You make **possible**

cisco

SD-Access Design

Important Design & Migration Principles

Shawn Wargo – Technical Marketing
Kedar Karmarkar – Technical Marketing

TECCRS-2812

LEARNING
Cisco DNA Center
Policy
Automation
Analytics
INTENT
CONTEXT
Intent-Based Network Infrastructure
Switch
Route
Wireless
SECURITY

cisco Live!

Barcelona | January 27-31, 2020

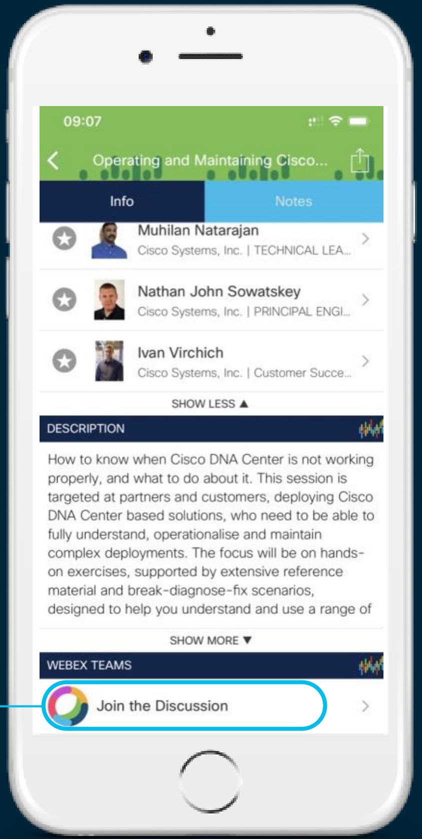
Cisco Webex Teams

Questions?

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

How

1. Find this session in the Cisco Events Mobile App
2. Click "Join the Discussion"
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

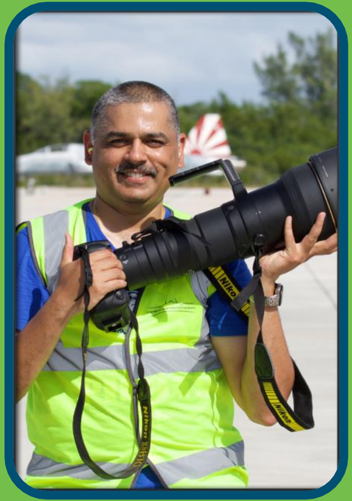
WEBEX TEAMS

SD-Access Team

Who Are We?

Shawn Wargo

Technical Marketing



Kedar Karmarkar

Technical Marketing

Agenda

- Introduction
- SD-Access Recap
- Design Strategy
- Design for Single-Site (Connect)

- Design for Single-Site (Policy)
- Design for Multi-Site
- Migration Considerations
- Summary

Introduction

Assumptions

IMPORTANT NOTICE

This session assumes you have received DNA Center & SD-Access Training

If not… please complete one or all of the following training materials:

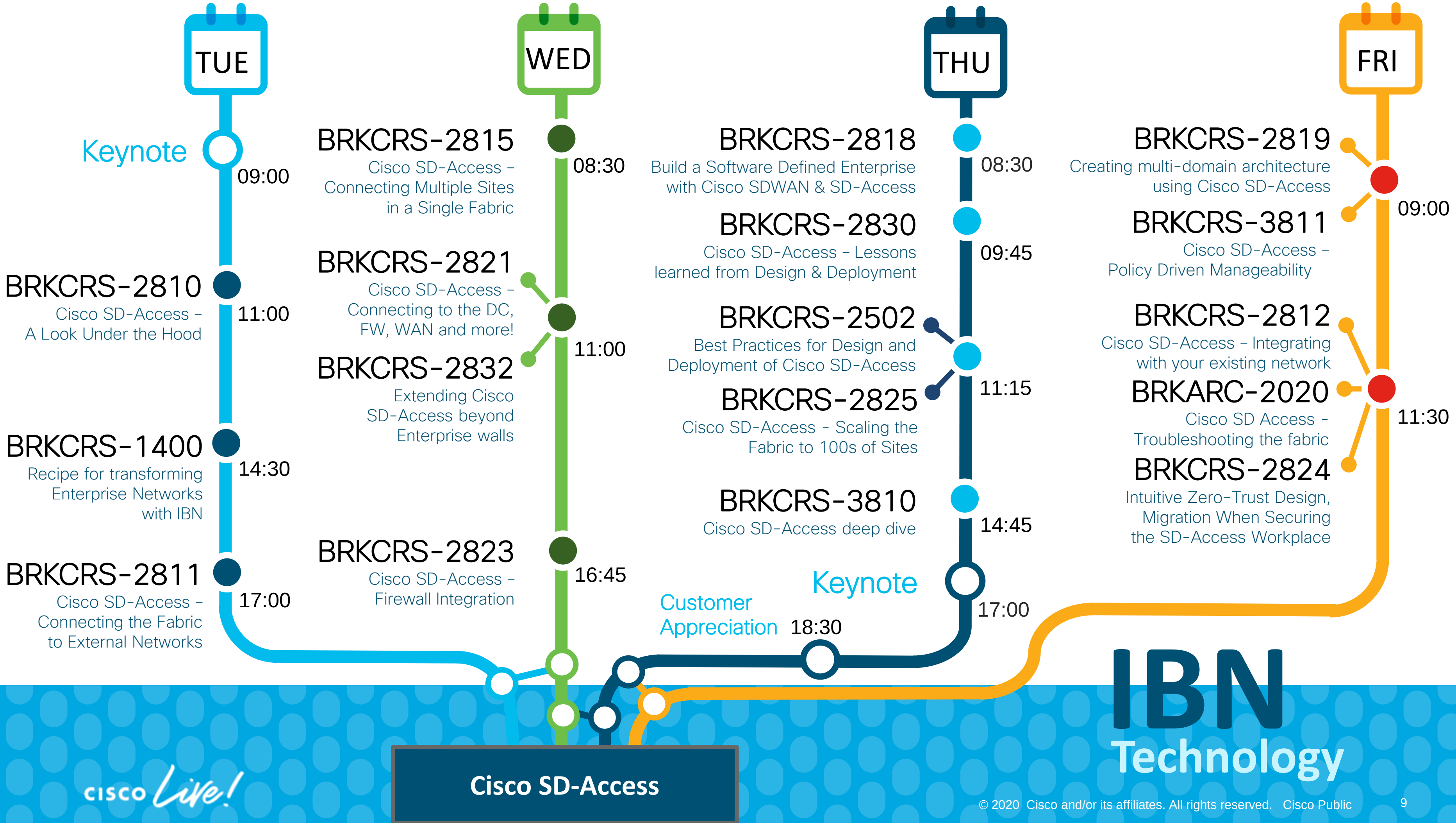
- CiscoLive
- Learning@Cisco
- dCloud Lab
- SDA Design CVD
- SDA Deploy CVD
- DNAC Guides

This session is based on DNAC / SDA 1.3.3, ISE 2.6 p2 and IOS-XE 16.12

- Product Compatibility Matrix

For a list of current capabilities, restrictions, limitations & caveats refer to:

- DNAC Release Notes



TUE

Keynote 09:00

BRKCRS-2810
Cisco SD-Access –
A Look Under the Hood
11:00

BRKCRS-1400
Recipe for transforming
Enterprise Networks
with IBN
14:30

BRKCRS-2811
Cisco SD-Access –
Connecting the Fabric
to External Networks
17:00

WED

BRKCRS-2815
Cisco SD-Access –
Connecting Multiple Sites
in a Single Fabric
08:30

BRKCRS-2821
Cisco SD-Access –
Connecting to the DC,
FW, WAN and more!

BRKCRS-2832
Extending Cisco
SD-Access beyond
Enterprise walls
11:00

BRKCRS-2823
Cisco SD-Access –
Firewall Integration
16:45

THU

BRKCRS-2818
Build a Software Defined Enterprise
with Cisco SDWAN & SD-Access
08:30

BRKCRS-2830
Cisco SD-Access – Lessons
learned from Design & Deployment
09:45

BRKCRS-2502
Best Practices for Design and
Deployment of Cisco SD-Access

BRKCRS-2825
Cisco SD-Access – Scaling the
Fabric to 100s of Sites
11:15

BRKCRS-3810
Cisco SD-Access deep dive
14:45

Keynote
17:00

Customer
Appreciation 18:30

FRI

BRKCRS-2819
Creating multi-domain architecture
using Cisco SD-Access

BRKCRS-3811
Cisco SD-Access –
Policy Driven Manageability
09:00

BRKCRS-2812
Cisco SD-Access – Integrating
with your existing network

BRKARC-2020
Cisco SD Access –
Troubleshooting the fabric

BRKCRS-2824
Intuitive Zero-Trust Design,
Migration When Securing
the SD-Access Workplace
11:30

Cisco SD-Access

IBN
Technology

Technical Depth

Scope is High-Level Design

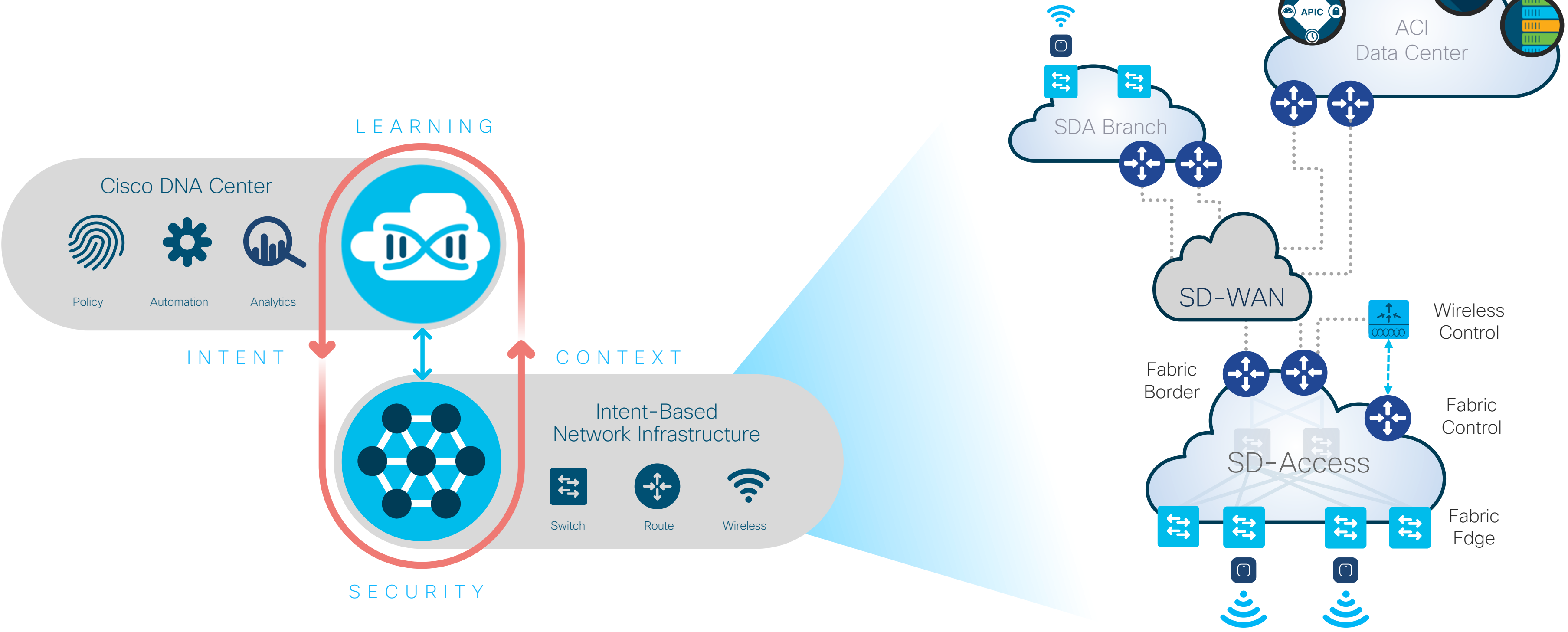
Looking @ the 30,000+ Foot View

There will be limited Technical Details

Only to explain the “What” & “Why”

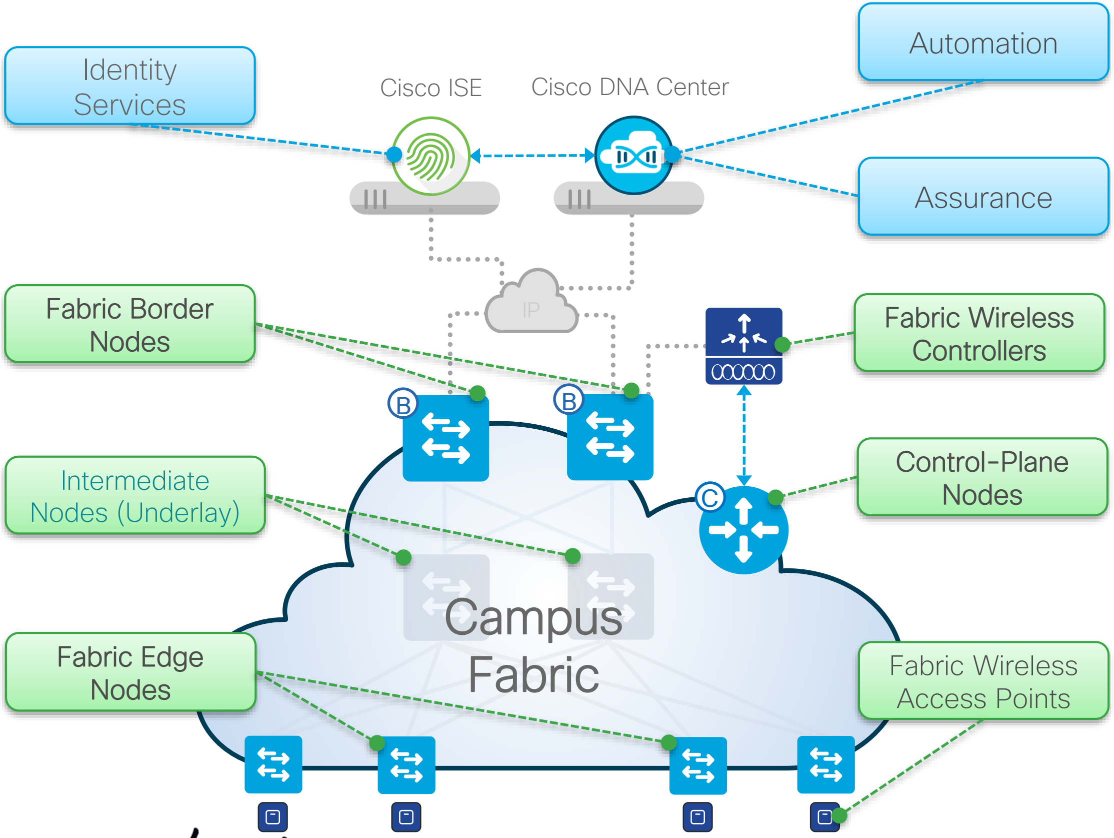
Cisco's Intent-Based Network

Delivered by Cisco Software Defined Access



Cisco SD-Access

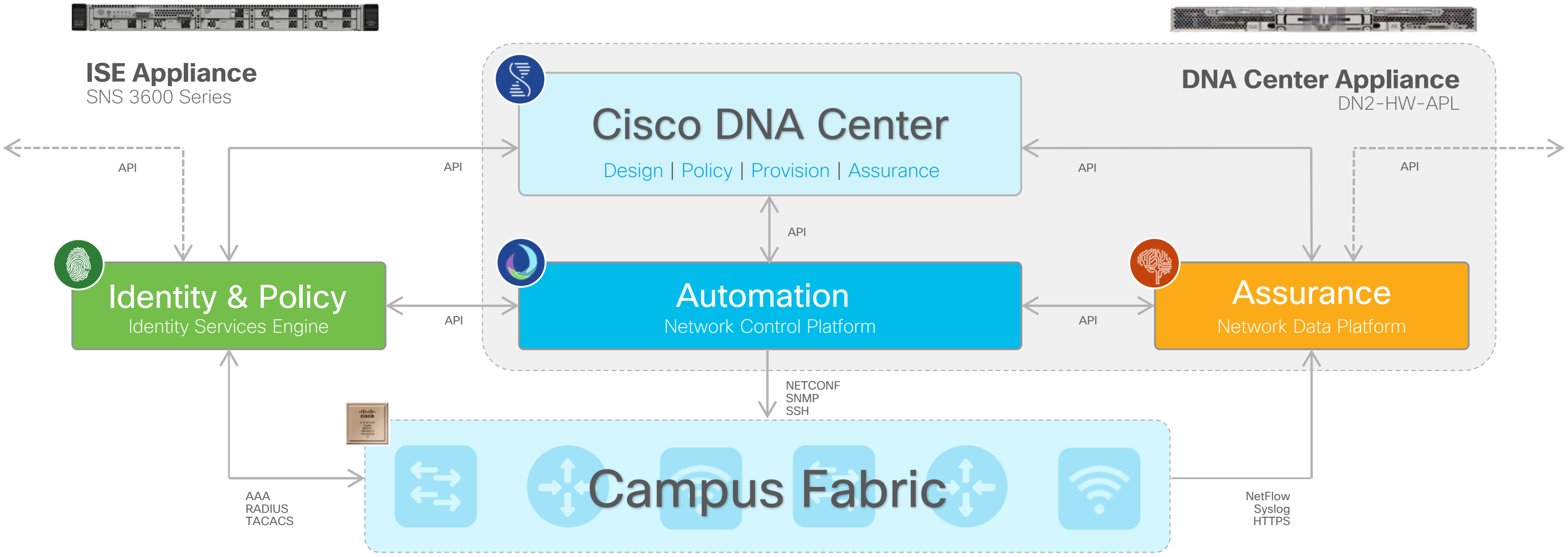
Fabric Roles & Terminology



- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

Cisco DNA Center

SD-Access – Key Components



Cisco Switches | Cisco Routers | Cisco Wireless

What's New?

Cisco DNA Center 1.3

Optimized for Distribution

SD-Access 1.2.10

February 2019

DNA Center 1.2.10, ISE 2.4 p6, IOS-XE 16.9.2s, AireOS 8.8

- SD-Access Extension for IoT (Beta)
- 3 node DNAC HA for Automation
- Catalyst 9800 Wireless Controller
- Fabric in a Box with Embedded Wireless on Catalyst 9300
- Nexus 7700 Series with M3 as Border, without MPLS license
- SDA-ACI Integration Improvements
- LAN Automation Enhancements

Optimized for Extension

SD-Access 1.3.0

June 2019

DNA Center 1.3.0, ISE 2.6 p1, IOS-XE 16.11.1s, AireOS 8.9

- SD-Access Extension for IoT (FCS)
- IPv6 overlay support for Wired + Wireless (AireOS) Endpoints
- Fabric Edge and Fabric in a Box on Catalyst 9500
- Fabric in a Box with Embedded Wireless on C9400, C9500
- SD-Access Border Simplification
- LAN Automation Enhancements

Optimized for Policy

SD-Access 1.3.3

NEW

January 2020

DNA Center 1.3.2, ISE 2.6 p2, IOS-XE 16.12.2s, AireOS 8.10

- Group-Based Access Control App (ACA)
- Application Visibility on Switches & WLCs
- Stealthwatch Security Analytics Service
- Cisco DNA Bonjour Service
- Firewall (ASA) support
- StackWise Virtual support
- L2 and Multicast Enhancements
- FiaB and eWLC Enhancements
- Intent APIs for SD-Access

Validated Designs

Design Strategy

CISCO VALIDATED DESIGN

The Challenge...

“I want to design and deploy a network”

Future Ready

On Time

Within Budget

Manageable

Best practices

Authorized Self-Study Guide
Implementing Cisco IOS Network Security (IINS)

LAN Design and Deployment using the Cisco Smart Business Architecture

Cisco live!

Design Options

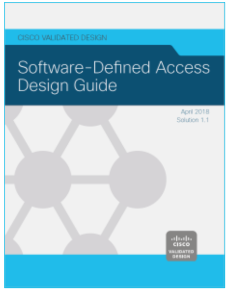
Platform Choices

Design References

TIP

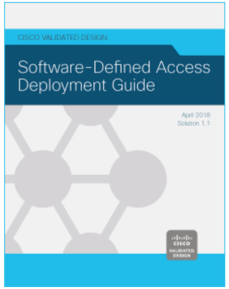
SDA CVD Documents

cisco.com/go/cvd/campus


CISCO VALIDATED DESIGN

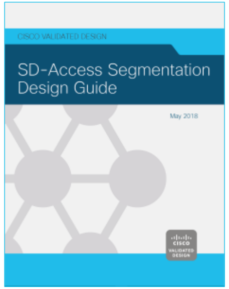
Software-Defined Access Design Guide

April 2018
Solution 1.1


CISCO VALIDATED DESIGN

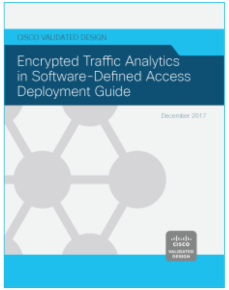
Software-Defined Access Deployment Guide

April 2018
Solution 1.1


CISCO VALIDATED DESIGN

SD-Access Segmentation Design Guide

May 2018

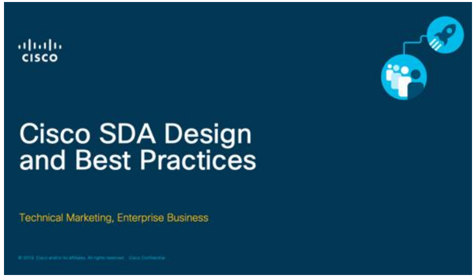

CISCO VALIDATED DESIGN

Encrypted Traffic Analytics in Software-Defined Access Deployment Guide

December 2017

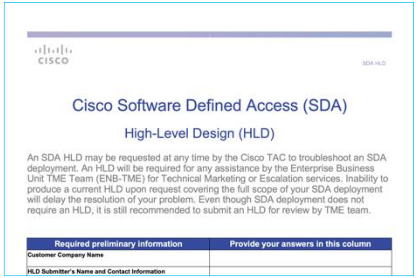
SDA Design Community

go2.cisco.com/SDA-Design


Cisco SDA Design and Best Practices

Technical Marketing, Enterprise Business

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


SDA HLD

Cisco Software Defined Access (SDA)

High-Level Design (HLD)

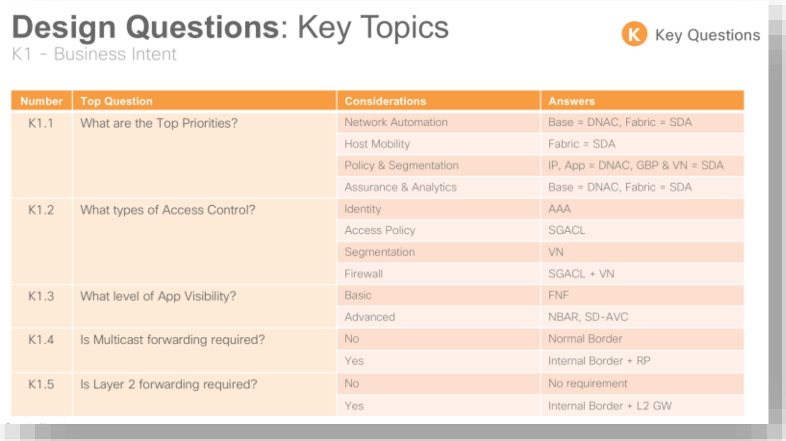
An SDA HLD may be requested at any time by the Cisco TAC to troubleshoot an SDA deployment. An HLD will be required for any assistance by the Enterprise Business Unit TME Team (ENB-TME) for Technical Marketing or Escalation services. Inability to produce a current HLD upon request covering the full scope of your SDA deployment will delay the resolution of your problem. Even though SDA deployment does not require an HLD, it is still recommended to submit an HLD for review by TME team.

Required preliminary information	Provide your answers in this column
Customer Company Name	
HLD Submitter's Name and Contact Information	

Design Strategy - End Goal

Utilizing this Design Strategy, you should be able to produce 2 key outcomes:

Network Requirements Doc (NRD)



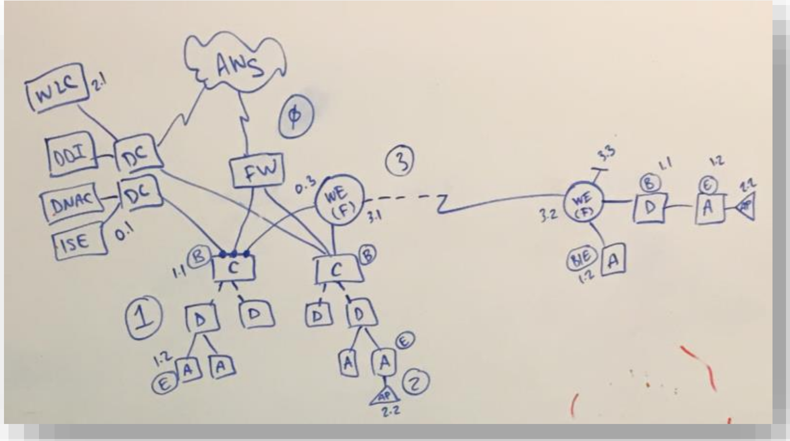
Design Questions: Key Topics

K1 - Business Intent

K Key Questions

Number	Top Question	Considerations	Answers
K1.1	What are the Top Priorities?	Network Automation	Base = DNAC, Fabric = SDA
		Host Mobility	Fabric = SDA
		Policy & Segmentation	IP, App = DNAC, GBP & VN = SDA
		Assurance & Analytics	Base = DNAC, Fabric = SDA
K1.2	What types of Access Control?	Identity	AAA
		Access Policy	SGACL
		Segmentation	VN
		Firewall	SGACL + VN
K1.3	What level of App Visibility?	Basic	FNF
		Advanced	NBAR, SD-AVC
K1.4	Is Multicast forwarding required?	No	Normal Border
		Yes	Internal Border + RP
K1.5	Is Layer 2 forwarding required?	No	No requirement
		Yes	Internal Border + L2 GW

High Level Design (HLD)



Design Strategy - Approach

SD-Access is an Enterprise Architecture

Divide and **Conquer**

Split the design into small manageable parts. Gather more details and set priorities

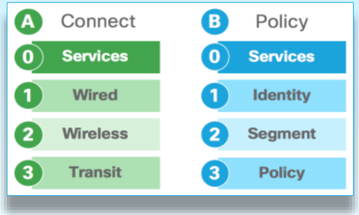
Grow as you **Go**

Start out small.
Build, expand, repeat.
Then connect them together

Design Strategy - Stages

4 Step Approach

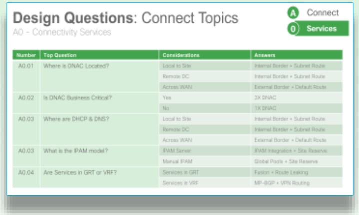
Planning



A Connect	B Policy
0 Services	0 Services
1 Wired	1 Identity
2 Wireless	2 Segment
3 Transit	3 Policy

- Define Scope
- Divide Tasks
- Set Priorities
- Order Steps

Questions



Design Questions: Connect Topics

A0 - Connectivity Services

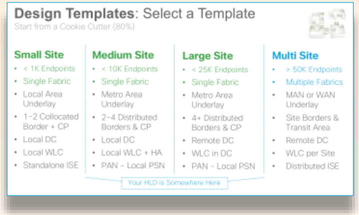
A Connect

0 Services

Number	Top Question	Considerations	Answers
A0.01	Where is DNAC Located?	Local to Site	Internal Border + Subnet Route
		Remote DC	Internal Border + Subnet Route
		Across WAN	External Border + Default Route
A0.02	Is DNAC Business Critical?	Yes	3X DNAC
		No	1X DNAC
A0.03	Where are DHCP & DNS?	Local to Site	Internal Border + Subnet Route
		Remote DC	Internal Border + Subnet Route
		Across WAN	External Border + Default Route
A0.03	What is the IPAM model?	IPAM Server	IPAM Integration + Site Reserve
		Manual IPAM	Global Pools + Site Reserve
A0.04	Are Services in GRT or VRF?	Services in GRT	Fusion + Route Leaking
		Services in VRF	MP-BGP + VPN Routing

- Ask Questions
- Key Points
- Connect Topics
- Policy Topics

Designs



Design Templates: Select a Template

Start from a Cookie Cutter (80%)

Small Site
- < 1K Endpoints
- Single Fabric
- Local Area Underlay
- 1-2 Collocated Border + CP
- Local DC
- Local WLC
- Standalone ISE

Medium Site
- < 10K Endpoints
- Single Fabric
- Metro Area Underlay
- 2-4 Distributed Borders & CP
- Local DC
- Local WLC + HA
- PAN - Local PSN

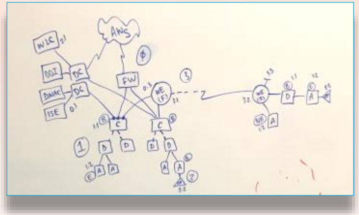
Large Site
- < 25K Endpoints
- Single Fabric
- Metro Area Underlay
- 4+ Distributed Borders & CP
- Remote DC
- WLC in DC
- PAN - Local PSN

Multi Site
- > 50K Endpoints
- Multiple Fabrics
- MAN or WAN Underlay
- Site Borders & Transit Area
- Remote DC
- WLC per Site
- Distributed ISE

Your HLD is Somewhere Here

- Based on Answer
- Based on Priority
- Based on Order
- Based on Scale

Customize



- Draw & Record
- Use Strategy
- Use Questions
- Use Templates

Planning & Preparation

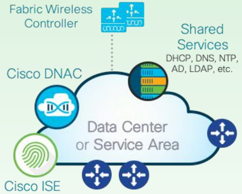
Design Strategy – Plan

4 Step Approach

Global Deployment

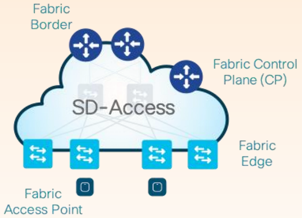
- Worldwide Scope
- Divided into Regions
- Scale of Network Devices, Endpoints per Region
- Determine Cisco DNA Center and ISE sizing

Shared Services


Fabric Wireless Controller
Shared Services
DHCP, DNS, NTP, AD, LDAP, etc.
Cisco DNAC
Data Center or Service Area
Cisco ISE

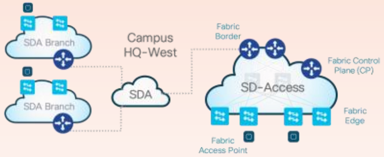
- Connections from Sites to Controllers
- DNA Center HA Cluster
- DNA Center Disaster Recovery
- ISE HA and Load-Balancing

Per Site Design



- Small, Medium and Large Site templates
- Fusion or Firewall
- Wireless Integration
- Per-Site VNs, IP Pools
- SGT assignment, Enforcement points
- Special Features (Multicast, L2, etc.)

Multi Domain



- Select Transit Type for Site-to-Site
- Interoperate with ACI or DC
- Interoperate with SDWAN or WAN
- Identity Federation
- Multi-Domain Policy

Design Strategy - Scope

“Connect” with –or– without “Policy”

TIP

A Connect Design

0 Services
- DNA Center
- DNS, DHCP & IPAM

1 Wired
- Fusion/Firewalls
- LAN Routers
- LAN Switches

2 Wireless
- SDA vs. OTT
- WLAN Controllers
- Access Points

3 Features
- L2 Broadcast
- IP Multicast
- Telemetry

B Policy Design

0 Services
- Identity Service Engine
- Outside ID Services

1 Identity
- Dynamic Assignment
- Static Assignment

2 Segment
- Virtual Networks
- Scalable Groups

3 Policy
- Firewall Rules
- Access Policies
- App Policies

C Transit
- MAN vs. WAN
- SDX vs. IP-Based

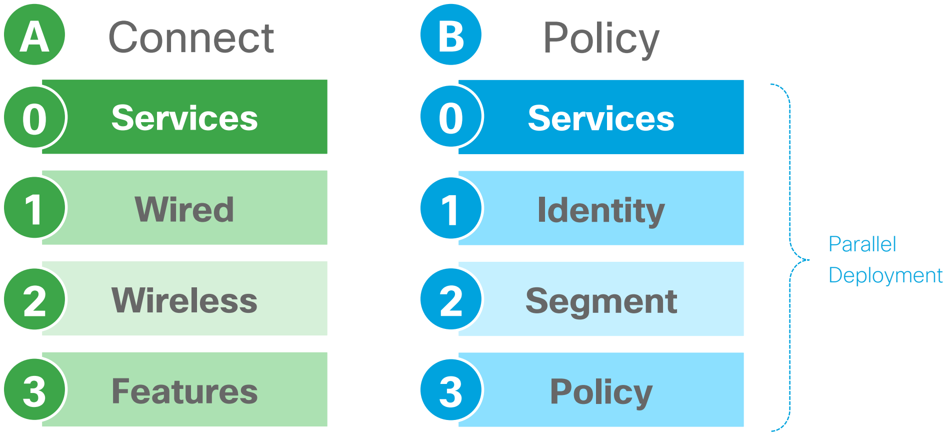
- Identity Propagation
- Multi-Domain Policy

Design Strategy - Divide Tasks

Parallel vs. Incremental

Parallel: Best for Greenfield

All of the elements are new and can be designed and deployed at the same time.

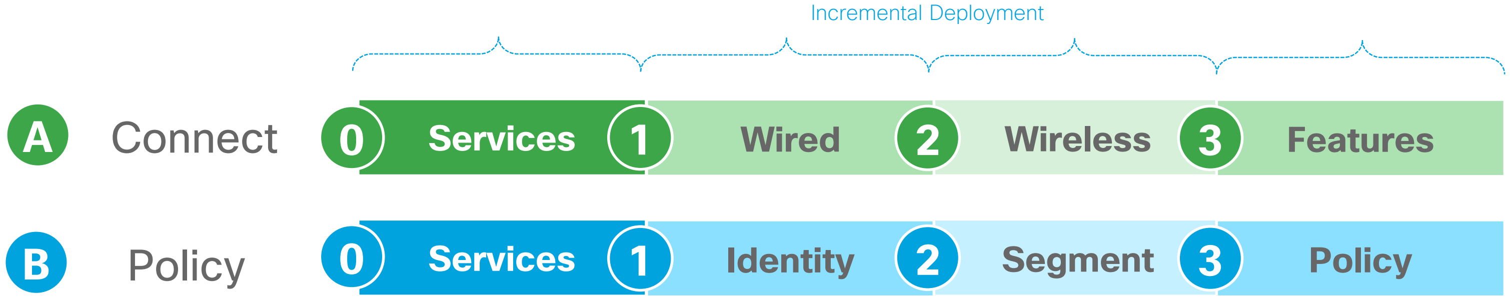


	A Connect	B Policy
0	Services	Services
1	Wired	Identity
2	Wireless	Segment
3	Features	Policy

Parallel Deployment

Incremental: Best for Brownfield

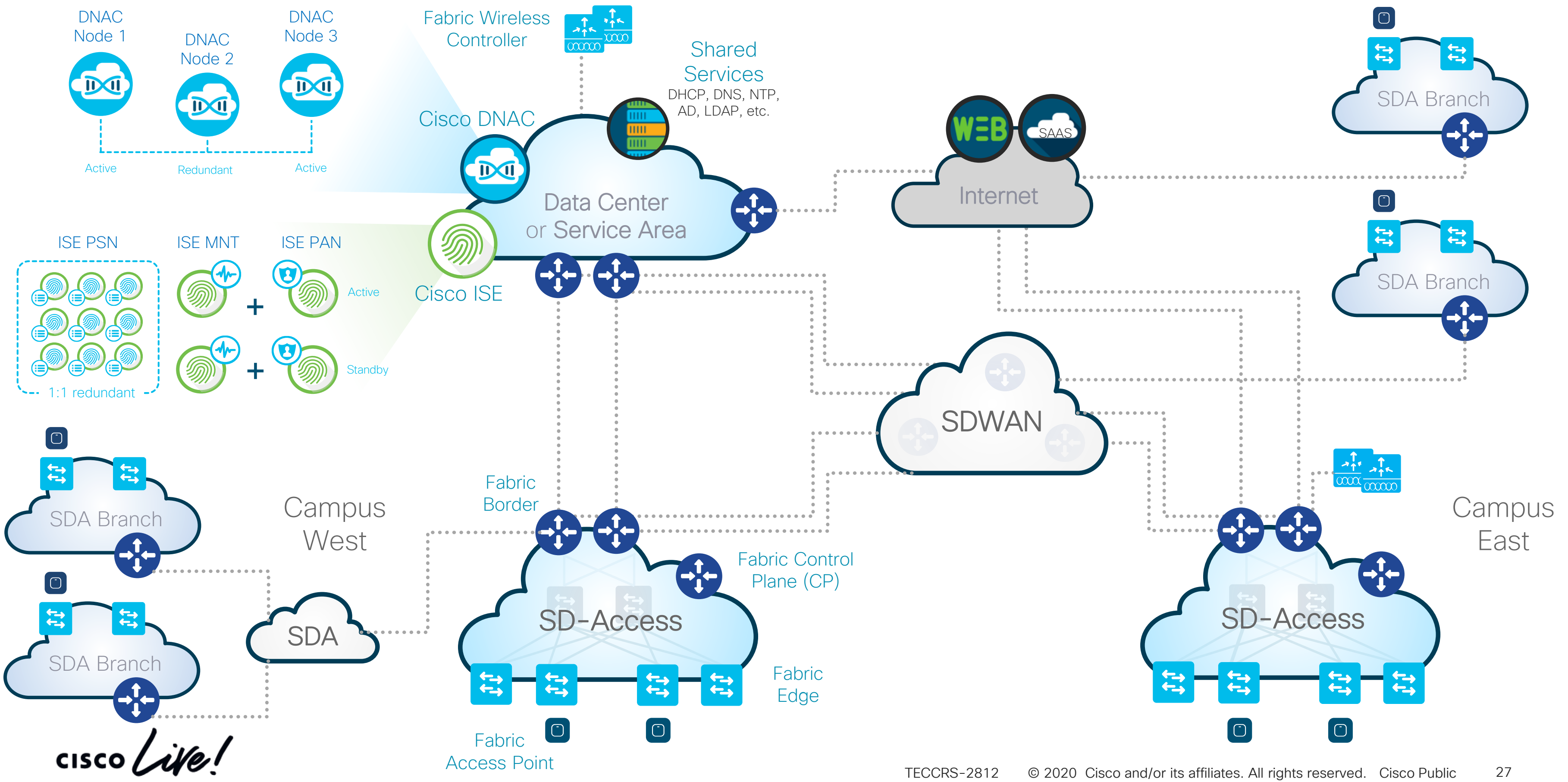
Some elements are new, others are existing, so each element should be deployed incrementally.



Incremental Deployment

	0	1	2	3
A Connect	Services	Wired	Wireless	Features
B Policy	Services	Identity	Segment	Policy

Design Overview & Terminology



Design Strategy

Requirement Questions

Design Questions - Requirements

Translating Business Intent into Technical Requirements

Can be 1001 Questions... Ask KEY Questions First

- Start with the “Business Intent” of the new design
- Start from a Global Perspective. Then Site-by-Site

Use a Modular approach to Divide & Conquer

- Start with KEY questions. Then Connect & Policy
- Step-by-Step, based on the Strategy & Priorities

Start the design as a Template ... then Customize

- Use the 80/20 rule. Templates cover 80%
- Templates have been tested and deployed
- Start out Simple. Then build up to Complex

Design Questions - Requirements

Translating Business Intent into Technical Requirements

K

Key Questions

Focus on Business Intent & Global Scope

A

Connect Questions

Focus on Topology & Features
(Per Site + Transit)

B

Comply Questions

Focus on Access & App Policy
(Per Site + Transit)

Design Questions - Key Points

Global / Regional Considerations

K Key Questions

- How many Regions?
  - Small, Medium or Large?
- Total number of Sites?
  - How many per Region?
- Total number of Endpoints?
  - How many per Region?
  - How many per Site?
- Total number of Nodes?
  - How many per Region?
  - How many per Site?

- Where will Services be located?
  - Local? DC? Over WAN?
  - What type of DCs?
  - Bandwidth or Latency limits?
- Is the DNA Center “Business Critical”?
  - Scale Considerations?
  - Redundancy Considerations?
- Is the ISE “Business Critical”?
  - Scale Considerations?
  - Redundancy Considerations?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Key Points

Transit Considerations

K Key Questions

- What is the Transit Underlay?
  - Metro Ethernet?
  - Private WAN (IP/MPLS)?
  - Internet Provider?
  - How many Providers?
- What types of Transits?
  - SD-Access?
  - SD-WAN?
  - IP-Based?
- Which Sites need Direct Internet?
  - Campus? Branch?
  - Via WAN or DC?
- Is VRF hand-off required?
  - All VRFs? Selective?
  - 1:1? 1:N? M:N?
  - Firewall considerations?
- Is SGT hand-off required?
  - All SGTs? Selective?
  - Native? Inline Tags? SXP?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Key Points

Site Considerations

K Key Questions

- Is this a Campus or Branch?
  - Campus? Branch?
  - Is there a local WAN?
- Is this a New or Existing Site?
  - Parallel? Incremental?
- Is this a Small, Medium or Large Site?
  - How many Users / Devices?
- Is this Site “Business Critical”?
  - Redundancy Considerations?
- What types of Border hand-off?
  - VRF & SGT Considerations?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Connect Topics

A0 - Connectivity Services

A Connect

0 Services

- Where are Connect Services located?
  - Where is DNA Center?
  - Where are DNS, DHCP, IPAM?
  - What is the IP Addressing?
  - Local? DC? Over WAN?
- Are Services in Global or VRF?
  - VRF Leaking (Fusion) involved?
  - Firewall Rules (DMZ) involved?

- What types of Services/Features?
  - Multicast or Broadcast?
  - Voice & Video (Collaboration)?
  - Data Collection (Netflow/SNMP)?
  - Client Services (mDNS)?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Connect Topics

A1 - Wired Considerations

A Connect

1 **Wired**

- How many Network Tiers?
  - What type(s) of Core/Border/CP node?
  - What type(s) of Access/Edge node?
  - Are there any Distribution/Intermediate?
- What is the Underlay?
  - What is the IP Addressing?
  - Automated Underlay?
  - Manual Underlay? What Protocol?
- Which nodes will be Control Plane?
  - Switch/Router/CSR?
  - Collocated or Distributed?
- Which nodes will be Border?
  - What type of hand-off? L2/L3?
  - What is the outside Protocol(s)?
  - Redundant Borders?
  - Collocated or Distributed?
- Which nodes will be Edge?
  - How many Edge nodes?
  - Any Edge @ Distribution?
- Will there be Extended Nodes?
  - How many Extended nodes?
  - What type of Edge connection?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Connect Topics

A2 - Wireless Considerations

A Connect

2 Wireless

- What type of Wireless?
  - Fabric Enabled Wireless?
  - Overlay Wireless (OTT)?
  - Mixed Mode (both)?
  - Cisco or 3rd Party?
- Which types of WLC?
  - How many Wireless Clients?
  - Where is the WLC connected?
  - Direct to Border? DC?
  - Redundancy considerations?
- Which types of APs?
  - How many Wireless APs?
  - What type of Edge connection?
  - How many APs per Edge?
- What about Guest Wireless?
  - Dedicated Guest VN?
  - Dedicated Guest CP/Border?
  - Central Web Auth (CWA)?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Connect Topics

A3 - Feature Considerations

A Connect

3 Features

- Do any Apps require L2 Broadcast?
  - How many Sites/Borders?
  - How many L2 Endpoints?
  - How many Pools (VLANs)?
  - ?
- Do any Apps require L3 Multicast?
  - New groups? Existing?
  - How many groups?
  - Where are the Source(s)?
  - Where are the Receiver(s)?
  - Where are the RPs?
- What types of Visibility/Telemetry?
  - Basic Flexible Netflow?
  - NBAR (AVC)?
  - External (SD-AVC)?
  - All flows? Some flows?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Policy Topics

B0 - Policy Services

B Policy

0 Services

- Where are Policy Services located?
  - Where is Cisco ISE?
  - Other ID/NAC Services?
  - Local? DC? Over WAN?
  - Cloud hosted?
- Are Services in GRT or VRF?
  - VRF Leaking (Fusion) involved?
  - Firewall Rules (DMZ) involved?
- Is the Cisco ISE “Business Critical”?
  - Scale Considerations?
  - Redundancy Considerations?

- What types of Policy Services?
  - Identity Services?
  - Firewall Services?
  - VPN/Encrypt Services?
  - IDS/IPS or NaaS/NaaE?
- Which Service controls Policy?
  - Cisco ISE?
  - Cisco DNAC + ACA?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Policy Topics

B1 - Identity Considerations

B Policy

1 Identity

- Do you need Static Assignment?
  - Where/Why is Static Identity used?
  - Which parts are Static? VLAN, IP?
  - Will these migrate to Dynamic?
- Do you need Dynamic Authentication?
  - Wired? Wireless? Both?
  - Where is Dynamic Identity used?
  - Do you use Device Profiling?
- What type(s) of Authentication?
  - 802.1X (EAPOL)?
  - MAC Address Bypass (MAB)?
  - Web Authentication (CWA)?
  - Easy Connect (AD Integration)?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Policy Topics

Segmentation Considerations

B Policy

2 **Segment**

- What areas need to be truly Isolated?
  - Separate Departments?
  - Secure Areas?
  - Guest Network?
  - Partners/Contractors?

- Where are VRFs Managed?
  - VRF Routing?
  - Firewalls? DMZ?
  - Local or End-2-End?
  - Scale considerations?
  - Redundancy considerations?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Policy Topics

Policy Considerations

- What types of Policies?
  - Access Control?
  - Quality of Service?
  - Policy Routing?
- What types of Access Control?
  - Basic Permit/Deny?
  - Complex L4 Ports?
  - Scale considerations?
- What types of Firewall Rules?
  - Basic Permit/Deny?
  - Complex L4 Ports?
  - Scale considerations?
- What types of Quality of Service?
  - Basic (Default) Queuing?
  - Complex Classification?
- What types of Policy Routing?
  - Traffic Engineering/Steering?
  - Redirect/Cache Services?
  - Redundancy considerations?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Strategy

Global Design

Solution Scale

Multiple Dimensions to Consider – Overall Scale is Cisco DNA Center

Cisco DNAC

Overall Scale
Cisco DNA Center

* Based on DN2-HW-APL-XL

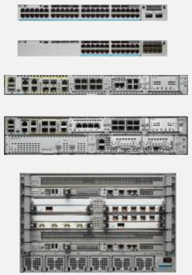
	Cisco DNAC (Overall Scale)	Cisco DNAC (Per Fabric Scale)
No. of Endpoints Max concurrent endpoints	*100,000 (40K Wired + 60K Wireless)	Same as Overall
No. of Fabric Nodes Includes all devices (Switches, Routers + WLC)	*5000	1000/Site
Access Points No of AP's + Sensors	*12,000 (200 Sensors)	Same as Overall
DNAC Sites No of Fabrics	*2000	N/A
Virtual Networks No of VN's	No Limit	256/Site
IP Pools Max No. of IP Pools	No Limit	600/Site
No. of Ports Physical and virtual across all devices	*480,000	Same as Overall

Scale Numbers

SD-Access

	SDA
Fabric Devices Max devices per Fabric	N/A
Access Points Max number of AP's	No. of Ports (100 AP/Site)
Client Endpoints Scalable Groups	CP Entries (3K – 200K)
IP Pools IP subnets (VLAN's)	N/A
Sites	N/A
Max Ports	No. of Ports
Max VN's	64 – 4K

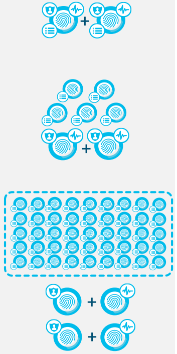
Scale Numbers



Cisco ISE

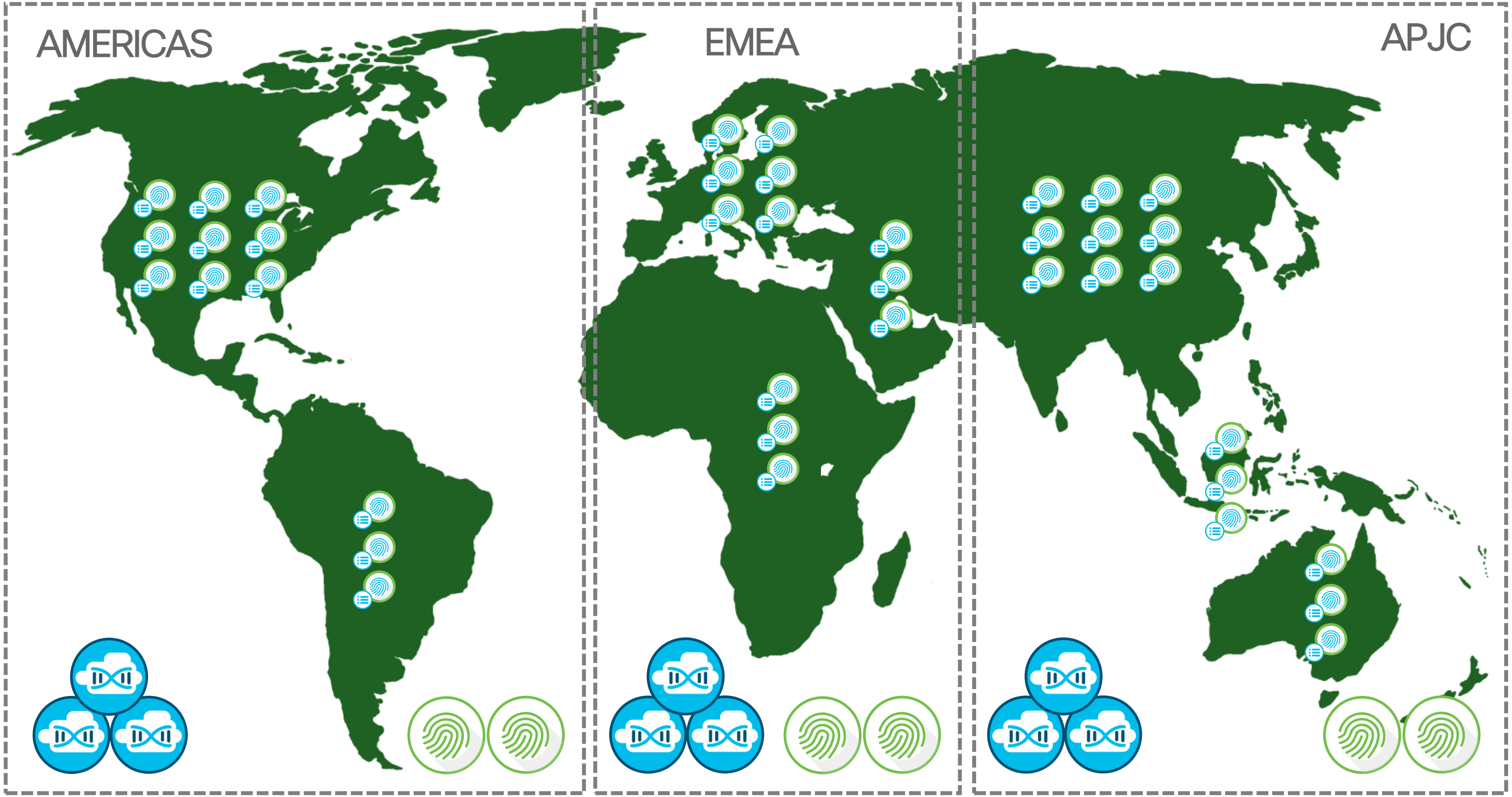
	Cisco ISE
Fabric Devices Max devices per Fabric	N/A
Access Points Max number of AP's	Max NAD devices
Client Endpoints Scalable Groups	10,000 – 2M
IP Pools IP subnets (VLAN's)	N/A
Sites	N/A
Max Ports	N/A Max 100K NAD
Max VN's	N/A

Scale Numbers



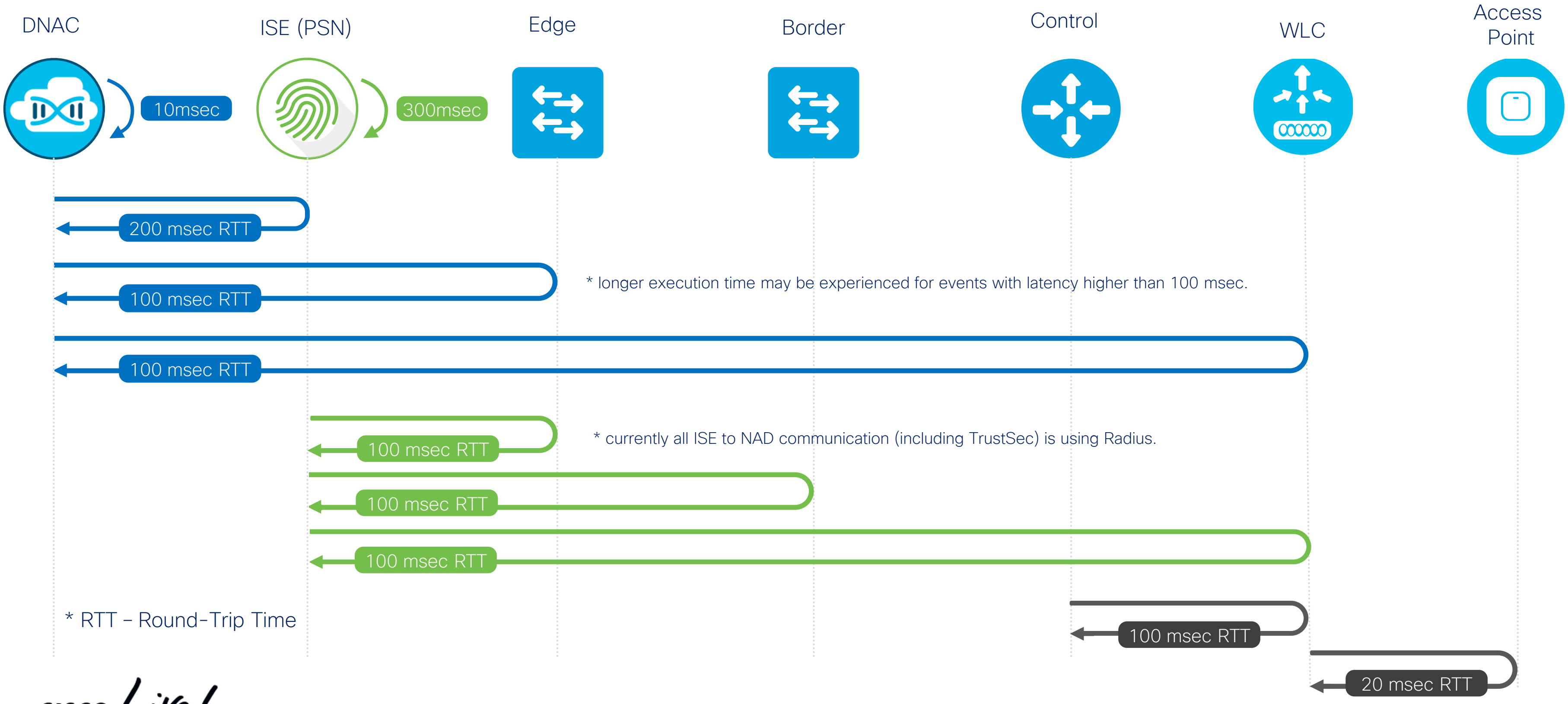
Global Design

Regional Controllers – Based on Scale & Latency



SD-Access Considerations

Latency Requirements (RTT)



* longer execution time may be experienced for events with latency higher than 100 msec.

* currently all ISE to NAD communication (including TrustSec) is using Radius.

* RTT – Round-Trip Time

A Connect

0 **Services**

Global Design

Connectivity Services

cisco Live!

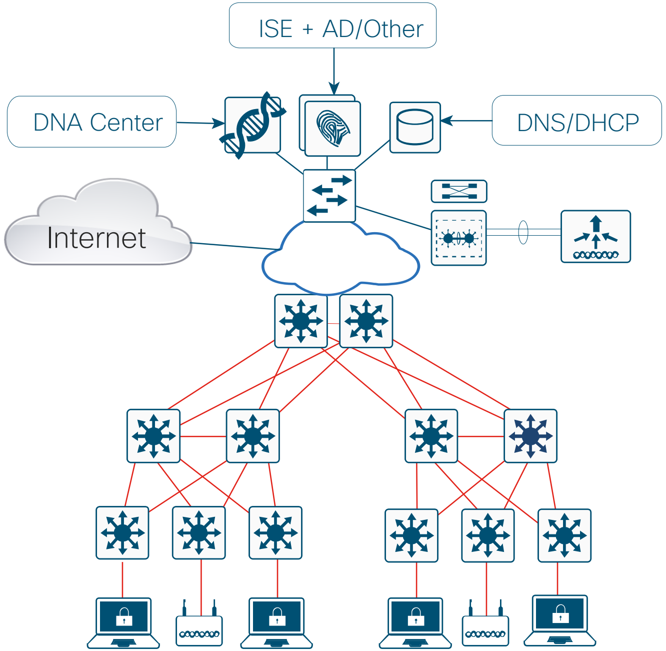
Connectivity Services

DNA Center Design for SD-Access

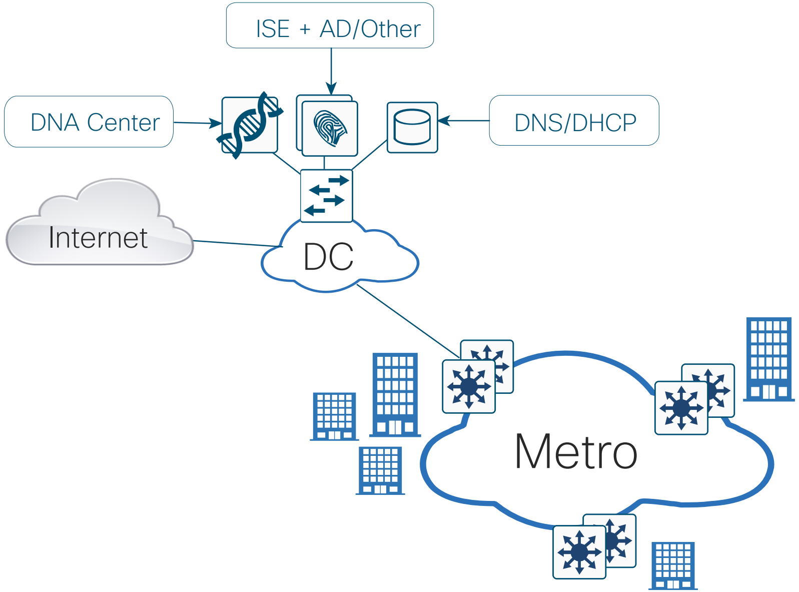
A Connect

0 **Services**

Local DC or Services Block



Remote DC (Over MAN/WAN)



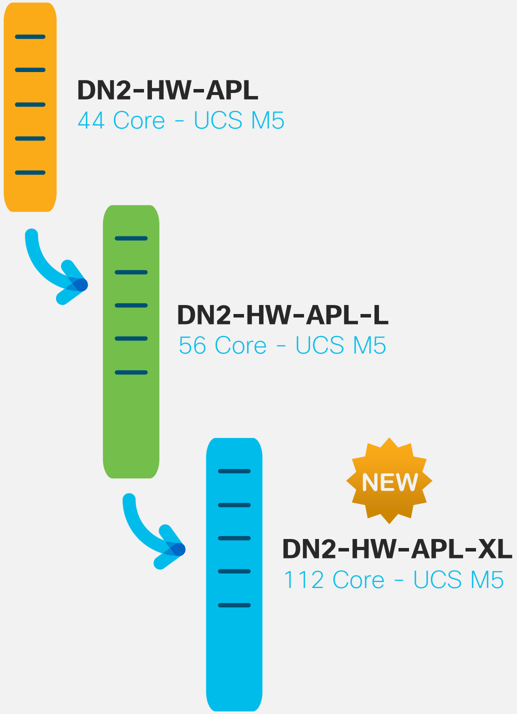
www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/datasheet-listing.html

Cisco DNA Center

Overall "Solution Scale" is Driven by Cisco DNAC

Cisco DNAC 1.3

		Cisco DNA Center		
		DN2-HW-APL 44 Core- UCS M5	**DN2-HW-APL-L** 56 Core- UCS M5	**DN2-HW-APL-XL** 112 Core- UCS M5
Infrastructure	Switches, Routers & WLC	1000	2000	5000
	Access Points	4000	6000	12000
	Endpoints (Wired + Wireless)	25K	40K	100K
	Sites	500	1000	2000
	Fabric Nodes	500/Site	600/Site	1000/Site
	IP Pools	300/Site	500/Site	600/Site
	Virtual Networks	64/Site	64/Site	256/Site
	Access Policies	5K	10K	25K

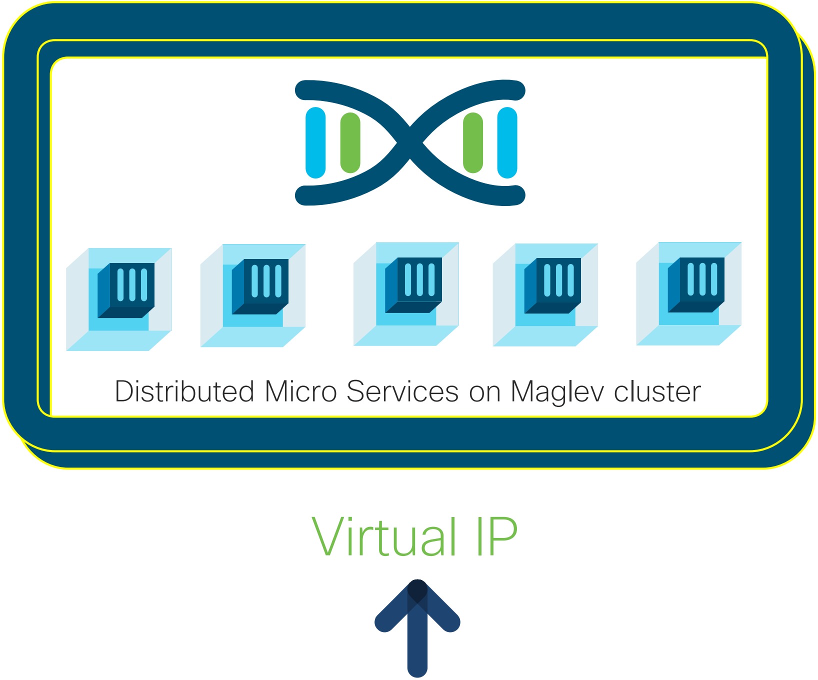


Cisco DNA Center

High Availability Cluster

A Connect

0 Services



1 or 3 appliance HA Cluster (more in future)

- Odd number to achieve quorum of distributed system

Seen as 1 logical DNAC instance

- Connect to Virtual (Cluster) IP
- Rare need to access individual nodes (e.g. SSH)

2 nodes active/sharing + 1 redundant

- Some services run multiple copies spread across nodes (e.g. databases)
- Other services run single copy and migrate from failed to redundant node

Single Appliance for Cisco DNA (Automation + Assurance)

Shared Services

IP Address Management

A Connect

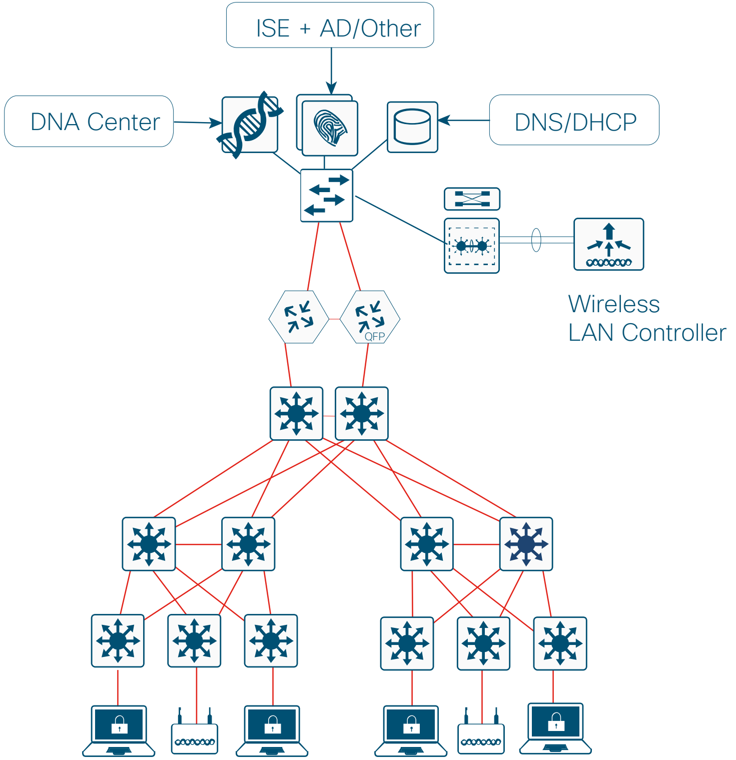
0 Services

IPAM Integration Considerations

- IPAM connection is a Pull model
- Used for acquisition of IP Pools (not DHCP, DNS, etc.)

