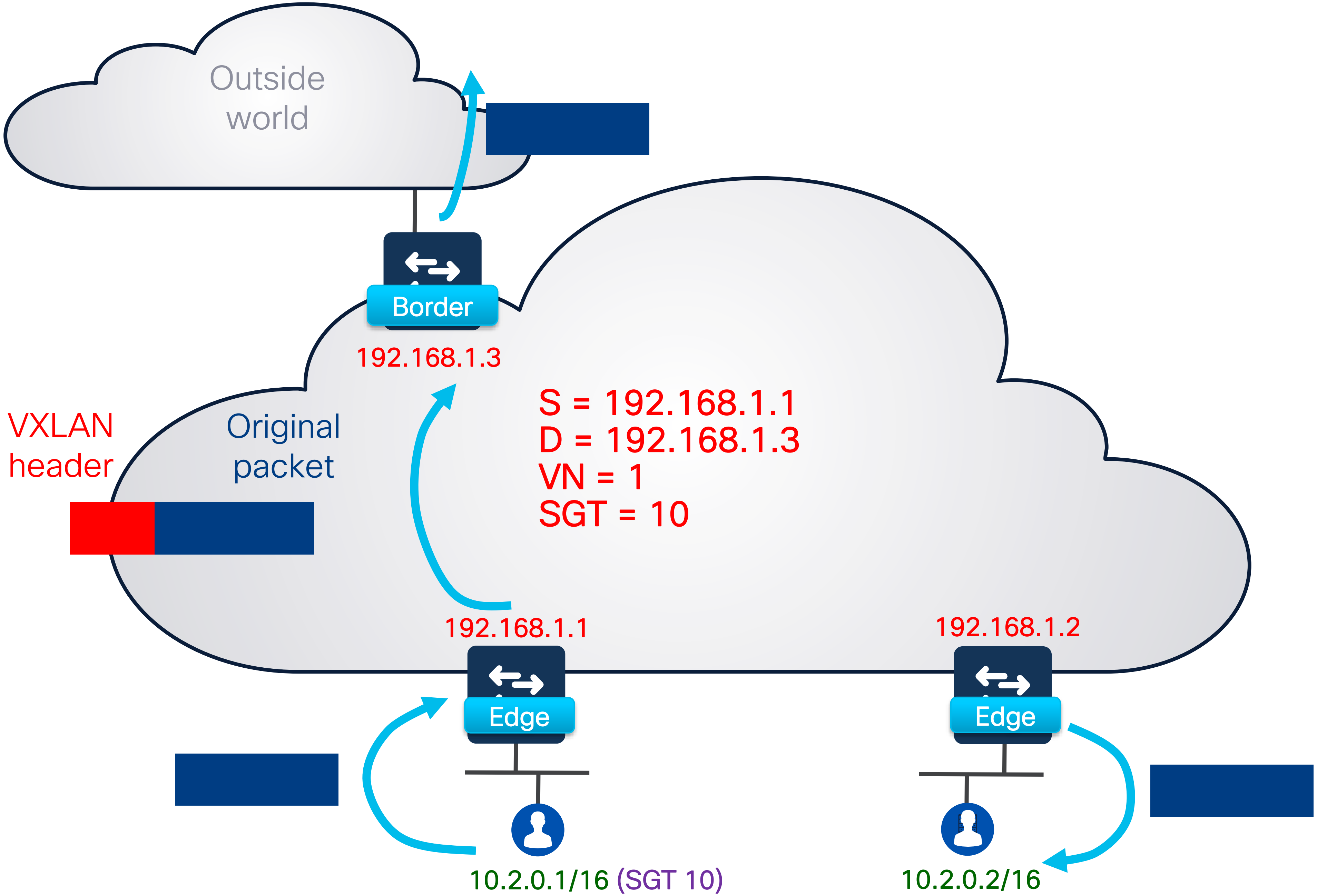


Host Database

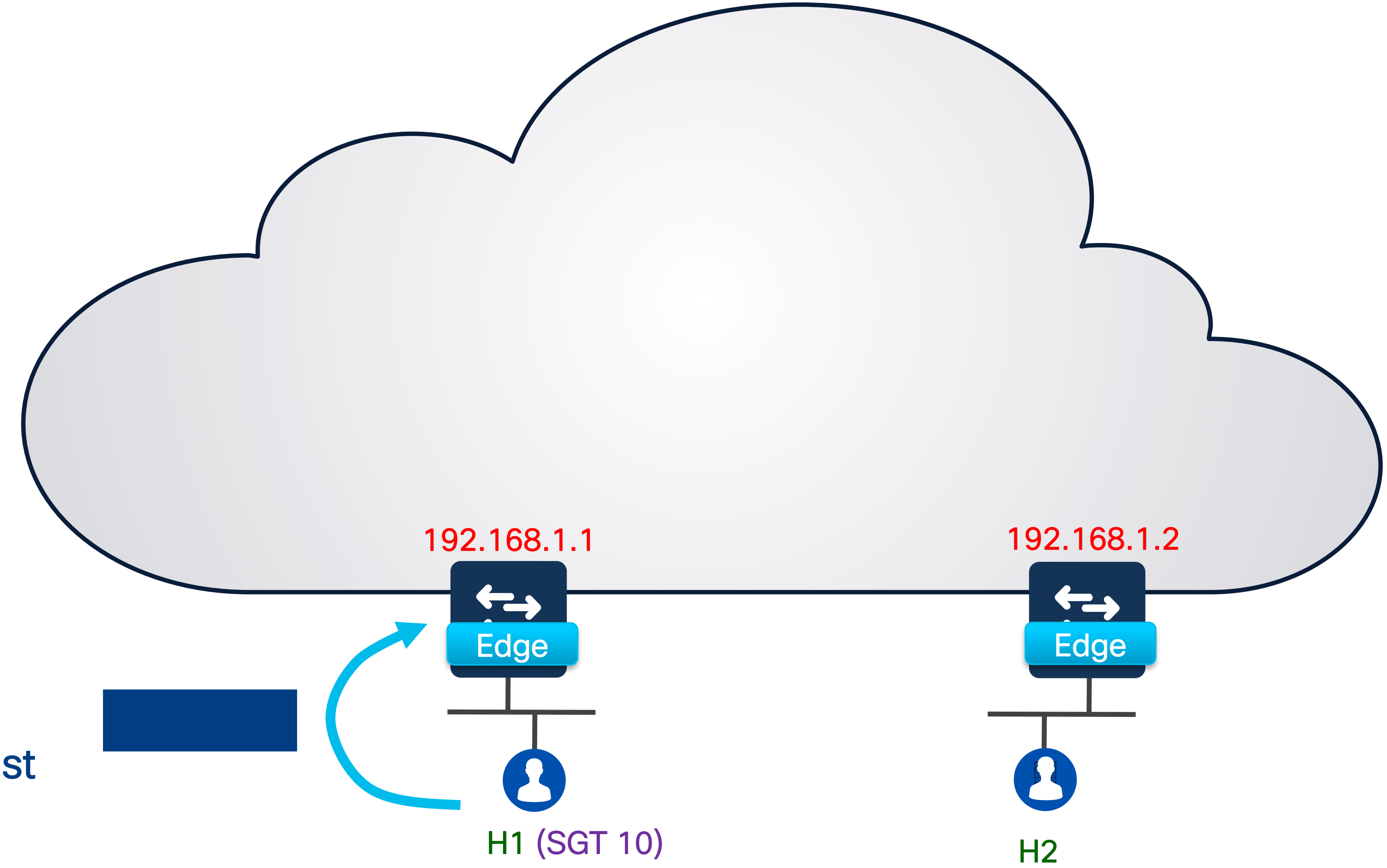
10.2.0.1/32 + MAC1 (VN 1) → 192.168.1.1
10.2.0.2/32 + MAC2 (VN 1) → 192.168.1.2
10.100.0.1/32 + MAC3 (VN 5) → 192.168.1.3

8.8.8.8 not in table

S = 10.2.0.1
D = 8.8.8.8


Outside world
Border
192.168.1.3
VXLAN header
Original packet
S = 192.168.1.1
D = 192.168.1.3
VN = 1
SGT = 10
192.168.1.1
192.168.1.2
Edge
Edge
10.2.0.1/16 (SGT 10)
10.2.0.2/16

Packet forwarding
L2 (default)



