cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Cisco SD-Access Design and Deployment Best Practices

BRKENS-2502b

Prashanth Kumar- Technical Marketing Engineer
Enterprise Network Business Group

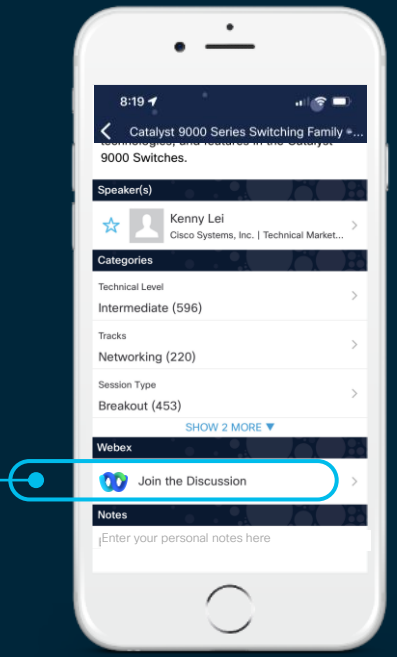
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2502b

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

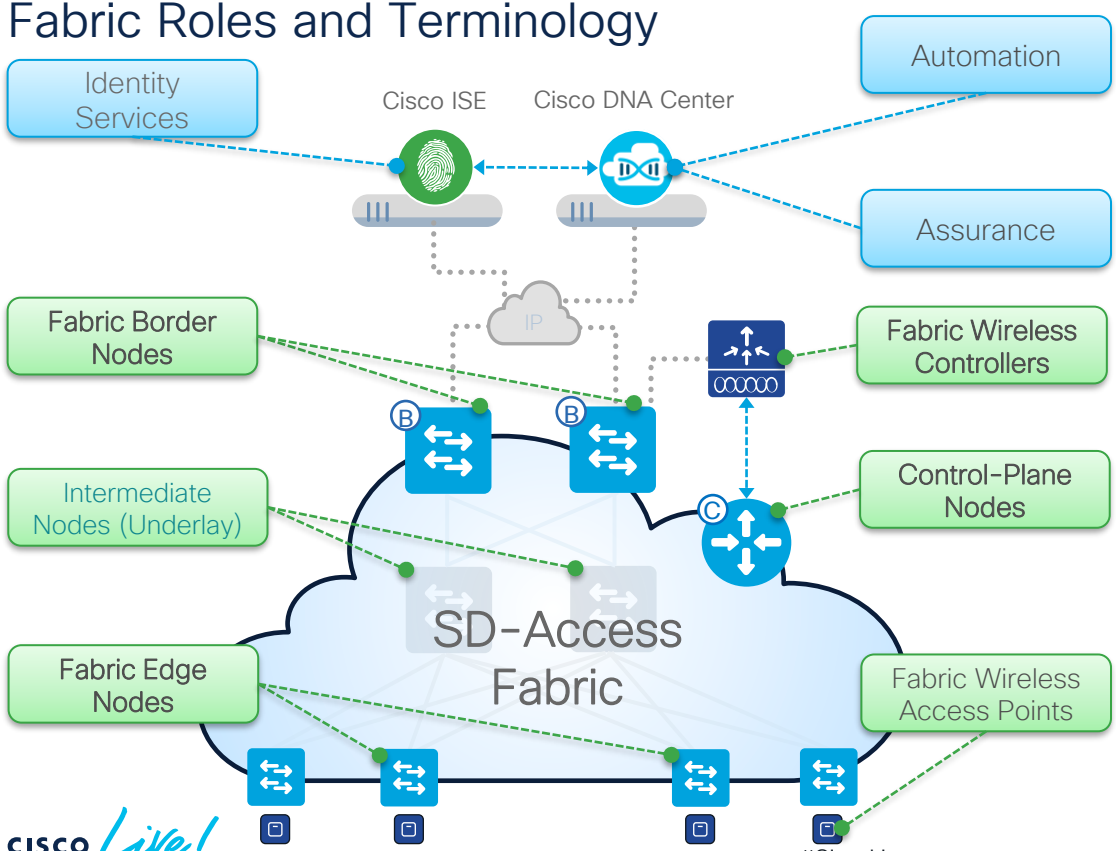
Agenda

- Multi-Site Overview
  - Design Strategy
- Multi-Site Design
  - SD-Access Transit
  - SD-WAN Transit
  - IP-Based Transit
- Migration Strategy
- Summary

For your reference

Cisco SD-Access

Fabric Roles and Terminology



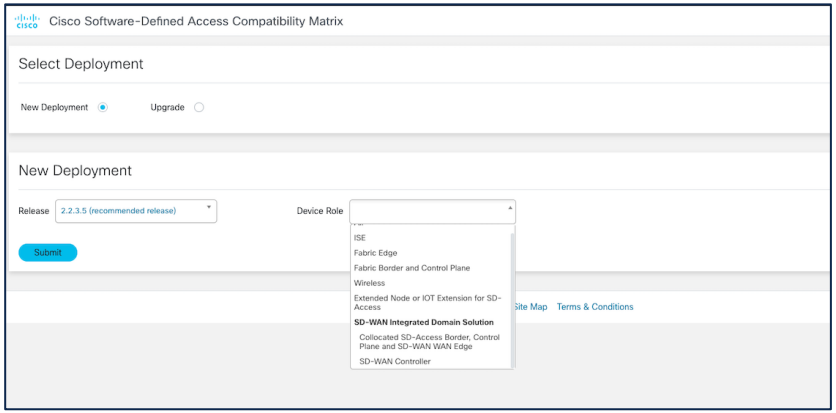
- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric network status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint 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

For your reference

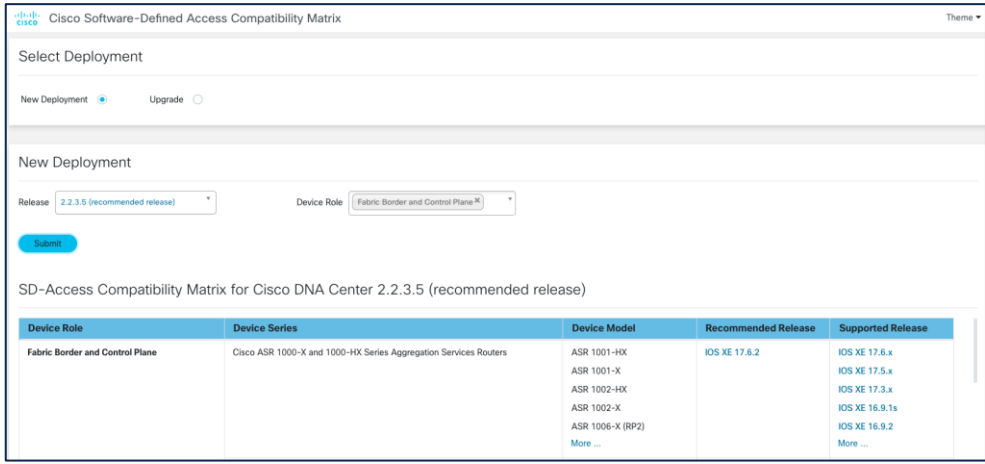
SD-Access Platform Support

Digital Platforms for your Cisco Digital Network Architecture

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



Platform support based on the Fabric Role



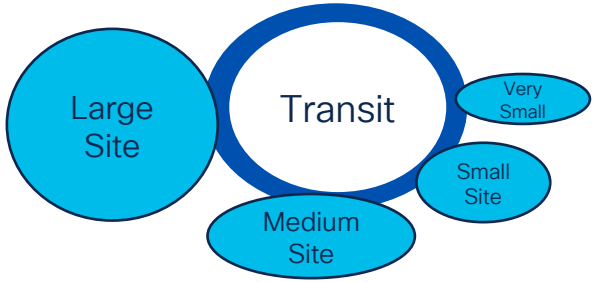
Supported Hardware and Software Version for all Cisco SD-Access components

Cisco SD-Access

Distributed Fabric Site Design Options

Managed by single Cisco DNA Center and ISE Deployment

Fabric Site Design	Distributed Site Design
High Availability & Scale defines Platform and Fabric Roles	Transport connection defines Transit type: IP | SD-Access | SD-WAN



- Administrative domain
- Site Survivability and Scale
- End-to-End Segmentation
- Unified and Consistent Policy

Cisco SD-Access Scale

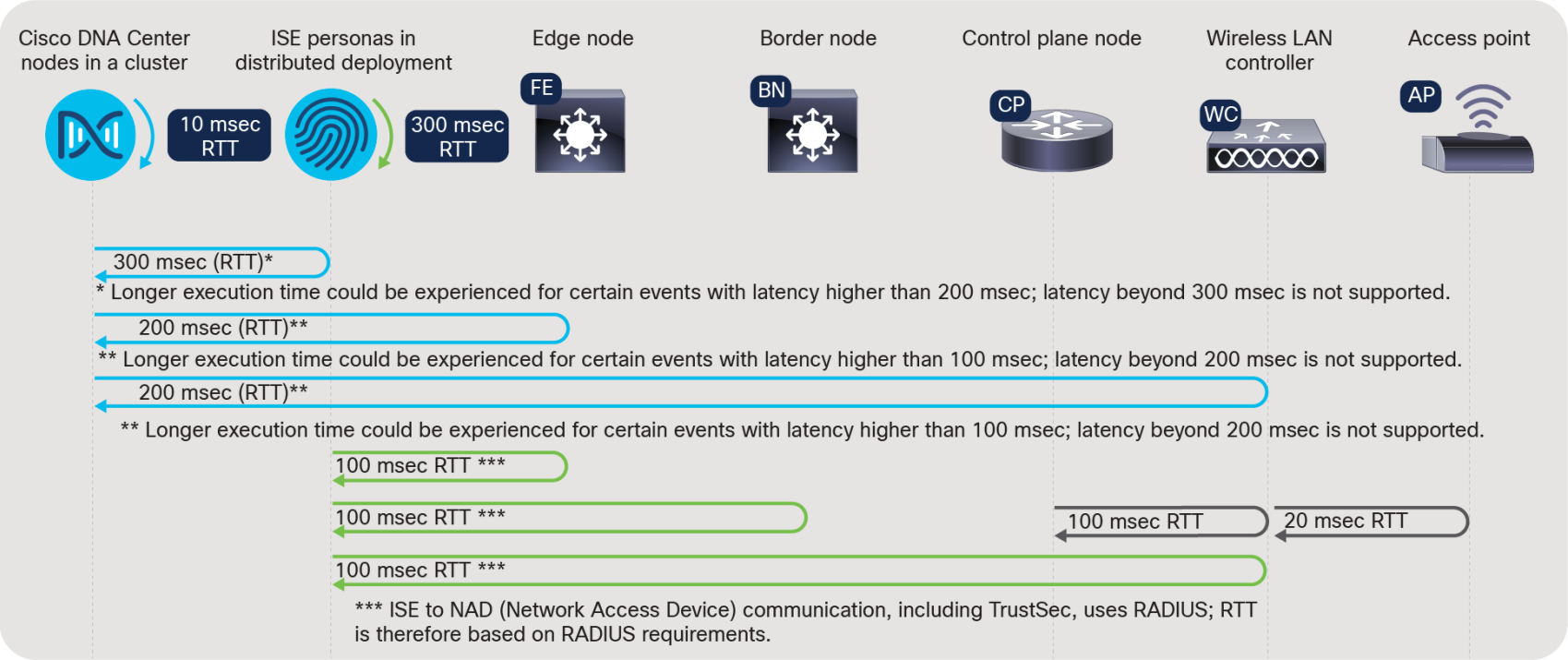
Fabric Scale based on DNA Appliance

	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
No of Fabric Domains	10	20	20
No of Fabric Sites	500	1000	2000
No of Virtual Networks	64/site	64/site	256/site
No of Fabric Devices	500/site	600/site	1000/site
No of Scalable Groups	4000	4000	4000
No of Access Contracts	500	500	500
No of Group-Based Policies	25000	25000	25000
No of IP Pools	100/site	300/site	600/site

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

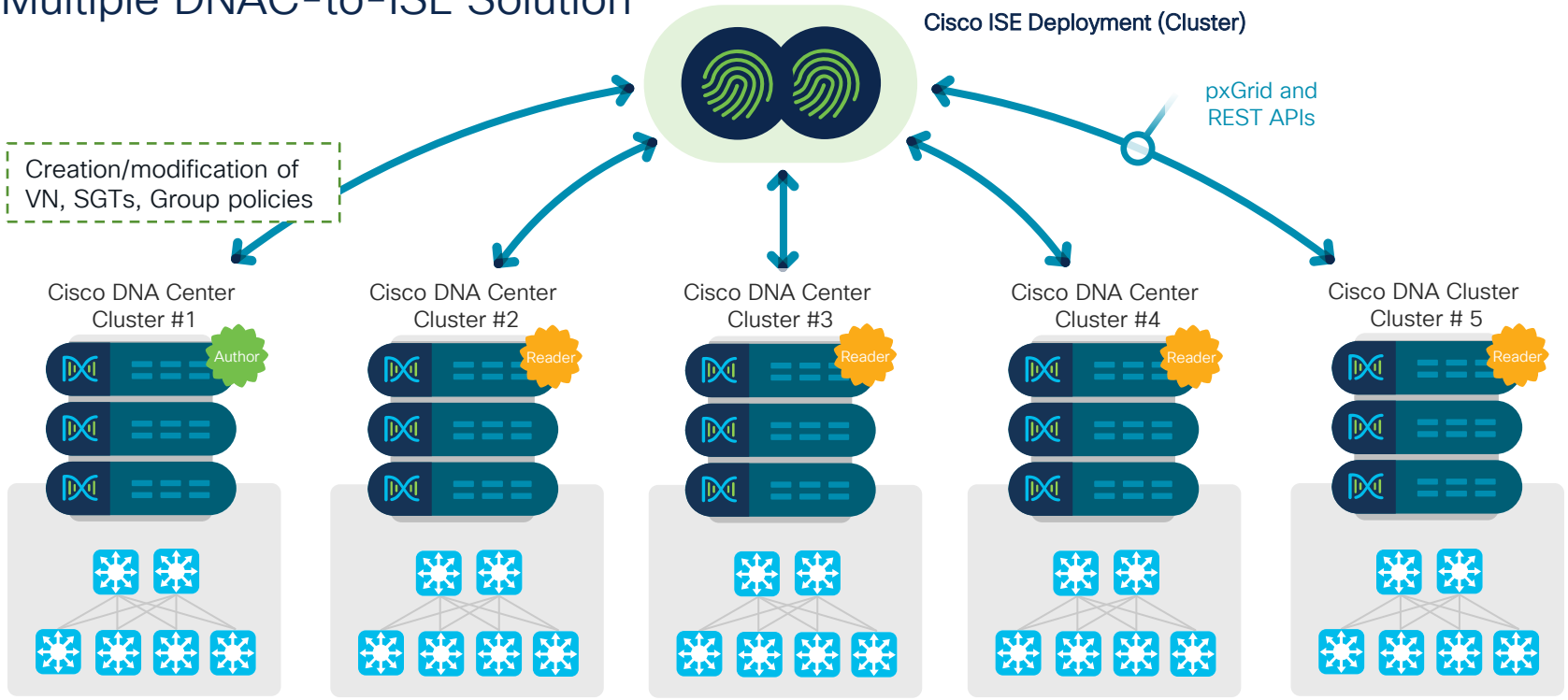
Cisco SD-Access

Latency Requirements



Multiple Cisco DNA Center

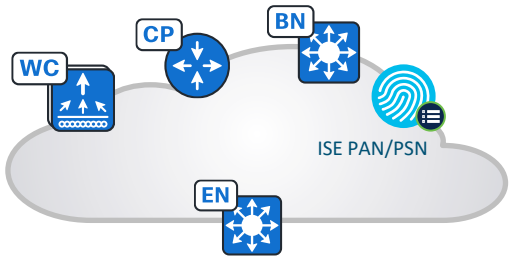
Multiple DNAC-to-ISE Solution*



* Limited Availability.
Reach out to Cisco representative for more details

Cisco SD-Access Design Options

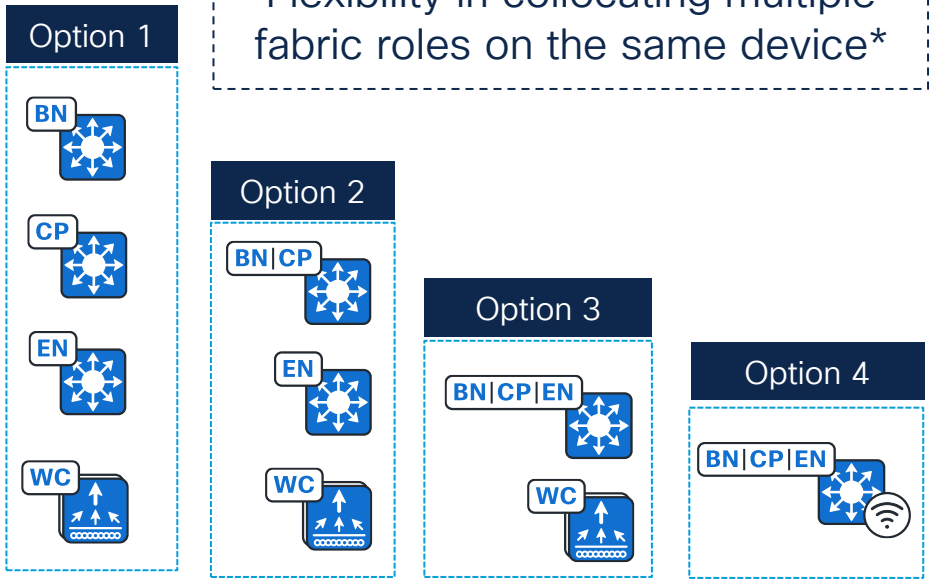
Fabric Site Design Options



Fabric Site

- Logical construct that contains:
  - Fabric Edge, Border, Control Plane
  - (optional) Wireless LAN Controller, Access Points
  - (optional) Extended Nodes
  - ISE PAN/PSN Node

Flexibility in collocating multiple fabric roles on the same device*

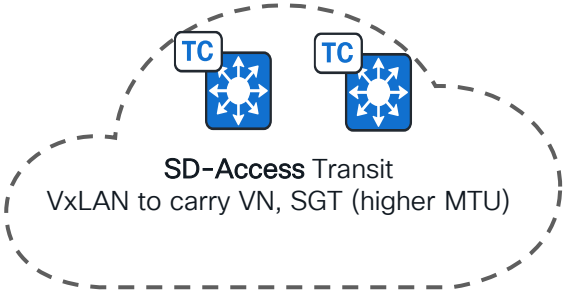


* Refer to Cisco SD-Access compatibility matrix for latest information

Cisco SD-Access Transit: SD-Access

Cisco SD-Access Deployment

Multisite Deployment with SD-Access Transit



SD-Access Transit is a native solution carrying VN and SGT between Fabric sites.

Key Considerations:

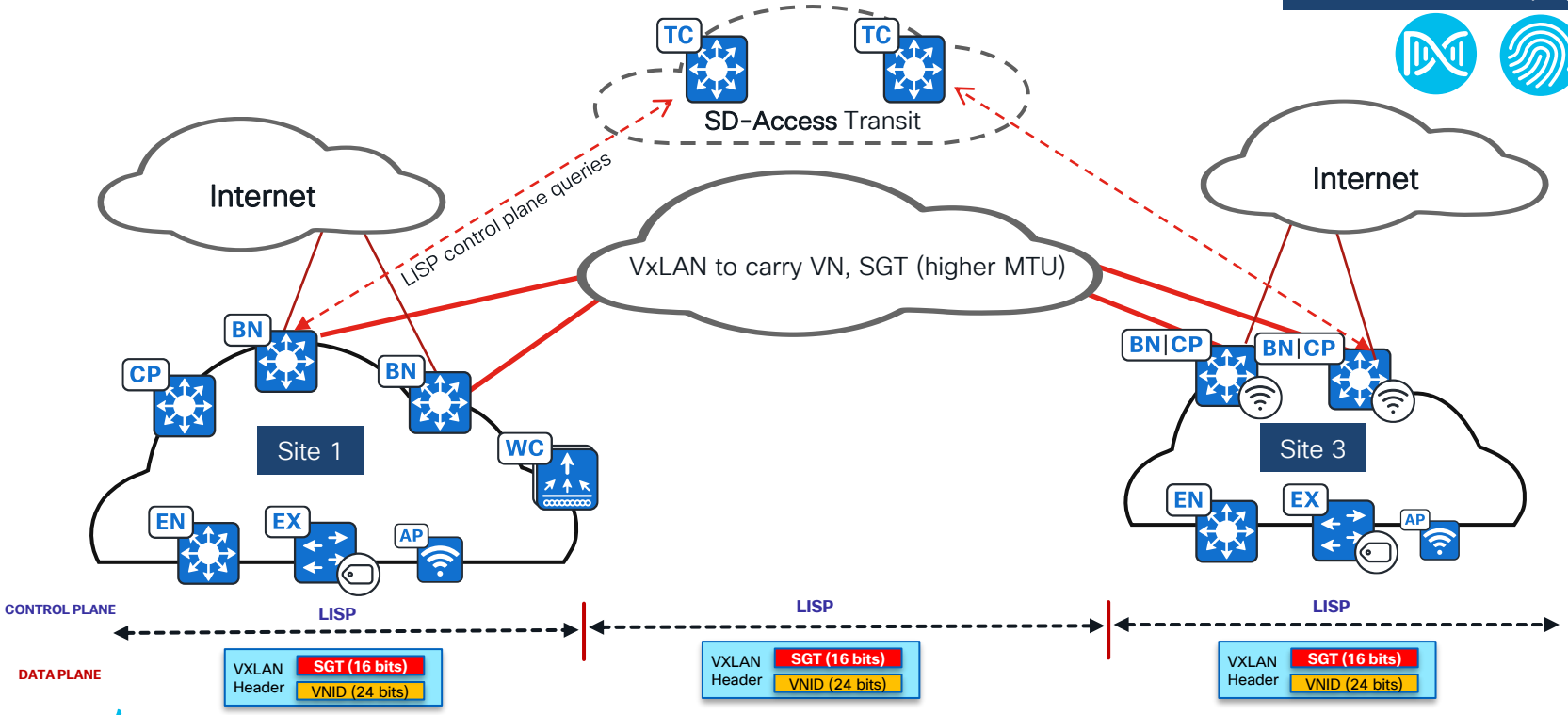
- Higher MTU support

- Transit Control Plane nodes are dedicated devices with IP reachability to every fabric site's Border nodes
- Transit Control Plane nodes is not required to be in data forwarding path
- Transit Control Plane nodes maintains aggregate prefixes of all Fabric sites
- Fabric site Border node should be either External or Anywhere border type to connect to SD-Access Transit.
- SD-Access Transit can be deployed with LISP-BGP (up to 2 nodes) or **LISP Pub/Sub** (up to 4 nodes)
- Fabric site connected to SD-Access Transit can provide Internet service to remote fabric sites.

Cisco SD-Access Deployment Options

Multisite Fabric Deployment with SD-Access Transit

Managed by single Cisco DNA cluster and ISE Deployment



Cisco SD-Access Transit: SD-WAN

Cisco SD-Access Deployment

Multisite Deployment with SD-WAN Transit

Cisco SD-WAN Transit provides capability to carry VN and SGT across WAN Transport.

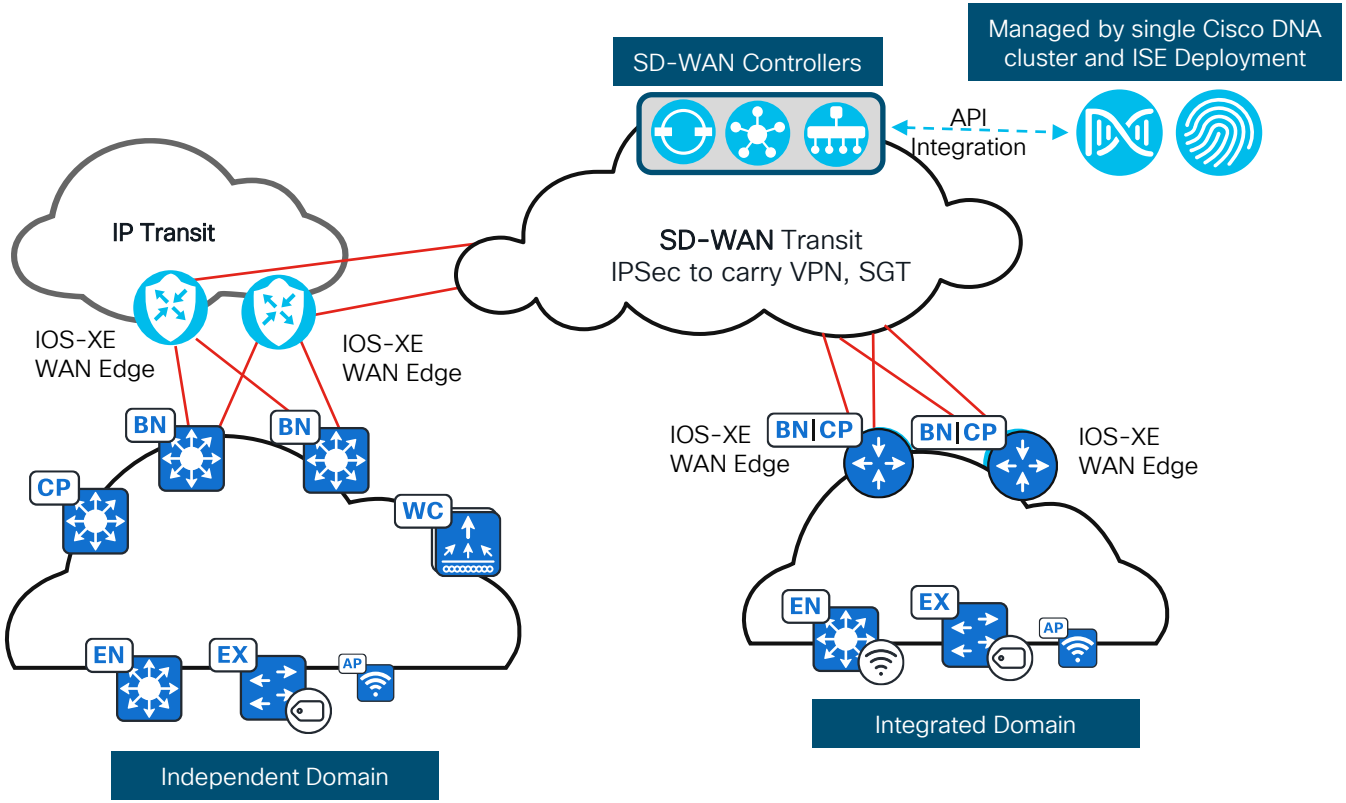
Key Considerations:

- Greenfield or Brownfield Fabric Site
- Fabric Site network requirements
- Border, WAN Edge platform capabilities.

- Cisco SD-WAN solution, powered by Cisco IOS-XE software provides highly secure and reliable WAN overlay topologies.
- IOS-XE WAN Edge devices provides flexibility to add-on security capabilities as Direct Internet Access (DIA), Application-Aware routing, Firewall, IPS and more..
- Cisco SD-Access provides flexibility to deploy integrated LAN and Wireless with consistent policy at scale.
- Cisco SD-Access and SD-WAN can be deployed with:
  - With **Integrated-Domain:** DNA Center and vManage are integrated.
  - With **Independent-Domain**: DNA Center are vManage are not integrated.

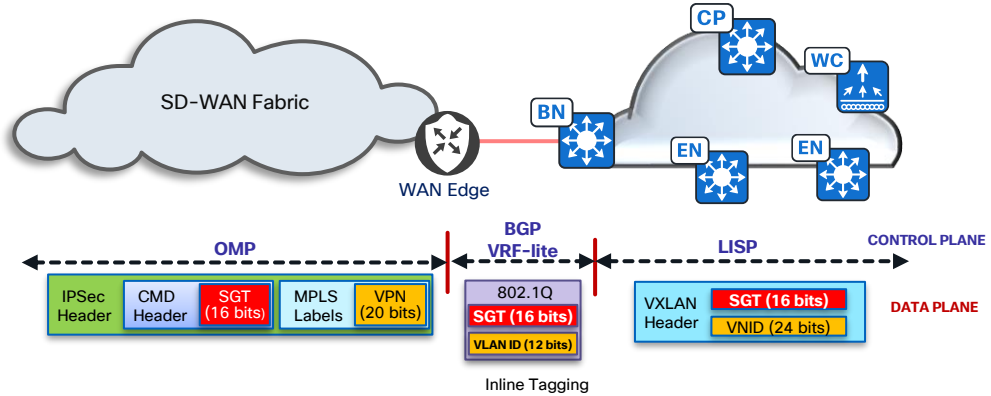
Cisco SD-Access Deployment Options

Transit – SD-WAN Transit



Cisco SD-Access Deployment

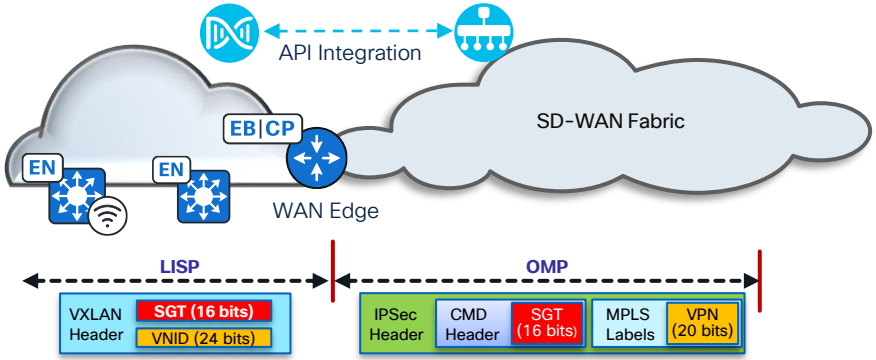
Cisco SDA|SDWAN Independent Deployment



- Cisco SD-WAN WAN Edge and SD-Access Border node are different devices, managed by respective domain controllers.
- Macro-segmentation (VN) is maintained with IP-Handoff between Fabric Border node and WAN Edge device.
- Micro-segmentation (SGT) is shared with Cisco TrustSec Inline tagging. This requires the WAN Edge router and the interface to support TrustSec.

Cisco SD-Access Deployment

Cisco SDA|SDWAN Integrated Deployment



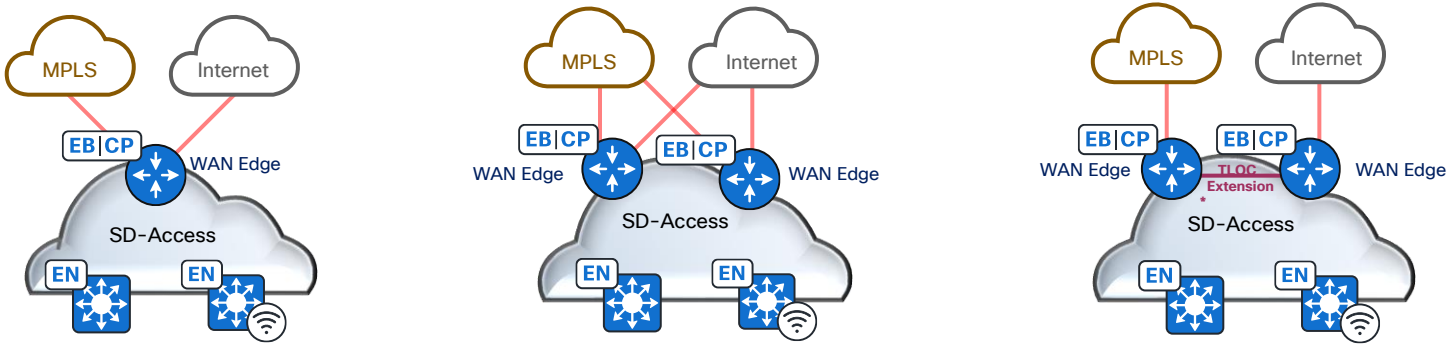
- Cisco vManage and DNA Center are integrated sharing WAN Edge device list and Service-VPN data.
- Cisco DNA Center maps the Fabric VNs to WAN Service-VPNs (1:1).
- Cisco SD-Access Fabric Site must be a Greenfield deployment.
- The router platform must support WAN Edge + colocated Border and Control Plane functionality. Max of 2 nodes can be deployed for the deployment.
- WAN Edge router learns the micro-segmentation (SGT) from VXLAN encapsulated packet and carries it in the IPSec CMD header across WAN transport.

For your reference

Cisco SD-Access Deployment

Cisco SDA|SDWAN Integrated Deployment Consideration

- Supported SD-WAN overlay network topologies .



- The following are <u>not supported</u> in the Integrated deployment model:
  - Multicast
  - IPv6
  - Layer 2 Flooding
  - LISP Pub-Sub
  - Layer 2 Border Handoff
  - SD-Access Transit
  - Multisite Remote Border

For your reference

Cisco SD-Access Transit

Cisco SDA|SDWAN Integrated & Independent Domain Deployment

Integrated Domain

- Cisco DNA Center and vManage are integrated.
- Provides ease of management and automation through integration of SD-Access and SD-WAN.

Independent Domain

- Cisco DNA Center and vManage are not integrated.
- Provides flexibility and independence between SD-Access and SD-WAN solution.

For your reference

Cisco SD-Access Transit

Cisco SDA|SDWAN Integrated & Independent Domain Deployment

- Assurance is visible in two locations:
  - Assurance for the SD-WAN and IOS-XE SD-WAN function is available on vManage.
  - Assurance for the colocated Border and Control Plane Node function along with the remainder of the SD-Access fabric is available on Cisco DNA Center.
  - Basic Assurance of WAN Edge is available in Cisco DNA Center for Integrated Domain deployment.

- Irrespective of Integrated or Independent domain deployment, solution provides:
  - Data plane integrations to main end-to-end segmentation.
  - Preserve SGT across WAN Infrastructure.
  - Consistent Group-Based policy across the enterprise.

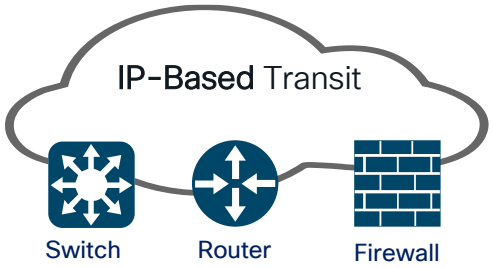
- Refer to Cisco SD-Access compatibility matrix for support/recommended hardware and software version

Cisco SD-Access Transit: IP-Based

For your reference

Cisco SD-Access Deployment

IP-Based Transit



IP-Based Transit connects Fabric to IP based external network.

Key Considerations:

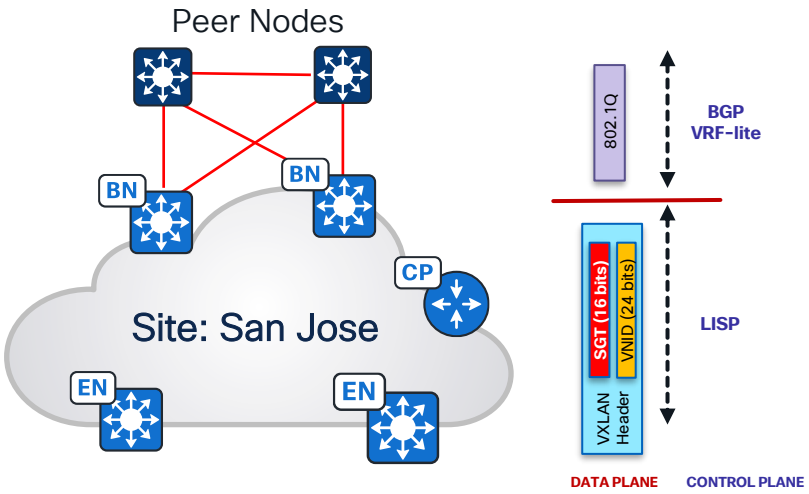
- Peer nodes must be Layer3 device – Switch, Router, Firewall.
- Peer network should support BGP.

- IP-Based transit leveraged to connect to rest of the company network or to Internet.
- Peer node can be either VRF aware or non-VRF aware.
- If peer node is VRF aware, leverage IP prefix lists to filter routes for inter-VRF communication
- If peer node is Firewall, implement stateful inspection for inter-VRF communication
- Cisco DNA Center automates the BGP handoff for each Virtual Network on the Fabric Border nodes.
- Peer Nodes configuration is manual today

Cisco SD-Access Deployment

IP-Based Transit

- If Border node is routing platform, L3 sub-interfaces will be provisioned to extend Virtual Networks
- If Border node is switching platform, SVI & trunk will be provisioned to extend Virtual Networks to Peer Network
- VXLAN is de-encapsulated on the Border node and native IP forwarded to Peer node.
- Security Group is not shared to Peer nodes natively. If required, Group can be shared using
  - Cisco Trustsec Inline Tagging from Border to Peer Nodes.
  - SXP connection from ISE to Peer Nodes.



Peer Network Configuration

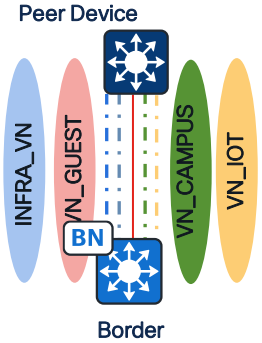
Layer 3 Handoff to External IP Domain

Extend

- Configure VRF
- Interfaces for each VN matching Border configuration

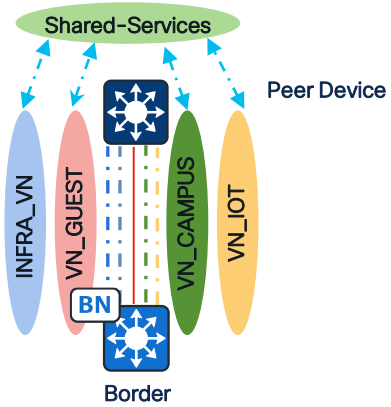
eBGP

- eBGP neighbors for each VN between Peer and Border node



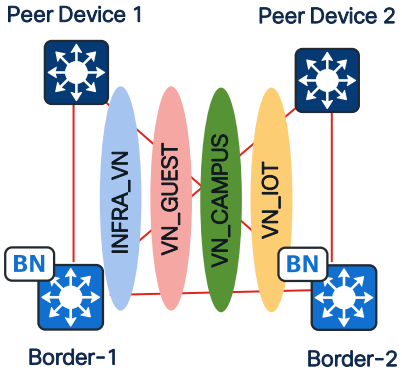
Route Leak

- Route-leak shared-services subnets to each VN
- Route-leak VN subnets into Global



iBGP

- iBGP neighbors for each VN between Border nodes

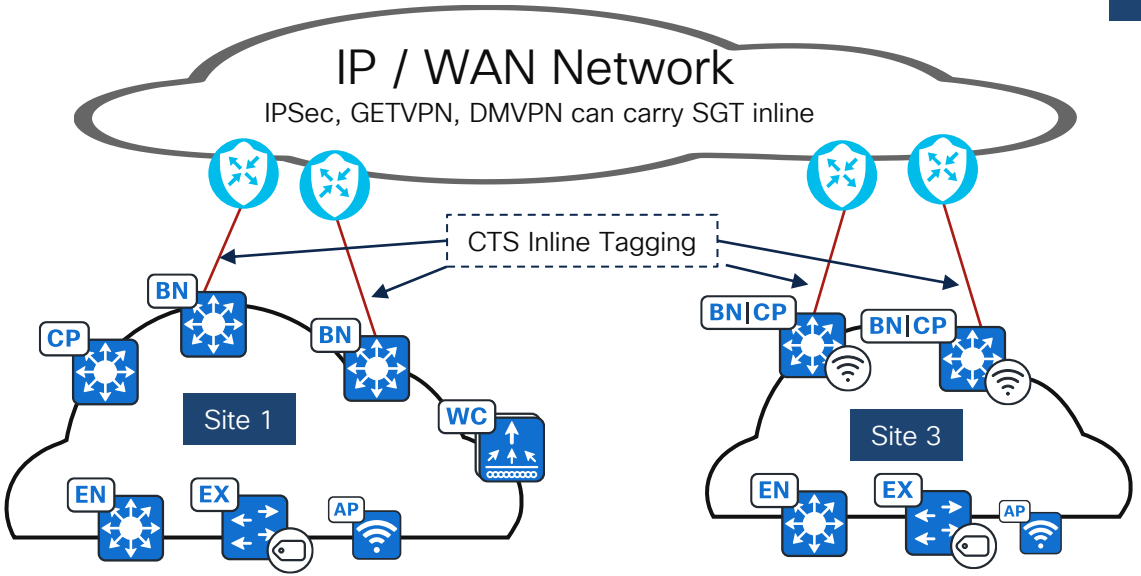


Not required at Fabric Site LISP Pub-Sub deployments.

Cisco SD-Access Deployment Options

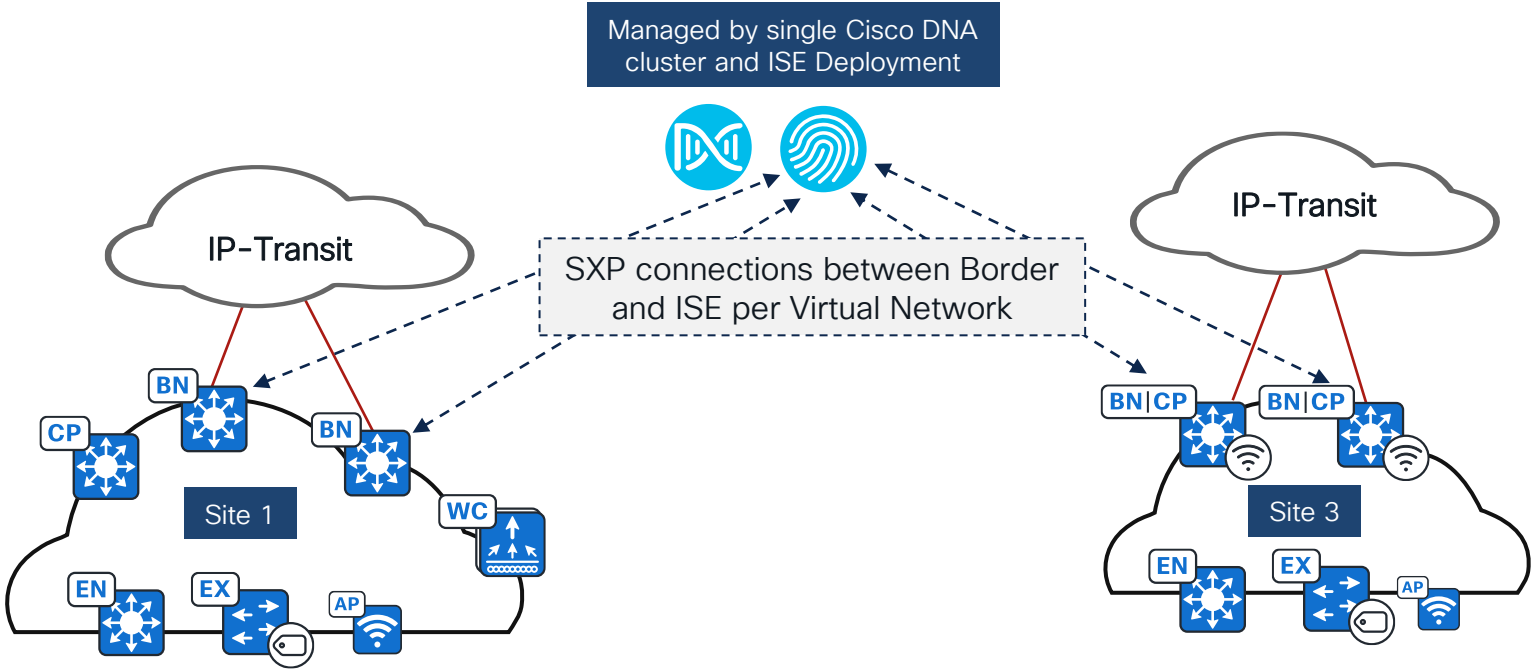
Multisite Fabric Deployment with IP-based Transit

Managed by single Cisco DNA cluster and ISE Deployment



Cisco SD-Access Deployment Options

Consistent Policy with SXP peering



Cisco SD-Access Migration Strategies

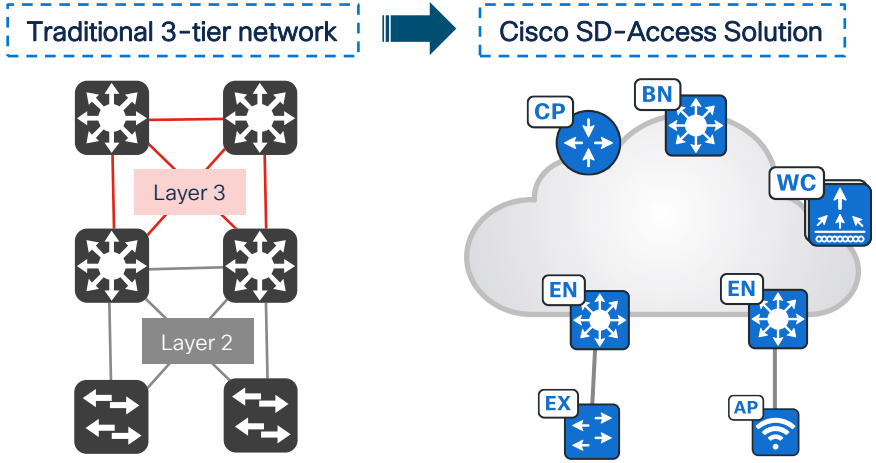
Cisco SD-Access

Fabric Migration Options

Cisco SD-Access solution provides flexible options to incrementally migrate existing network into Fabric environment.

Migration options include:

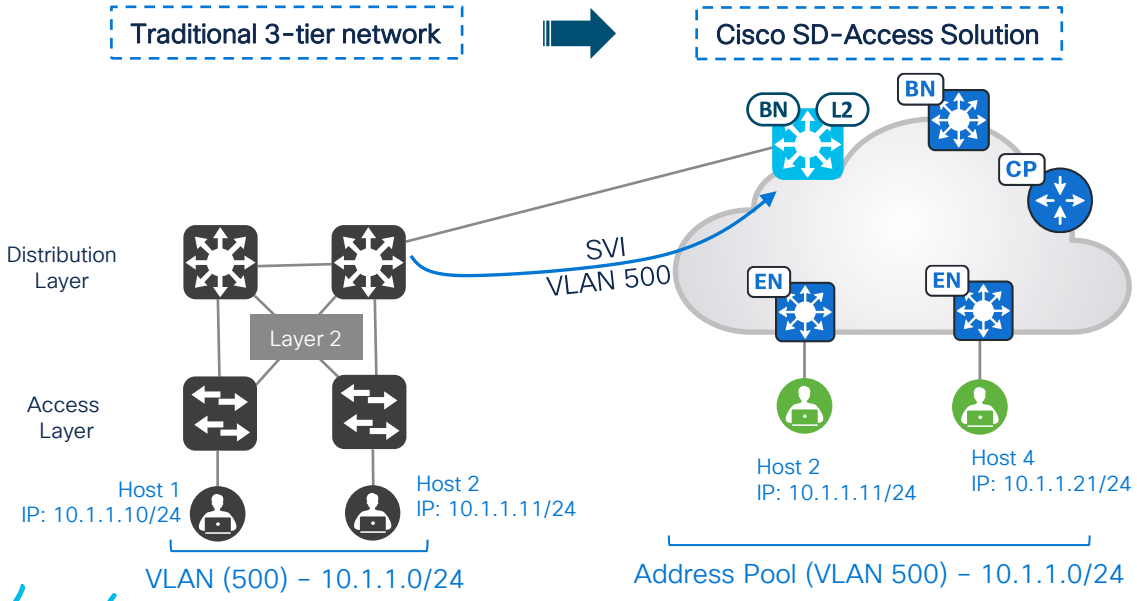
- Port-by-Port
- Switch-by-Switch
- connect Layer-2 Switching Domain



Cisco SD-Access

Fabric Migration Option - Layer2 Border Handoff

- Layer2 Border allows fabric and traditional network operate on the same subnet
- Layer2 Border hosting the anycast-gateway functionality for traditional network

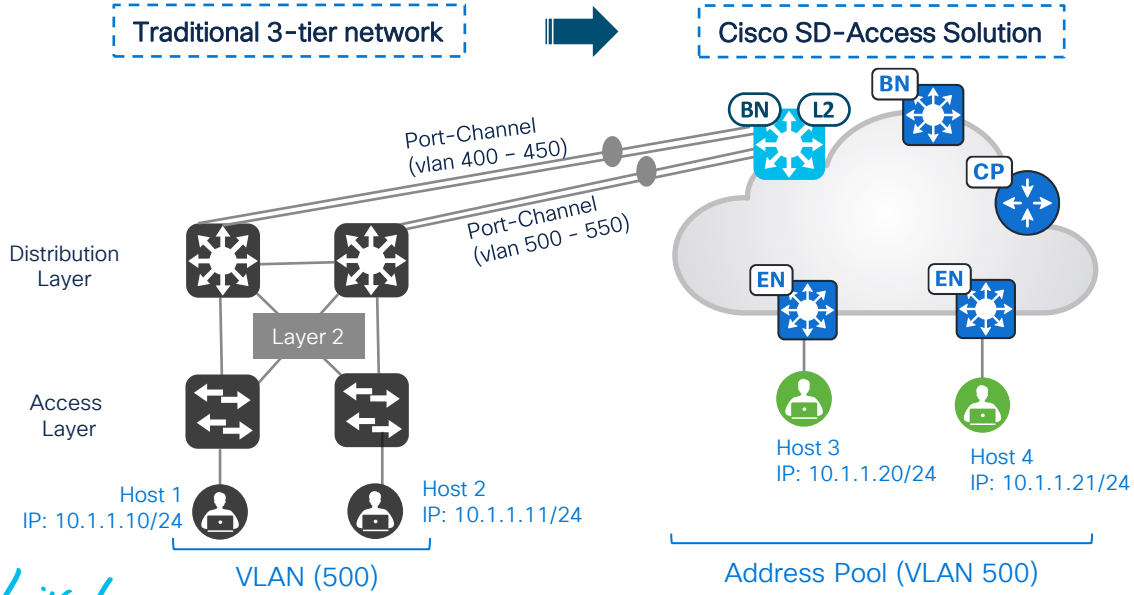


Migrating Port by Port

Cisco SD-Access

Fabric Migration Option - Layer2 Border Handoff

- Layer2 Border allows fabric and traditional network operate on the same subnet.
- Layer2 Border hosting the gateway functionality for traditional network



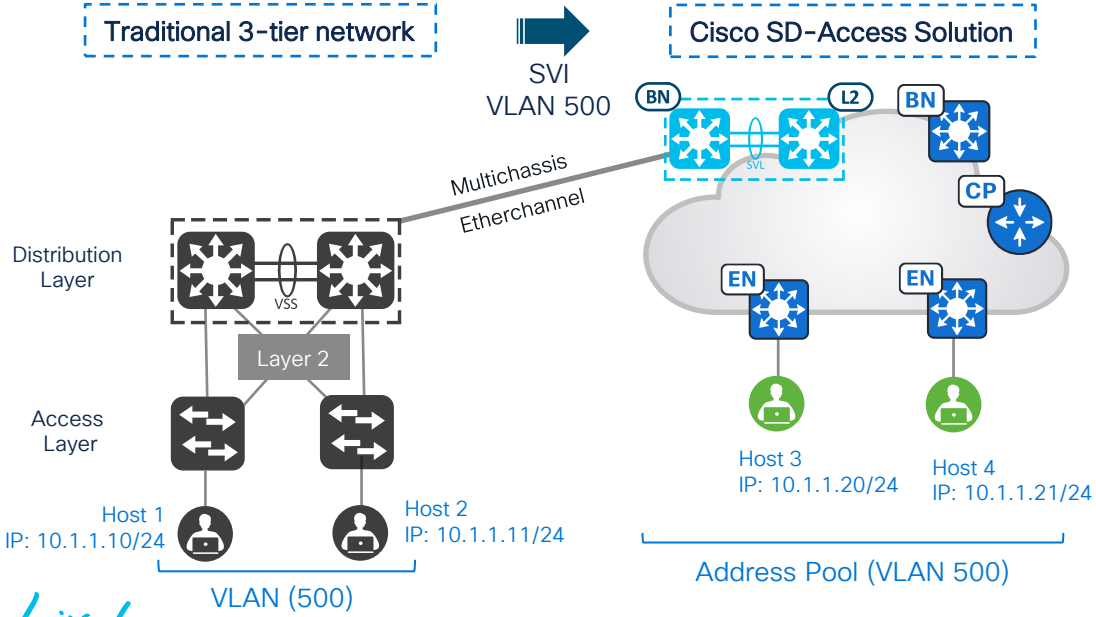
Migrating Port by Port

For your reference

Cisco SD-Access

Fabric Migration Option - Layer2 Border Handoff

- Layer2 Border allows fabric and traditional network operate on the same subnet
- Layer2 Border hosting the gateway functionality for traditional network

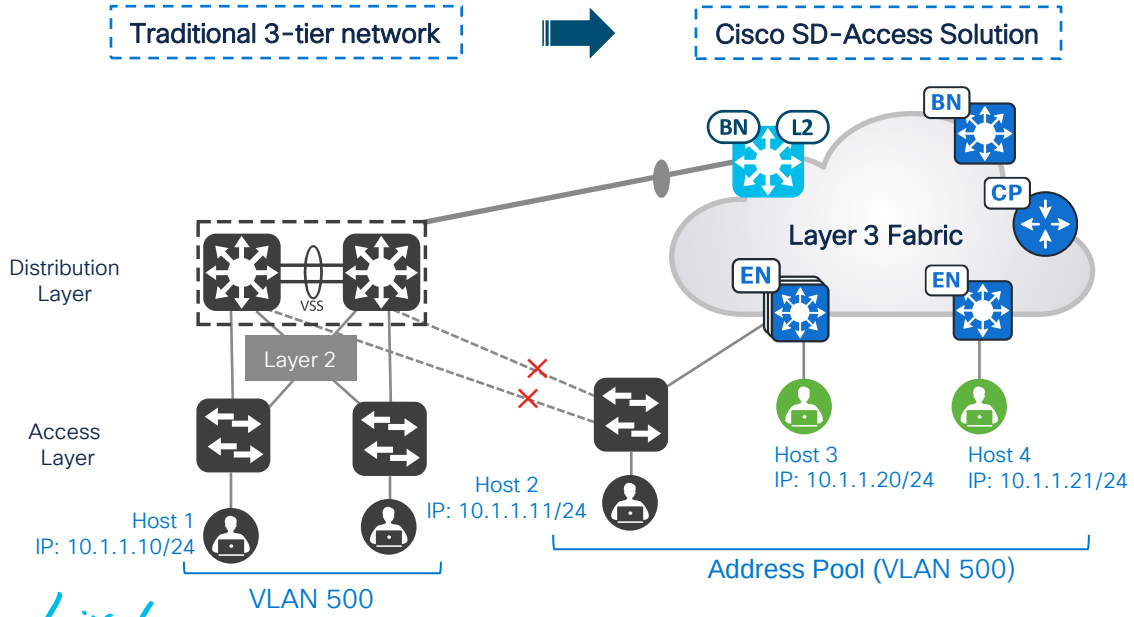


Migrating Port by Port

Cisco SD-Access

Fabric Migration Option – Retain Layer2 access layer

- Connect layer 2 access-switch (or) 3rd party switch to Edge node via trunk link.
- Edge node hosting the anycast-gateway.



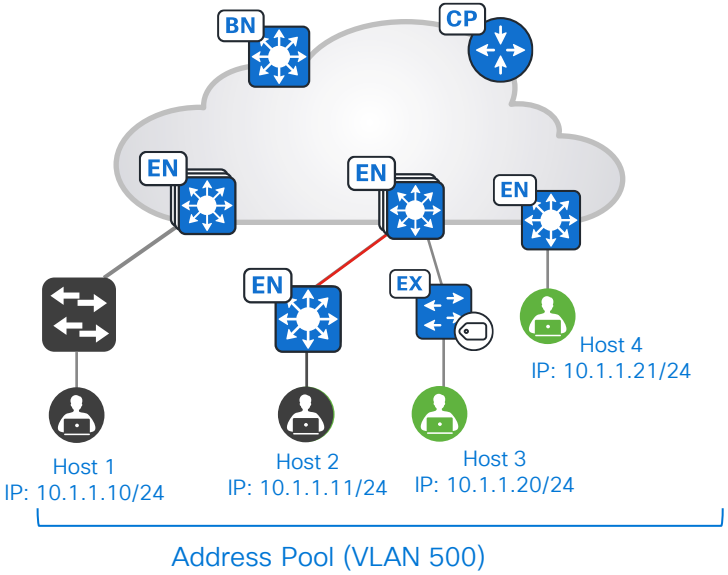
Retaining existing Layer 2 switch in Fabric provides

- Virtual Network segmentation
- SGT will be based on VLAN-SGT binding on the Edge node.

Cisco SD-Access

Fabric Migration Option – Convert Layer2 access layer

- Retain layer2 Switch
- Convert layer2 access-layer to Edge or Policy Extended Node role



- Retain Layer 2 access-switch
- Migrate Switch into Edge role

For your reference

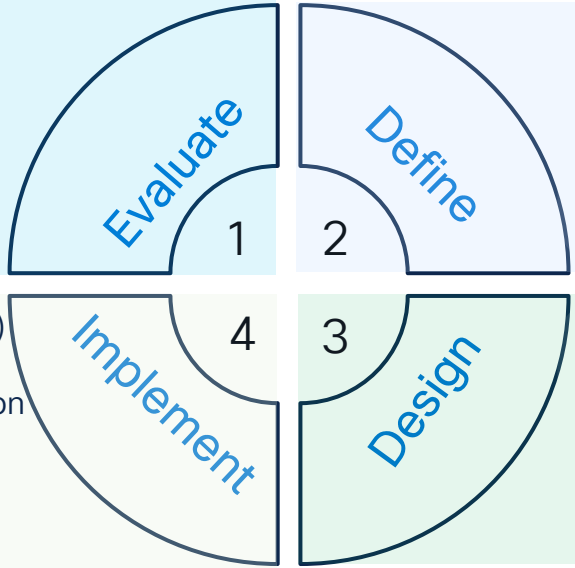
Cisco SD-Access Deployment Lifecycle

For your reference

Cisco SD-Access

Deployment Lifecycle

- Understand current network
- (wired, wireless, IoT, WAN)
- Platform in the network
- Endpoints, traffic types
- Subnets
- Current access-policies



- Segmentation (macro, micro)
- Policy/access-control
- Single or Multi site
- Scale
- Integration with other domains

- Hands on - Lab it !(small-scale PoC)
- Learn the technology.
- Leverage workflow-based automation to built robust network
- Validate your network
- Continue to add usecases
- Integrate with ecosystems

- Start small and build to scale
- Research and pick right platform
- Segmentation strategy
- Strategize for robust/resilient network
- Migration strategy
- Leverage Design Tool to help here..

https://fwm.cisco.com/

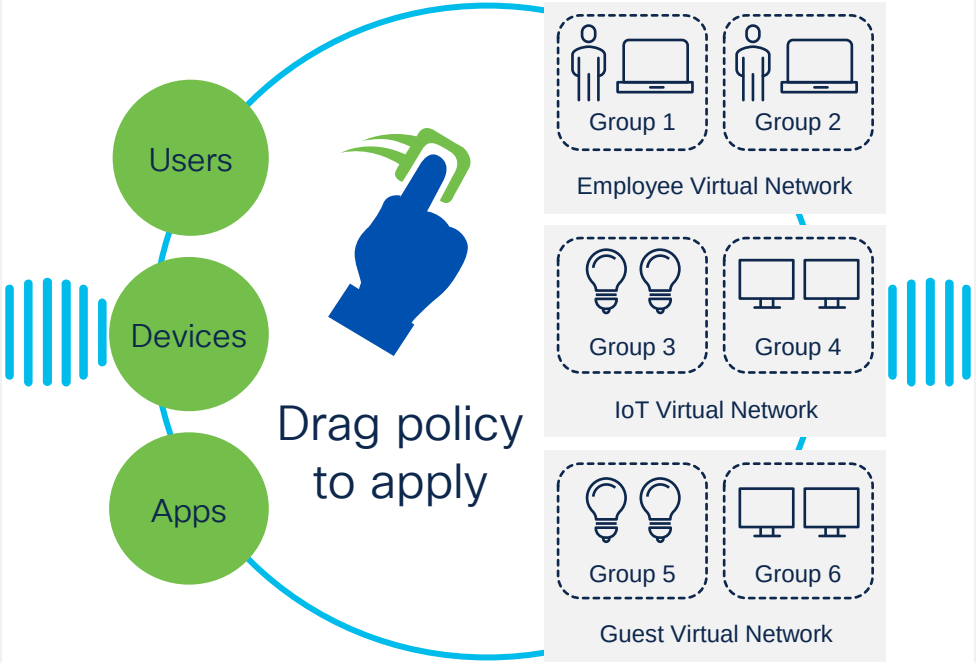
Summary

Secure onboarding of users and devices

Segmentation and Access Control

Before SD-Access

- VLAN and IP address based
- Create IP based ACLs for access policy
- Deal with policy violations and errors manually



After SD-Access

- No VLAN or subnet dependency for segmentation and access control
- Define one consistent policy
- Policy follows Identity

Completely Automated | Group-Based Policy | Policy follows Identity

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/dnacenter

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

cs.co/en-cvds

Validated Architectures, Prescriptive Guidance, Confidence to Deploy

- 6 Validated Design Guides
- 12 Prescriptive Deployment Guides

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

Thank you

cisco Live!

ALL IN

#CiscoLive