DHCP scopes for SD-Access

- Requires Option 82 reflection
- Requires Fabric IP Pools (Border SVI) to be leaked to Shared Services
- Fabric IP pools should not overlap



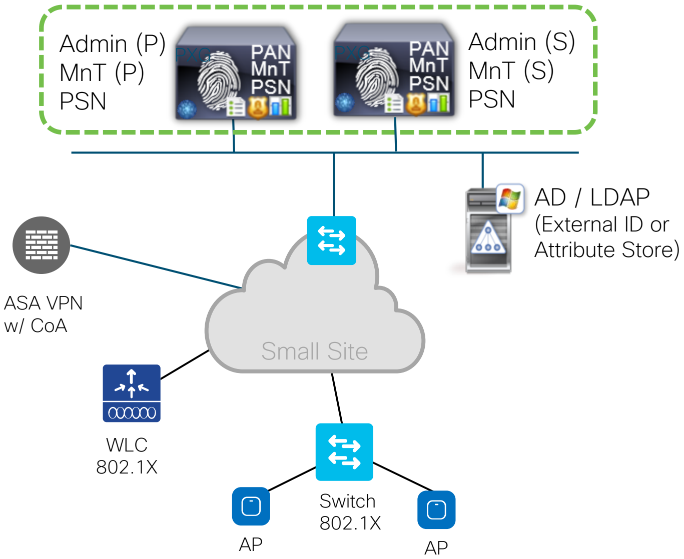
Global Design

Policy Services

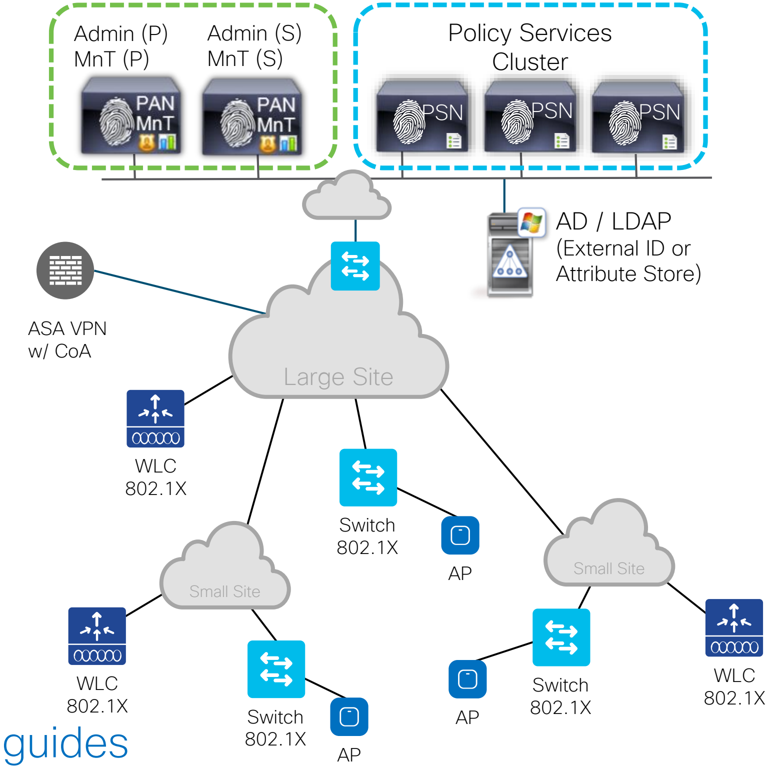
Policy Services

ISE Design for SD-Access

Standalone ISE + HA



Distributed ISE + HA



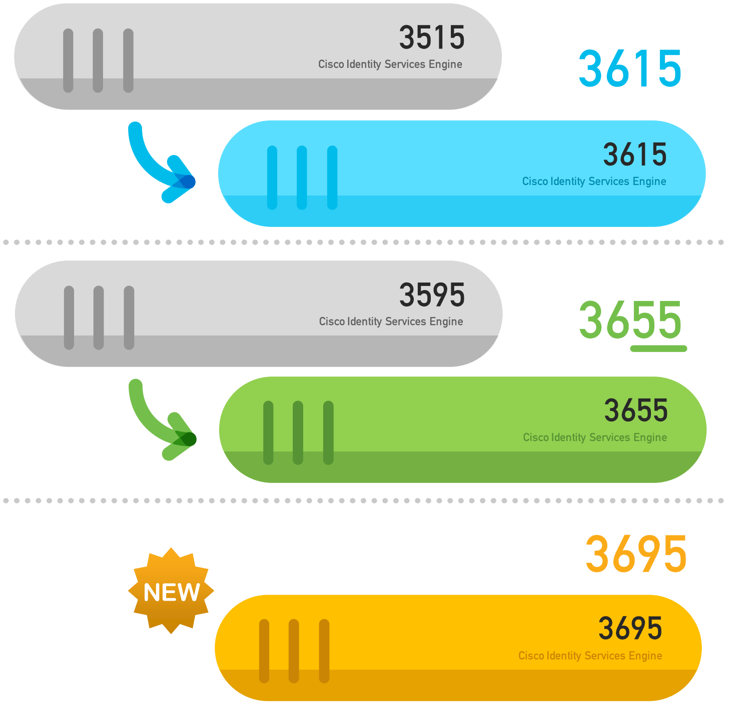
http://cs.co/ise-guides

Cisco ISE

SNS-3600 Appliances

B Policy

0 Services



3515
Cisco Identity Services Engine
3615
3615
Cisco Identity Services Engine
3595
Cisco Identity Services Engine
3655
3655
Cisco Identity Services Engine
NEW
3695
3695
Cisco Identity Services Engine

What are we solving?

- Increased endpoint capacity per appliance and deployment
- UCS M4 End Of Sale – Feb 2019

How do we solve it?

- New appliances based on UCS M5

Prerequisites

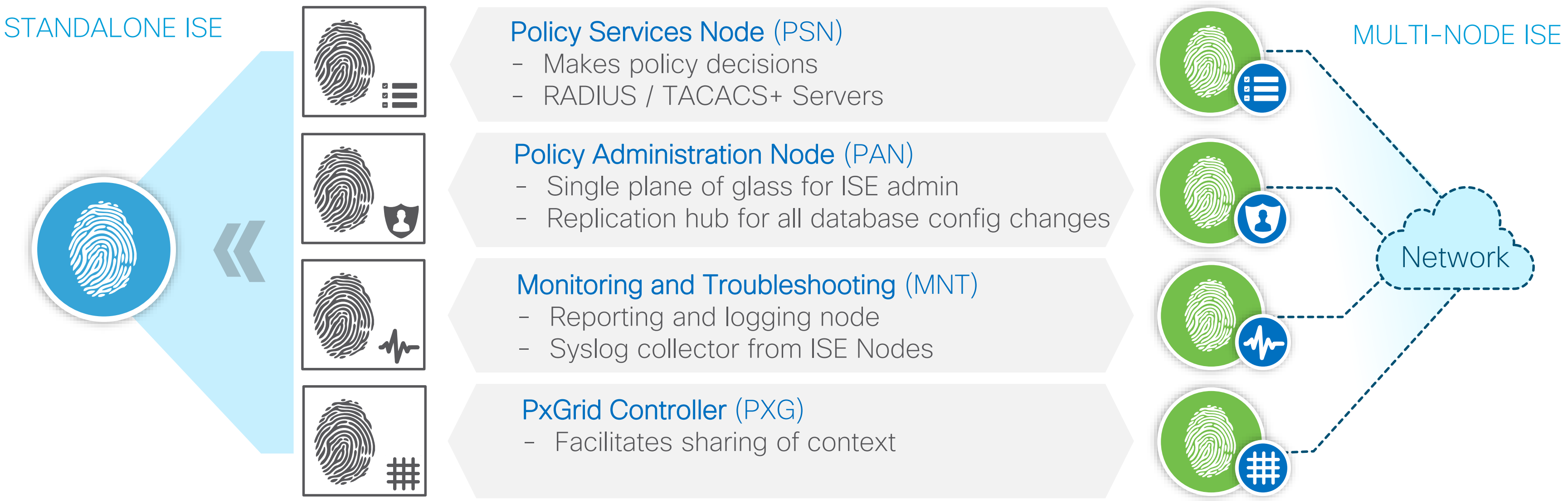
- Must be running ISE 2.6
- http://cs.co/ise-feedback

Cisco ISE

Deployment Options

B Policy

0 **Services**



Policy Services Node (PSN)
- Makes policy decisions
- RADIUS / TACACS+ Servers

Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Replication hub for all database config changes

Monitoring and Troubleshooting (MNT)
- Reporting and logging node
- Syslog collector from ISE Nodes

PxGrid Controller (PXG)
- Facilitates sharing of context

Single ISE Node (Virtual / Appliance)	Multiple Nodes (Virtual / Appliance)
Up to 20,000 concurrent endpoints	Up to 500,000 concurrent endpoints

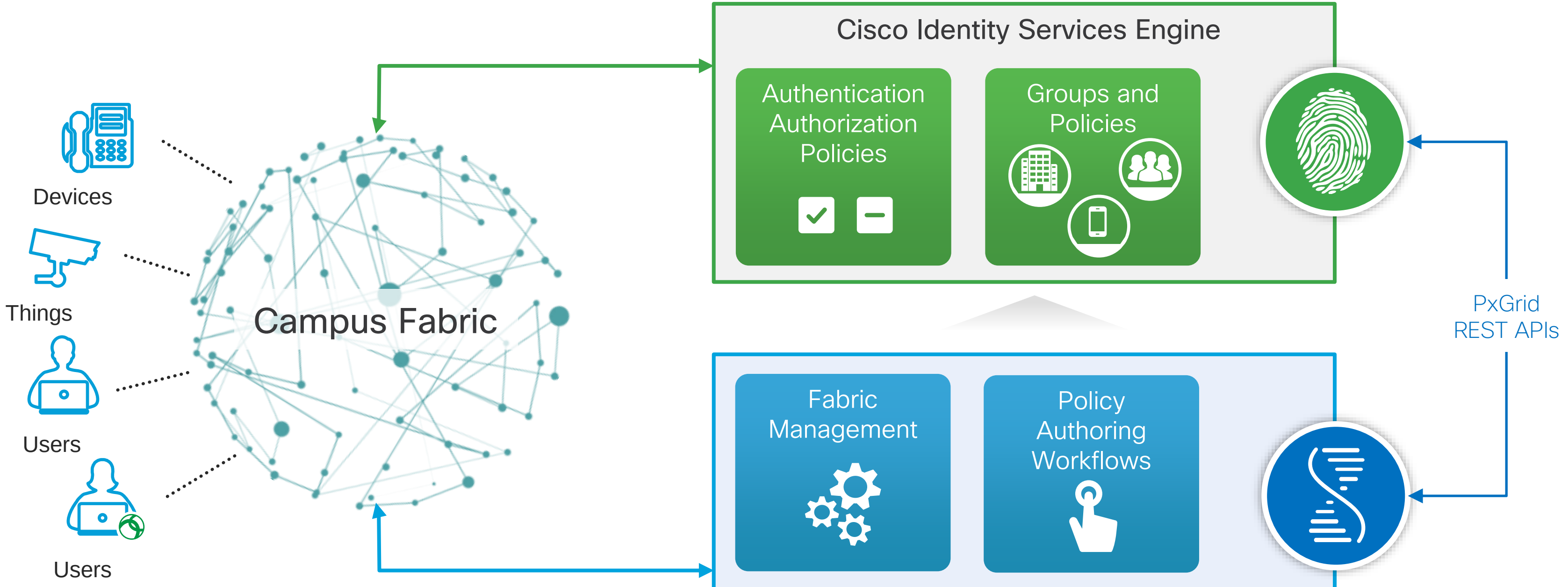
http://cs.co/ise-guides

DNA Center and ISE integration

Identity and Policy Automation

B Policy

0 **Services**



DNA Center and ISE integration

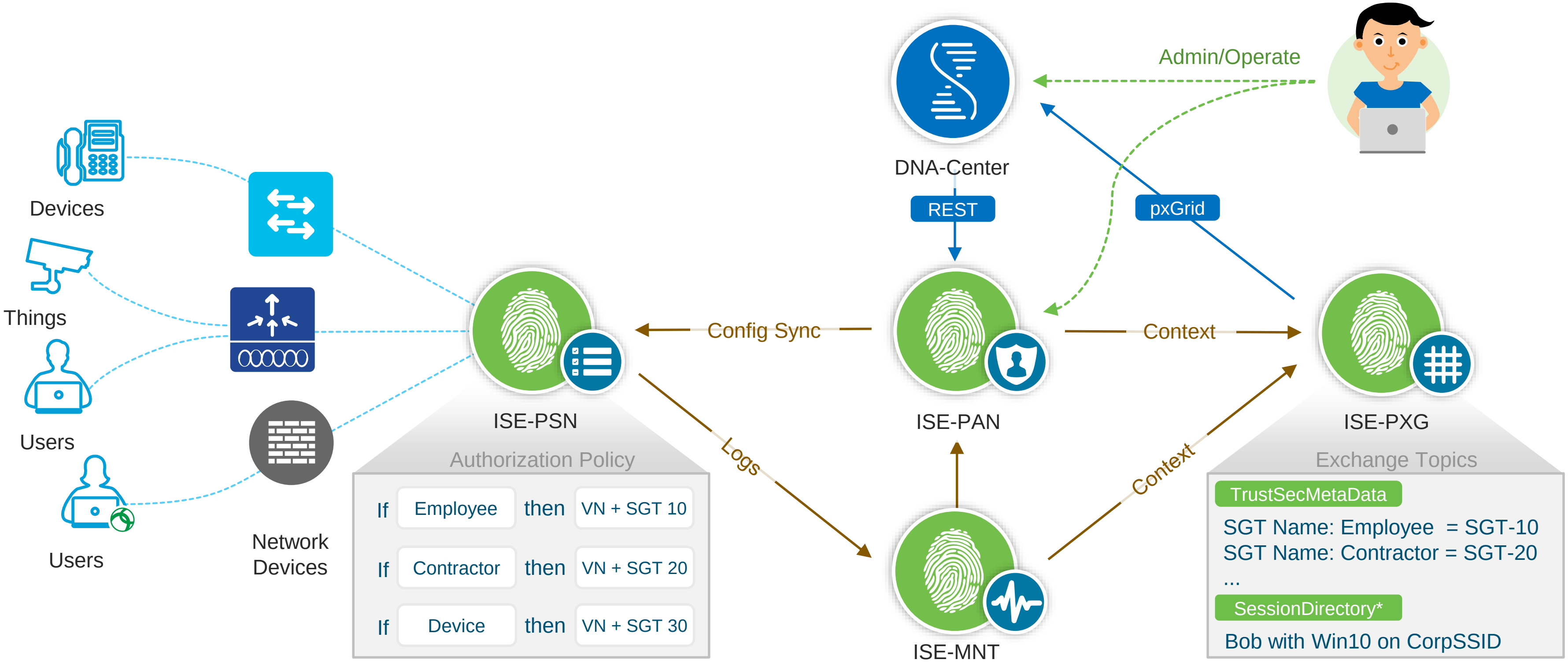
Top Considerations – Before DNAC 1.3 & ISE 2.4

- You must deploy one or more ISE version 2.3+ nodes on your network.
- If you use a multi-host ISE deployment, integrate with the Policy Admin Node (PAN).
- PxGrid service must be enabled on the ISE admin node that you plan to integrate.
- The ISE node must have SSH enabled.
- The ISE node must be reachable on the IP address of eth0 interface from DNA Center.
- The ISE CLI and GUI user accounts must use the same username and password

Cisco ISE roles in SD-Access

B Policy

0 **Services**



Authorization Policy

If	Employee	then	VN + SGT 10
If	Contractor	then	VN + SGT 20
If	Device	then	VN + SGT 30

Exchange Topics

TrustSecMetaData

SGT Name: Employee = SGT-10
SGT Name: Contractor = SGT-20
...

SessionDirectory*

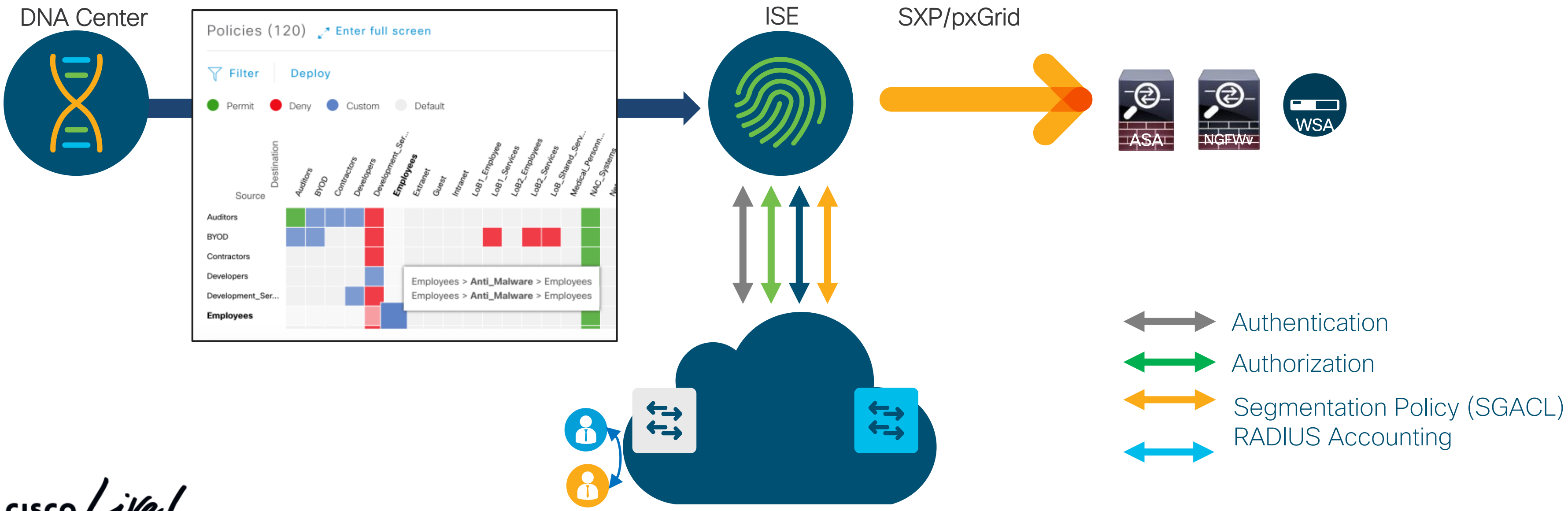
Bob with Win10 on CorpSSID

* Example Only: Not used today

GBAC integration with ISE NEW

Top Considerations – New in DNAC 1.3.1

Define all Access Control Policies in DNAC
Synched to ISE (includes SG/VN/Pool association)
ISE Authorization Profiles select Scalable Group and VN / IP Pool
NAD receives SGT in RADIUS AuthZ response
NAD requests policy download (as needed) based on SGT



Policies (120) Enter full screen

Filter | Deploy

● Permit ● Deny ● Custom ○ Default

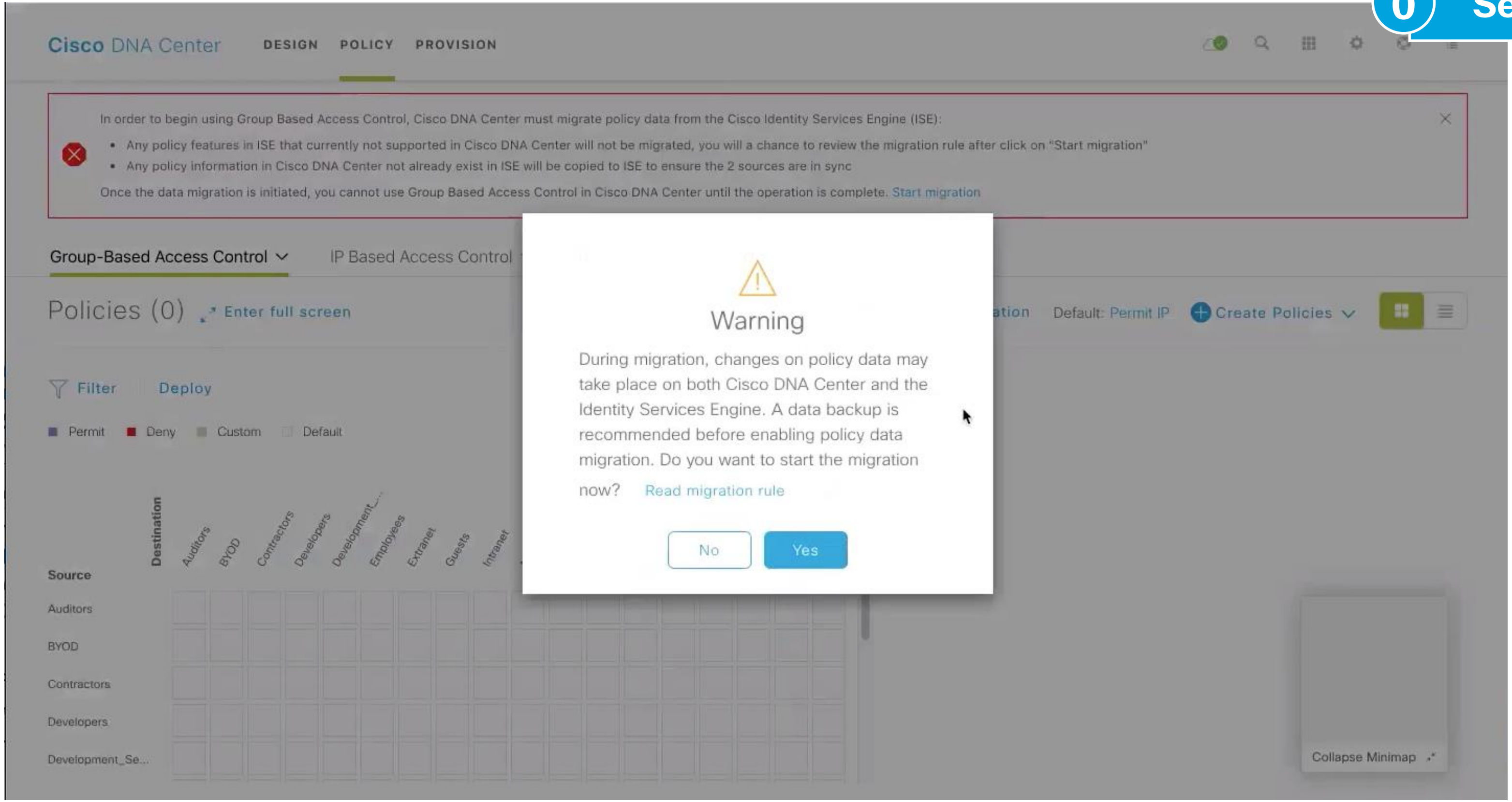
Source \ Destination	Auditors	BYOD	Contractors	Developers	Development_Ser...	**Employees**	Extranet	Guest	Intranet	LoB1_Employee	LoB1_Services	LoB2_Employees	LoB2_Services	LoB_Shared_Serv...	Medical_Personn...	NAC_Systems	Ne...
Auditors	🟩	🟦	🟦	🟦	🟥											🟩	
BYOD	🟦	🟦			🟥						🟥		🟥	🟥		🟩	
Contractors					🟥											🟩	
Developers					🟦												
Development_Ser...				🟦	🟥												
Employees					🟥	🟦										🟩	

Employees > **Anti_Malware** > Employees
Employees > **Anti_Malware** > Employees

Policy Migration / Sync with ISE

B Policy

0 **Services**



In order to begin using Group Based Access Control, Cisco DNA Center must migrate policy data from the Cisco Identity Services Engine (ISE):

- Any policy features in ISE that currently not supported in Cisco DNA Center will not be migrated, you will a chance to review the migration rule after click on "Start migration"
- Any policy information in Cisco DNA Center not already exist in ISE will be copied to ISE to ensure the 2 sources are in sync

Once the data migration is initiated, you cannot use Group Based Access Control in Cisco DNA Center until the operation is complete. Start migration

Warning

During migration, changes on policy data may take place on both Cisco DNA Center and the Identity Services Engine. A data backup is recommended before enabling policy data migration. Do you want to start the migration now? Read migration rule

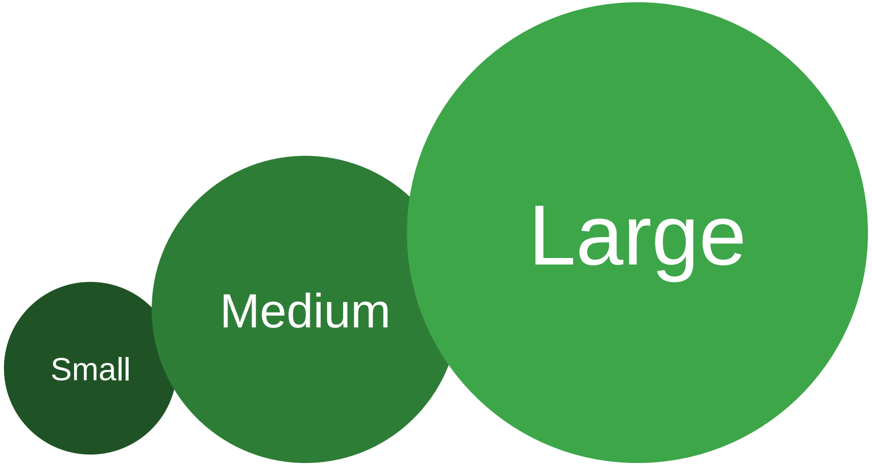
No Yes

Design Strategy
Site Templates

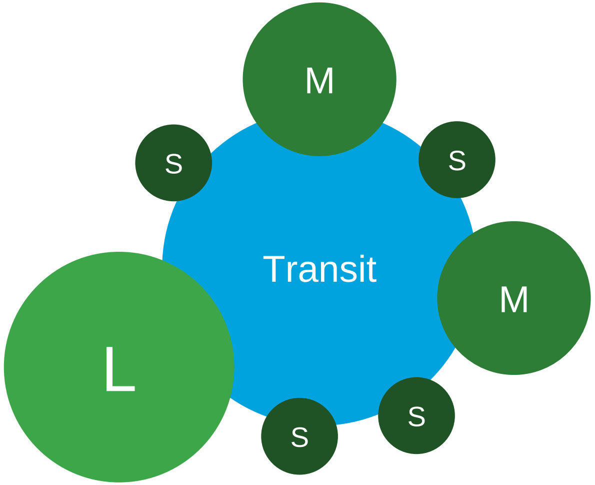
High Level Design - Templates

Start from a Cookie Cutter (80%)

Basic Goal is for fewer, larger Fabric Sites



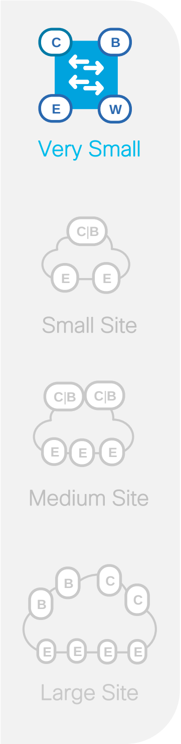
Some Needs require split into Multiple Sites



- ✓ Underlay Network (MTU, Latency, etc.)
- ✓ Wireless Client Roaming (< 20ms Latency)
- ✓ Direct Internet Access (@ Remote Sites)
- ✓ Survivable Remote Sites (Local CP/Borders)

Very Small Site

Fabric In A Box (FIAB)



Overview

- **Single Branch or Wiring Closet (IDF)**
- **Total endpoints < 2K** (software limit)
- Border, CP, Edge and WLC on a single box

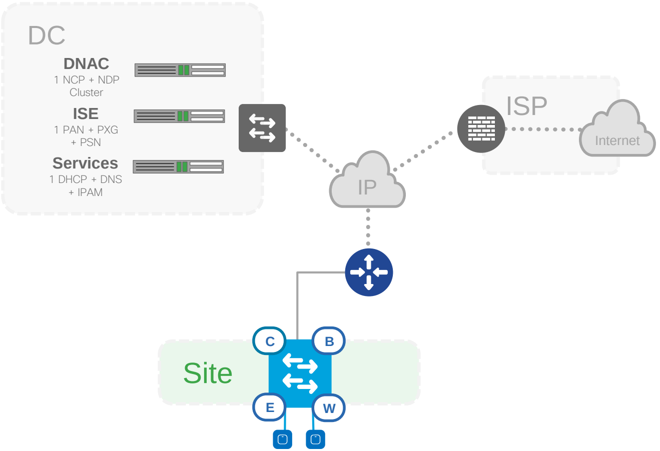
Benefits

- Reduces cost of SDA for very small sites
- Supports Embedded-Wireless on C9K (as of SDA 1.2.10 & IOS-XE 16.10.1)
- Limited Survivability for the CP & Border

NOTE: Platforms scale may be higher but these are solution tested numbers

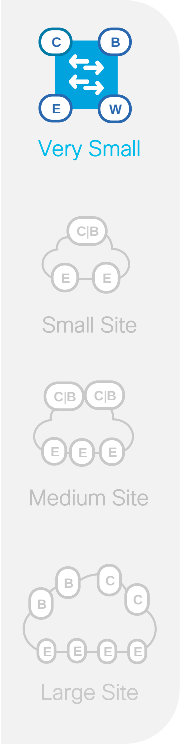
	Border, Control and Edge		
	9300	9400	9500
End Points/Hosts	< 2K	< 2K	< 2K
Fabric Nodes	1	1	1
Virtual Networks	< 8	< 8	< 8
IP Pools	< 8	< 8	< 8
Access Points (eWLC limit)	100	100	100
	B, CP & FE		

Sample Topology



Very Small Site

Fabric In A Box (FIAB) + Stacking



Overview

- **Single Branch or Wiring Closet (IDF)**
- **Total endpoints < 2K** (software limit)
- Border, CP, Edge and WLC on a single box
- **Max of 8 switches** in a Stack
  - All the stack members must be the same platform
  - If a stack member fails, the next available member takes over the CP and Border functions

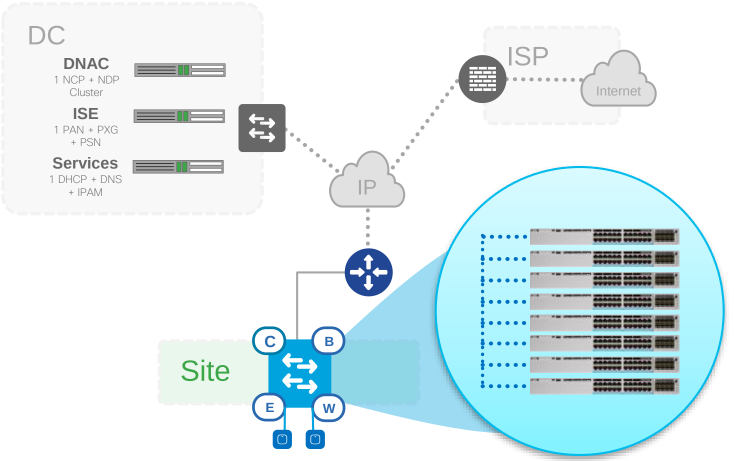
Benefits

- Reduces cost of SDA for very small sites
- Supports Embedded-Wireless on C9K (as of SDA 1.2.10 & IOS-XE 16.10.1)
- Improved Survivability for CP & Border
- Additional ports available for endpoints

NOTE: Platforms scale may be higher but these are solution tested numbers

	Border, Control and Edge
	9300
End Points/Hosts	< 2K
Fabric Nodes	1
Virtual Networks	< 8
IP Pools	< 8
Access Points (eWLC limit)	100
	B, CP & FE

Sample Topology



cisco Live!

Small Site

NOTE: Platforms scale may be higher but these are solution tested numbers

	Border, Control		Edge	
	9300	9500	9300	9200
End Points/Hosts	< 10K	< 10K	< 10K	< 2K
Fabric Nodes	2 CP+B (Collocated)	2 CP+B (Collocated)	< 25	< 25
Virtual Networks	< 32	< 32	< 32	< 4
IP Pools	< 100	< 100	< 100	< 100
Access Points			< 100	< 100
	B + C		E	

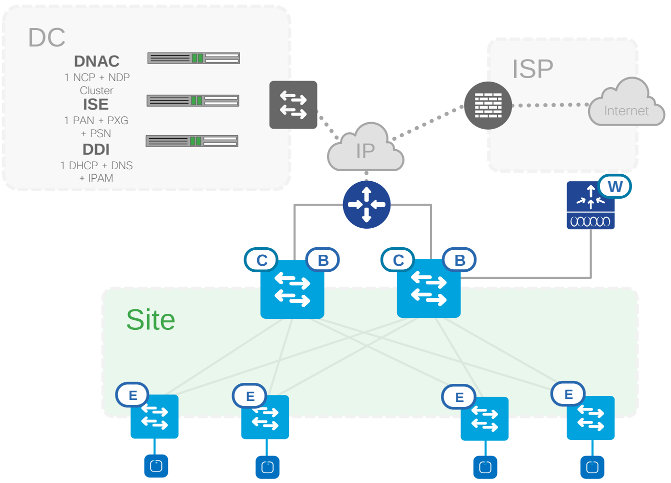
Overview

- Tends to be single Building or Office
- **2 Tier with one or few wiring closets** (IDFs)
- **Total endpoints < 10K** (recommended)
- 1-2 Collocated Border & CP on same box
  - Redundancy for Border or CP
- 1-2 Local Wireless Controller

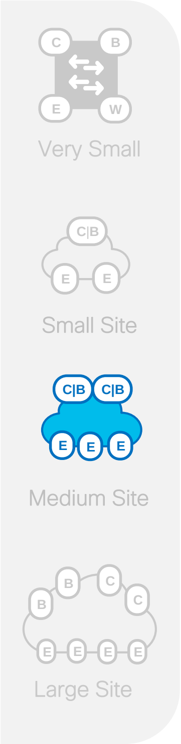
Benefits

- Simple Collocated CP + External Border (Single Exit)
- Flexibility & load-distribution with dedicated Edges
- Increased wireless scale with Local WLC
- Supports Embedded-Wireless on C9K (as of SDA 1.2.10 & IOS-XE 16.10.1)
- Provides <1000 dynamic authentications
- Provides <250 group-based policies

Sample Topology



Medium Site



Overview

- Tends to be a few Buildings and/or Floors
- **2-3 Tier with Multiple wiring closets** (MDF & IDF)
- **Total endpoints < 25K** (recommended)
- 1-2 Collocated Border & CP on same box
  - use dedicated CP for better redundancy
- 1-2 Local Wireless Controller
- Dedicated Edge (9300 stacks or 9400 modular)

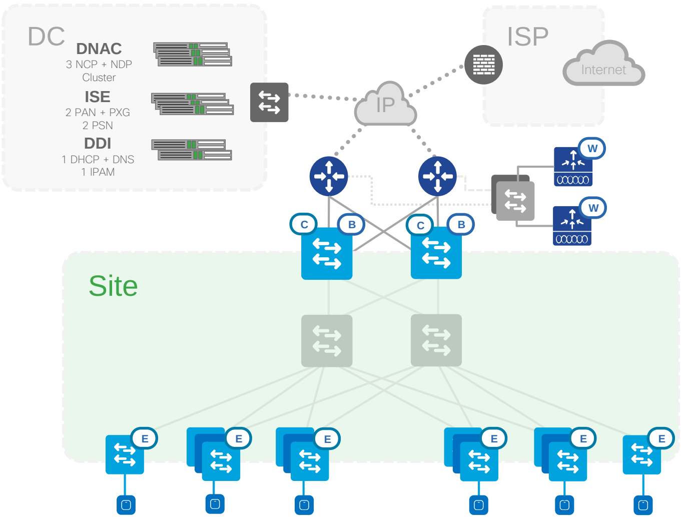
Benefits

- Increased scale over a small design
- Can choose Co-located or Distributed CP + Border (Single Exit) design
- Increased WLC scale, bandwidth and redundancy via Services Block or local Data Center
- < 25,000 dynamic authentications
- < 1000 group-based policies

NOTE: Platforms scale may be higher but these are solution tested numbers

	Border, Control		Edge	
	9500	9400	9300	9200
End Points/Hosts	< 25K	< 25K	< 25K	< 2K
Fabric Nodes	2 B, 2 C	2 B, 2 C	< 250	< 250
Virtual Networks	< 64	< 64	< 64	< 4
IP Pools	< 200	< 200	< 200	< 100
Access Points	< 1000	< 1000	<1000	< 100
	B + C		E	

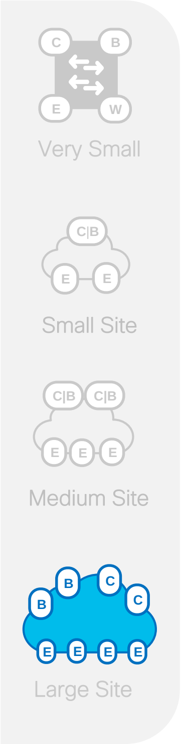
Sample Topology



Large Site

NOTE: Platforms scale may be higher but these are solution tested numbers

	Border, Control		Fabric Edge	
	9600	9500	9400	9300
End Points/Hosts	< 50K	< 50K	< 50K	< 50K
Fabric Nodes	4 C, 4 B	4 C, 4 B	<1000	<1000
Virtual Networks	< 256	< 256	< 256	< 256
IP Pools	< 500	< 500	< 500	< 500
Access Points	< 2000	< 2000	< 2000	< 2000
	B, CP		FE	



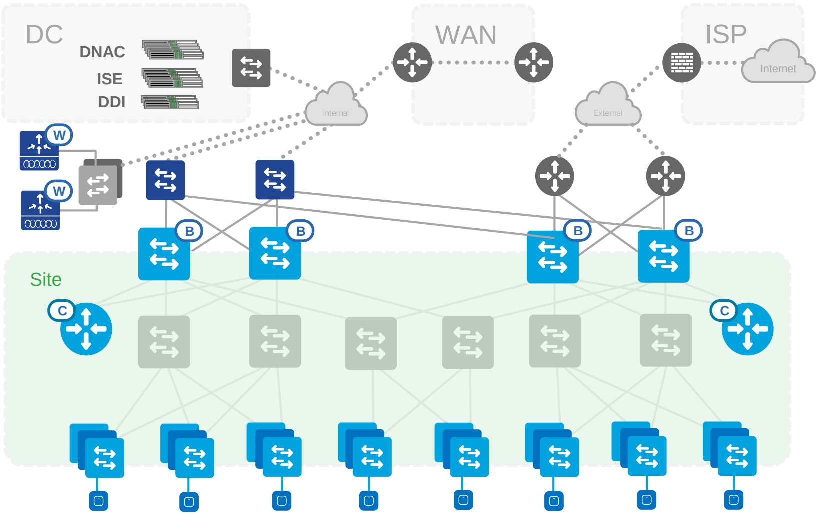
Overview

- Tends to be a multiple Buildings and/or Floors
- **3-4 Tier with Multiple wiring closets** (MDF & IDF)
- **Total endpoints < 10K** (recommended)
- Dedicated CP's for higher redundancy
  - Max CP nodes = 4
- Dedicated Borders for multiple site exits
  - Max Border nodes = 4

Benefits

- Dedicated Borders provide multiple exits to different DC's, WAN or Internet
- Full Survivability for CP and Borders (requires iBGP)
- Increased Scale with Dedicated CP + 2-4 Borders
- WLCs can be local or in a remote Data Center (20ms)
- < 25,000 dynamic authentications
- < 2000 group-based policies

Sample Topology



Designing a Single Site

A Connect

0 Services

Designing a Single-Site Connectivity Services

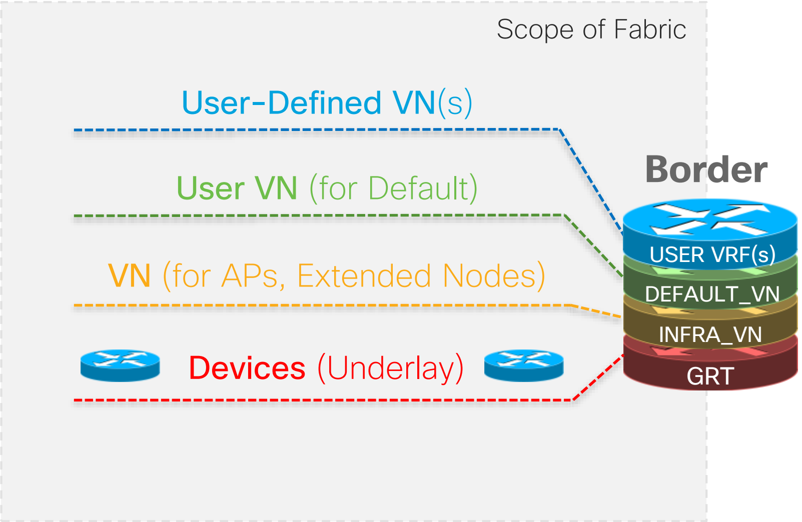
Shared Services with Fusion

How VNs work in SD-Access

A Connect

0 **Services**

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



Shared Services with Fusion

How VNs work in SD-Access

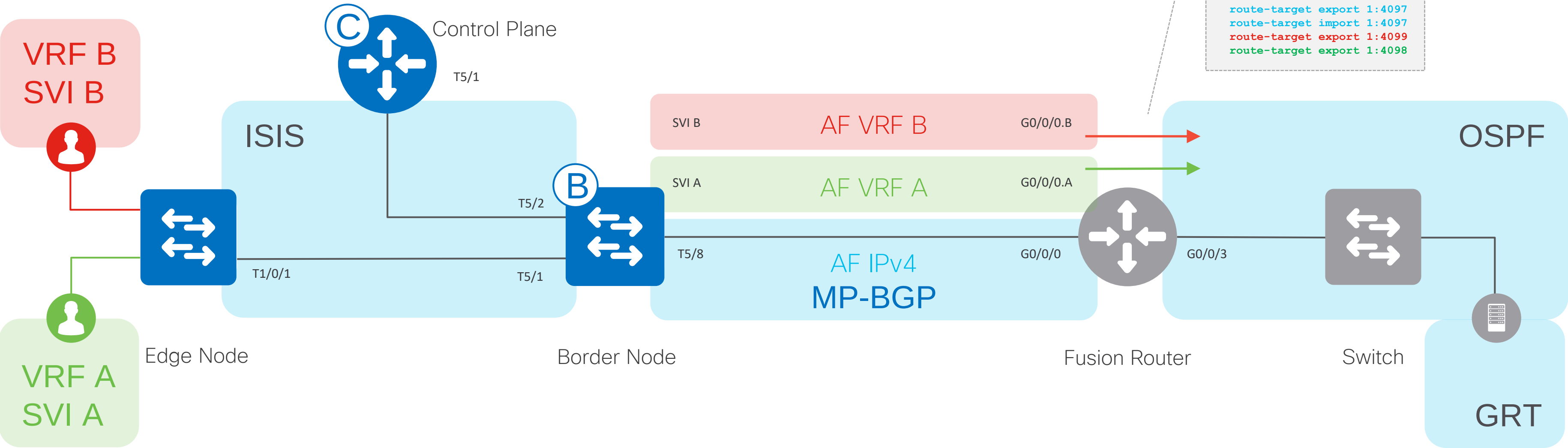
A Connect

0 Services

What is Fusion Router?

- Device to provide communication (via route-leaking) between VNs and Shared Services
- Designs connecting to existing Global Routing Table should use a “Fusion” router with MP-BGP, VRF-Lite & VRF import/export or other conventional route-leaking configurations

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

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



SD-Access to ACI Connectivity

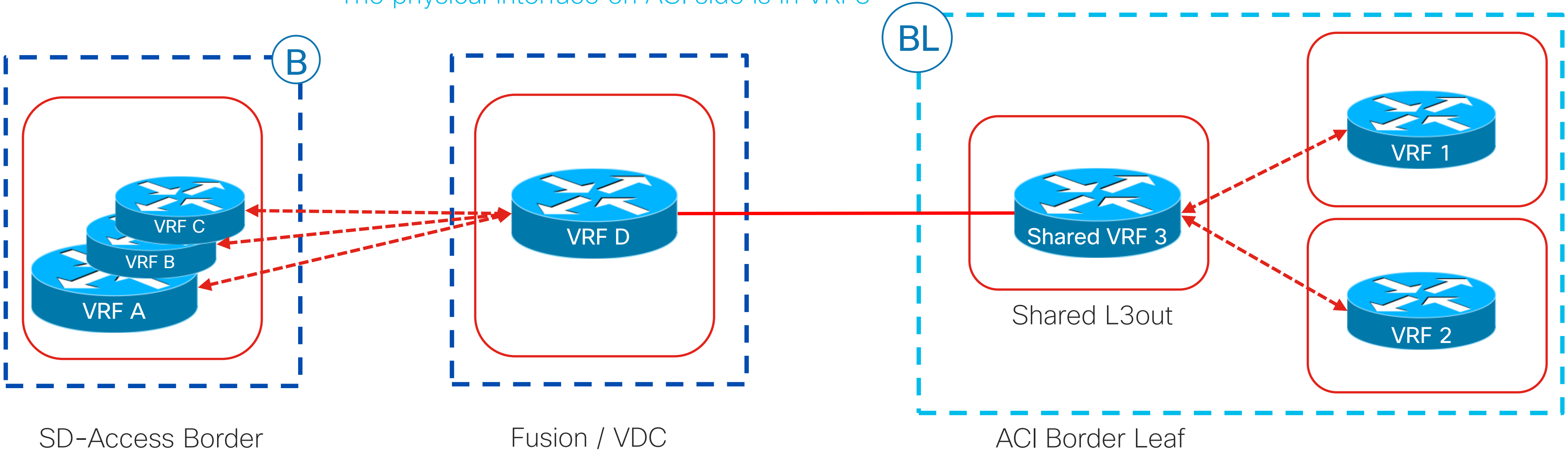
Campus to DC connection via Fusion Router

A Connect

0 **Services**

“VRF D” in SDA is connected to “VRF 3” on ACI

- The physical interface on SDA side is in VRF D
- The physical interface on ACI side is in VRF3



In the current releases, ISE does not support VRF/VN semantics
It is assumed that connectivity between Campus VRFs and DC VRFs is provisioned

A Connect

1 Wired

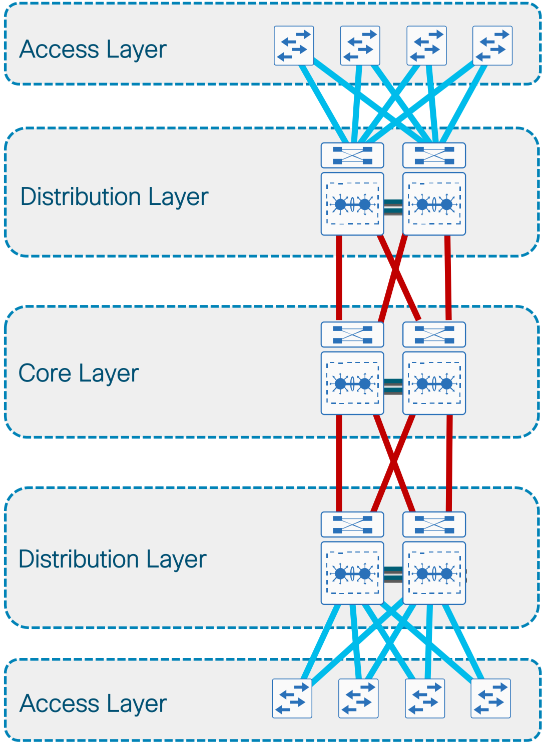
Designing a Single-Site Wired Connectivity

Cisco Validated Design

Hierarchical Network

A Connect

1 Wired



Building Block

- Each layer has specific role
- Modular building blocks (hierarchical)
- Easy to understand, grow and troubleshoot
- Creates small fault domains (clear demarcation)
- Promotes load balancing and resiliency

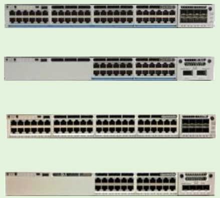
SD-Access Platform Selection

Wired Connectivity – Lead with C9K and ISR4K

Switching

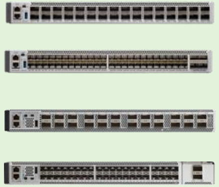
Common HW & SW – UADP & IOS-XE
CP, Border & Edge (All Platforms)

C9200 Series



C9300 Series

C9400 Series

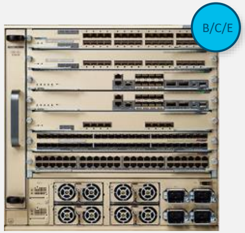


C9500 Series

C9600 Series

C3K Series

C4500 + Sup8E

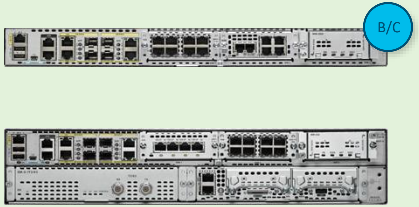


C6800 + Sup6T

N7700 + Sup2E

Routing

Common HW & SW – QFP & IOS-XE
CP, Border & SD-WAN cEdge*



ISR 4300 & 4400

ASR1000 X & HX Series

cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-739242.html

Cisco Validated Design

Routed Access for SD-Access Underlay

A Connect

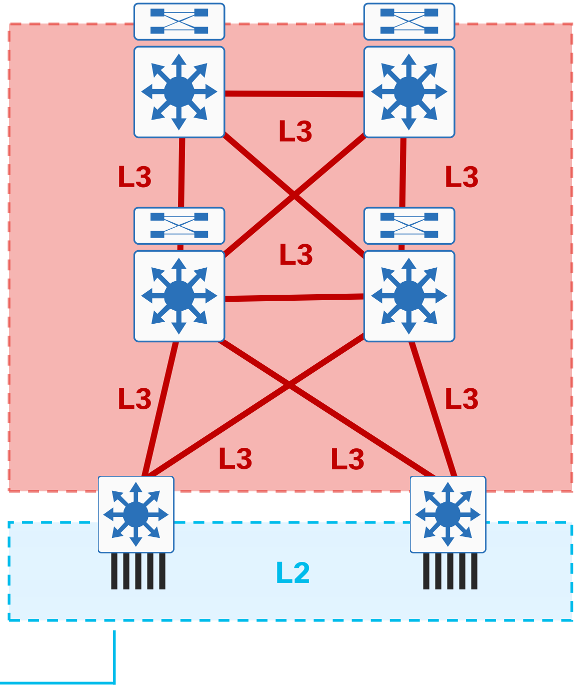
1 **Wired**

Simplified Forwarding & Management

- No VLAN trunking configuration required
- No STP config/tuning/features (root bridge, loopguard…)
- No default gateway config/tuning (HSRP, VRRP, GLBP)
- No matching of STP and HSRP priority
- No L2/L3 multicast topology inconsistencies
- No asymmetric flooding

L2 Port “access” features still apply:

- Spanning Tree, Portfast, BPDU Guard
- Port Security, IPSG
- DHCP Snooping, DAI
- Storm Control, etc.



Underlay Considerations

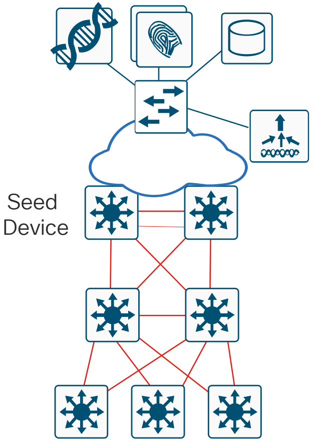
Manual and Automated

A Connect

1 **Wired**

Manual Underlay

- Routed Access Network
- System MTU 9100
- Loopback 0 with /32 subnet
- Resiliency – BFD, ECMP, NSF
- Multicast – ASM, SSM
- CLI, SNMP credentials
- Discover & Manage devices
- Upgrade Software version



Automated Underlay

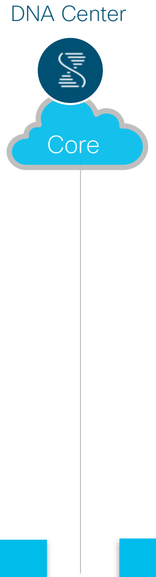
- Discover Seed Device
- Input IP Address Pool
- Start LAN Automation
  - ✓ Discover the network device
  - ✓ Onboard the network device
  - ✓ Upgrade software
- Stop LAN Automation
  - ✓ Complete Configs (L3 interface, IS-IS)
  - ✓ Manage Device in Cisco DNA-Center

DNA Center LAN Automation

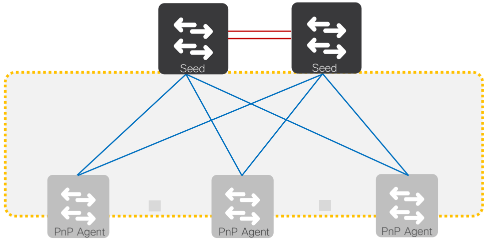
Catalyst Switch Role Support

A Connect

1 **Wired**

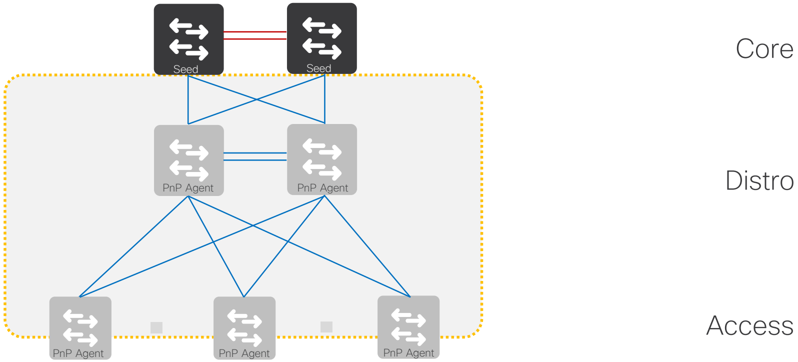


2 Tier – Collapsed Core Design



Layer	Role	Supported Switch
Distribution	Seed	Catalyst 9600 | 9500 | 9400 | 3850 | 6800
Access	PnP Agent	Catalyst 9400 | 9300 | 4500E | 3850 | 3650

3 Tier – Multi-Layer Campus Design



Layer	Role	Supported Switch
Core	Seed	Catalyst 9600 | 9500 | 9400 | 3850 | 6800
Distribution	PnP Agent	Catalyst 9000 | 4500E | 3850 | 3650
Access	PnP Agent	Catalyst 9400 | 9300 | 4500E | 3850 | 3650

cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/b_dnac_sda_lan_automation_deployment.html

SD-Access Overlay

Considerations

A Connect

1 Wired

Overlay IP Pool Considerations

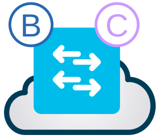
- Reserve separate IP pools for “Border Handoff”
  - Should NOT overlap with LAN Automation pools
- Reserve separate IP pools for “Multicast Signaling”
- Reserve separate IP pools for “Fabric APs” and assign to INFRA-VN only
- Reserve separate IP pools for “Extended Nodes” and assign to INFRA-VN only

Host Onboarding Considerations

- Use default option for IP Pools – e.g. L2 extension is turned ”on”
- When using L2 Flooding, it requires underlay to enable multicast

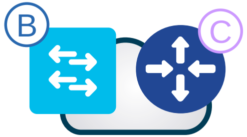
SD-Access - Border Design

Collocated vs. Distributed Borders



Collocated Design

- Border and Control Plane are on the same device
- Simple Design (less config)
- Best when only a few (1 or 2) Collocated Border + CP nodes
- Best for Small Sites (less than 10K endpoints)



Distributed Design

- Border and Control Plane are on different devices
- Additional configurations required
- Multiple Border nodes can connect to the same (single or set of) multiple Control Plane nodes
- Best for Medium or Large Sites (more than10K endpoints)

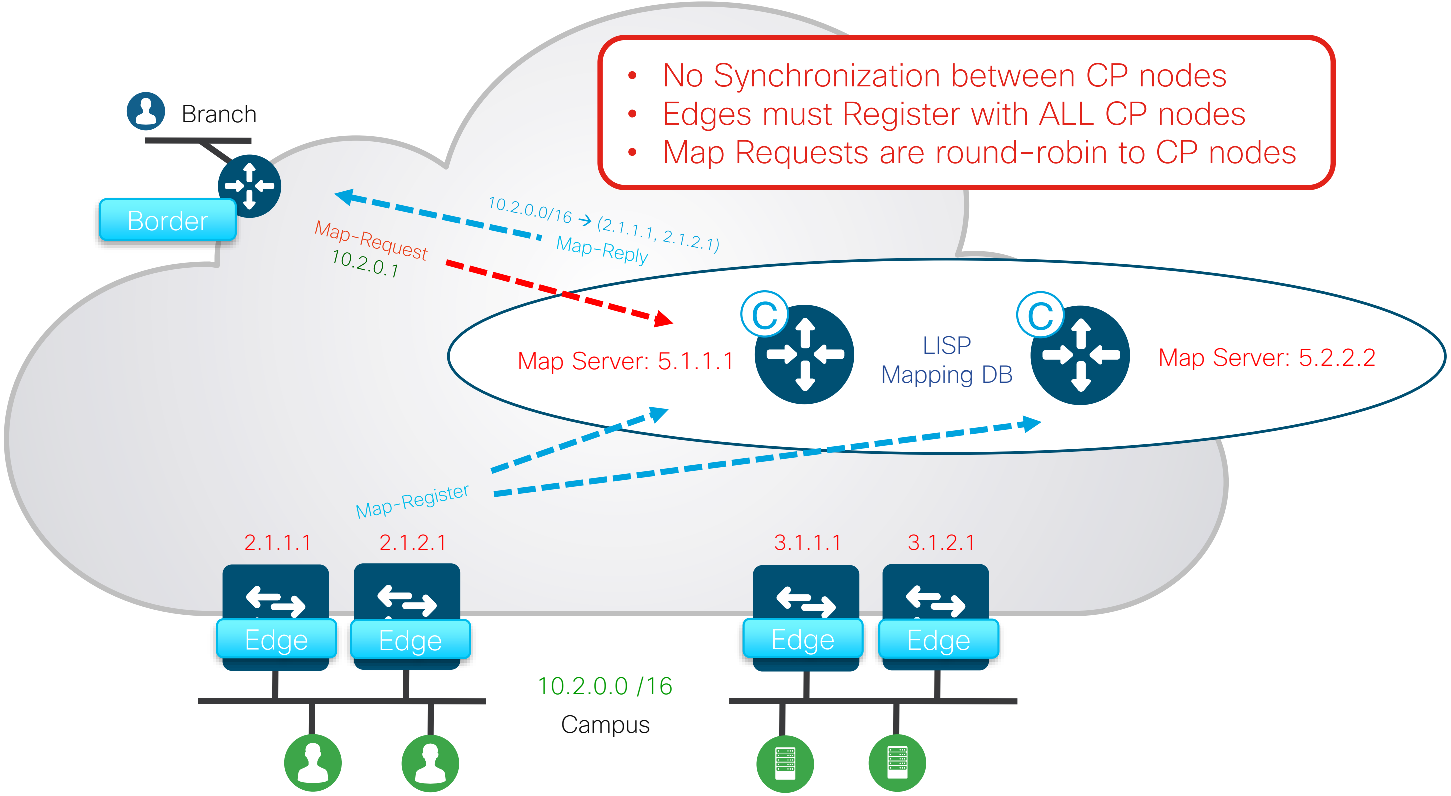
SD-Access CP Redundancy

Design CP node redundancy for equivalency

A Connect

1 Wired

- No Synchronization between CP nodes
- Edges must Register with ALL CP nodes
- Map Requests are round-robin to CP nodes



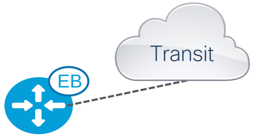
SD-Access Border

Choosing the Right type of Border

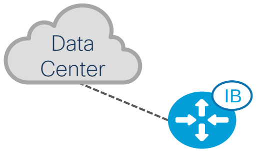
A Connect

1 Wired

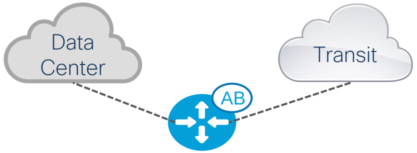
- When to use **External (Outside)** border?
  - ➢ When we want to connect ONLY to the SDA Transit or an IP Transit (e.g. Internet).



- When to use **Internal (Rest of Company)** border?
  - ➢ When we want to connect **ONLY** a site to the known areas of the company like DC, WAN etc.



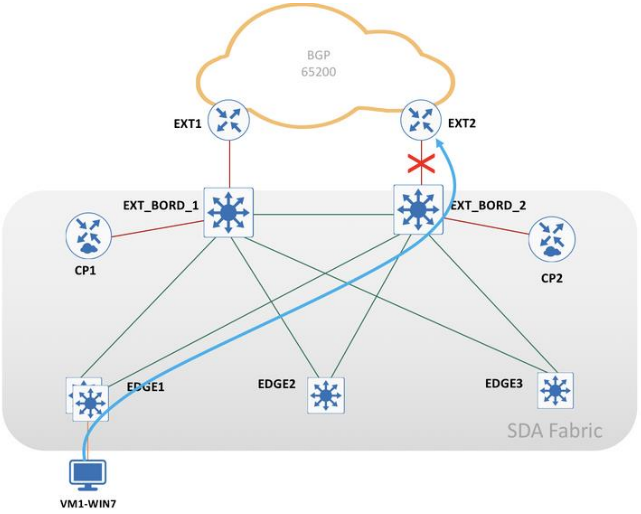
- When to use **Internal + External (Anywhere)** border?
  - ➢ When we want to connect to SDA Transit or IP Transit, and **ALSO** to known areas like DC, WAN, etc.