ARP

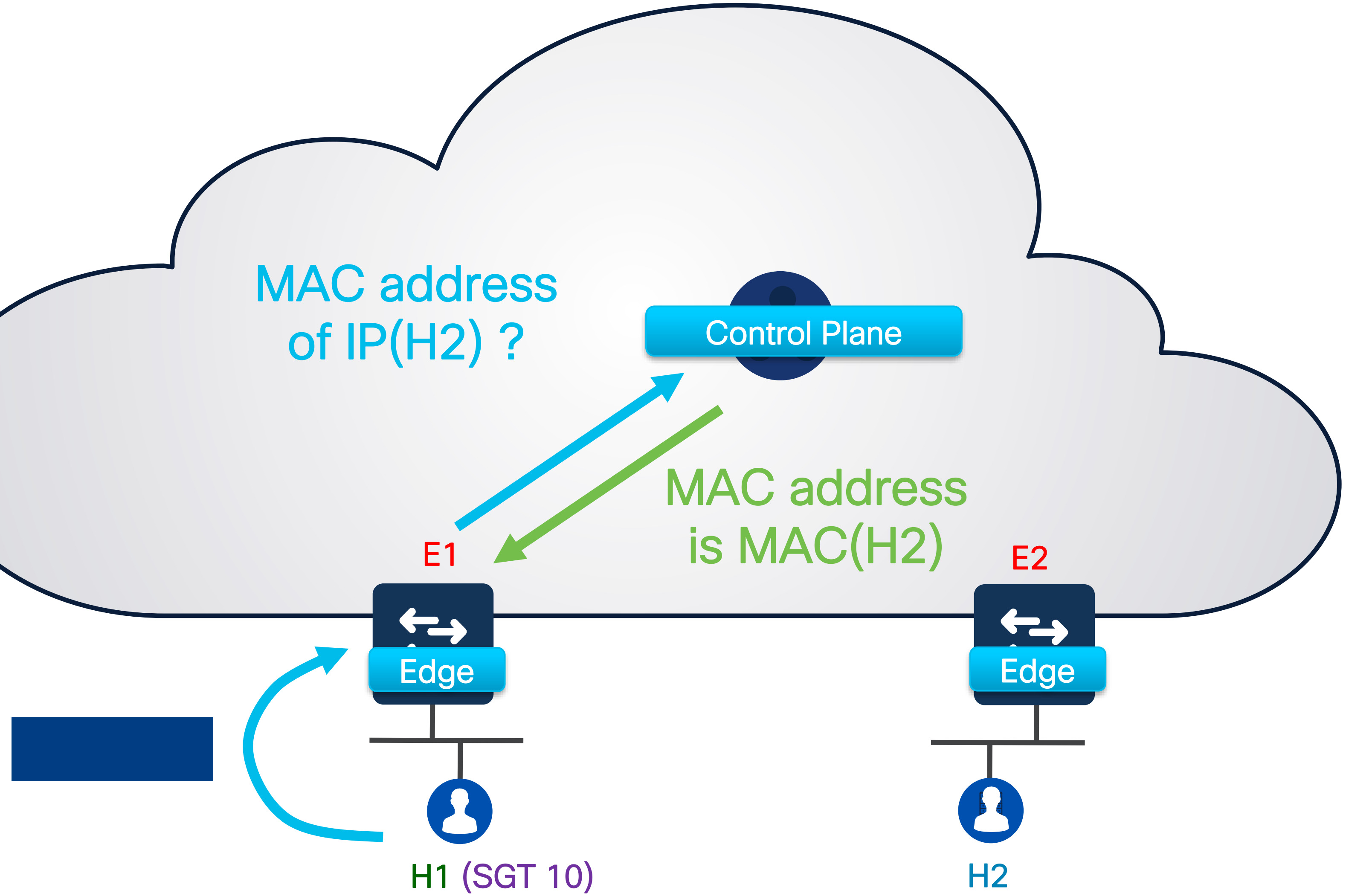
S = MAC1
D = Broadcast

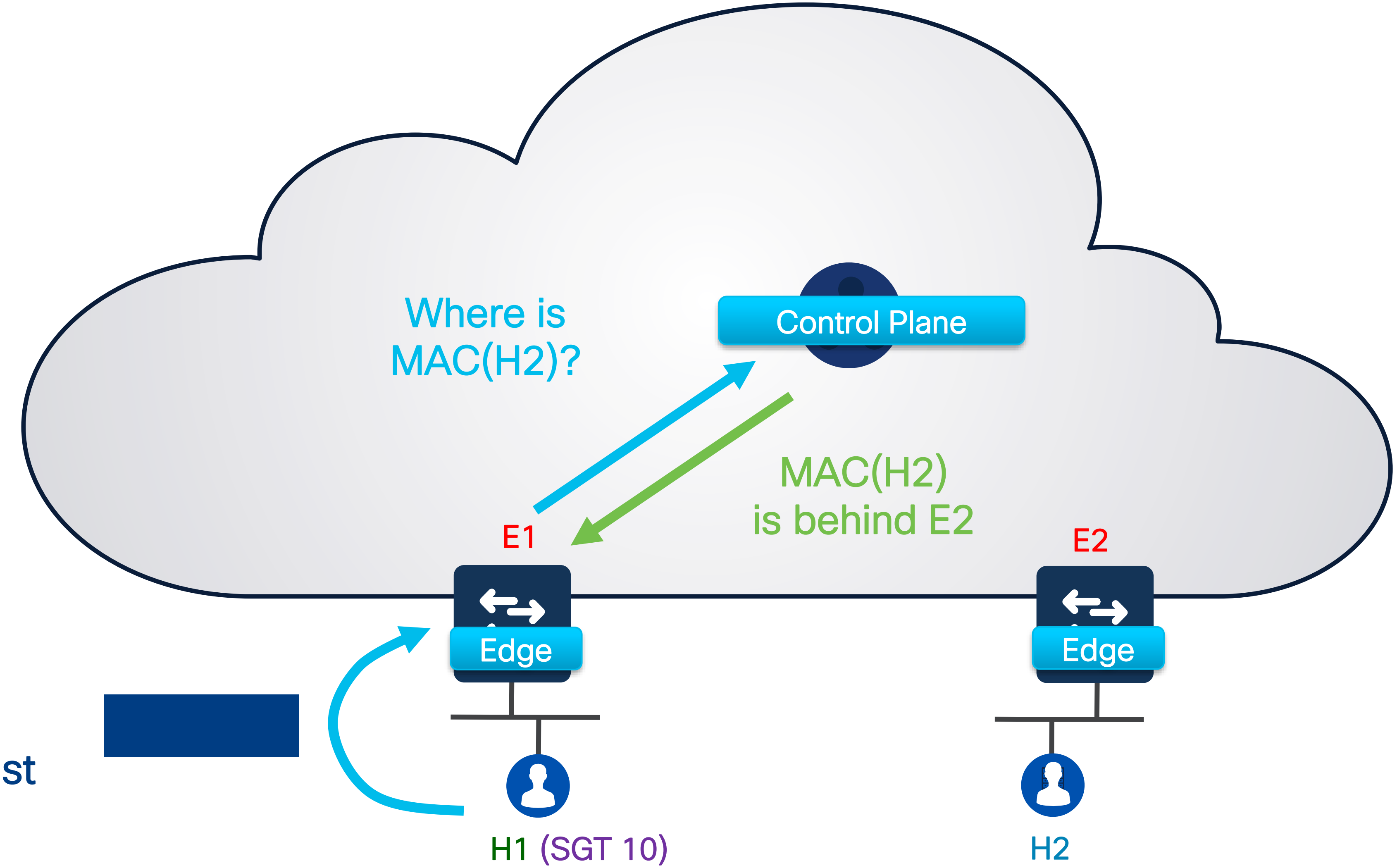
Req = IP2

ARP

S = MAC1
D = Broadcast

Req = IP2

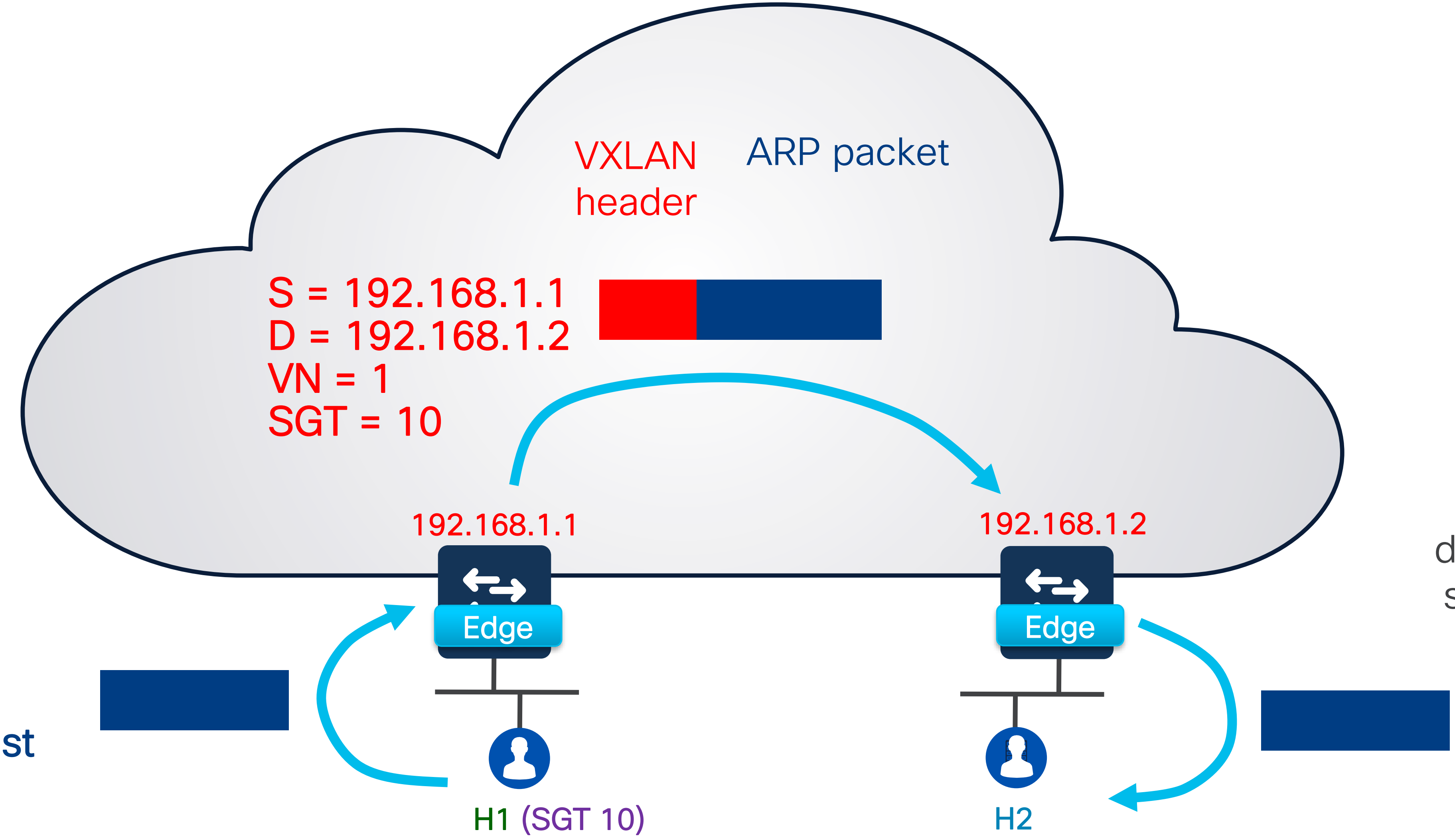




ARP

S = MAC1
D = Broadcast

Req = IP2



VXLAN header

ARP packet

S = 192.168.1.1
D = 192.168.1.2
VN = 1
SGT = 10

192.168.1.1

192.168.1.2

H1 (SGT 10)

H2

ARP

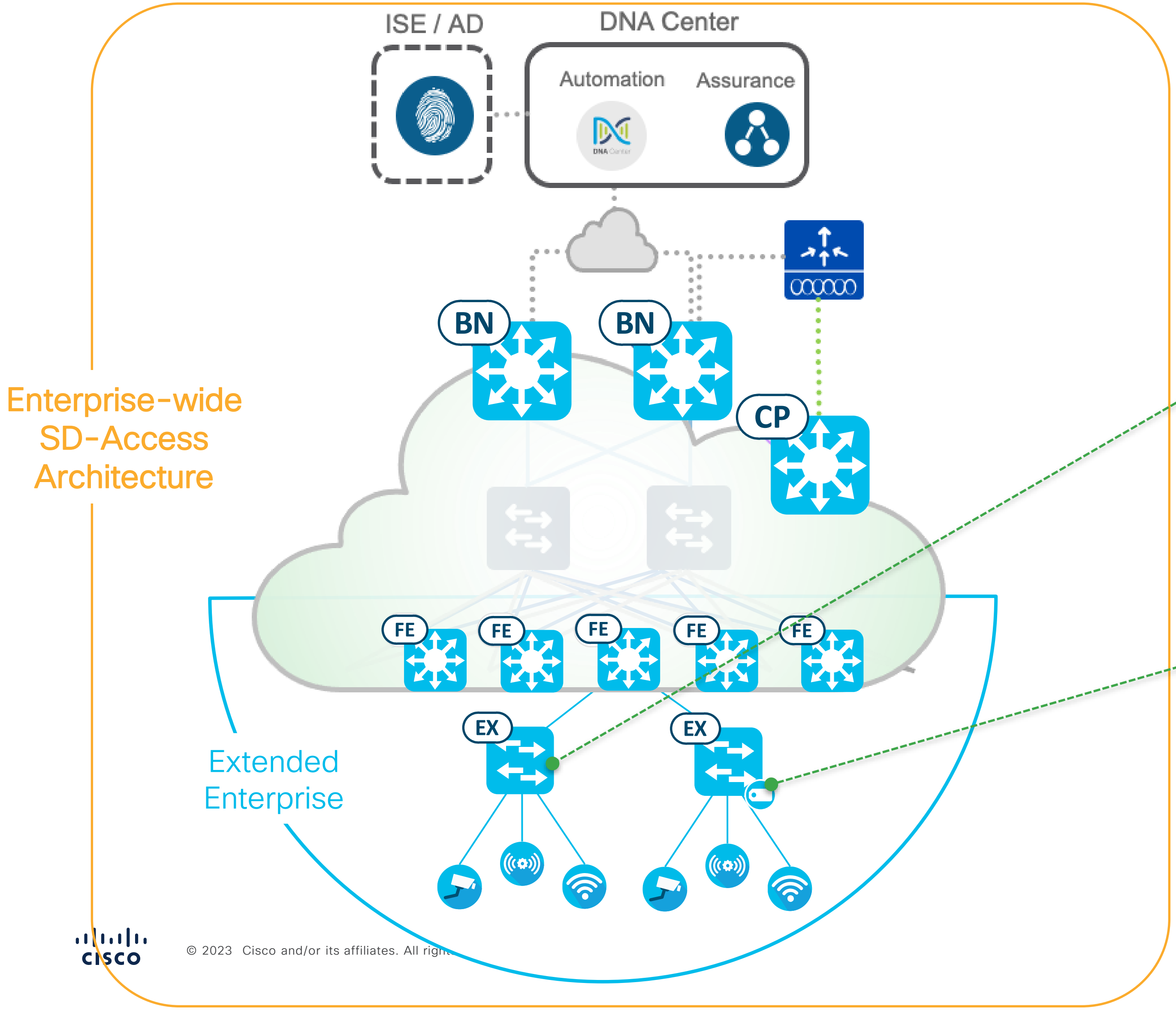
S = MAC1
D = Broadcast

Req = IP2

ARP is decapsulated and sent to MAC(H2)

Refermons le capot...

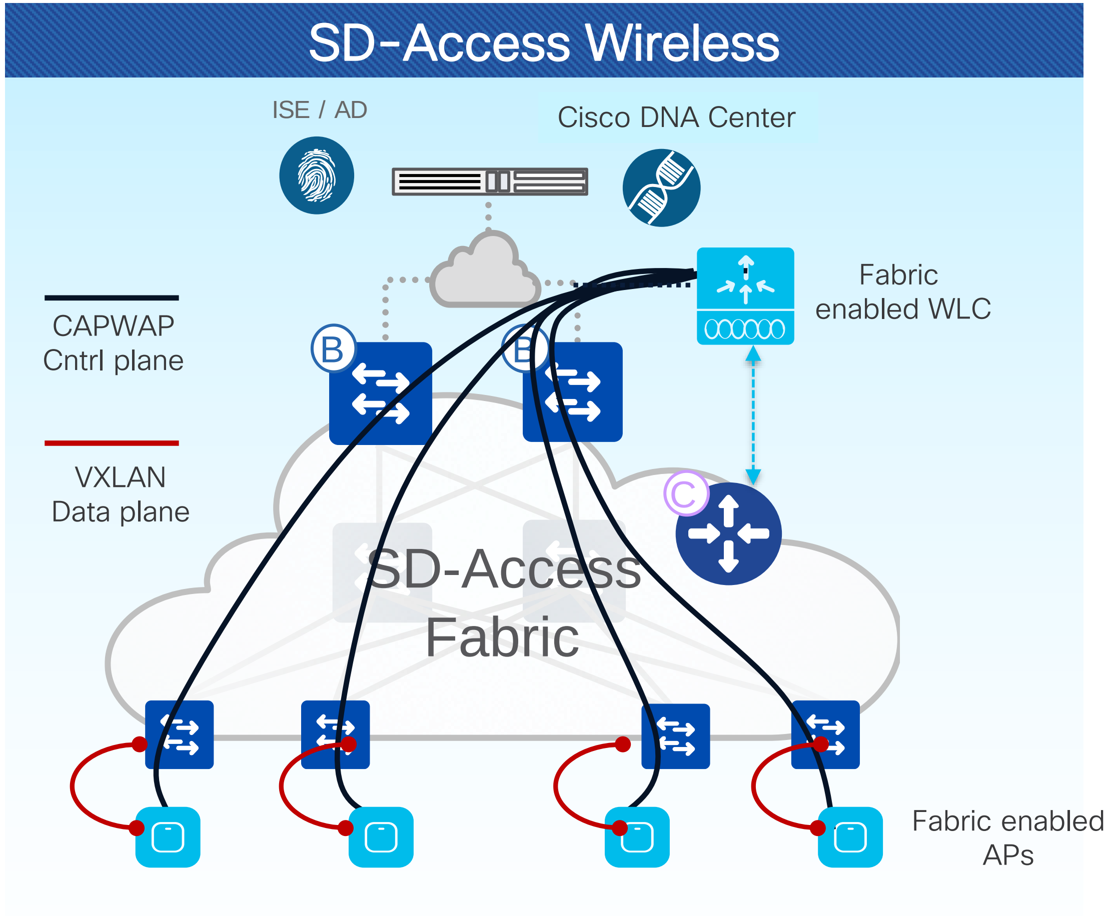
Cisco SDA – Extended Nodes



Extended Node – A Edge access device that connects Wired Endpoint Devices to the SDA Fabric via a Fabric Edge Node

