
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Lessons Learned From Multi-Domain IBN Architectures in SDA, SDWAN and ACI

Dhrumil Prajapati, Jeremy Bowman
Delivery Architects

BRKENS-3000

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?

Dhrumil Prajapati

Delivery Architect

Technology and Transformation Group – CX

6+ Years @ Cisco

CCIE #28071 (R/S, SP)

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

@DhruPrajapati

Who are we?

Jeremy Bowman

Delivery Architect

Cisco CX

6+ 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

cisco Live!

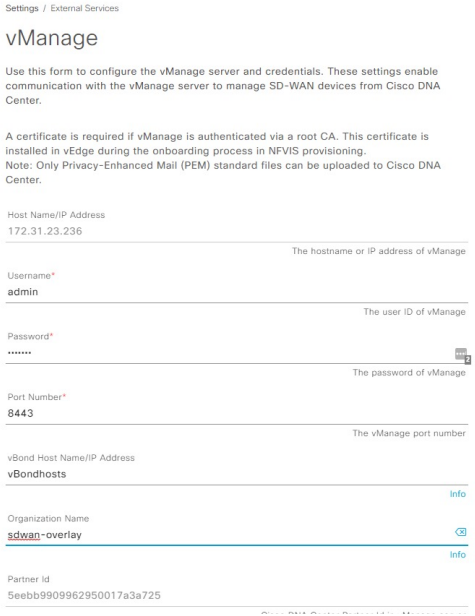
Why Multi-Domain?

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

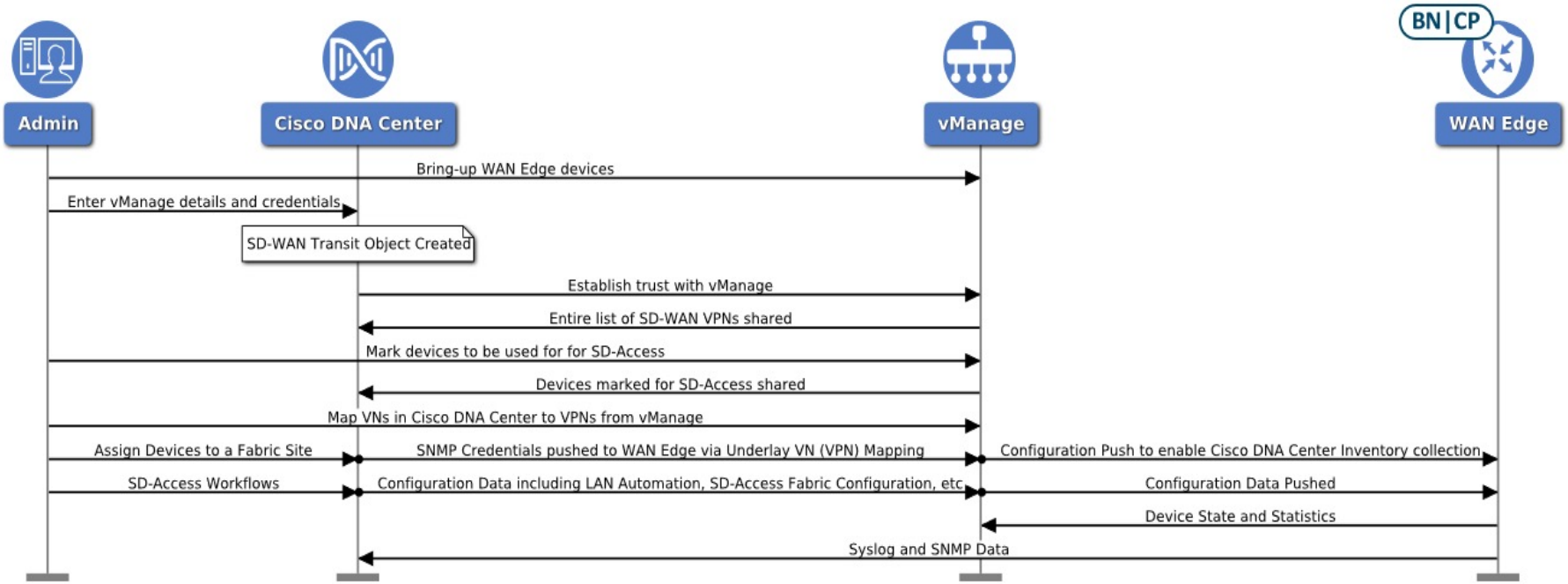
- Multi-Domain Architectures
  - Extend Segmentation
  - Utilize orchestration
  - Make the entire enterprise one IBN enclave