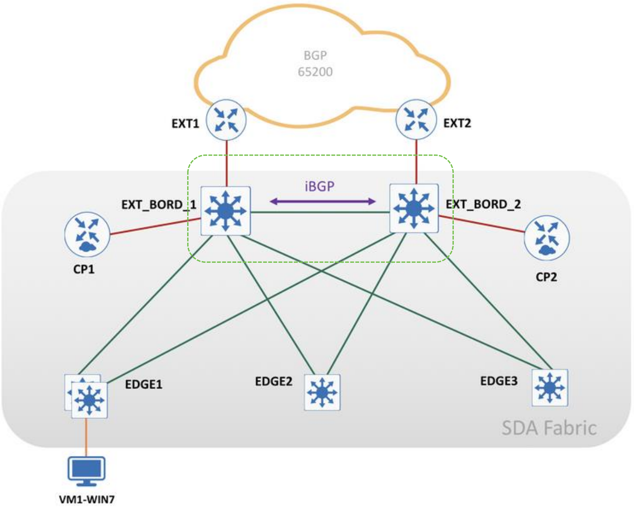
Overlay Considerations

Borders requires iBGP between nodes

- Internet routing (0.0.0.0/0) failures on Borders (e.g. link to Fusion) are not notified to the others.
- If the Border remains online… this may result in a black-hole!
- Configuring an iBGP session (using VRF-Lite for overlay VNs) between Borders will resolve this.



Before: External Failure leads to Black Hole

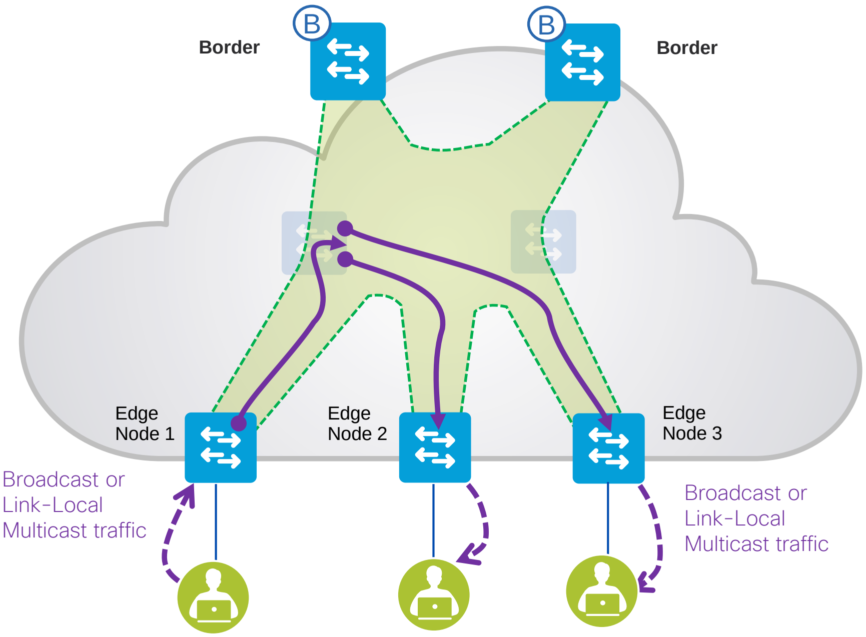


After: iBGP notifies other Borders of External Failure

Layer 2 Flooding in SD-Access

A Connect

1 **Wired**


B
Border
B
Border
Edge Node 1
Edge Node 2
Edge Node 3
Broadcast or Link-Local Multicast traffic
Broadcast or Link-Local Multicast traffic

- ✓ Silent Host Support
- ✓ Allows Layer 2 flooding within an IP Subnet/vlan
- ✓ Broadcast, Link Local Multicast and ARP flooding support
- ✓ PIM-SM* used in the Underlay for multicast transport of Layer 2 frames.

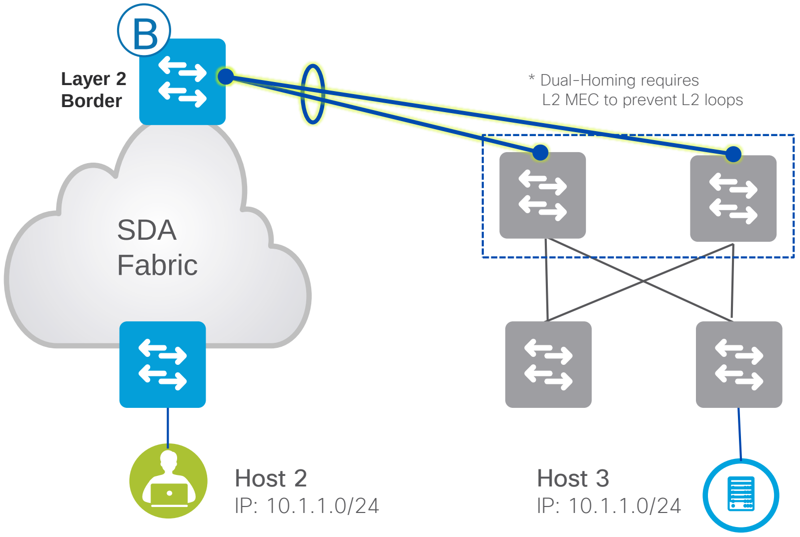
* LAN Automation enables PIM by default.
If using manual underlay – PIM must be enabled.

cisco Live!

Border Layer 2 Handoff

A Connect

1 Wired



Fabric hosts in Address Pool (1024)

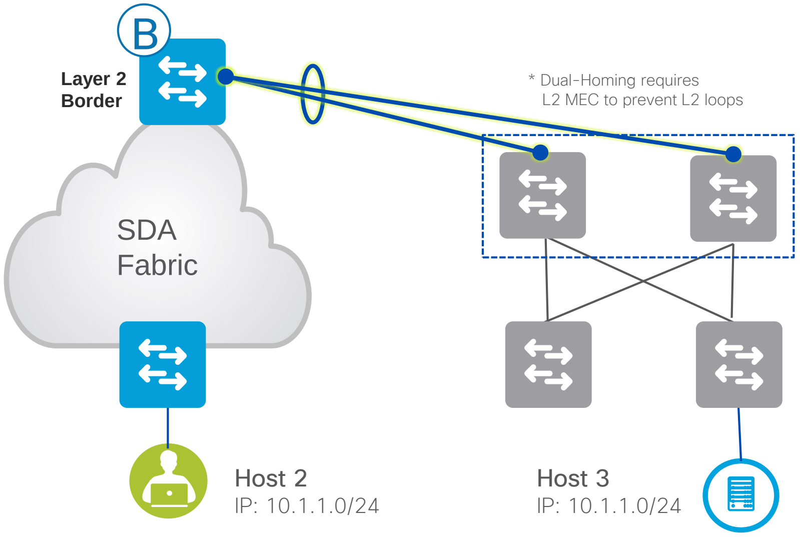
Traditional hosts in VLAN (300)

- ✓ Migration use case: same IP subnet resides inside and outside of fabric
- ✓ End points from outside (non-fabric) are registered to the CP node by Layer 2 Border
- ✓ SVI for external VLAN resides on Layer 2 Border (not outside)

Border Layer 2 Handoff

A Connect

1 Wired



Fabric hosts in Address Pool (1024)

Traditional hosts in VLAN (300)

✓ Layer 2 Border supports only 4K host registrations across ALL the external VLANs

✓ Layer 2 Border does not support any multi-homing.

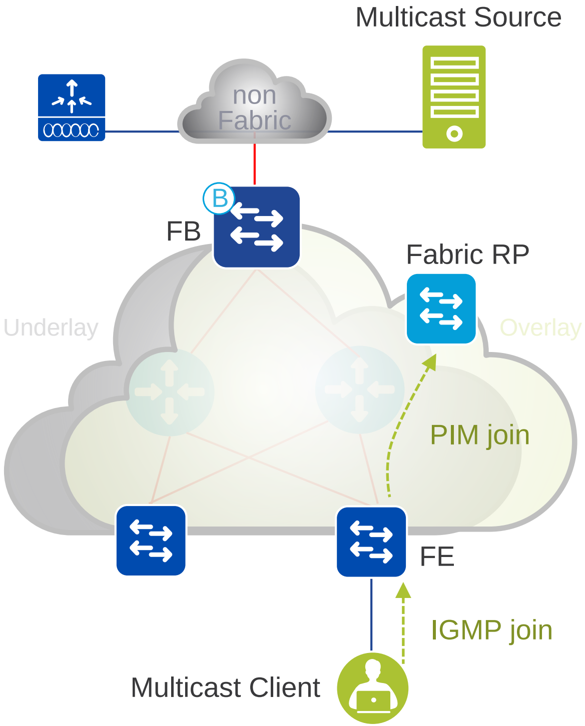
- External switch cannot handoff same VLAN/s to more than one Layer 2 Border.

Multicast Overlay

Receiver Join to Fabric RP

A Connect

1 Wired



- Multicast Client (receiver) is in the Fabric Overlay
- Multicast Source can be in the Fabric Overlay (via FE) and/or outside the Fabric (via FB)
- PIM-SM (or SSM) is enable to run in the Overlay
- A Fabric RP (PIM-SM) needs to be present in the Overlay, as part of the Endpoint IP space

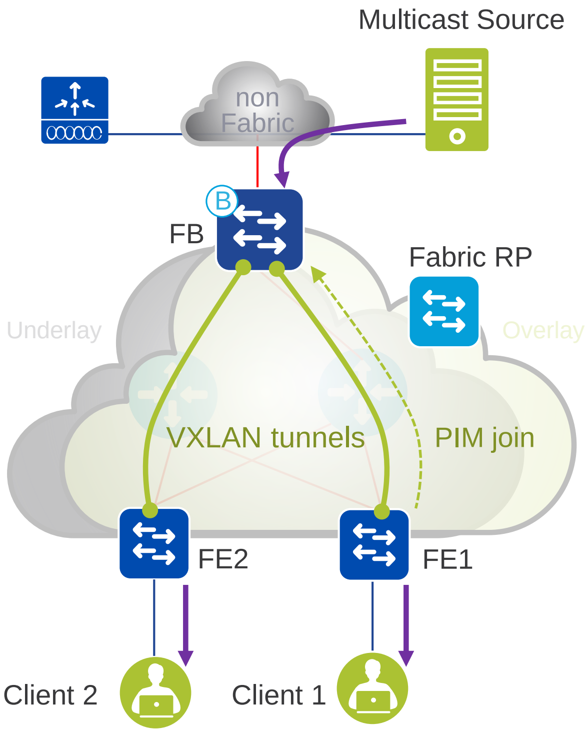
1. The Client sends IGMP join for a specific multicast Group (G)
2. The Fabric Edge (FE) node receives the IGMP join
3. The IGMP join triggers a new PIM join towards the Fabric Rendezvous Point (RP)

Multicast Overlay

SPT Switchovers and Replications

A Connect

1 **Wired**

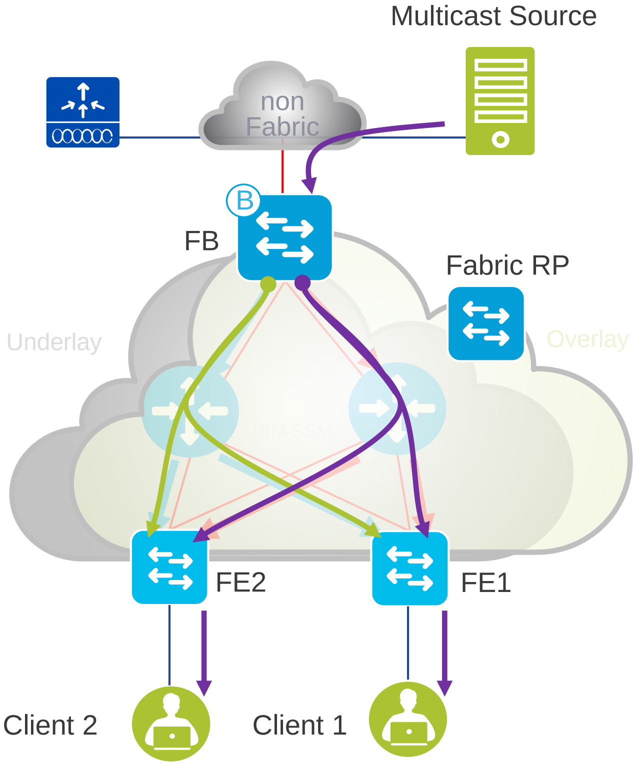


1. Once the first multicast packet arrives on the receiver node, the shortest path tree (SPT) switchover occurs, which triggers a new PIM join directly to the source node.
2. The source node now knows which receiver nodes have clients attached, based on received PIM joins for the specific multicast Group.
3. The source node creates a copy of the original packet for each remote node, VXLAN encapsulates the traffic and then unicasts it to each of the remote nodes (known as head-end replication).
4. Each receiver node receives the VXLAN packets, decapsulates, applies policy, and then sends the original multicast packet to the port connected to the Client

Native Multicast in SD-Access

A Connect

1 Wired

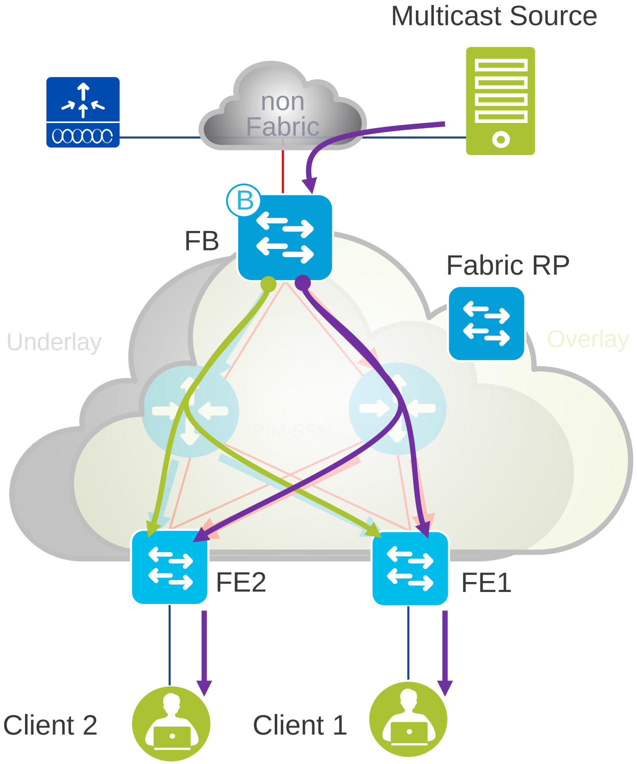


- ✓ Significantly reduces replication load at the Head-End
- ✓ Significantly improves overall scale and reduces latency
- ✓ Best option for 3-4 Tier networks

Native Multicast in SD-Access

A Connect

1 Wired



- ✓ Existing multicast behavior in overlay (PIM ASM and SSM supported)
- ✓ Each multicast group in Overlay is mapped to a group in Underlay
- ✓ PIM SSM is used in the Underlay for multicast transport
- ✓ Per Site multicast configuration: either head-end or native

SD-Access – C9K & C6K Comparison

*N7K supports only External border

Capabilities	Catalyst 9K	Catalyst 6K	Nexus 7K*
Border node	✓	✓	✓
Control Plane node	✓	✓	✗
Fabric in a Box	✓	✗	✗
SDA Embedded WLC	✓	✗	✗
SDA Multi-Site	✓	✗	✗
L2 Border & L2 Flooding	✓	✓	✗
Native Multicast	✓	✓	✗
IPv6 Endpoints	✓	✗	✗
LAN Automation (Seed)	✓	✓	✗

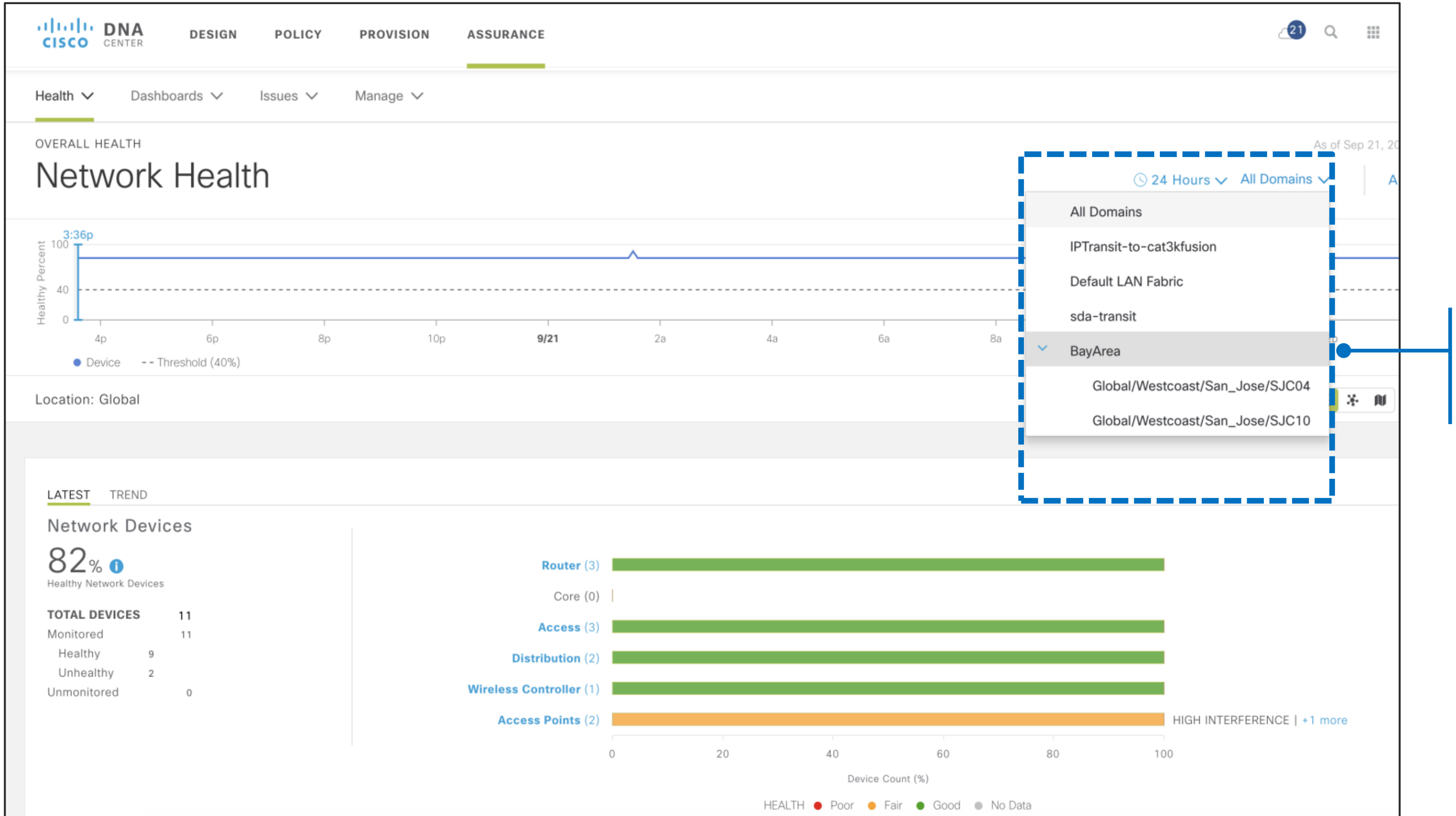
Built for SD-Access

SD-Access Assurance

Monitoring Network Health for Individual Fabric Sites

A Connect

1 Wired

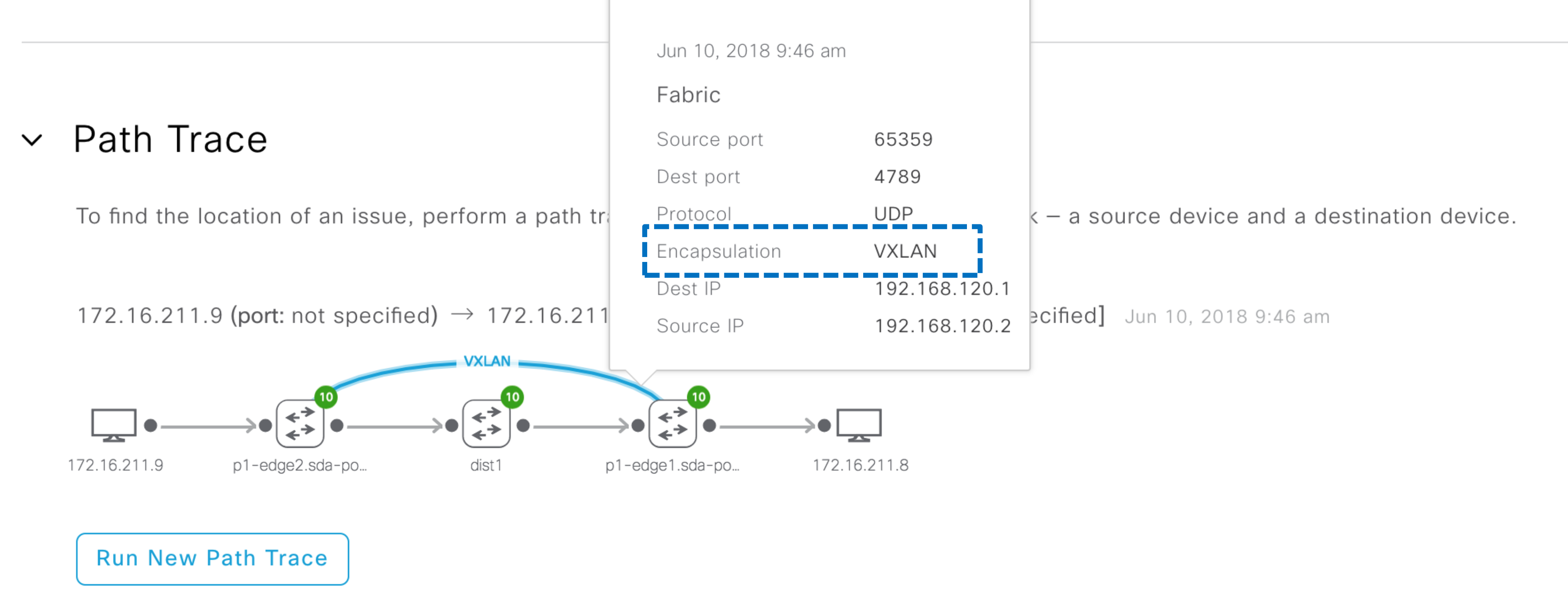


TOTAL DEVICES	11
Monitored	11
Healthy	9
Unhealthy	2
Unmonitored	0

Aggregated view across all SDA Fabric Domains & Sites

SD-Access Assurance

Path Trace for Fabric Wired to Wired Client



Path Trace

To find the location of an issue, perform a path tr k – a source device and a destination device.

172.16.211.9 (port: not specified) → 172.16.211 ecified] Jun 10, 2018 9:46 am

Jun 10, 2018 9:46 am

Fabric

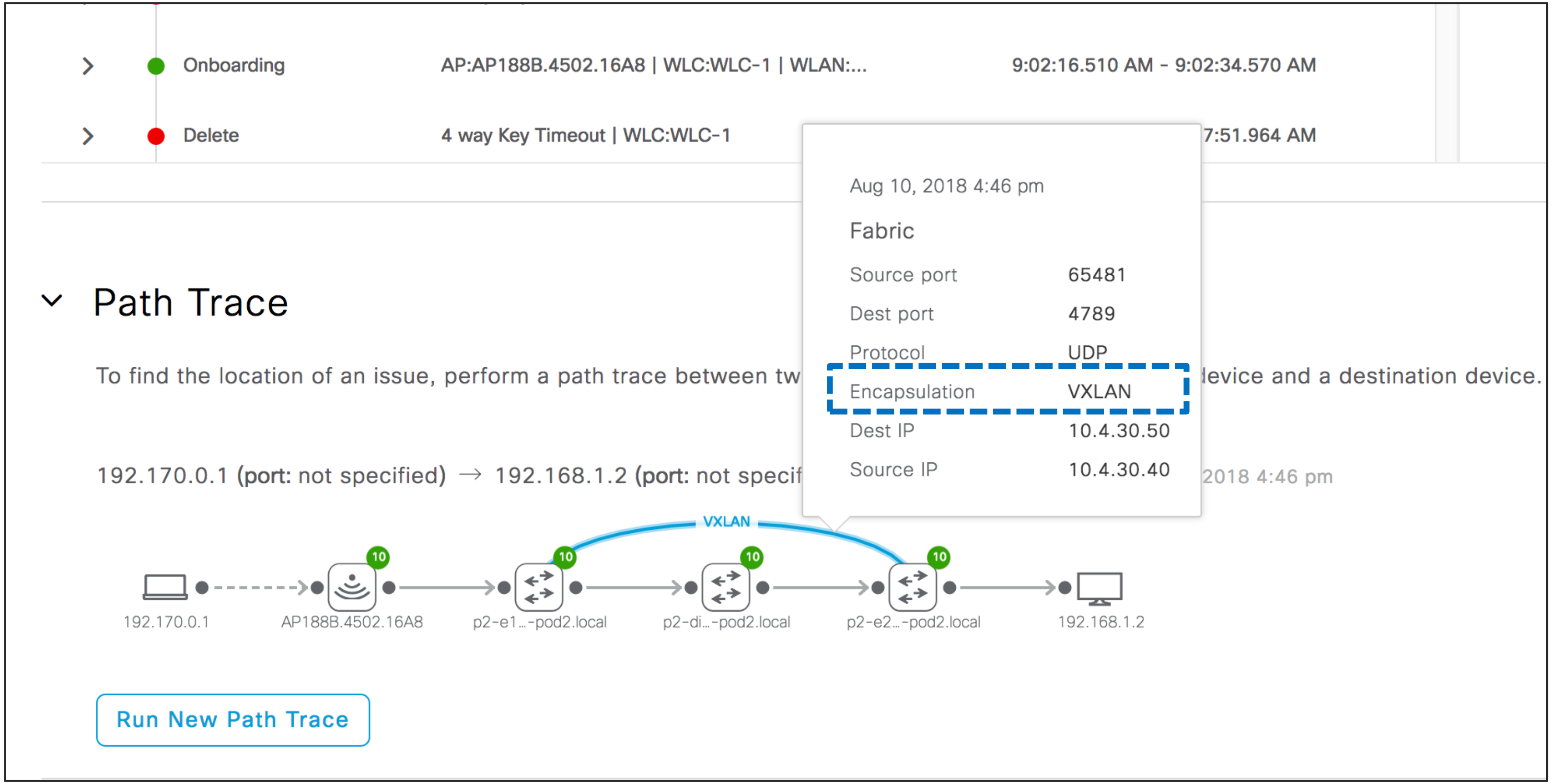
Source port	65359
Dest port	4789
Protocol	UDP
Encapsulation	VXLAN
Dest IP	192.168.120.1
Source IP	192.168.120.2

SD-Access Path Trace

Network Troubleshooting – Path Trace for Wireless Client to Wired Client

A Connect

1 Wired



● Onboarding	AP:AP188B.4502.16A8 | WLC:WLC-1 | WLAN:...	9:02:16.510 AM - 9:02:34.570 AM
● Delete	4 way Key Timeout | WLC:WLC-1	7:51.964 AM

Path Trace

To find the location of an issue, perform a path trace betwe tw device and a destination device.

192.170.0.1 (port: not specified) → 192.168.1.2 (port: not specif 2018 4:46 pm

Aug 10, 2018 4:46 pm

Fabric

Source port	65481
Dest port	4789
Protocol	UDP
Encapsulation	VXLAN
Dest IP	10.4.30.50
Source IP	10.4.30.40

Run New Path Trace

A Connect

2 Wireless

Designing a Single-Site Wireless Connectivity

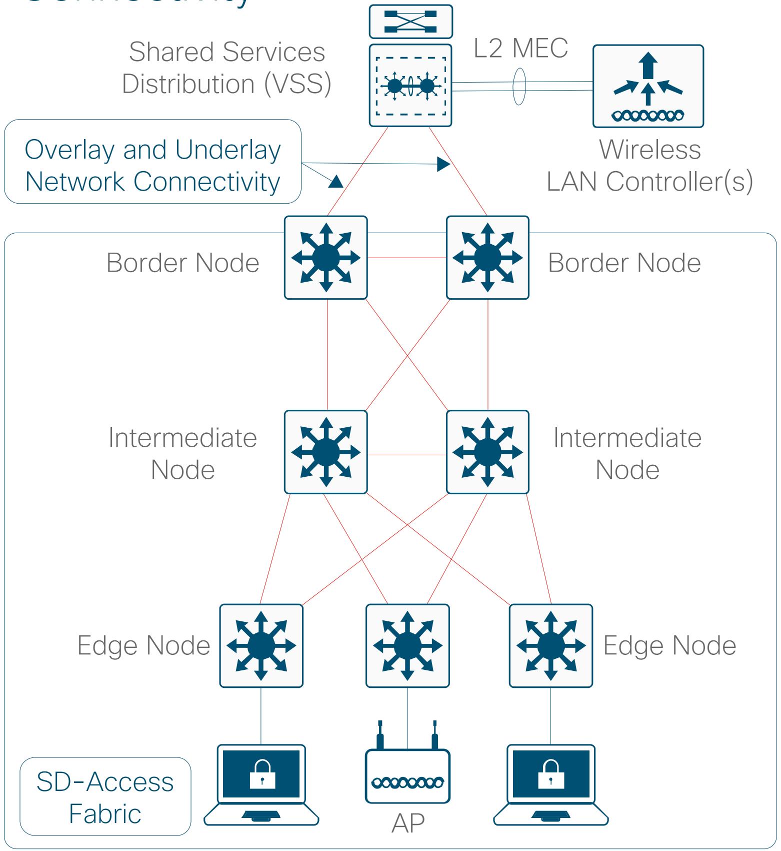
cisco Live!

SD-Access Wireless

Connectivity

A Connect

2 **Wireless**



- ✓ WLC typically connect to a "shared services" Distribution Block or Border
  - Management IP address in Global Routing Table
- ✓ AireOS WLC can talk to 2 CP nodes
- ✓ Access Points connect to Fabric Edge
  - APs reside in INFRA_VN (GRT) and form CAPWAP connection to WLC
- ✓ AP to WLC latency under 20 ms

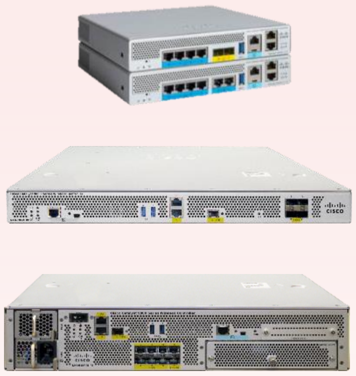
SD-Access Platforms

Fabric Enabled Wireless

For more details: cs.co/sda-compatibility-matrix

Catalyst 9800

NEW



- Catalyst 9800-L
- Catalyst 9800-40
- Catalyst 9800-80
- Catalyst 9800-CL

Catalyst 9100

NEW

- Catalyst 9130
- Catalyst 9120/9115
- 1G/mG RJ45 (Uplink)

AireOS WLC

- AIR-CT3504
- AIR-CT5520
- AIR-CT8540

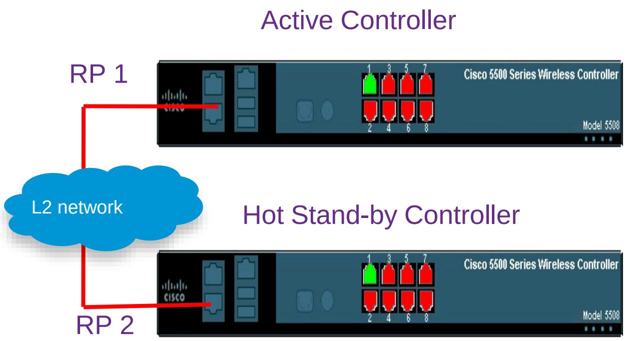
AireOS AP

- 1800/2800/3800/4800
- 1700/2700/3700*
- 1G/mG RJ45 (Uplink)

* No IPv6, AVC, FNF

SD-Access Wireless

WLC Stateful Switchover (SSO)



- ✓ True 1:1 High Availability. One WLC in Active and other in Hot Standby
- ✓ Configuration on Active is synched to Standby WLC
- ✓ Licenses, AP CAPWAP state, Clients in “RUN” state

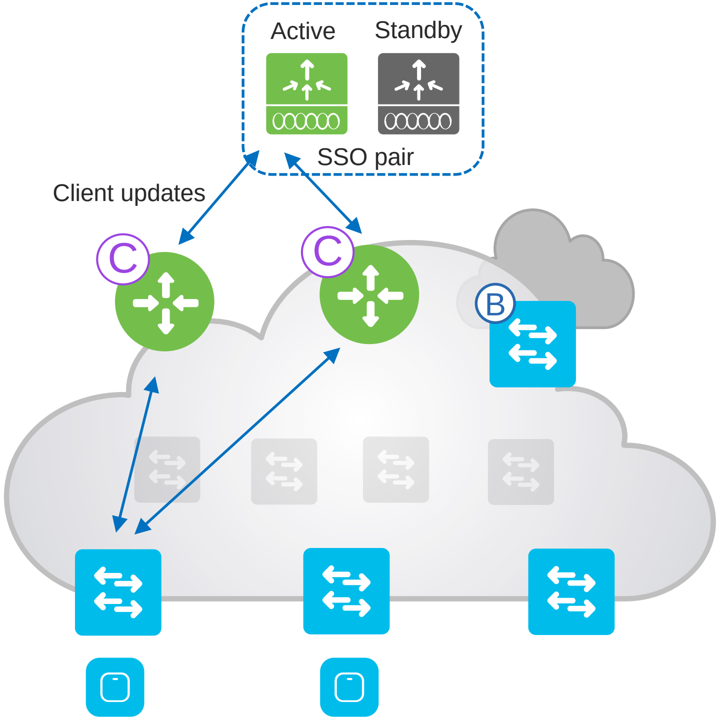
cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html

SD-Access Wireless

Redundancy Considerations

A Connect

2 **Wireless**



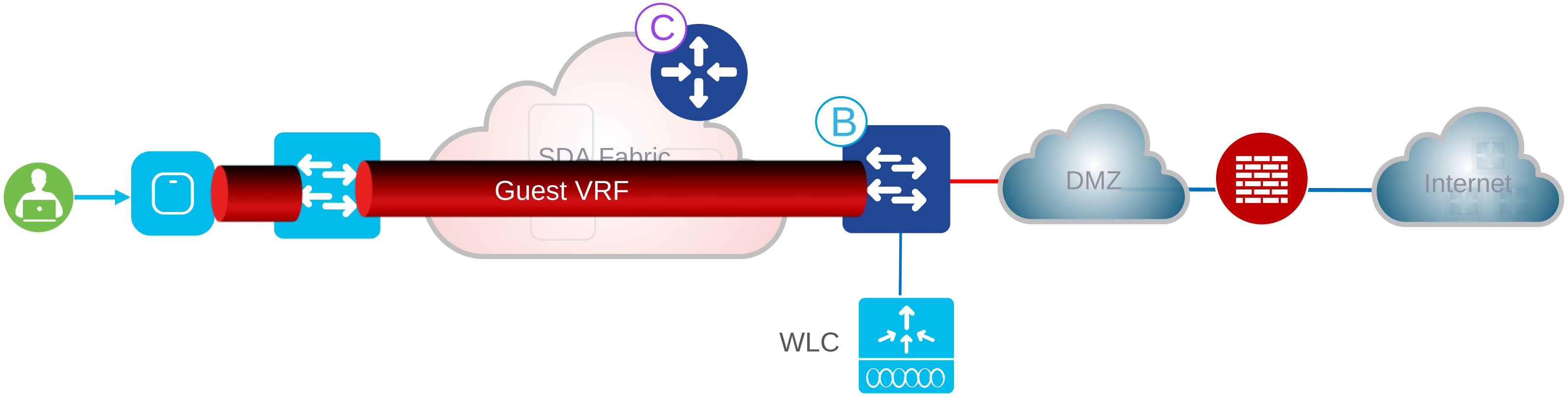
- ✓ WLC registers wireless clients in Host Tracking DB
- ✓ Control Plane redundancy is supported in Active / Active configuration
- ✓ WLC is configured with two CP nodes with information sync across both
- ✓ Stateful redundancy with WLC SSO pair. Active WLC updates Control nodes

SD-Access Guest Wireless

Guest as a dedicated Virtual Network

A Connect

2 **Wireless**



✓ Guest and Enterprise clients share the same Enterprise CP node

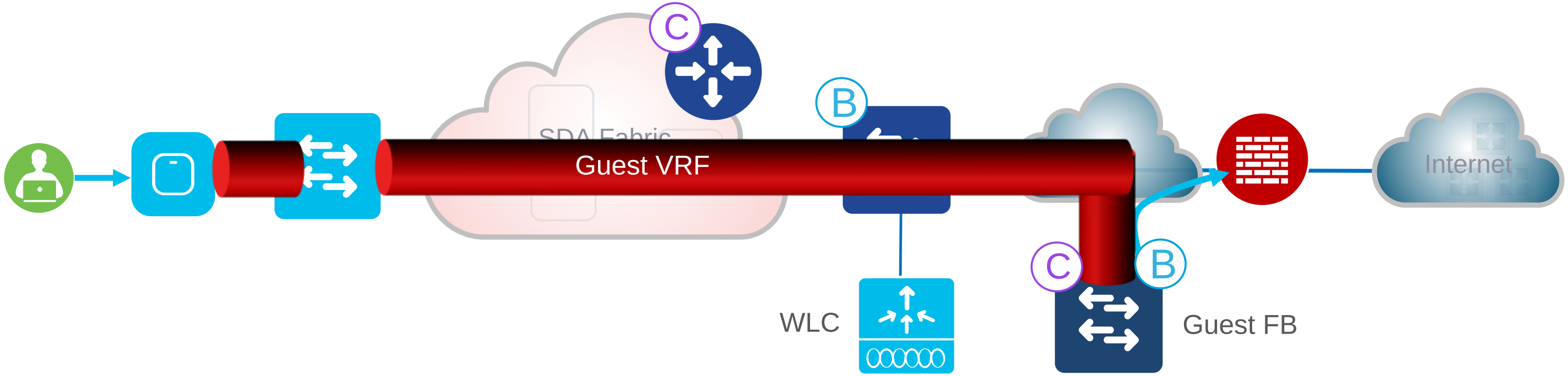
✓ Guest SSID is associated to a dedicated VN in Fabric leveraging Fabric segmentation (VNI, SGT) for guest traffic isolation

SD-Access Guest Wireless

Guest as a dedicated Guest Fabric Border and Control Plane

A Connect

2 **Wireless**



✓ Complete Control plane and Data plane separation from Enterprise traffic

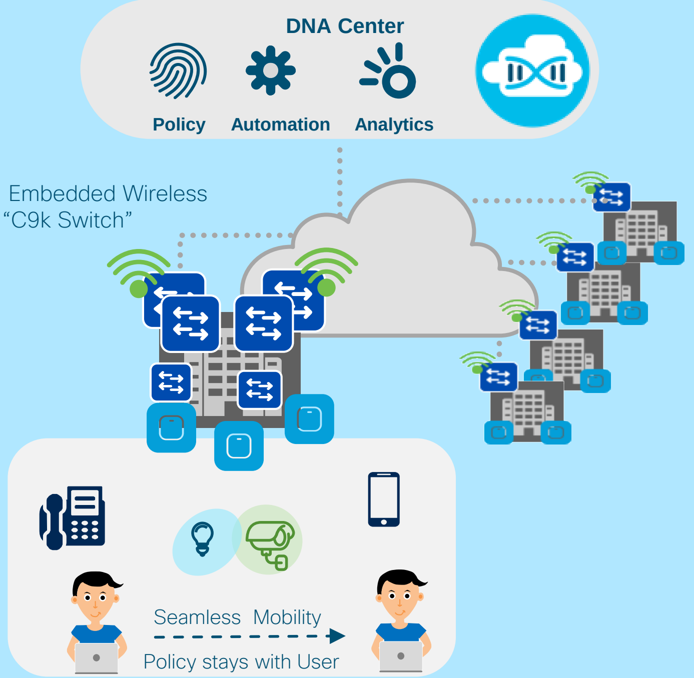
✓ No additional Anchor WLC: Guest traffic is optimized, sent directly to the DMZ

SD-Access Embedded Wireless

A Connect

2 **Wireless**

Support 200 APs and 4000 Clients per Site with HA
Flexible Deployment - Multi-tier Campus and Branch



- Extend rich C9K services like ETA to wireless
- Extend policy-based segmentation to wireless
- Seamless shared services and WAN integration

- Wireless scale for 802.11ax / Wave-2
- Seamless Mobility (No VLAN spans)
- No WAN Link dependency

- Lower TCO
- Robust HA
- Simple / Intuitive Workflows

* Supports 400 AP and 8000 clients w/o HA

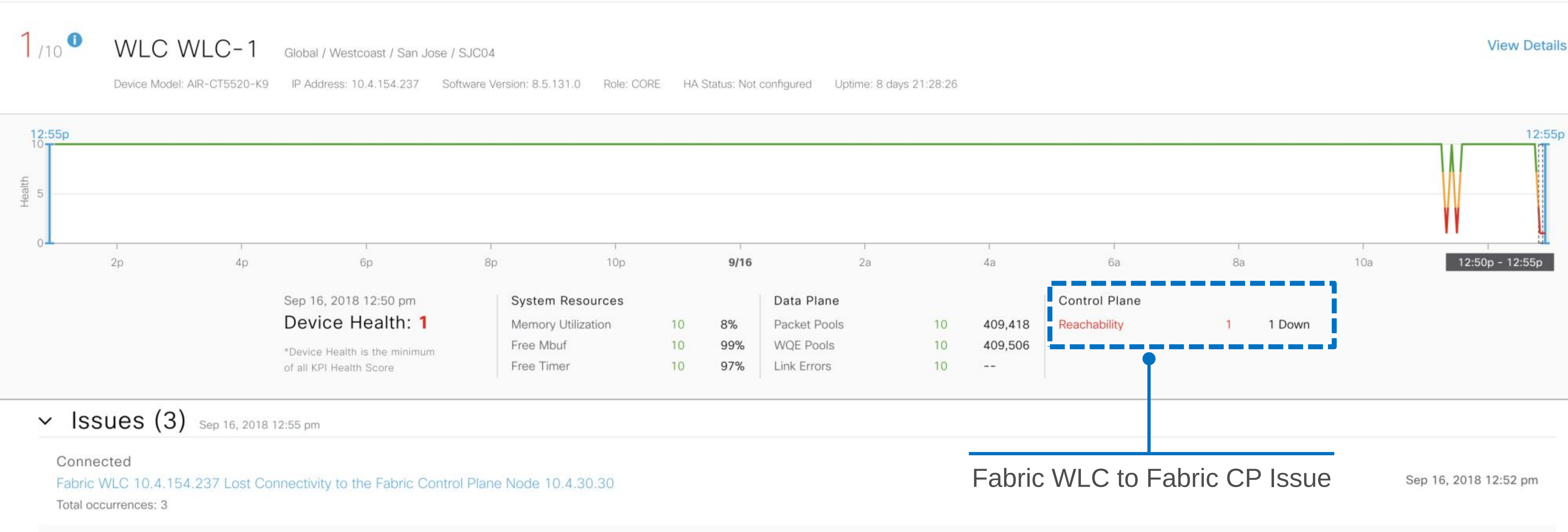
Optimized Solution for Branch and Small Campus

SD-Access Assurance

Monitoring WLC connectivity to Enterprise and Guest Control Plane

A Connect

2 **Wireless**



1 /10 WLC WLC-1 Global / Westcoast / San Jose / SJC04 View Details

Device Model: AIR-CT5520-K9 IP Address: 10.4.154.237 Software Version: 8.5.131.0 Role: CORE HA Status: Not configured Uptime: 8 days 21:28:26

Sep 16, 2018 12:50 pm

Device Health: 1

*Device Health is the minimum of all KPI Health Score

System Resources		
Memory Utilization	10	8%
Free Mbuf	10	99%
Free Timer	10	97%

Data Plane		
Packet Pools	10	409,418
WQE Pools	10	409,506
Link Errors	10	--

Control Plane		
Reachability	1	1 Down

Issues (3) Sep 16, 2018 12:55 pm

Connected

Fabric WLC 10.4.154.237 Lost Connectivity to the Fabric Control Plane Node 10.4.30.30

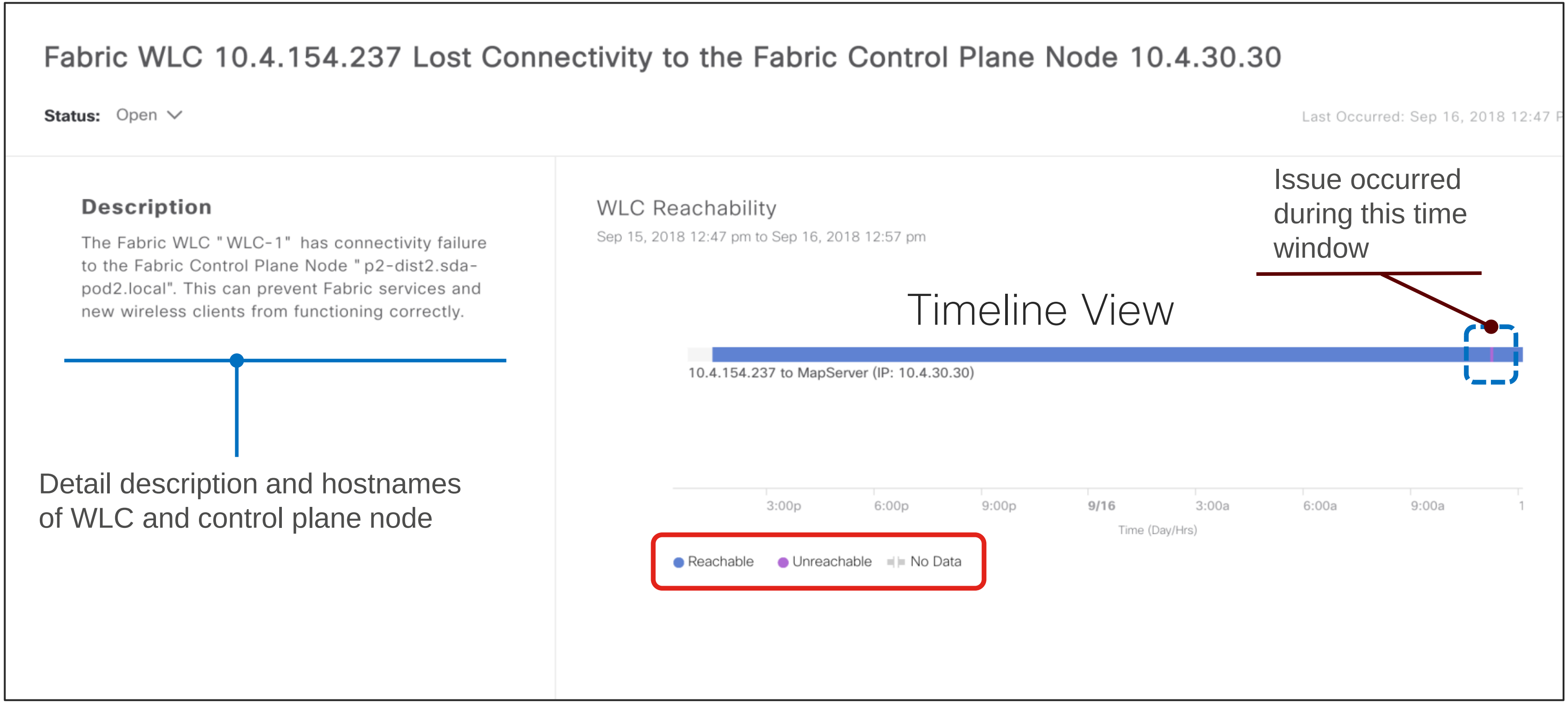
Total occurrences: 3

Sep 16, 2018 12:52 pm

Fabric WLC to Fabric CP Issue

SD-Access Assurance

Monitoring WLC connectivity to Enterprise and Guest Control Plane



Fabric WLC 10.4.154.237 Lost Connectivity to the Fabric Control Plane Node 10.4.30.30

Status: Open

Last Occurred: Sep 16, 2018 12:47 P

Description

The Fabric WLC "WLC-1" has connectivity failure to the Fabric Control Plane Node "p2-dist2.sda-pod2.local". This can prevent Fabric services and new wireless clients from functioning correctly.

WLC Reachability

Sep 15, 2018 12:47 pm to Sep 16, 2018 12:57 pm

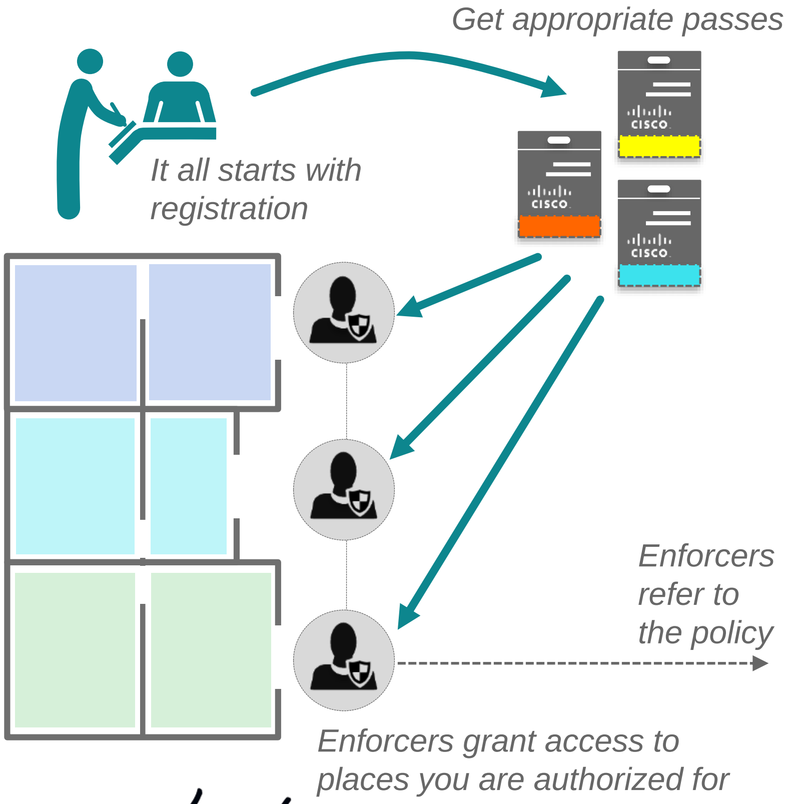
Timeline View

Issue occurred during this time window

Detail description and hostnames of WLC and control plane node

Designing a Single-Site Policy Services

Segmentation at CiscoLive

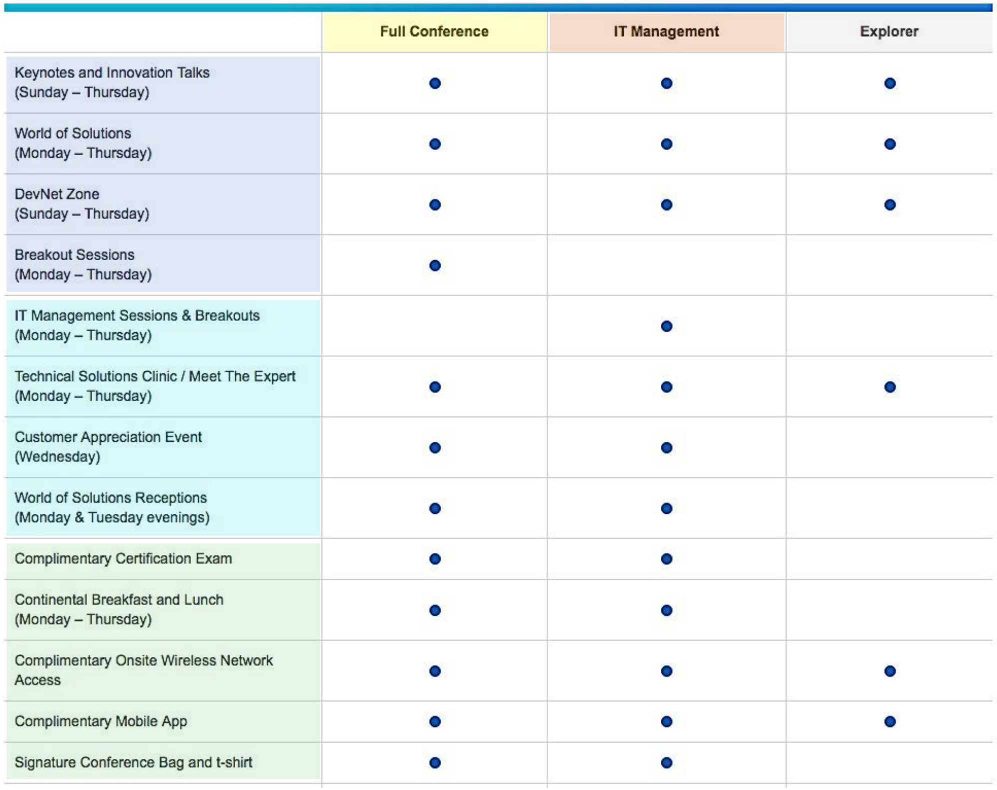


Get appropriate passes

It all starts with registration

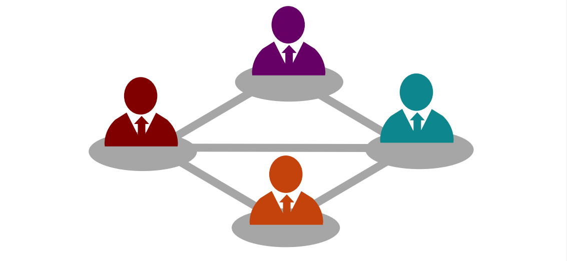
Enforcers refer to the policy

Enforcers grant access to places you are authorized for

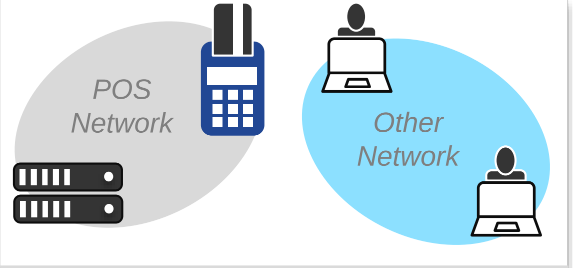


	Full Conference	IT Management	Explorer
Keynotes and Innovation Talks (Sunday – Thursday)	●	●	●
World of Solutions (Monday – Thursday)	●	●	●
DevNet Zone (Sunday – Thursday)	●	●	●
Breakout Sessions (Monday – Thursday)	●		
IT Management Sessions & Breakouts (Monday – Thursday)		●	
Technical Solutions Clinic / Meet The Expert (Monday – Thursday)	●	●	●
Customer Appreciation Event (Wednesday)	●	●	
World of Solutions Receptions (Monday & Tuesday evenings)	●	●	
Complimentary Certification Exam	●	●	
Continental Breakfast and Lunch (Monday – Thursday)	●	●	
Complimentary Onsite Wireless Network Access	●	●	●
Complimentary Mobile App	●	●	●
Signature Conference Bag and t-shirt	●	●	

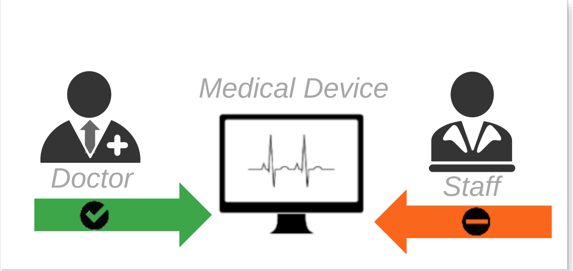
Factors governing Segmentation



Line of business – BU segmentation

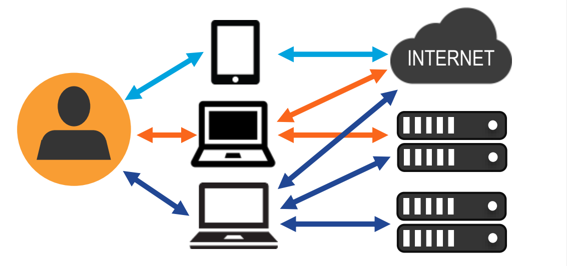


Payment Card Industry

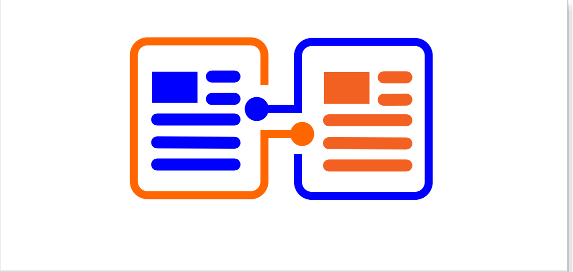


Hospital Network

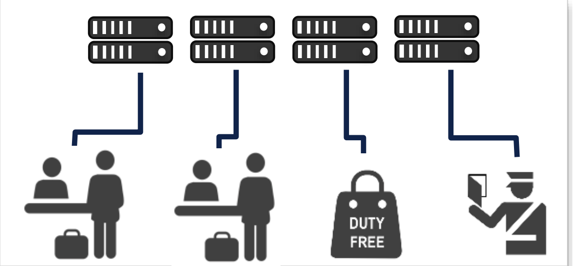
As networks evolve, granular segmentation is desired



Bring-Your-Own-Device



Mergers and Acquisitions



Multi-Tenancy

Cisco TrustSec functions

B Policy

0 **Services**

5	Employee
6	Voice
7	Partner

Classification

- Assigning SGTs
- Static Assignments
- Dynamic Assignments

Propagation

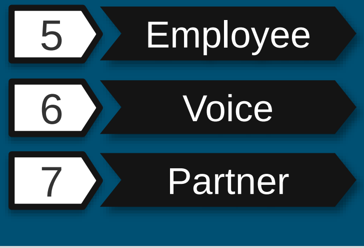
- Inline SGT
- SXP and pxGrid

Enforcement

- Security Group ACL
- Internal Enforcement
- External Enforcement

Designing a Single-Site Identity Policy

Cisco TrustSec functions

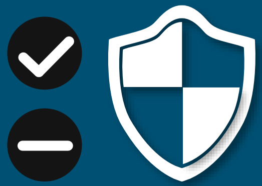


Classification

- Assigning SGTs
- Static Assignments
- Dynamic Assignments

Propagation

- Inline SGT
- SXP and pxGrid



Enforcement

- Security Group ACL
- Internal Enforcement
- External Enforcement

Identity Policy – Access

Authentication & Authorization

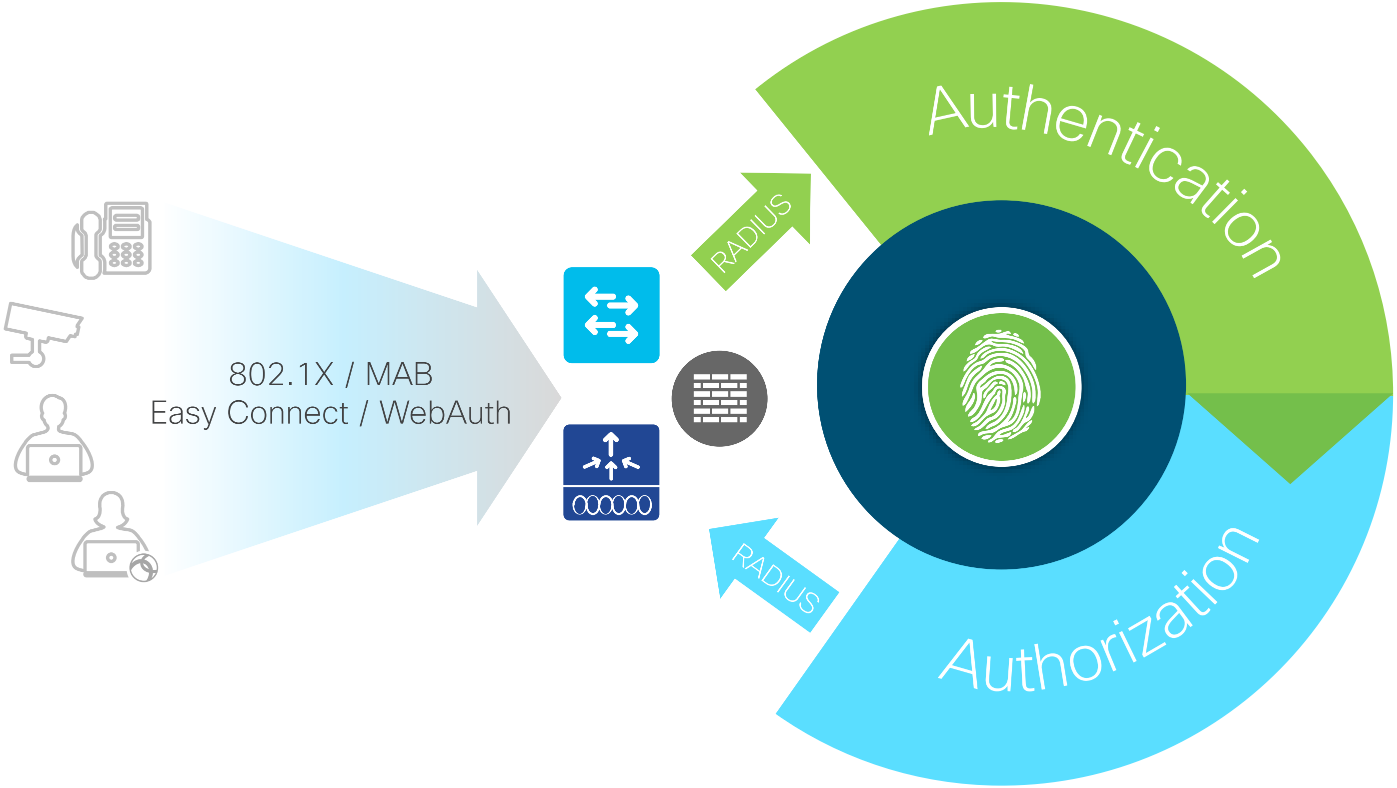
B Policy

1 **Identity**

Access Policy
↓
Authentication +
Authorization

Who goes in which Group?

Based on what criteria?

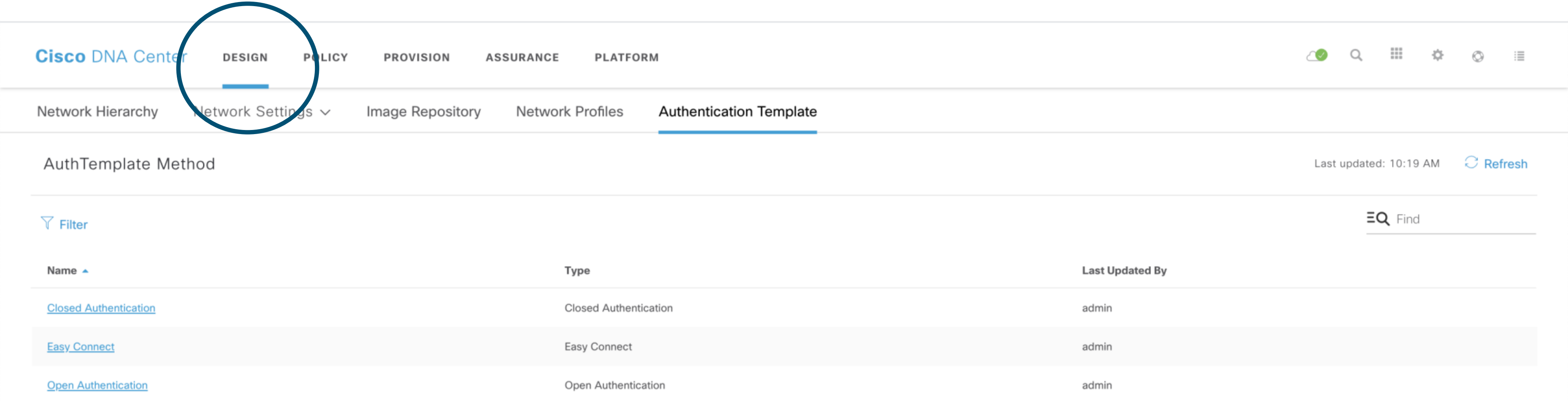


Authentication Templates

Global Authentication Templates

B Policy

1 **Identity**

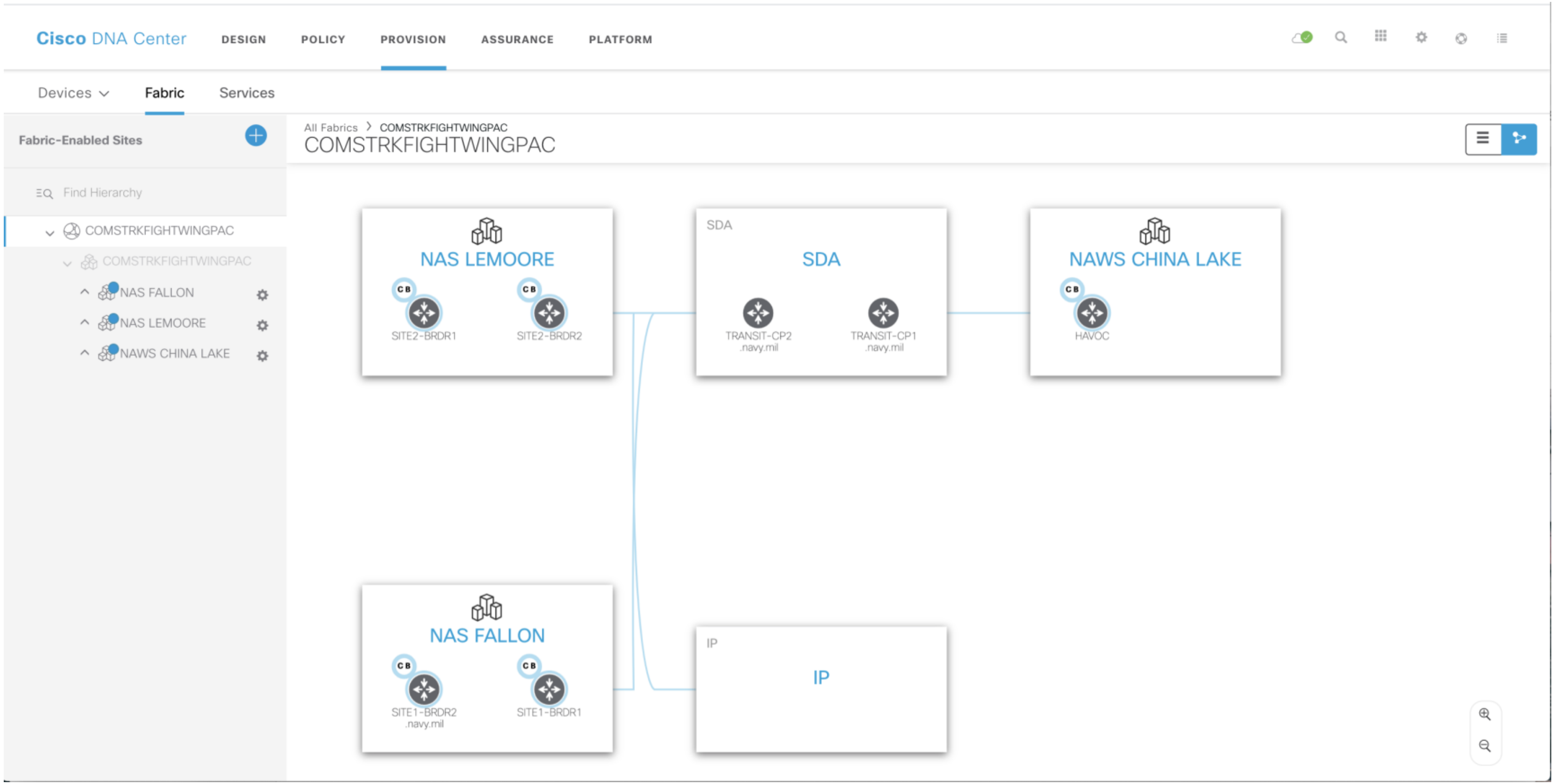


AuthTemplate Method

Last updated: 10:19 AM

Name	Type	Last Updated By
Closed Authentication	Closed Authentication	admin
Easy Connect	Easy Connect	admin
Open Authentication	Open Authentication	admin

Fabric Sites at Multiple Locations

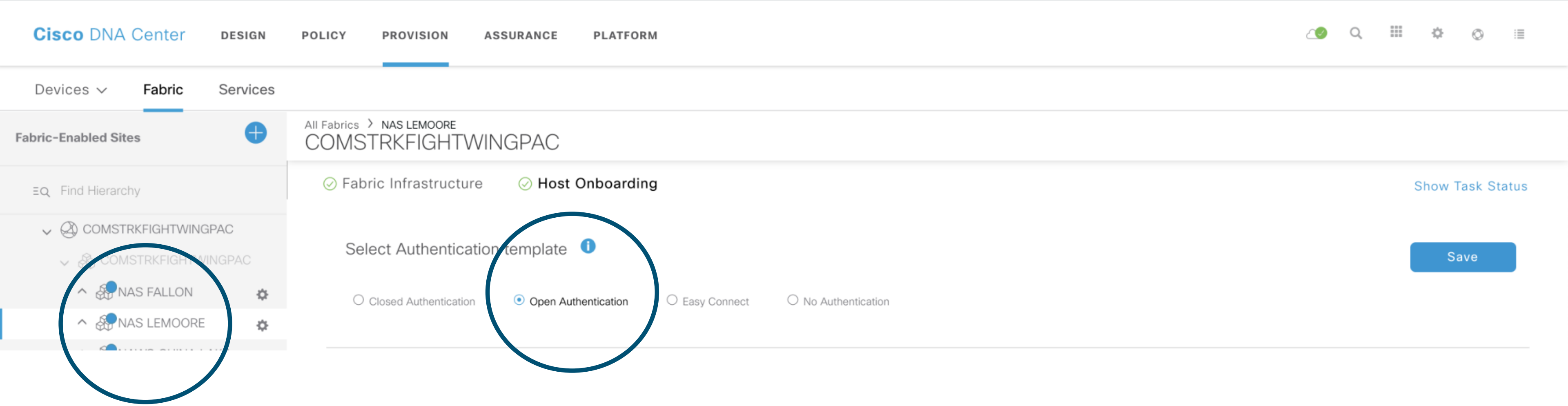


Authentication Template

Per-Site Authentication Template

B Policy

1 Identity



All Fabrics > NAS LEMOORE

COMSTRKFIGHTWINGPAC

✓ Fabric Infrastructure ✓ Host Onboarding

Show Task Status

Select Authentication template

○ Closed Authentication ● Open Authentication ○ Easy Connect ○ No Authentication

Save

cisco Live!

Designing a Single-Site Segmentation

Macro vs. Micro Segmentation

Virtual Networks

Complete Isolation

Standalone Environments

When/Why to Use?

1. Default Policy: Endpoints are NOT ABLE to communicate
2. Selective Permit rules typically via Firewall
3. Different Lines of Business, Compliance, Partners, etc.

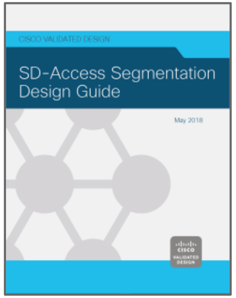
Scalable Groups

Logical Separation

Flexible Access Control

When/Why to Use?

1. Default Policy: Endpoints are ABLE to communicate
2. Selective Deny rules typically via Group ACL
3. Different Teams, Privileges, Responsibilities, etc.



CISCO VALIDATED DESIGN

SD-Access Segmentation Design Guide

May 2018

www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Segmentation-Design-Guide-2018MAY.pdf

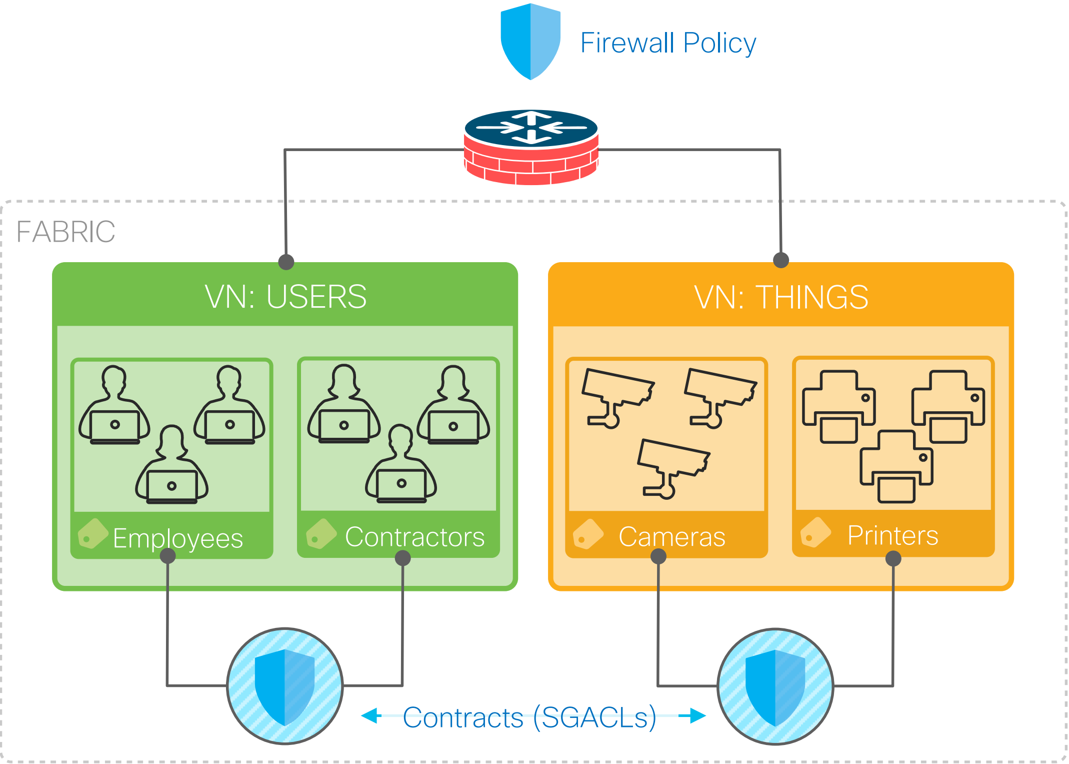
SDA enables Macro & Micro-segmentation

Inter-VN routing and policy enforcement on 'Fusion' or 'Firewall'

Macro segmentation with 'Virtual Networks'

Micro segmentation with 'Scalable Groups'

Contracts control access between SGTs

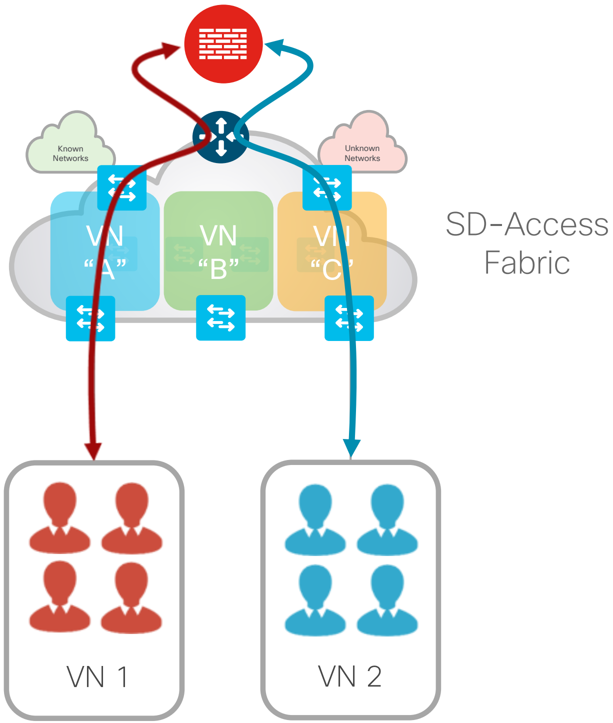


SD-Access Macro Segmentation

How many VRF/VNs – External Considerations

B Policy

2 **Segment**



IP Handoffs – Considerations:

- VRF-Lite configurations
- Fusion Router configuration
- Redistributions
- Configuration management
- Inter-VN Multicast requirements
- Platform scale

The 4 Common Virtual Networks

Some variation appears in 80% of networks

B Policy

2 **Segment**

Campus/Staff

Employees, Contractors, etc.

PCs, Phones, Printers, etc.

Guest/BYOD

Visitors, Clients, Partners, etc.

BYOD, Guest Wi-Fi, etc.

BMS/IOT

Robots, Pumps, Panels, etc.

HVAC, Lights, CCTV, etc.

Records/Research

Developers, Finance, Labs, etc.

PCs, Servers, Databases, etc.

May use DEFAULT_VN

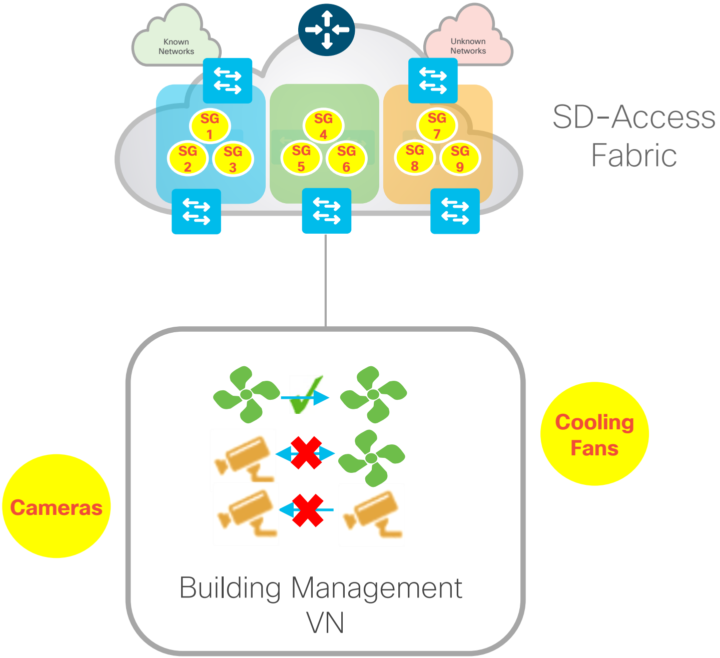
Micro-Segmentation Group Tags

SD-Access Segmentation

Two Level Hierarchy - Micro Level

B Policy

2 **Segment**



Scalable Group (SG)

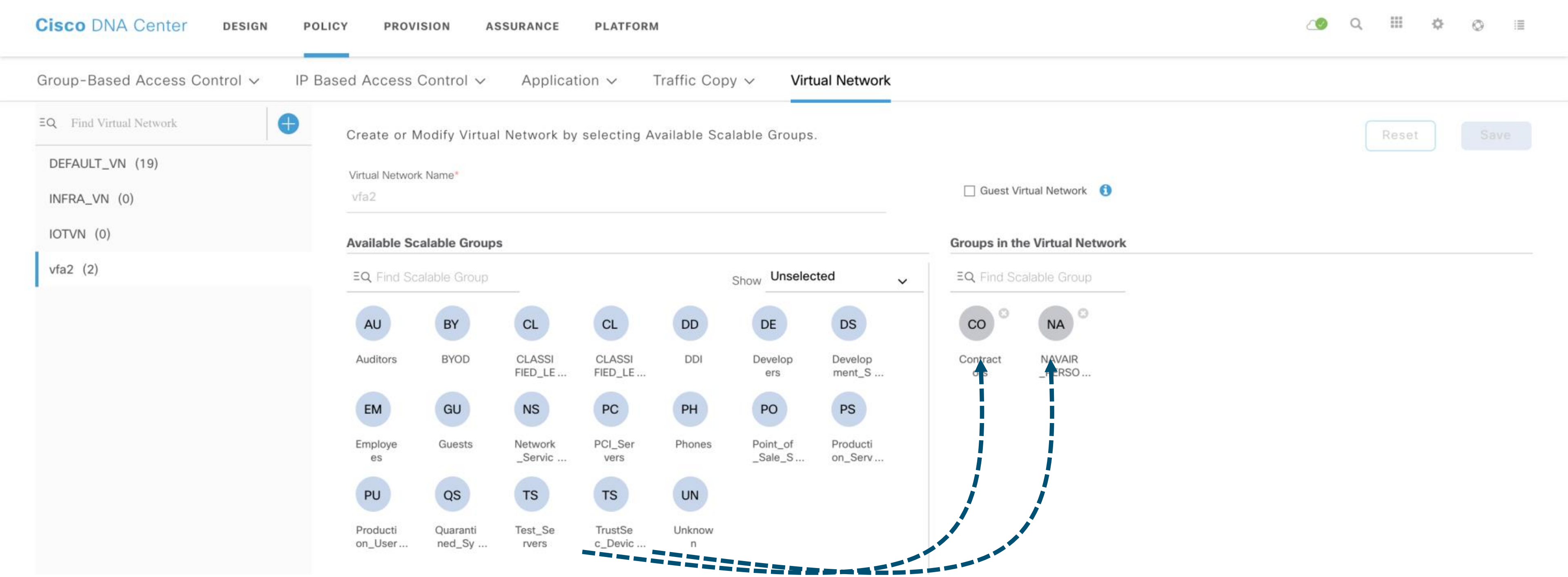
Second-level Segmentation ensures role based access control between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

SD-Access Segmentation

Assigning Scalable Groups to Virtual Networks

B Policy

2 **Segment**



DEFAULT_VN (19)

INFRA_VN (0)

IOTVN (0)

vfa2 (2)

Create or Modify Virtual Network by selecting Available Scalable Groups.

Virtual Network Name*: vfa2

□ Guest Virtual Network

Available Scalable Groups

Find Scalable Group — Show: Unselected

AU Auditors; BY BYOD; CL CLASSIFIED_LE ...; CL CLASSIFIED_LE ...; DD DDI; DE Developers; DS Development_S ...; EM Employees; GU Guests; NS Network_Servic ...; PC PCI_Servers; PH Phones; PO Point_of_Sale_S ...; PS Production_Serv ...; PU Production_User ...; QS Quarantined_Sy ...; TS Test_Servers; TS TrustSec_Devic ...; UN Unknown

Groups in the Virtual Network

Find Scalable Group

CO Contractors; NA NAVAIR_PERSO ...

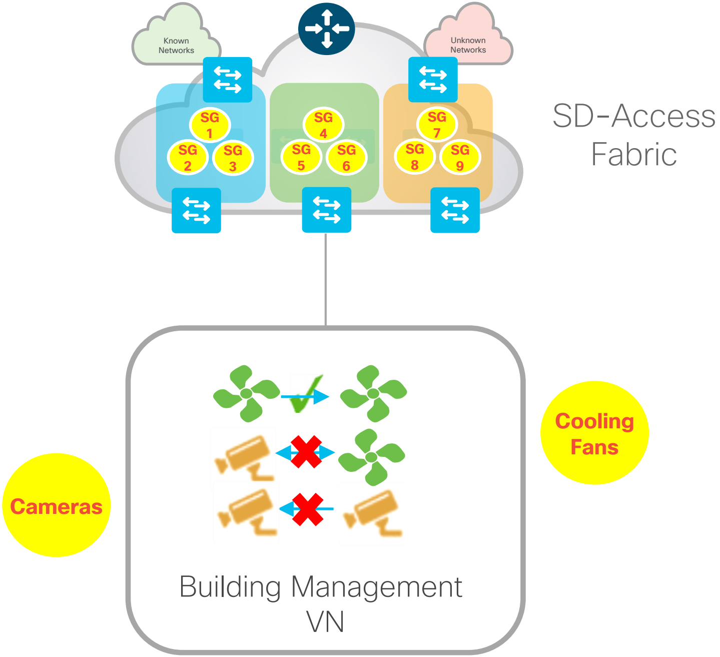
SD-Access Segmentation

Micro-Level aka Group Tags

- Lines of Businesses
- Roles within LoBs
- Differentiated access within fabric, external to fabric
- Start small – make batches for example and give out to LoBs
- Make the numbers significant to the LoB – for example, 1000-1999 is for Finance, 2000-2999 is for HR and so on
- Hold some in reserve – just like IP Subnets
- Establish process of requesting more Group Tags

SD-Access Segmentation

Micro Level – Scale of various parameters



Scale:

- Tag Bindings – refer to platform scale
  - 9300 can scale to 8k, whereas a 3850 can scale to 4k

IP-2-Tag Binding

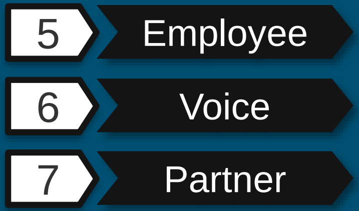
```
C9300#sh cts role-based sgt-map vrf SJC15_VN all details
%IPv6 protocol is not enabled in VRF SJC15_VN
Active IPv4-SGT Bindings Information

IP Address             Security Group                         Source
=======================================================================
192.168.6.3            4:Employees                             LOCAL
192.168.6.4            5:Contractor                            LOCAL
192.168.6.5            4:Employees                             LOCAL
192.168.6.6            4:Employees                             LOCAL
192.168.6.7            6:Auditor                               LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 5
Total number of active   bindings = 5
```

Count towards 8K limit

Cisco TrustSec Functions

B Policy

2 **Segment**



Classification

- Assigning SGTs
- Static Assignments
- Dynamic Assignments

Propagation

- Inline SGT
- SXP and pxGrid

Enforcement

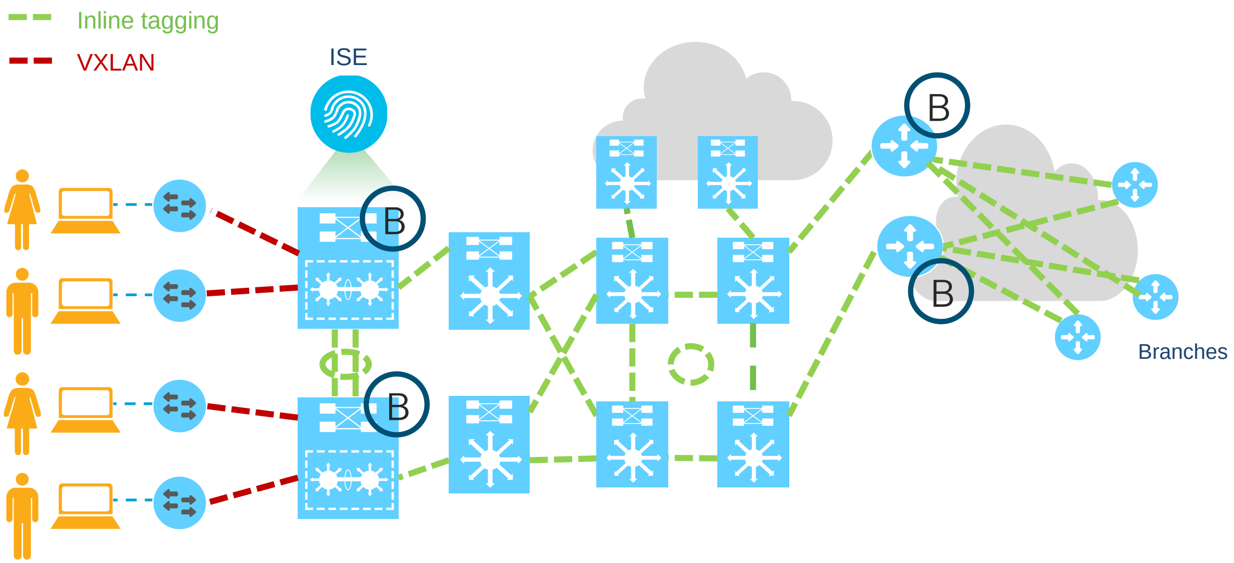
- Security Group ACL
- Internal Enforcement
- External Enforcement

Group Tag Propagation

Inline propagation

B Policy

2 **Segment**



- Simple & Scalable where devices support inline tagging in hardware
- SGT information stays with traffic

Propagation options

- Ethernet
- IPsec
- DM-VPN
- GET-VPN
- GRE
- **VXLAN**

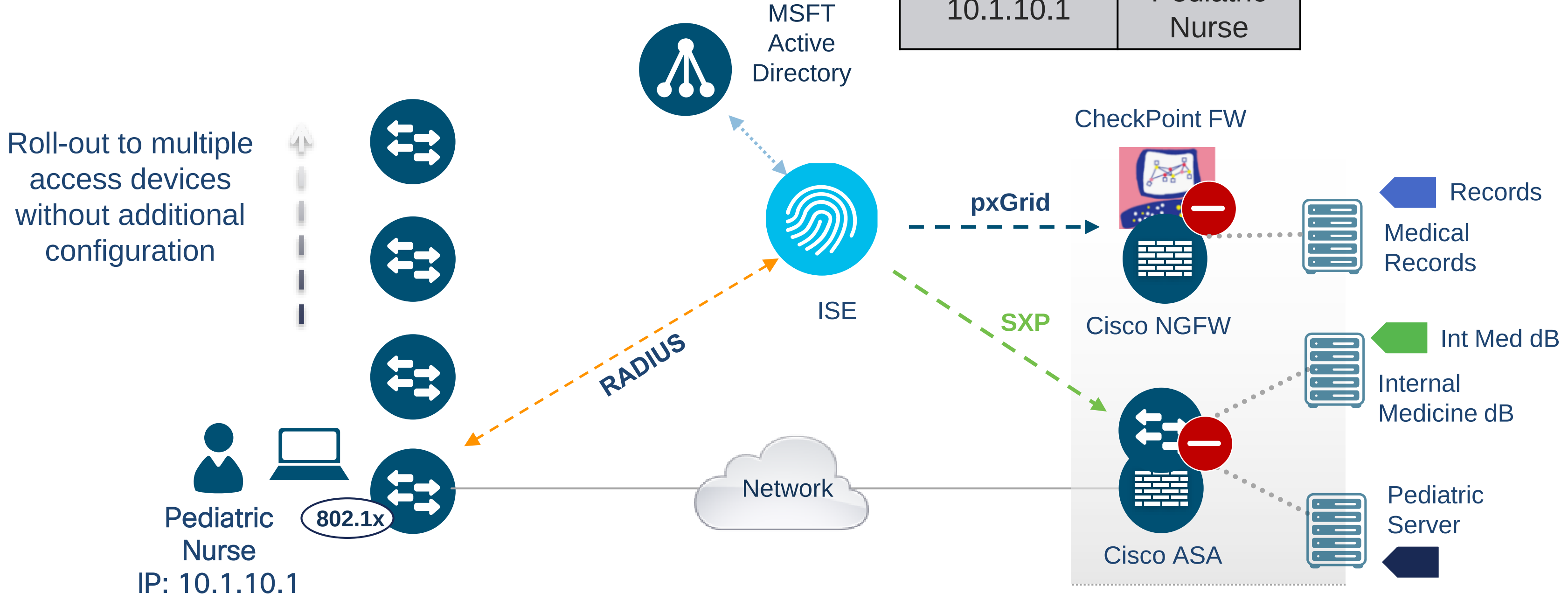
Supporting devices

- Catalyst switches
- WLAN controllers
- Nexus switches
- Integrated Service Routers
- Industrial Ethernet Switches
- ASR 1000
- ASA 5500-x
- Firepower Threat Defense

Group Tag Propagation

Secure eXchange Protocol (SXP) and pxGrid

IP Address	SGT
10.1.10.1	Pediatric Nurse

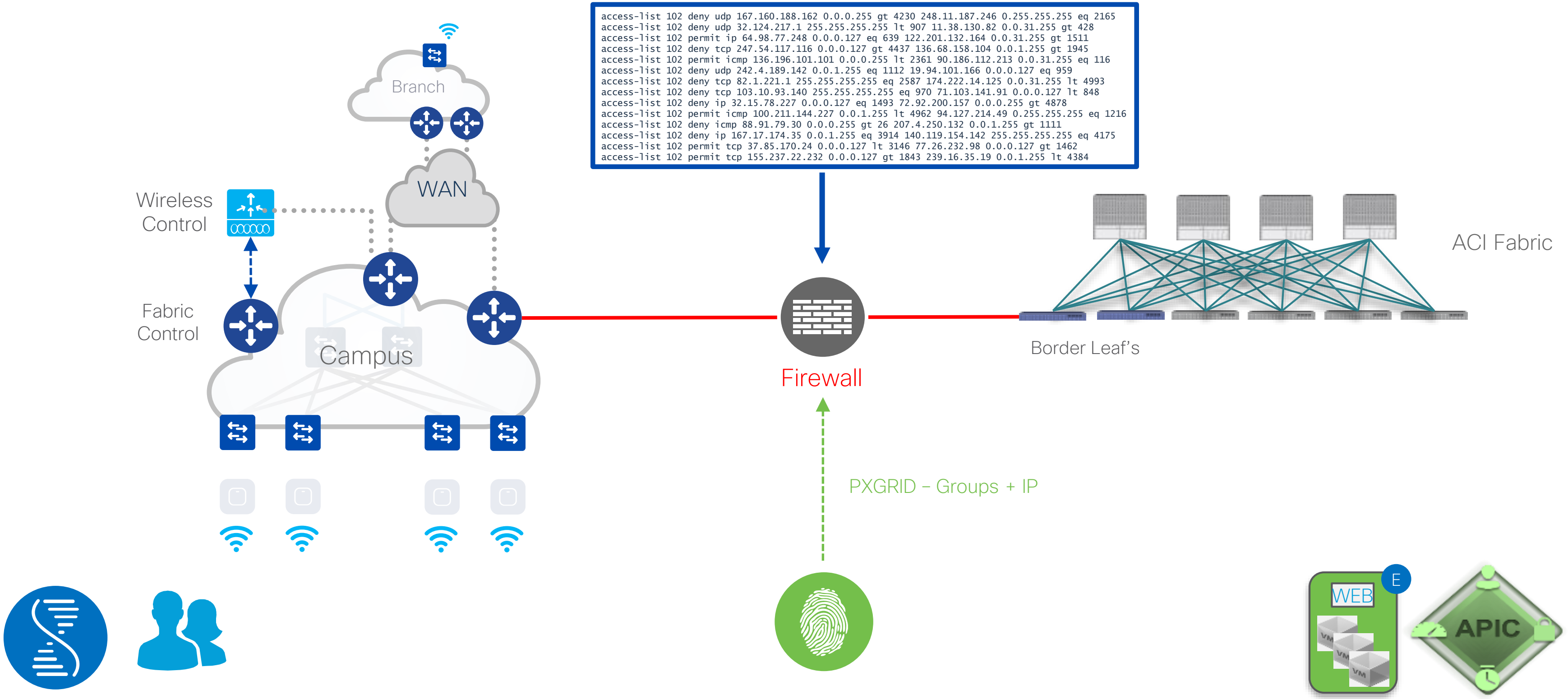


Roll-out to multiple access devices without additional configuration

SDA & Firewall Identity Exchange

B Policy

2 **Segment**



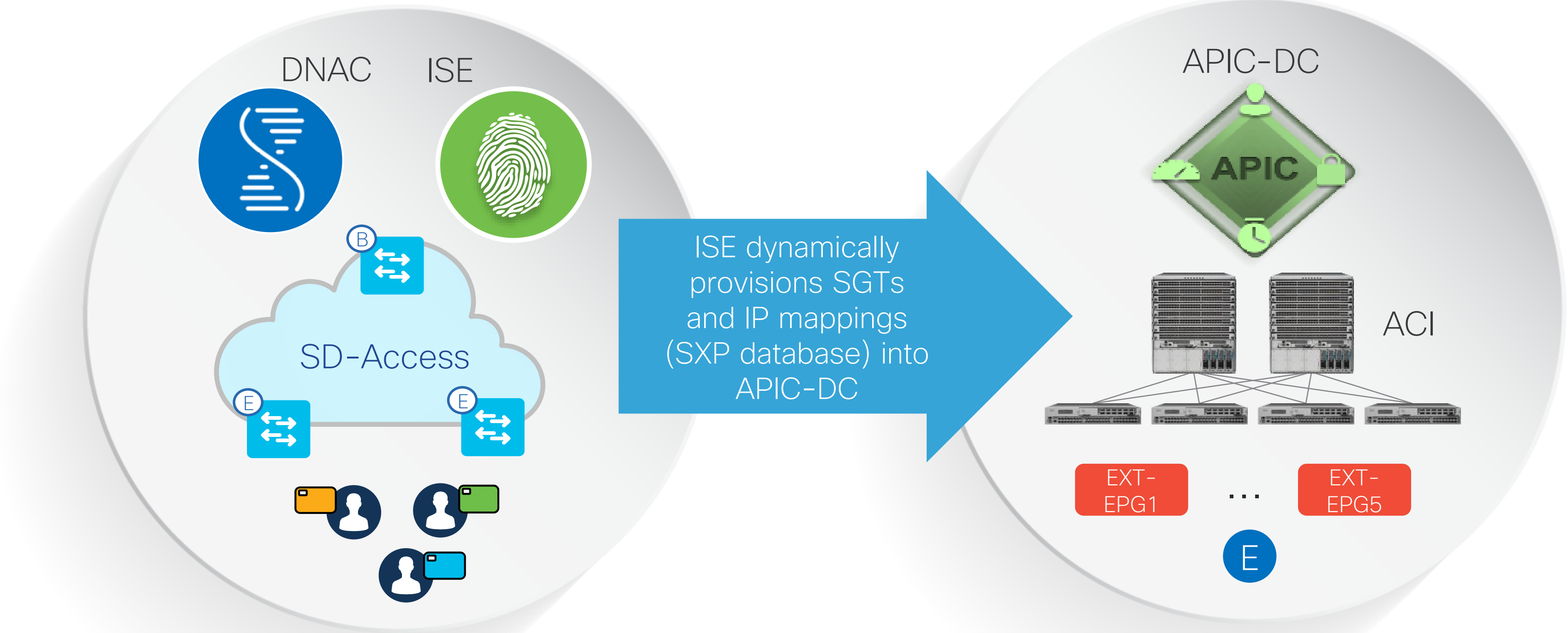
```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny 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
```

SDA & ACI Identity Exchange

Fabric SGTs Provisioned in ACI

B Policy

2 **Segment**



ISE dynamically provisions SGTs and IP mappings (SXP database) into APIC-DC

SDA SGTs (from Cisco ISE)

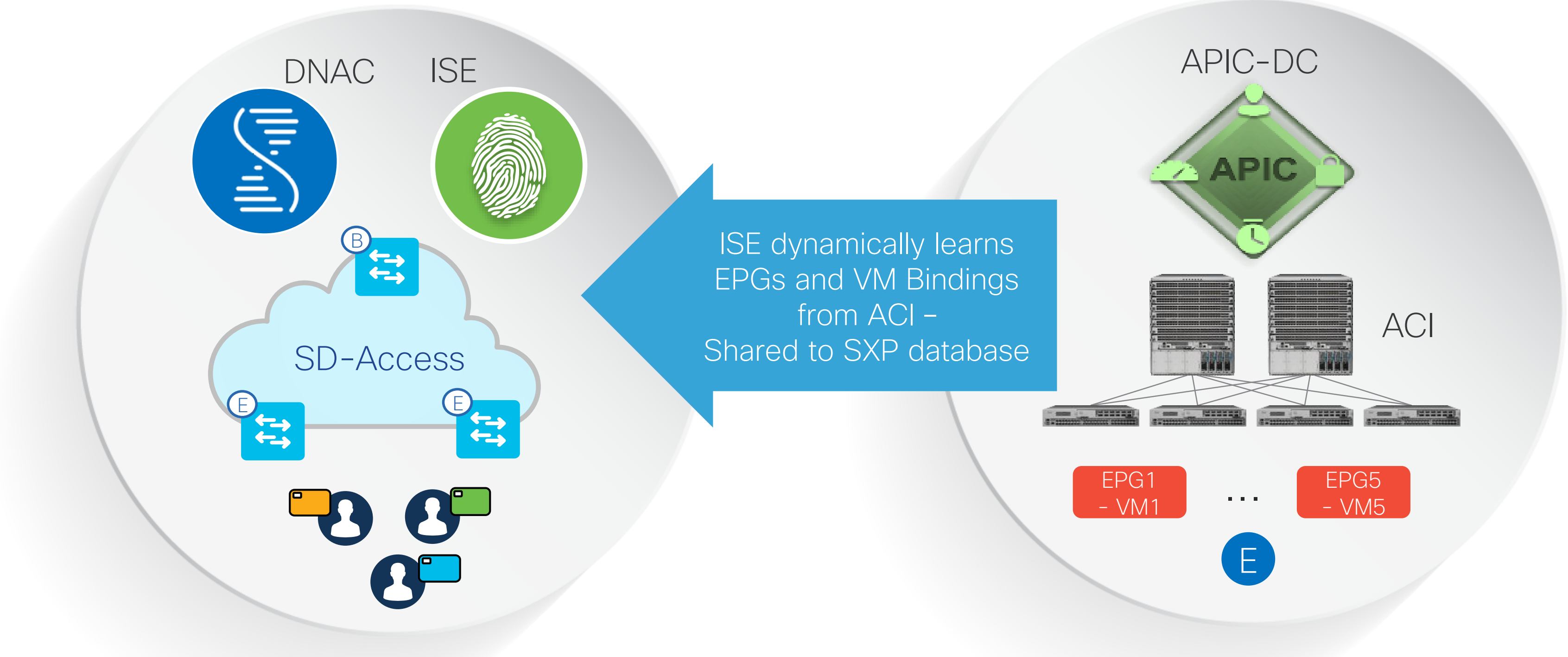
External EPGs (Outside ACI Fabric)

SDA & ACI Identity Exchange

ACI Fabric EPGs Provisioned in SD-Access

B Policy

2 **Segment**



ISE dynamically learns EPGs and VM Bindings from ACI – Shared to SXP database

ACI SGTs (from APIC-DC)

Internal EPGs (Inside ACI Fabric)

Designing a Single-Site Segmentation

Macro vs. Micro Segmentation

Virtual Networks

Complete Isolation

Standalone Environments

When/Why to Use?

1. Default Policy: Endpoints are NOT ABLE to communicate
2. Selective Permit rules typically via Firewall
3. Different Lines of Business, Compliance, Partners, etc.

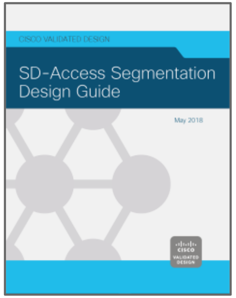
Scalable Groups

Logical Separation

Flexible Access Control

When/Why to Use?

1. Default Policy: Endpoints are ABLE to communicate
2. Selective Deny rules typically via Group ACL
3. Different Teams, Privileges, Responsibilities, etc.



CISCO VALIDATED DESIGN

SD-Access Segmentation Design Guide

May 2018

www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Segmentation-Design-Guide-2018MAY.pdf

SDA enables Macro & Micro-segmentation

B Policy

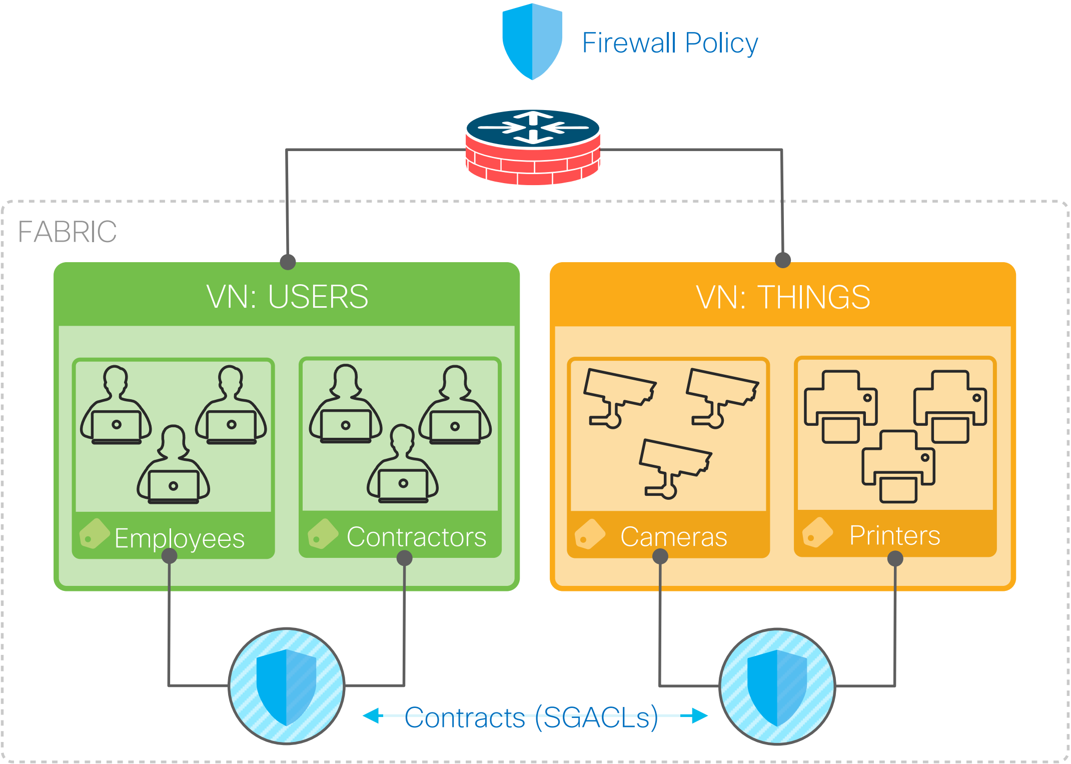
2 **Segment**

Inter-VN routing and policy enforcement on 'Fusion' or 'Firewall'

Macro segmentation with 'Virtual Networks'

Micro segmentation with 'Scalable Groups'

Contracts control access between SGTs

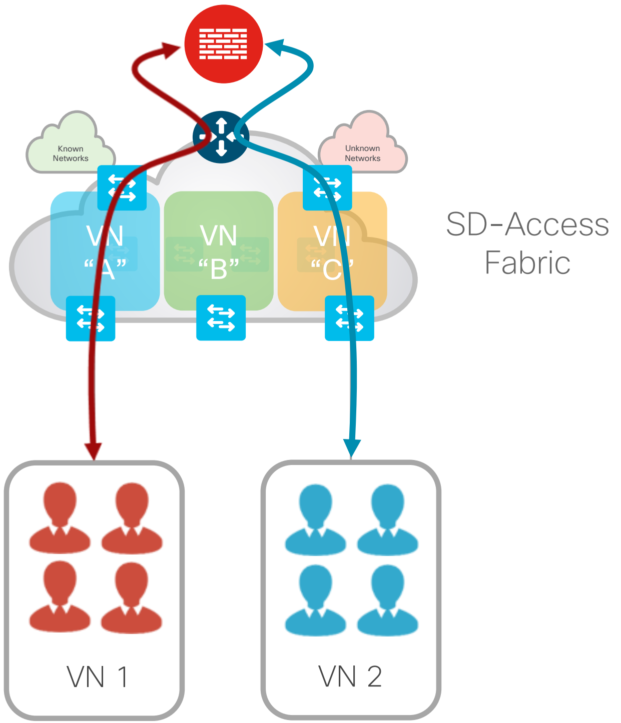


SD-Access Macro Segmentation

How many VRF/VNs – External Considerations

B Policy

2 **Segment**



IP Handoffs – Considerations:

- VRF-Lite configurations
- Fusion Router configuration
- Redistributions
- Configuration management
- Inter-VN Multicast requirements
- Platform scale

The 4 Common Virtual Networks

Some variation appears in 80% of networks

Campus/Staff

Employees, Contractors, etc.

PCs, Phones, Printers, etc.

Guest/BYOD

Visitors, Clients, Partners, etc.

BYOD, Guest Wi-Fi, etc.

BMS/IOT

Robots, Pumps, Panels, etc.

HVAC, Lights, CCTV, etc.

Records/Research

Developers, Finance, Labs, etc.

PCs, Servers, Databases, etc.

May use DEFAULT_VN

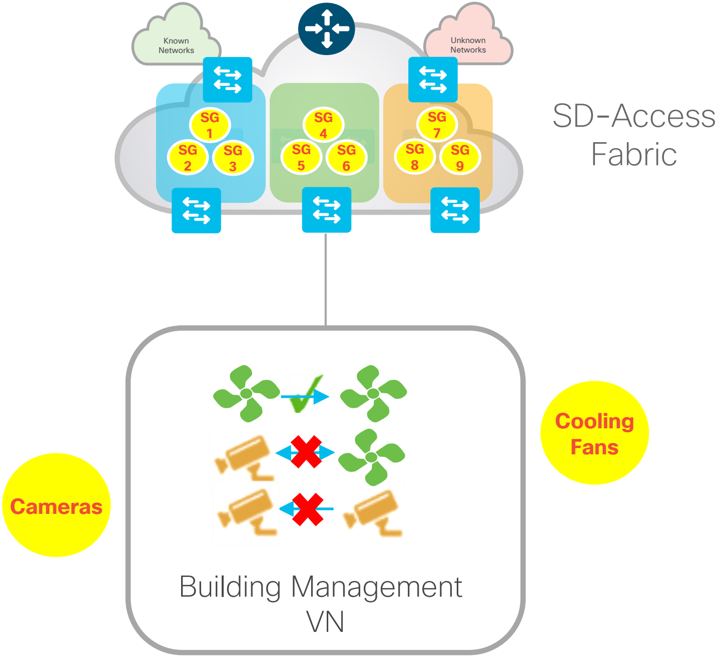
Micro-Segmentation Group Tags

SD-Access Segmentation

Two Level Hierarchy - Micro Level

B Policy

2 **Segment**



Scalable Group (SG)

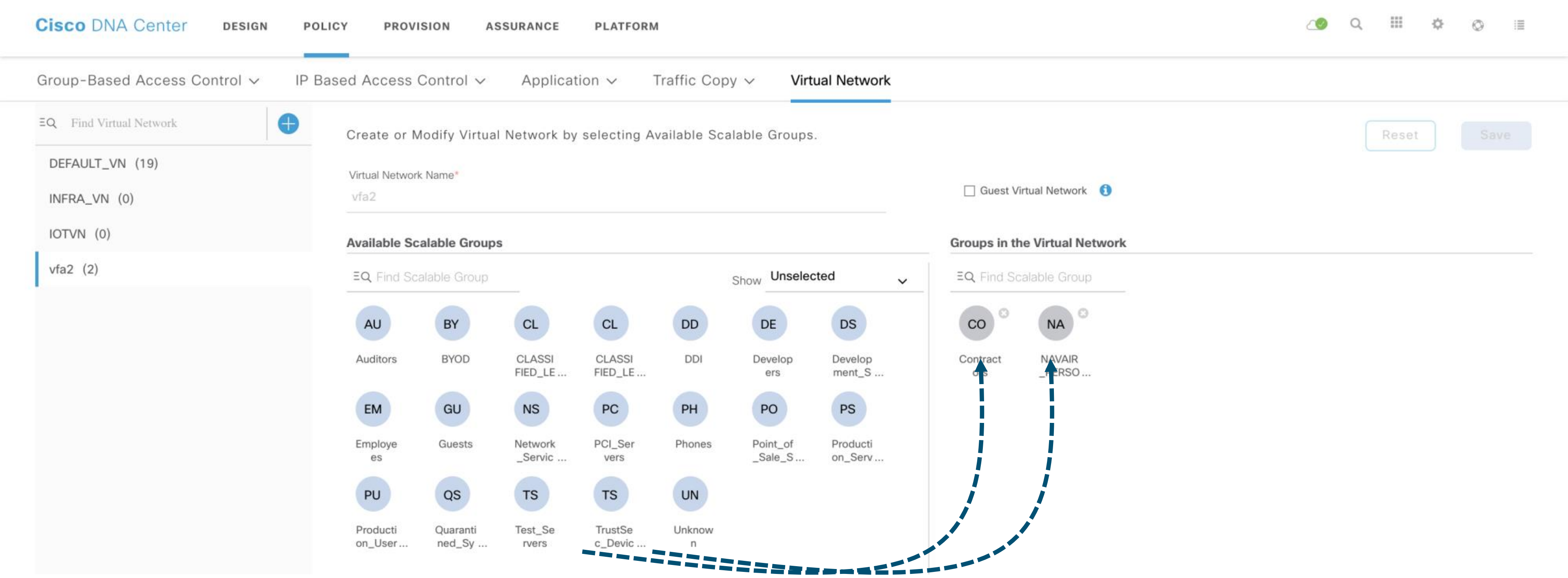
Second-level Segmentation ensures role based access control between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

SD-Access Segmentation

Assigning Scalable Groups to Virtual Networks

B Policy

2 Segment



DEFAULT_VN (19)
INFRA_VN (0)
IOTVN (0)
vfa2 (2)

Create or Modify Virtual Network by selecting Available Scalable Groups.

Virtual Network Name*: vfa2

□ Guest Virtual Network

Available Scalable Groups

Show: Unselected

AU Auditors, BY BYOD, CL CLASSIFIED_LE ..., CL CLASSIFIED_LE ..., DD DDI, DE Developers, DS Development_S ..., EM Employees, GU Guests, NS Network_Servic ..., PC PCI_Servers, PH Phones, PO Point_of_Sale_S ..., PS Production_Serv ..., PU Production_User ..., QS Quarantined_Sy ..., TS Test_Servers, TS TrustSec_Devic ..., UN Unknown

Groups in the Virtual Network

CO Contractors, NA NAVAIR_PERSO ...

SD-Access Segmentation

Micro-Level aka Group Tags

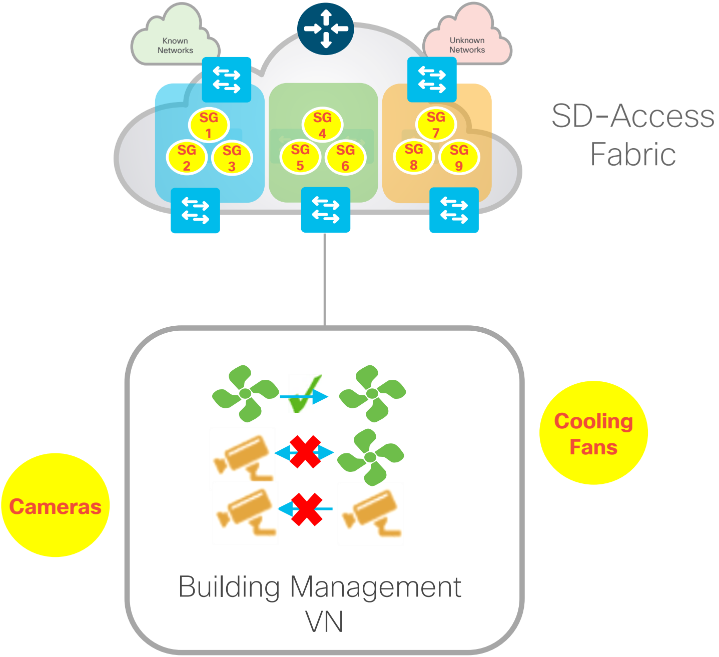
- Lines of Businesses
- Roles within LoBs
- Differentiated access within fabric, external to fabric
- Start small – make batches for example and give out to LoBs
- Make the numbers significant to the LoB – for example, 1000-1999 is for Finance, 2000-2999 is for HR and so on
- Hold some in reserve – just like IP Subnets
- Establish process of requesting more Group Tags

SD-Access Segmentation

Micro Level – Scale of various parameters

B Policy

2 **Segment**



Scale:

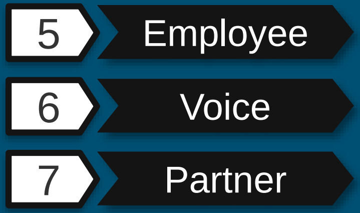
- Tag Bindings – refer to platform scale
  - 9300 can scale to 8k, whereas a 3850 can scale to 4k

IP-2-Tag Binding

```
C9300#sh cts role-based sgt-map vrf SJC15_VN all details
%IPv6 protocol is not enabled in VRF SJC15_VN
Active IPv4-SGT Bindings Information

IP Address          Security Group                          Source
=======================================================================
192.168.6.3         4:Employees                              LOCAL
192.168.6.4         5:Contractor                            LOCAL
192.168.6.5         4:Employees                             LOCAL
192.168.6.6         4:Employees                             LOCAL
192.168.6.7         6:Auditor                               LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 5
Total number of active   bindings = 5
```

Count towards 8K limit

Cisco TrustSec Functions



Classification

- Assigning SGTs
- Static Assignments
- Dynamic Assignments

Propagation

- Inline SGT
- SXP and pxGrid

Enforcement

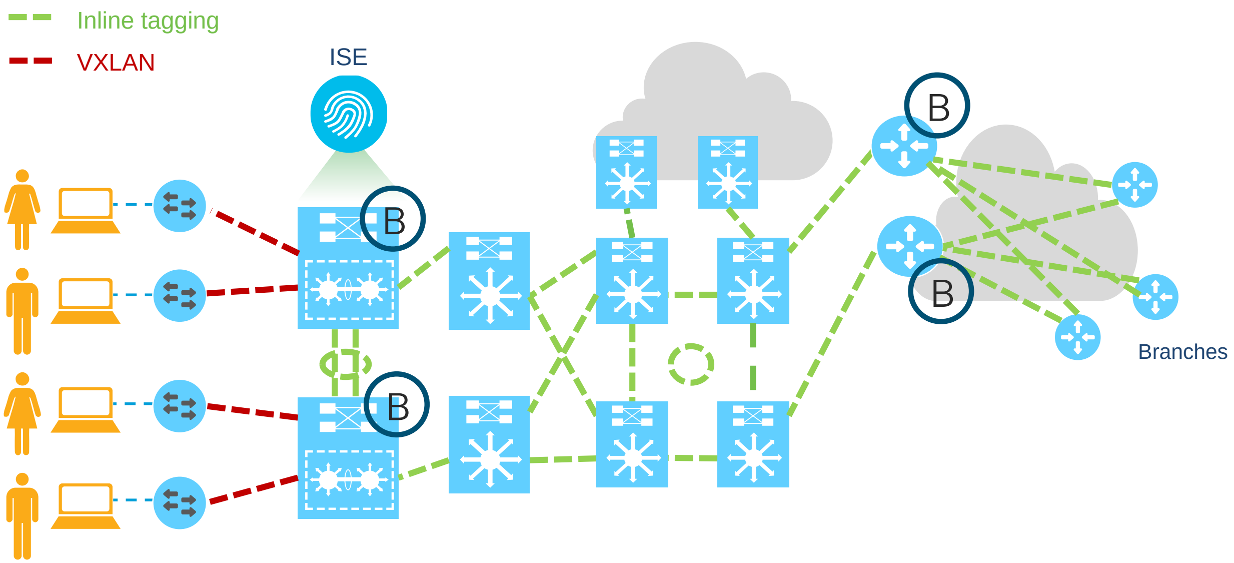
- Security Group ACL
- Internal Enforcement
- External Enforcement

Group Tag Propagation

Inline propagation

B Policy

2 **Segment**



- Simple & Scalable where devices support inline tagging in hardware
- SGT information stays with traffic

Propagation options

- Ethernet
- IPsec
- DM-VPN
- GET-VPN
- GRE
- **VXLAN**

Supporting devices

- Catalyst switches
- WLAN controllers
- Nexus switches
- Integrated Service Routers
- Industrial Ethernet Switches
- ASR 1000
- ASA 5500-x
- Firepower Threat Defense

Group Tag Propagation

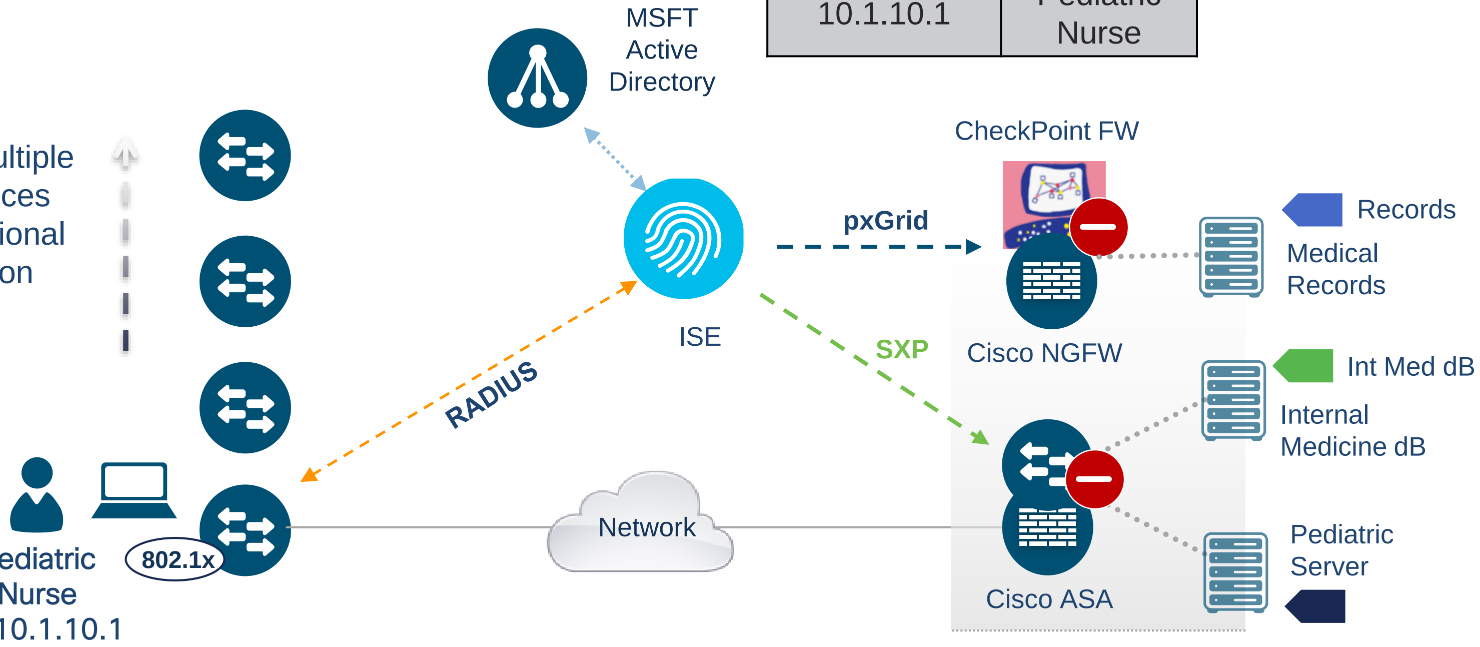
Secure eXchange Protocol (SXP) and pxGrid

B Policy

2 **Segment**

IP Address	SGT
10.1.10.1	Pediatric Nurse

Roll-out to multiple access devices without additional configuration



MSFT Active Directory

ISE

RADIUS

pxGrid

SXP

CheckPoint FW

Cisco NGFW

Cisco ASA

Network

Pediatric Nurse
IP: 10.1.10.1

802.1x

Records

Medical Records

Int Med dB

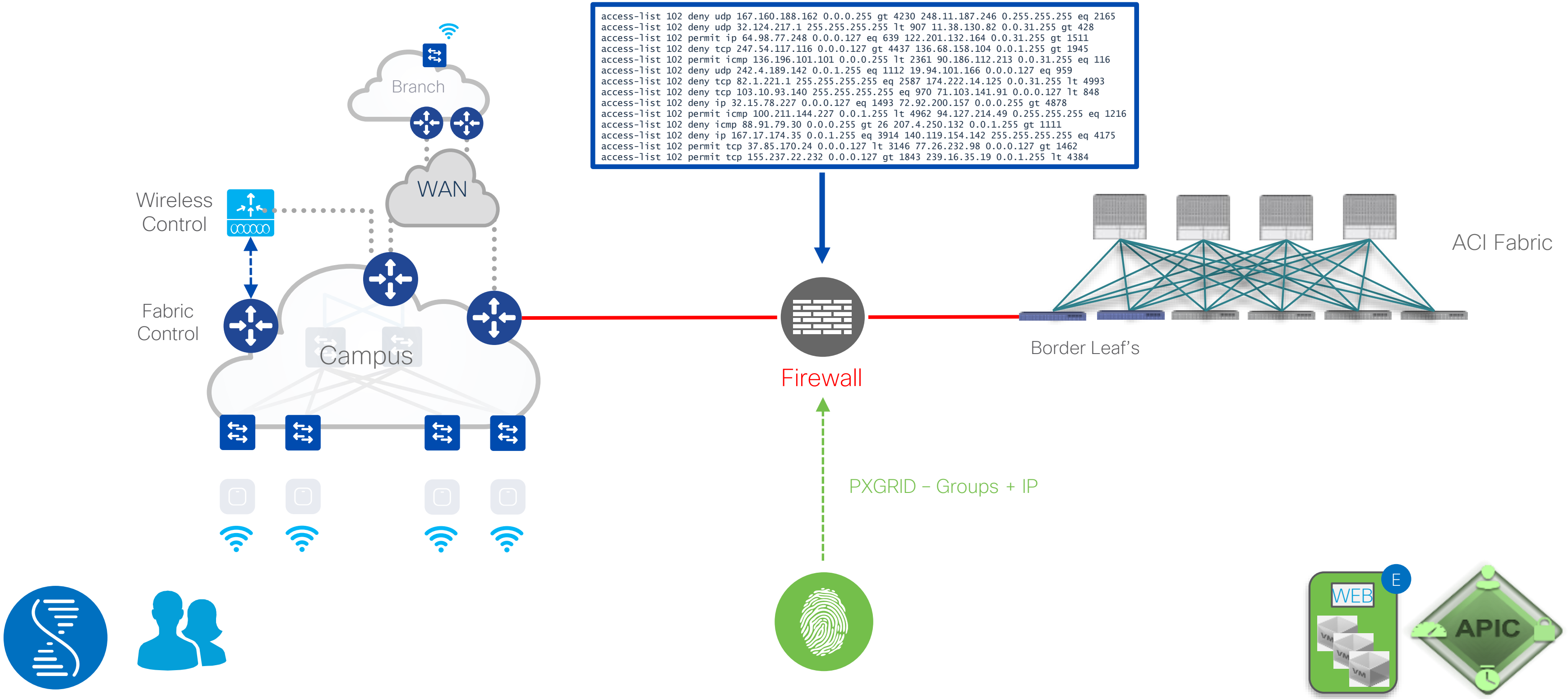
Internal Medicine dB

Pediatric Server

SDA & Firewall Identity Exchange

B Policy

2 **Segment**



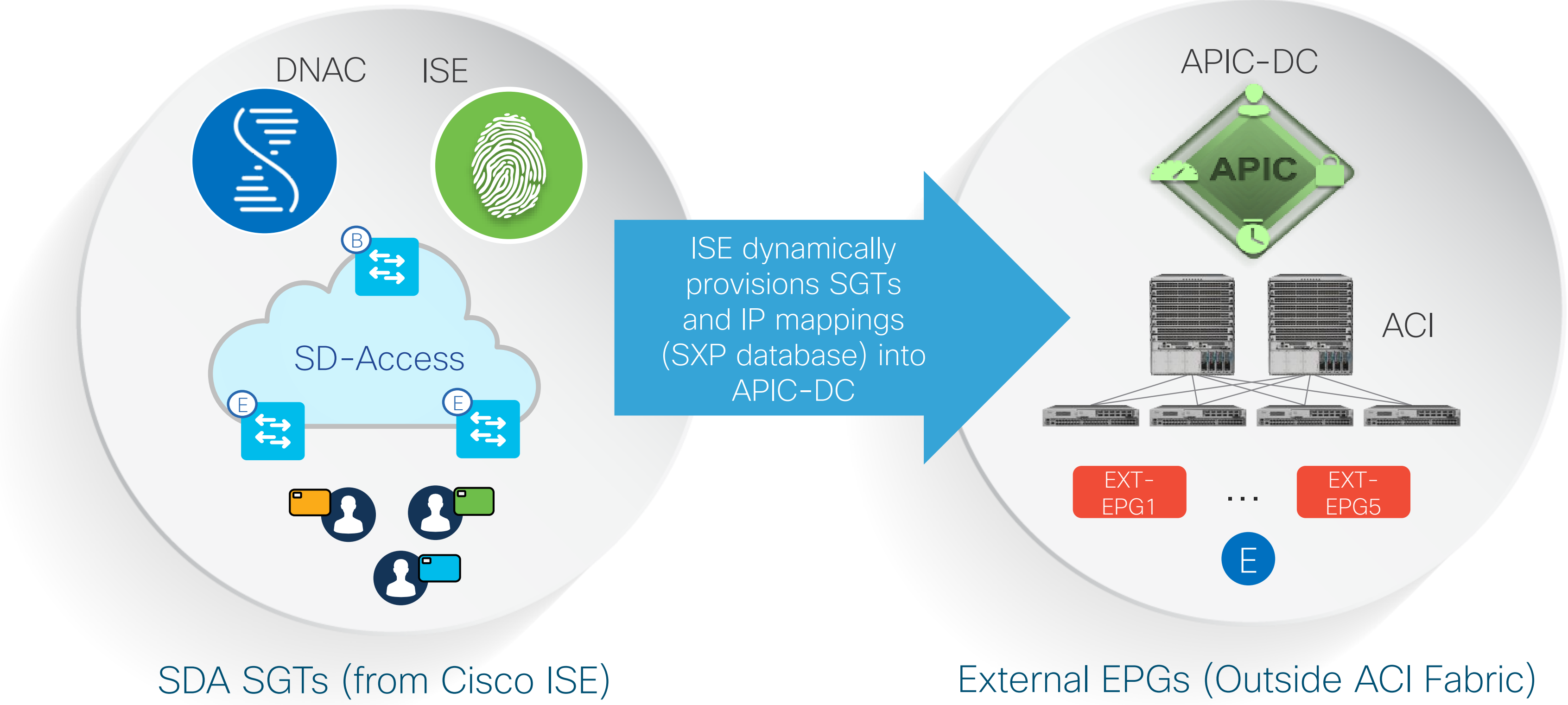
```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny 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
```

SDA & ACI Identity Exchange

Fabric SGTs Provisioned in ACI

B Policy

2 **Segment**



ISE dynamically provisions SGTs and IP mappings (SXP database) into APIC-DC

SDA SGTs (from Cisco ISE)

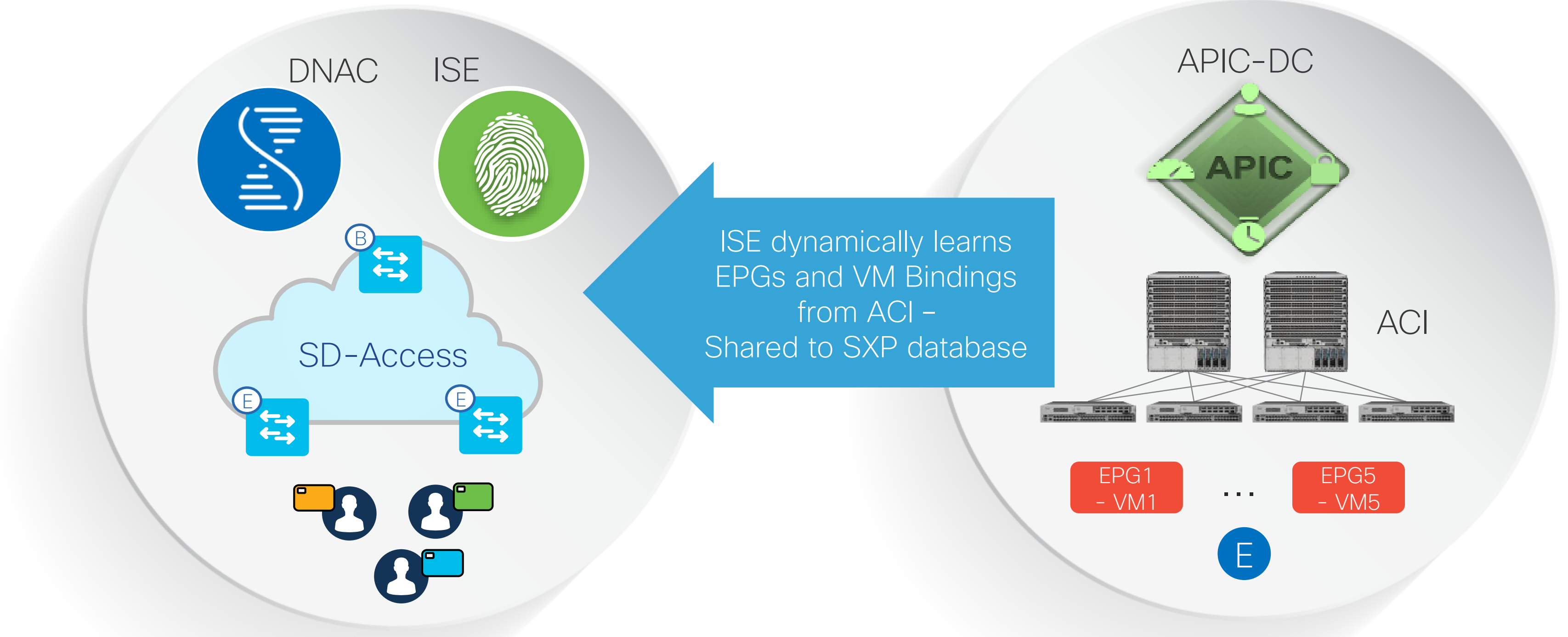
External EPGs (Outside ACI Fabric)

SDA & ACI Identity Exchange

ACI Fabric EPGs Provisioned in SD-Access

B Policy

2 **Segment**



ISE dynamically learns EPGs and VM Bindings from ACI – Shared to SXP database

ACI SGTs (from APIC-DC)

Internal EPGs (Inside ACI Fabric)

Designing a Single-Site Group-Based Policy

SD-Access Policy

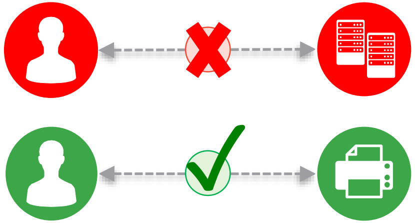
Policy Types

Access Control Policy

↓

Who can access What?