Policy Extended Node – An extended node with Trustsec capabilities

Wireless fully integrated into SDA

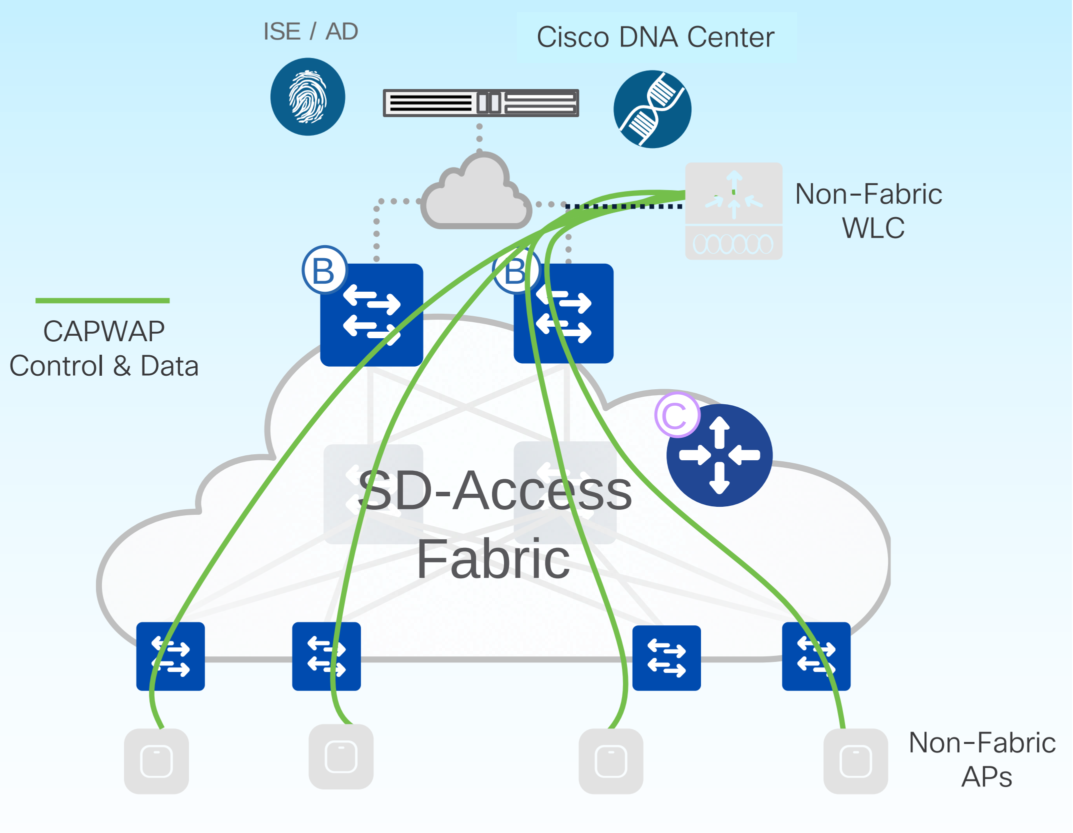


- CAPWAP Control Plane, VXLAN Data plane
- All integrated in Fabric, SD-Access advantages
- Requires software upgrade (8.5+)
- Optimized for 802.11ac Wave 2 and 11ax APs

- True wireless integration with Fabric
- Provides all the advantages of SDA for wireless clients:
  - Full automation with Cisco DNA Center
  - Hierarchical segmentation (VRF and SGT)
  - Same policy as wired
  - Distributed Data Plane with no drawbacks
  - Optimized traffic path for Guest
- Recommended option

Wireless Overt The Top (OTT)

CUWN wireless Over The Top (OTT)

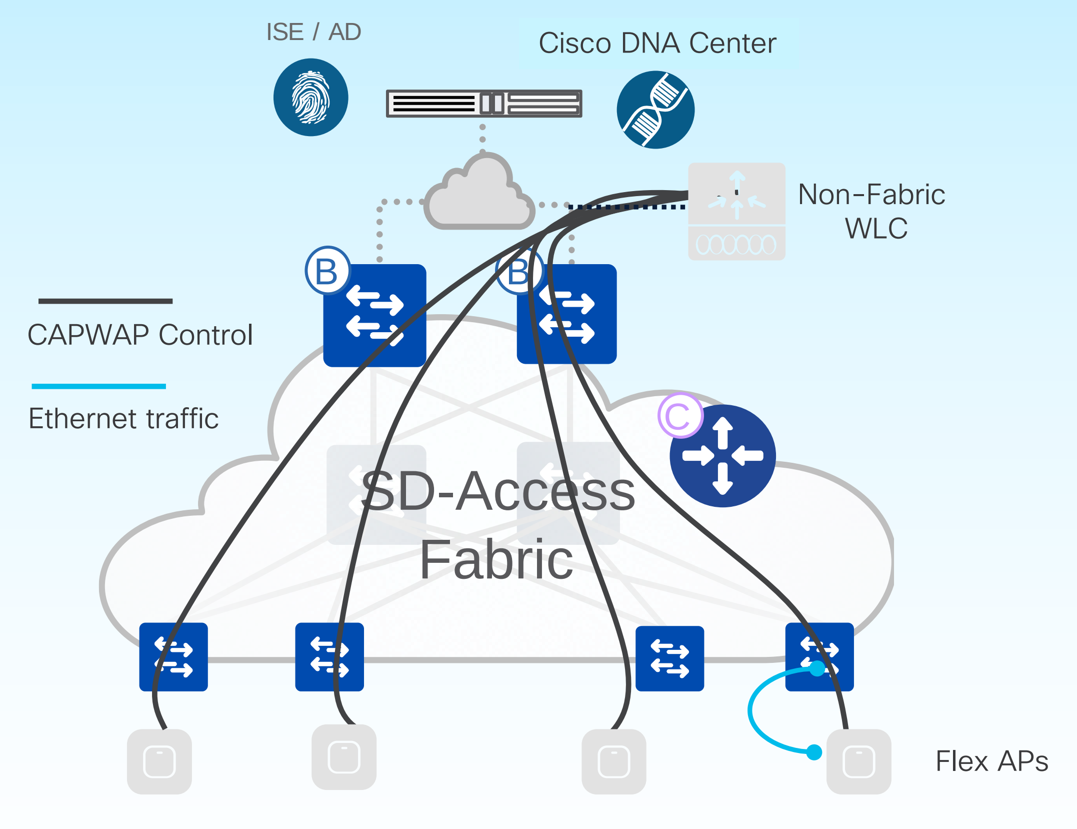


- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport
- Supported on any WLC/AP software and hardware
- <u>Only Centralized mode is supported today</u>

- **No SDA advantages for wireless**
- Migration step to full SD-Access
- Customer wants/need to first migrate wired (different Ops teams managing wired and wireless, get familiar with Fabric, different buying cycles, etc.) and leave wireless “as it is”
- Customer cannot migrate to Fabric yet (older APs, need to certify the new software, etc.)

Wireless FlexConnect Over The Top (OTT)

FlexConnect Over The Top (OTT)



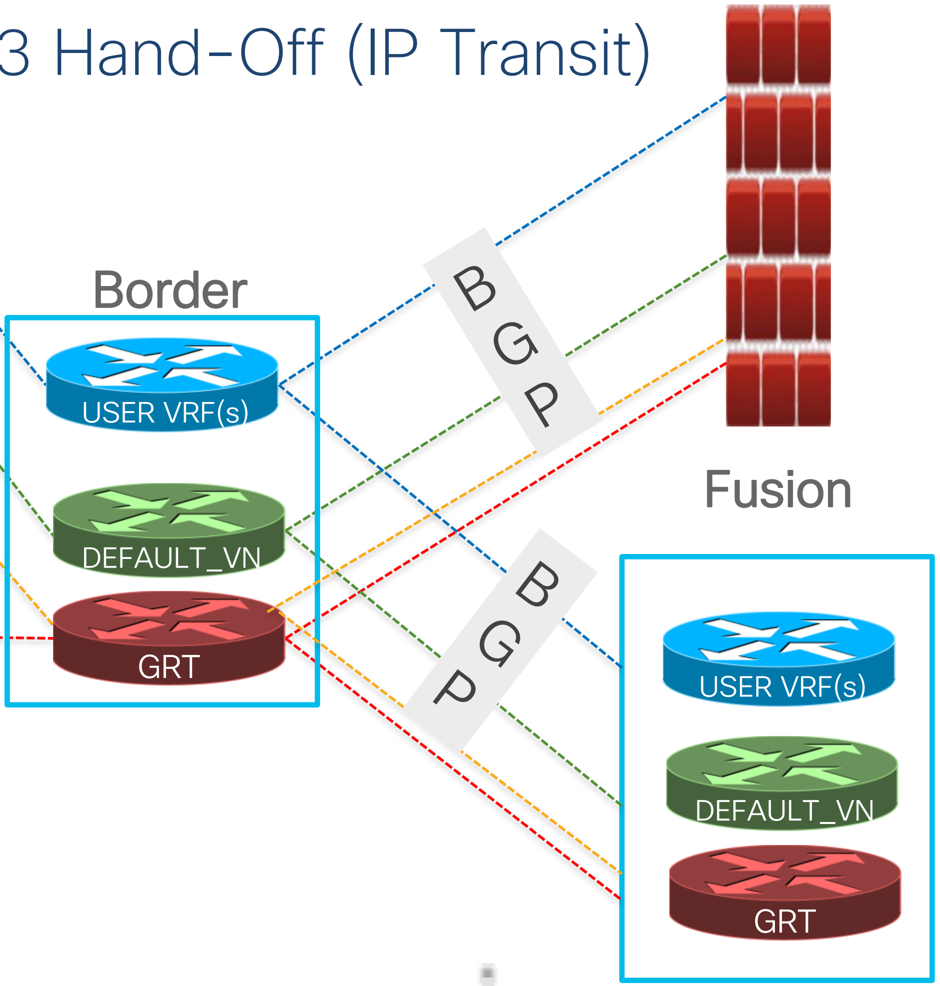
- CAPWAP for Control Plane
- Data plane is locally switched. Wireless traffic is treated like wired traffic.
- Supported with DNAC 2.1.2.x

- FlexConnect local switching supported as of SDA 2.1.2.x
- It is used as a temporary option to help transitioning from non-SDA to SDA networks

Connecting SDA Sites to Rest of World

SD-Access Fabric Border L3 Hand-Off (IP Transit)

- User-Defined VNs can be added or removed on-demand
- DEFAULT_VN is an actual "User VN" provided by default
- INFRA_VN is only for Access Points and Extended Nodes in GRT
- Fabric Devices (Underlay) connectivity is in the Global Routing Table



Option #1:
Fusion with route-leaking to interconnect VNs (here: Firewall with global routing + ACLs)

Option #2:
Fusion keeps VN separation (here: Router / L3 Switch with multiple VRFs)

Fully automated by Cisco DNAC

NOT automated

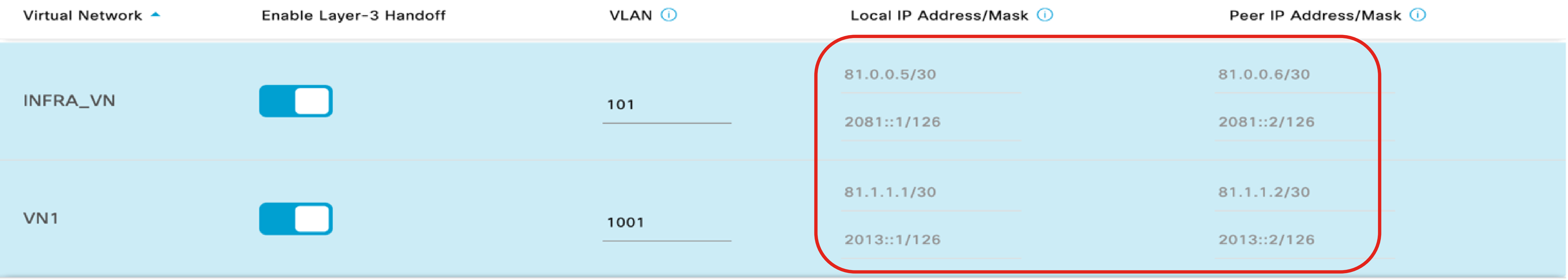
Custom Border layer 3 handoff

Use Case

- Prior to Cisco DNA Center 2.3.4.x release, SD-Access Border layer 3 handoff automation will automatically select subnet for establishing eBGP routing relationship with peer device.
- Certain deployment scenarios need flexibility with their IP address and subnet mask for their Border node automation.

Details

- From Cisco DNA Center 2.3.4.x release, user will have the option to manually allocate IP address and subnet mask for each layer 3 handoff enabled virtual networks.
- User can choose the current existing functionality which is to automate the layer 3 handoff ip or manually configure the ip addresses.
- Supported for both IPv4 and IPv6 handoff
- Can't have mixed mode i.e., manual and automated allocation at the same time is not supported. It is one or the other.