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



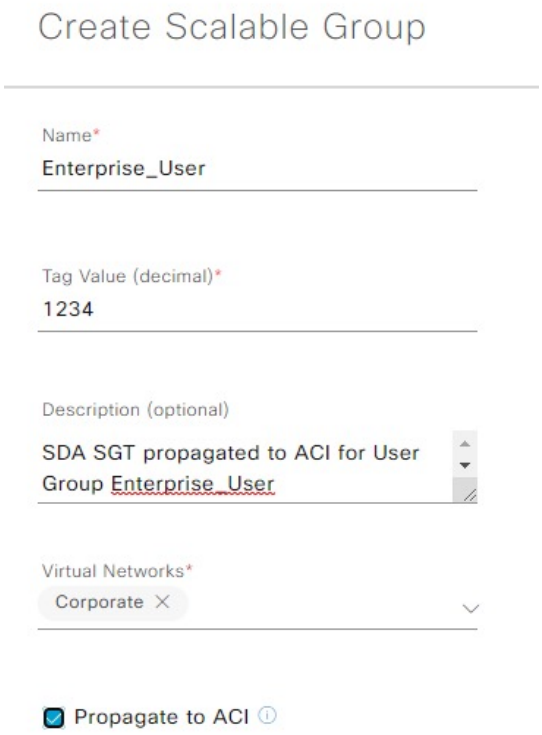
SDA and SDWAN Integration



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



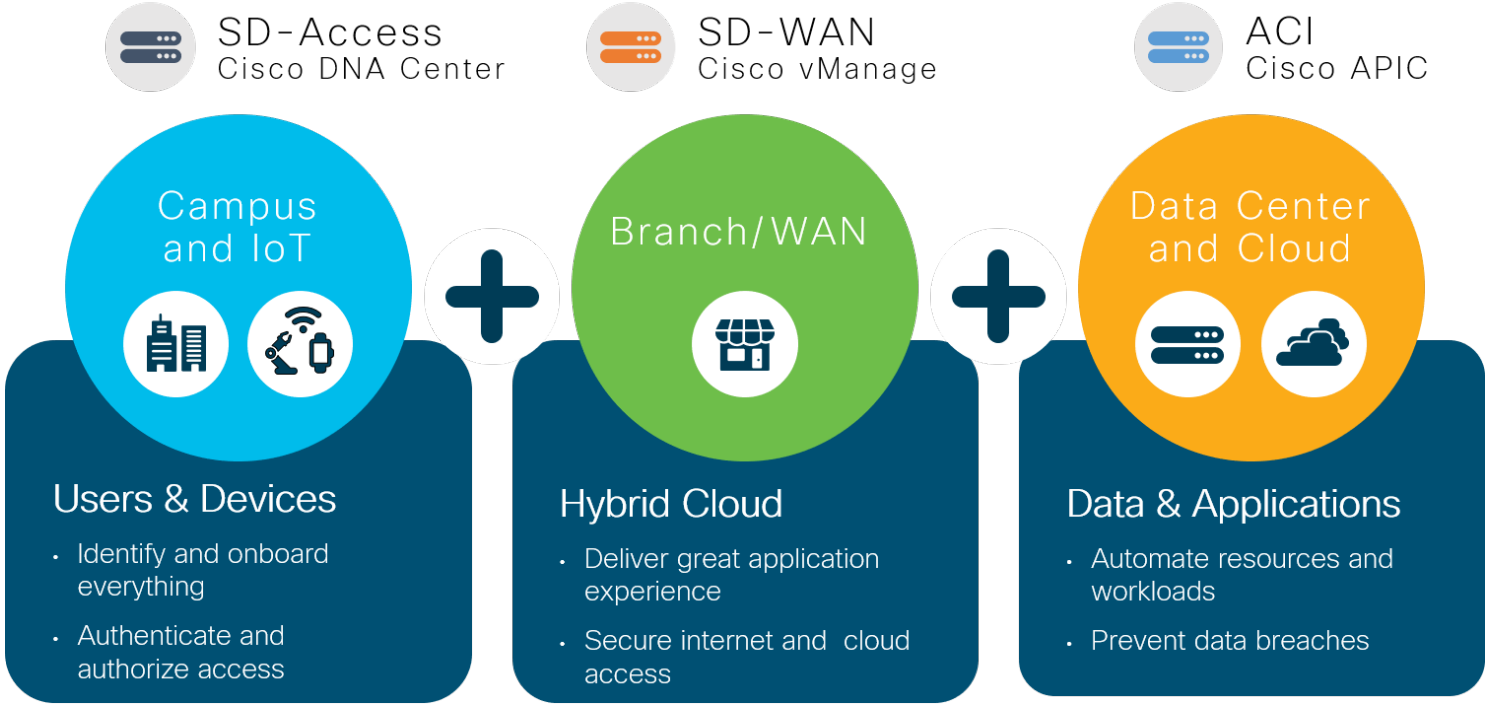
What Is Involved In ACI & SDWAN Integration?

- 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



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

cisco Live!

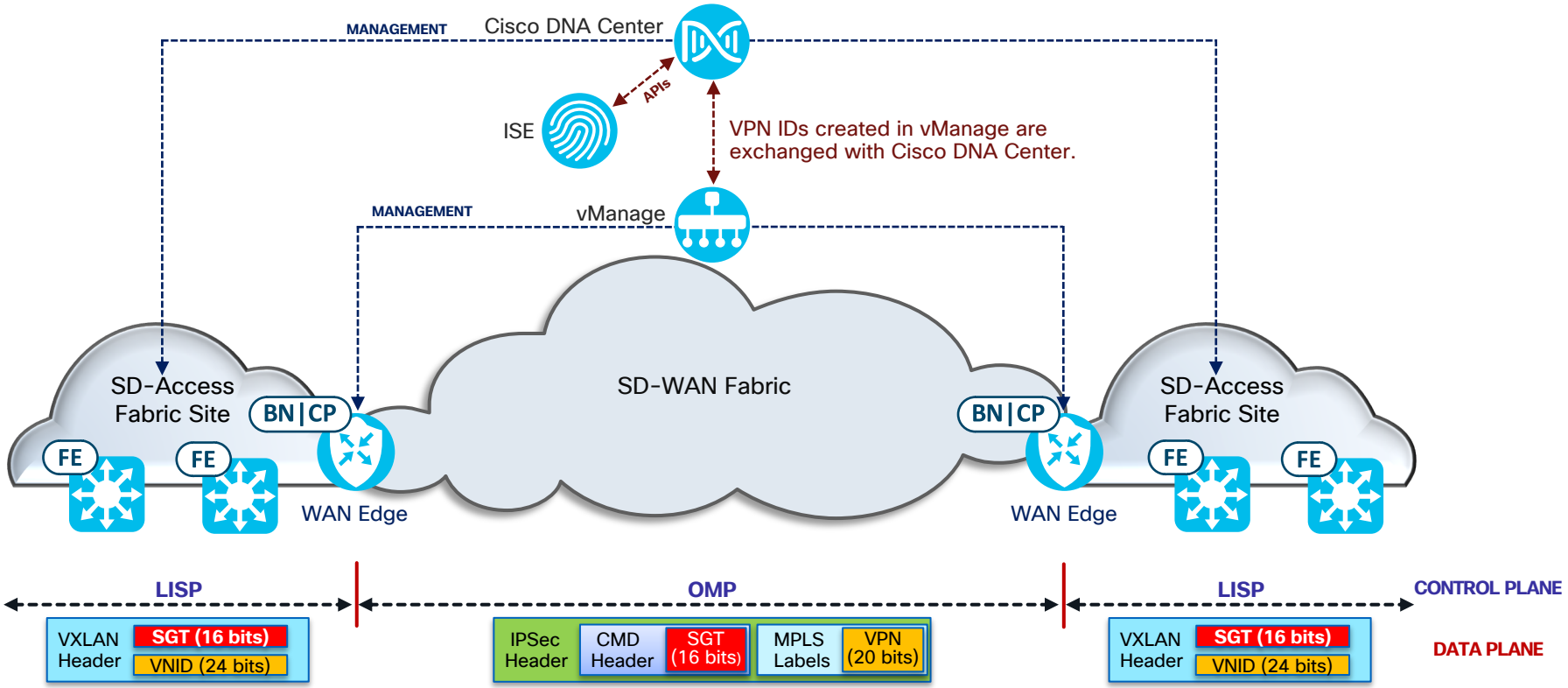
SDA and SDWAN Deployments

- 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

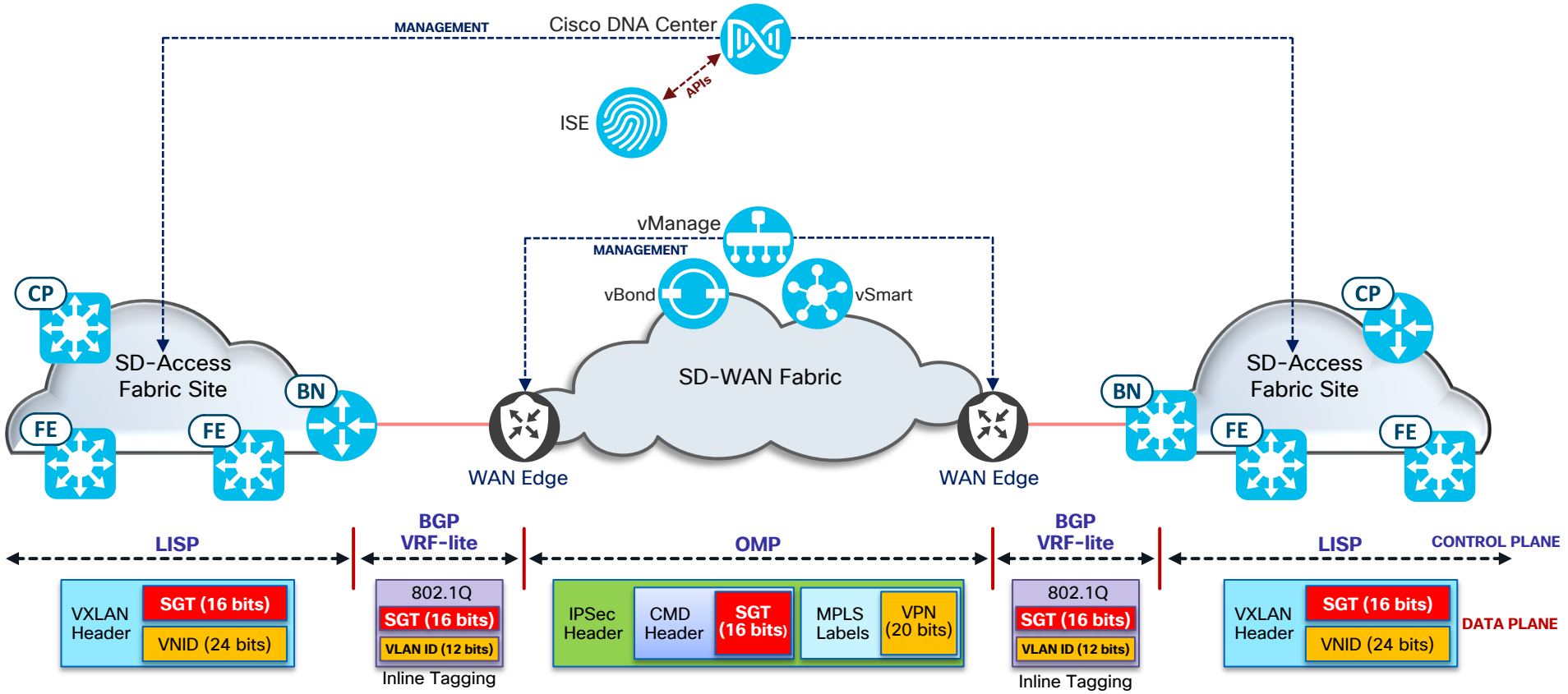
SDA and SDWAN Deployments Contd.

- 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)



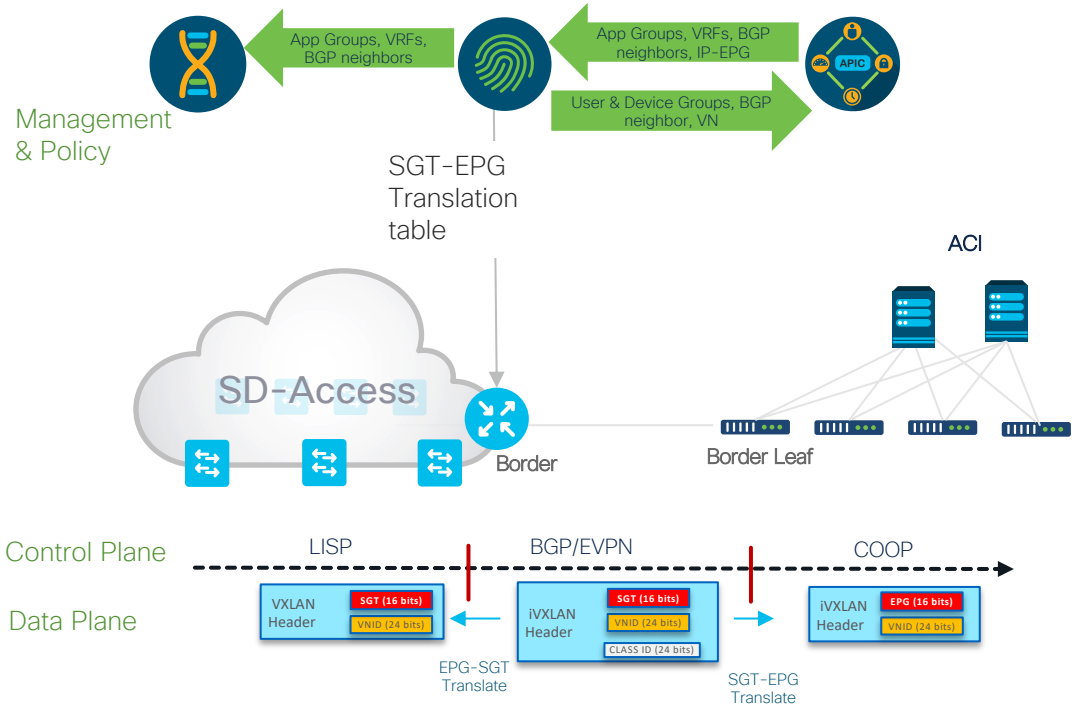
SDA to SDWAN Integration (Two-Box)



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

cisco Live!

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.

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive