

CISCO *Live!*



#CiscoLive



The bridge to possible

Cross and Multidomain Integrations for SDA and ACI

Markus Harbeck Principal Architect – CX PM Cross Domain
@mhgrisu
BRKXAR-2002

CISCO *Live!*

#CiscoLive

CCIE #8087
CCDE #20130015



Cisco Webex app

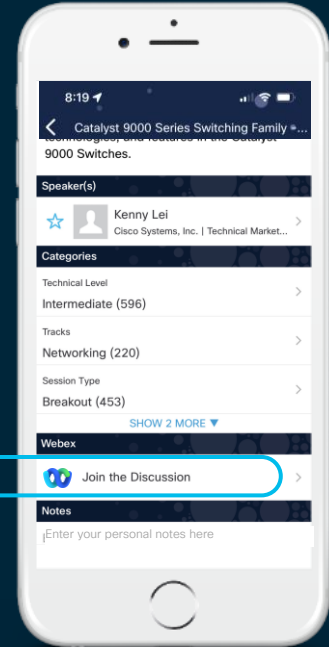
Questions?

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

How

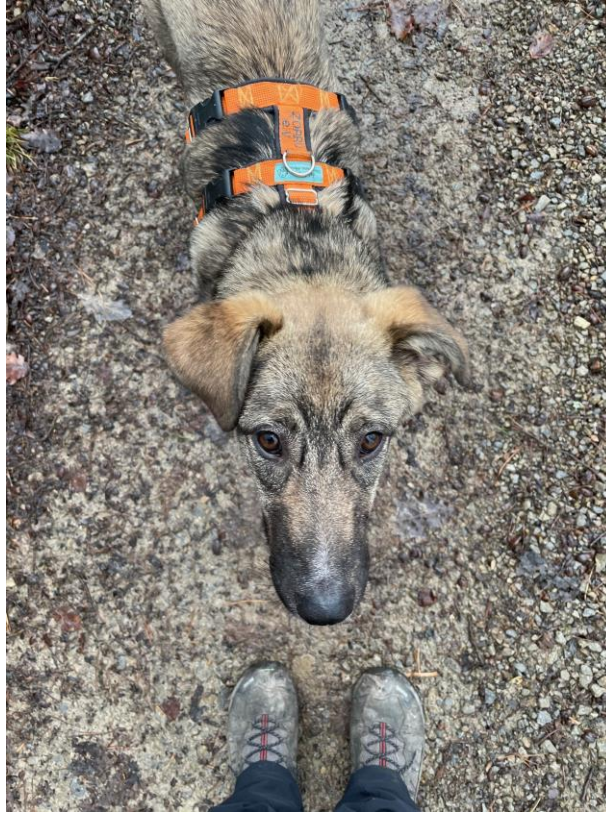
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXAR-2002>

Multidomain




Integrating Campus and Data Center automation let you focus on what really matter
→ Where is the dog ?



Agenda

- SDA – ACI overview – THE WHY!
- What is needed for SDA – ACI integration?
- Policy across SDA and ACI
- How is the integration achieved?
- Summary



Short Hint:
*“My English might be bad
but although sexy”*

Source: Henning Bornemann –
“Thank you for Deutsche Bahn”

Who has the following challenges?



Integrate and Automate NNI between SDA and ACI

Examples: SDA to ACI how can I transport my Group Tag



Applying and enforcing consistent policy constructs across enterprise

Examples: Maintaining the identity from the edge across IT



End to End Visibility between SDA and ACI

Example: ensure NNI / Border hand off is in healthy conditions

The Intent Evolution by my kids

2013

Do you recognize your network?

2015

Can you automate this Network?

2019

Integration and Multidomain

2022

End to End IT
Campus via WAN to Cloud and DC

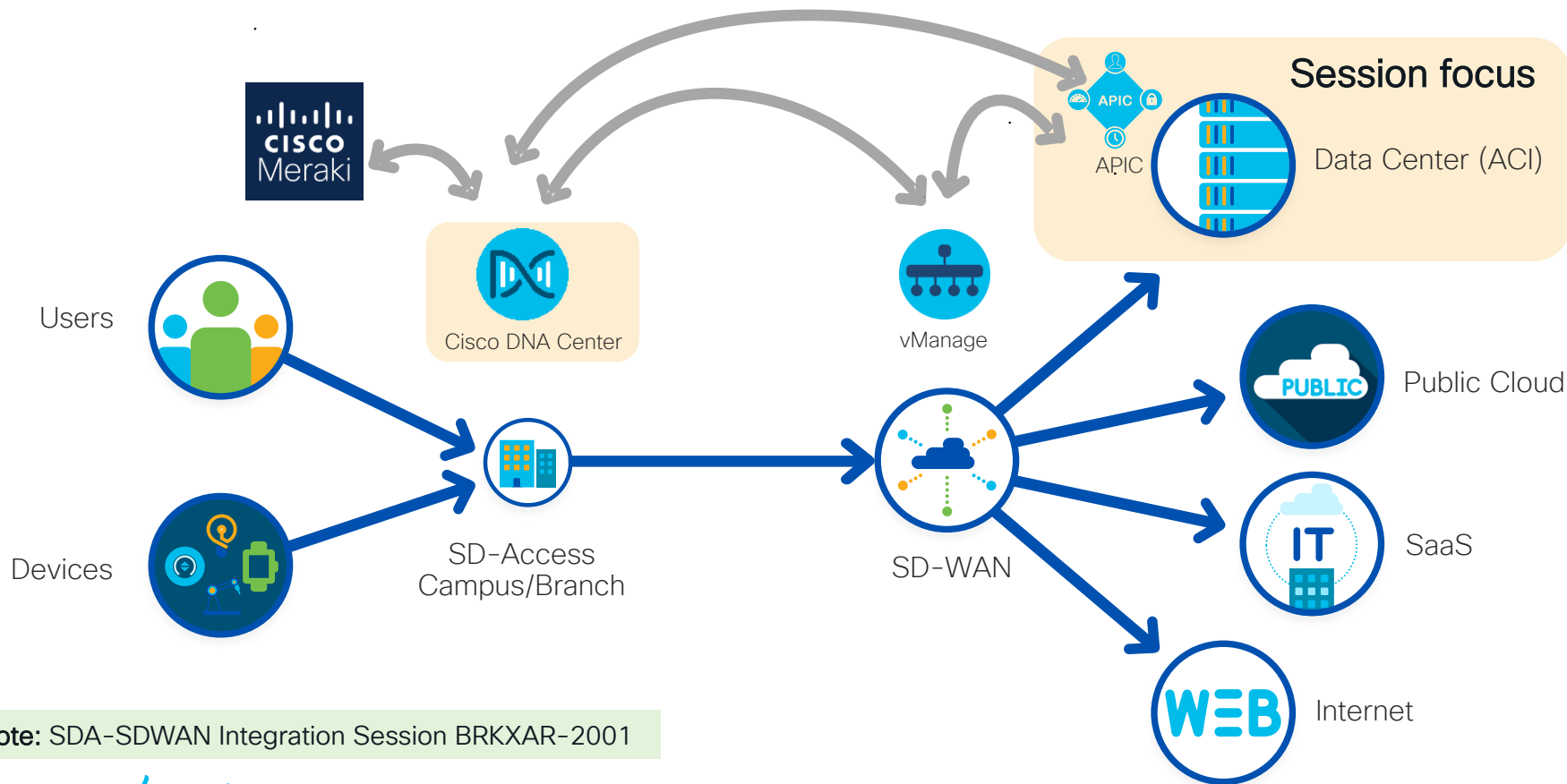


Copyright by Saskia



Copyright by Hanna

Cisco provides pairwise domain integrations today



Note: SDA-SDWAN Integration Session BRKXAR-2001

Who is Markus Harbeck?

Personal:

- Location: Eschborn, Germany (near Frankfurt) but lives in Bavaria
- Interests: My family, my 2 kids, Horse back riding, motor cycling, hiking

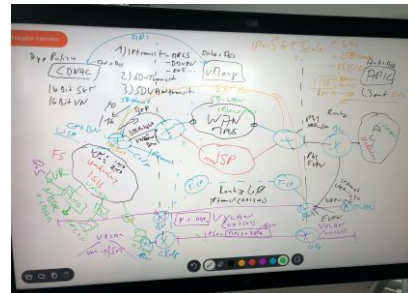
My Background:

- CLI Junkie since 1996 for all Routing and Switching
- Joined CISCO October 2010
- Before; 12 years, operations, engineering, application engineering at Lufthansa Systems (Airline)
- Book Author – Cisco DNA Assurance 2018
- Close Customer relations and interlock
- Tiger Teams and BU Advisor

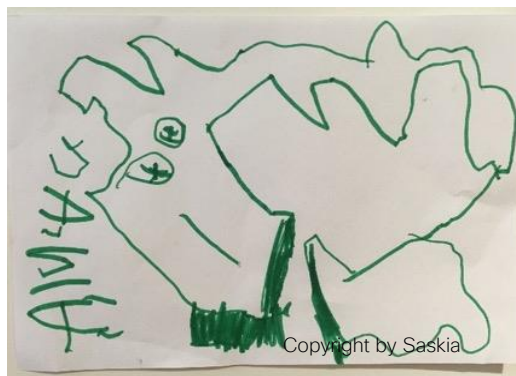
Current Projects:

- X – Domain / Architecture
- Orchestration and X Domain
- End to End Observability
- Analytics, Assurance, Migration, Automation
- Services, Automation X, NG Analytics
- SDA, ACI, SDWAN, ITSM, Secure Remote Workforce
- Cisco DNA Center since day1 in 2014

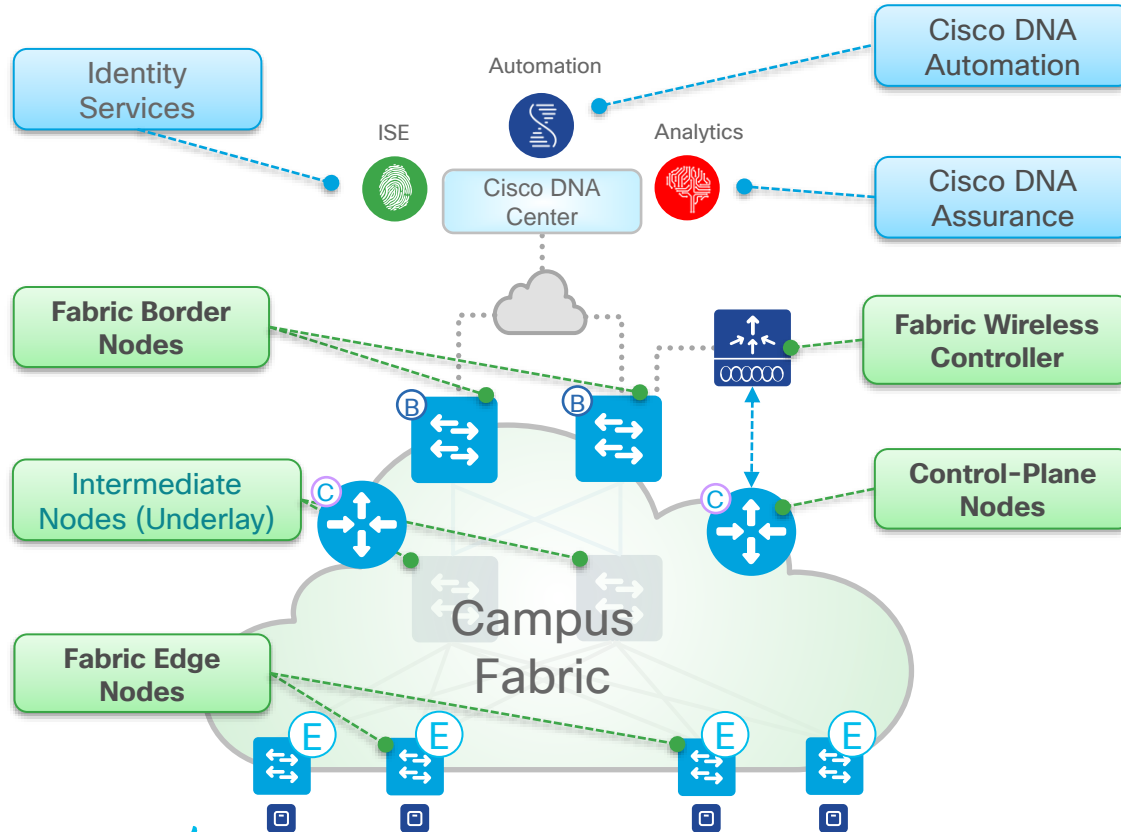
My Kids view on Cisco DNA Center and Network Design