Virtual Network ▲	Enable Layer-3 Handoff	VLAN ⓘ	Local IP Address/Mask ⓘ	Peer IP Address/Mask ⓘ
INFRA_VN	☑	101	81.0.0.5/30 2081::1/126	81.0.0.6/30 2081::2/126
VN1	☑	1001	81.1.1.1/30 2013::1/126	81.1.1.2/30 2013::2/126

SD-Access Extranet

Use Case

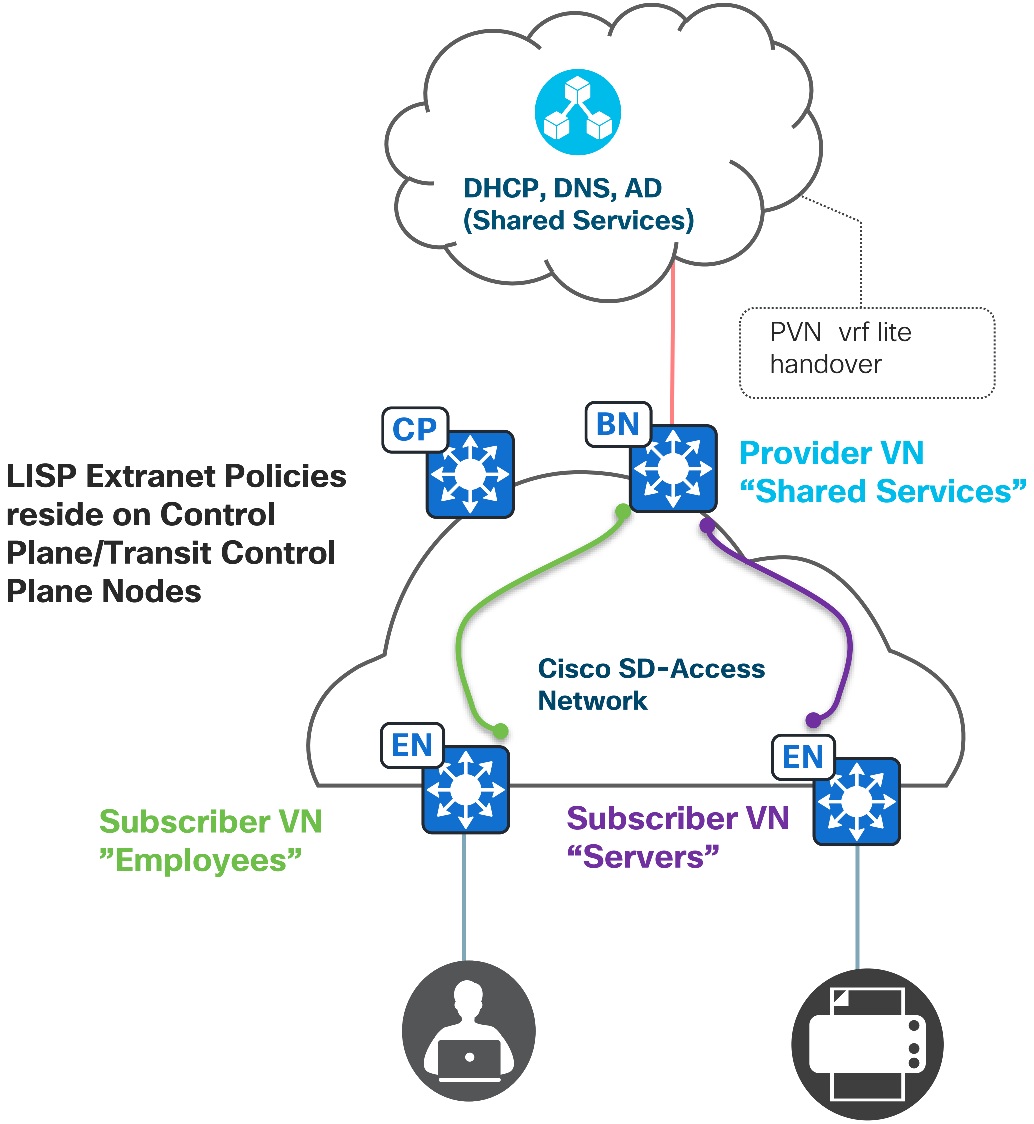
- LISP Extranet provides flexible, and scalable method for achieving Shared services, Internet access to hosts inside the fabric by simplifying the SD-Access fabric deployment and providing a more efficient and policy-based method of communication.
- Lisp Extranet helps in avoiding route-leaking performed outside fabric to access Shared services and Internet.

Details

- Extranet policy is orchestrated and maintained via Cisco DNA Center.
- LISP Extranet achieves this simplicity by introducing the concept of provider VNs and Subscriber VNs:
  - Provider VNs are usually provider of Shared Services , Internet, DC are located.
  - Subscriber VNs are where hosts (or users of shared services or Internet , DC) reside.
  - LISP Extranet policy allows communications between Provider and Subscriber VNs .
  - Provider VN can be a dedicated VN or Infra VN.
  - Provider VN cannot be a Subscriber VN.
  - Provider to Provider Policy is not supported.
  - Subscriber to Subscriber Policy is not supported.

Considerations

- Extranet is not supported on routing platforms.
- Extranet policies are supported with Lisp Pub/Sub fabric only.
- Extranet is not supported for Multicast
- Overlapping IP Pool support and IPDB are not supported with Extranet



☰ Active poll

0 👥

Join at

slido.com

#2460 020

Passcode:

afebum

Il faut utiliser SD-Access extranet pour faire communiquer les différents VN entre eux.

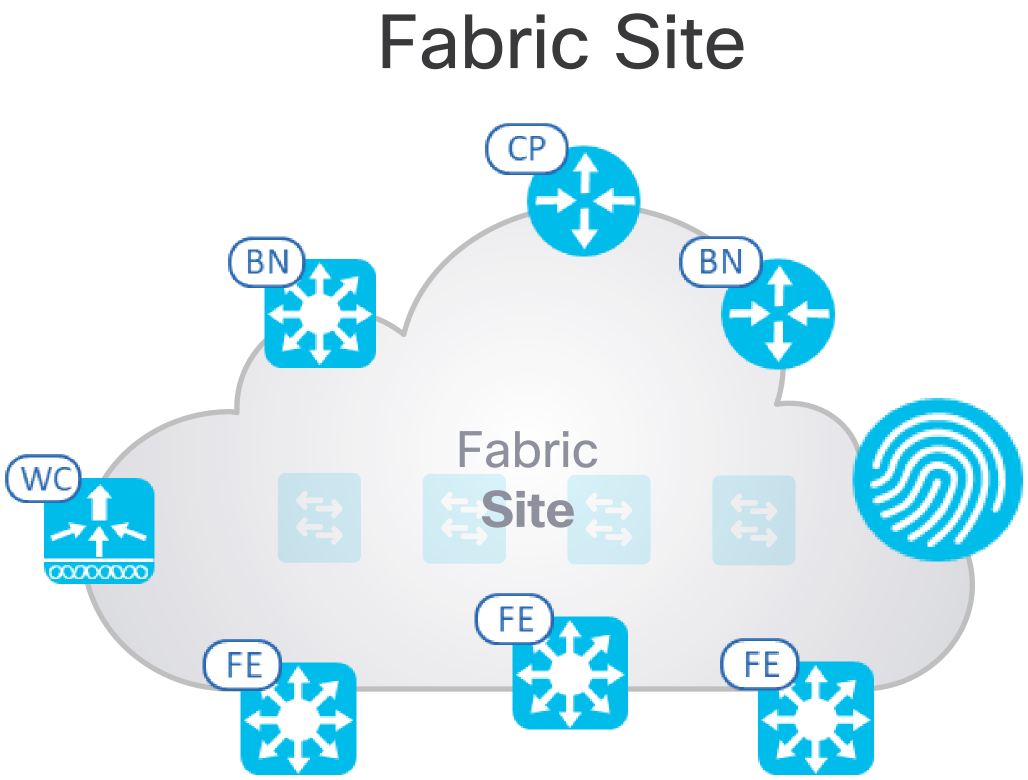
Vrai

0%

Faux

0%

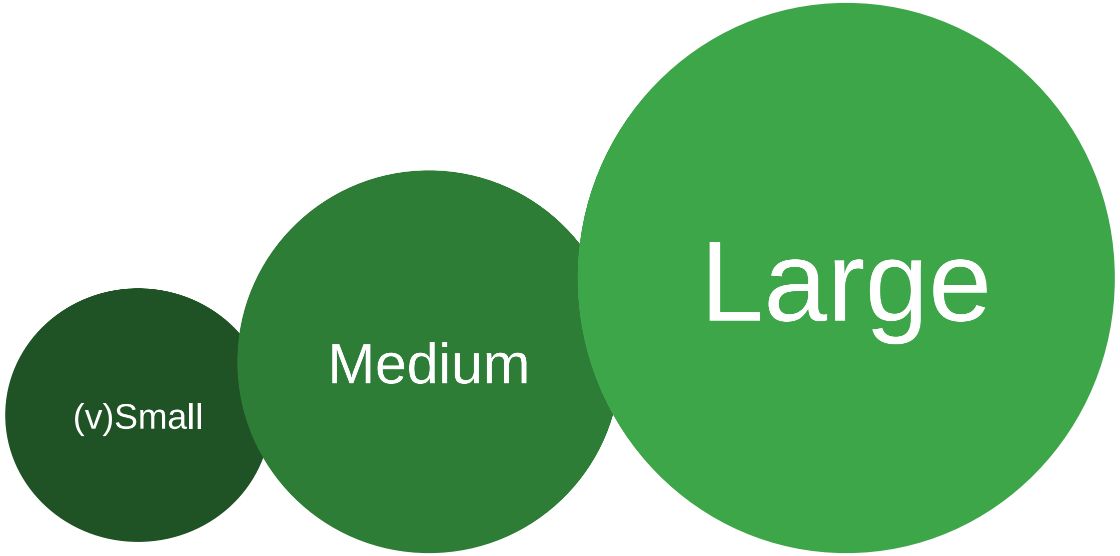
What is a Fabric Site



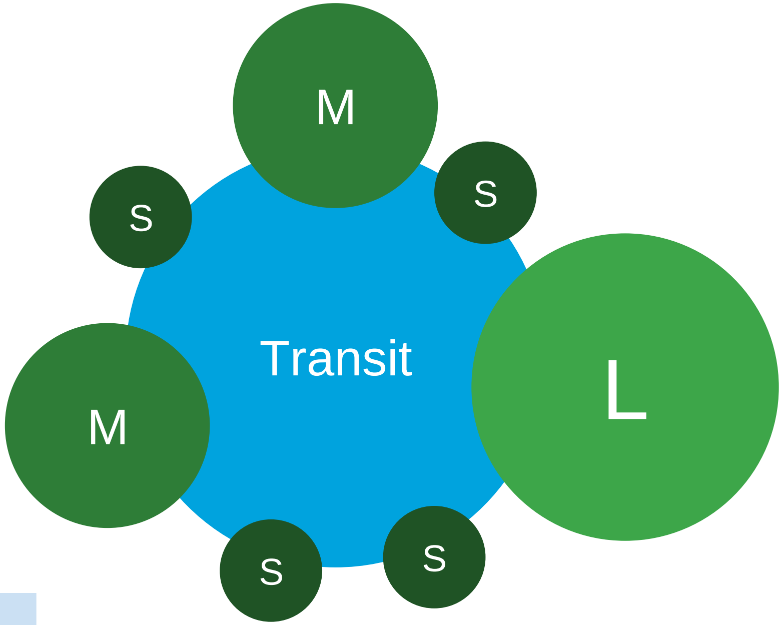
- **Fabric Site = HA Zone**
- Each Fabric Site has dedicated and individual
  - (CP) Control-Plane(s)
  - (BN) Border Node(s)
  - (FE) Fabric Edge(s)
  - (WC) Fabric WLC(s)
  - IP Pools
- Each Fabric Site can have individual
  - Set of active Virtual Networks (VNs)
  - ISE Policy Service Node(s)
- **Benefits**
  - Scalability
  - Resiliency
  - Survivability.
- **Fabric Site** may cover a single physical location, multiple locations, or just a subset of a location

Why Multiple Sites?

Basic Goal is for *fewer, larger* Fabric Sites



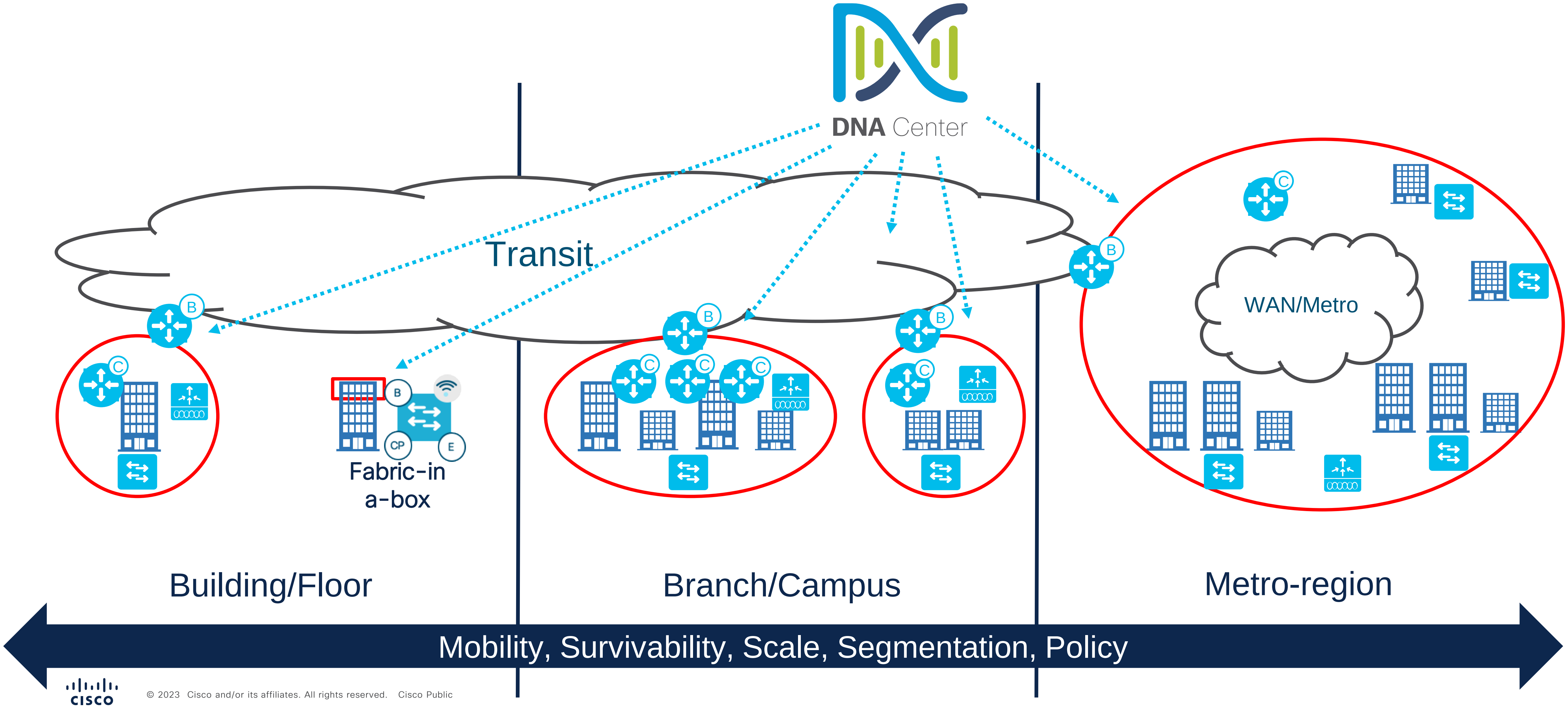
Some Needs *require split* into Multiple Sites