Permit / Deny Rules
for Group-to-Group Access



Application Policy

↓

How to treat Traffic?

QoS for Applications
or Application Caching

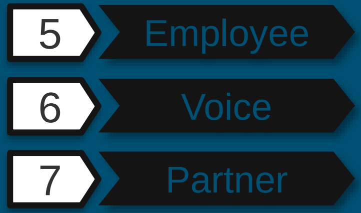
Traffic Copy Policy

↓

Need to Monitor Traffic?

Enable SPAN Services
for specific Groups or Traffic

Cisco TrustSec Functions

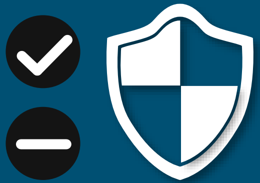


Classification

- Assigning SGTs
- Static Assignments
- Dynamic Assignments

Propagation

- Inline SGT
- SXP and pxGrid



Enforcement

- Security Group ACL
- Internal Enforcement
- External Enforcement

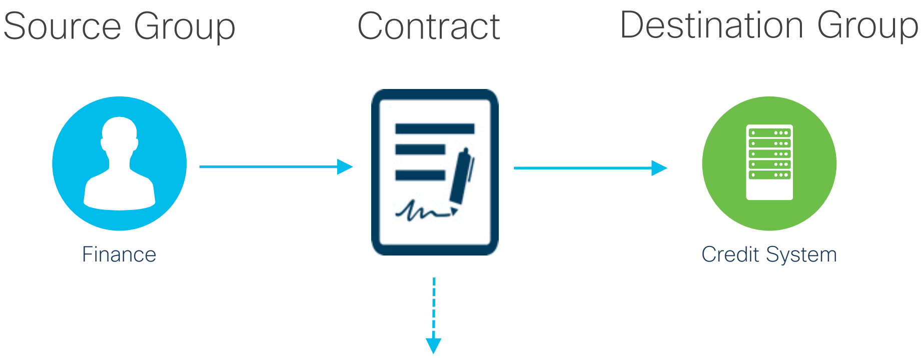
SD-Access Policy

SG-Access Control Policies

B Policy

3 **Policy**

Default is Permit



Source Group

Contract

Destination Group

Finance

Credit System

CLASSIFIER: PORT ▼

ACTION: DENY ▼

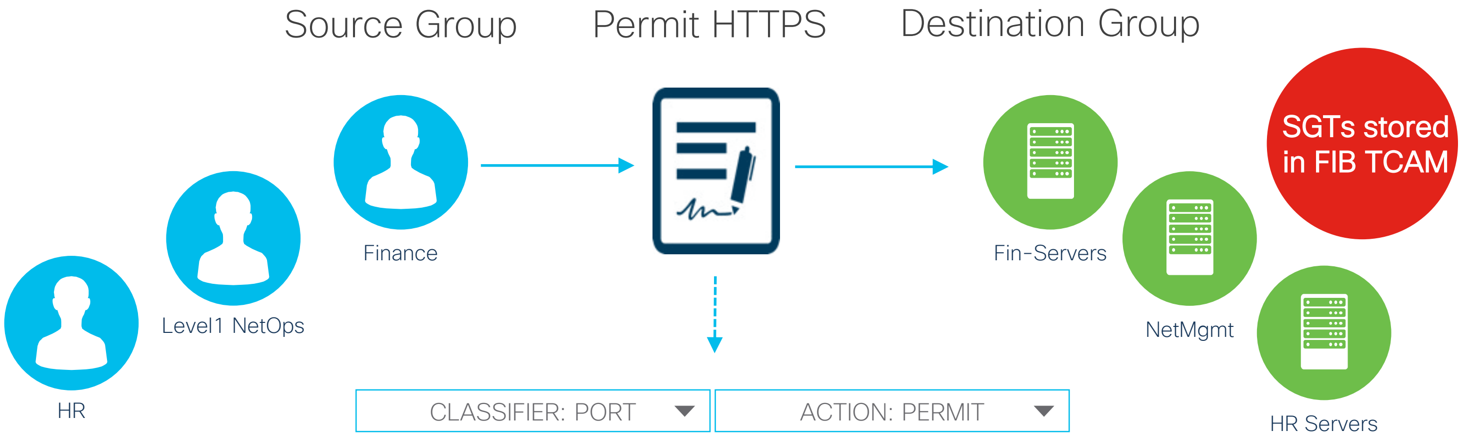
Classifier Type	Action Type
Port Number	Permit
Protocol Name	Deny
Application Type	Copy

Deny Rules in Campus

All groups in a Policy must belong to the same Virtual Network

SD-Access Policy

SG-ACL in Switch TCAM



SGTs stored in FIB TCAM

CLASSIFIER: PORT

ACTION: PERMIT

Protocol Name	L4 Port	Action Type
TCP	443	Permit
IP	-	Deny

Contract stored in ACL TCAM

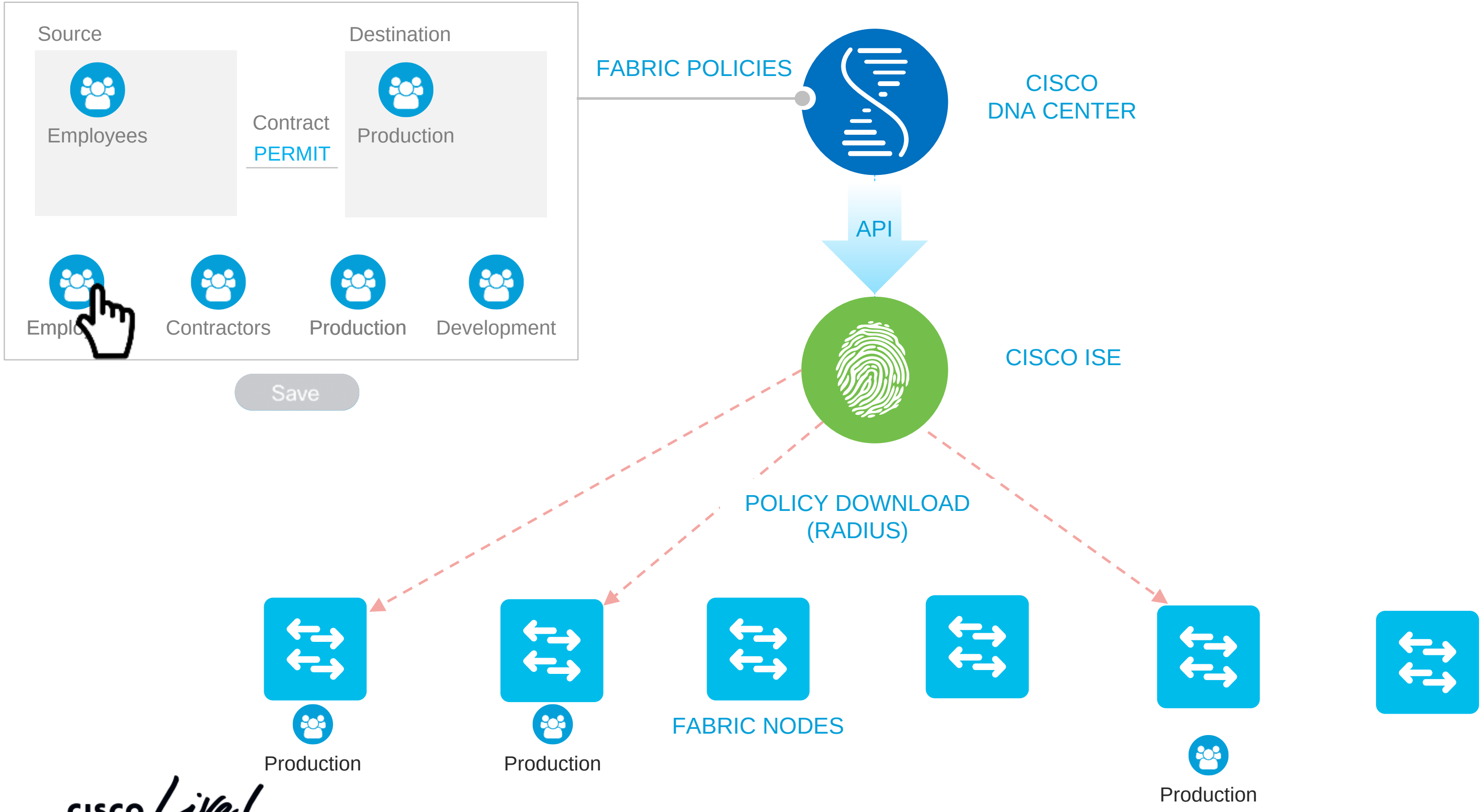
THESE ARE STILL TWO ENTRIES IN TCAM

SD-Access Policy

Scalable Group Policy rollout

B Policy

3 **Policy**



Source

Employees

Contract

PERMIT

Destination

Production

Employees

Contractors

Production

Development

Save

FABRIC POLICIES

CISCO DNA CENTER

API

CISCO ISE

POLICY DOWNLOAD (RADIUS)

FABRIC NODES

Production

Production

Production

You could go crazy!!

B Policy

3 **Policy**

Write it down on a spreadsheet!

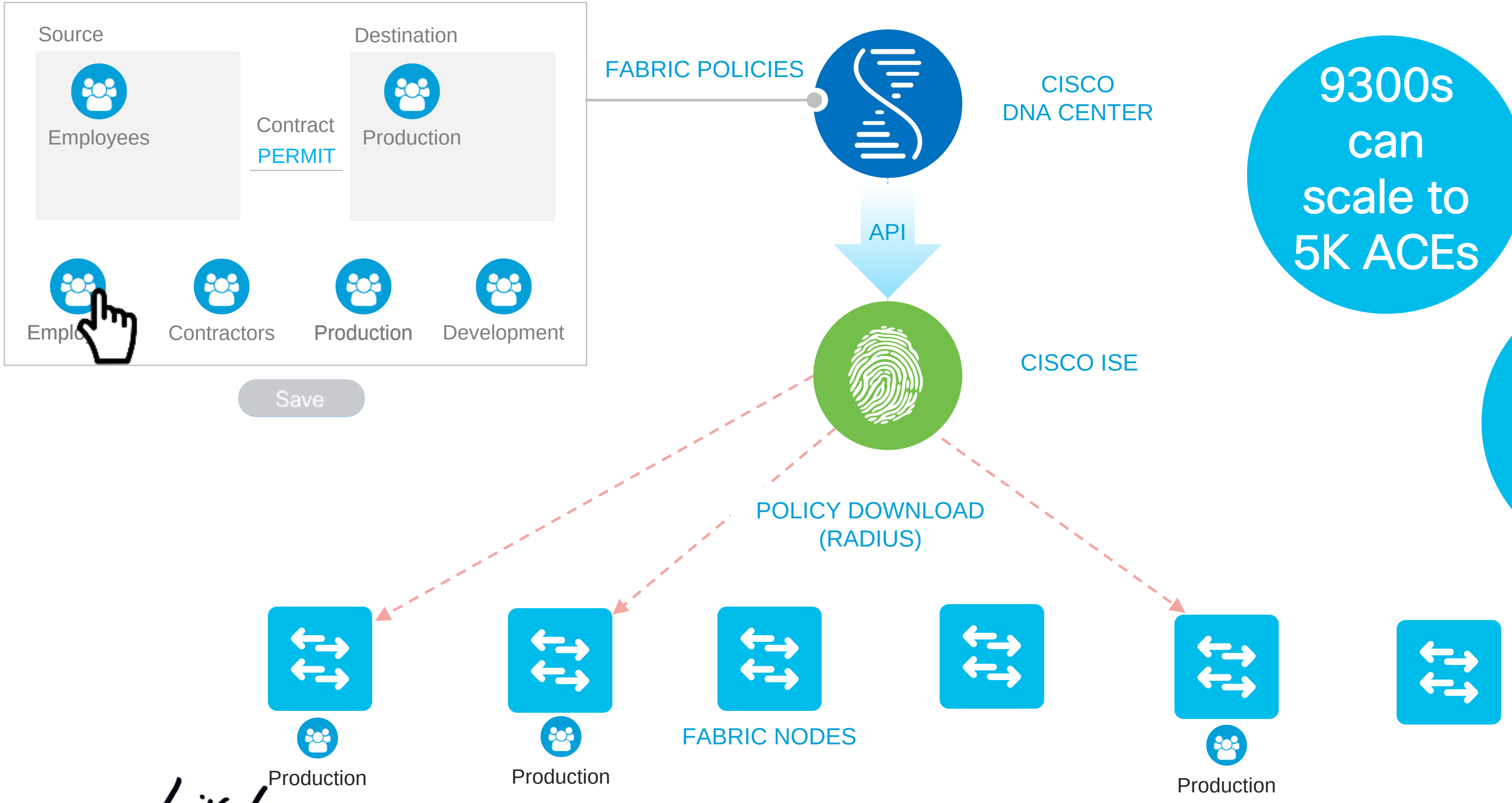
	Destination Group	Data Center Control Domain										Corporate Control Domain										
	Source Group	AD Servers	Network Services	Unified Communications	HVAC	App1	App2	App3	Security Applications	PartnerVDI Control Domain	Internet DMZ	Device1App1	Device2App1	Device1App2	User1App1	User1App2	User1App3	HVAC	BYOD Access	Quarantine	Security	Unified Communications
Data Center Control Domain	AD Servers	✓	❑	❑	✗	❑	❑	❑	❑	✗	✗	✗	✗	✗	❑	❑	❑	✗	✗	❑	✗	✗
	Network Services	❑	✓	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑	❑
	Unified Communications	❑	❑	✓	✗	✗	✗	✗	❑	✗	✗	✗	✗	✗	❑	❑	❑	✗	✗	✗	✗	✓
	HVAC	✗	❑	✗	✓	✗	✗	✗	✗	❑	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
	App1	❑	❑	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	❑	✗	✗	✗
	App2	❑	❑	✗	✗	✗	✓	✗	✗	✗	✗	❑	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗
	App3	❑	❑	✗	✗	✗	✗	❑	✗	✗	❑	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
	Security Applications	❑	❑	❑	✗	✗	✗	✗	✓	✗	❑	✗	✗	✗	✗	✗	✗	✗	✗	✗	❑	✗
	Partner VDI Control Domain	✗	❑	✗	❑	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	❑
	Internet DMZ	✗	❑	✗	✗	✗	✗	❑	❑	✗	✓	✗	✗	✗	❑	❑	❑	✗	✗	✗	✗	✗
Corporate Site Control Domain	Device1App1	✗	❑	✓	✗	✓	❑	✗	✗	✗	✗	❑	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Device2App1	✗	❑	✗	✗	✓	✗	✗	✗	✗	✗	✗	❑	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Device1App2	✗	❑	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	❑	✗	✗	✗	✗	✗	✗	✗	✗
	User1App1	❑	❑	❑	✗	✓	✗	✗	✗	✗	❑	✗	✗	✗	❑	❑	❑	✗	❑	✗	✗	❑
	User1App2	❑	❑	❑	✗	✗	✓	✗	✗	✗	❑	✗	✗	✗	❑	❑	❑	✗	❑	✗	✗	❑
	User1App3	❑	❑	❑	✗	✗	✗	✓	✗	✗	❑	✗	✗	✗	❑	❑	❑	✗	❑	✗	✗	❑
	HVAC	✗	❑	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	❑	✗	✗	✗	✗
	BYOD Access	✗	❑	✗	✗	❑	✗	✗	✗	✗	✗	✗	✗	✗	❑	❑	❑	✗	❑	✗	✗	✗
	Quarantine	❑	❑	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	❑	✗	✗
	Security	✗	❑	✗	✗	✗	✗	✗	❑	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	❑	✗
	Unified Communications	✗	❑	✓	✗	✗	✗	✗	✗	❑	✗	✗	✗	✗	❑	❑	❑	✗	✗	✗	✗	❑

SD-Access Policy

Scalable Group Policy rollout

B Policy

3 **Policy**

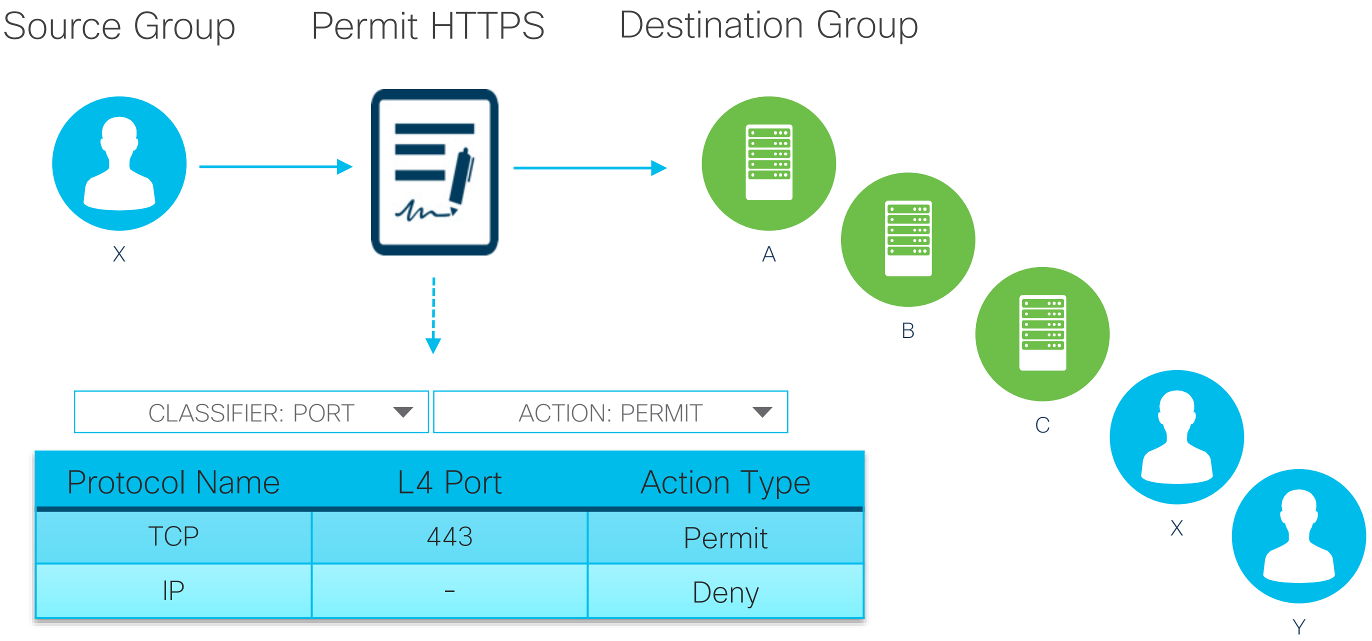


9300s can scale to 5K ACEs

3850s can scale to 1350 ACEs

SD-Access Policy

Group Tags and their use in SG-ACLs as Source and Destinations



CLASSIFIER: PORT ▼ ACTION: PERMIT ▼

Protocol Name	L4 Port	Action Type
TCP	443	Permit
IP	-	Deny

255 unique Destination Group Tags in a SG-ACL on a Catalyst 9000 Series Switch

IP-2-Tag Binding

```
C9300#sh cts role-based sgt-map vrf SJC15_VN all details
%IPv6 protocol is not enabled in VRF SJC15_VN
Active IPv4-SGT Bindings Information

IP Address          Security Group                           Source
========================================================================
192.168.6.3          4:Employees                              LOCAL
192.168.6.4          5:Contractor                             LOCAL
192.168.6.5          4:Employees                              LOCAL
192.168.6.6          4:Employees                              LOCAL
192.168.6.7          6:Auditor                                LOCAL

IP-SGT Active Bindings Summary
==========================================
Total number of LOCAL    bindings = 5
Total number of active   bindings = 5
```

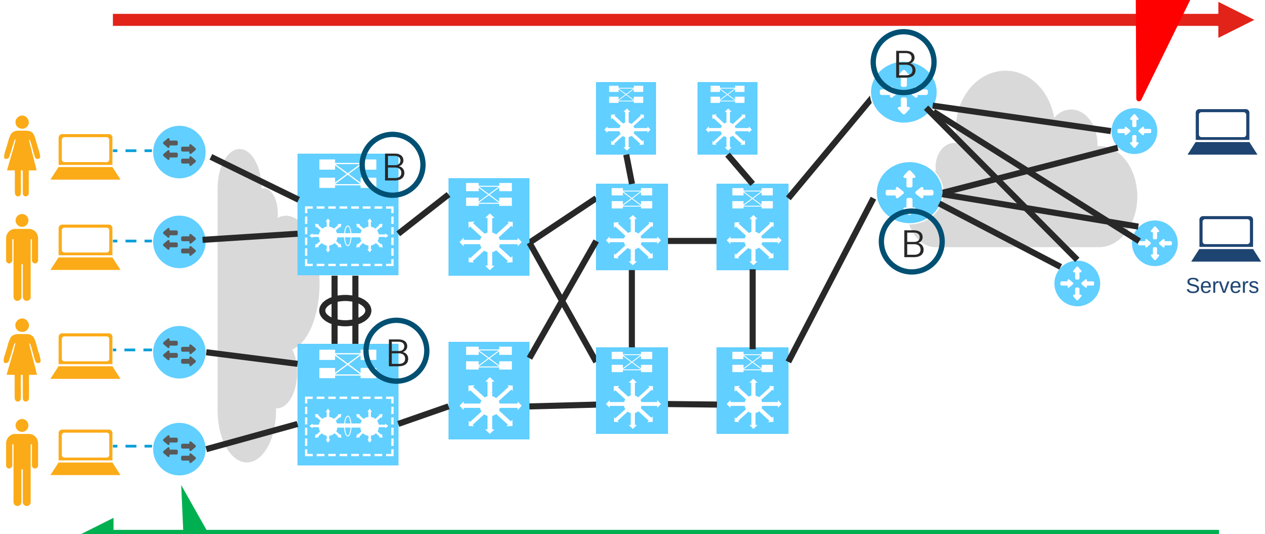
Count towards 255 limit

SD-Access Policy

Enforcement Point Considerations

B Policy

3 **Policy**



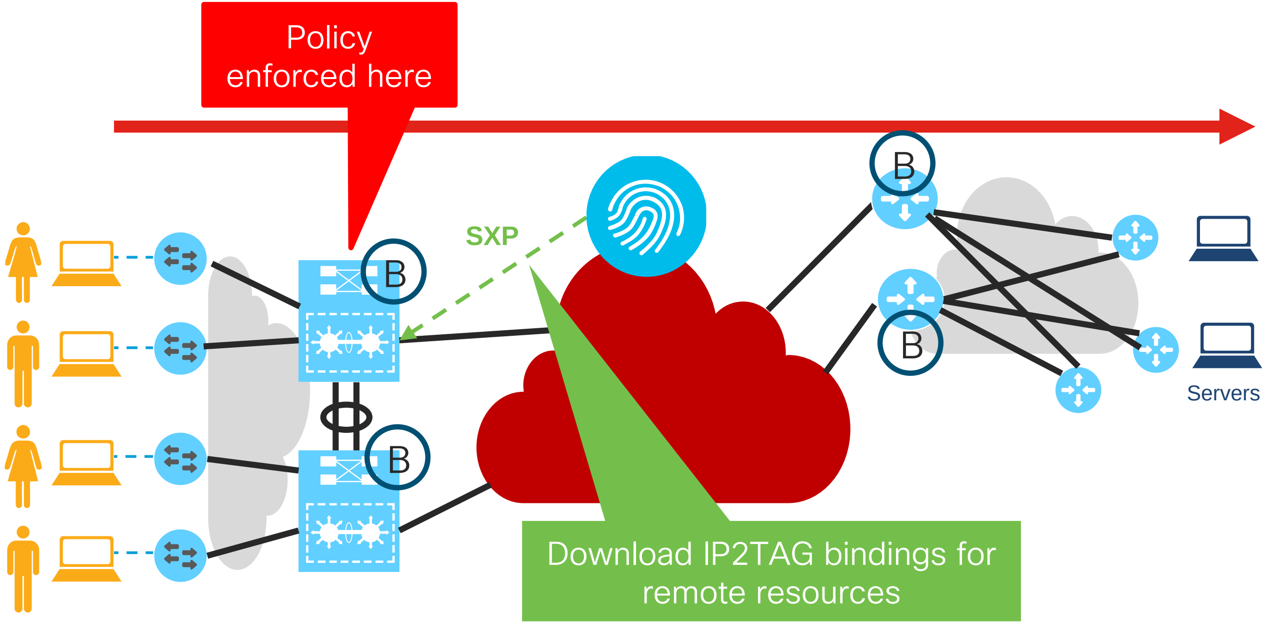
Policy enforced here

Policy enforced here

Default Egress Enforcement used by TrustSec: Efficient, and Scalable

SD-Access Policy

Enforcement Point Considerations

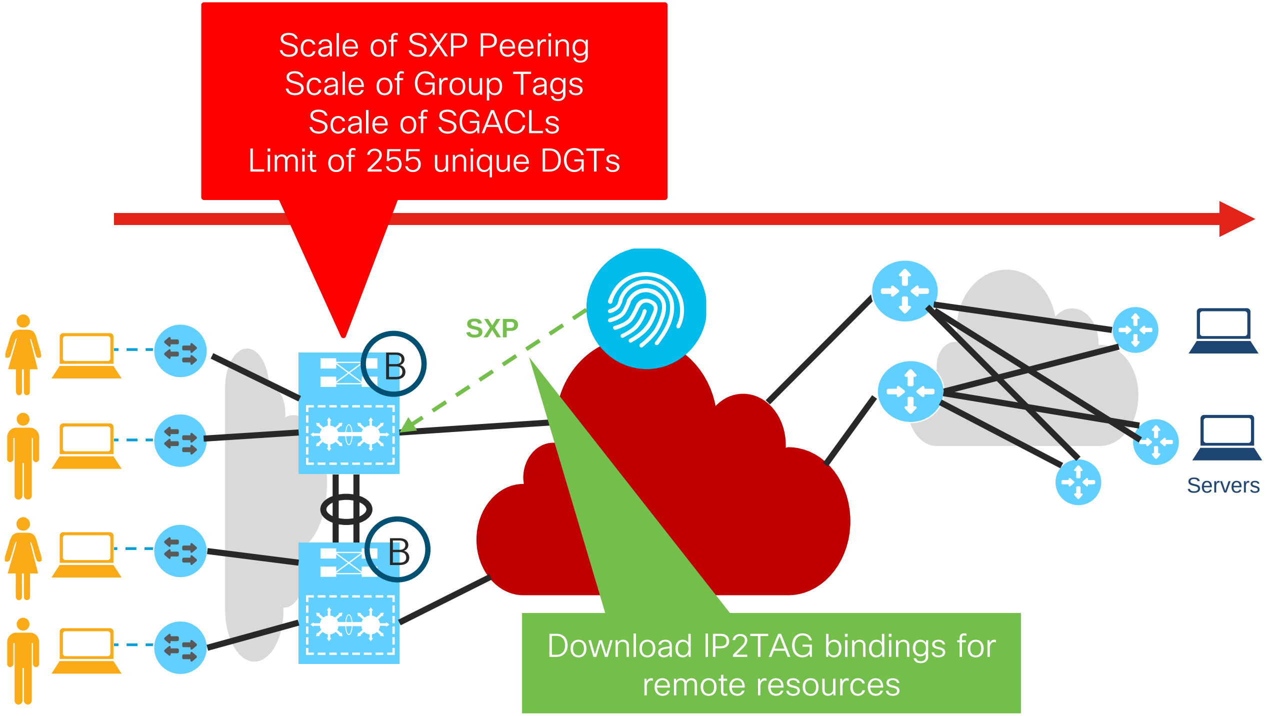


Policy enforced here

Download IP2TAG bindings for remote resources

SD-Access Policy

Enforcement Point Considerations



Scale of SXP Peering
Scale of Group Tags
Scale of SGACLs
Limit of 255 unique DGTs

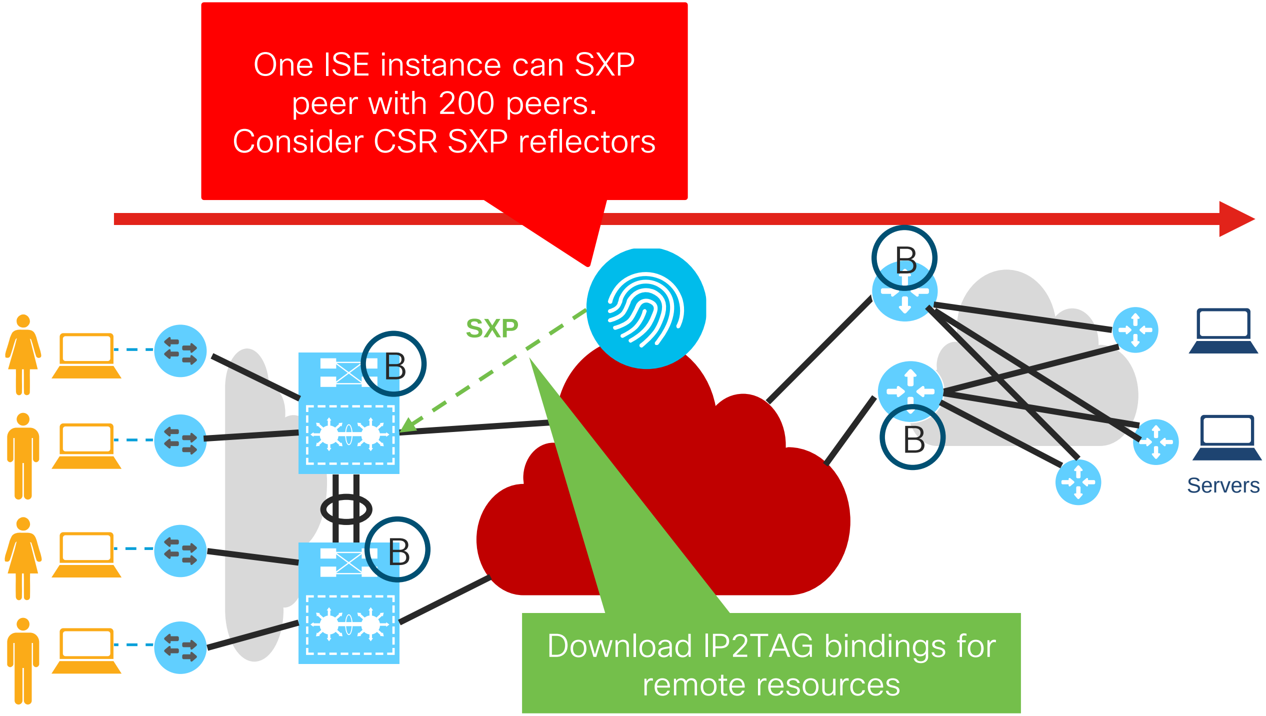
Download IP2TAG bindings for remote resources

SD-Access Policy

Enforcement Point Considerations: ISE Peering Scale

B Policy

3 Policy



One ISE instance can SXP peer with 200 peers. Consider CSR SXP reflectors

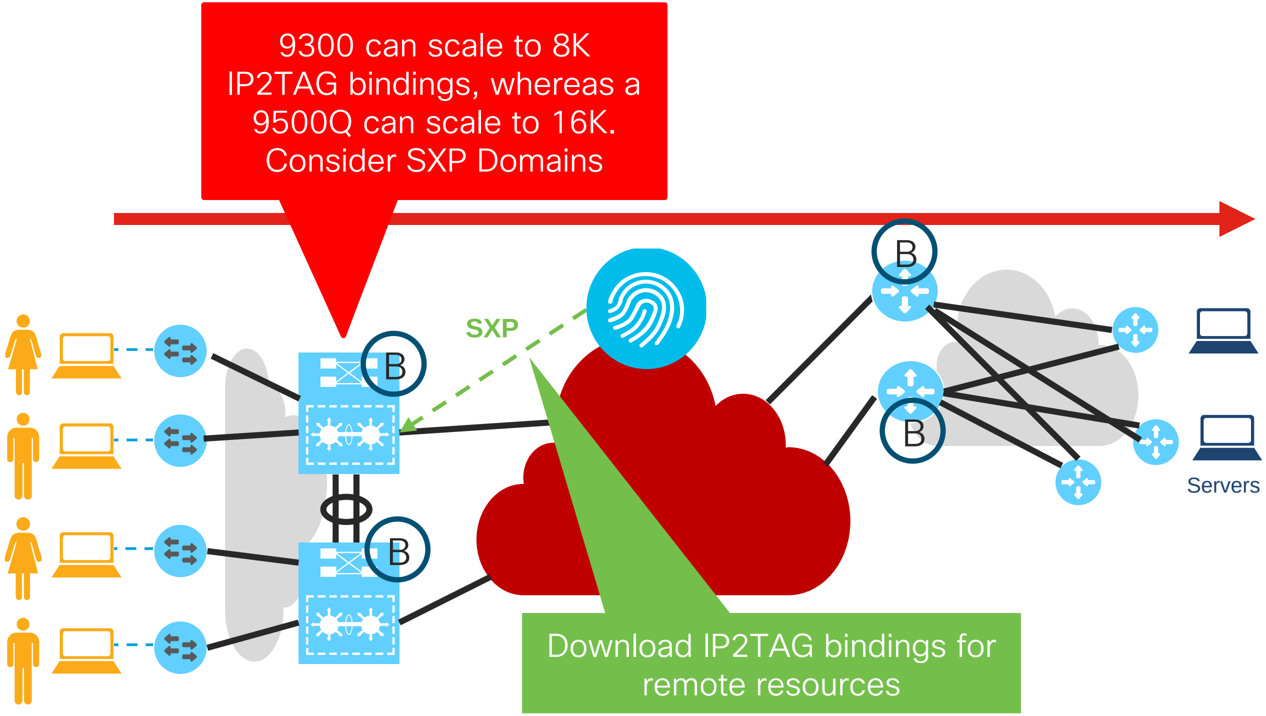
Download IP2TAG bindings for remote resources

SD-Access Policy

Enforcement Point Considerations on a Border – IP2Tag Bindings

B Policy

3 **Policy**



9300 can scale to 8K IP2TAG bindings, whereas a 9500Q can scale to 16K. Consider SXP Domains

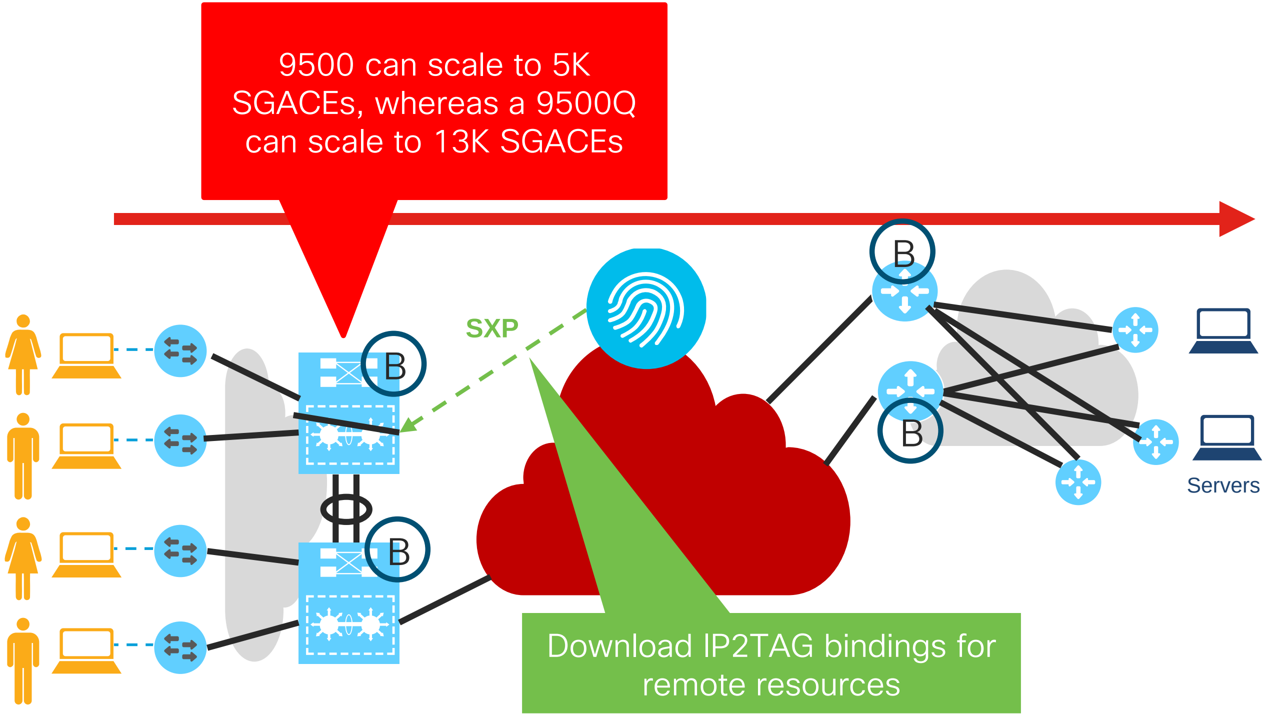
Download IP2TAG bindings for remote resources

SD-Access Policy

Enforcement Point Considerations on a Border - SG-ACE scale

B Policy

3 **Policy**



9500 can scale to 5K SGACEs, whereas a 9500Q can scale to 13K SGACEs

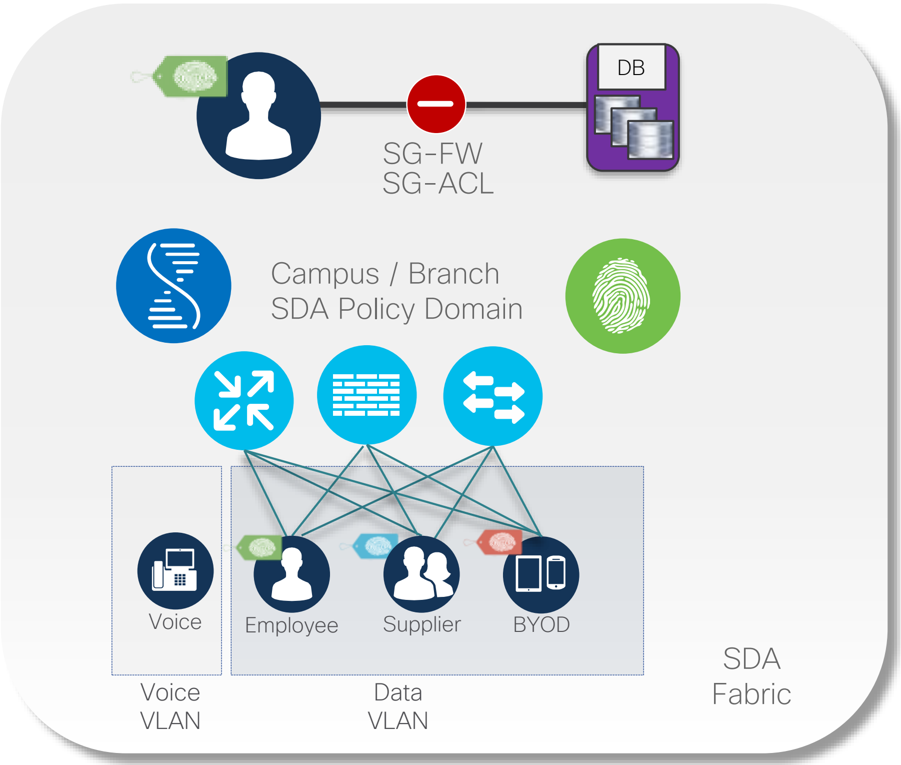
Download IP2TAG bindings for remote resources

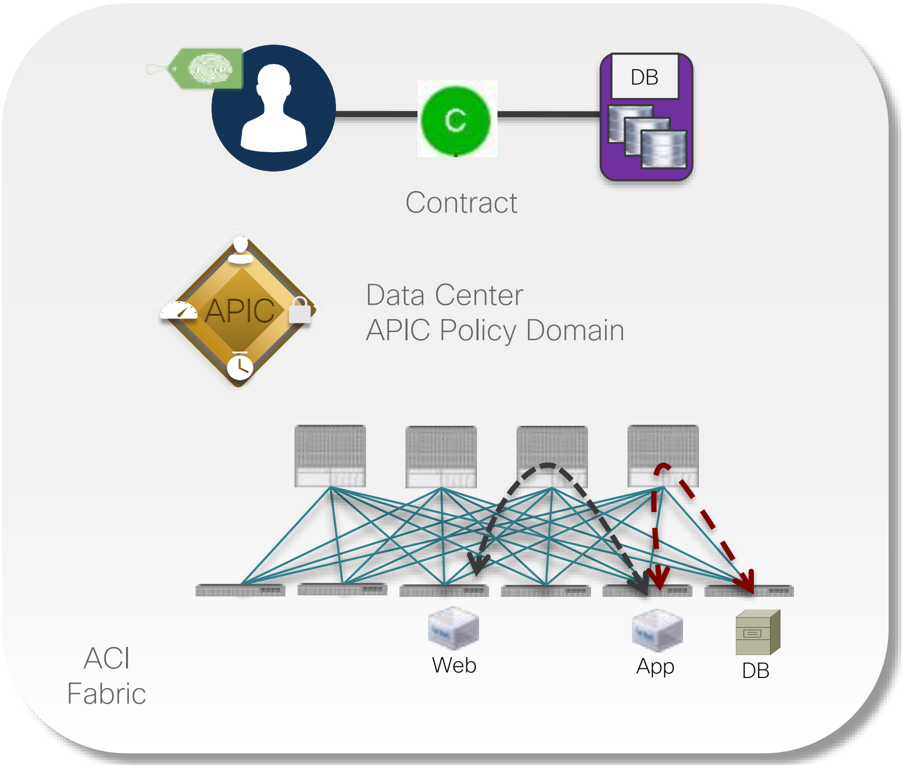
SD-Access Policy

Enabling Group-based Policy in each Domain

B Policy

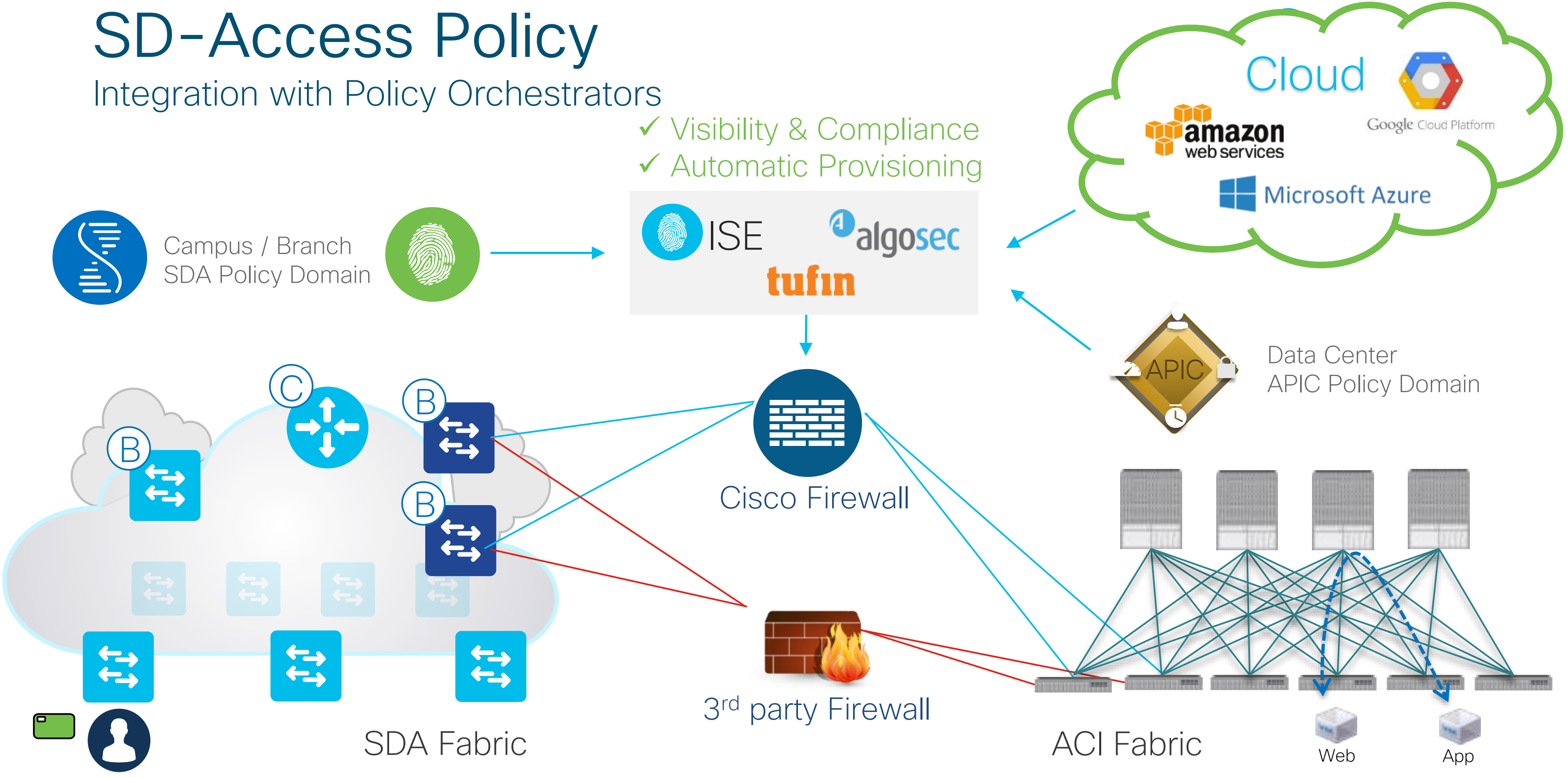
3 **Policy**





SD-Access Policy

Integration with Policy Orchestrators



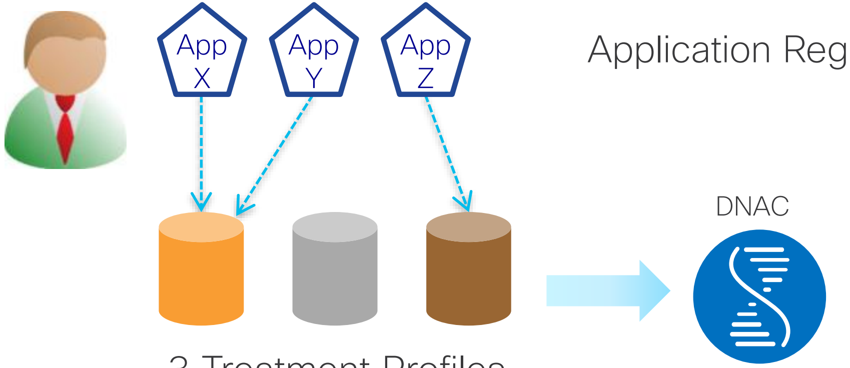
SD-Access Policy

Application Policy = QoS

Application Policy
↓
Traffic Treatment
QoS

Inner DSCP is copied to Fabric (VXLAN) DSCP

Path Optimization
App Compression
App Caching

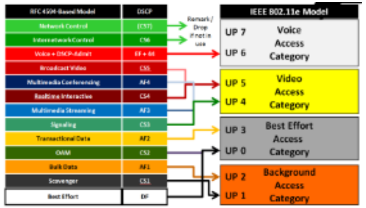


3 Treatment Profiles

Application Registry

Application X
IP-Prefix / URL = X.X.X.X /24
UDP/TCP Ports = 63837-64101

Application Z
IP-Prefix / URL =Z.Z.Z.Z /22
UDP/TCP Ports = 80

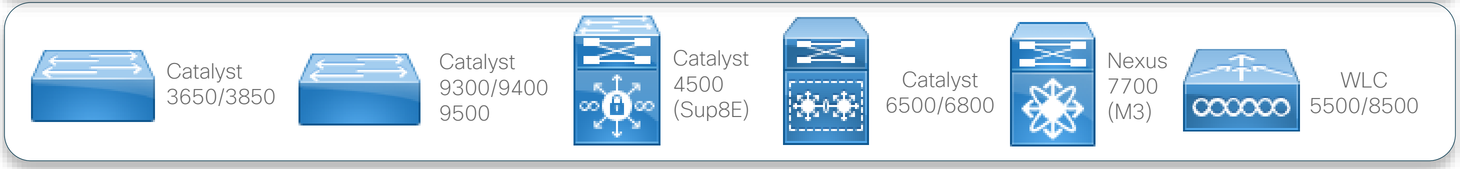


RFC 4594-Based Model	DSCP
Network Control	(CS7)
Internetwork Control	CS6
Voice + DSCP-Admit	EF + 44
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
OAM	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

Remark / Drop if not in use
IEEE 802.11e Model
UP 7 UP 6 Voice Access Category
UP 5 UP 4 Video Access Category
UP 3 UP 0 Best Effort Access Category
UP 2 UP 1 Background Access Category

Normalize QoS Configs

Polaris (3K), IOS-XE (4K), IOS (6K), NX-OS (N7K), AireOS (WLC/AP)

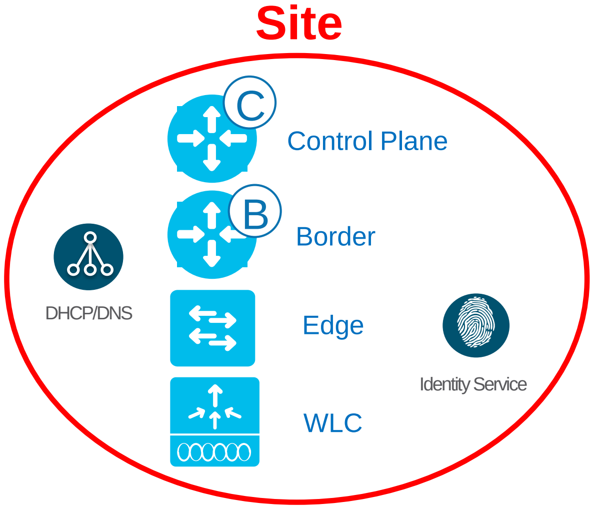


Single vs Multiple Sites

SD-Access for Distributed Campus

Fabric Sites and Domains

- A **Fabric Site** is an independent fabric area with a unique set of network devices: Control Plane, Border, Edge, WLC, and ISE PSN (optional)
- 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 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
- IP Pools (or subnets) are unique to each fabric site

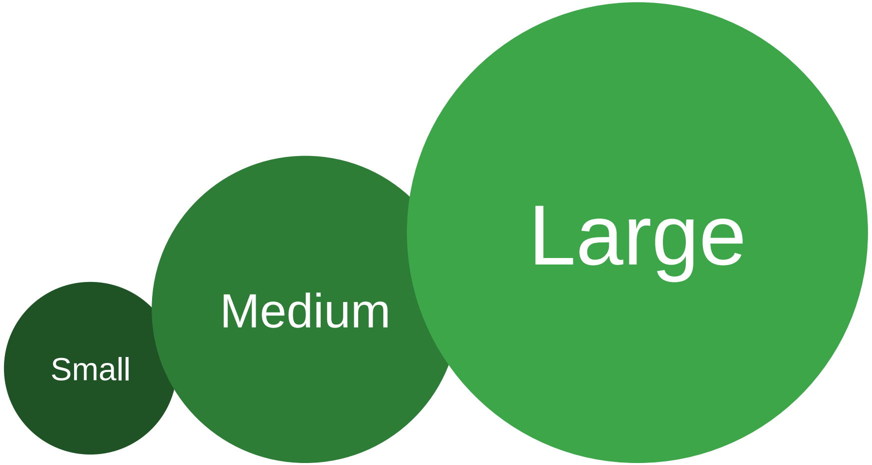


High Level Design - Templates

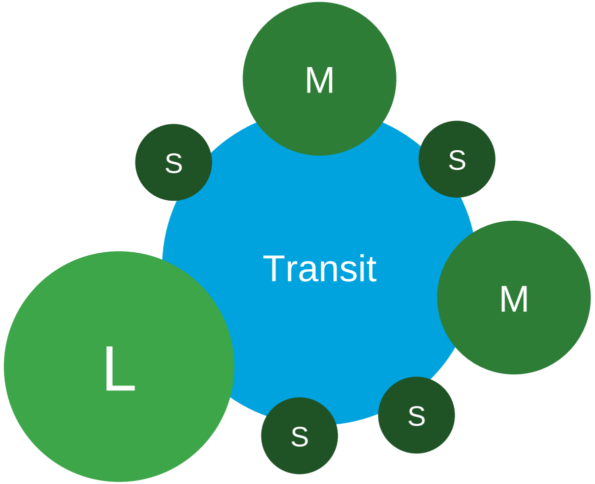
Start from a Cookie Cutter (80%)

RECAP

Basic Goal is for fewer, larger Fabric Sites



Some Needs require split into Multiple Sites



- ✓ Underlay Network (MTU, Latency, etc.)
- ✓ Wireless Client Roaming (< 20ms Latency)
- ✓ Direct Internet Access (@ Remote Sites)
- ✓ Survivable Remote Sites (Local CP/Borders)

C Transit

Connect Multiple Sites Transit Connectivity

Connecting Multiple Fabric Sites

Fabric Sites Transit Types

C Transit

- Multiple Fabric Sites are connected to each other using a **Transit**
- There are three 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
  - **SD-WAN Transit*** - Enables automation of seamless propagation of VRF/SGT from SD-Access to SD-WAN
  - **IP-Based Transit** - Leverages a traditional IP-based (VRF-LITE, BGP,MPLS) network, which requires remapping of VRFs and SGTs between sites

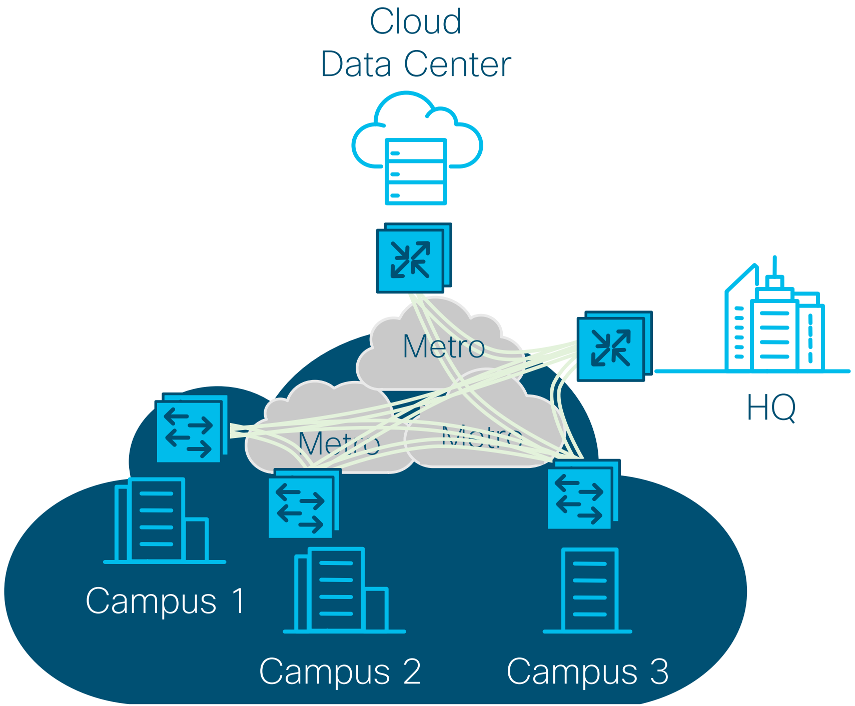
C Transit

Designing for Multi-Site SDA Transit

Transit Connectivity

Why SD-Access Transit?

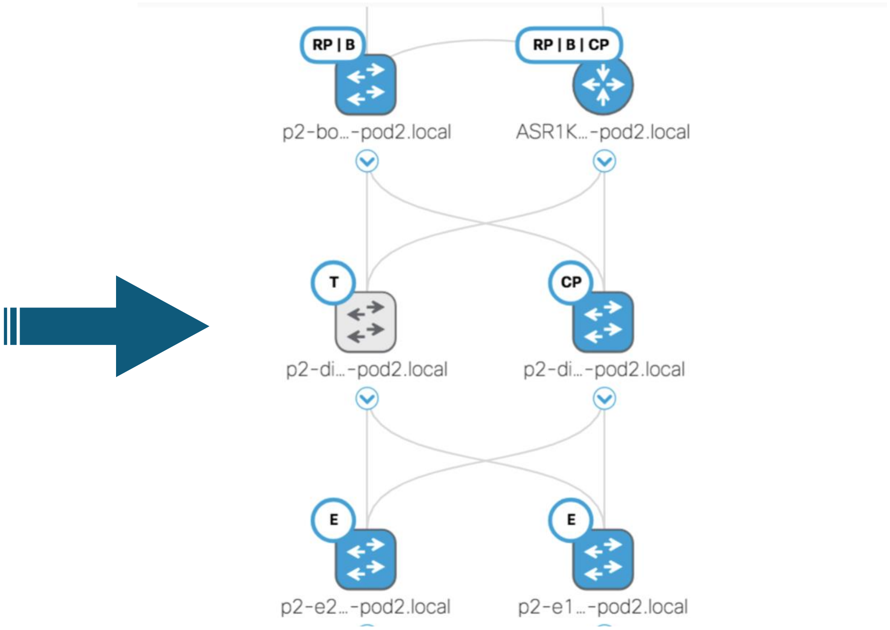
C Transit



- ✓ Fully automated Site-to-Site connection
- ✓ Seamless policy propagation
- ✓ From the policy perspective, all sites behave as one
- ✓ Sites in same Metro Area, Campus, or even Building, or sites across traditional WAN with central IP-Transit

Transit Connectivity

MTU and Transit Control Plane Node

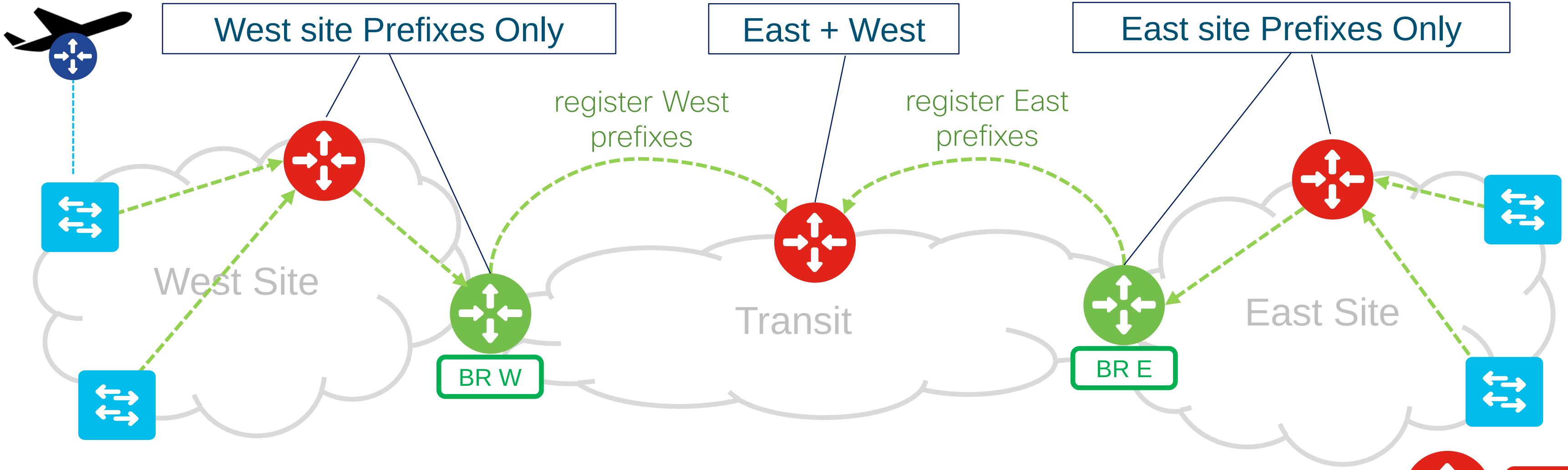


- ✓ Higher than 1500 bytes MTU Support from service provider
- ✓ Needs a separate Transit Control Plane node/s
- ✓ IP reachability from all Site Border node/s
- ✓ Can be in Data center or in another fabric site

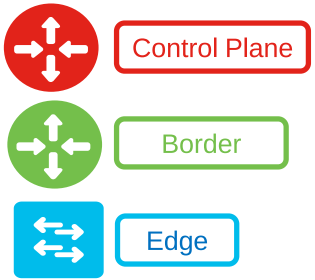
SD-Access Transit

Control Plane Scale Considerations

C Transit



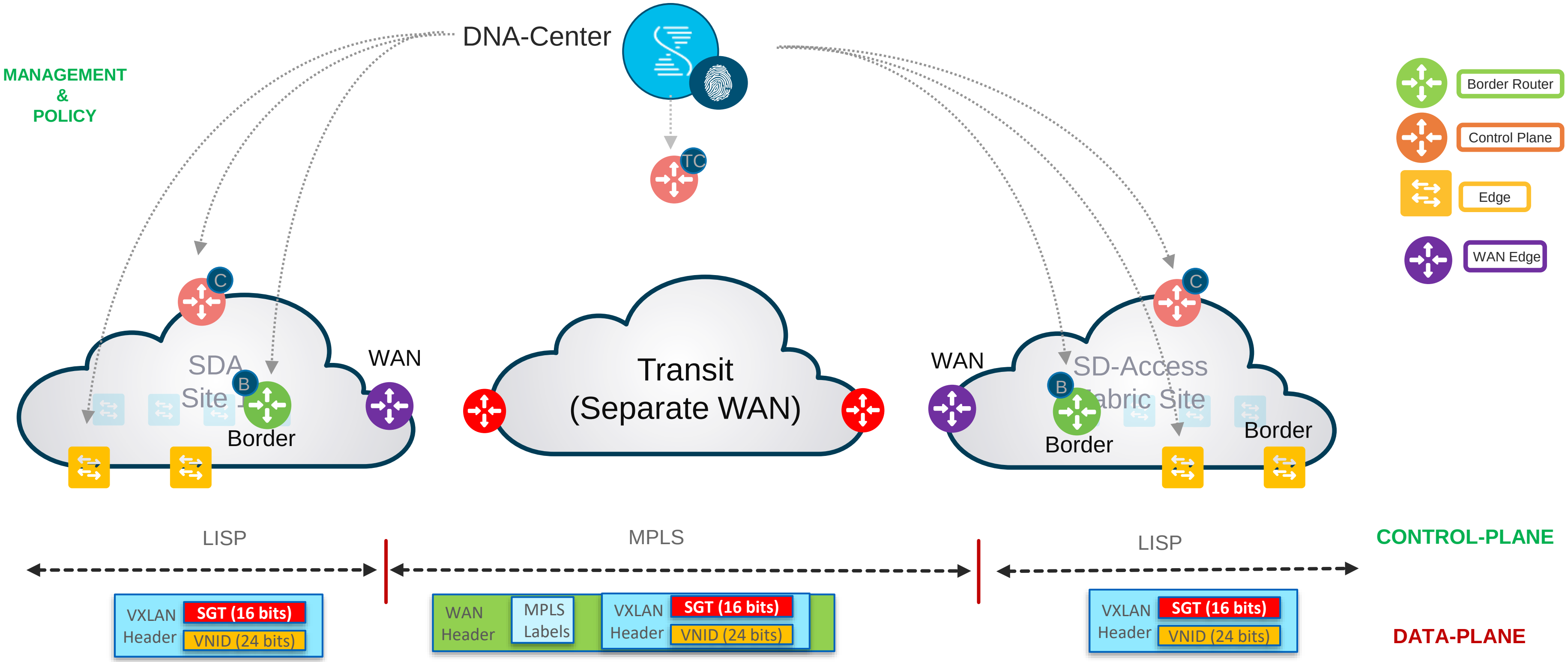
- Border Routers only hold the Soft state for local site prefixes only
- Hard/Forwarding state instantiated on Border Routers strictly on-demand
- Control Plane of the stub sites holds only local host mappings. No remote mappings
- Cross site summary mappings registered in Transit Control Plane



Transit Connectivity

C Transit

Packet Walk in SD-Access Transit – For Site-to-Site connectivity

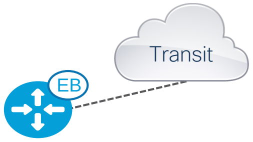


SD-Access for Distributed Campus

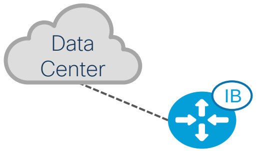
SD-Access + IP Transit (Choosing the Right type of Border)

RECAP

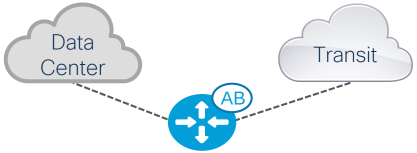
- When to use External (Outside) border?
  - When we want to connect ONLY to the SDA Transit or an IP Transit to unknown subnets (e.g. Internet).



- When to use Internal (Rest of Company) border?
  - When we want to connect ONLY a site to the IP Transit known subnets of the company (like DC, WAN etc.)



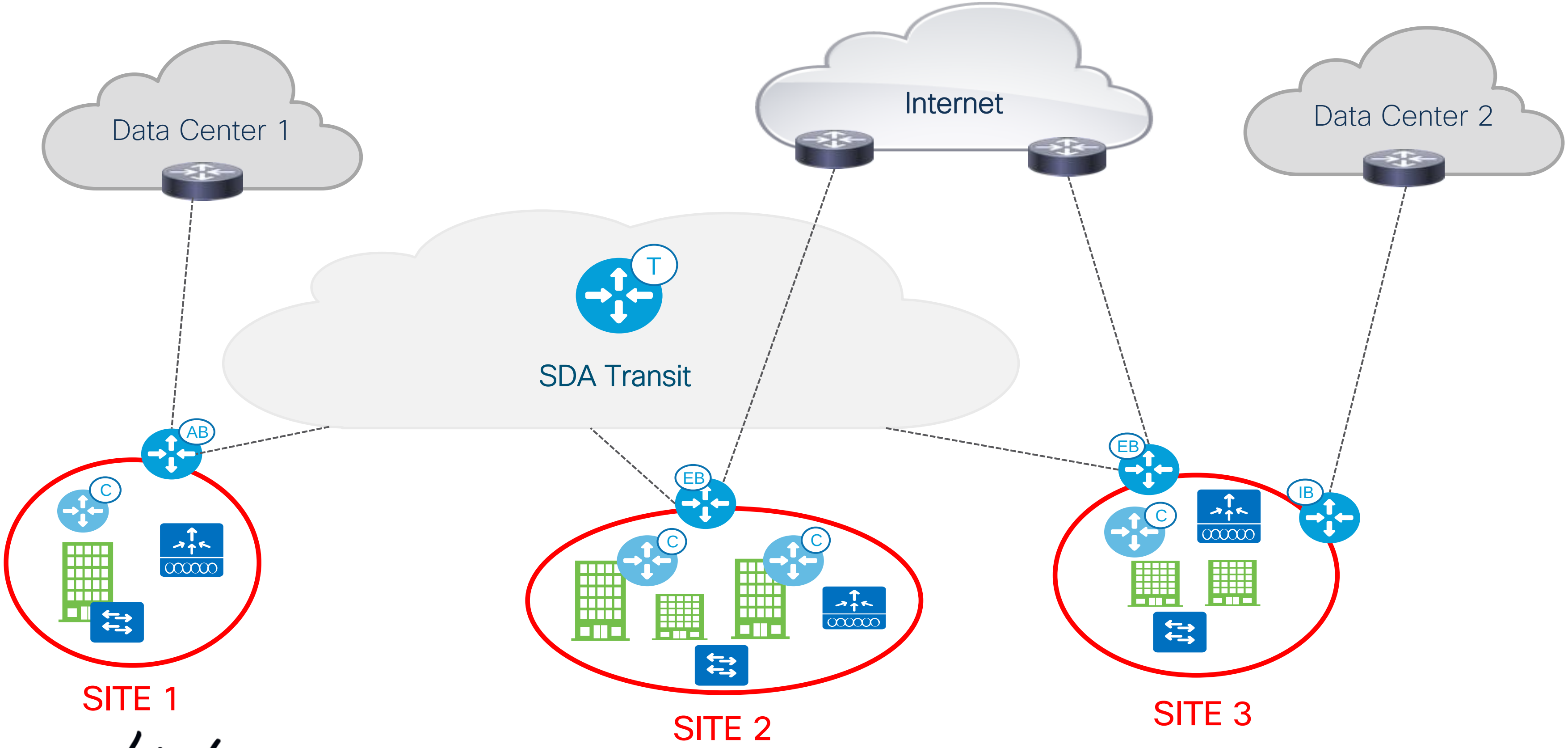
- When to use Internal + External (Anywhere) border?
  - When we want to connect to SDA Transit or IP Transit, AND to known areas like DC, WAN, etc.



SD-Access for Distributed Campus

C Transit

30,000 Foot View



SD-Access Distributed campus

Fabric Border Support Matrix

C Transit

SDA Border Node	SD-Access Transit	IP Transit
C9K	YES	YES
ASR1K/ISR4K	YES	YES
C6K	YES	YES
N7K	NO	YES

SD-Access Distributed campus

Detailed Session on SD-Access Distributed Campus

C Transit

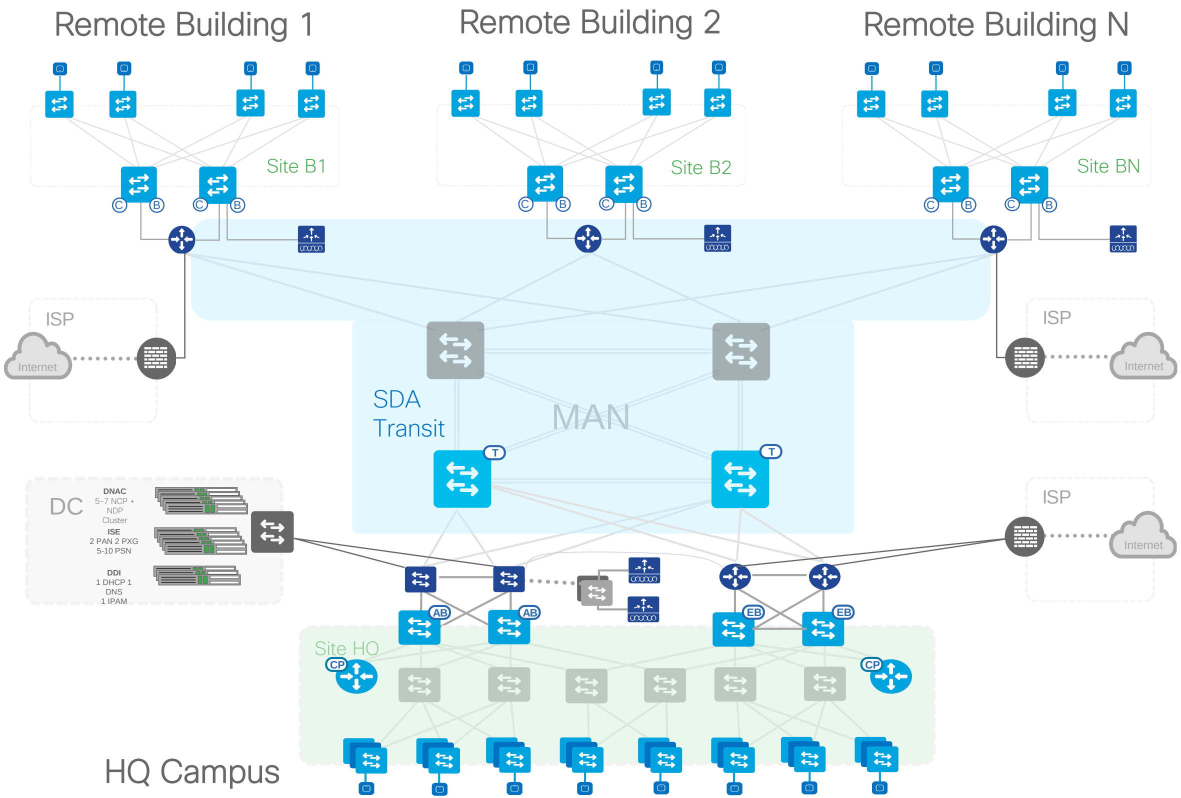
BRKCRS-2815 SD-Access: Connecting Multiple Sites in a Single Fabric Domain

Wednesday 0830

Multi Site – Metro Area

SD-Access Transit

C Transit



Key Decision Points

- Tends to be like a Metro area with multiple buildings or sites
- Requires direct Internet access at multiple sites
- Requires local resiliency and smaller fault domains
- 2 Transit CP
- 2-4 Site Borders (Multiple Exits)
- Looking at > 50,000 dynamic authentications and > 1000 group based policies

C Transit

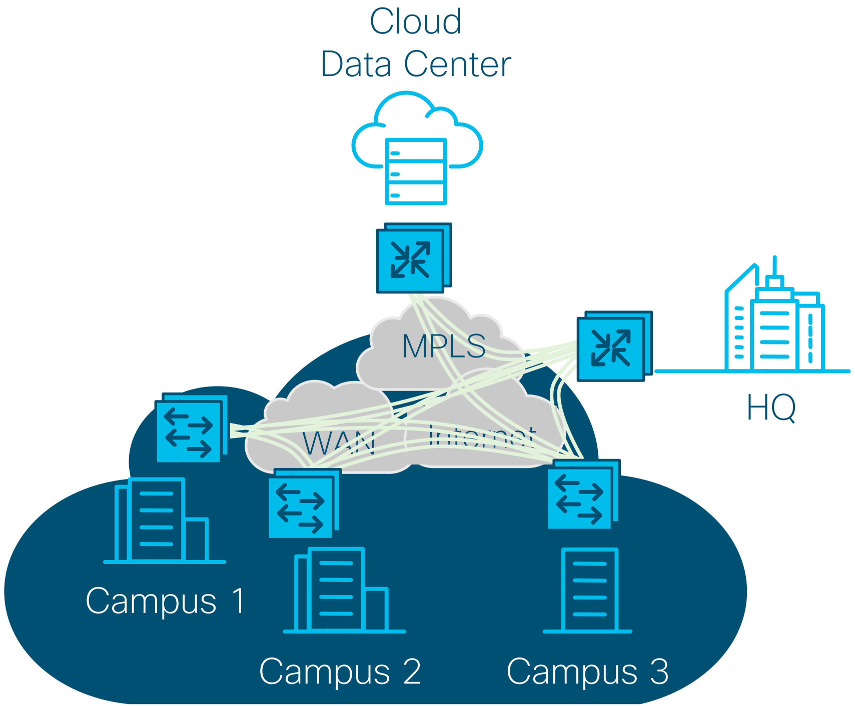
Designing for Multi-Site SD-WAN* Transit

* Q4CY19

Transit Connectivity

C Transit

Why SD-WAN Transit?

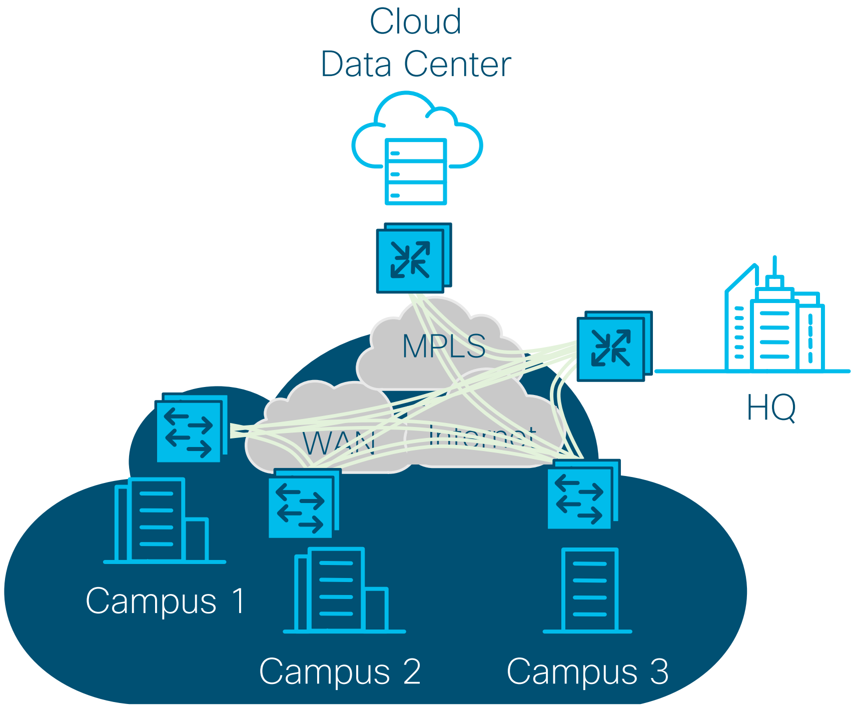


- ✓ Fully automated Site-to-Site SDA-to-SDWAN connections
- ✓ Seamless policy propagation
- ✓ SD-WAN benefits (application routing) for Inter-Site traffic
- ✓ Stitching of existing VPNs in SD-WAN in SD-Access by DNA Center and vManage integration

Transit Connectivity

SD-WAN Transit Considerations

C Transit

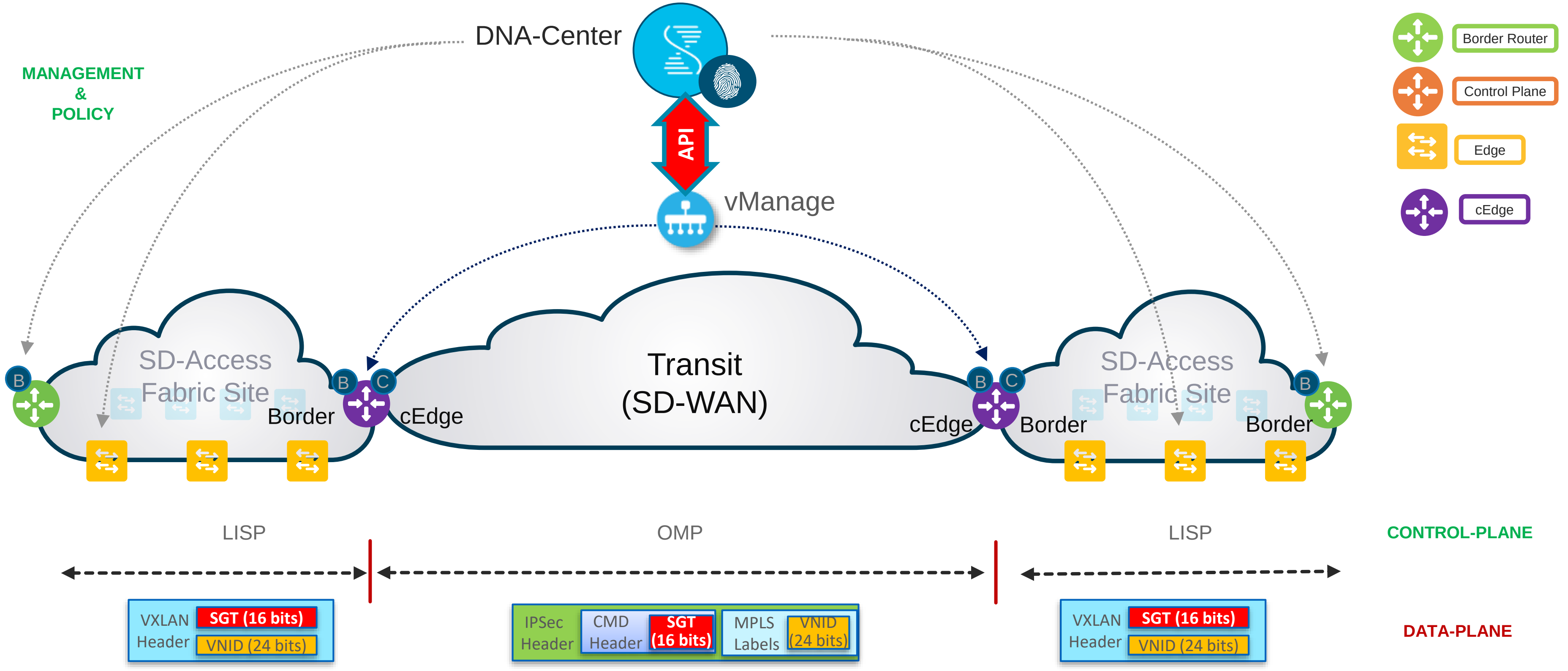


- ✓ One-box solution i.e. SD-Access Border/CP node is cEdge
- ✓ DNA Center integrates with vManage using REST API
- ✓ vManage orchestrates the cEdge for WAN as well as SD-Access (LAN)
- ✓ Configuration of SD-Access supplied by DNA Center
- ✓ Assurance on DNA Center for SD-Access

Transit Connectivity

Packet Walk in SD-WAN Transit

C Transit



SD-Access Distributed campus

Detailed Session on SD-Access Distributed Campus

C Transit

BRKCRS-2818: Build a Software Defined Enterprise with Cisco SD-WAN and Cisco SD-Access

Thursday 0830

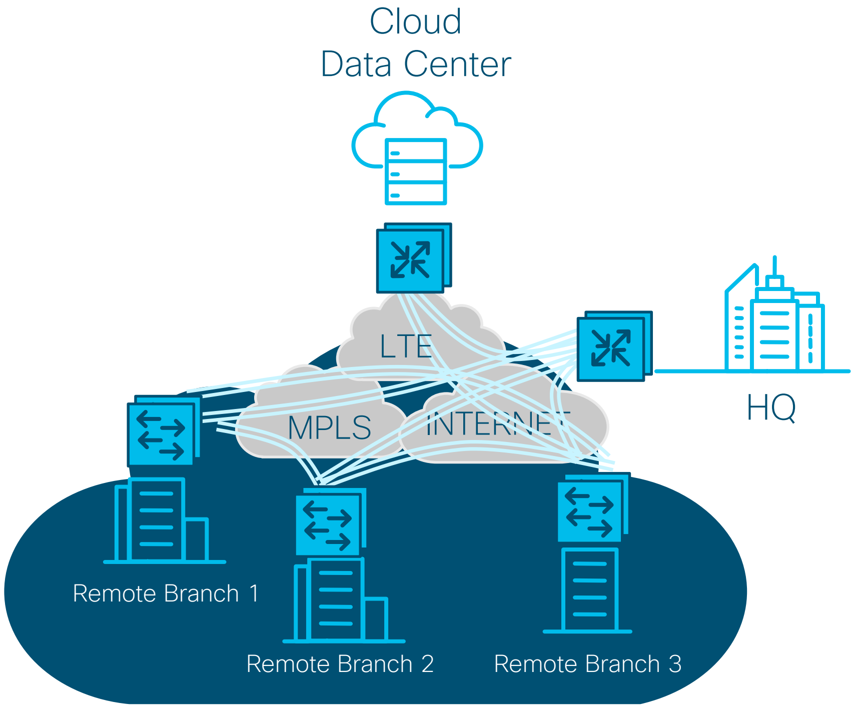
C Transit

Designing for Multi-Site IP Transit

Transit Connectivity

Why IP Based Transit?

C Transit



- ✓ Customers already using existing WAN or have adopted SD-WAN
- ✓ SP cannot support higher MTU
- ✓ Needs no additional nodes
- ✓ Service Insertion

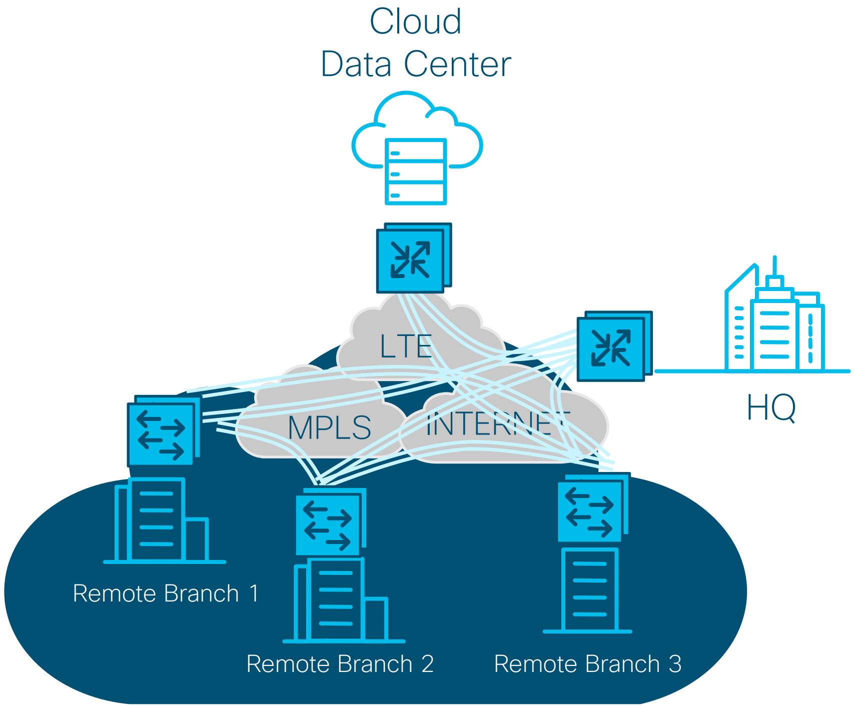
Typical use cases

- Internet Handoff
- P2P IPSEC encryption
- Policy Based Routing
- WAN Accelerators
- Traffic engineering
- Mobile Backhaul LTE

Transit Connectivity

IP Based Transit Considerations

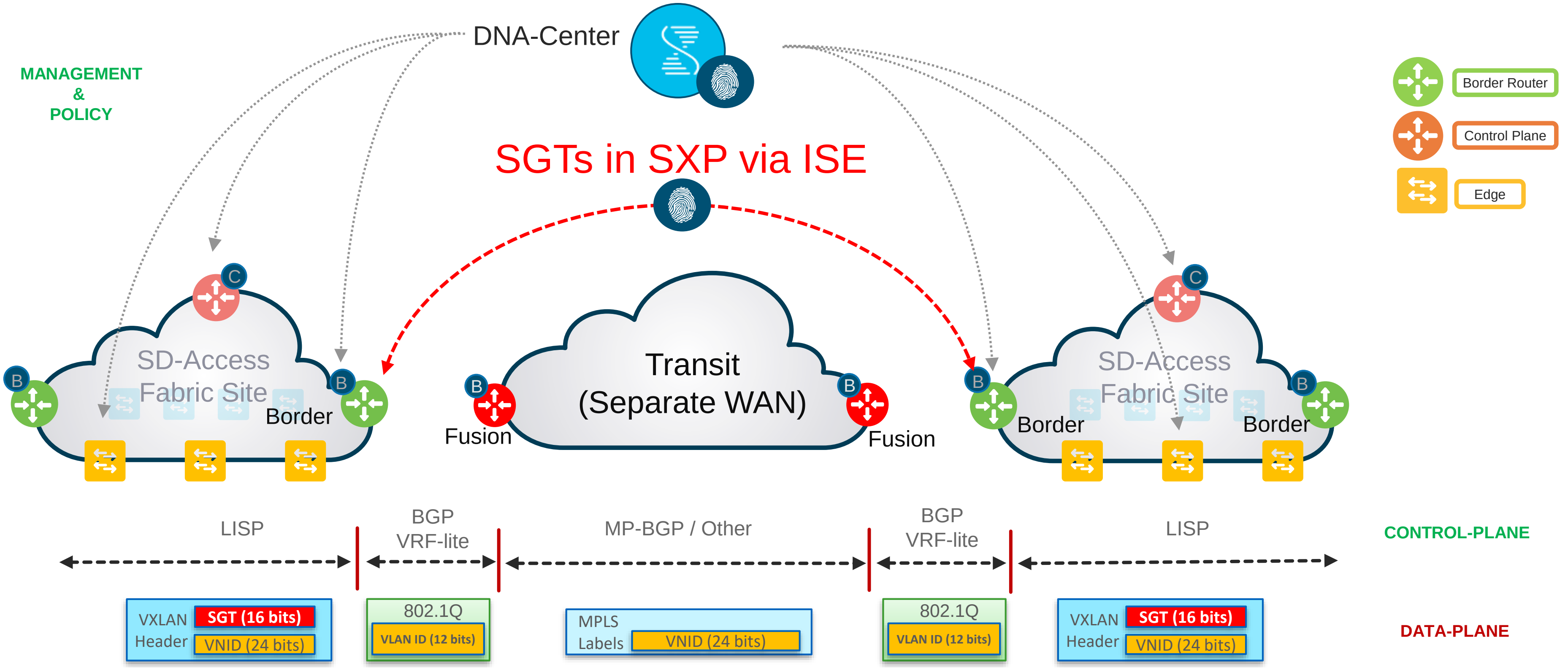
C Transit



- ✓ Manual configuration on the upstream router (fusion) from Site Border
- ✓ If using existing VRFs on Fusion, maintain proper segmentation of SD-Access VRFs and existing VRFs
- ✓ If using Global Routing table (GRT) on fusion, use IP ACLs on fusion to maintain security
- ✓ Avoid causing routing loops

Multiple Site with IP-based WAN Transit

C Transit

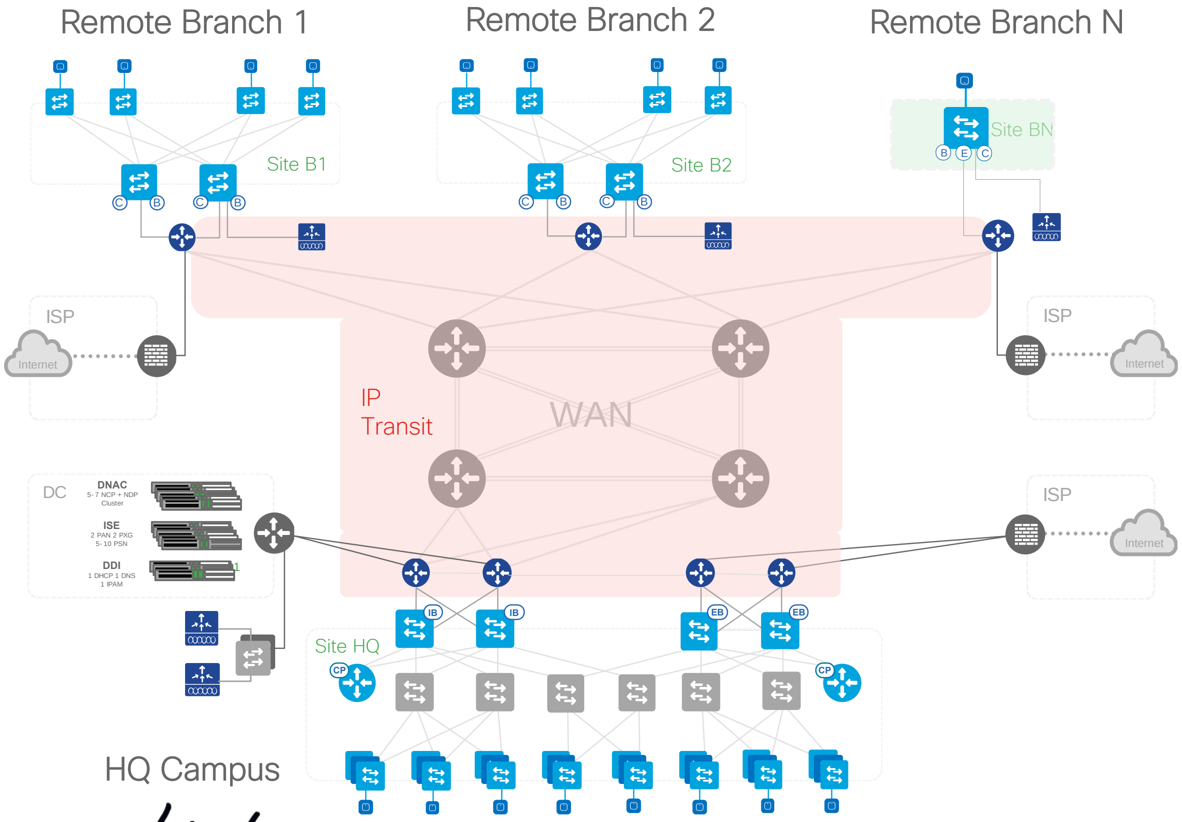


cisco Live!

Multi Site - Wide Area

IP Transit

C Transit



Key Decision Points

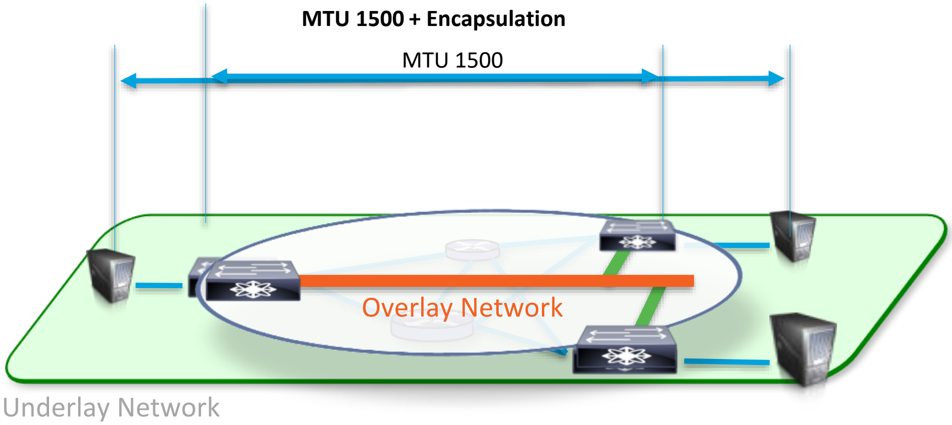
- Tends to be many remote branch offices connected via traditional IP WAN/MPLS or SD-WAN*
- Requires direct Internet access
- Requires site-to-site encryption
- Requires traffic engineering and policy based routing
- 2 Control Plane Nodes
- 2-4 Borders (Multiple Exits)

Migration Considerations

It’s the small things that matter !!!

Existing Network MTU

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



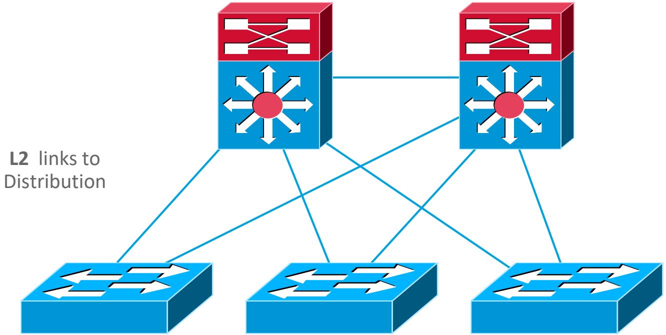
TCP MSS

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

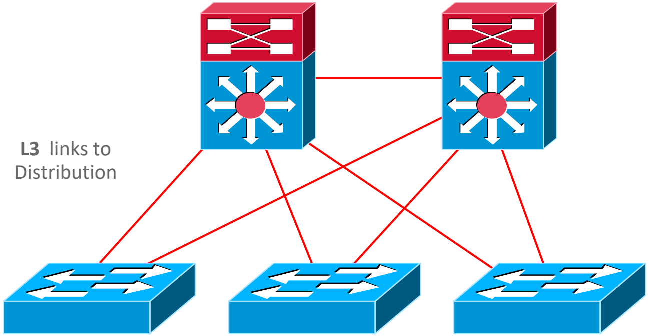
As of now, Jumbo MTU is mandatory on all switches.

Re-configuration of Access Layer

- Layer-2 **Switched Access** today



- **Routed Access** tomorrow



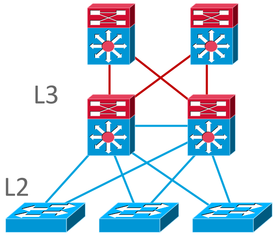
Physical Network Topology

Cisco SD-Access fabric runs over most topologies:

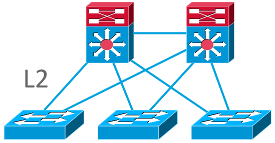
- Traditional 3-tier hierarchical network
- Collapsed core/aggregation
- Routed access
- U-topology

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

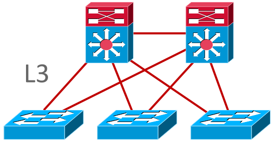
follow campus CVDs with routed access:
www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html



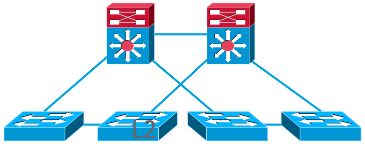
3-Tier Hierarchical



Collapsed Core



Routed Access

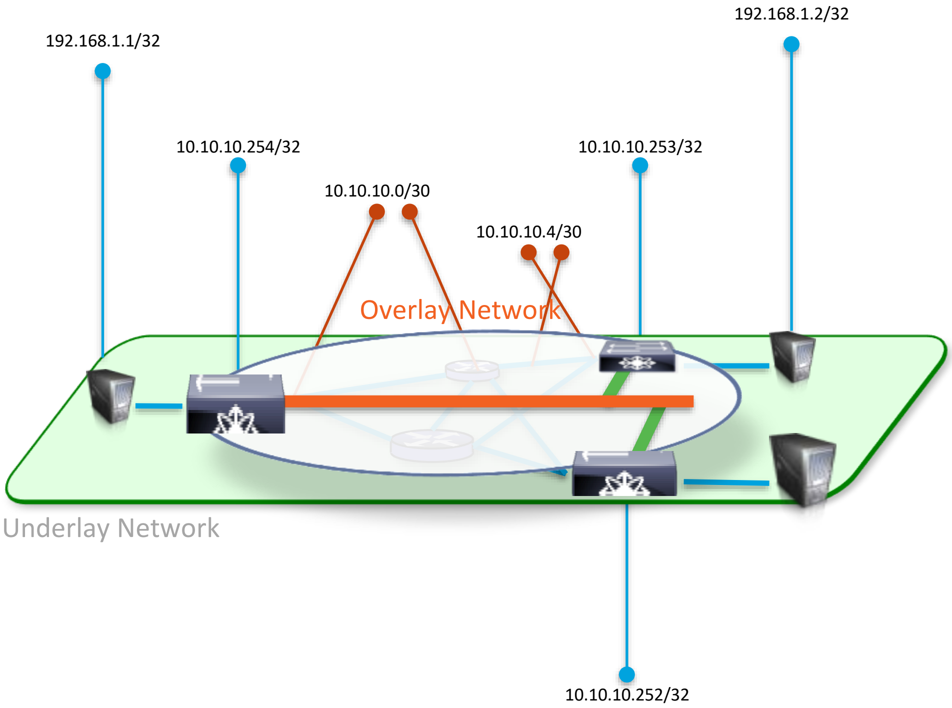


U-Topology

IP Addressing for Underlay and Overlay

Know your IP addressing and IP scale requirements

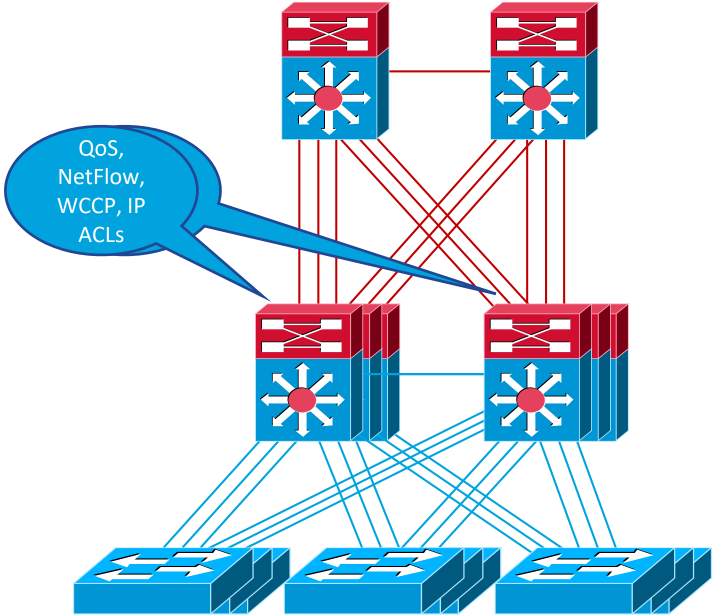
- **IPv4 only** (today)
- Fabric uses Loopback 0 as Source-Interface for Encapsulation
- Best to use single Aggregate for all Underlay Links and Loopbacks



Features enabled today

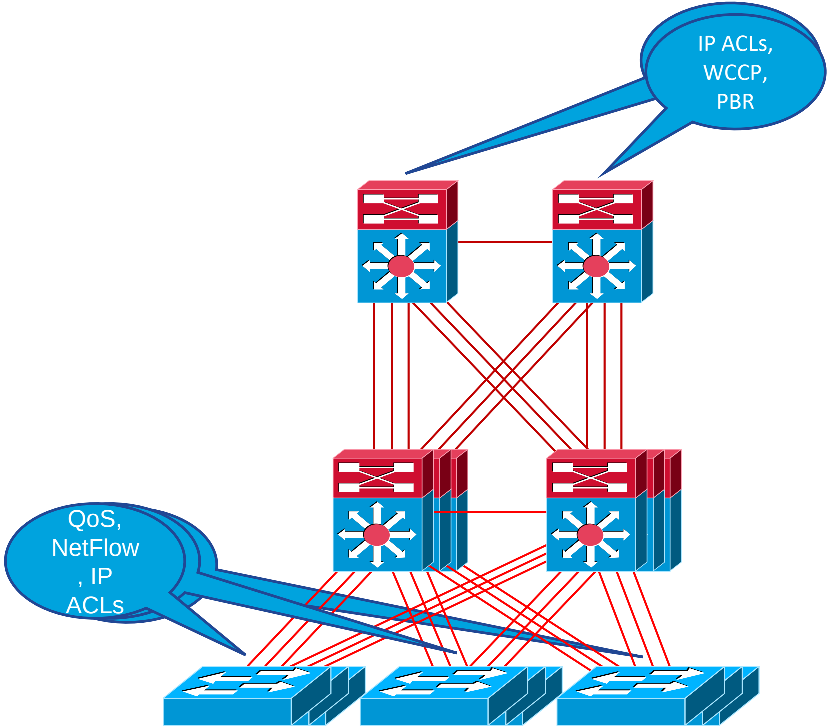
Where are policies applied today?

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



Move to different points in the fabric network

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

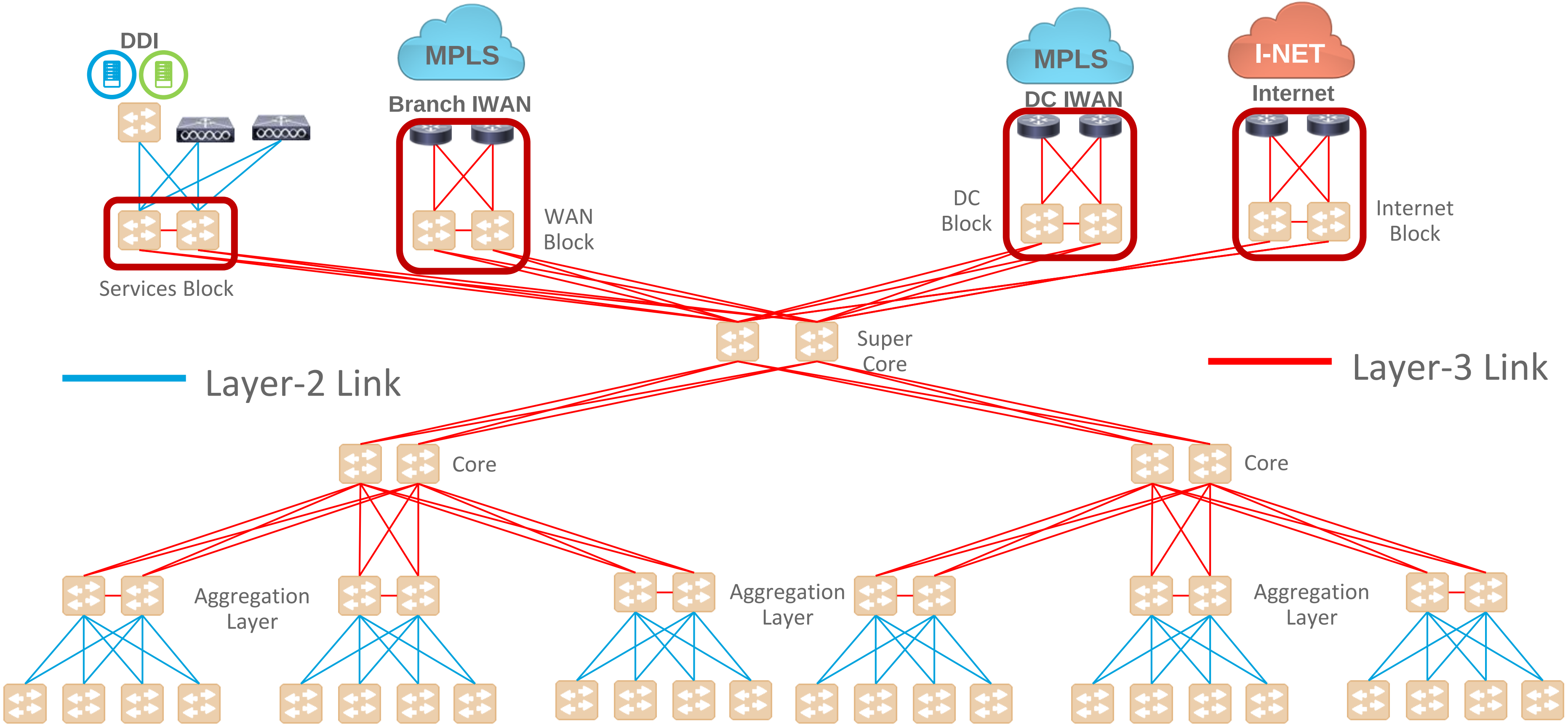


Two Basic Types of Deployments

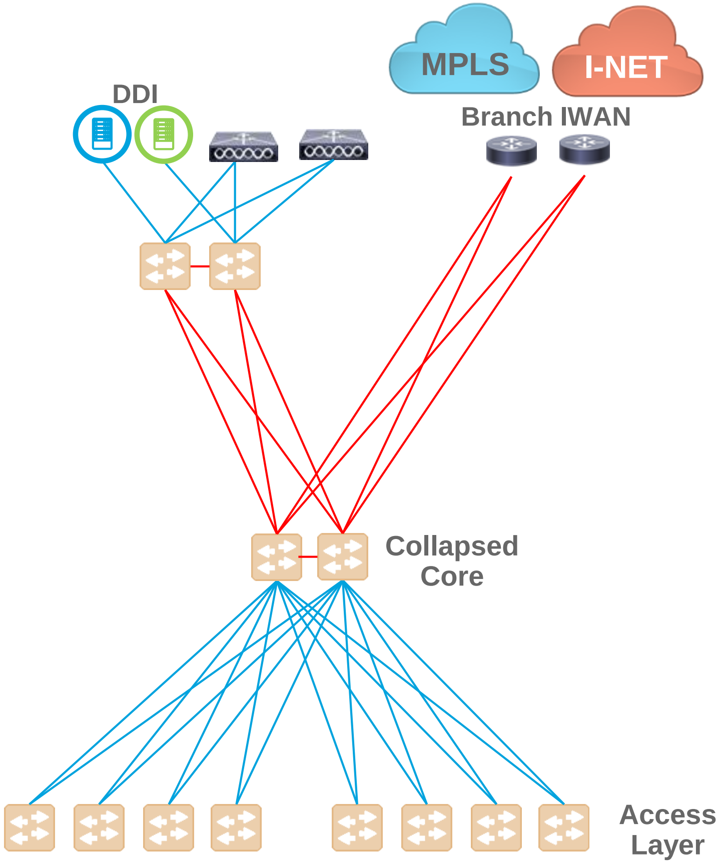
- Campus Networks/(Large Sites)

- Branch Networks/(Small Sites)

Typical Campus Networks



Typical Branch Networks



Two Basic Approaches to Migration

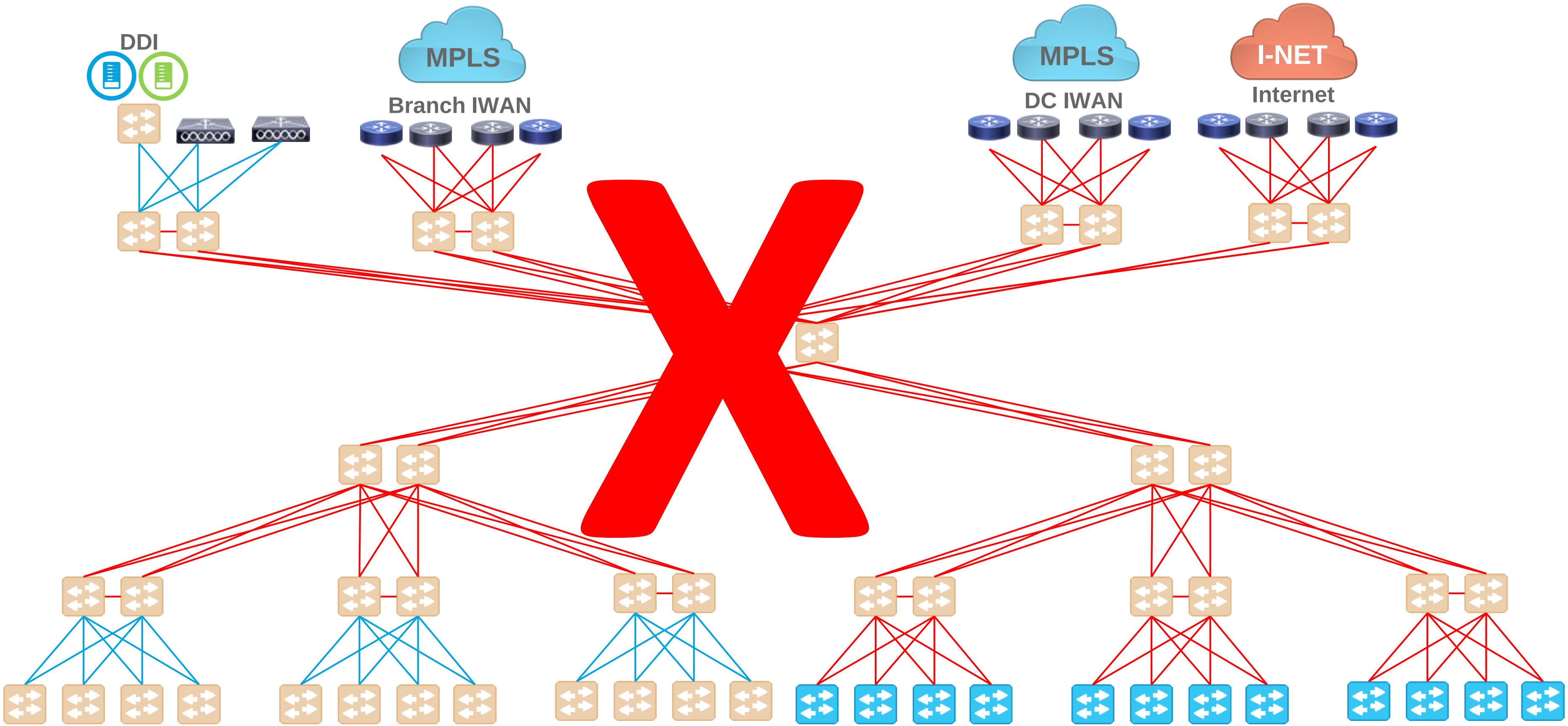
- Parallel Deployment (all at once)

- Incremental Deployment (one at a time)

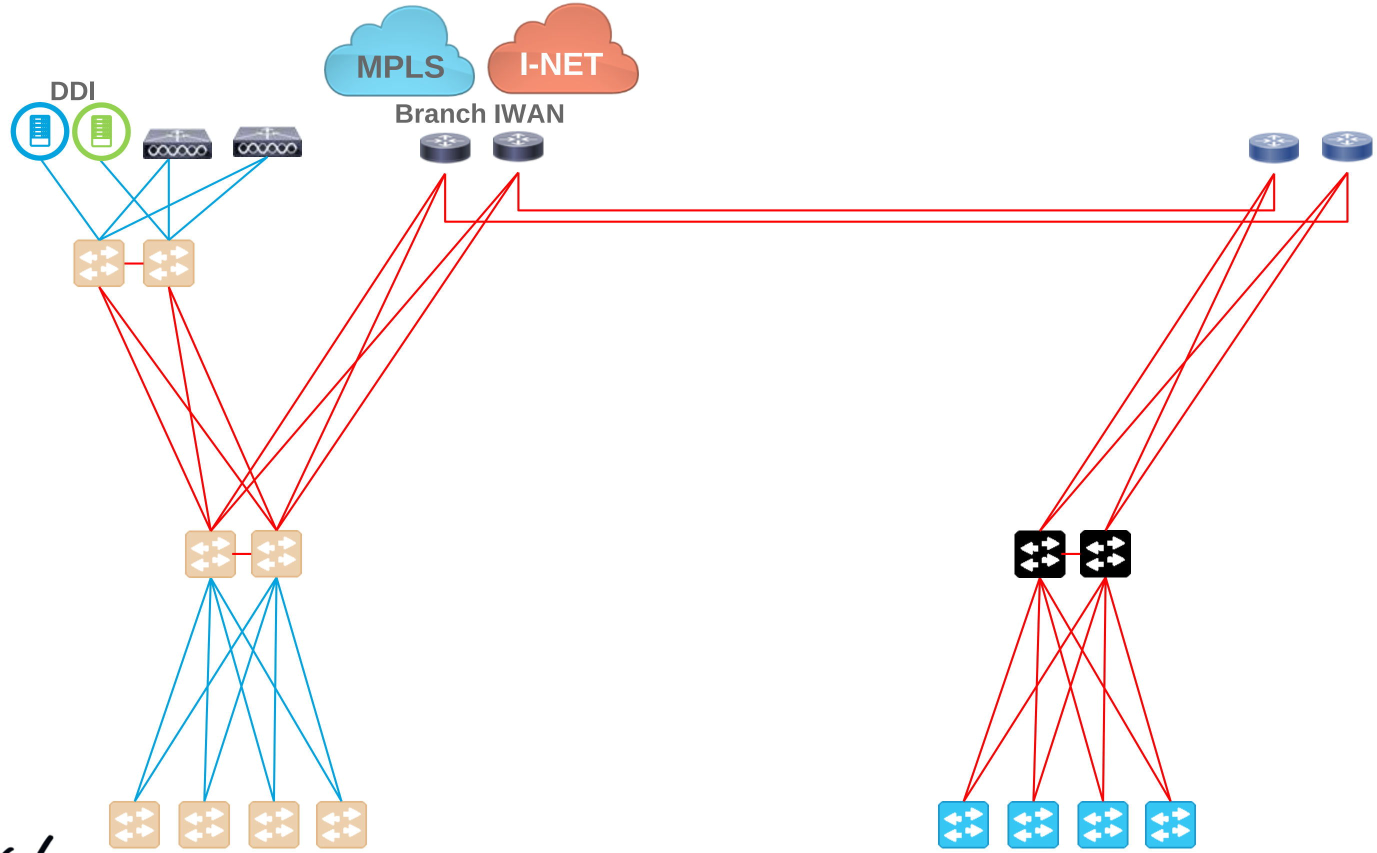
Migration Approaches: Parallel vs Incremental

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

Parallel Install may not feasible for Campus Networks



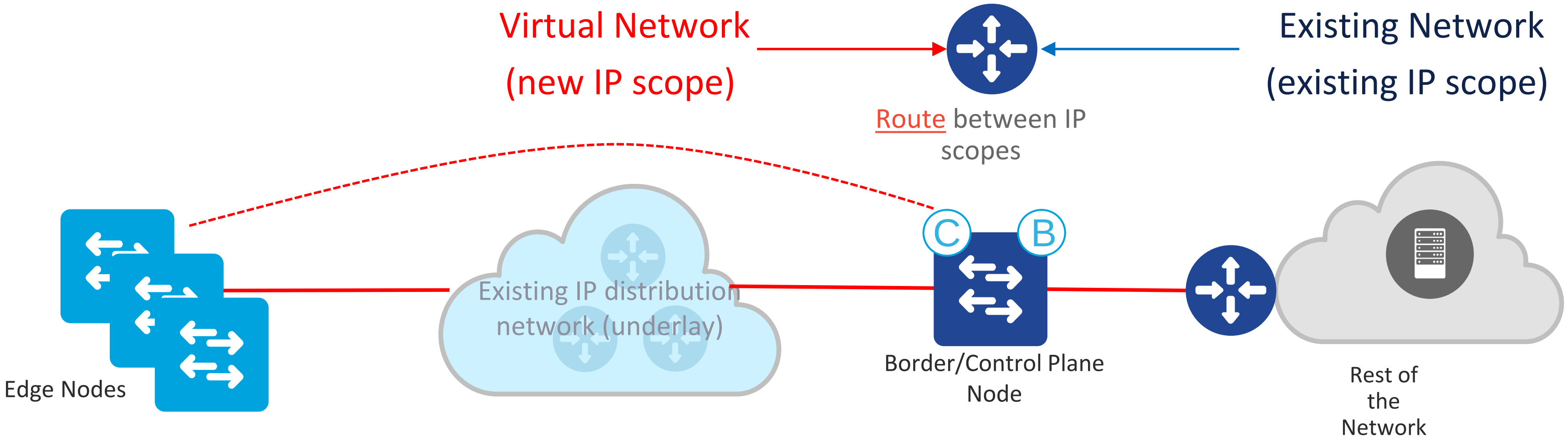
Parallel Install for Branch Networks



SD-Access Migration

Using New Subnets & Switches

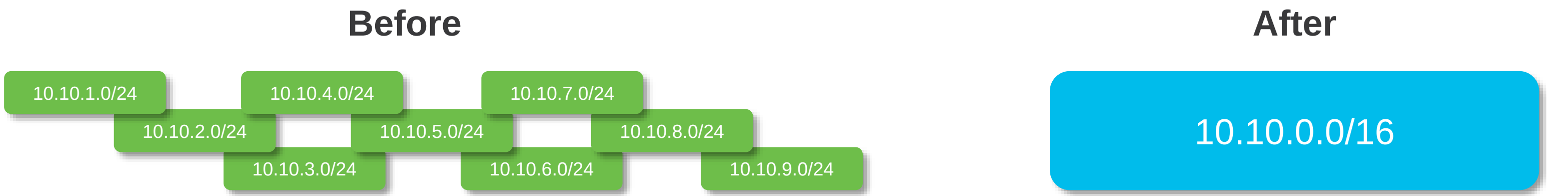
Incremental Migration – High Level concept



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

Considerations for using new subnets to transition

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



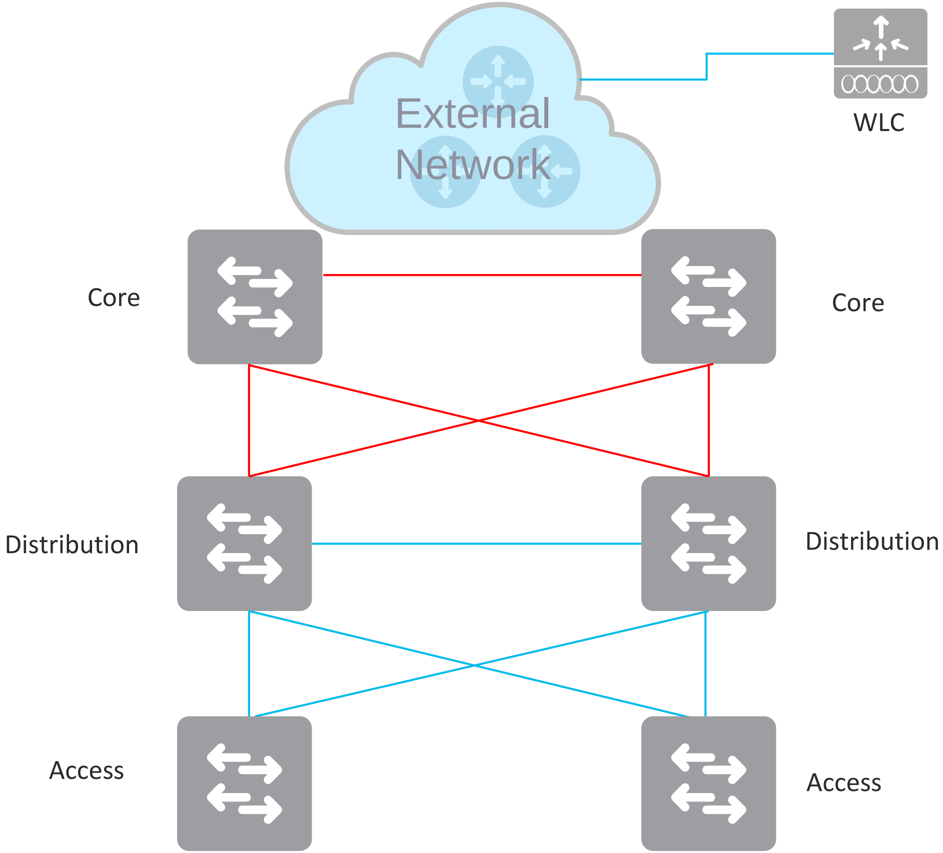
Before

10.10.1.0/24
10.10.2.0/24
10.10.3.0/24
10.10.4.0/24
10.10.5.0/24
10.10.6.0/24
10.10.7.0/24
10.10.8.0/24
10.10.9.0/24

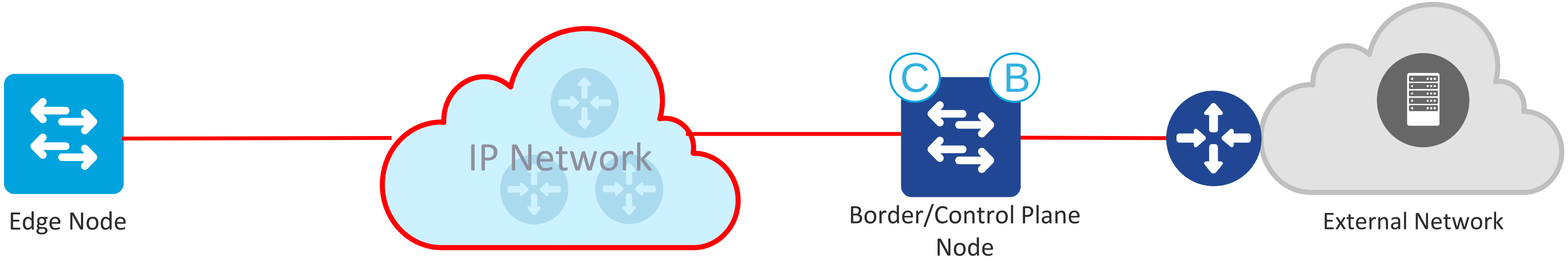
After

10.10.0.0/16

Reference Network Topology to begin Migration



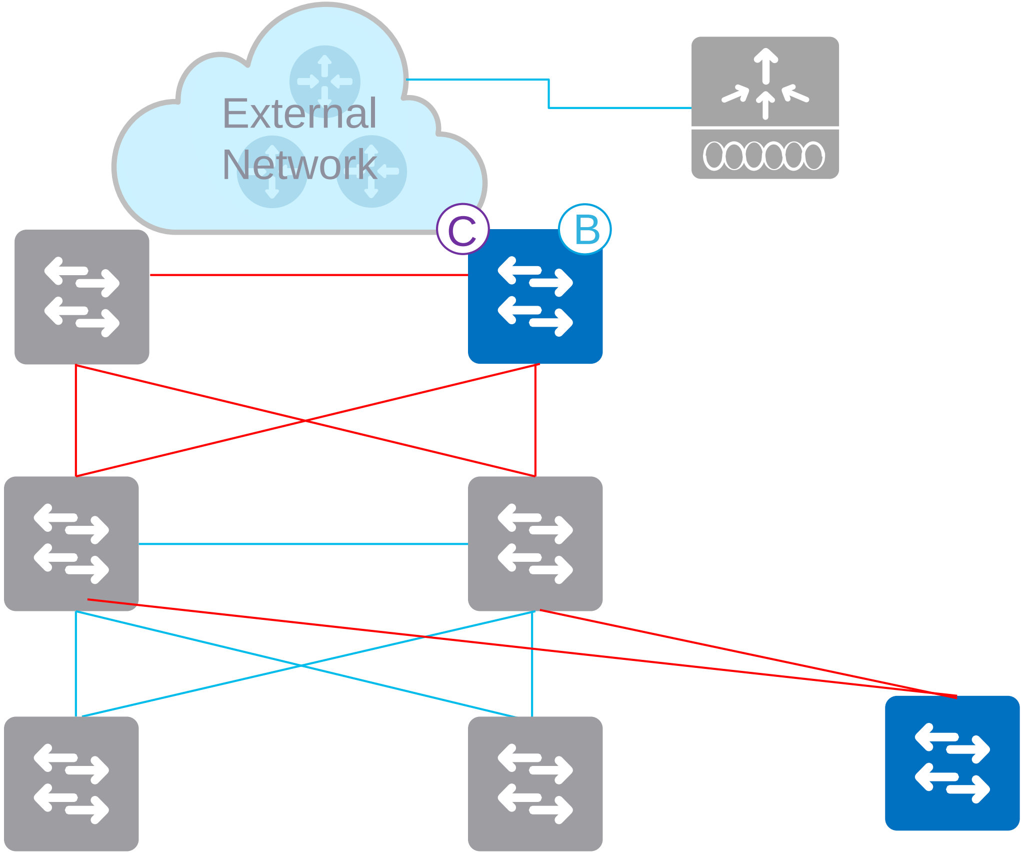
Getting Started



- Configure one Core that will act as the Default Fabric Border
- Host the Control Plane on the Default Fabric Border for simplicity
- Add a switch in the access layer that will act as the Fabric Edge

Insert Fabric Edge in Access

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

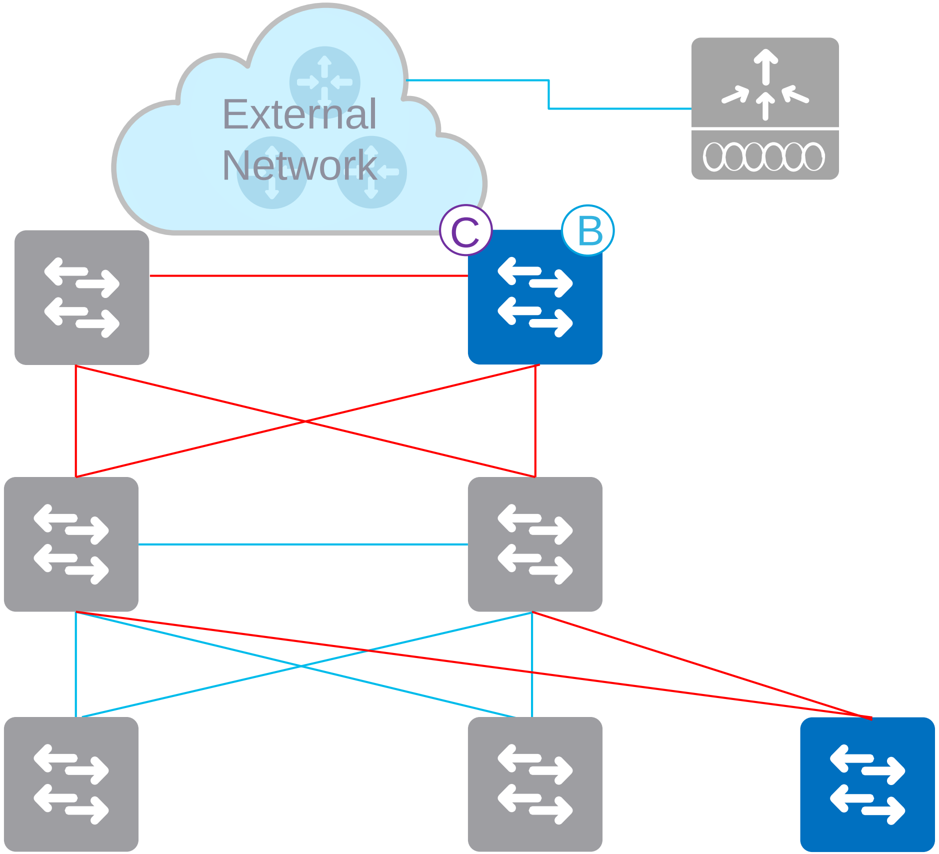


Connecting Default Fabric Border

- Option 1: Reconfigure Existing Core

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

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

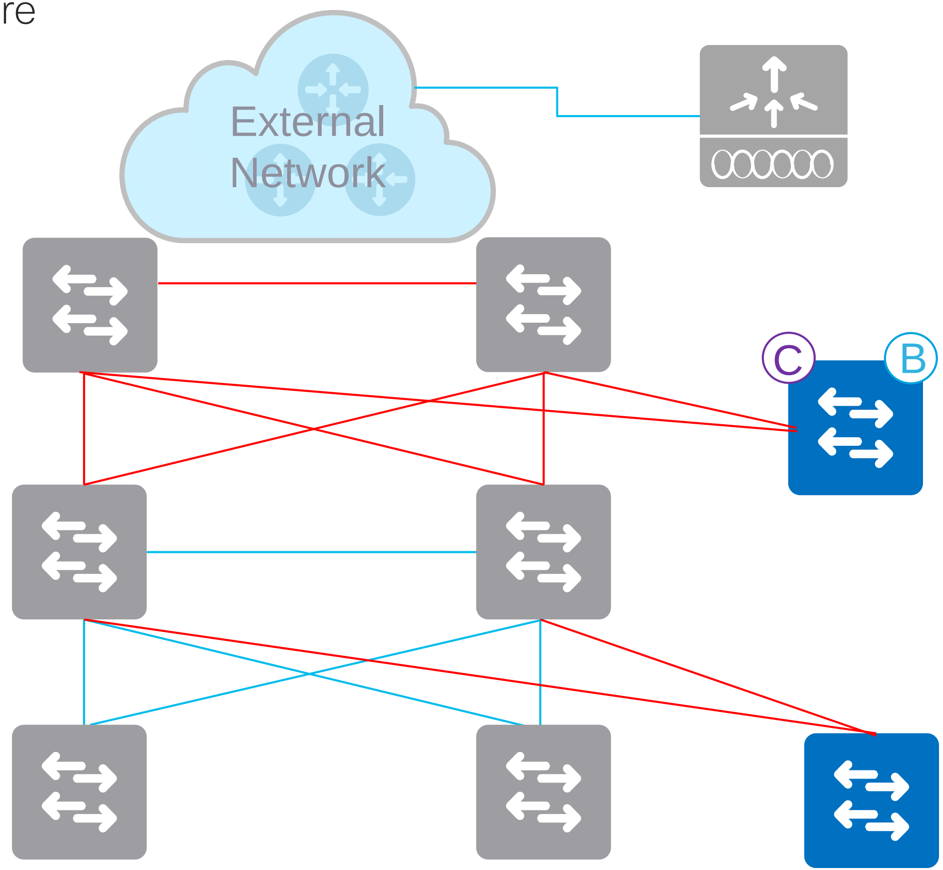


Connecting Default Border

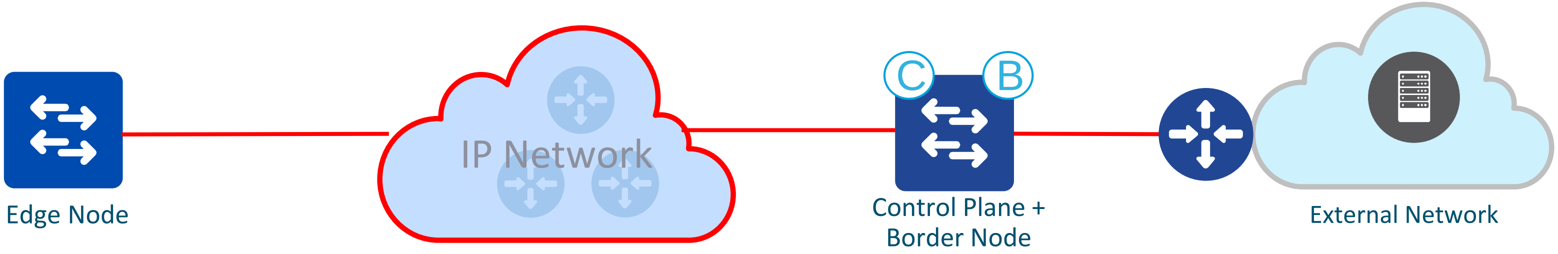
- **Option 2**: Connect new switch to the existing core

If the existing core does not support Fabric functionality,

Connect a new switch to the existing core layer that will be a B/CP



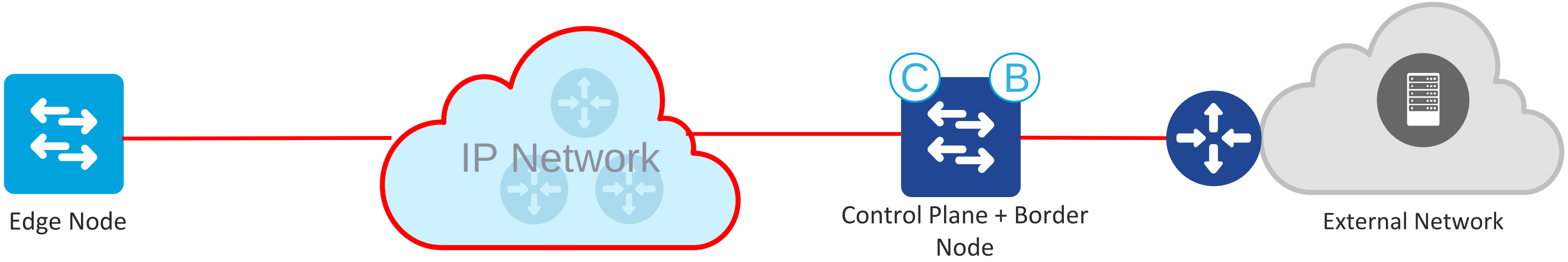
Prepping the Switch



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

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

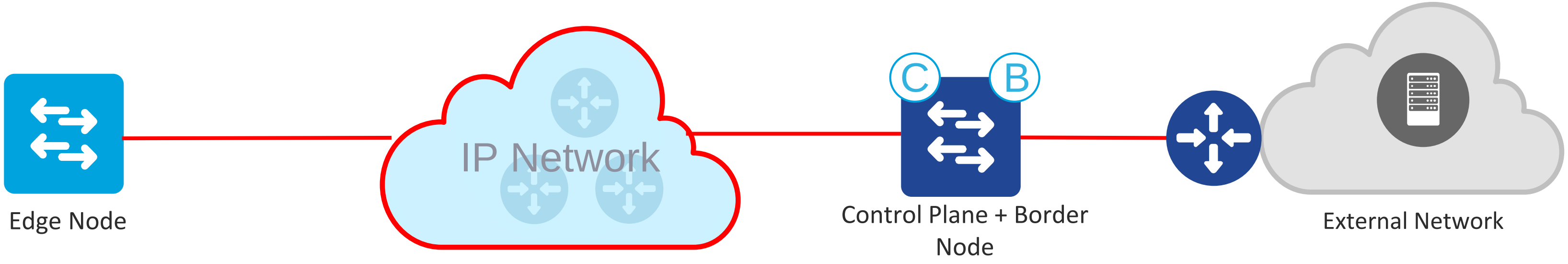
Getting Started Steps – ISIS as an IGP



```
router isis
 passive-interface Loopback0
 net 49.0001.XXXX.XXXX.XXXX.00
 is-type level-2-only
 ispf level-2
 log-adjacency-changes
 metric-style wide level-2
 no hello padding
 authentication mode md5 level-2
 authentication key-chain ON
```

```
interface GigabitEthernet x/x
 ip router isis
 isis network point-to-point
 isis metric <metric> level-2
 isis circuit-type level-2-only
 isis authentication mode md5 level-2
 isis authentication key-chain ON
 carrier-delay ms 0
 dampening
```

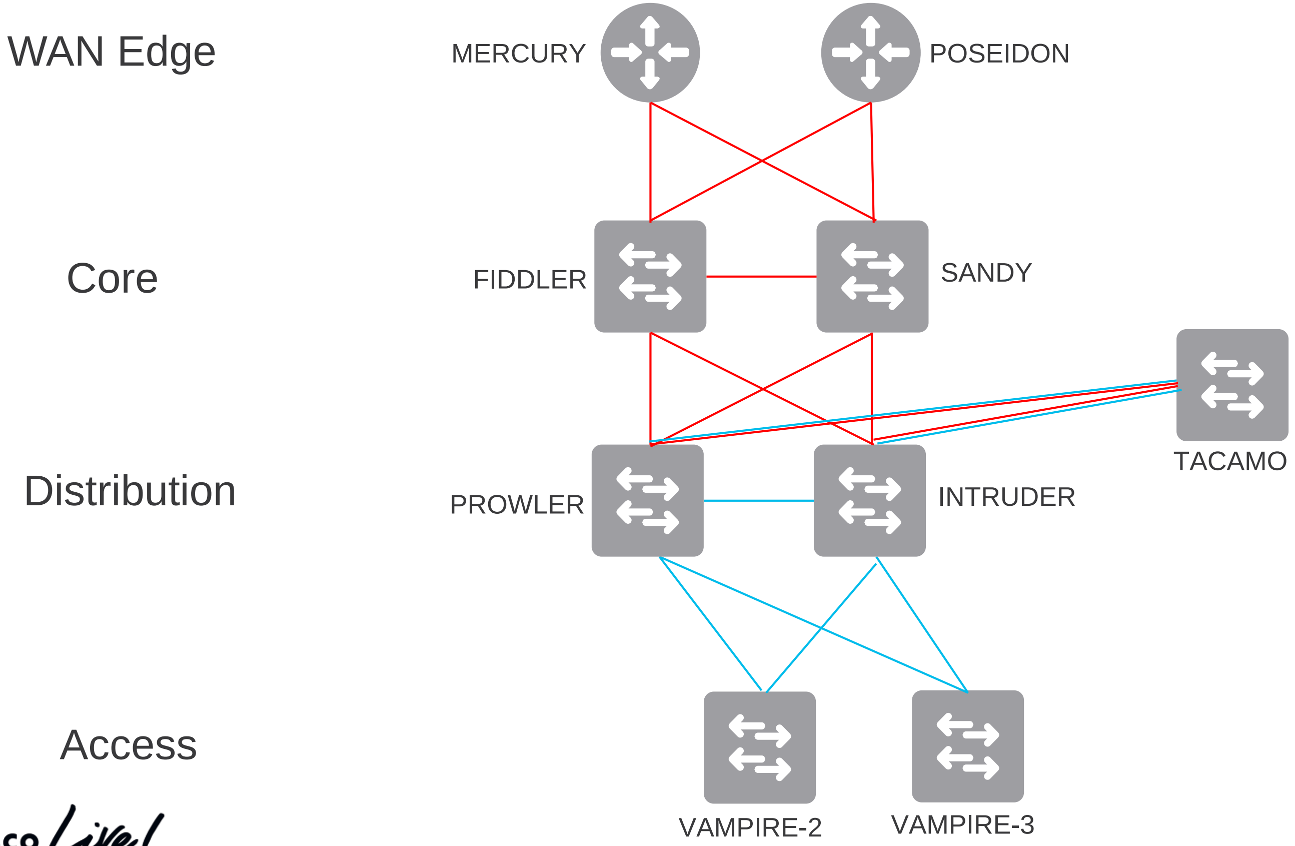
Getting Started Steps – OSPF as an IGP



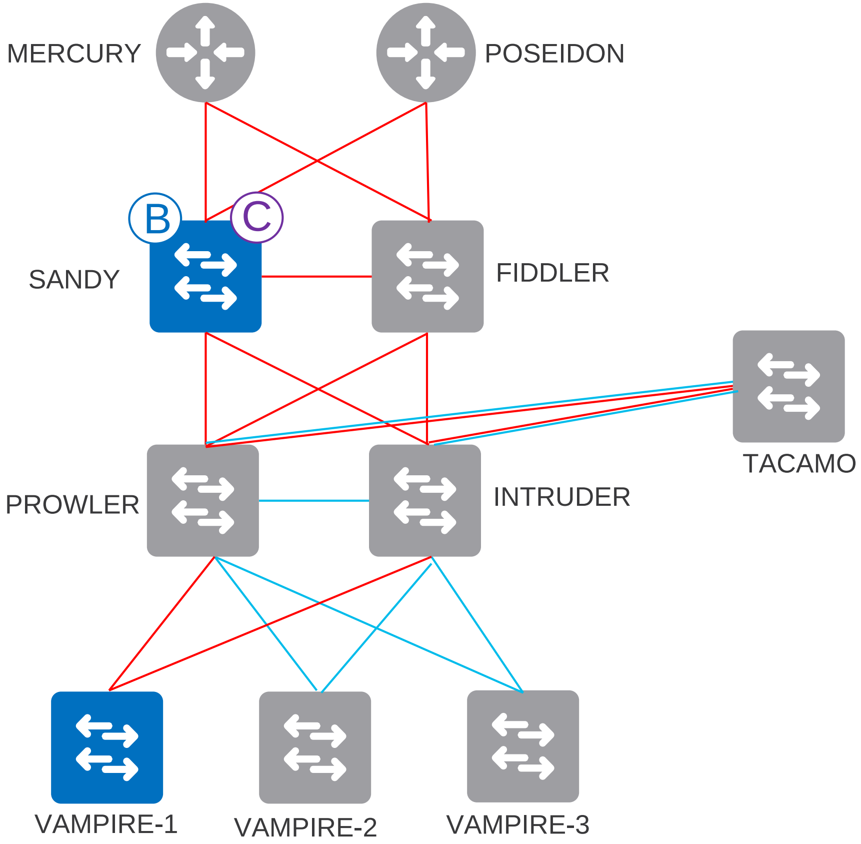
```
interface GigabitEthernet1/1/1
 no switchport
 ip address 192.168.22.58 255.255.255.252
!
interface GigabitEthernet1/1/2
 no switchport
 ip address 192.168.22.38 255.255.255.252
!
interface Loopback0
 ip address 192.168.21.9 255.255.255.255
 ip ospf network point-to-point
```

```
router ospf 1
 router-id 192.168.21.9
 passive-interface default
 no passive-interface GigabitEthernet1/1/1
 no passive-interface GigabitEthernet1/1/2
 network 192.168.21.9 0.0.0.0 area 0
 network 192.168.22.38 0.0.0.0 area 0
 network 192.168.22.58 0.0.0.0 area 0
```

Existing Network Topology

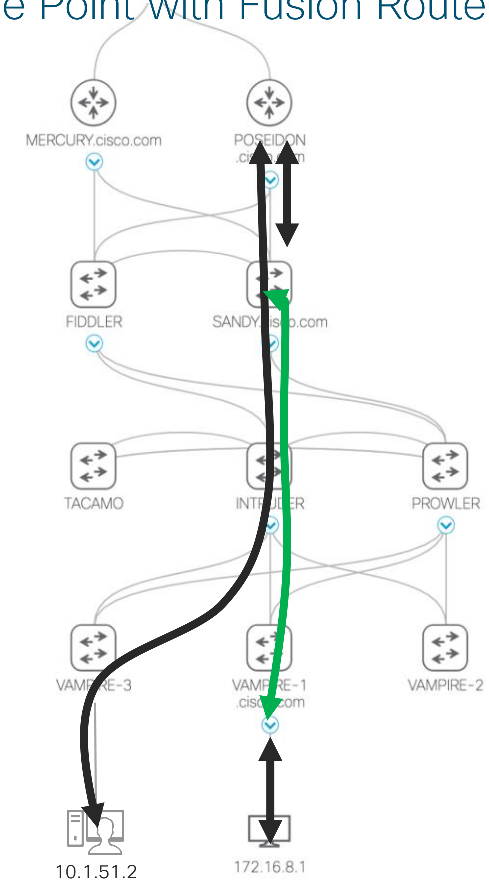


Current State of the Network



Communications in SD-Access Fabric

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

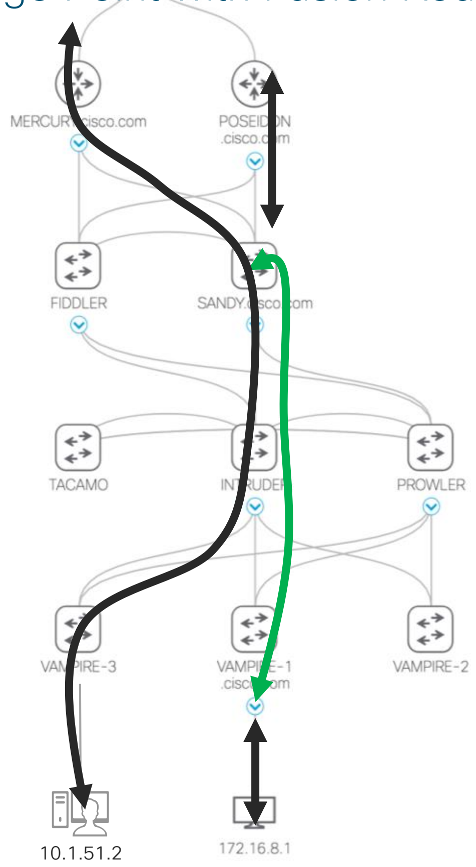


⟷ Un-encapsulated packet

⟷ VXLAN encapsulated packet

Communications in SD-Access Fabric

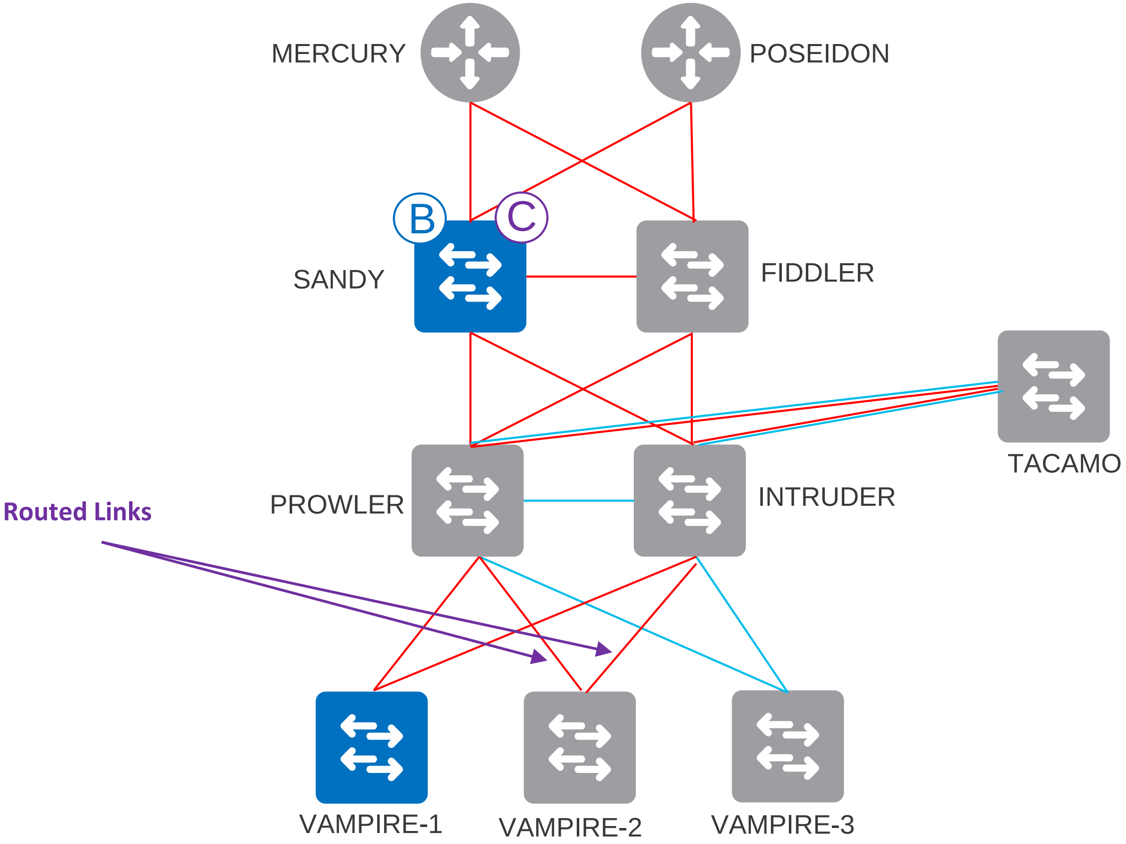
North-South: Fabric Border is Exchange Point with Fusion Router



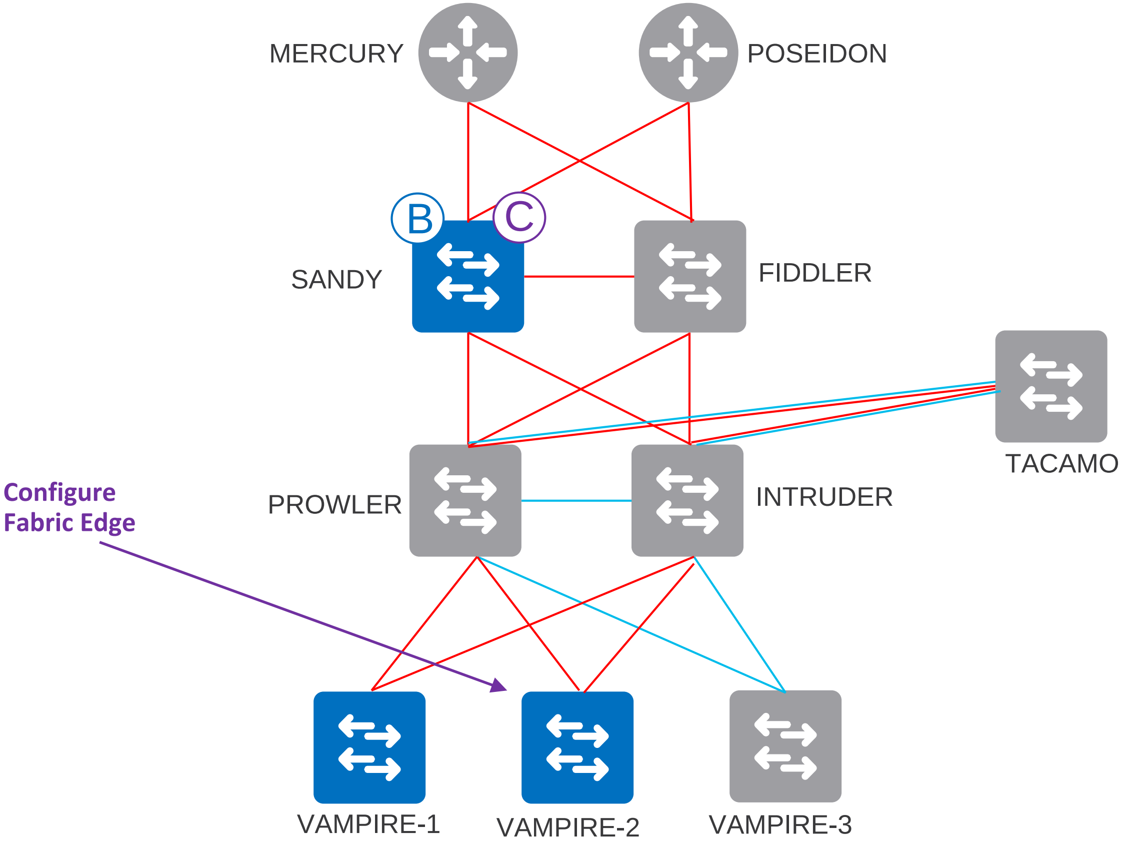
⟷ Un-encapsulated packet

⟷ VXLAN encapsulated packet

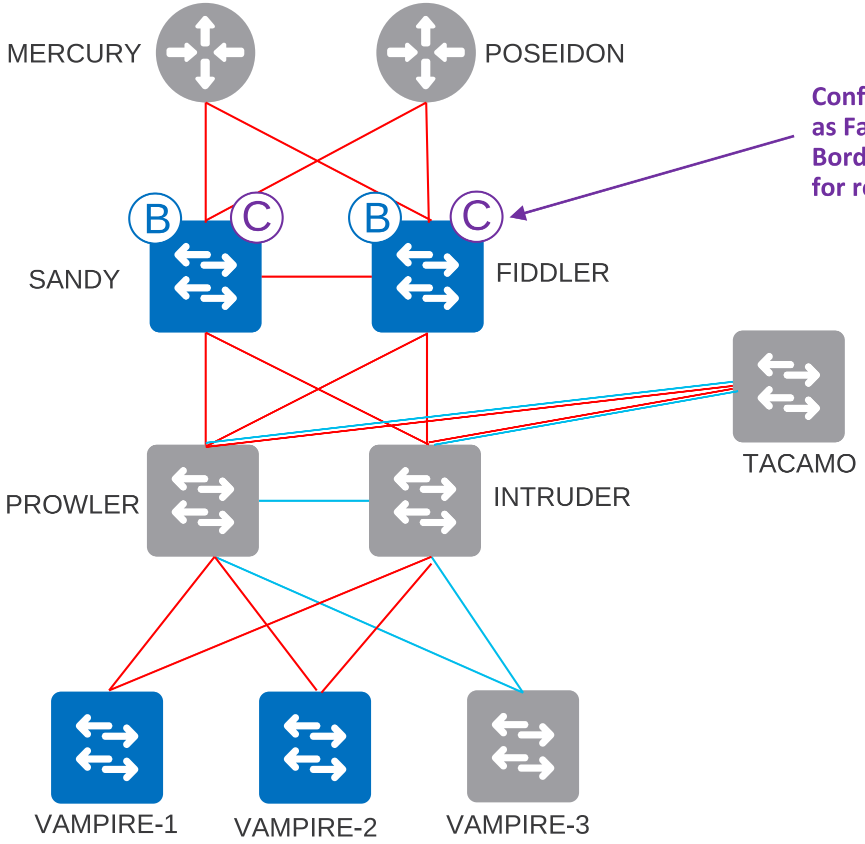
Re-configure Links: L2 to L3 Routed Links



Configure Fabric Edge on Access Switch

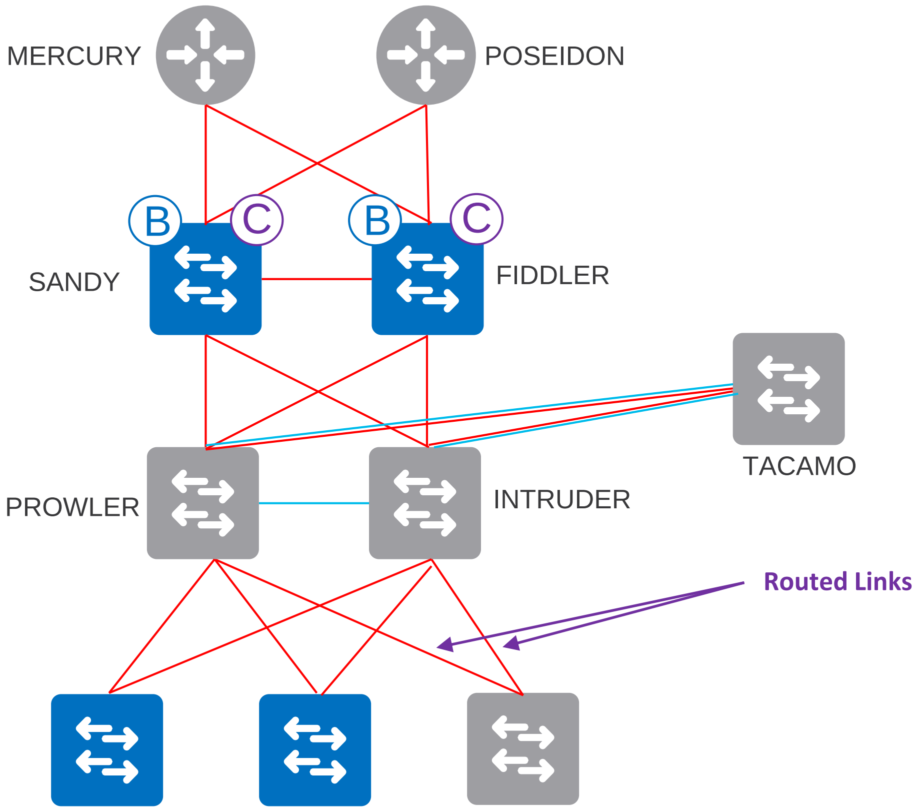


Redundant Fabric Border/Control Plane node

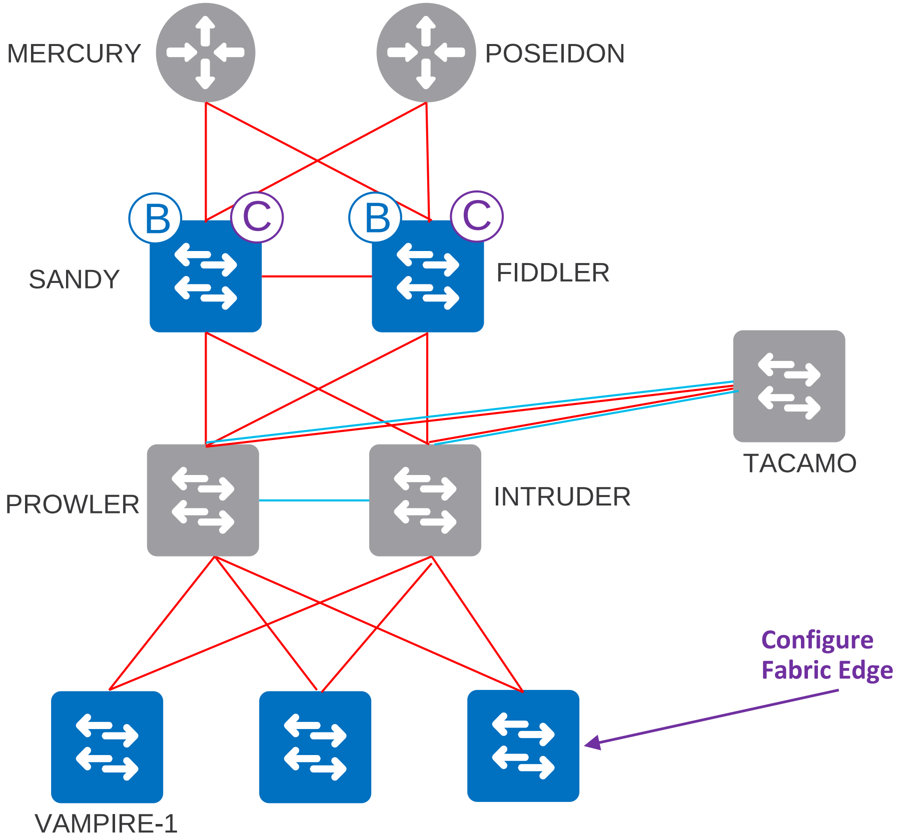


Configure second core as Fabric Border/Control Plane for redundancy

Reconfigure Links: L2 to L3 Routed links

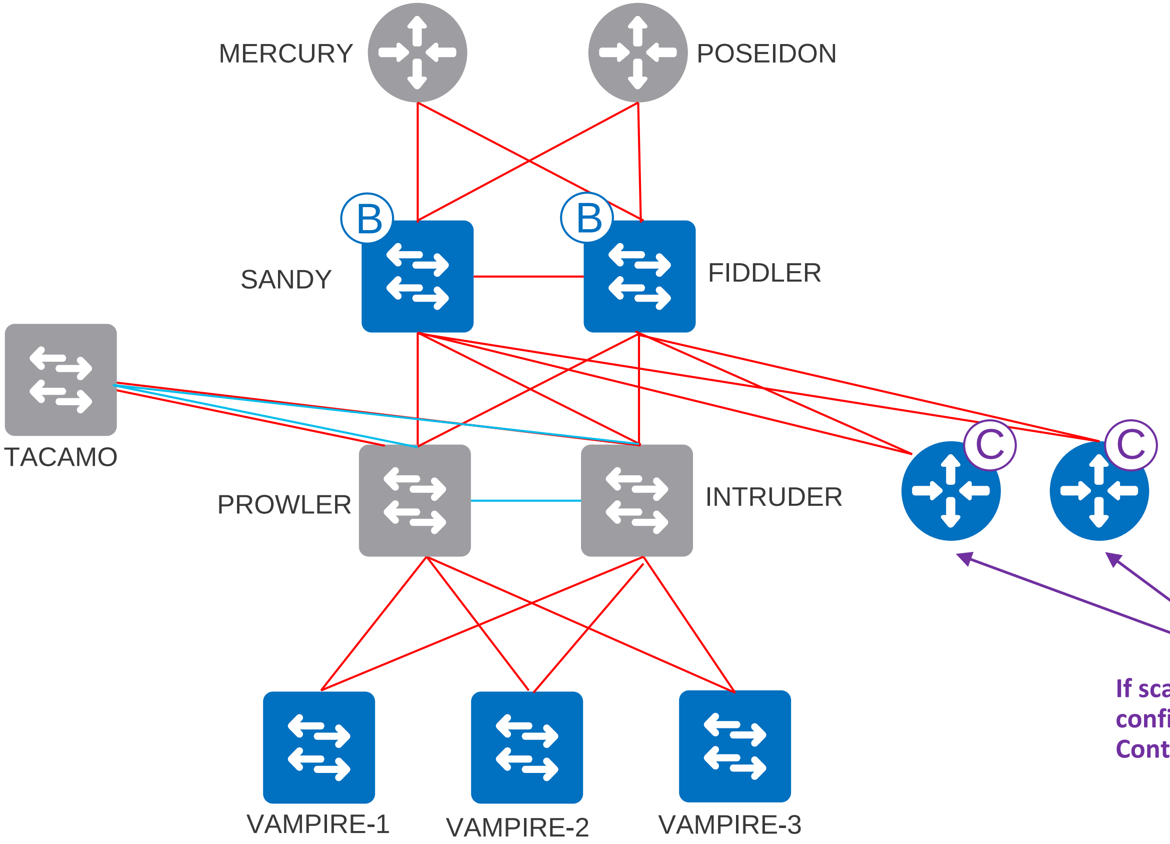


Configure Fabric Edge on Access



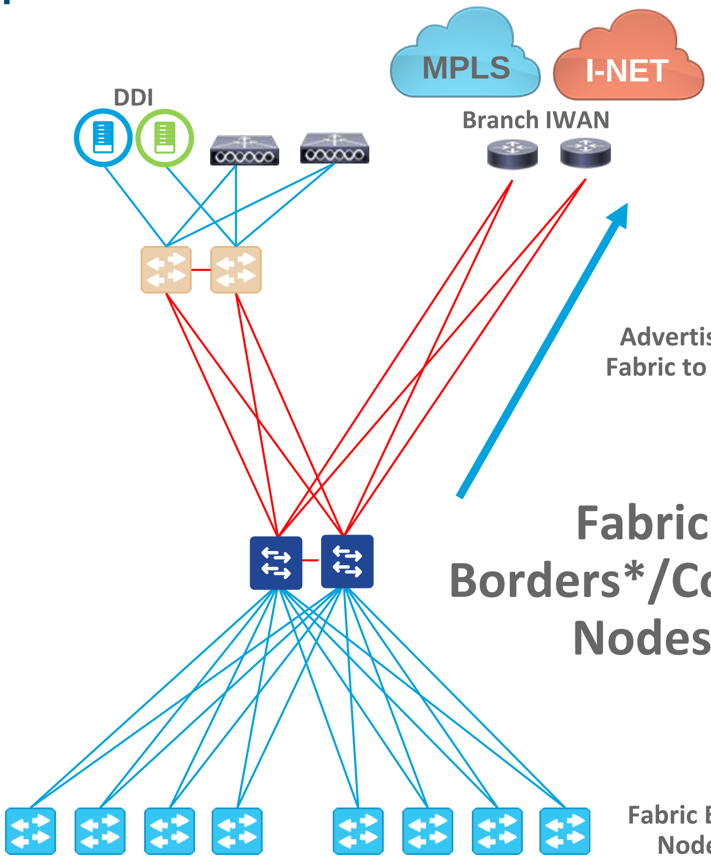
Configure Fabric Edge

Distribute Control Plane node for Scale



If scale demands configure dedicated Control Plane nodes

Branch Design



Advertise Routes from Fabric to External Router

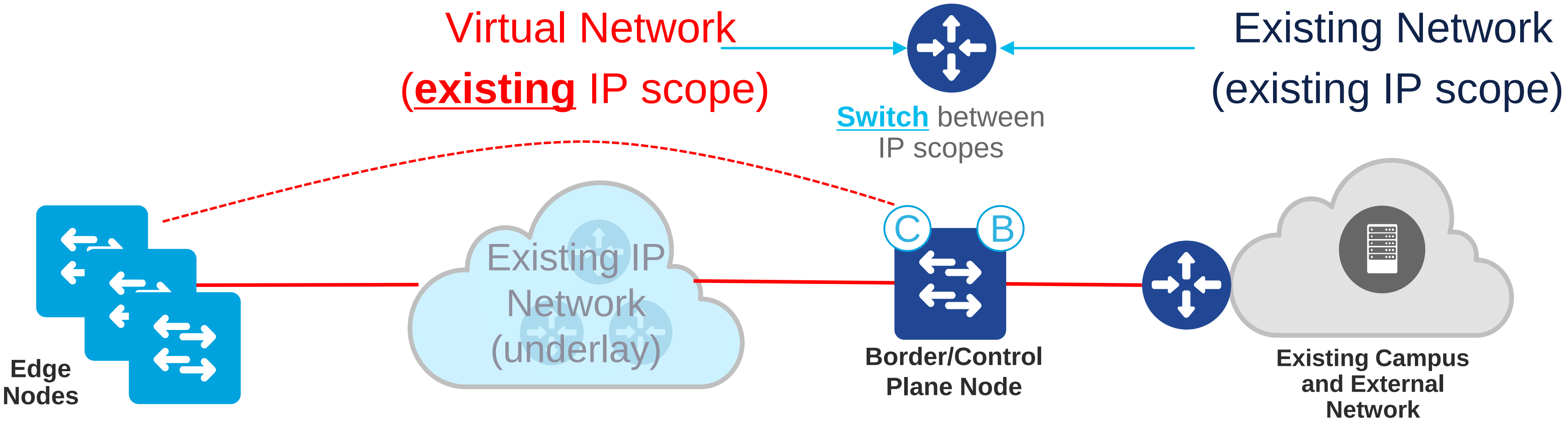
Fabric Borders*/Control Nodes

Fabric Edge Nodes

* Optionally advertise external known networks from Fabric Border

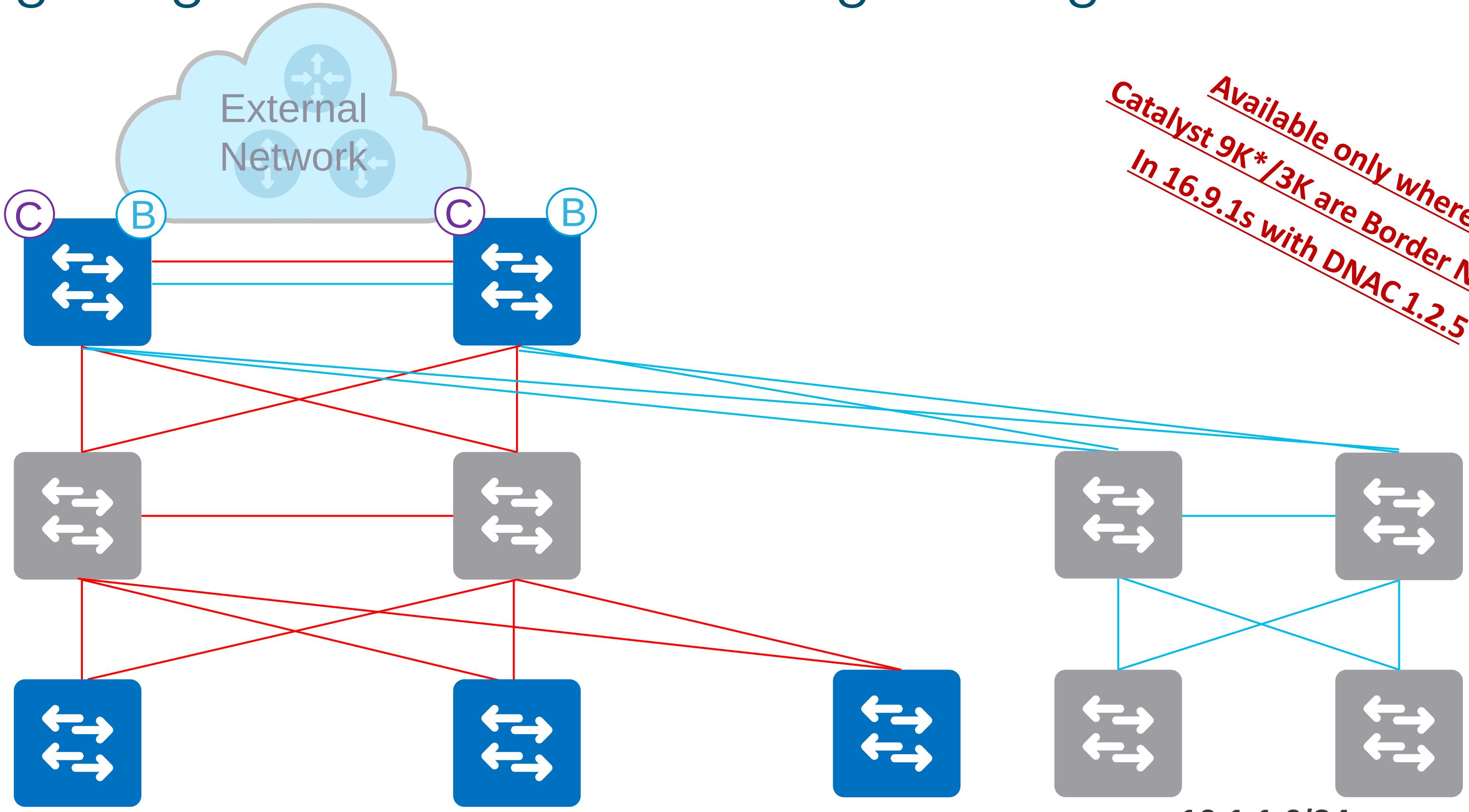
Migrating with Existing Switches, Existing Subnets

Incremental Migration – High Level concept



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

Migrating to SD-Access retaining existing subnets



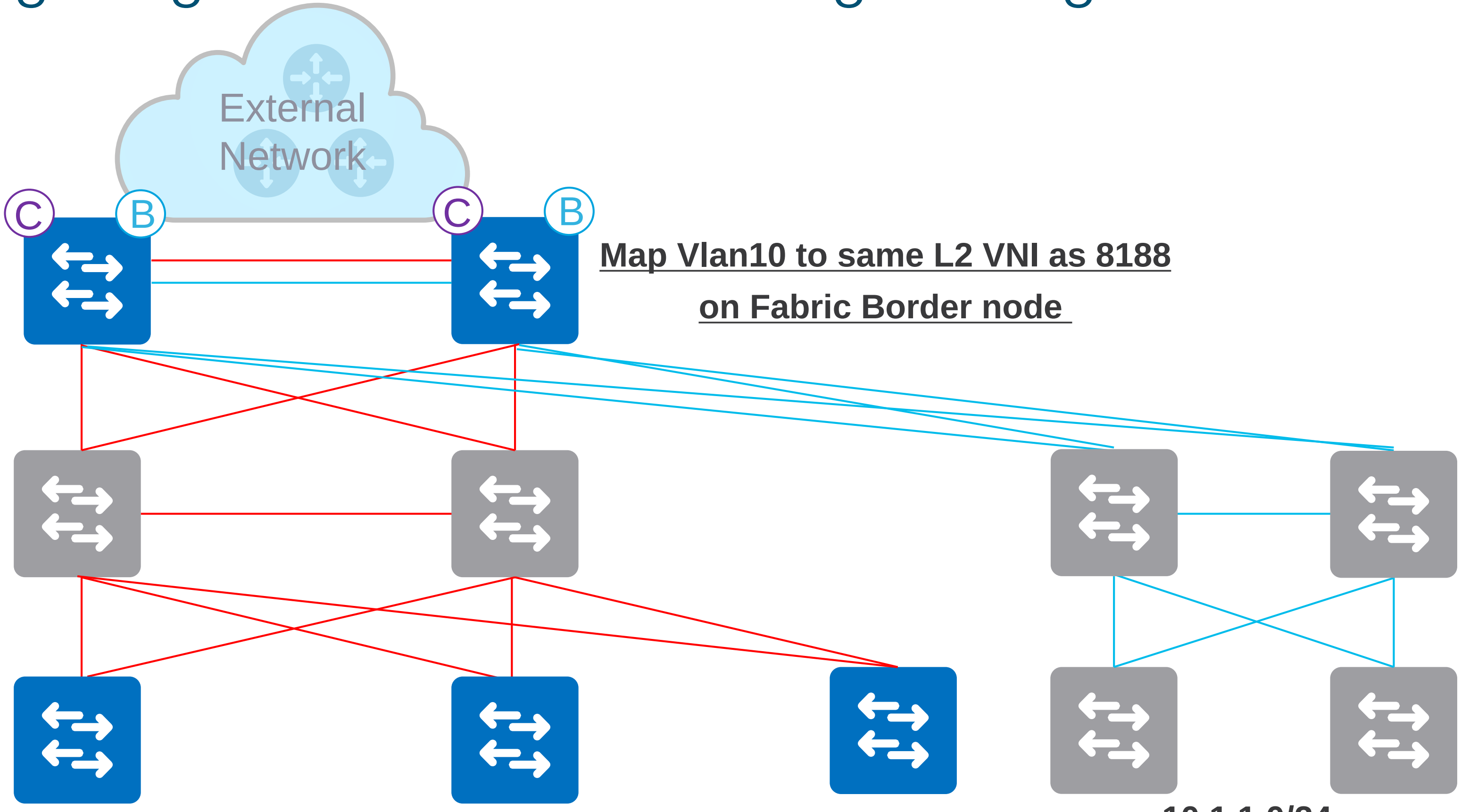
Available only where Catalyst 9K*/3K are Border Nodes In 16.9.1s with DNAC 1.2.5

10.1.1.0/24 VLAN 1021 L2 VNI = 8188

10.1.1.0/24

VLAN10

Migrating to SD-Access retaining existing subnets



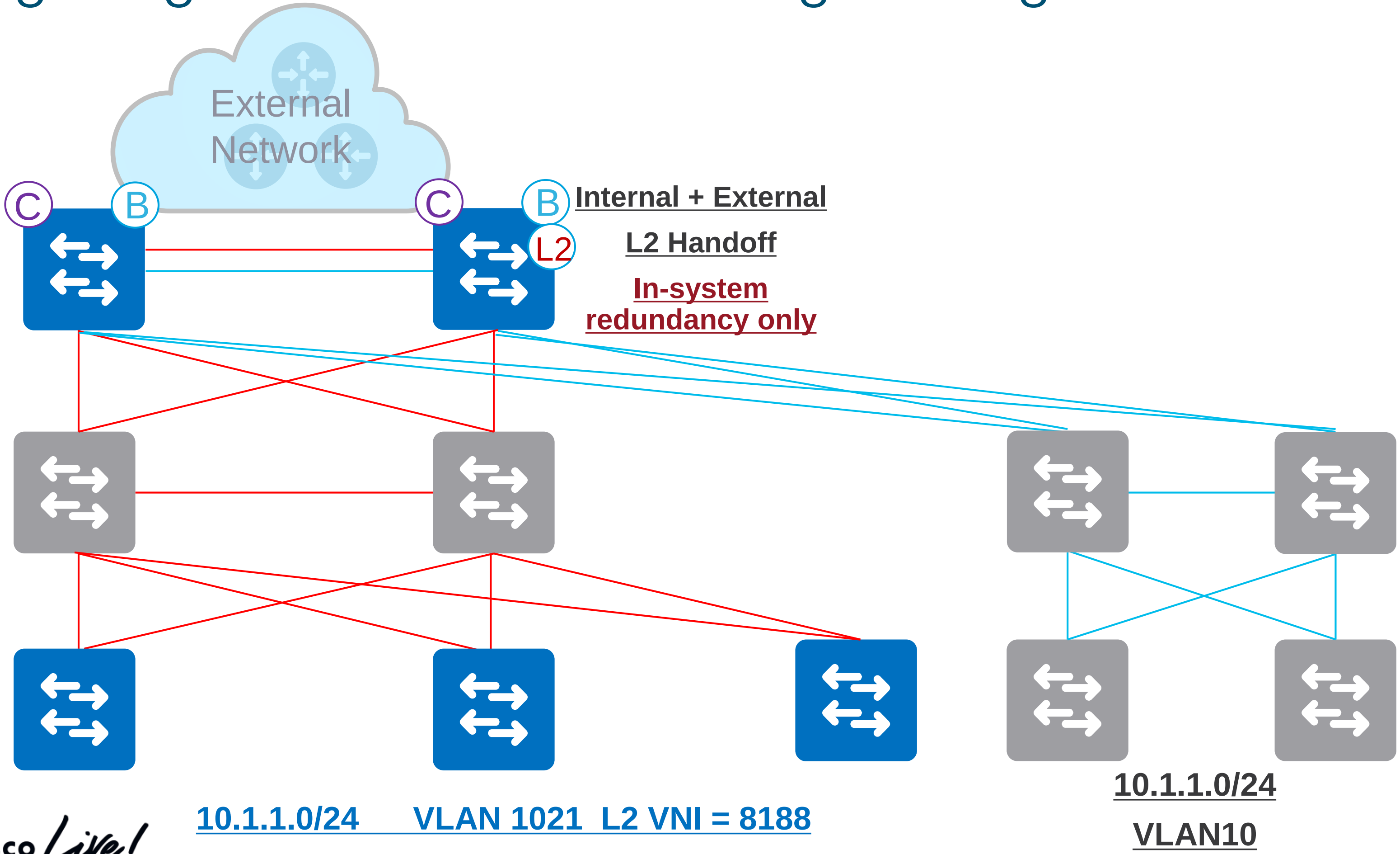
Map Vlan10 to same L2 VNI as 8188
on Fabric Border node

10.1.1.0/24   VLAN 1021 L2 VNI = 8188

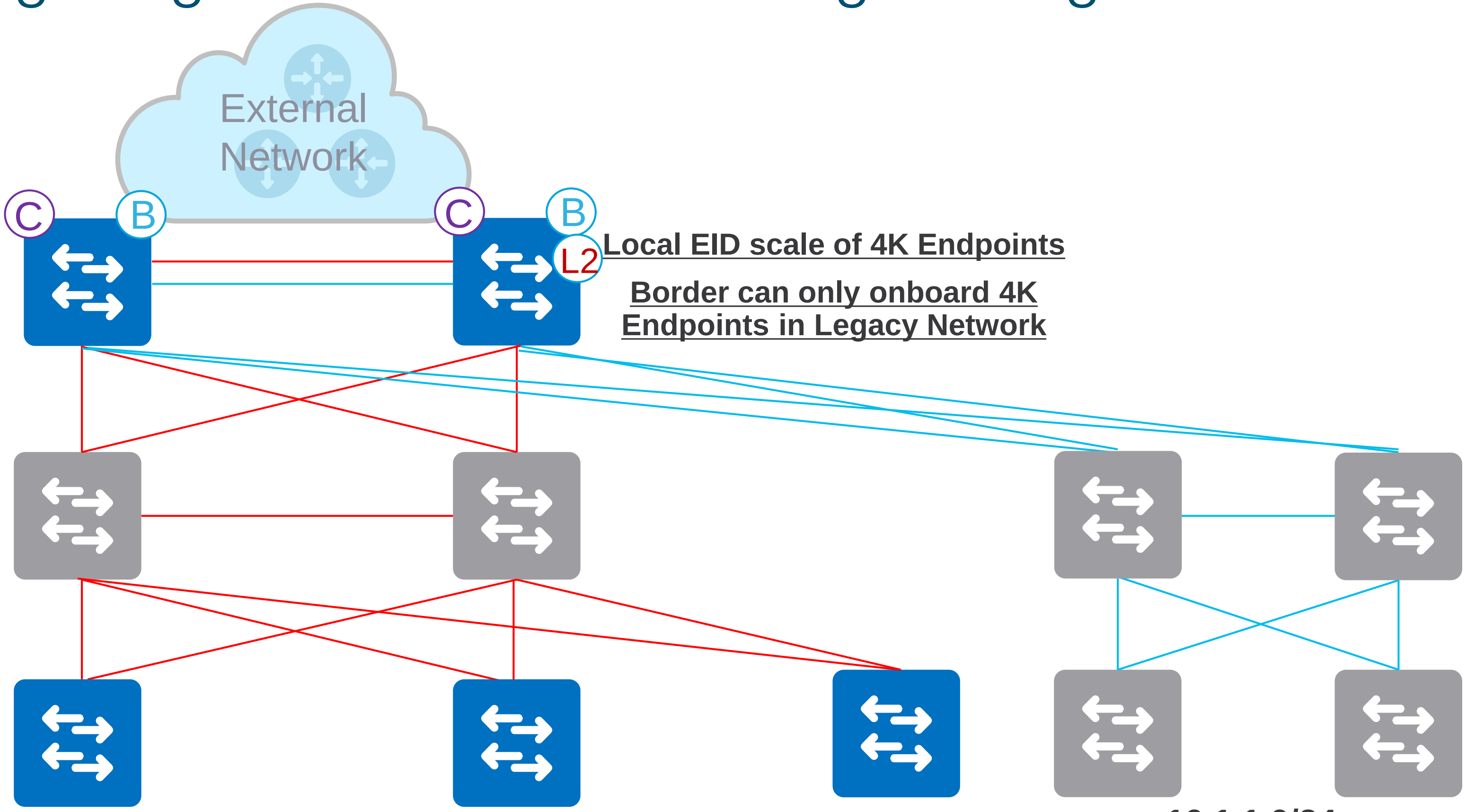
10.1.1.0/24

VLAN10

Migrating to SD-Access retaining existing subnets



Migrating to SD-Access retaining existing subnets



Local EID scale of 4K Endpoints

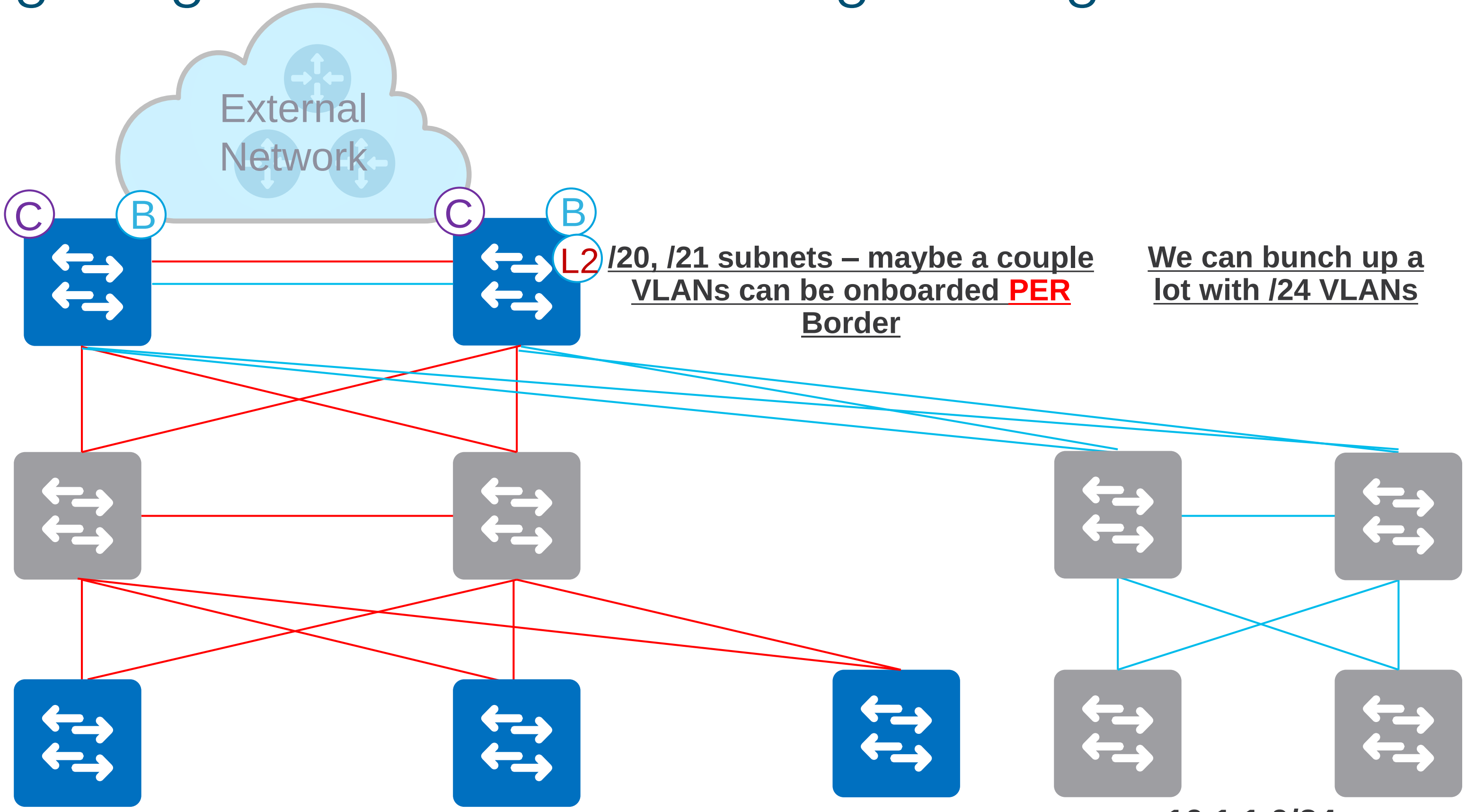
Border can only onboard 4K Endpoints in Legacy Network

10.1.1.0/24 VLAN 1021 L2 VNI = 8188

10.1.1.0/24

VLAN10

Migrating to SD-Access retaining existing subnets



/20, /21 subnets – maybe a couple VLANs can be onboarded PER Border

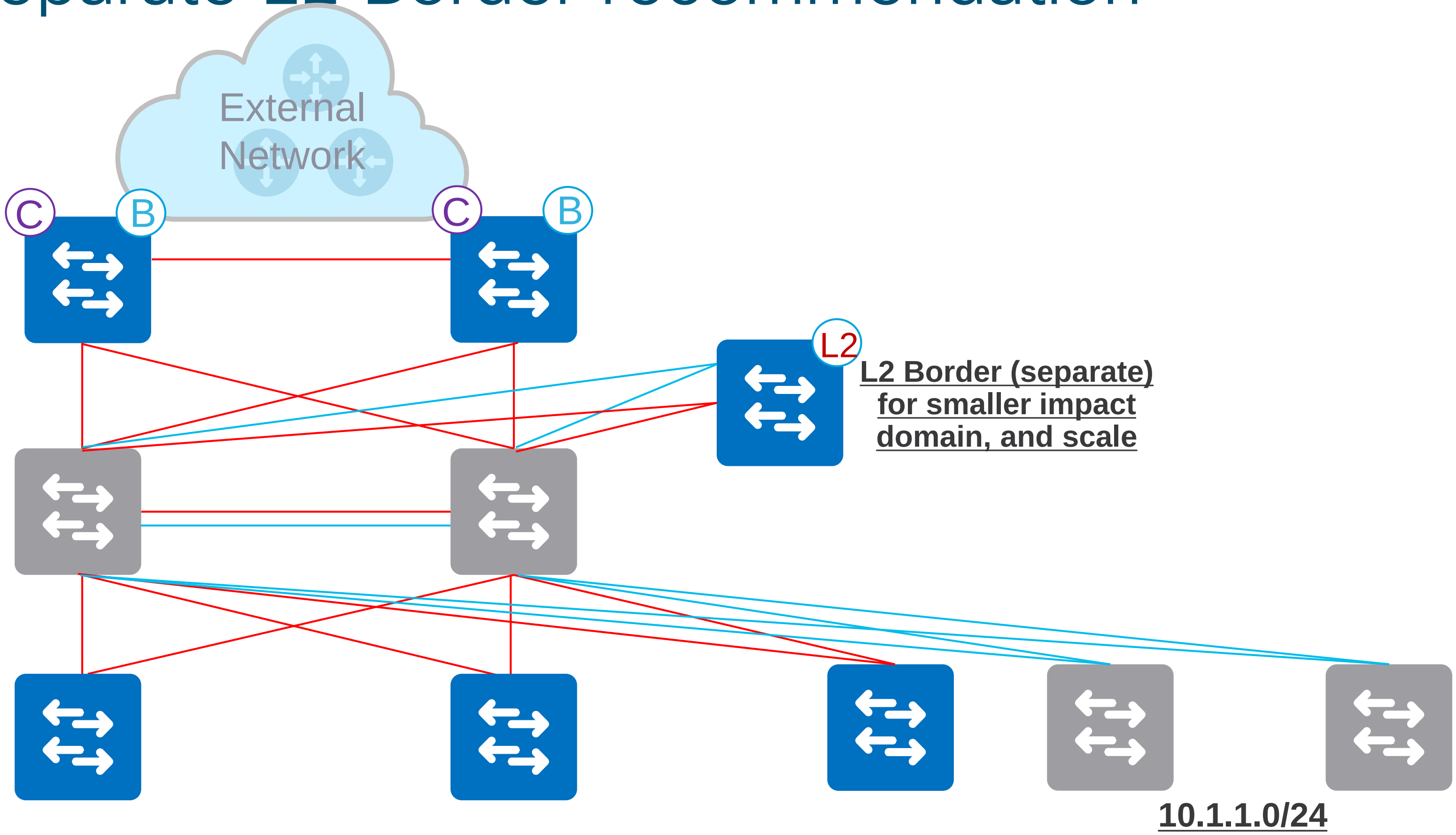
We can bunch up a lot with /24 VLANs

10.1.1.0/24 VLAN 1021 L2 VNI = 8188

10.1.1.0/24

VLAN10

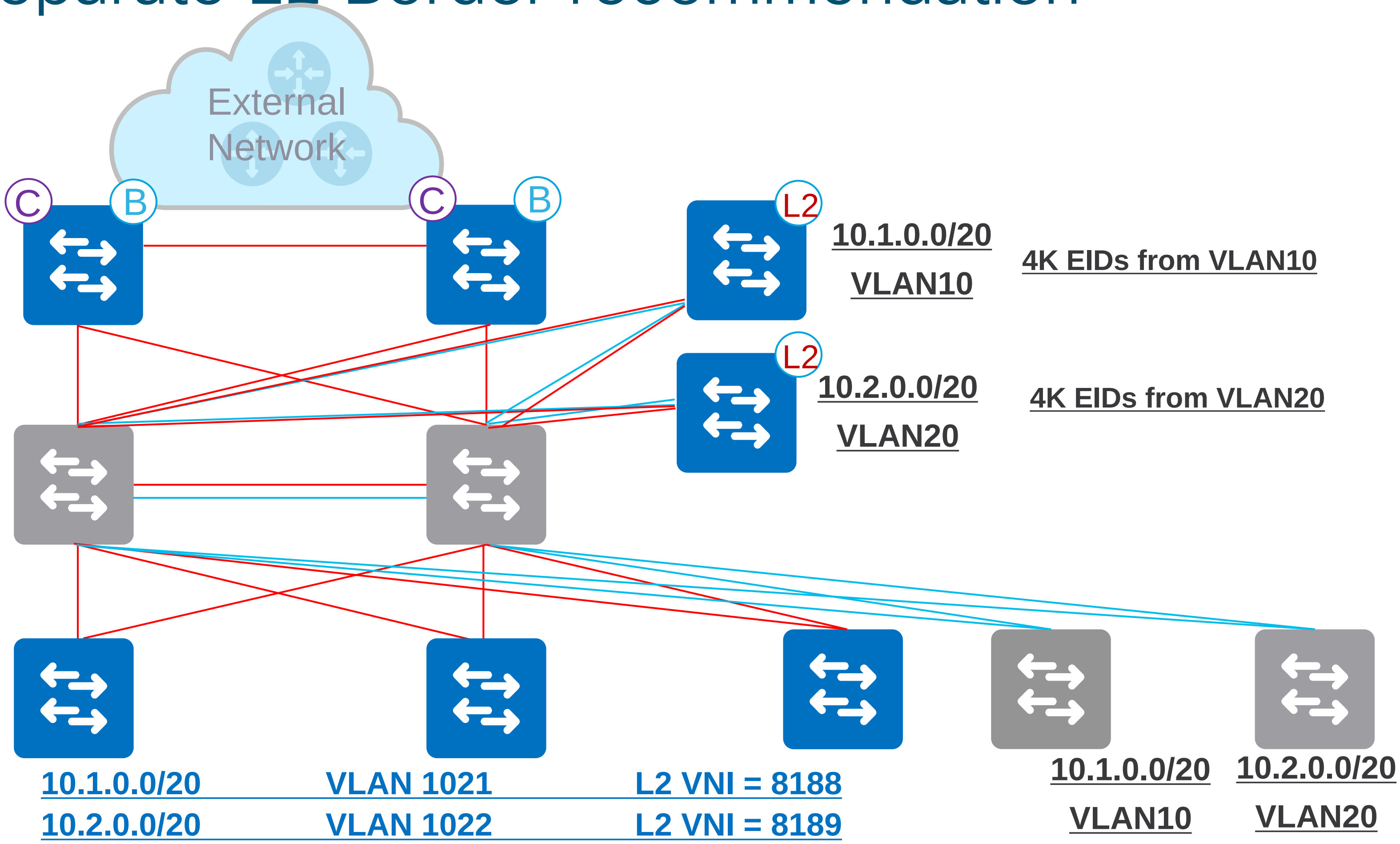
Separate L2 Border recommendation



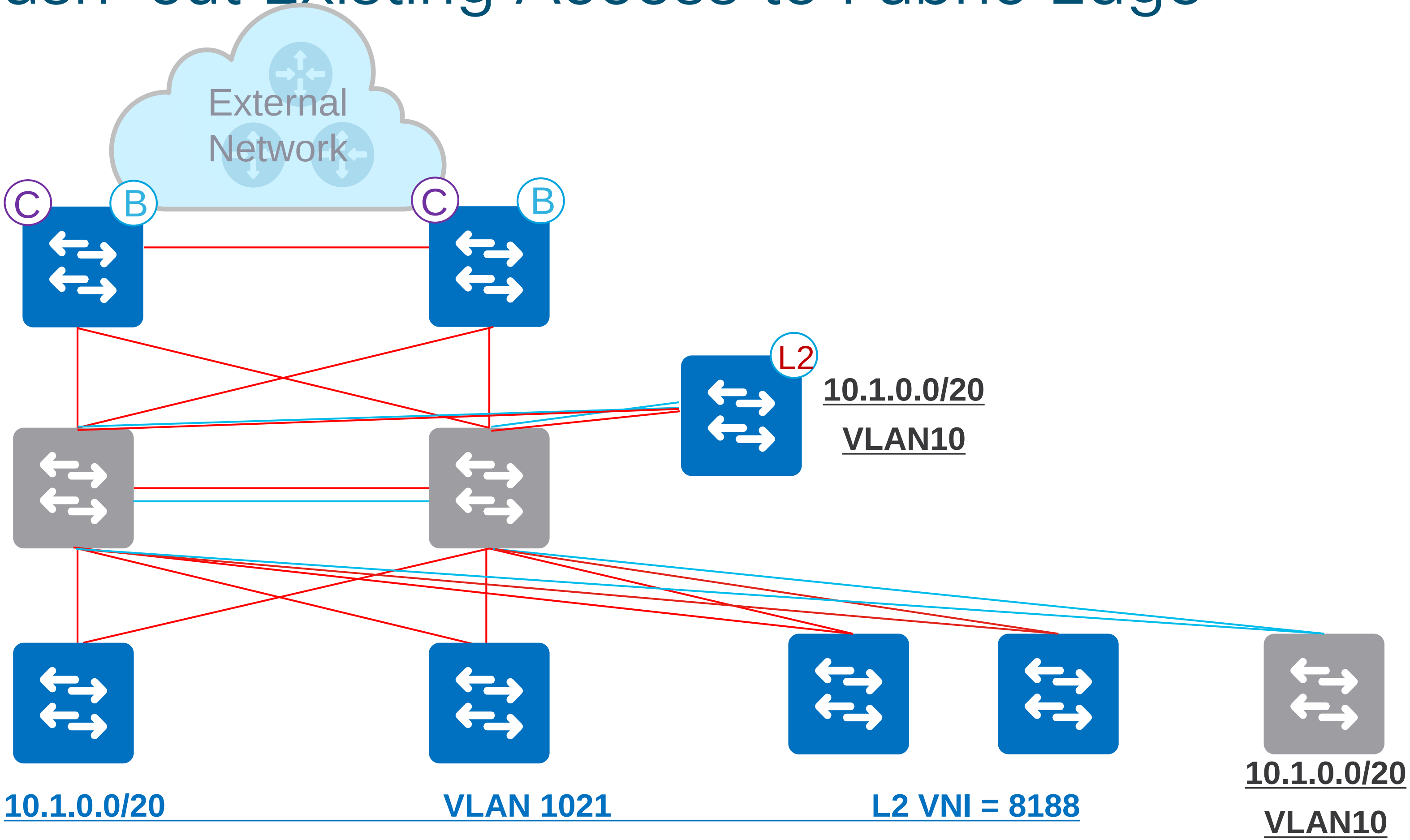
L2 Border (separate) for smaller impact domain, and scale

10.1.1.0/24 VLAN 1021 L2 VNI = 8188

Separate L2 Border recommendation

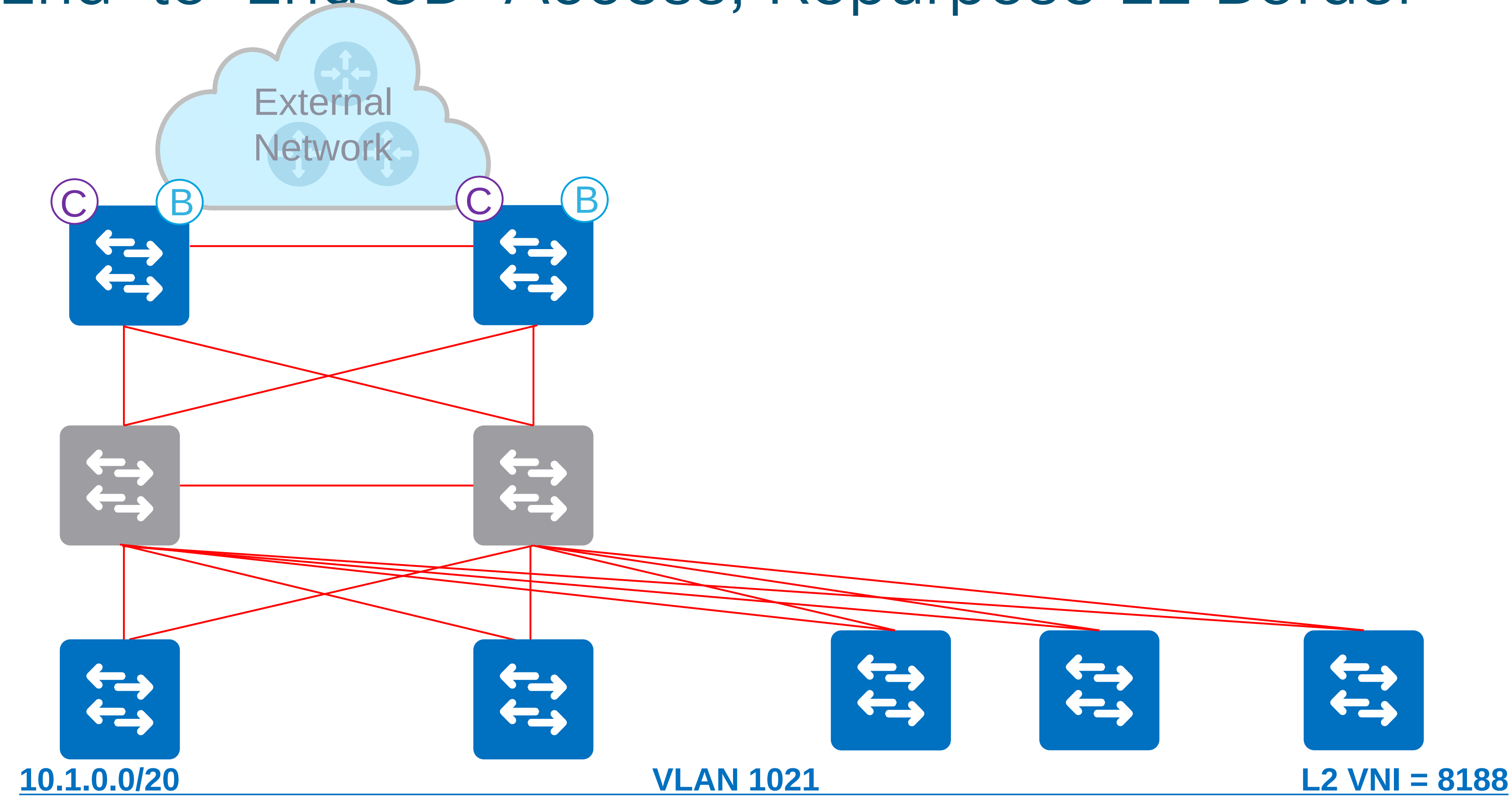


Flash-cut Existing Access to Fabric Edge



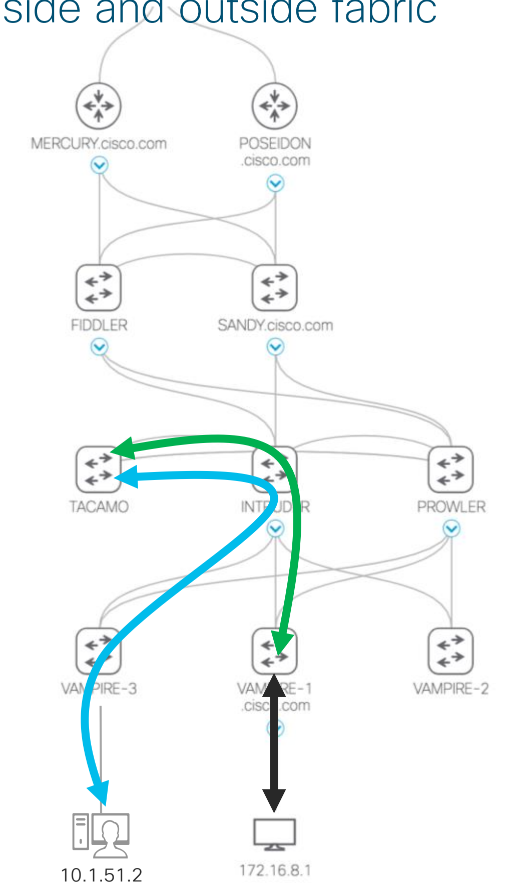
10.1.0.0/20 VLAN 1021 L2 VNI = 8188

End-to-End SD-Access, Repurpose L2 Border



Communications in SD-Access Fabric

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



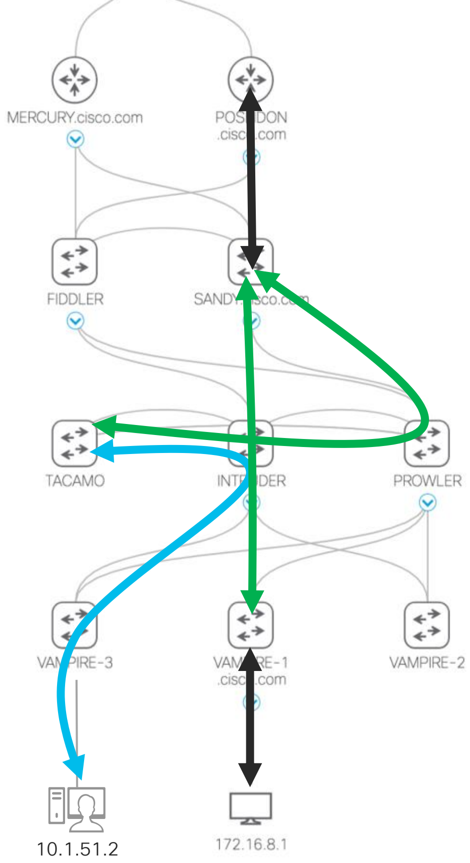
↔ Bridged packet

↔ Un-encapsulated packet

↔ VXLAN encapsulated packet

Communications in SD-Access Fabric

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



↔ Bridged packet

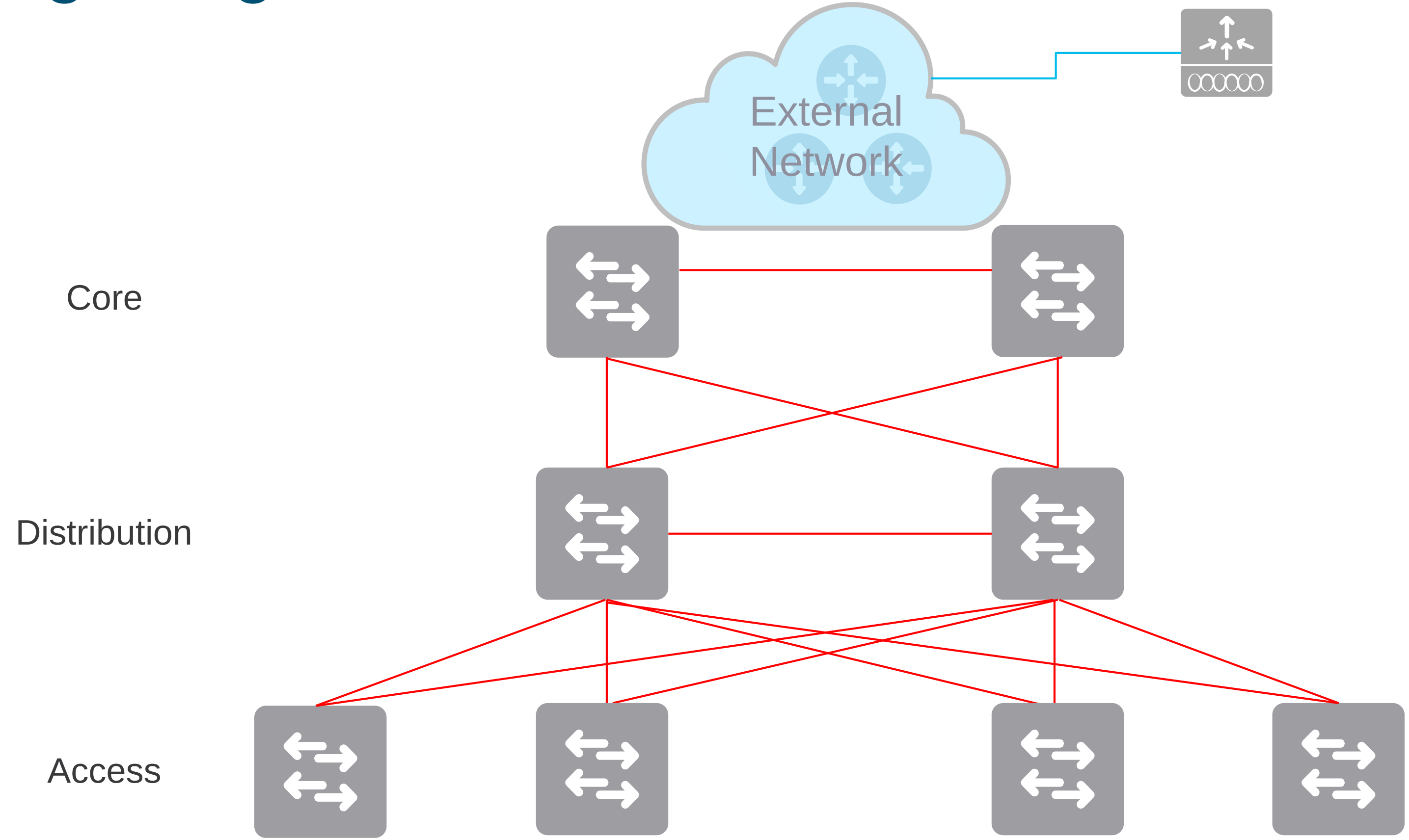
↔ Un-encapsulated packet

↔ VXLAN encapsulated packet

SD-Access Migration

Routed Access with existing subnets, existing switches

Migrating Routed Access to Cisco SD-Access

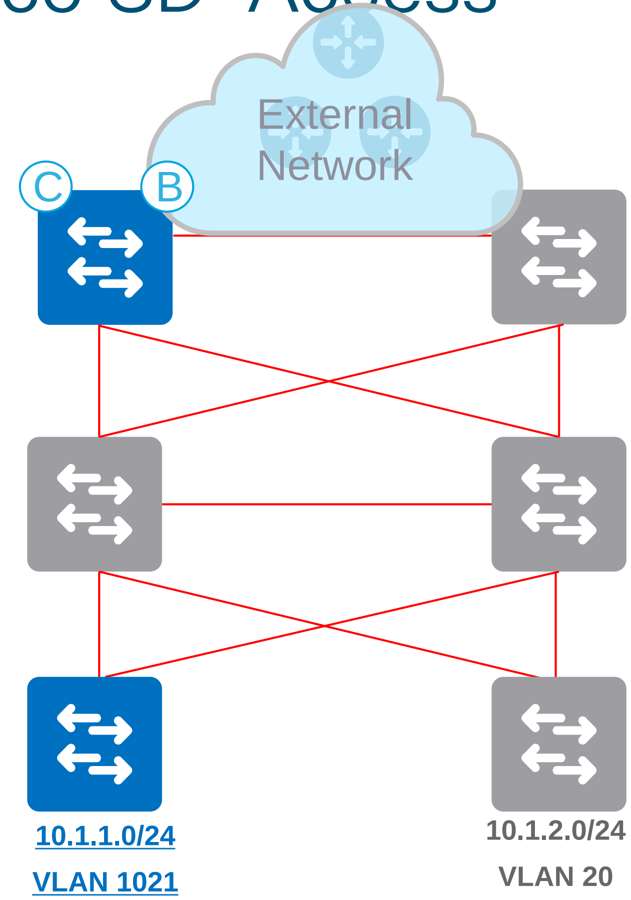


Routed Access Design Considerations

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

Routed Access Migration to Cisco SD-Access

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

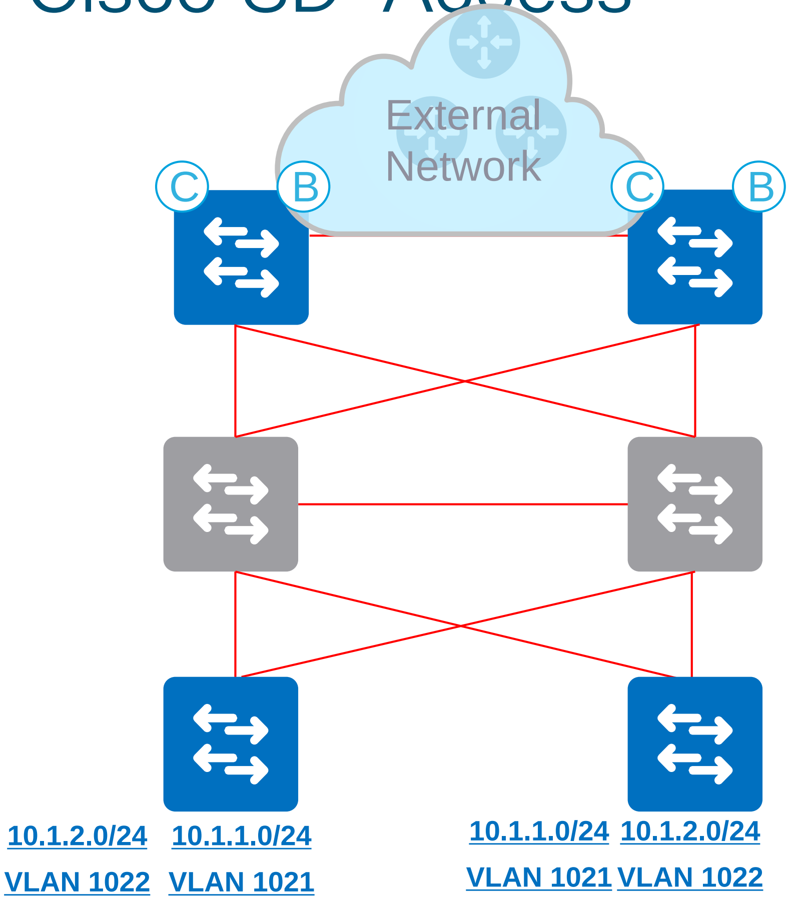


Routed Access Migration to Cisco SD-Access

- Repeat the process for other VLANs on the Fabric Edge

- Repeat the same process on other access switches in converting them to Fabric Edge

- Migration is One-Switch—At-A-Time – **NOT** – One-Vlan-At-A-Time

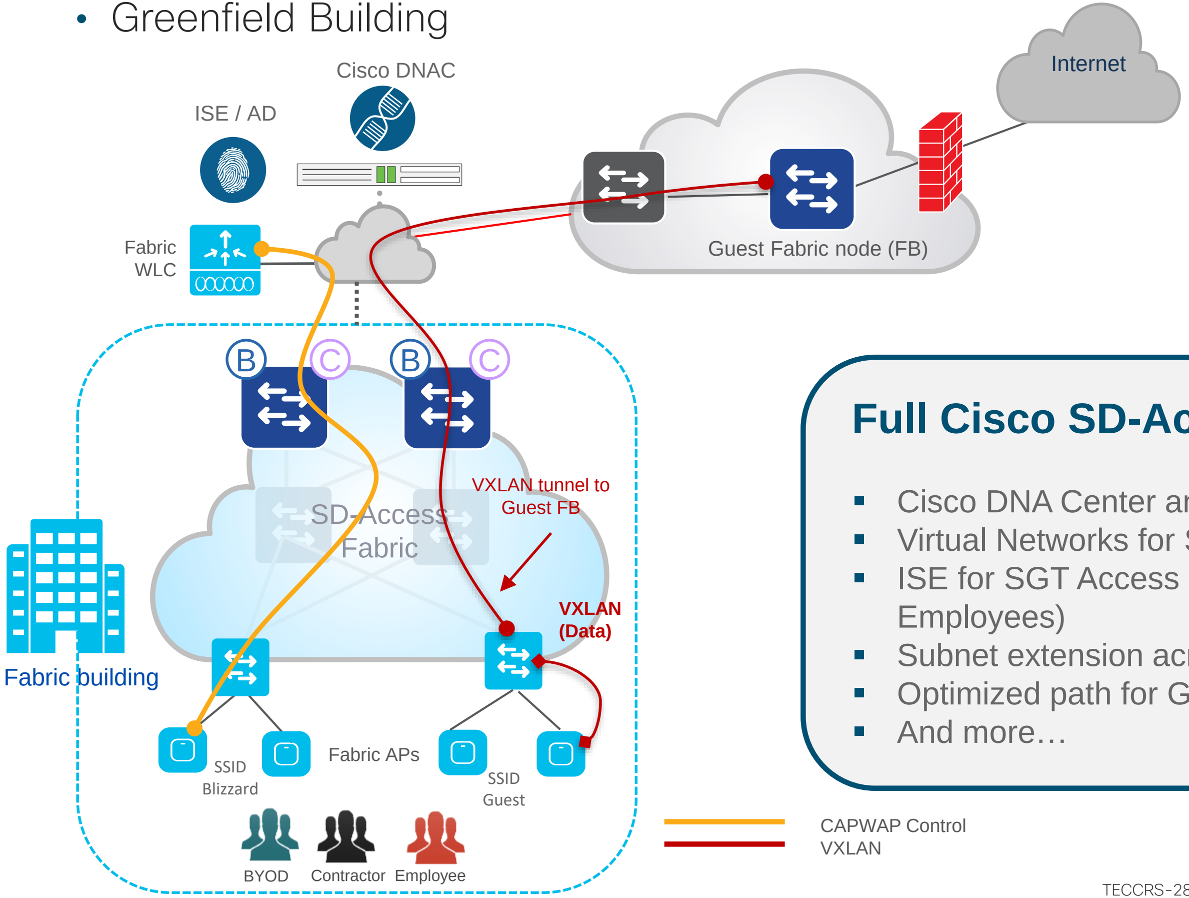


SD-Access Migration

Migrating Wireless into SD-Access

Cisco SD-Access Wireless Adoption

- Greenfield Building

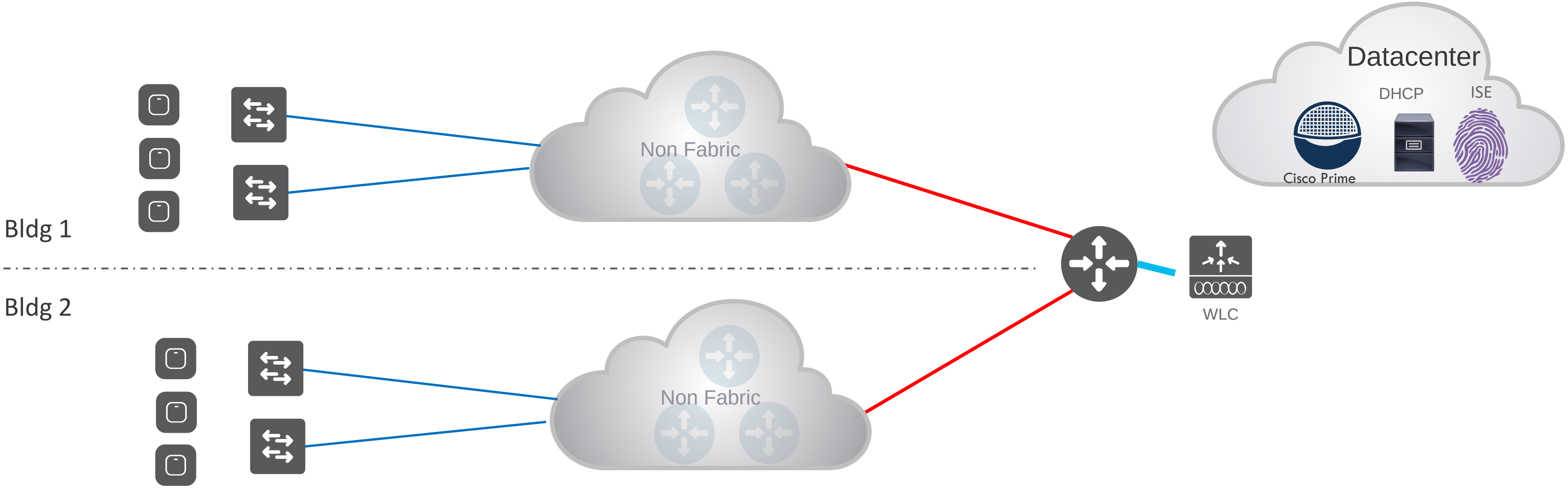


🟧 CAPWAP Control
🟥 VXLAN

Full Cisco SD-Access Wireless value

- Cisco DNA Center and NDP for Automation & Assurance
- Virtual Networks for Segmentation (ex Employee, IoT, Guest)
- ISE for SGT Access Control within VRF (ex. Contractor, BYOD, Employees)
- Subnet extension across Campus with distributed data plane
- Optimized path for Guest and no Anchor WLC
- And more…

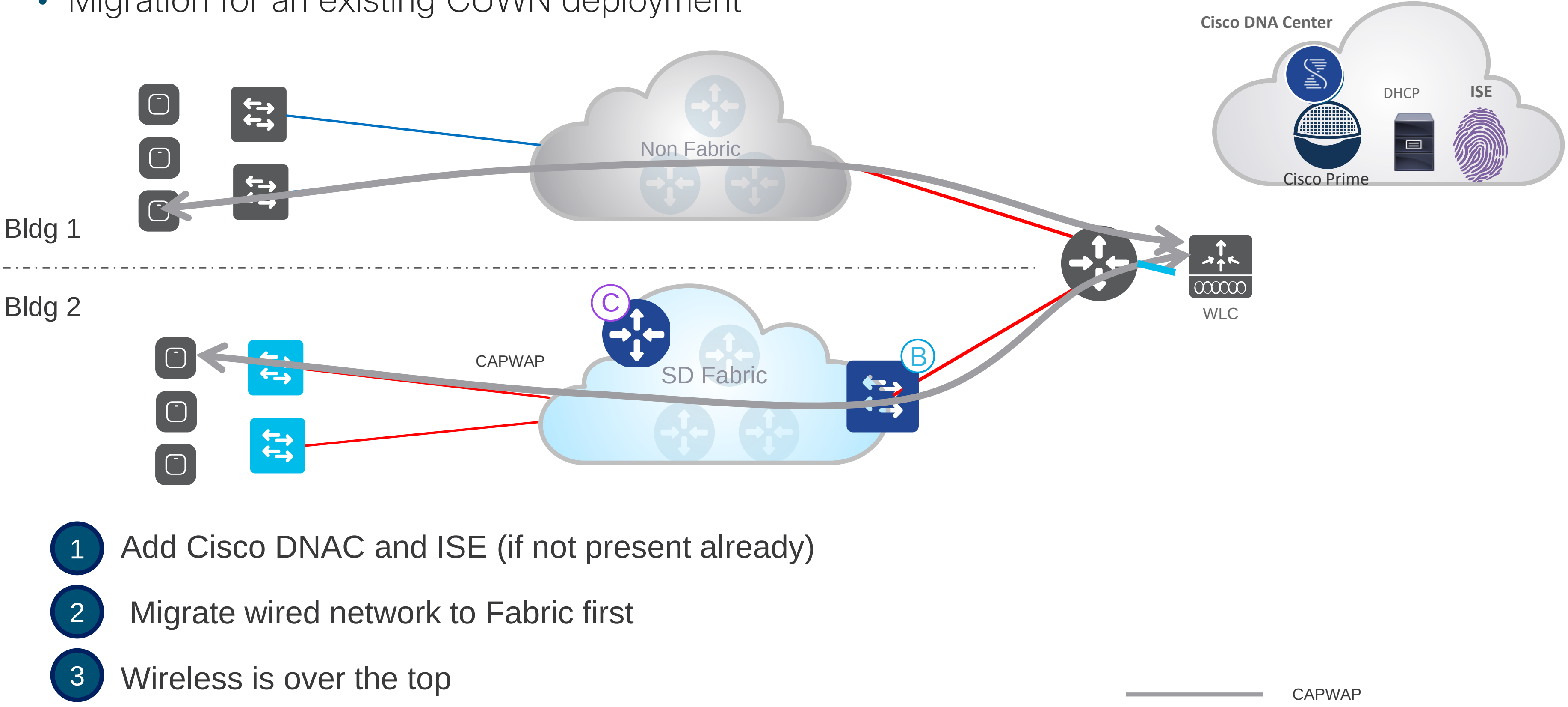
Migrating to Cisco SD-Access Wireless from CUWN



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

Cisco SD-Access Wireless Adoption

- Migration for an existing CUWN deployment



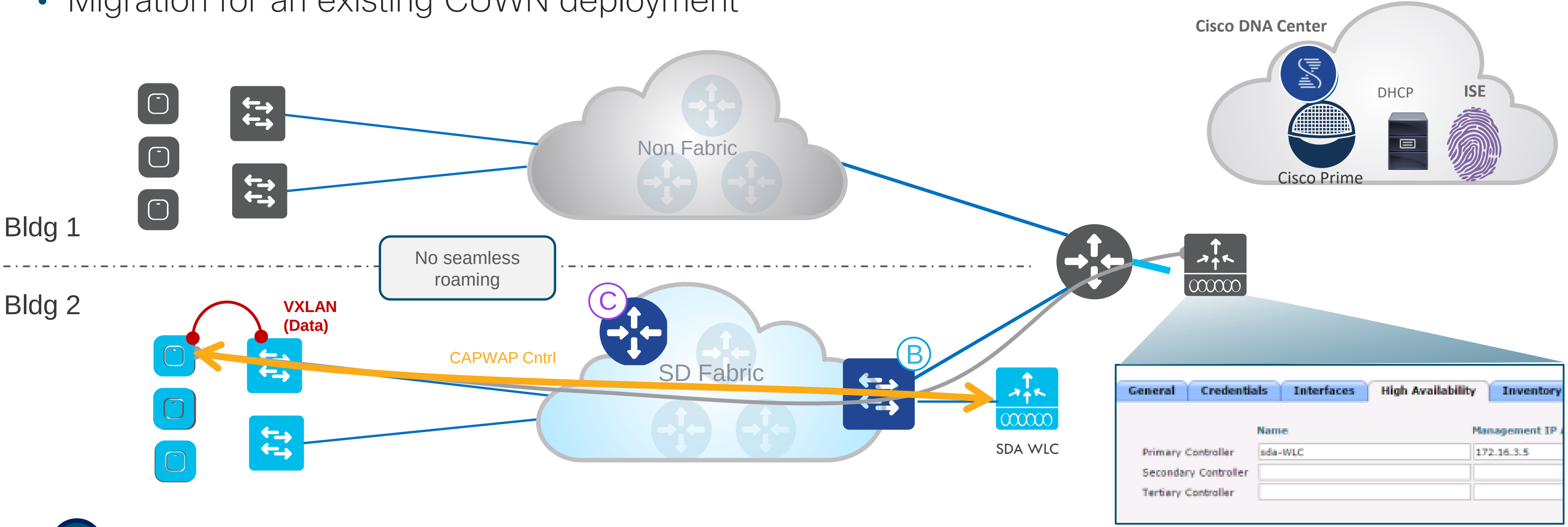
1 Add Cisco DNAC and ISE (if not present already)

2 Migrate wired network to Fabric first

3 Wireless is over the top

Cisco SD-Access Wireless Adoption

- Migration for an existing CUWN deployment



General | Credentials | Interfaces | High Availability | Inventory

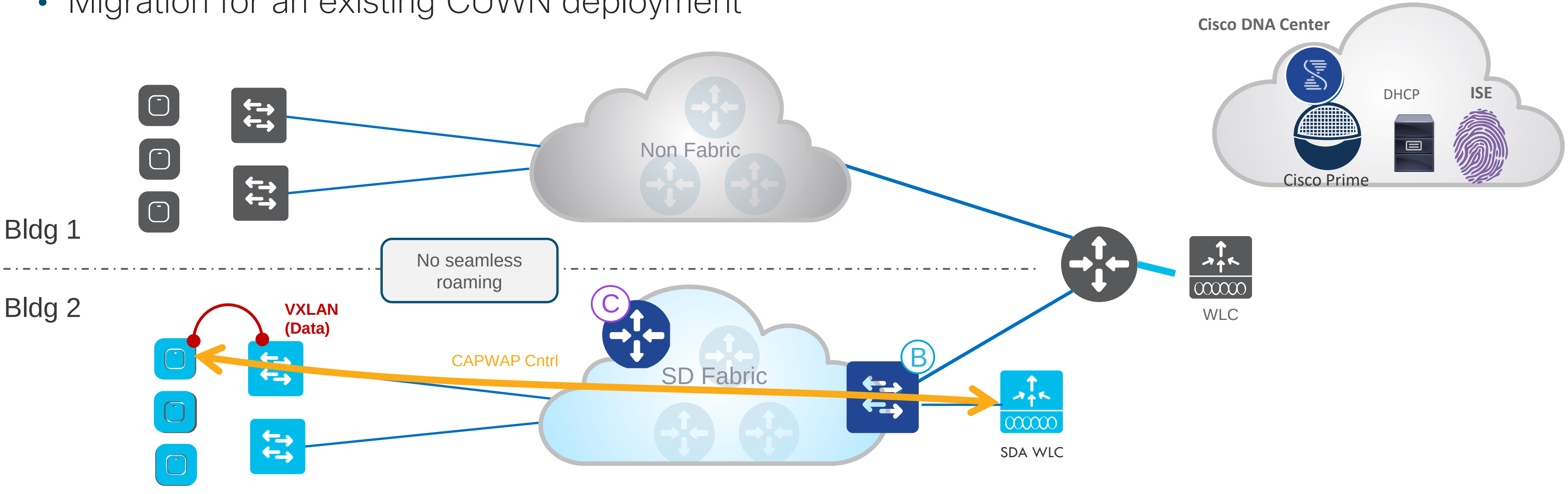
	Name	Management IP
Primary Controller	sda-WLC	172.16.3.5
Secondary Controller		
Tertiary Controller		

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

🟧	CAPWAP Control
🟥	VXLAN

Cisco SD-Access Wireless Adoption

- Migration for an existing CUWN deployment



Recommendations

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

Design Principles

Summary

Design Strategy - Scope

“Connect” with or without “Policy”

RECAP

A Connect Design

0 Services
- DNA Center
- DNS, DHCP & IPAM

1 Wired
- Fusion/Firewalls
- LAN Routers
- LAN Switches

2 Wireless
- SDA vs. OTT
- WLAN Controllers
- Access Points

3 Features
- L2 Broadcast
- IP Multicast
- Telemetry

B Policy Design

0 Services
- Identity Service Engine
- Outside ID Services

1 Identity
- Dynamic Assignment
- Static Assignment

2 Segment
- Virtual Networks
- Scalable Groups

3 Policy
- Firewall Rules
- Access Policies
- App Policies

C Transit

- MAN vs. WAN
- SDX vs. IP-Based

- Identity Propagation
- Multi-Domain Policy

Design Questions - Requirements

Translating Business Intent into Technical Requirements

RECAP

K

Key Questions

Focus on Business Intent & Global Scope

A

Connect Questions

Focus on Topology & Features
(Per Site + Transit)

B

Comply Questions

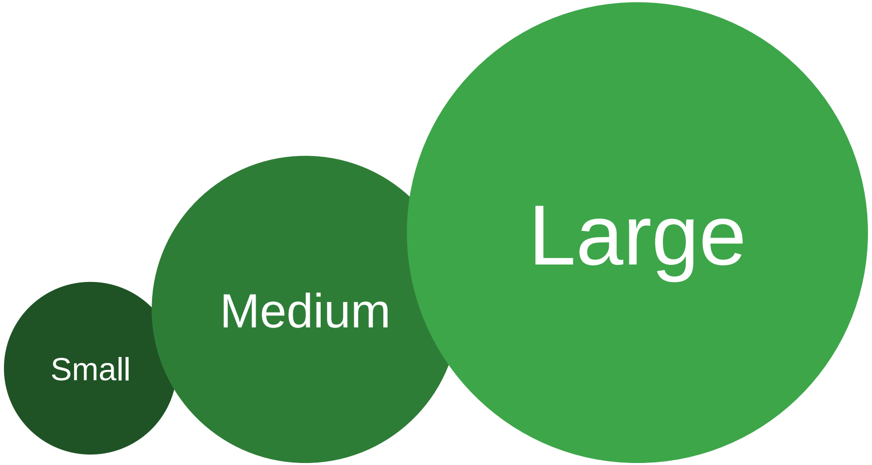
Focus on Access & App Policy
(Per Site + Transit)

High Level Design - Templates

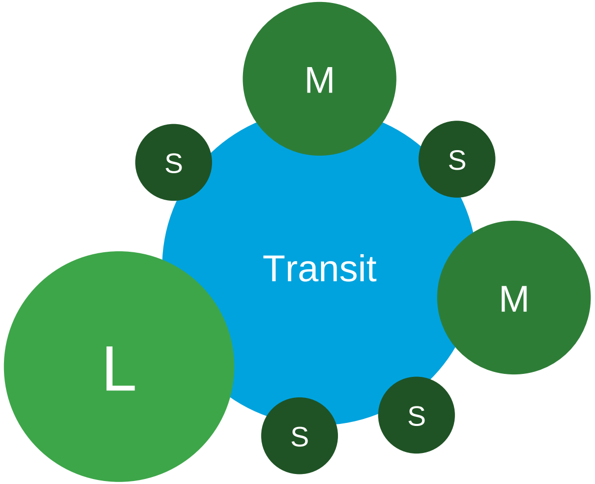
Start from a Cookie Cutter (80%)

RECAP

Basic Goal is for fewer, larger Fabric Sites



Some Needs require split into Multiple Sites



- ✓ Underlay Network (MTU, Latency, etc.)
- ✓ Wireless Client Roaming (< 20ms Latency)
- ✓ Direct Internet Access (@ Remote Sites)
- ✓ Survivable Remote Sites (Local CP/Borders)

Call to Action

What should you do next?

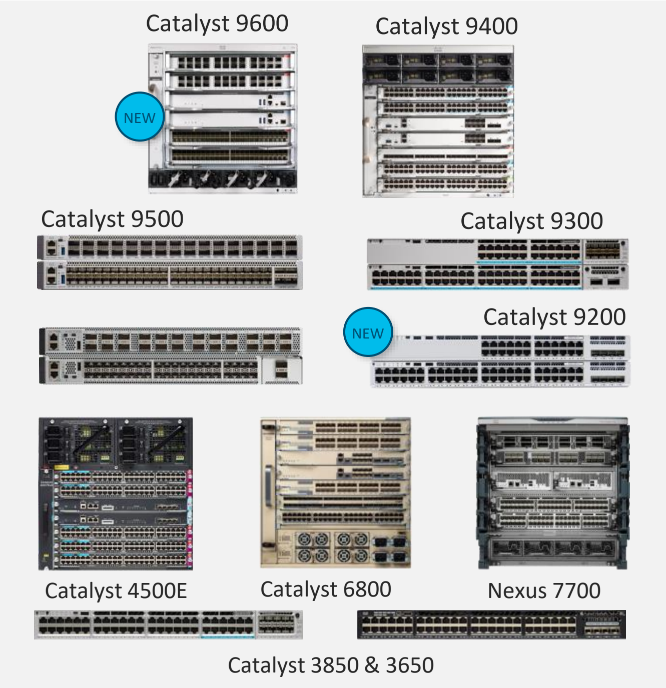
- Study SD-Access Design & Deploy CVD
- Create NRD & HLD designs for each Site
- Prepare your designs for SDA Multi-Site

SD-Access Support

Digital Platforms for your Cisco Digital Network Architecture

For more details: cs.co/sda-compatibility-matrix

Switching



Catalyst 9600

Catalyst 9400

Catalyst 9500

Catalyst 9300

Catalyst 9200

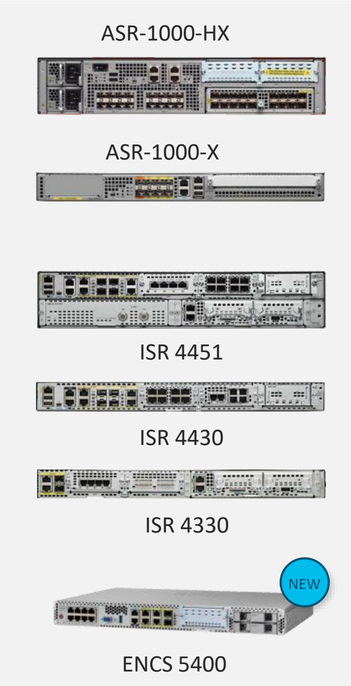
Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3850 & 3650

Routing



ASR-1000-HX

ASR-1000-X

ISR 4451

ISR 4430

ISR 4330

ENCS 5400

Wireless

Catalyst 9800

Catalyst 9100 APs

AIR-CT8540

AIR-CT3504

AIR-CT5520

Aironet
Wave 1 APs*

Aironet
Wave 2 APs

Extended

Cisco Digital Building

Catalyst 3560-CX

Cisco IE 3K/4K/5K

SD-Access Resources

Would you like to know more?

cisco.com/go/dna

cisco.com/go/sdaccess

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

cisco.com/go/cvd

- SD-Access Design Guide
- SD-Access Deployment Guide
- SD-Access Segmentation Guide

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

MENU
CISCO
Don't worry–we're here to get you caught up on what you missed at the Wired for Wireless event. Watch recording
Watch overview video
Read news blog
Benefits
What's inside
Case Studies
Resources
For Partners
Contact Cisco

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.

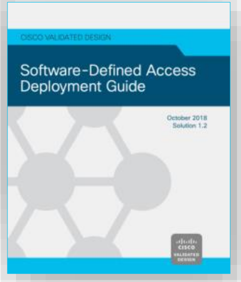
Improve the workforce experience

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

CISCO VALIDATED DESIGN

Software-Defined Access Design Guide

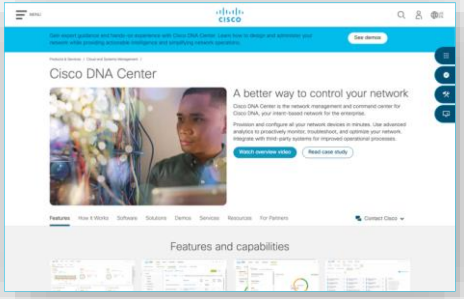
December 2018
Solution 1.2



CISCO VALIDATED DESIGN

Software-Defined Access Deployment Guide

October 2018
Solution 1.2



Get 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.

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

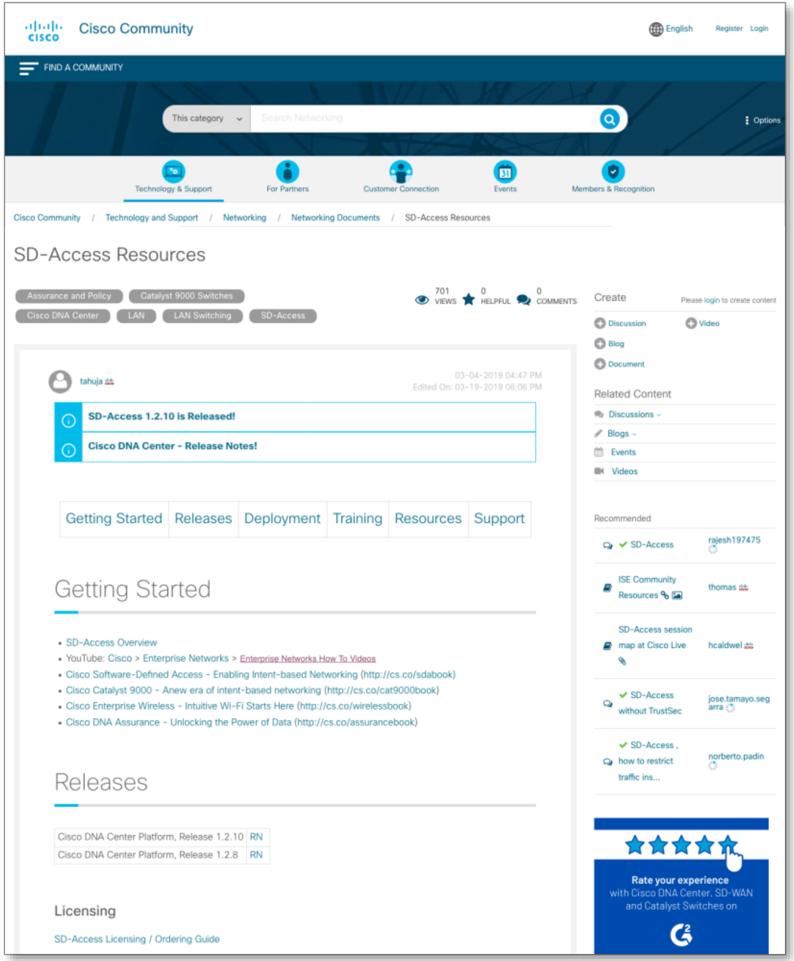
SD-Access Resources

Would you like to know more?

cs.co/sda-resources

cs.co/sda-community

- Search from your Browser
- Indexed by Search Engines
- Discuss with Experts & Friends
- Supported by SD-Access TMEs
- 24-hour First-Response Time
- Questions are marked Answered



Cisco Community / Technology and Support / Networking / Networking Documents / SD-Access Resources

SD-Access Resources

Assurance and Policy · Catalyst 9000 Switches · Cisco DNA Center · LAN · LAN Switching · SD-Access

701 VIEWS 0 HELPFUL 0 COMMENTS

tahuja

03-04-2019 04:47 PM
Edited On: 03-19-2019 06:06 PM

SD-Access 1.2.10 is Released!

Cisco DNA Center - Release Notes!

Getting Started | Releases | Deployment | Training | Resources | Support

Getting Started

- SD-Access Overview
- YouTube: Cisco > Enterprise Networks > Enterprise Networks How To Videos
- Cisco Software-Defined Access - Enabling Intent-based Networking (http://cs.co/sdabook)
- Cisco Catalyst 9000 - Anew era of intent-based networking (http://cs.co/cat9000book)
- Cisco Enterprise Wireless - Intuitive Wi-Fi Starts Here (http://cs.co/wirelessbook)
- Cisco DNA Assurance - Unlocking the Power of Data (http://cs.co/assurancebook)

Releases

Cisco DNA Center Platform, Release 1.2.10	RN
Cisco DNA Center Platform, Release 1.2.8	RN

Licensing

SD-Access Licensing / Ordering Guide

Create — Please login to create content

Discussion · Video · Blog · Document

Related Content

- Discussions
- Blogs
- Events
- Videos

Recommended

✓ SD-Access	rajesh197475
ISE Community Resources	thomas
SD-Access session map at Cisco Live	hcaldwel
✓ SD-Access without TrustSec	jose.tamayo.segarra
✓ SD-Access , how to restrict traffic ins...	norberto.padin

Rate your experience with Cisco DNA Center, SD-WAN and Catalyst Switches on

Learn more with Learning@Cisco

http://digital-learning.cisco.com

CISCO CERTIFIED CCIE

	SD-Access Fundamentals - Customer	URL
1	**Getting Started with Cisco DNAC Assurance (A-ADNAC-ASSUR) v1.0** Installing Cisco DNA Center Overview, Setting Up Wireless Assurance	https://digital-learning.cisco.com/course/60049
2	**Preparing the Identity Services Engine (ISE) for SDA (CUST-SDA-ISE) v1.0** TrustSec, ISE with DNAC, Device Profiling and Creating Groups and Policies	https://digital-learning.cisco.com/course/59741
3	**Planning and Deploying SDA Fundamentals (CUST-SDA-FUND) v1.0** Campus Fabric, Wireless, Guest Access, Underlay, Micro Segmentation, Multicast	https://digital-learning.cisco.com/course/59740
4	**SDA 1.2 Update (A-SDA-12UPDT)** SD-Access Extensions and SD-Access for Distributed Campus	https://digital-learning.cisco.com/course/59933
5	**Cisco DNA Center Fast Start Use Cases (A-SDA-FASTSTART)** Installing Cisco DNA Center Release 1.2.6, Demos on Deploying Wireless Assurance and SD-Access	https://digital-learning.cisco.com/course/60874

Special offering: ✓ Curriculum is **FREE** to customers ✓ Earn up to **25 Points** for CCIE CEP!! ✓ Over **33 hours** of video instruction

SD-Access Testimonials

Live Customer SD-Access Deployments

wipro

TEXAS A&M UNIVERSITY

JADE HOCHSCHULE
Wilhelmshaven Oldenburg Elsfleth

IBM
Network Services

AstraZeneca

RoyalCaribbean INTERNATIONAL

70 Years of Beauty Creation
AMOREPACIFIC

750+
Production
Deployments

UoN University of Northampton

ALABAMA GREAT SEAL

SAFETY TREATMENT RESPONSIBILITY
DEPARTMENT OF STATE HOSPITALS

MONTANA STATE UNIVERSITY 1893 BOZEMAN - MONTANA

felixplatterspital

Children's Hospital LOS ANGELES
We Treat Kids Better

DB BAHN

SCENTSY

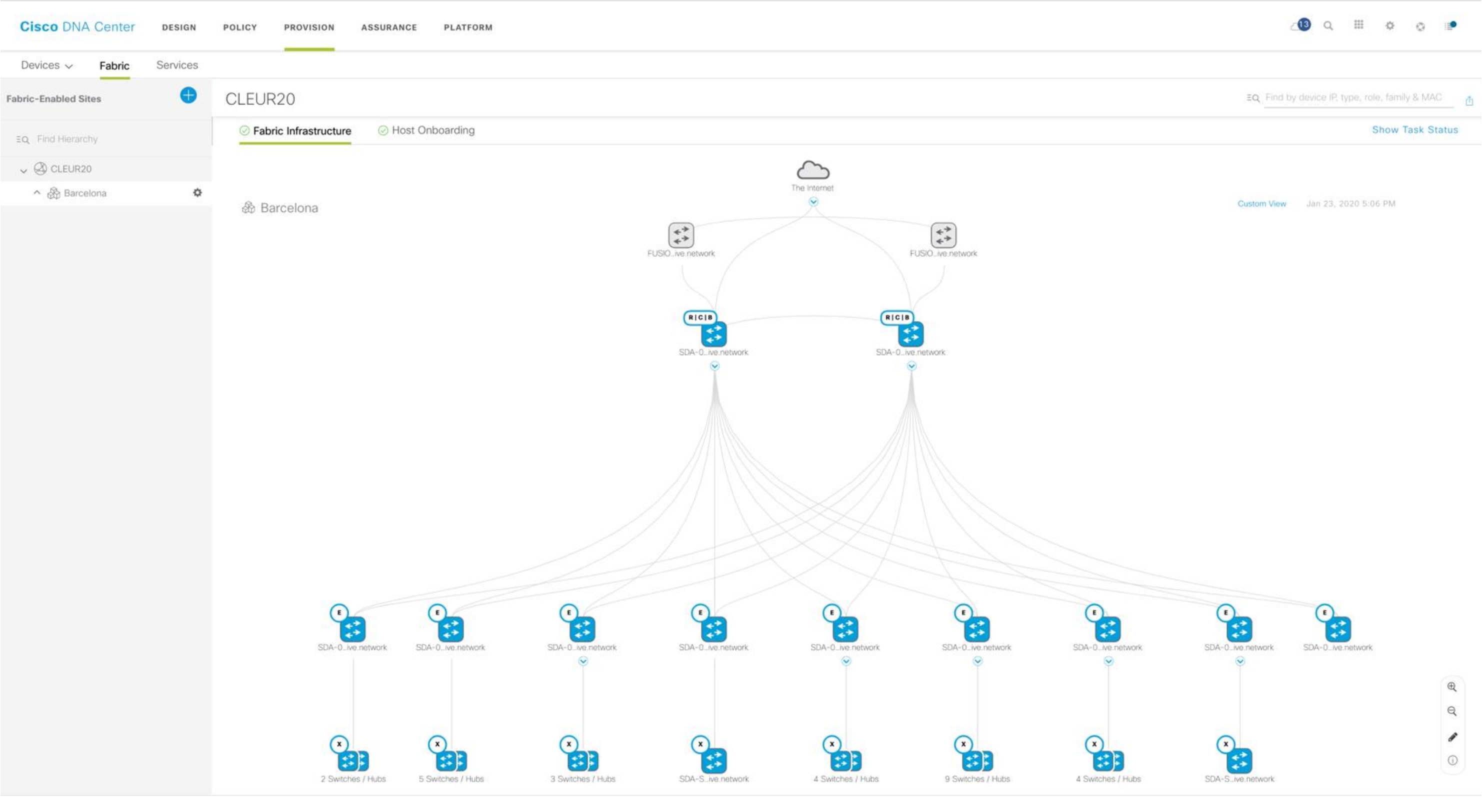
CISCO
Cisco IT

cisco Live!

www.cisco.com/c/en/us/solutions/enterprise-networks/network-architecture-customer-success-stories.html

SD-Access @ CiscoLive Barcelona

Cisco DNA Center with SD-Access Fabric – Hall 5.0



Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Thank you

You make **possible**