CCIE #8087
CCDE #20130015

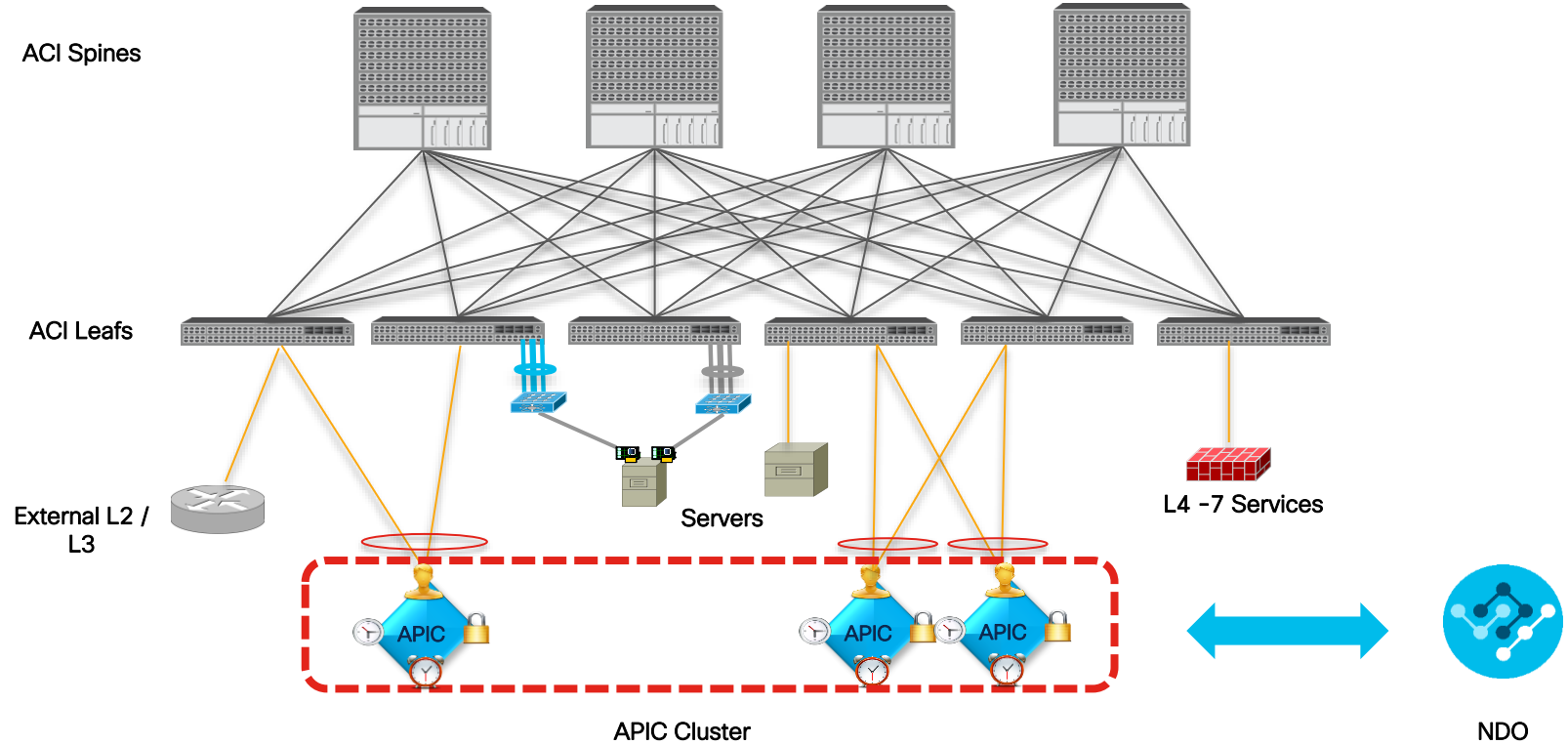


Fabric roles & terminology

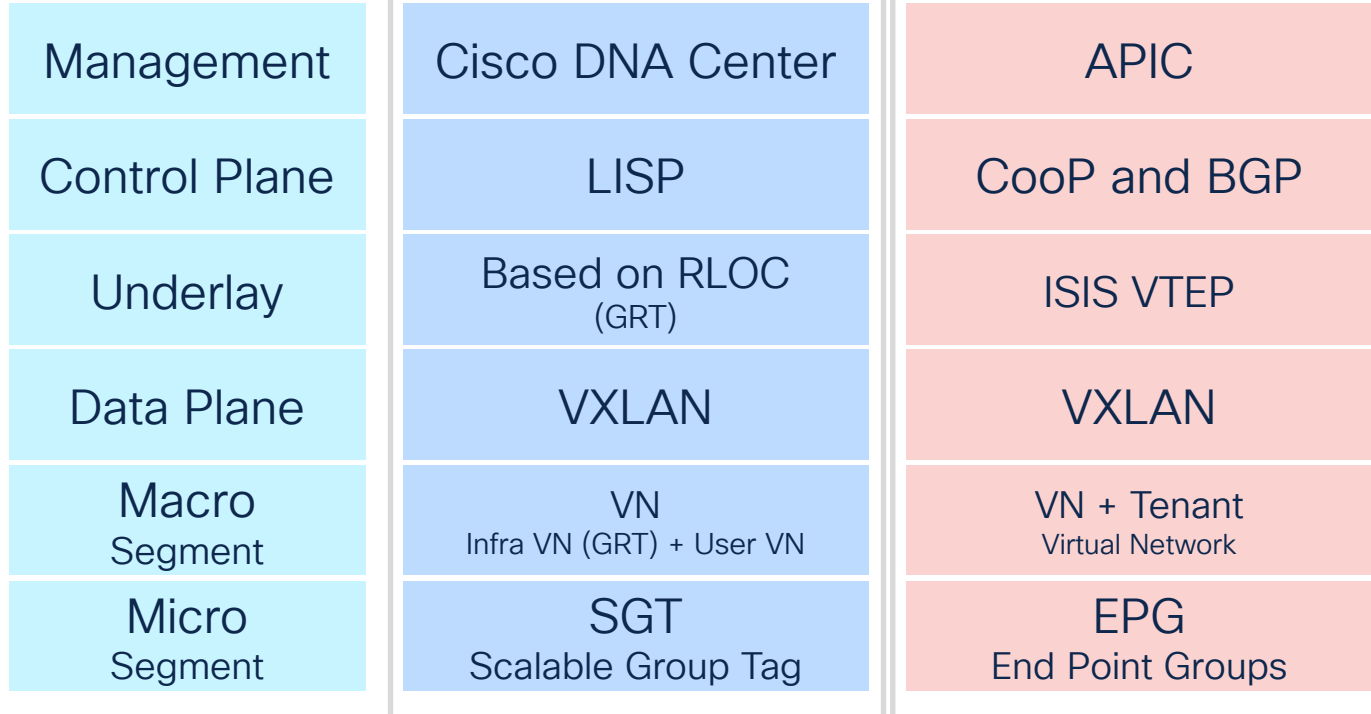


- **Cisco DNA Automation** – provides simple GUI management and intent based automation (e.g. NCP) and context sharing
- **Cisco DNA Assurance** – Data Collectors (e.g. NDP) analyze Endpoint to App flows and monitor fabric status
- **Identity Services** – NAC & ID Systems (e.g. ISE) for dynamic Endpoint 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 SDA Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects APs and Wireless Endpoints to the SDA Fabric

ACI



SDA and ACI together



What is SDA – ACI integration



SDA and ACI



Solution 1.0
Policy Plane



Solution 3.0
Data Plane

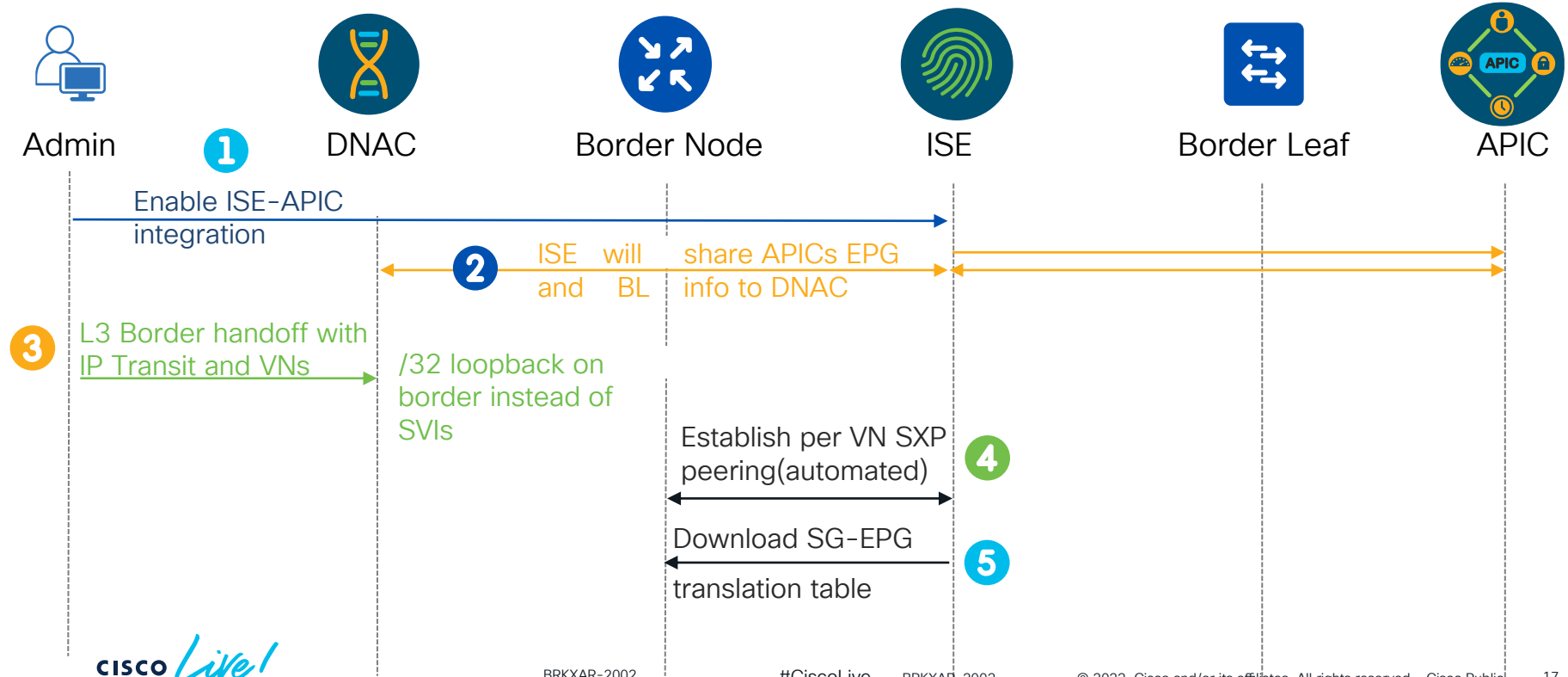
What happened to phase 2



Day 0 operations for 1.0

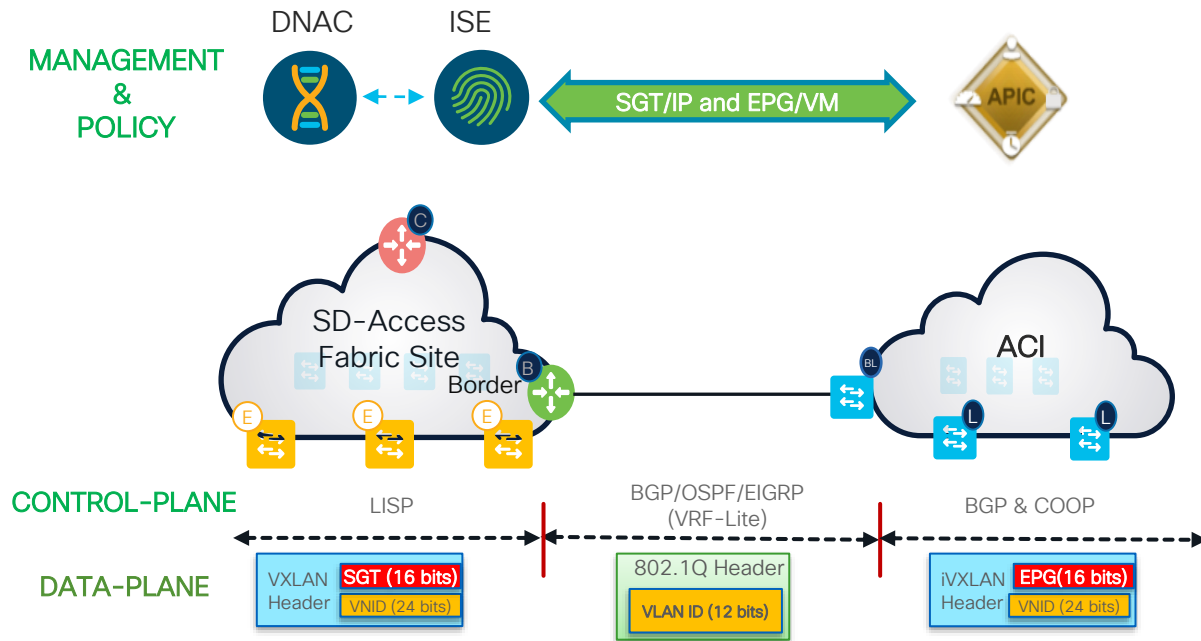
Pre-requirements:

pxGrid between DNAC and ISE is running



ACI and SDA pairwise integration phase 1

SDA-ACI: Group/Identity Mapping Federation



API Based Cross Domain Identity Federation

Group and Group Membership {IP, group} communicated between the domains via APIC API