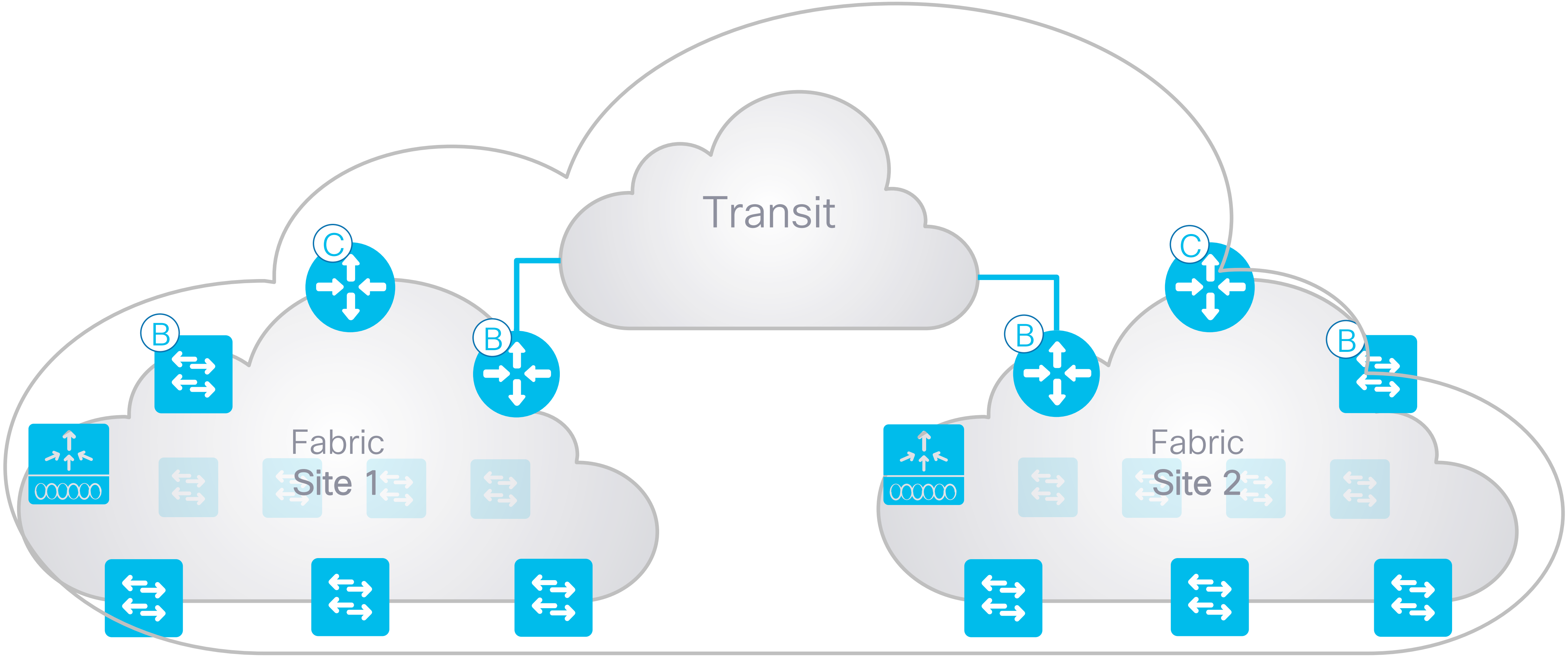
- ✓ Higher scale due to more number of sites (Control plane per site)
- ✓ Wireless Client Roaming (< 20ms Latency)
- ✓ Direct Internet Access (@ Remote Sites)
- ✓ Survivable Remote Sites (Local CP/Borders)
- ✓ Transit MTU insufficient (IP Transit)

[Cisco DNA Center Appliance scale & specifications]

Diverse types of fabric sites



Fabric Sites & Domains

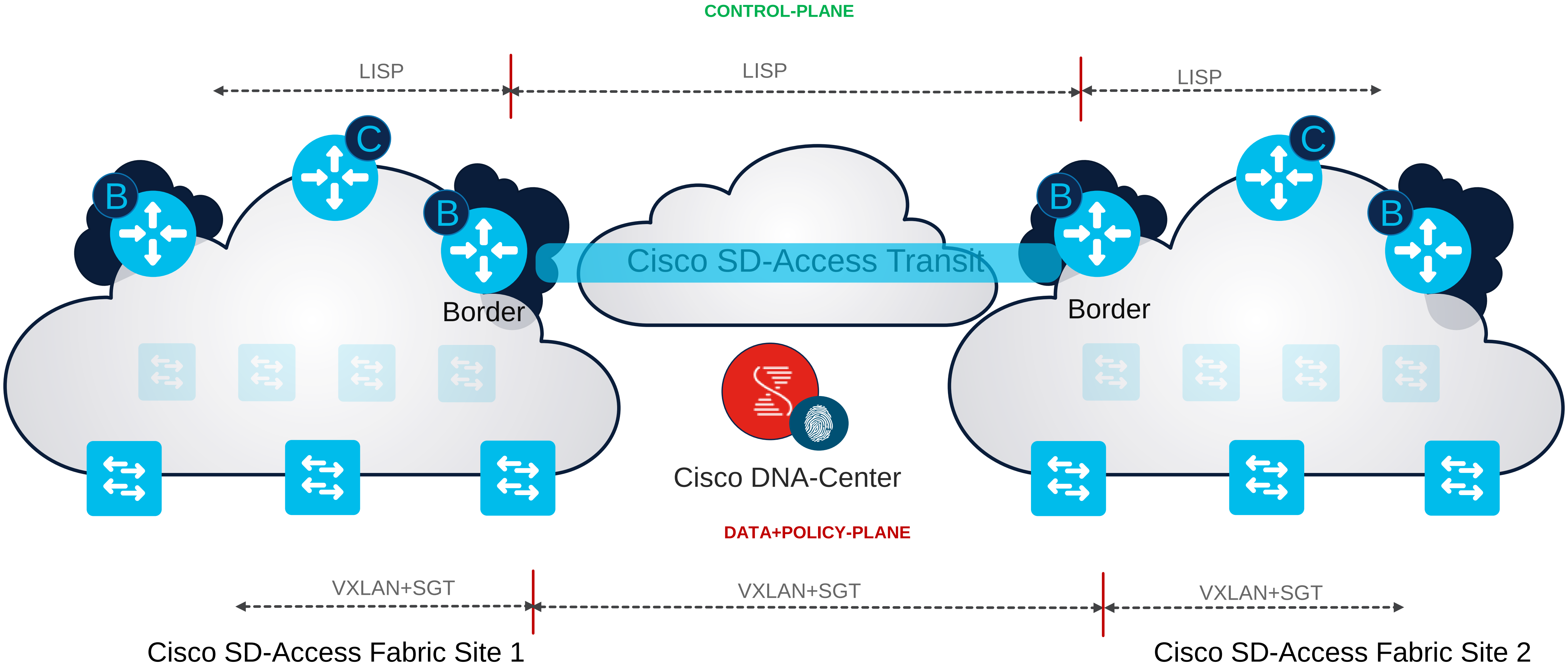


Transit/Peer Network Types

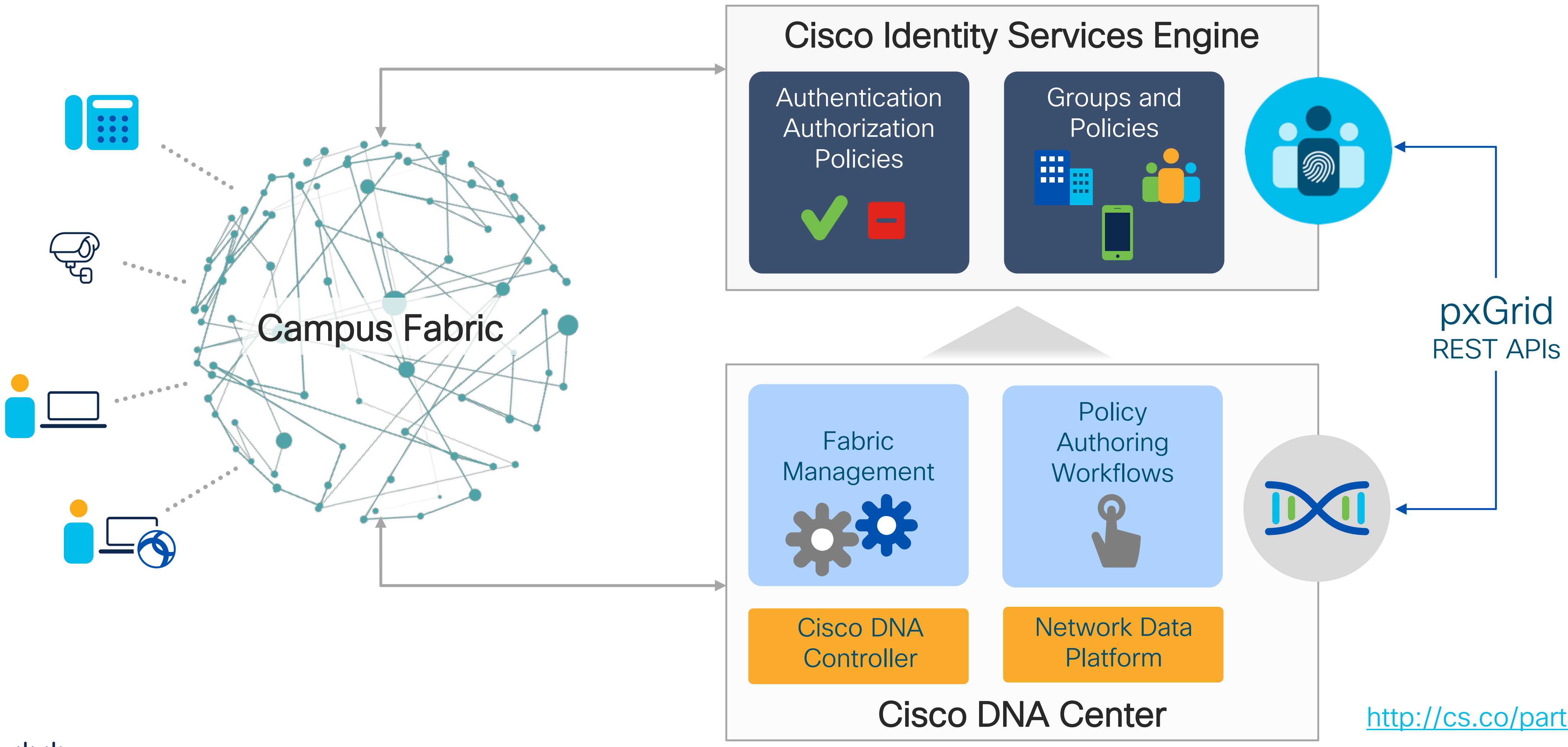
- IP-Based Transit - Leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.
- Cisco SD-Access Transit - Enables a native Cisco SD-Access (VXLAN,SGT) fabric, with a domain-wide Control Plane node for inter-site communication.
- Cisco SD-WAN Transit – Leverages the Cisco SD-WAN as transit and carries the context in the Cisco SD-WAN encapsulation.
- **Layer-2 Handoff** – For Brownfield migration or Default GW on Firewall (this option should be avoided if possible)

Interconnecting SDA Sites

SDA Transit



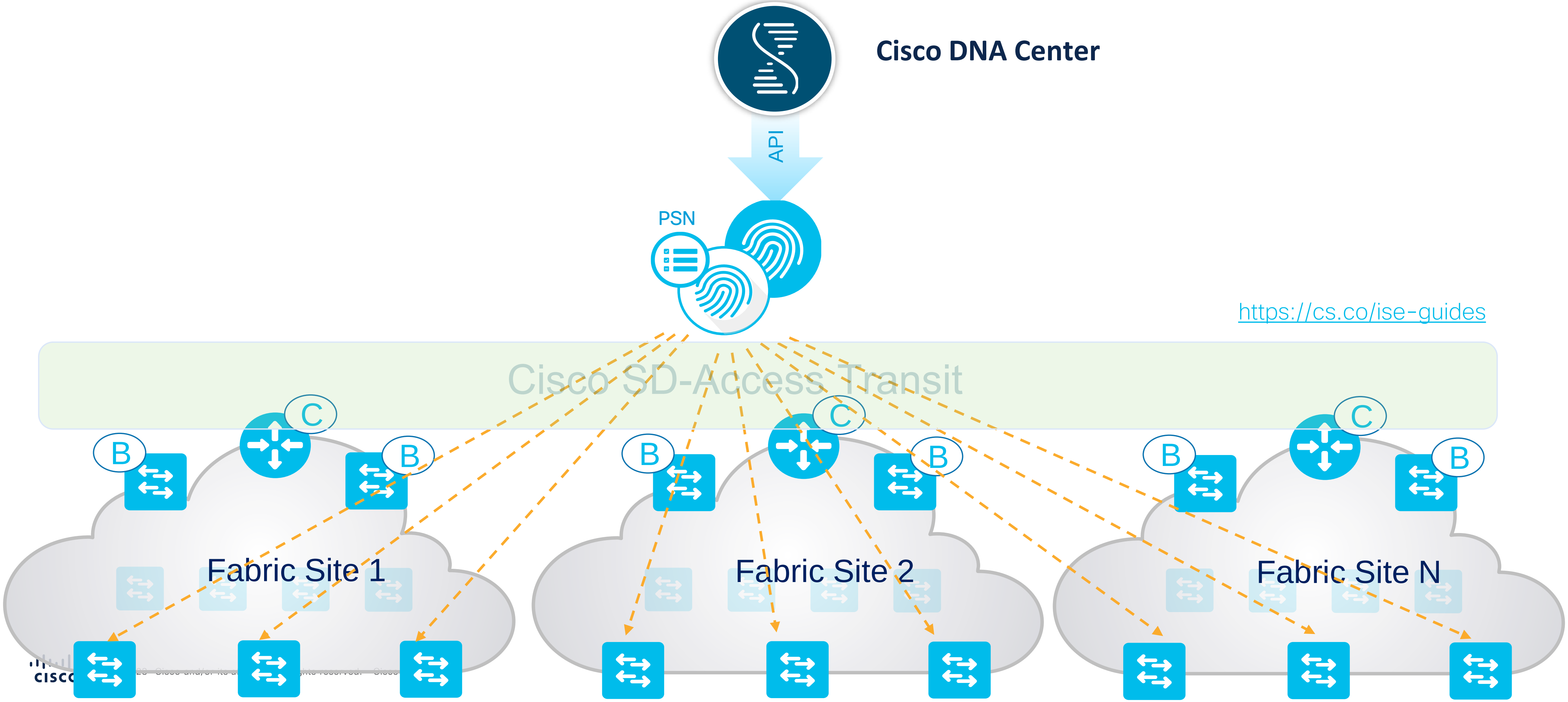
ISE and Cisco DNA Center Integration for Policy Automation



