cisco Live!

#CiscoLive

The bridge to possible

Lessons Learnt from Large Multi-Domain IBN Architectures

SD-Access, SD-WAN and ACI

Dhrumil and Jeremy

BRKENS-3832

Cisco Webex App

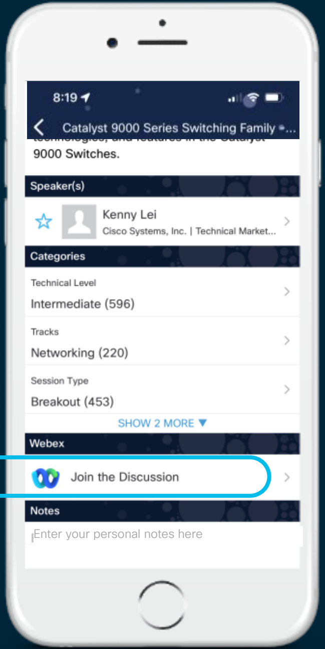
Questions?

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.



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-3832

Agenda

- Introduction
- Design and Deployment Best Practices
  - SDA & SDWAN Integration
  - SDA and ACI Integration
  - SDWAN and ACI Integration
  - 100,000ft view on Multi-Domain Design
- Deployment and Migration Lessons Learned from Large Scale Deployments

Who are we?

CISCO CERTIFIED CCIE ROUTING AND SWITCHING

CISCO CERTIFIED CCIE SERVICE PROVIDER

CISCO CERTIFIED CCDE DESIGN

Dhrumil Prajapati

Sr. Delivery Architect

Technology and Transformation Group – CX

7+ Years @ Cisco

CCIE #28071 (R/S, SP)

CCDE #20210002

Specialized in: SD-Access, SD-WAN, MPLS, Campus LAN and WAN

@DhruPrajapati

Who are we?

Jeremy Bowman

Sr. Delivery Architect

Cisco CX

7+ Years @ Cisco

CCIE #51241 (R/S, Security)

CCDE #2018::16

Specialized in: Full Enterprise IBN with Security

@ciscojdb1

jdb1@cisco.com

Design and Deployment Best Practices

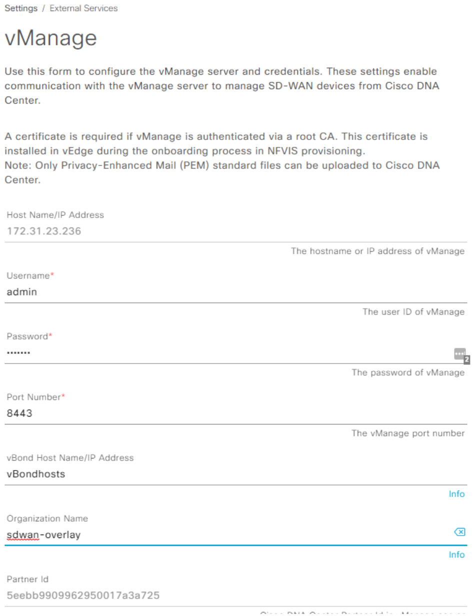
Why Multi-Domain?

- Individual architectures introduce
  - Segmentation
  - Automation
  - Within a single enterprise domain

- Multi-Domain Architectures
  - Extend Segmentation
  - Utilize orchestration
  - Make the entire enterprise one IBN enclave

What Is Involved In SDA & SDWAN Integration?

- Steps
  - DNAC and vManage integration
  - vManage owns each cEdge and assigns to DNAC
  - Provision SDA specific changes through DNAC, SDWAN specific changes via vManage
- Results
  - SDA VNs and SDWAN Service VPNs tied together
  - SDA SGT information propagated via SDWAN
  - cEdge participates in both fabric domains
  - Consistent application and security policy
  - API based communication between DNAC and vManage



Settings / External Services

vManage

Use this form to configure the vManage server and credentials. These settings enable communication with the vManage server to manage SD-WAN devices from Cisco DNA Center.

A certificate is required if vManage is authenticated via a root CA. This certificate is installed in vEdge during the onboarding process in NFVIS provisioning.
Note: Only Privacy-Enhanced Mail (PEM) standard files can be uploaded to Cisco DNA Center.

Host Name/IP Address
172.31.23.236
The hostname or IP address of vManage

Username*
admin
The user ID of vManage

Password*
•••••••
The password of vManage

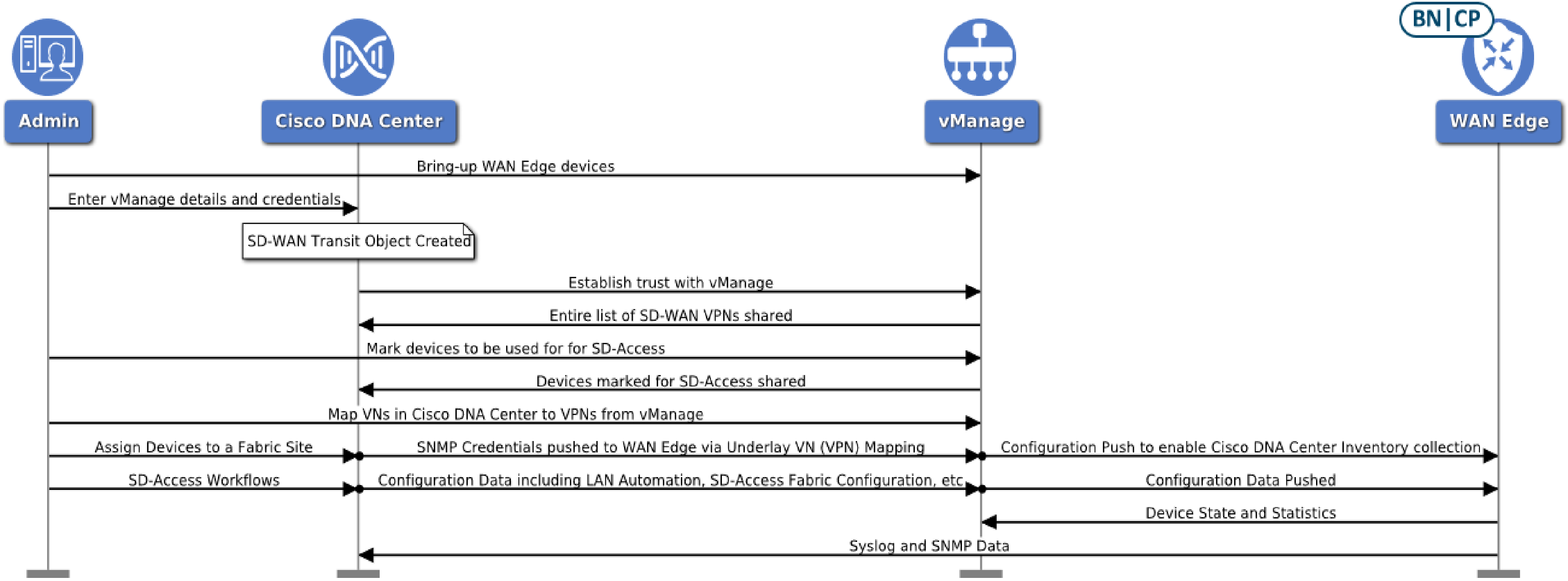
Port Number*
8443
The vManage port number

vBond Host Name/IP Address
vBondhosts
Info

Organization Name
sdwan-overlay
Info

Partner Id
5eebb9909962950017a3a725
Cisco DNA Center Partner Id in vManage server

SDA and SDWAN Integration



Admin

Cisco DNA Center

vManage

BN | CP

WAN Edge

Bring-up WAN Edge devices

Enter vManage details and credentials

SD-WAN Transit Object Created

Establish trust with vManage

Entire list of SD-WAN VPNs shared

Mark devices to be used for for SD-Access

Devices marked for SD-Access shared

Map VNs in Cisco DNA Center to VPNs from vManage

Assign Devices to a Fabric Site

SNMP Credentials pushed to WAN Edge via Underlay VN (VPN) Mapping

Configuration Push to enable Cisco DNA Center Inventory collection

SD-Access Workflows

Configuration Data including LAN Automation, SD-Access Fabric Configuration, etc

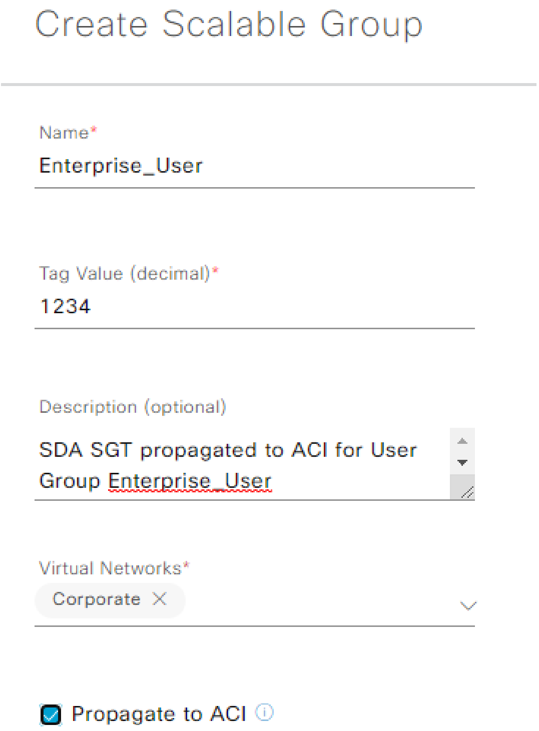
Configuration Data Pushed

Device State and Statistics

Syslog and SNMP Data

What Is Involved In SDA & ACI Integration?

- Steps
  - DNAC and APIC both integrate with ISE
  - API based interconnection
- Results
  - SDA VNs and ACI Contexts tied together
  - SDA SGTs and ACI EPGs mapped
  - Consistent policy throughout



Create Scalable Group

Name*
Enterprise_User

Tag Value (decimal)*
1234

Description (optional)
SDA SGT propagated to ACI for User Group Enterprise_User

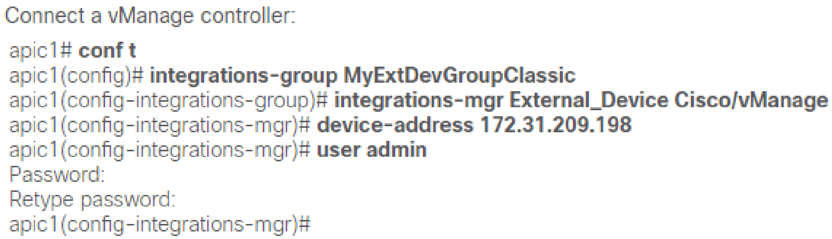
Virtual Networks*
Corporate ✕

☑ Propagate to ACI ⓘ

What Is Involved In ACI & SDWAN Integration?

- Steps
  - APIC integrates with vManage
  - Associate WAN SLA Policy with Contracts
  - ACI Tenants matched to SDWAN VPNs

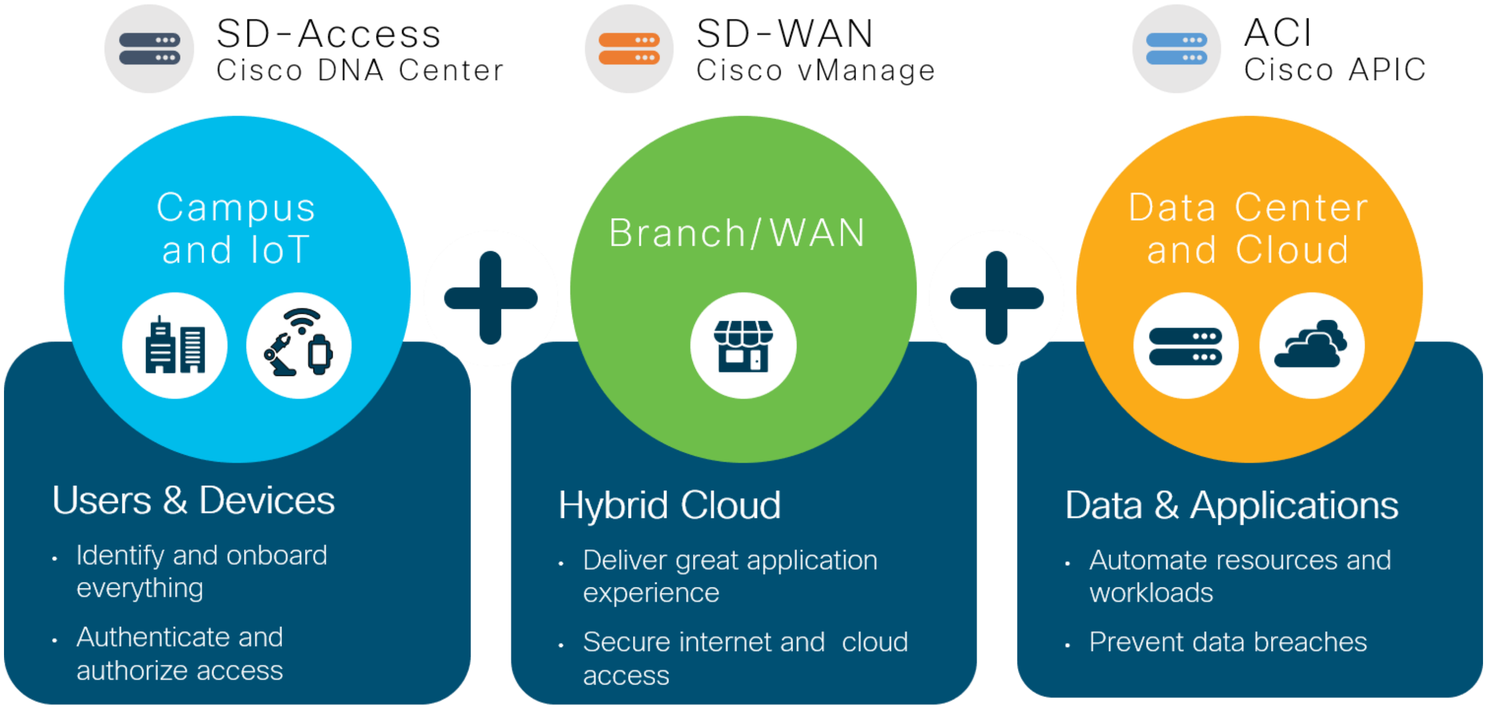
- Results
  - Tenants control SDWAN AAR
  - DC Segmentation is maintained to the branch



Connect a vManage controller:

```
apic1# conf t
apic1(config)# integrations-group MyExtDevGroupClassic
apic1(config-integrations-group)# integrations-mgr External_Device Cisco/vManage
apic1(config-integrations-mgr)# device-address 172.31.209.198
apic1(config-integrations-mgr)# user admin
Password:
Retype password:
apic1(config-integrations-mgr)#
```

Really Really High-Level View



SD-Access
Cisco DNA Center

SD-WAN
Cisco vManage

ACI
Cisco APIC

Campus and IoT

Branch/WAN

Data Center and Cloud

Users & Devices

- Identify and onboard everything
- Authenticate and authorize access

Hybrid Cloud

- Deliver great application experience
- Secure internet and cloud access

Data & Applications

- Automate resources and workloads
- Prevent data breaches

100,000 ft view

- SDA
  - Endpoints dynamically assigned SGTs and placed into VNs
- SDWAN
  - Extends segmentation
  - Applies APIC/DNAC per-VPN security and application policy.
- ACI
  - End-to-end policy and segmentation automatically enforced

Lessons Learned From Large Scale Deployments

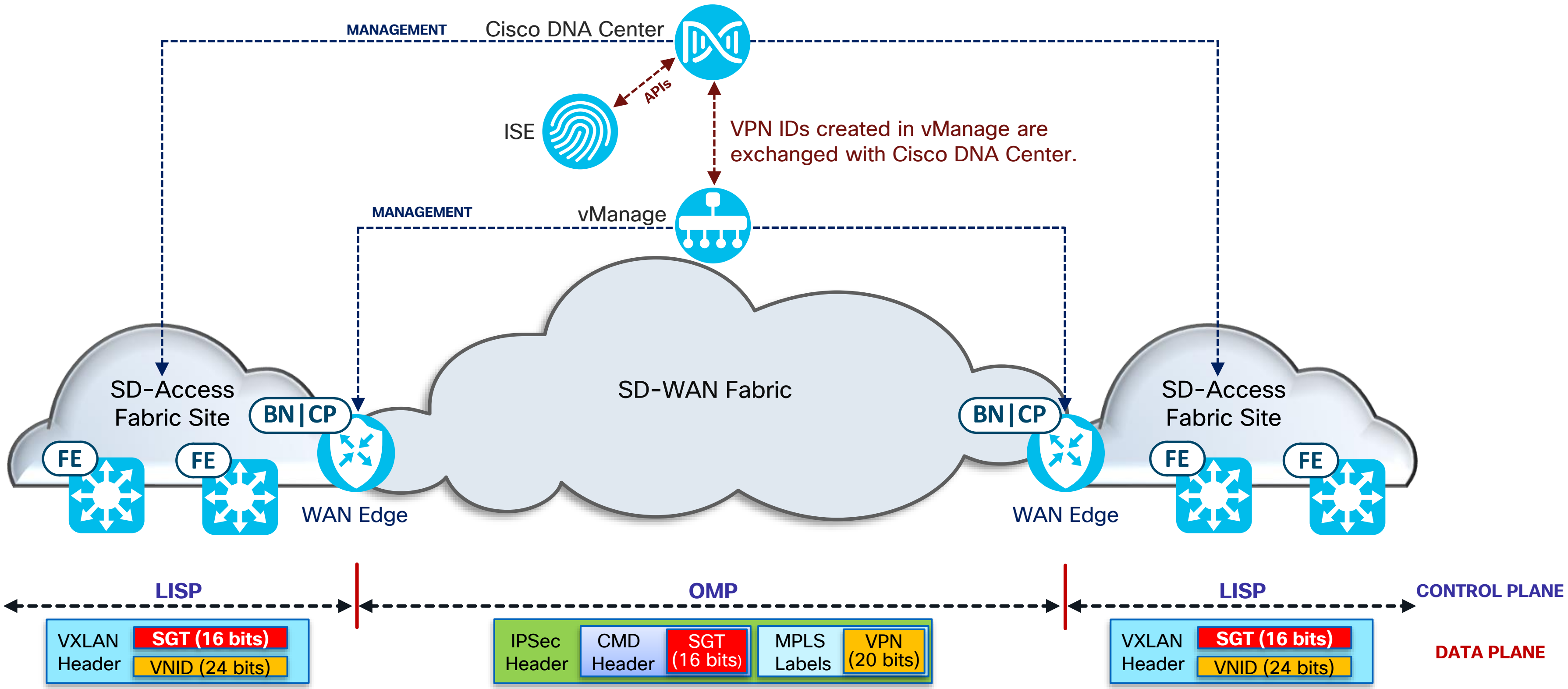
SDA and SDWAN Deployments

- Today available in fully automated "one-box" solution or partly manual "two-box" solution
- One-box solution (integrated solution)
  - Features SDA BN/CP and SDWAN WAN Edge in a single box.
  - Must be an ASR 1000 or ISR 4000 series router
- Two-box solution (non-integrated solution)
  - Clear demarcation between SDA and SDWAN architectures
  - SDA BNs can be ISR4K, ASR1K or Cat9K switches, SDWAN edges can be ISR4K or ASR1K series routers
  - SDA and SDWAN designs can be implemented at a different pace

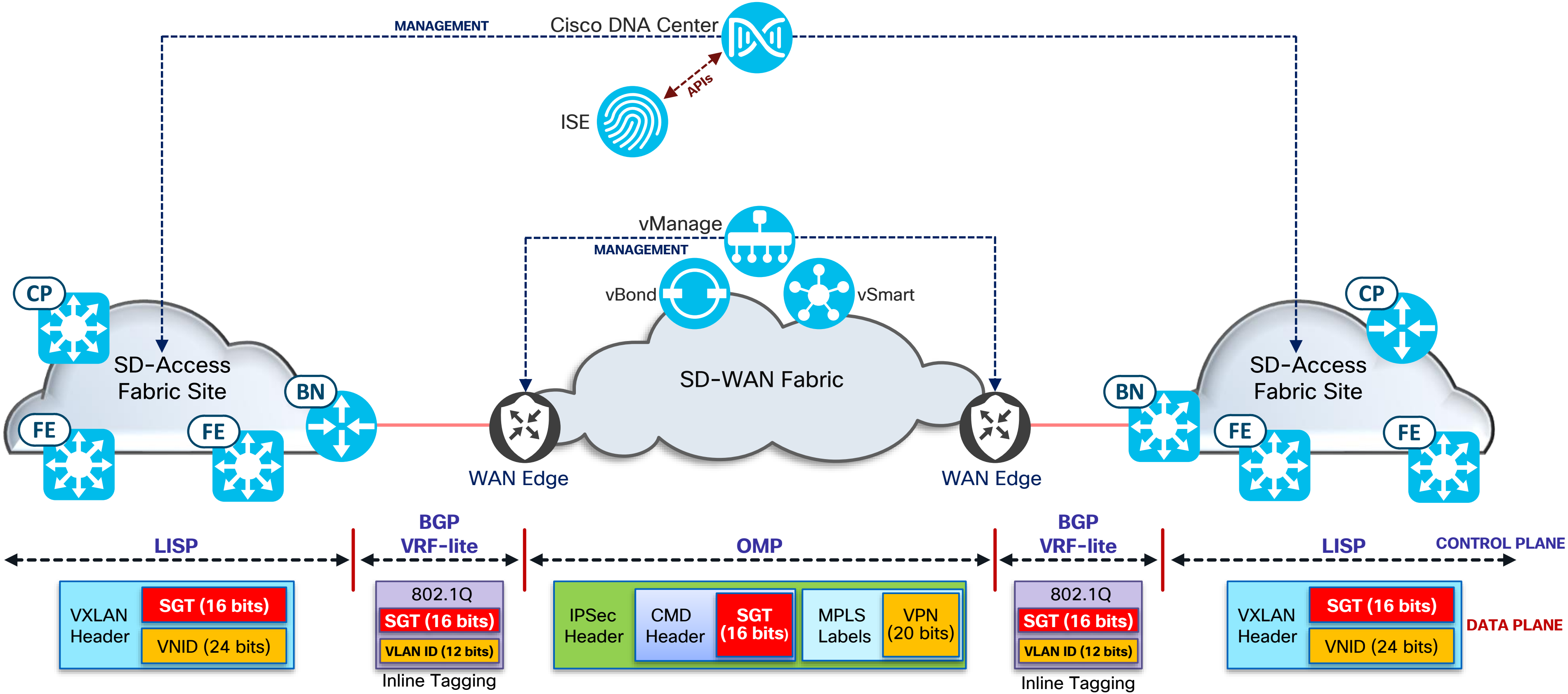
SDA and SDWAN Deployments Contd.

- Majority of customers have employed two-box solution for modularity of deployment and flexibility in operations
- Mapping of VNs and VPNs is crucial
- Inter-site traffic flow greatly depends on SDWAN tunnel design and SDWAN underlay.
- For Multi-Regional (Global) networks, consistency across multiple DNAC clusters is key.
- Special consideration for inter-VN routing within the site

SDA to SDWAN Integration (One-Box)



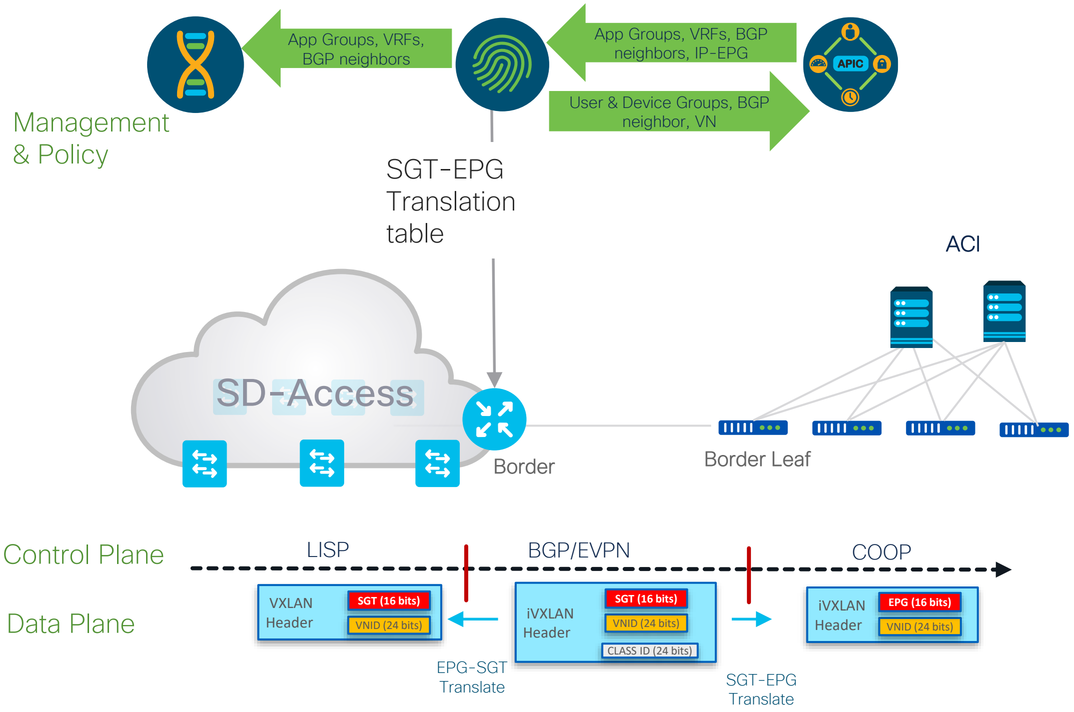
SDA to SDWAN Integration (Two-Box)



ACI and SDA Deployments (Phase 2 Integration)

- SGT to EPG mapping is critical, leverage ISE for consistency.
- Create contracts on both side of the fabric - SDA and ACI
- Integration strategies:
  - Border/CP at Data Center by treating DC as a site
  - VRF-Lite / Tunnels from HQ BN/CP to DC
  - BGP/EVPN with VRF-Lite to extend macro and micro segmentation
  - Leveraging CMD between SDA Border Nodes and ACI Border Leafs
- A good use case for Multi-Site Remote Border!

SDA and ACI Integration (Phase 2)



ACI and SDWAN Deployments

- ACI Border Leaf to SDWAN cEdge – Standardize Naming/VLANs
- Scale of BGP Peering Sessions
- Visualize traffic flow – Source and Destination
- Verify and document contracts and AAR policies to ensure efficient routing through WAN.
- WAN MTU consideration crucial
- Very limited capability in current phase

Lessons Learned From Large Scale Migrations

SDA and SDWAN Migrations

- Order of operations is key!
- Underlay of SDA and Trusted VN needs to be bridged to overlay of SDWAN
- DC first approach – get those cEdge headends built first
- At branch, install SDWAN first, test it and then proceed with SDA
- Infrastructure and UAT testing is very critical
- TrustSEC needs to be configured on SDWAN first and then SDA BN
- For sub-interfaces, TrustSEC must be enabled on physical and all sub-interfaces

ACI and SDA Migrations

- Border nodes and Border Leafs integration is key
- Data center as a site architecture with BGP/EVPN/VXLAN
- Currently SDWAN in the middle is not supported
- SXP configuration on BNs crucial for end-to-end segmentation
- Always verify and test this in a lab and use it as a certification test bed

ACI and SDWAN Migrations

- Order of operations is critical
- ACI to cEdge Aggregation Layer facilitates migration of hosts/applications to ACI and non-migrated WAN to SDWAN independently.
- Convert cEdge to CLI mode > fine-tune ACI to SDWAN connectivity > update SDWAN template > reattach template for efficient turn up of the solution
- More enhancements are in roadmap.

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