ISE acts as the API initiator and registers for ACI attach/detach events

Control Plane

Single VRF BGP/OSPF/EIGRP (MP-BGP is not supported in this phase)

Data Plane

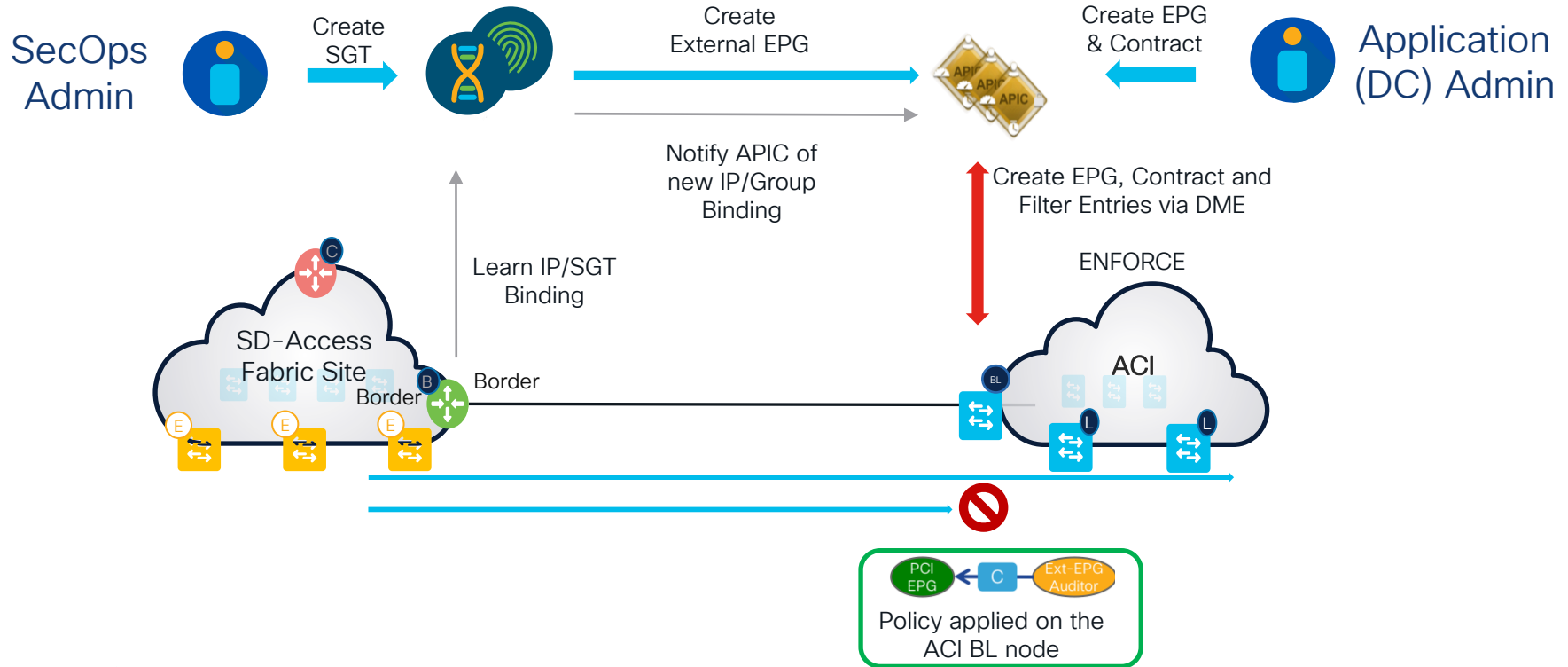
802.1Q between the domains, VXLAN with 2 labels (VNID and ClassID) internal to the domains

- DNA Version 1.2.10 and later
- ISE Version 2.4 Patch 6 and later

- ACI 3.2 and later

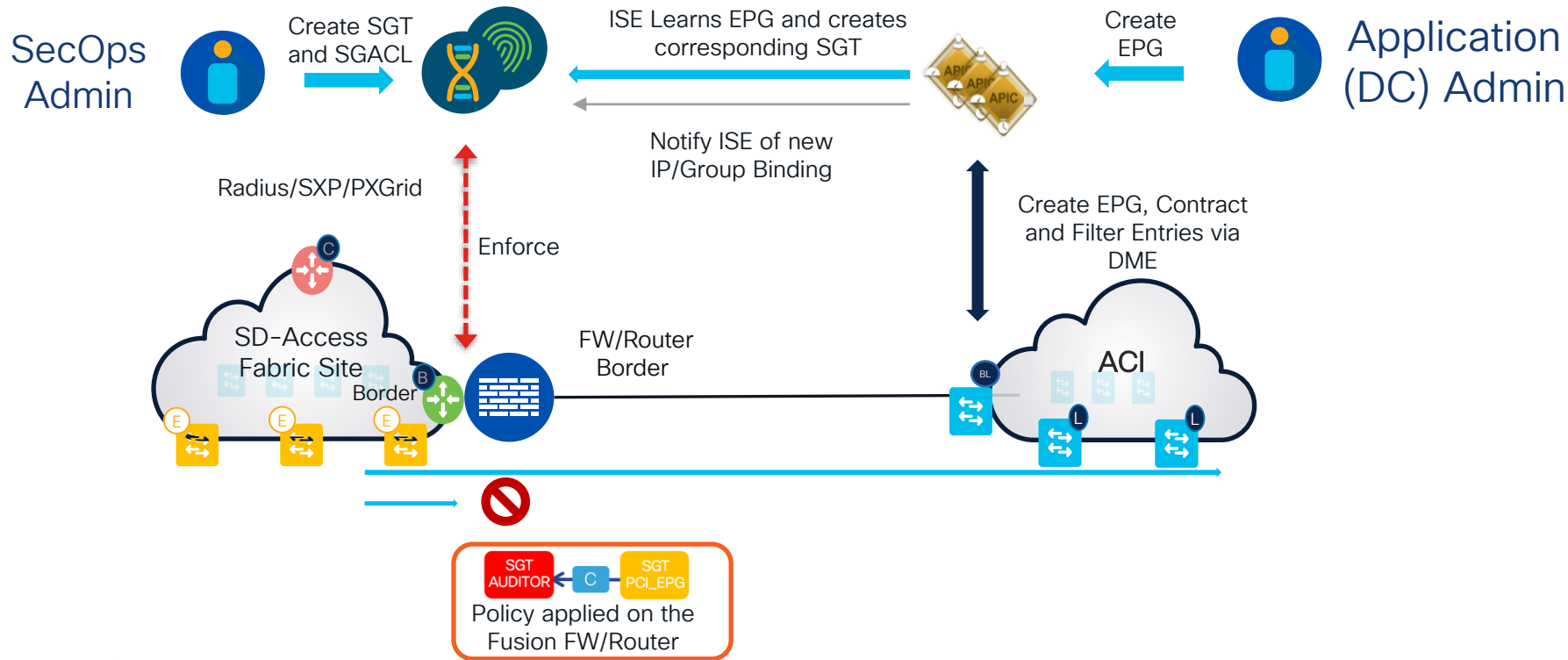
ACI and SDA pairwise integration phase 1

Policy applied on **ACI Border** (option 1)



ACI and SDA pairwise integration phase 1

Policy applied on Fusion Router/Firewall (option 2)