http://cs.co/partner-ise

ISE Distributed Deployment

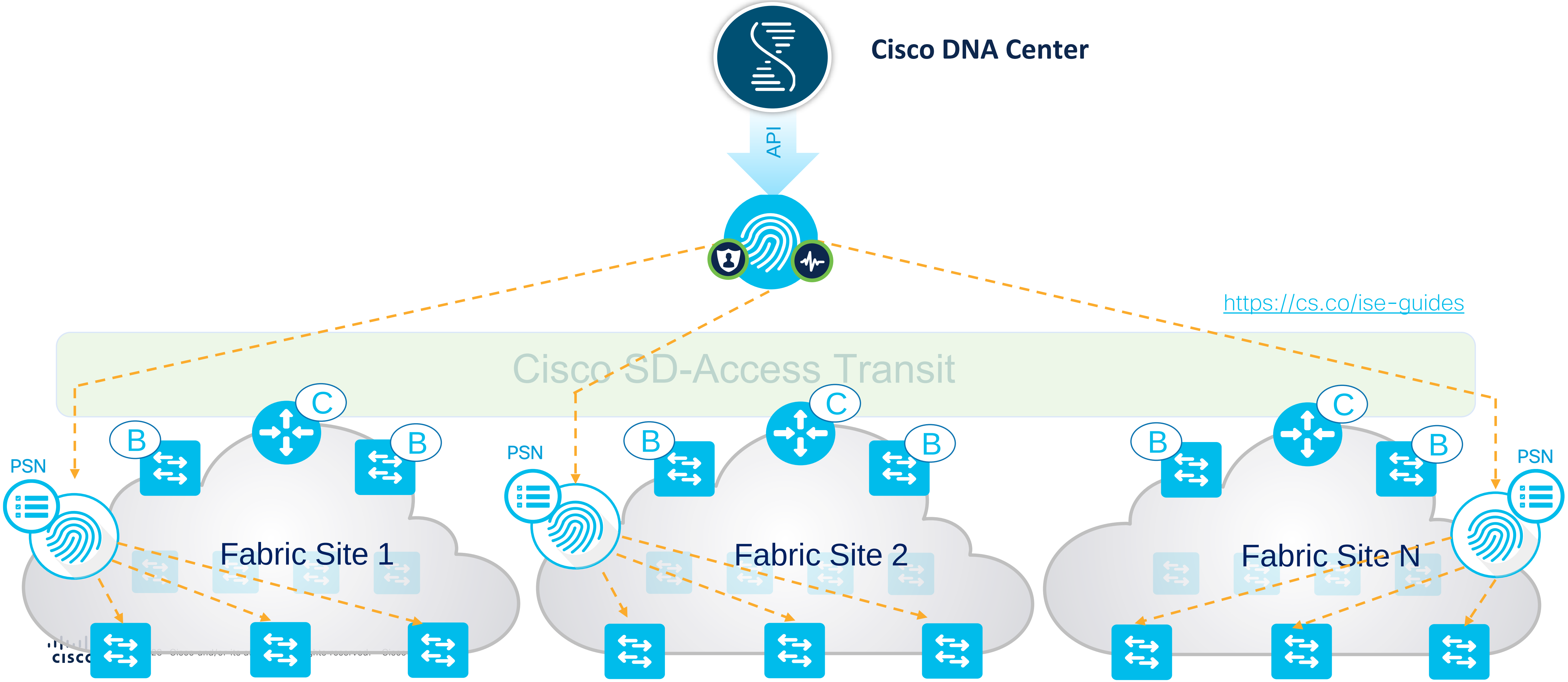
Model 1 - Centralized PSN



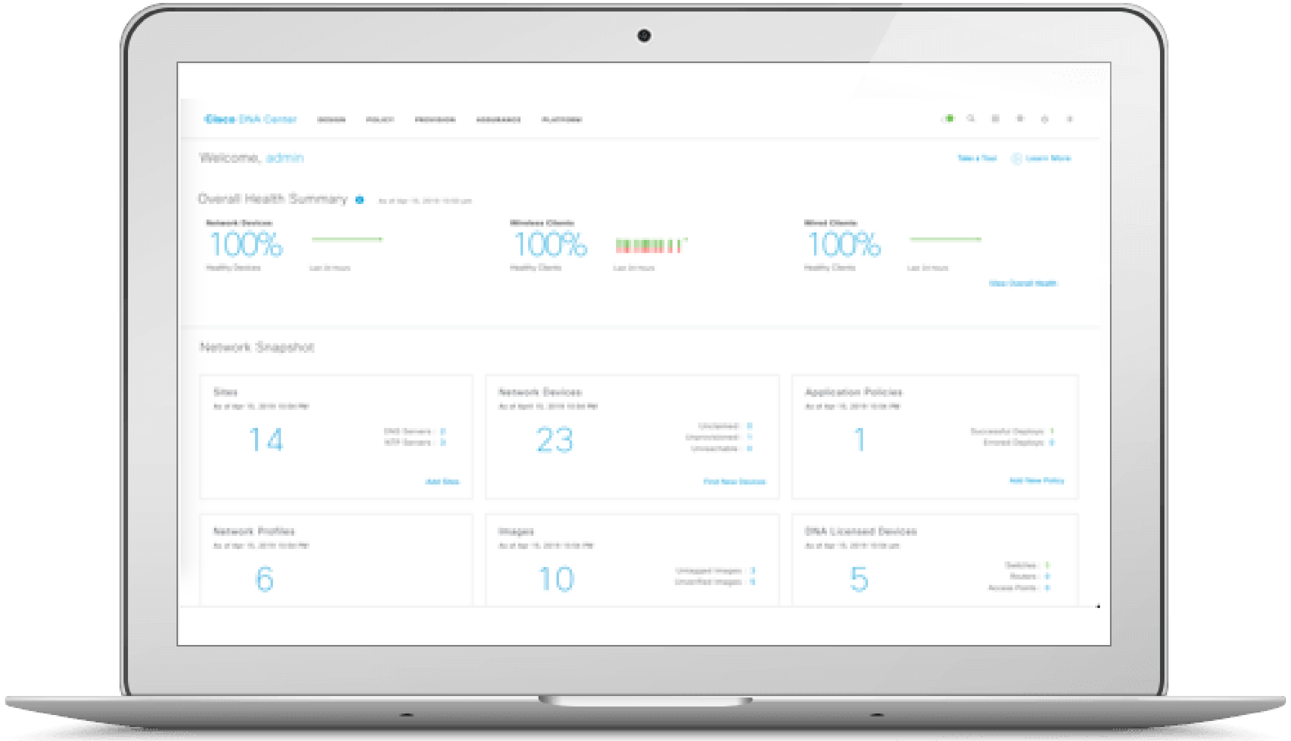
https://cs.co/ise-guides

ISE Distributed Deployment

Model 2 - Dedicated PSN per Site



https://cs.co/ise-guides


Cisco DNA Center
DESIGN
POLICY
PROVISION
ASSURANCE
PLATFORM
Welcome, admin
Take a Tour
Learn More
Overall Health Summary
Network Devices
100%
Healthy Devices
Last 24 hours
Wireless Clients
100%
Healthy Clients
Last 24 hours
Wired Clients
100%
Healthy Clients
Last 24 hours
View Overall Health
Network Snapshot
Sites
14
DNS Servers
NTP Servers
Add Sites
Network Devices
23
Unclaimed
Unprovisioned
Unreachable
Find New Devices
Application Policies
1
Successful Deploys
Errored Deploys
Add New Policy
Network Profiles
6
Images
10
Untagged Images
Unverified Images
DNA Licensed Devices
5
Switches
Routers
Access Points

Démo

Cisco DNA Center Scale

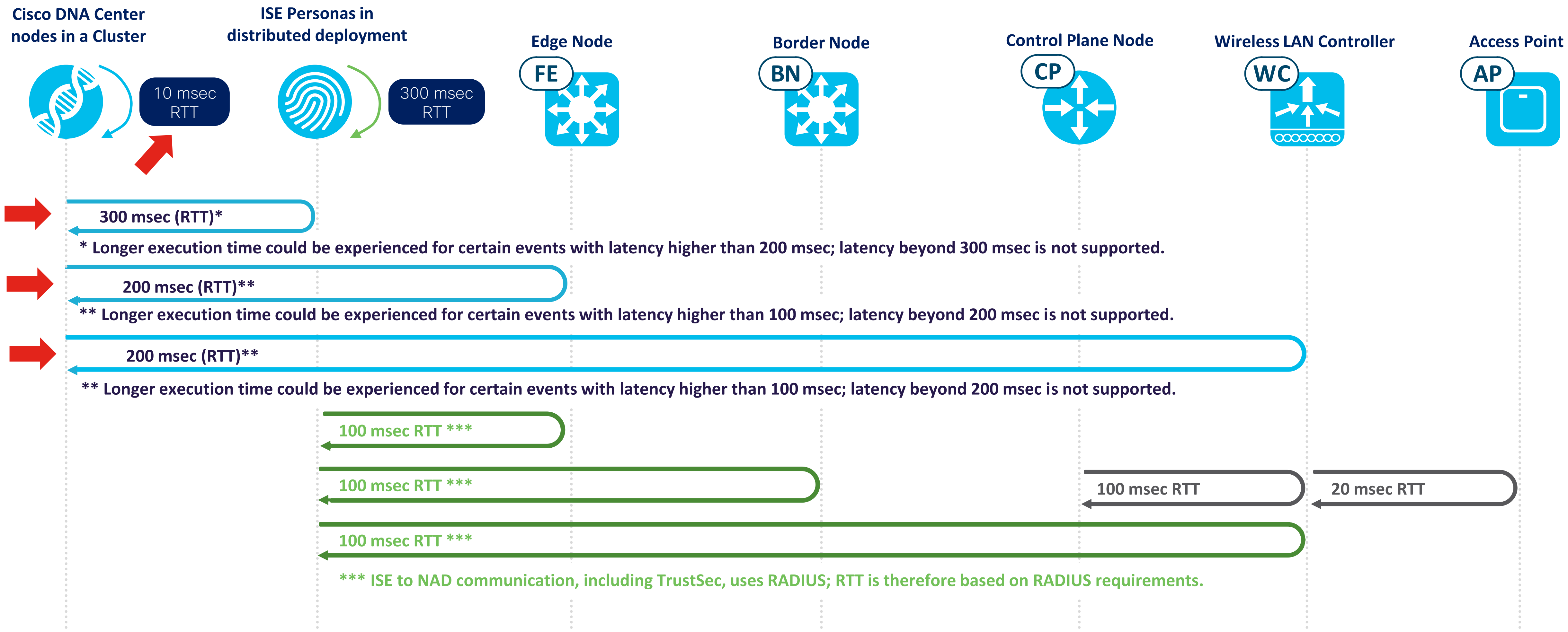
For Your Reference

Description	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
Endpoints (concurrent)	25000	40000	100,000 (Ratio removed starting 2.1.1)
Network Devices	1000	2000	5000
AP’s	4000	6000	13000
DNAC Sites	500	1000	2000
Access Control Policies	25000	25000	25000
Access Contracts	500	500	500
Per Fabric Site Scale			
Fabric Nodes	500	600	1200
VNs	64	64 => 128 (starting 2.2.1)	256
IP Pools	100	300	600 => 1000 (starting 2.2.1)

Latency between DNAC to device: 200ms (RTT)

Cisco DNAC and SDA Maximum Supported Latency

For Your Reference



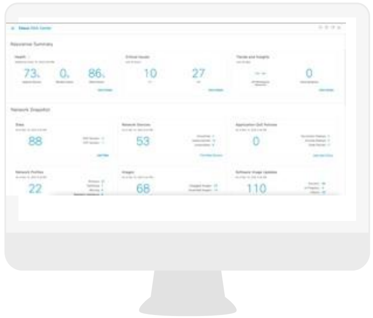
* Longer execution time could be experienced for certain events with latency higher than 200 msec; latency beyond 300 msec is not supported.

** Longer execution time could be experienced for certain events with latency higher than 100 msec; latency beyond 200 msec is not supported.

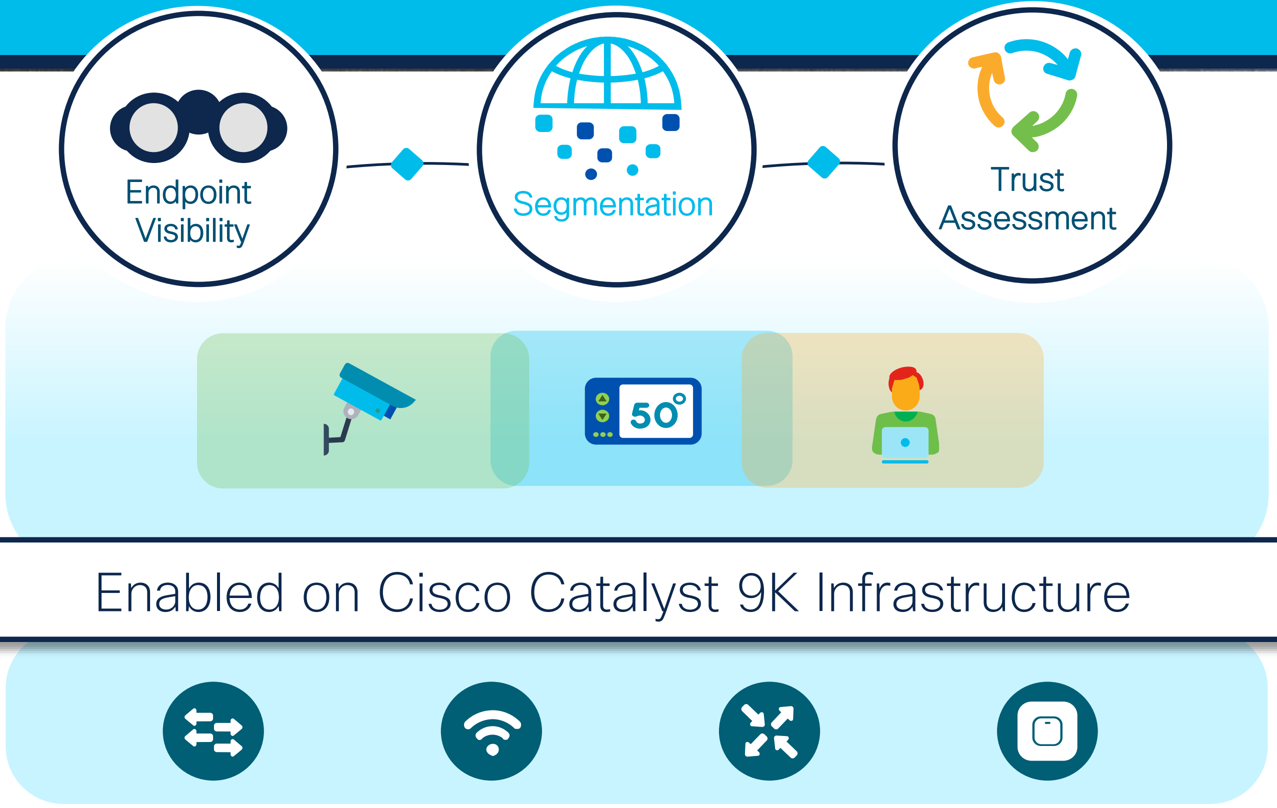
** Longer execution time could be experienced for certain events with latency higher than 100 msec; latency beyond 200 msec is not supported.

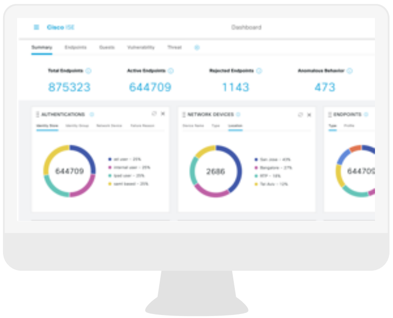
*** ISE to NAD communication, including TrustSec, uses RADIUS; RTT is therefore based on RADIUS requirements.

Three pillars of Workplace Zero Trust Security



Cisco DNA Center



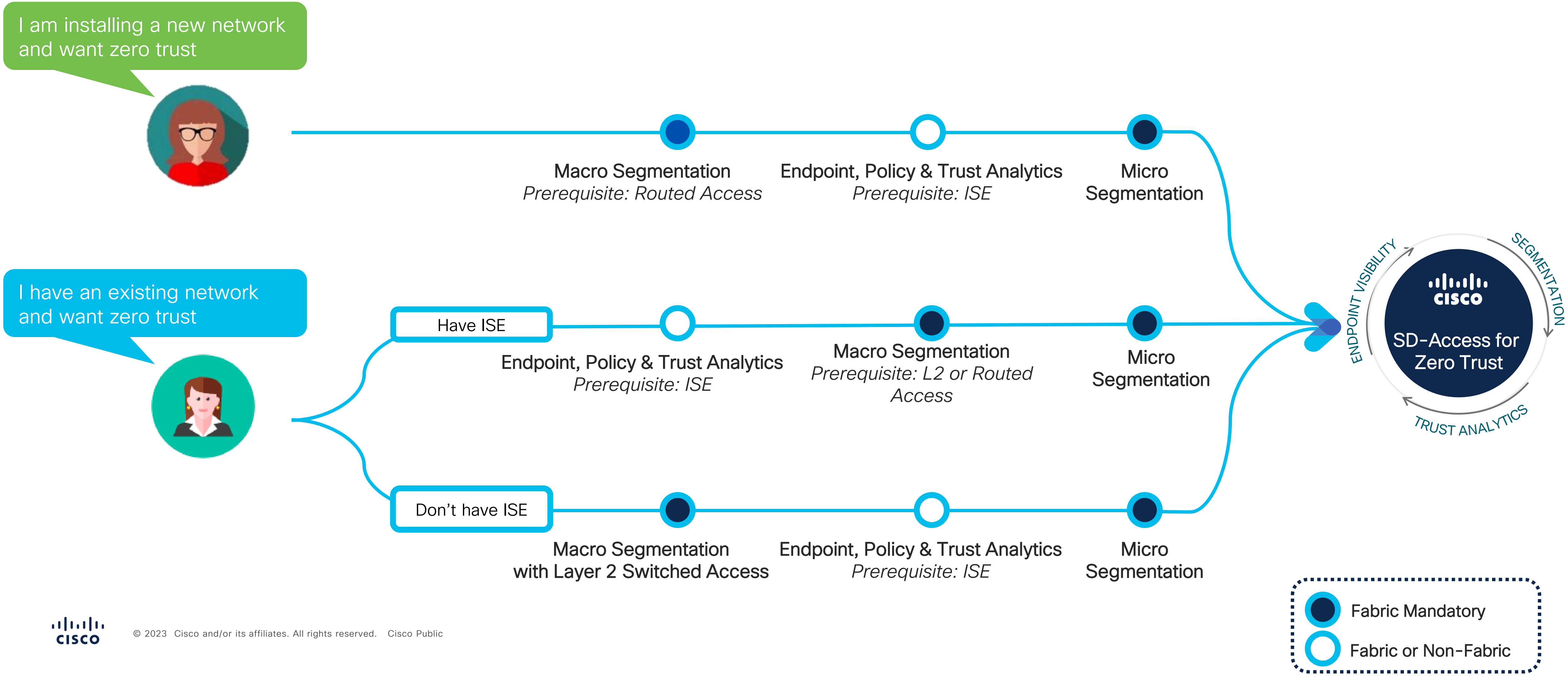


Cisco ISE

Enabled on Cisco Catalyst 9K Infrastructure

Flexible Options removes barriers to Quick Value

Customizable and phased implementation of an extensible network



I am installing a new network and want zero trust

● Macro Segmentation
Prerequisite: Routed Access

○ Endpoint, Policy & Trust Analytics
Prerequisite: ISE

● Micro Segmentation

I have an existing network and want zero trust

Have ISE

○ Endpoint, Policy & Trust Analytics
Prerequisite: ISE

● Macro Segmentation
Prerequisite: L2 or Routed Access

● Micro Segmentation

Don't have ISE

● Macro Segmentation with Layer 2 Switched Access

○ Endpoint, Policy & Trust Analytics
Prerequisite: ISE

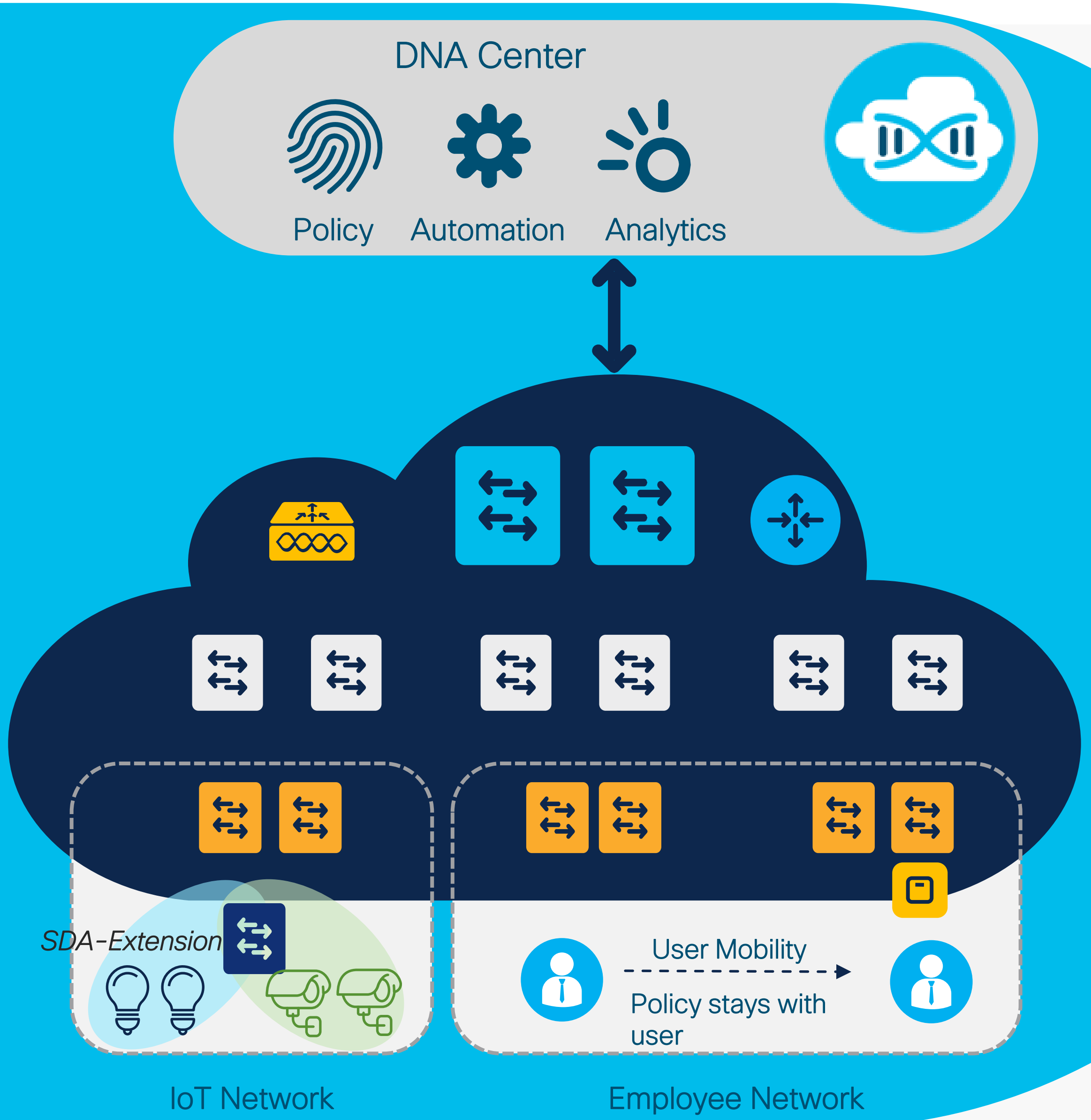
● Micro Segmentation

● Fabric Mandatory

○ Fabric or Non-Fabric

Software-Defined Access

Networking at the speed of Software!



Identity-based Policy & Segmentation

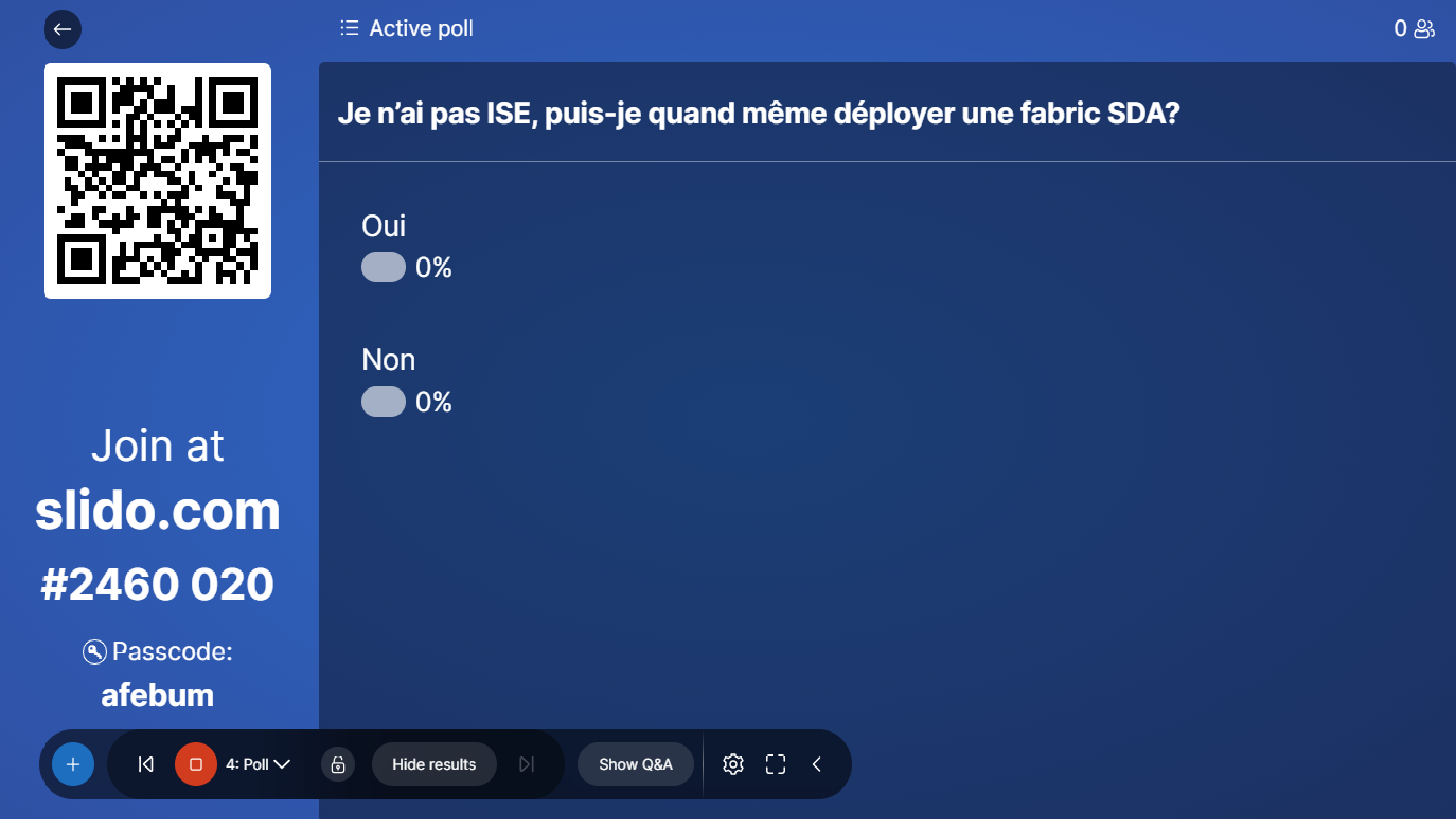
Decoupled security policy definition from VLAN and IP Address

Automated Network Fabric

Single Fabric for Wired & Wireless with Workflow-based Automation

Insights & Telemetry

Analytics and insights into user and application behavior



Active poll

0

Je n’ai pas ISE, puis-je quand même déployer une fabric SDA?