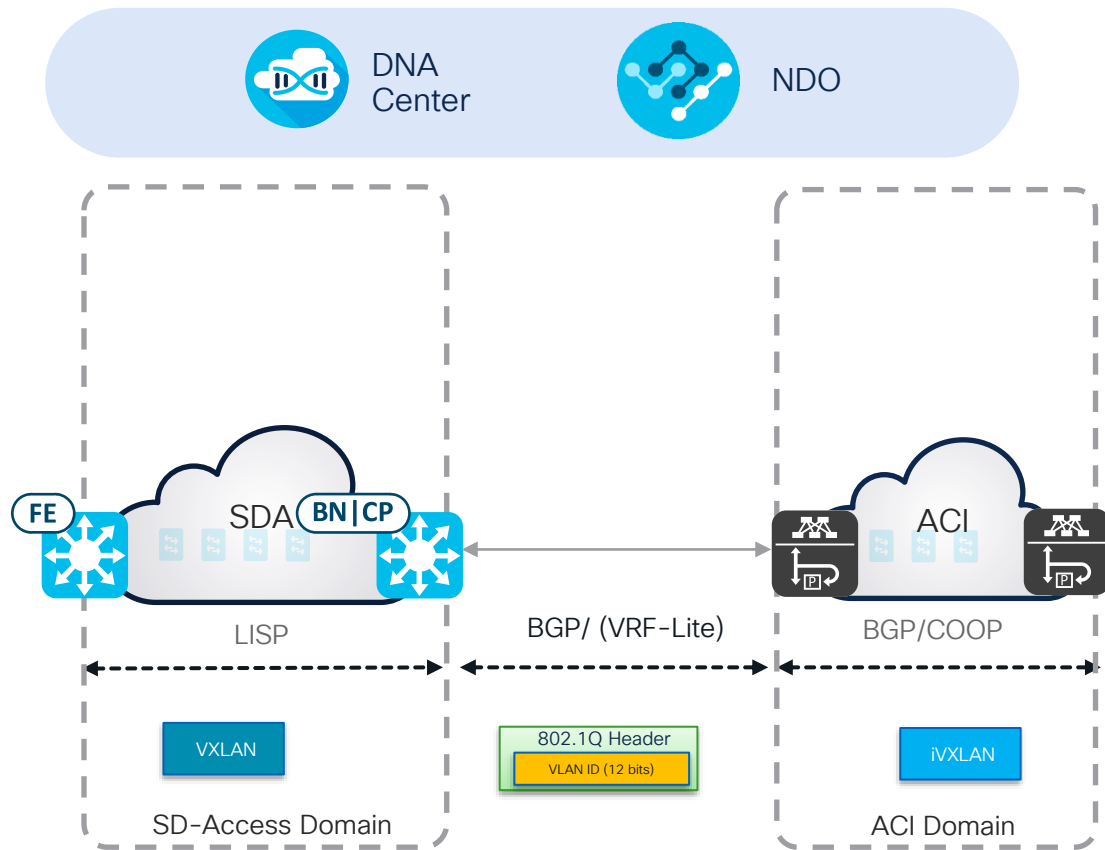
ACI-SDA phase 3.0 Macro-segmentation

Cisco SD-Access and Cisco ACI integration 3.0

Macro segmentation

Use Case

Secure the network with automated provisioning of end-to-end macro-segmentation between the Campus and DC domains

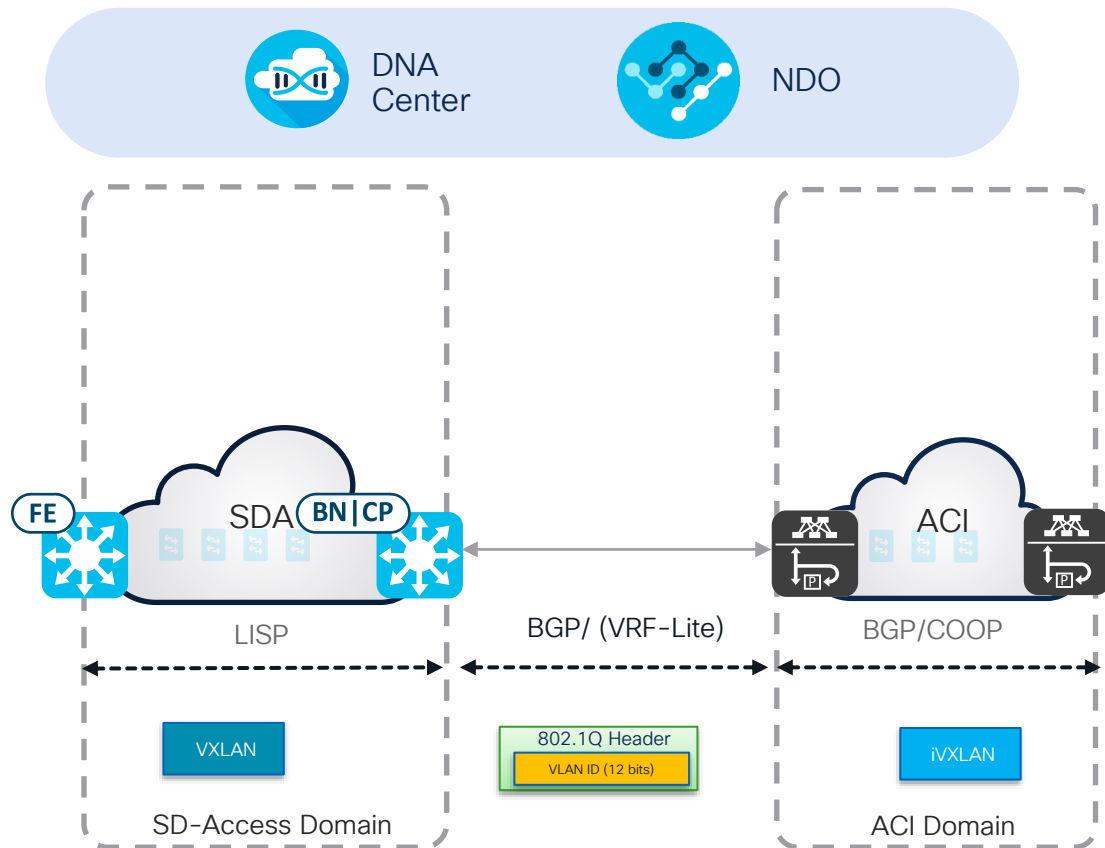


Cisco SD-Access and Cisco ACI integration 3.0

Macro segmentation

Details

- Automate connectivity end-end at VN level
- VN to VRF Connectivity Automation
- Allows automatic stitching of Campus VNs to Multi-DC VRFs
- DNA Center and NDO integrated
- Macro Segmentation (VRF Granularity)
- Cross-domain operational visibility
- Cross-domain peering status
- Verify campus networks reachable from DC



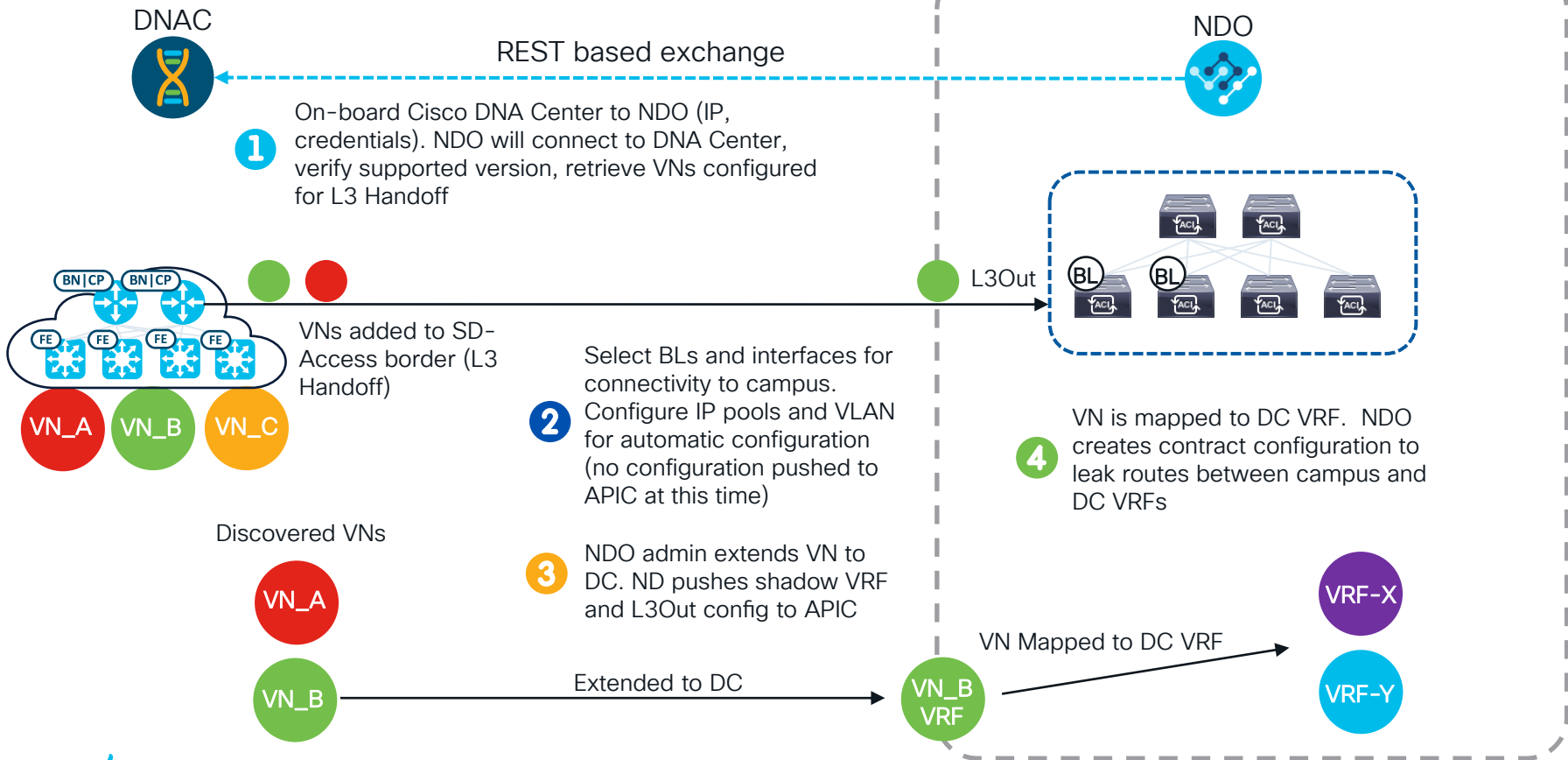
Solution components/supported versions

Product	Supported Versions
ACI	4.2(4) and later
Nexus Dashboard Orchestrator	3.7(1g) and later
Cisco DNA Center	2.3.3 and later

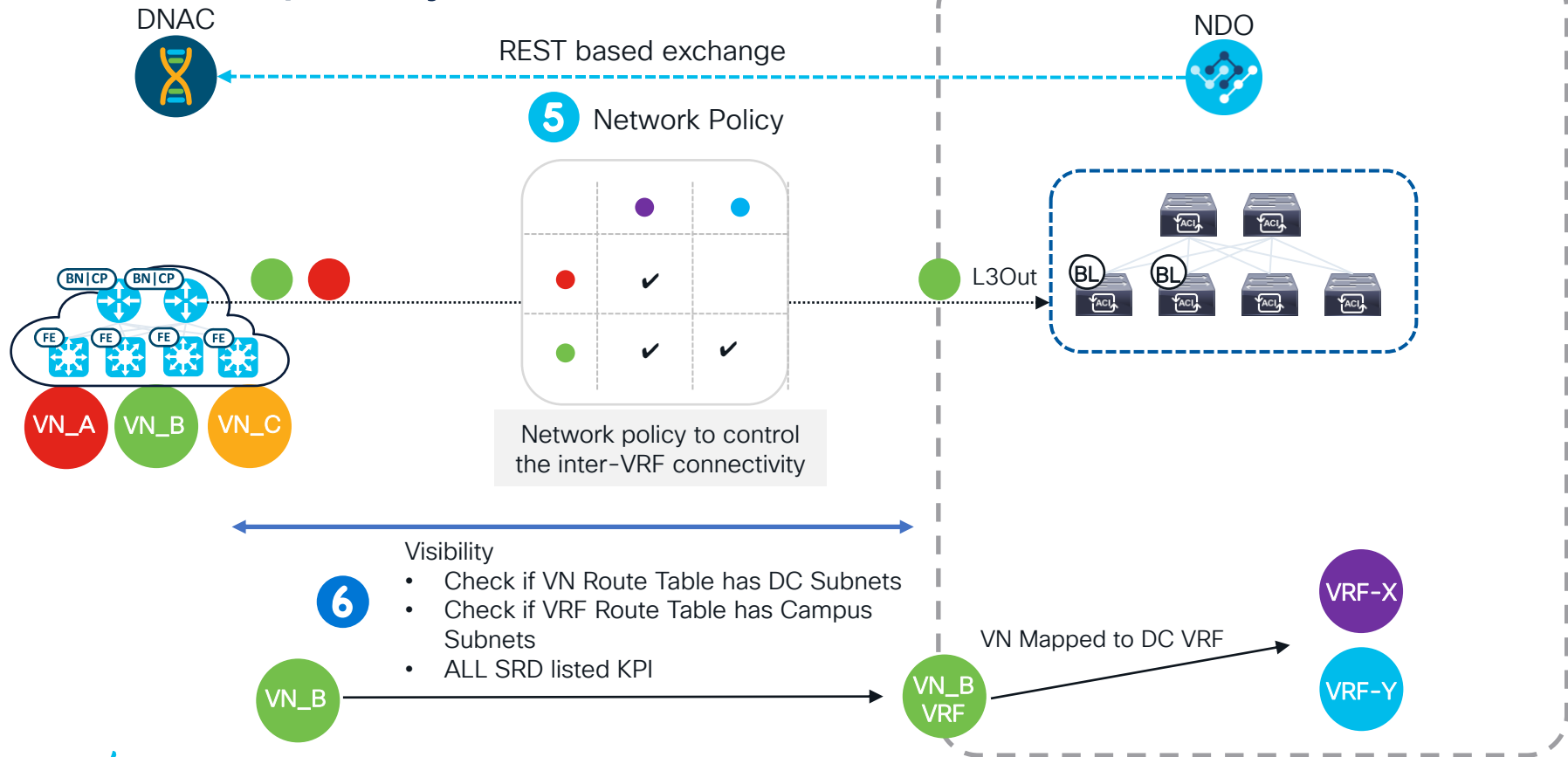
Topologies:

- Multi-campus (supports SDA and non-SDA)
- Multi-DC with Nexus Dashboard Orchestrator
- DMZ/Transit FW option between DC and Campus

Enablement workflow



Network policy



Integrating Campus and Data Center automation let you focus on what really matter -> Where is the dog ?



Demo time

Cisco SDA – ACI integration

Cisco DNA Center



Policy



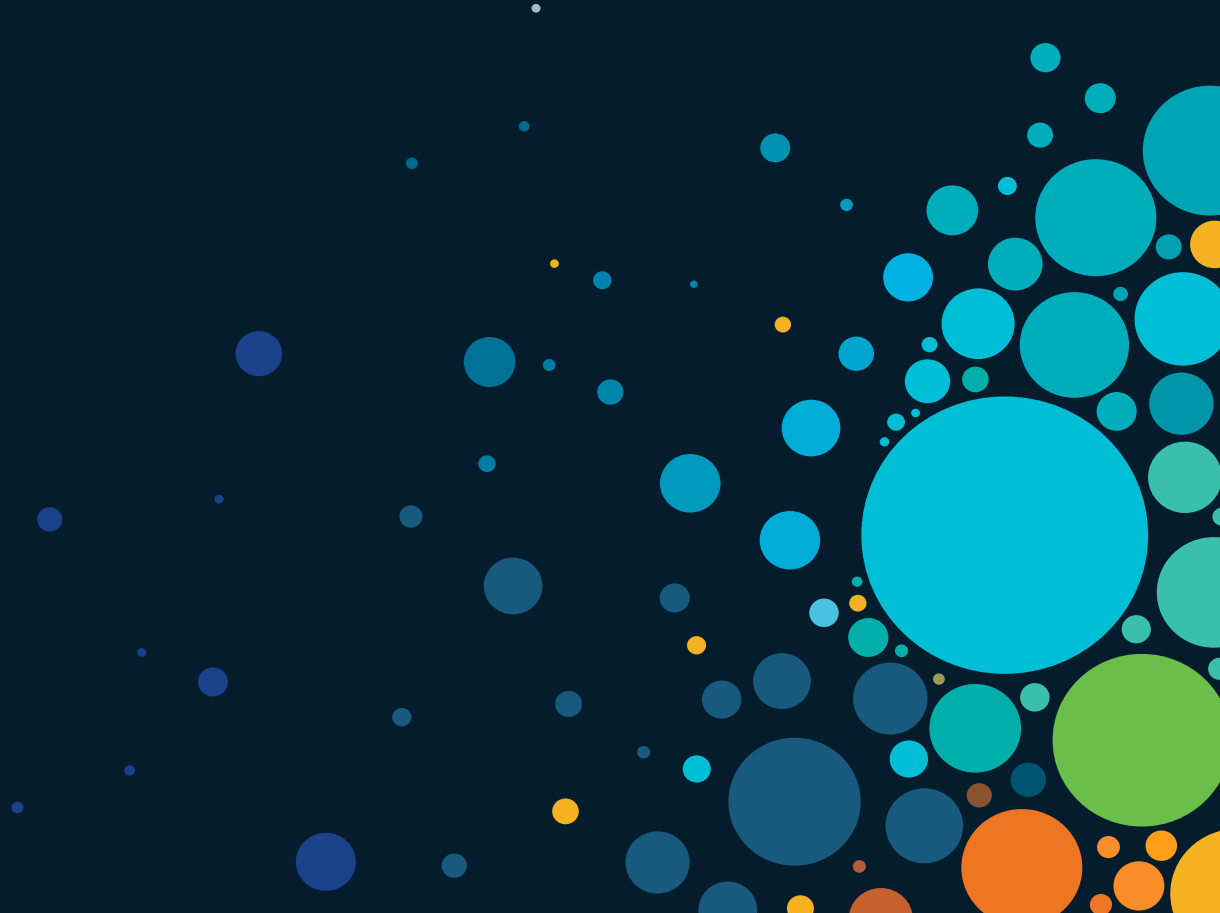
Automation



Analytics



Supported topologies

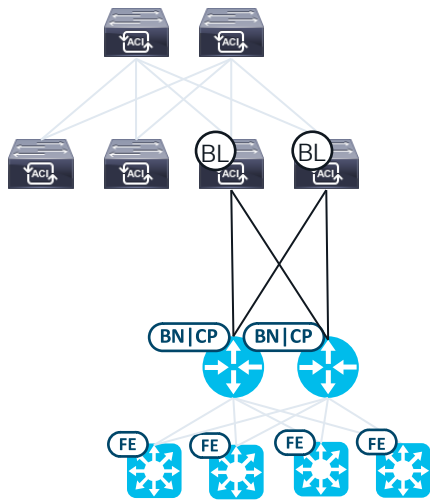


Inter-domain peering

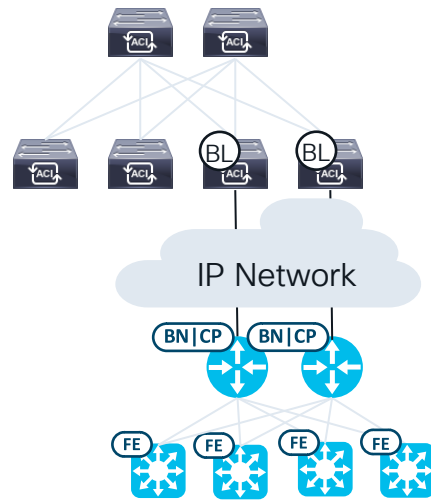
Supported configurations

Campus borders can be directly connected to ACI border leaf switches or over an intermediate network.