Oui

0%

Non

0%

Join at

slido.com

#2460 020

Passcode:

afebum

SD-Access Resources

General

cisco.com/go/sdaccess

- SD-Access At-A-Glance
- SD-Access Ordering Guide
- SD-Access Solution Data Sheet
- SD-Access Solution White Paper

Don't worry—we're here to get you caught up on what you missed at the Wired for Wireless event. Watch recording

Solutions / Cisco Digital Network Architecture (Cisco DNA) /

Software-Defined Access

Get network speed, security, and peace of mind

Ease your network management worries. Cisco Software-Defined Access (SD-Access) gives you a single network fabric, from the edge to the cloud. You can set policy-based automation for users, devices, and things.

Provide access to any application, without compromising on security. All while gaining awareness of what is hitting your network.

And with automatic segmentation of users, devices, and applications, you can deploy and secure services faster.

What you can do with SD-Access

Enhance security and compliance

Use end-to-end segmentation to keep user, device, and application traffic separate without redesigning the network.

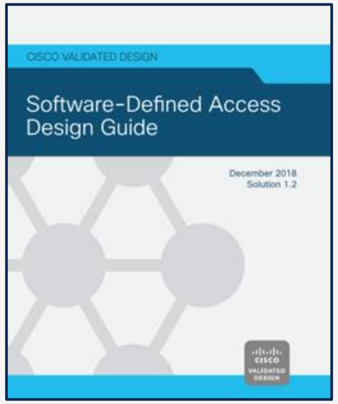
Improve the workforce experience

Automate user access policy and apply the right policies for users or devices to any application, across the network.

Technical

cs.co/en-cvds

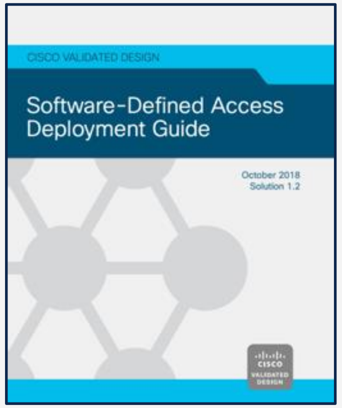
- SD-Access Design Guide
- SD-Access Deployment Guide
- SD-Access Segmentation Guide
- SD-Access book for Industry Verticals



CISCO VALIDATED DESIGN

Software-Defined Access Design Guide

December 2018
Solution 1.2



CISCO VALIDATED DESIGN

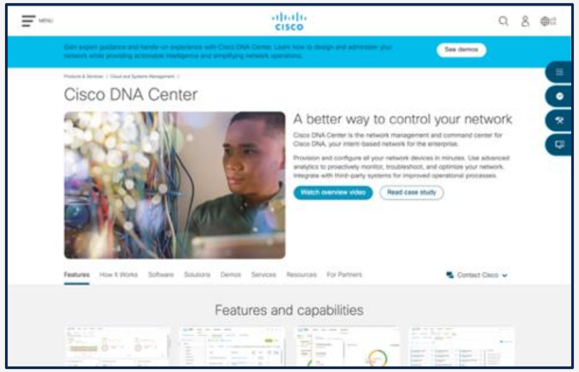
Software-Defined Access Deployment Guide

October 2018
Solution 1.2

Related

cisco.com/go/dnacenter

- Cisco DNA Center At-A-Glance
- Cisco DNA ROI Calculator
- Cisco DNA Center Data Sheet
- Cisco DNA Center 'How To' Video Resources
- Cisco DNA Solution Builder



Gain expert guidance and hands-on experience with Cisco DNA Center. Learn how to design and administer your network while providing actionable intelligence and simplifying network operations.

Products & Services / Cloud and Systems Management /

Cisco DNA Center

A better way to control your network

Cisco DNA Center is the network management and command center for Cisco DNA, your intent-based network for the enterprise.

Provision and configure all your network devices in minutes. Use advanced analytics to proactively monitor, troubleshoot, and optimize your network. Integrate with third-party systems for improved operational processes.

Features and capabilities

Clôture

Avez-vous des questions ?

Si vous avez posé une question sur le panneau de Q&R (Q&A en anglais) ou que vous revenez sur la communauté dans les jours qui suivent notre webinaire, nos experts peuvent encore vous aider !

Participez dans e forum Ask Me Anything (AMA) avant le 30 juin.

https://bit.ly/AMA-jun23

Faites valoir votre opinion

Répondez à notre enquête pour…

- Proposer des nouveaux sujets
- Évaluer nos experts et contenus
- Envoyer vos commentaires ou suggestions

Cliquez sur le lien

https://bit.ly/WEBenq-jun23

Nos réseaux sociaux

LinkedIn

[Cisco Community]

Twitter

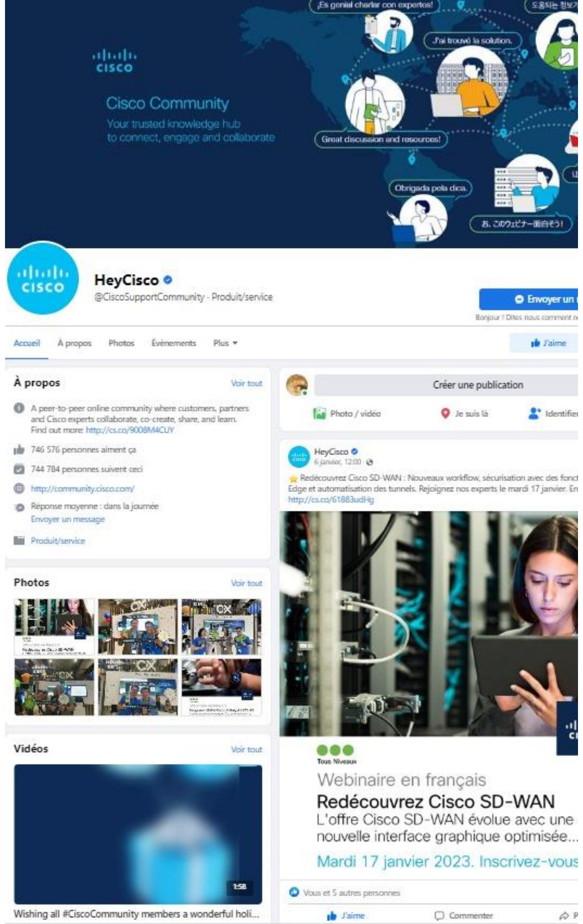
[@CiscoCommunity]

YouTube

[CiscoCommunity]

Facebook

[CiscoCommunity]



HeyCisco

@CiscoSupportCommunity · Produit/service

Bonjour ! Dites-nous comment n

À propos

A peer-to-peer online community where customers, partners and Cisco experts collaborate, co-create, share, and learn. Find out more: http://cs.co/9008M4CUY

746 576 personnes aiment ça

744 784 personnes suivent ceci

http://community.cisco.com/

Réponse moyenne : dans la journée

Envoyer un message

Produit/service

Photos

Vidéos

Wishing all #CiscoCommunity members a wonderful holi...

HeyCisco

6 janvier, 12:00

Redécouvrez Cisco SD-WAN : Nouveaux workflow, sécurisation avec des fonct Edge et automatisation des tunnels. Rejoignez nos experts le mardi 17 janvier. En http://cs.co/61883udHg

Tous Niveaux

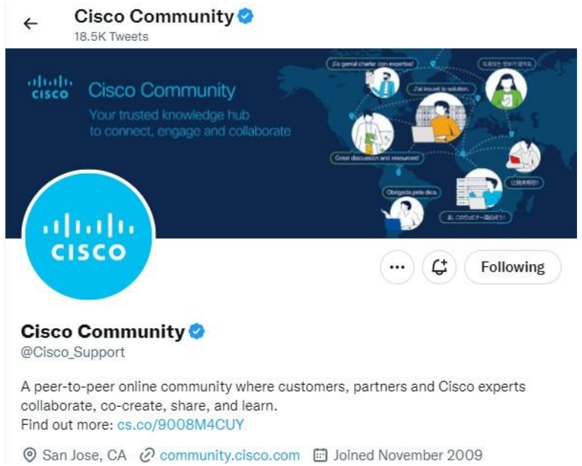
Webinaire en français

Redécouvrez Cisco SD-WAN

L'offre Cisco SD-WAN évolue avec une nouvelle interface graphique optimisée...

Mardi 17 janvier 2023. Inscrivez-vous

Vous et 5 autres personnes


Cisco Community
Your trusted knowledge hub to connect, engage and collaborate
Following

Cisco Community

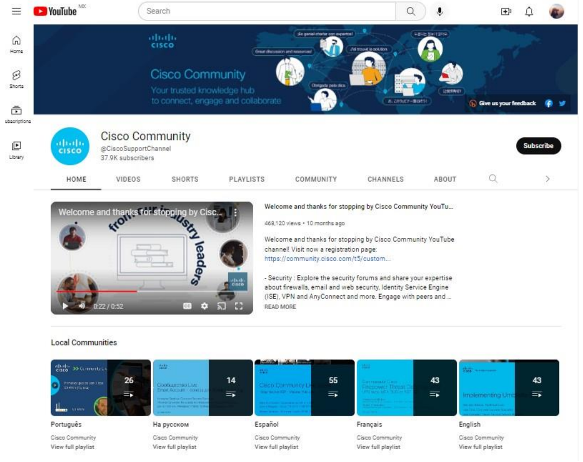
18.5K Tweets

Cisco Community

@Cisco_Support

A peer-to-peer online community where customers, partners and Cisco experts collaborate, co-create, share, and learn.
Find out more: cs.co/9008M4CUY

San Jose, CA community.cisco.com Joined November 2009



Cisco Community

@CiscoSupportChannel

37.9K subscribers

Welcome and thanks for stopping by Cisco Community YouTu...

468,120 views • 10 months ago

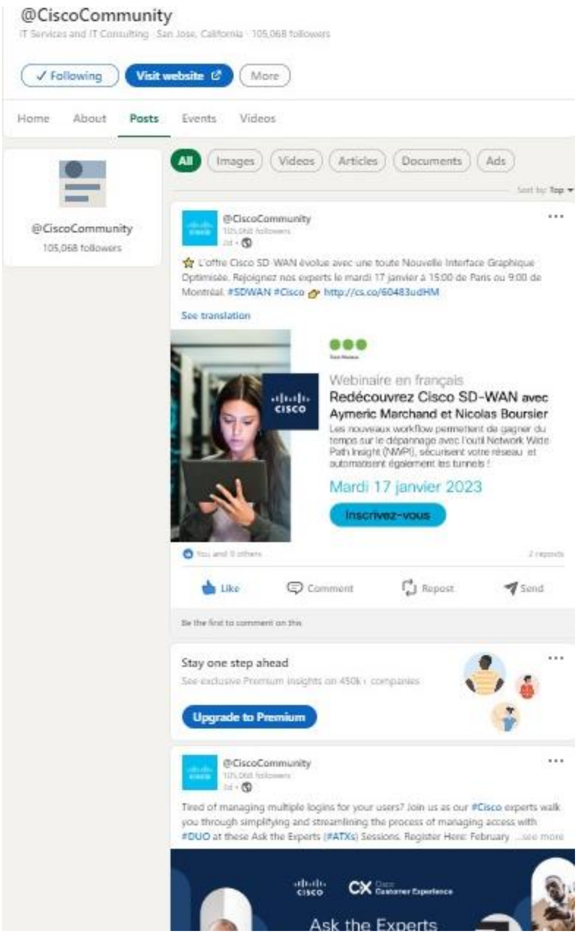
Welcome and thanks for stopping by Cisco Community YouTube channel! Visit now a registration page: https://community.cisco.com/t5/custom...

- Security : Explore the security forums and share your expertise about firewalls, email and web security, Identity Service Engine (ISE), VPN and AnyConnect and more. Engage with peers and ...

READ MORE

Local Communities

Português	На русском	Español	Français	English
26	14	55	43	43
Cisco Community	Cisco Community	Cisco Community	Cisco Community	Cisco Community
View full playlist	View full playlist	View full playlist	View full playlist	View full playlist



@CiscoCommunity

IT Services and IT Consulting · San Jose, California · 105,068 followers

@CiscoCommunity

105,068 followers

@CiscoCommunity

105,068 followers

2d •

L'offre Cisco SD-WAN évolue avec une toute Nouvelle Interface Graphique Optimisée. Rejoignez nos experts le mardi 17 janvier à 15:00 de Paris ou 9:00 de Montréal. #SDWAN #Cisco http://cs.co/60483udHM

See translation

Webinaire en français

Redécouvrez Cisco SD-WAN avec Aymeric Marchand et Nicolas Boursier

Les nouveaux workflow permettent de gagner du temps sur le dépannage avec l'outil Network Wide Path Insight (NWPI), sécurisent votre réseau et automatisent également les tunnels !

Mardi 17 janvier 2023

Inscrivez-vous

You and 9 others · 2 reposts

Be the first to comment on this

Stay one step ahead

See exclusive Premium insights on 450k+ companies

@CiscoCommunity

105,068 followers

3d •

Tired of managing multiple logins for your users? Join us as our #Cisco experts walk you through simplifying and streamlining the process of managing access with #DUO at these Ask the Experts (#ATXs) Sessions. Register Here: February ...see more

The bridge to possible