Direct back-to-back connections

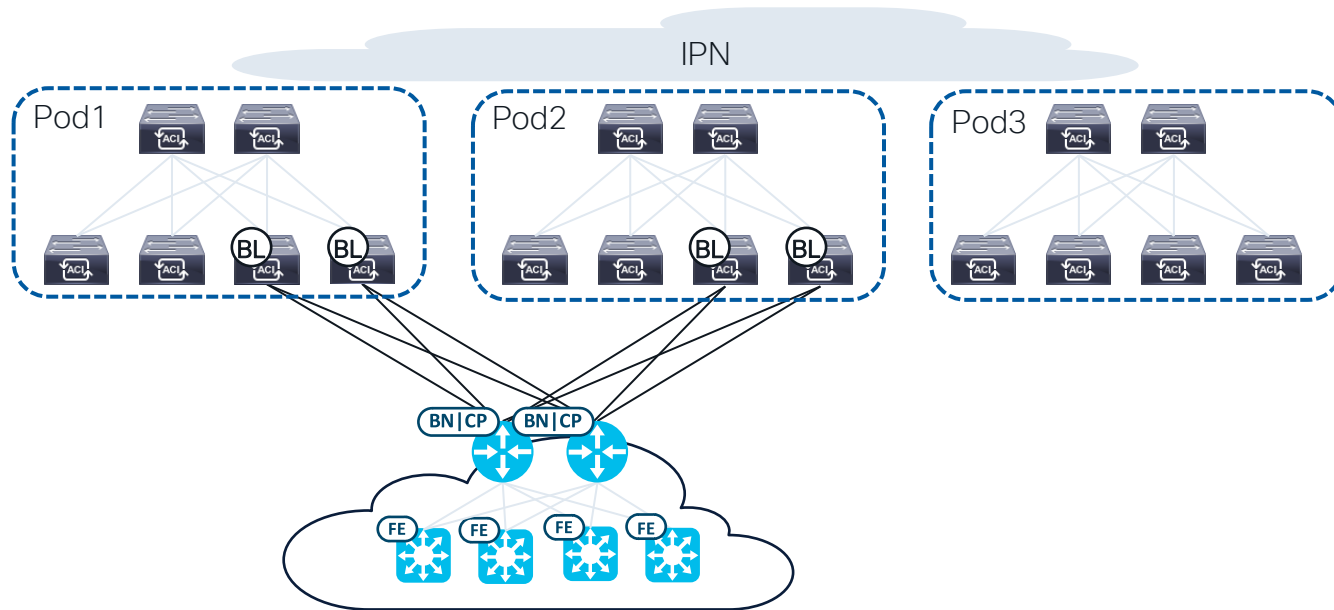


Connected via an IP network



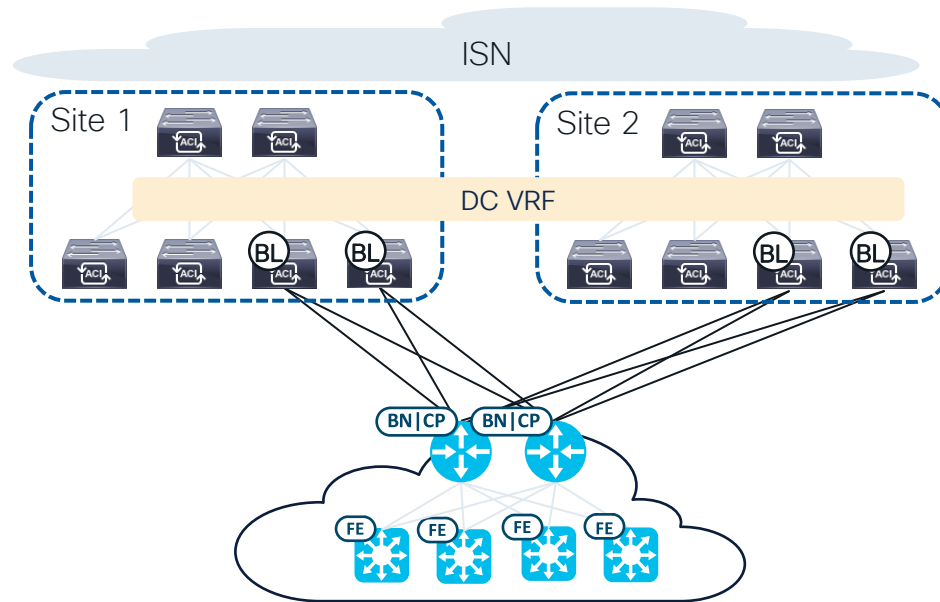
Supported DC topologies

- Border leaf switches from multiple pods is supported
- It is not required to have a BL to campus peering from all pods



Supported DC topologies

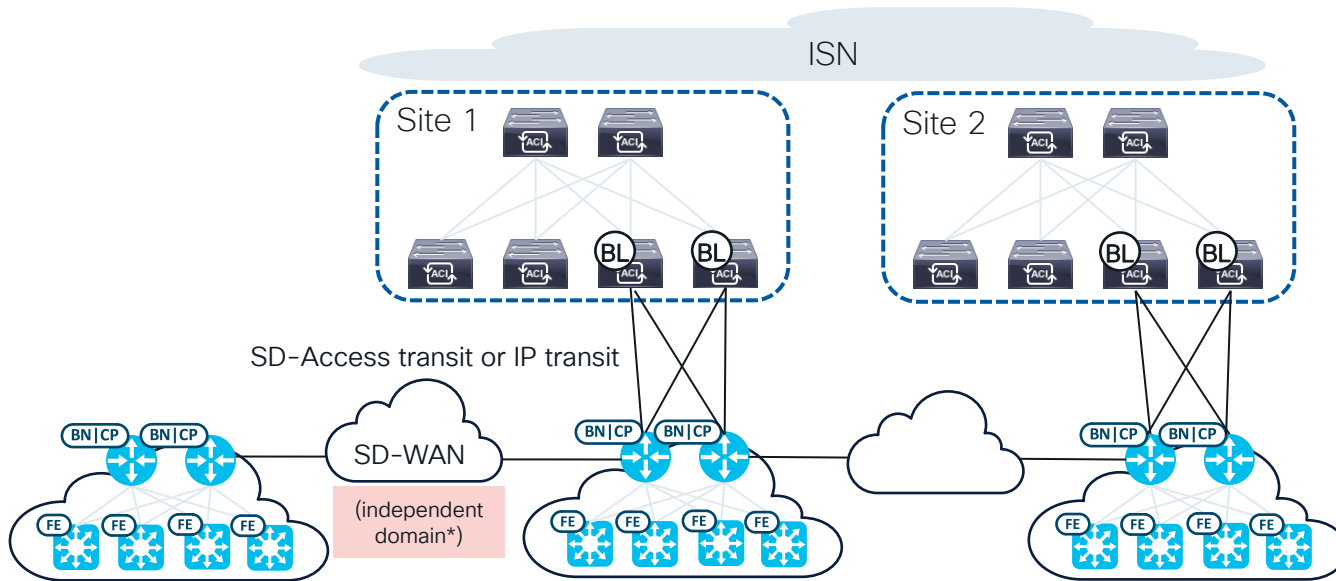
- When DC VRF is stretched across sites, each site must peer to campus borders



Supported Campus topologies

Multi Site

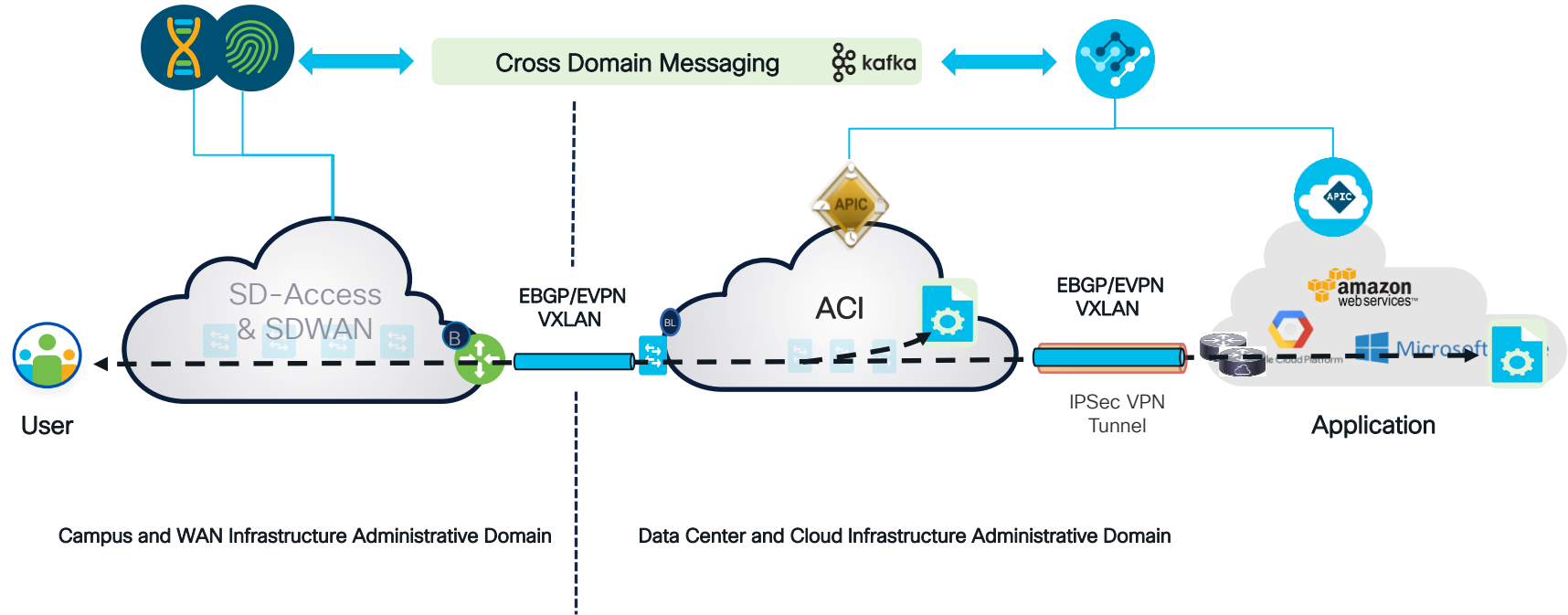
- Campus sites do not need to peer directly to DC border leaf switches
- Remote campus sites can connect to peering campus site over SD-Access transit or IP transit



*The SD-WAN domain in this example is an independent domain and not integrated with the SD-Access domain *Refer to BRKXAR-2001*

Multi-Cloud Data Center is Multi-Domain Capable

Connect any user to all applications



How does
everything else fit ?

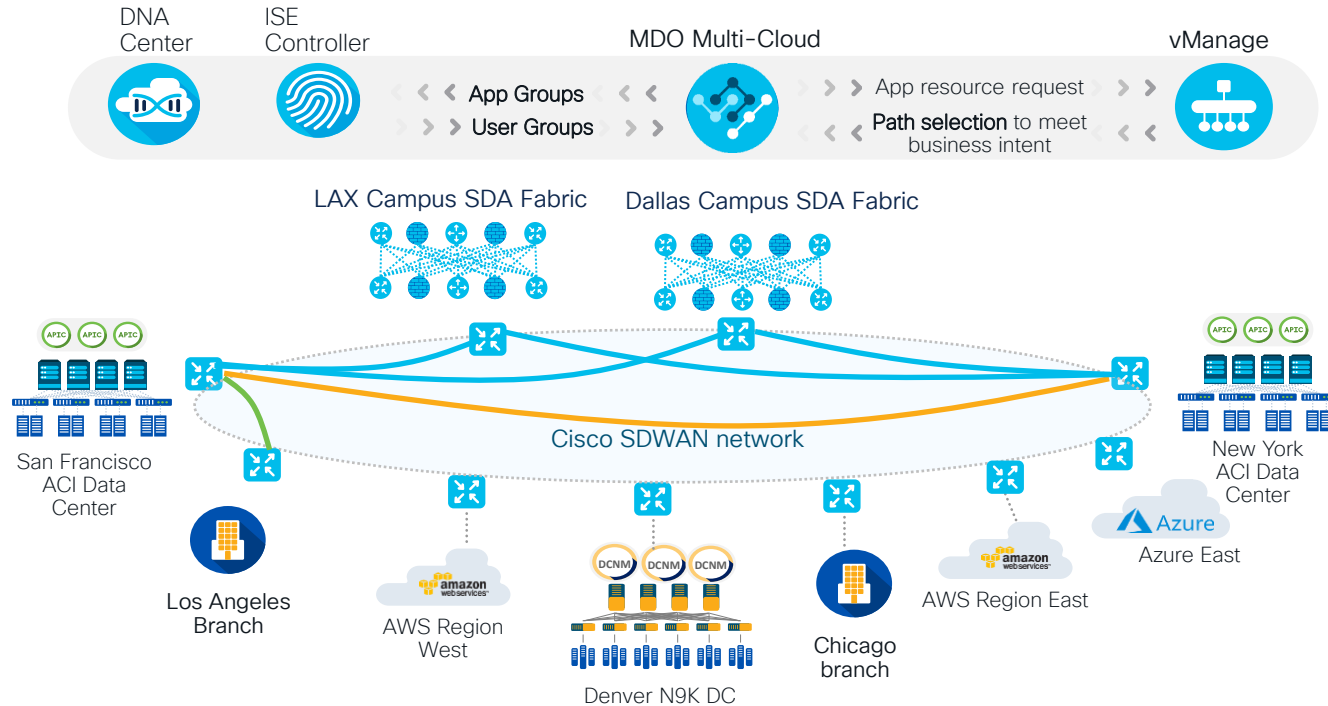


Integrating Campus and Data Center automation let you focus on what really matter -> Where is the dog ?



It is a little step with huge impact

Extending the integrations



Summary



ACI SDA resources

Would you like to know more?



For your
reference



Products and Services

Solutions

Support

Learn

Explore Cisco

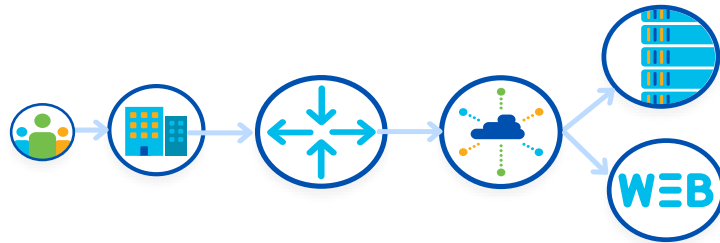
Home / Support /

Cisco ACI Multi Domain Connector and Multi Domain Manager User Guide, Release 1.0

[ACI-SDA 3.0 Guide](#)

Next steps

1. Experience the Integrated network – try it out
2. Enable End 2 End Automation and Analytics
3. Enable Security End 2 End
4. Leverage your installed base



User – Connection – Application

As Angus said:
Have a drink on me



Technical session surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

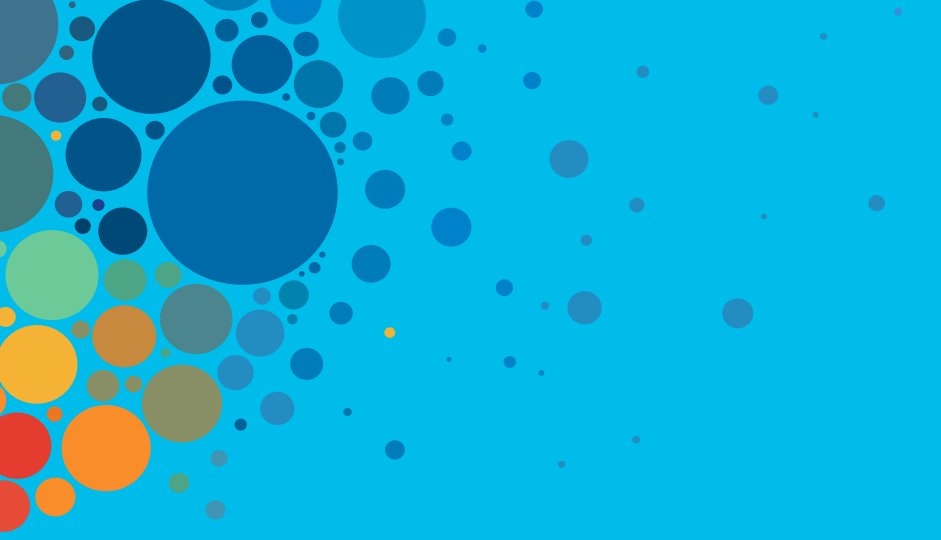
Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive