



# 1 to 100

Master All Steps of Deployment, Integration,  
and Migration of Large SDA and SD-WAN Networks

Dhrumil Prajapati - Principal Architect  
Jennifer Bowman - Principal Architect  
BRKENS-3834



# Webex App

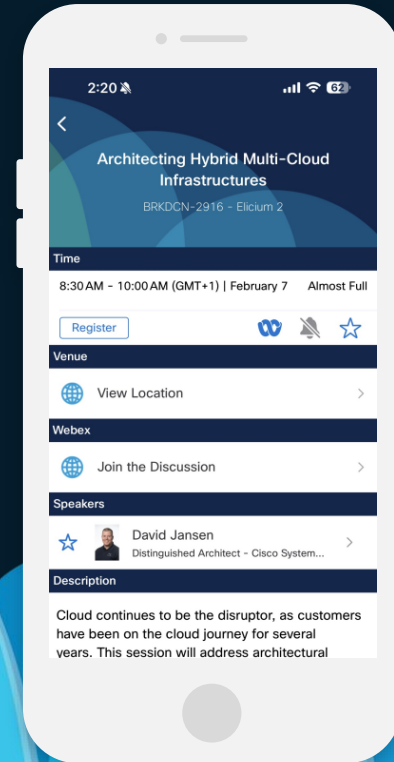
## Questions?

Use the Webex app 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 the Webex app or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

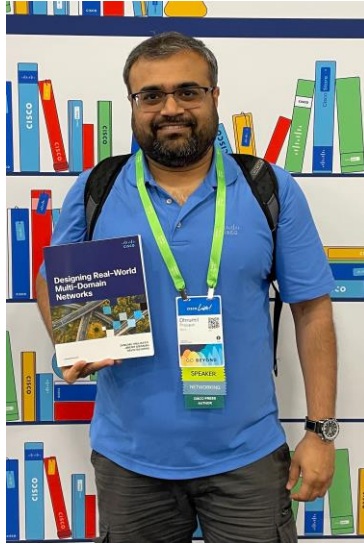
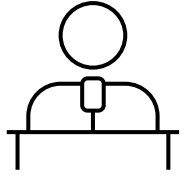
Webex spaces will be moderated by the speaker until February 28, 2025.



# Agenda

- Introduction
- Design and Deployment Best Practices
  - SDA & SDWAN Integration
  - 100,000ft view on Multi-Domain Design
- Deployment and Migration Lessons Learned from Large Scale Deployments
  - Having a solid Foundation
  - What is the migration process?
  - Lessons Learnt
- Conclusion

# Who are we?



## Dhrumil Prajapati

Principal Architect

GES Architectures - CX

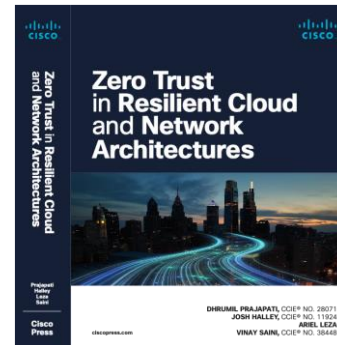
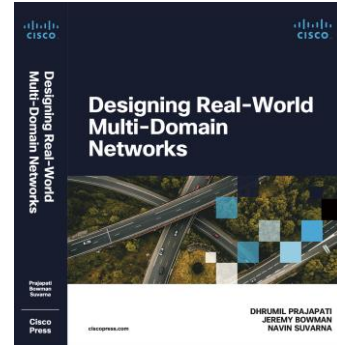
10+ Years @ Cisco

CCIE #28071 (R/S, SP)

CCDE #20210002

**Specialized in:** SD-Access, SD-WAN, MPLS, Multi-Domain Networks, Cloud, Automation

@DhruPrajapati



**cisco** Live!

# Who are we?



## Jennifer Bowman

Sr. Delivery Architect

Cisco CX

10+ Years @ Cisco

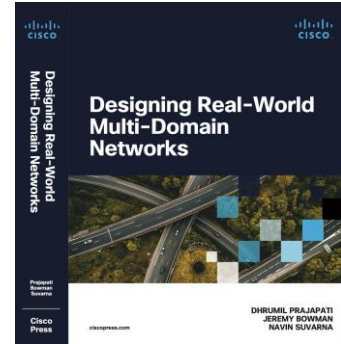
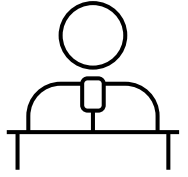
CCIE #51241 (Security, R/S)

CCDE #2018::16

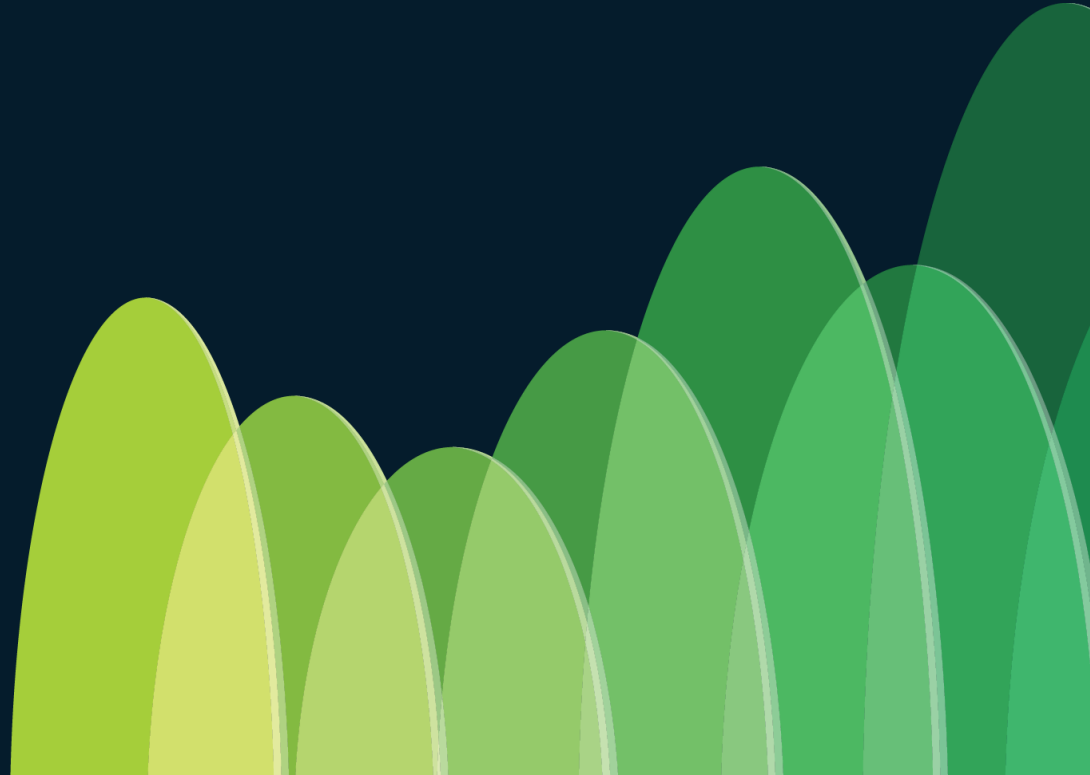
Specialized in: Full Enterprise IBN  
with Security and Automation

@ibnsrevenge

[jdb1@cisco.com](mailto: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

- Catalyst Center and Manager integration
- SDWAN Manager owns each cEdge and assigns to Catalyst Center
- Provision SDA specific changes through Catalyst Center, SDWAN specific changes via Manager

## • 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 Catalyst Center and Manager

Host Name/IP Address

172.31.23.236

Username\*

admin

Password\*

\*\*\*\*\*

Port Number\*

8443

vBond Host Name/IP Address

vBondhosts

Organization Name

sdwan-overlay

Partner Id

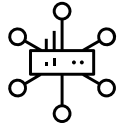
5eebb9909962950017a3a725



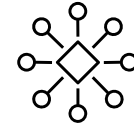
# Really Really High-Level View



SD-Access  
Catalyst Center



SD-WAN  
Catalyst Manager



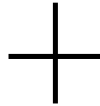
ACI  
APIC Controller

Campus  
and IOT

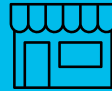


Users and Devices

Identify and Onboard Everything  
Authenticate and Authorize Access

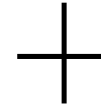


Branch &  
WAN



Hybrid Cloud

Deliver Great Application Experience  
Secure Internet and Cloud Access



Cloud &  
Data Center



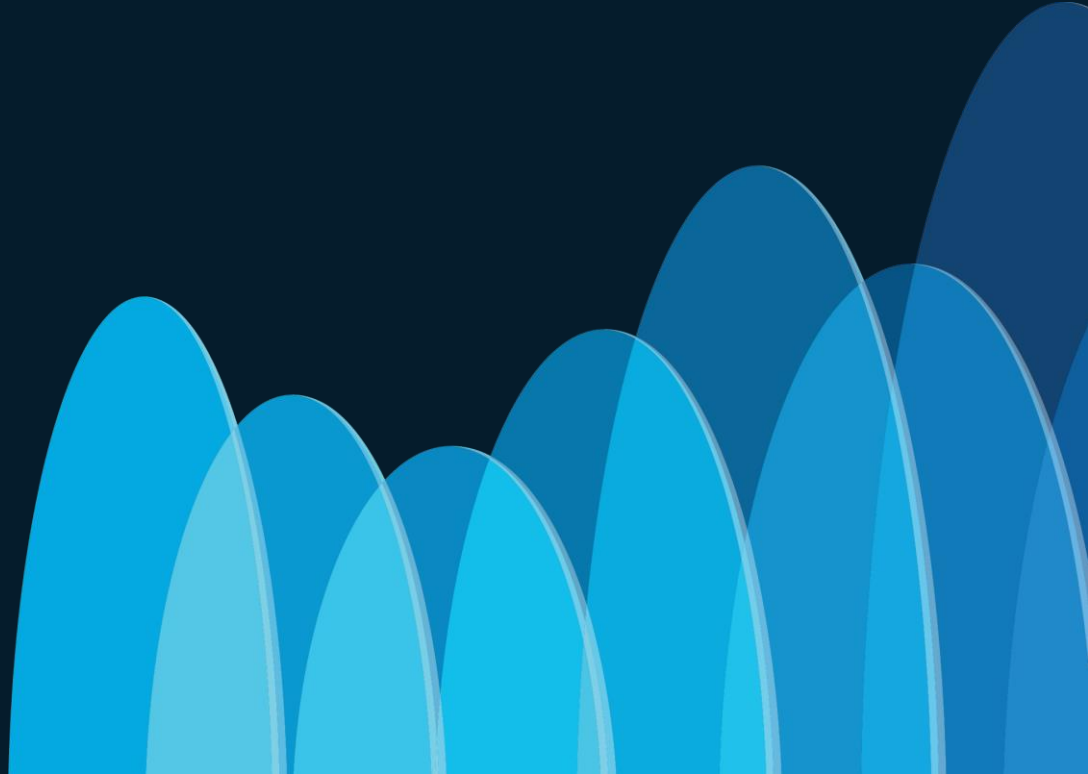
Data & Applications

Automate Resource and Workflows  
Prevent Data Breaches

# 100,000 ft view

- SDA
  - Endpoints dynamically assigned SGTs and placed into VNs
  - Macro and Micro-segmentation
  - Unified wired and wireless networks
- SDWAN
  - Extends and bridges segmentation
  - Applies Catalyst Center per-VPN security and application policy.
  - Enables end-to-end segmentation

# What did we learn from Large Deployments?



# SD-Access and SDWAN Deployments



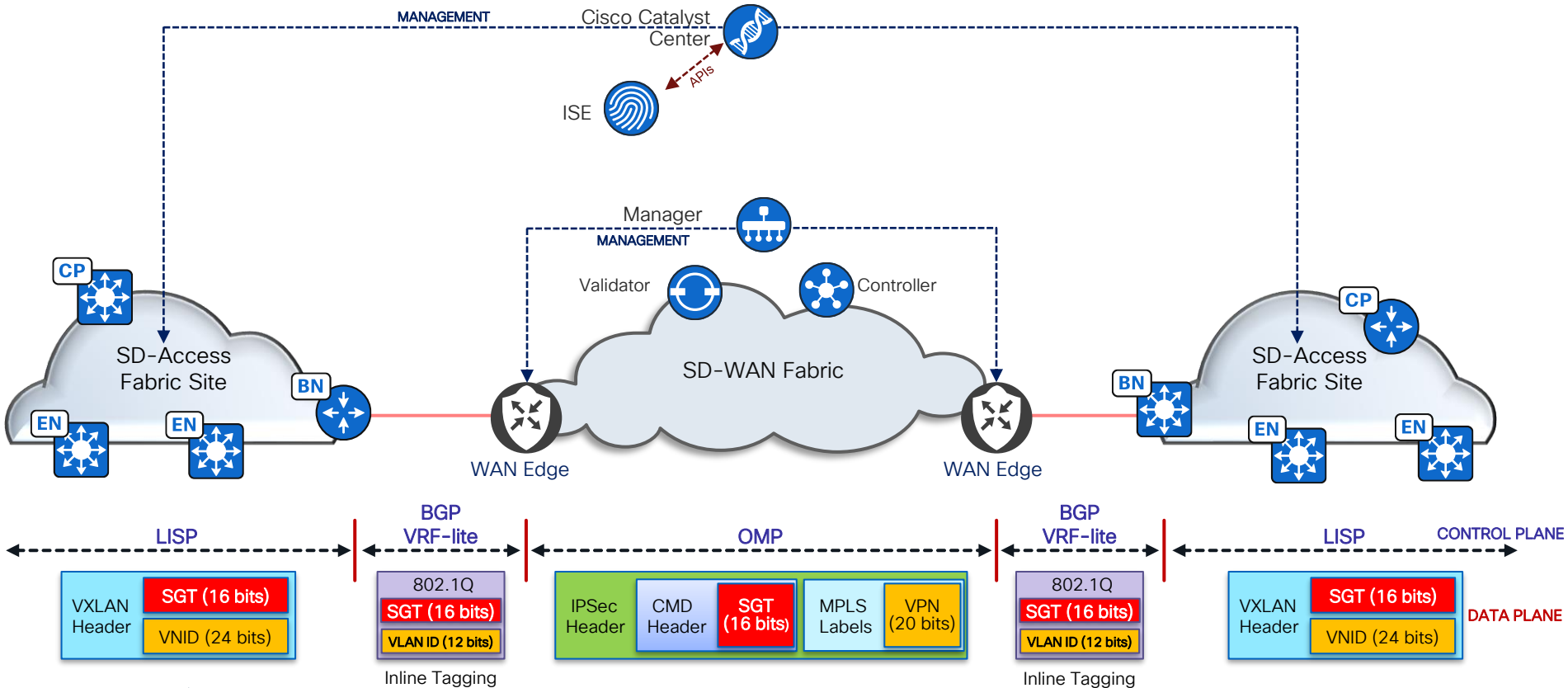
- Today available in partly manual “two-box” solution
- Two-box solution (non-integrated solution)
  - Clear demarcation between SDA and SDWAN architectures
  - SDA BNs can be ISR4K, ASR1K or Cat9K switches, SDWAN edges can be ISR4K, Cat8k or ASR1K series routers
  - SD-Access and SDWAN designs can be implemented at a different pace

# SD-Access and SDWAN Deployments

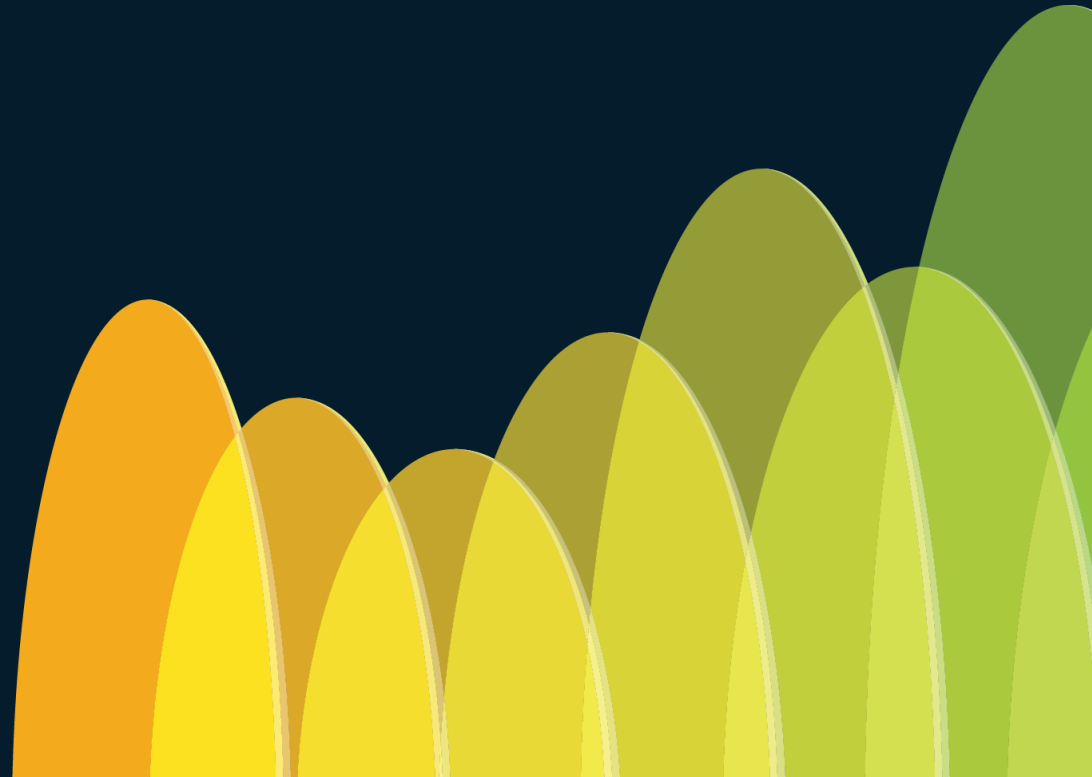


- Majority of customers have employed **two-box solution** for modularity of deployment and flexibility in operations
- Mapping of VNs and VPNs is crucial
- Inter-site traffic flow greatly depends on **SDWAN tunnel design** and **SDWAN underlay**.
- For Multi-Regional (Global) networks, consistency across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

# SDA to SDWAN Integration (Two-Box)



# Migrating the Beast!



Prepared by Dhrumil Prajapati  
BRKENS-3830  
Cisco Live US 2022

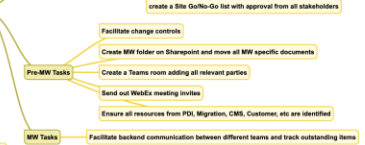
## SDA Site Deployment Checklist

### Plan, Design, Implement

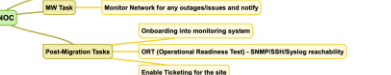
### One-Time Tasks



### PMO



### CMS/NOCC



### Customer



### Partner

### SD-WAN

### SDA

### Physical Installation

### Pre-MW Tasks

### MW Tasks

### Post-MW Tasks

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Spares to carry

### Migration Team

### Pre Checks

### Provision

### MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

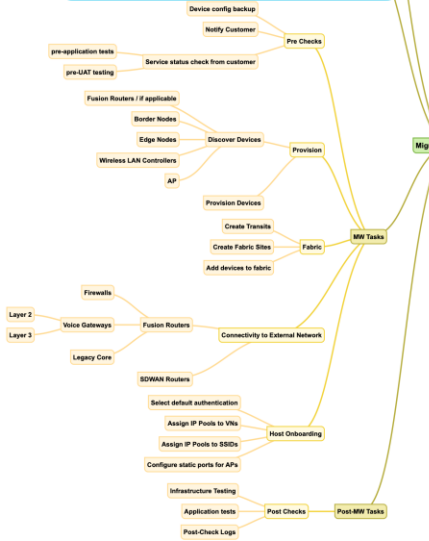
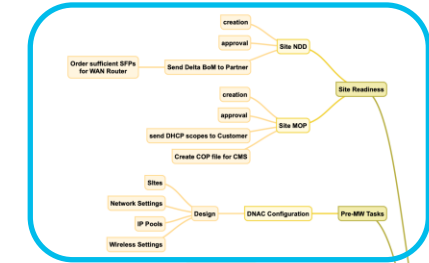
### Post-MW Tasks

### Post-MW Tasks

### Post-MW Tasks

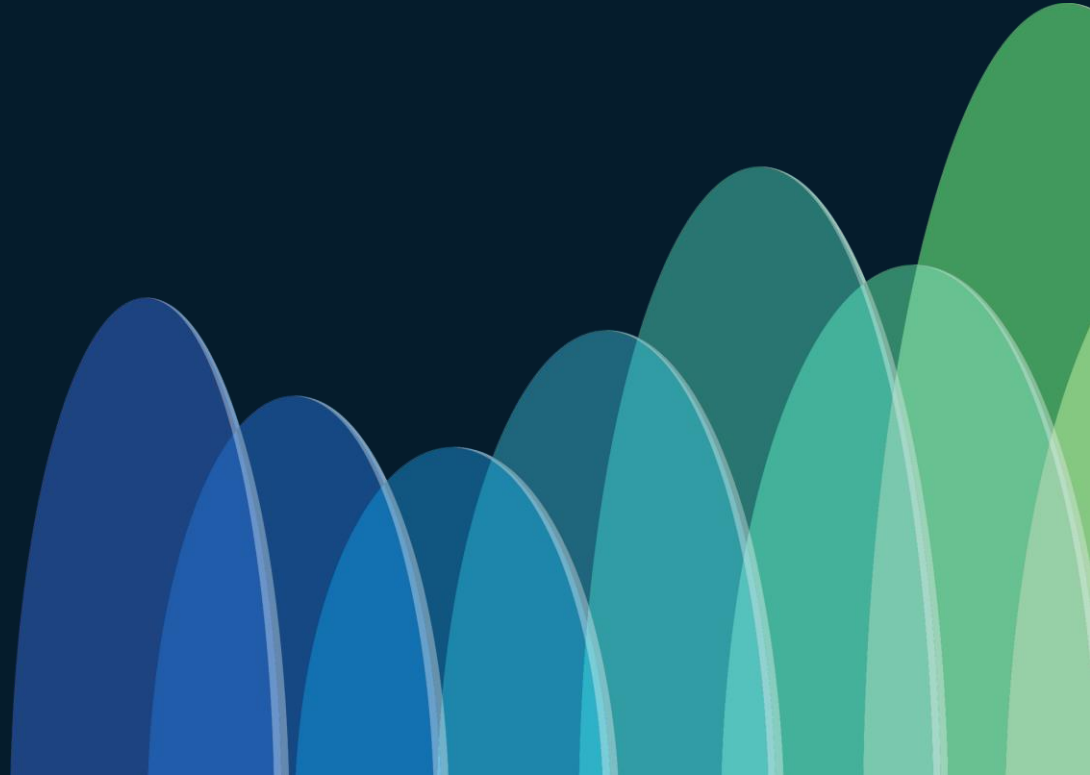
### Post-MW Tasks

### Post-MW Tasks

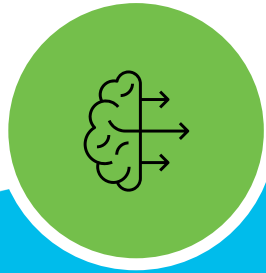




# Having a Solid Foundation



# 5 Pillars and a Bedrock



PDI/AMO



PMO



Migration  
Team



Customer



Partner

Automation

# Plan Design Implementation / AMO

## Design & Drive

CC ISE Integration  
AAA Certificates Fabric Domain  
SGT VN Policy Profiling  
KT and Pilot Sites

## Templates & Tools

Golden SDWAN Templates  
Endpoint Discovery  
Delta & Underlay Configs

## Testing & Validation

Testing XL,L,M+,SM,XS Design  
Snowflakes Validation  
L2BN functionality

## Post MW Hypercare

First 24hr hypercare support



Bringing stakeholders together



PMO : Build The City



Setting realistic schedules



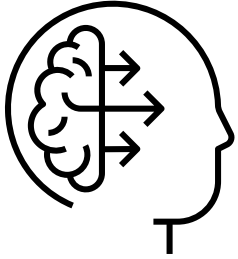
Chase timelines and engineer requests



Bridging the gap and ensuring good customer sentiment

**CISCO** *Live!*

# Migration Team



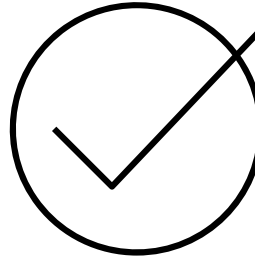
## Site Readiness

Network Design Document

BoM Preparation

MoP Preparation

Target Design

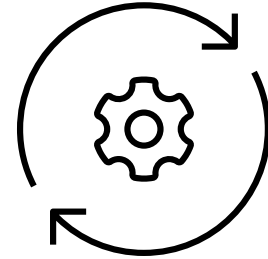


## Pre-Migration Window

Catalyst Center  
Configuration

Staging of Devices

UAT



## Migration Window

Discover & Provision

Add to Fabric – L2/L3

External Networks

Host Onboarding & Post Check

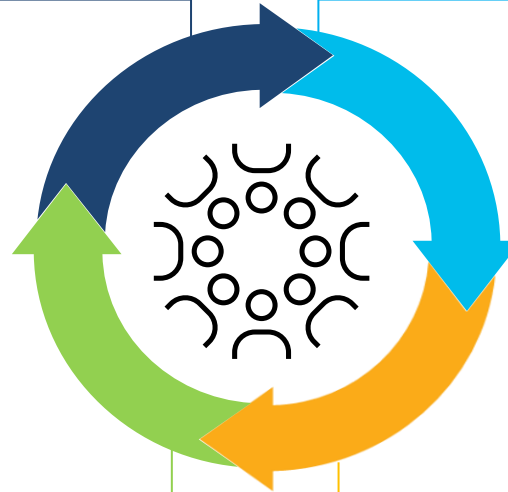
# Customer

## Site Readiness Tasks

- ✓ Circuit ID and Handoff Type
- ✓ Site Technical POC
- ✓ Site Survey Information
- ✓ Decommission of Old Circuit

## Migration Window

- ✓ User Acceptance Testing
- ✓ Circuit Provider Ticket if required
- ✓ Correct DNS on DHCP Scopes



## Pre-Migration

- ✓ Site Remediation Completed
- ✓ Adequate Power & Connectors
- ✓ Rack space & unmanaged devices

## Post-Migration

- ✓ Post Migration UAT
- ✓ Coordination with Cisco for wireless/wired Testing

# Partner

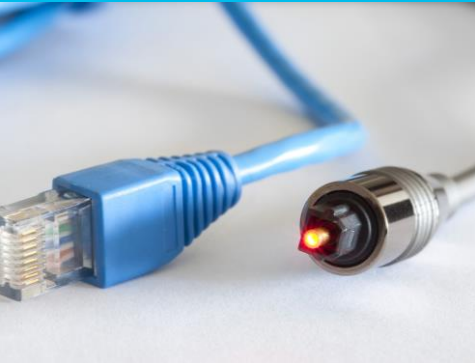
## Staging

- Code Upgrade
- License & eWLC package
- Load Bootstrap
- Manager Reachability



## MW & Post MW

- Cable Moves as per MoP
- AP mounting
- Device Cleanup & Decommission



## Pre-MW

- Verify on-site inventory
- Rack, Stack, Power
- Cable all Devices



## Readiness

- SFP : Copper & Fiber
- Cables: Console, Patch Cord
- Fibers: SMF, MMF
- Equipment: Label Marker

# Automation In SDA/SDWAN

## Why is it needed?



Large Site can have over 15000 endpoints

Validation & UAT can miss a lot of endpoints

## How Automation Helps



Underlay Config generator reduced MOP time



Reduced Migration Time with Fabric Config Generator



Site Snapshot & Overview of endpoints

## Automation Possibilities



Legacy Hardware Readiness & Assessment Tools



Endpoint Discovery & Site Overview



CC Site Hierarchy Push



Fabric Fusion Config Generator



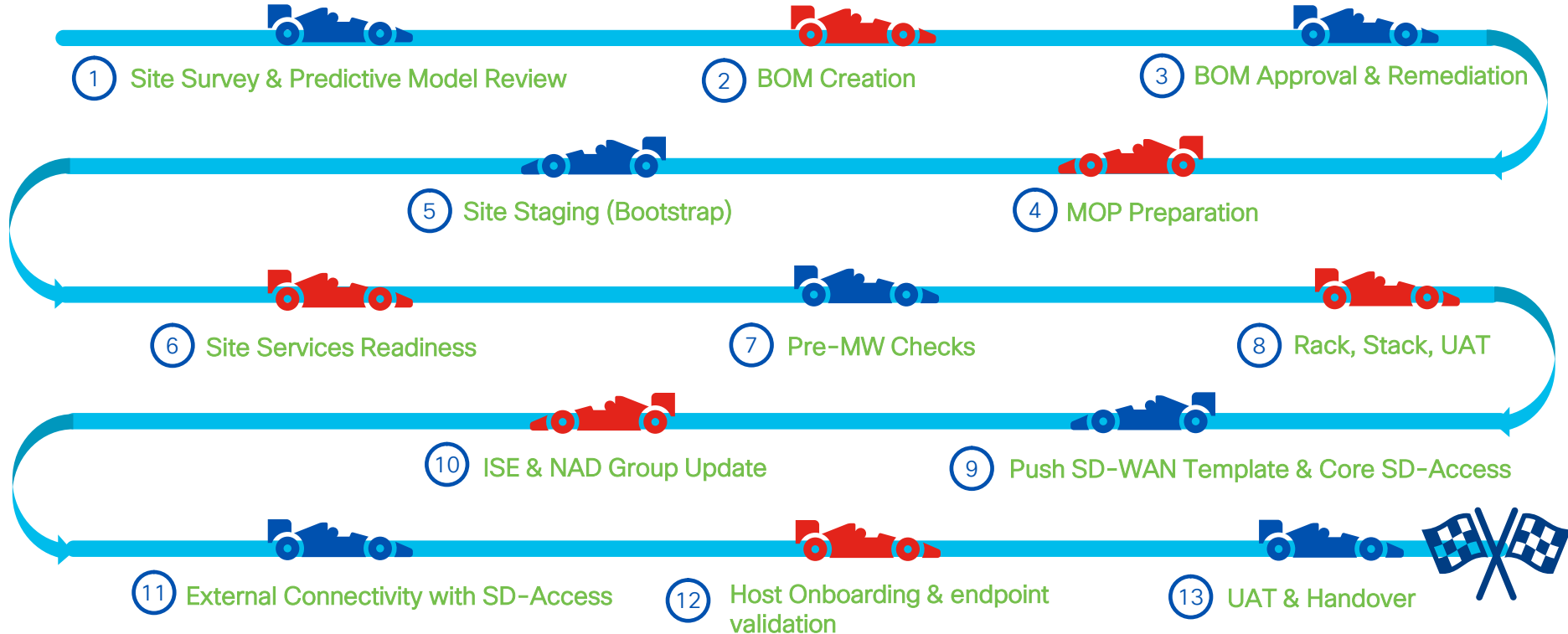
Pre & Post Ping Sweep and Routing Delta



# What is the Migration Process?



# Migration Pit Stops/Checkpoints



# Migration Approaches

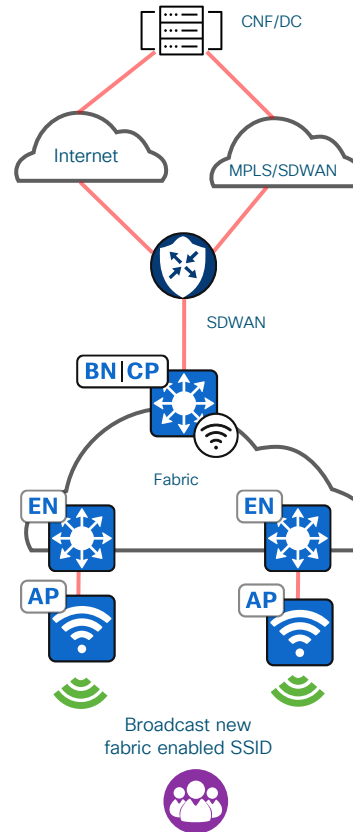
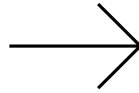
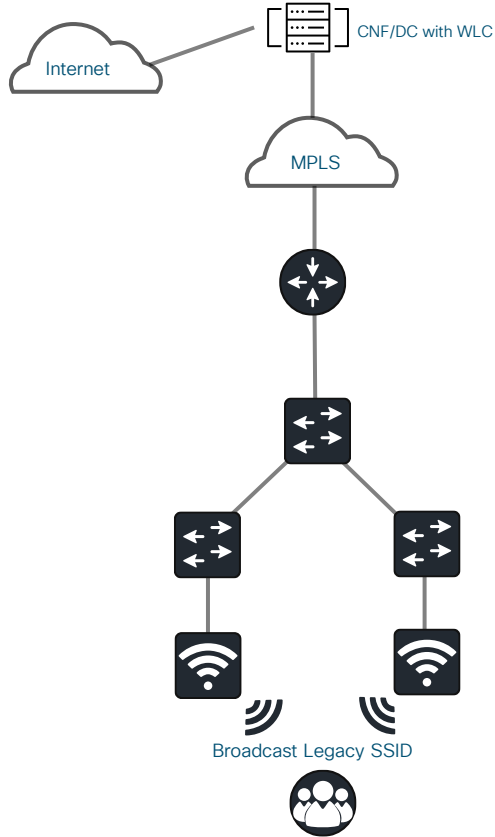
## Single Step

- Move from current state to end state in 1 Maintenance Window
- Suited for Small Sites
- Process:
  - Move to SD-WAN
  - Replace and/or upgrade LAN switches to SD-Access
  - Migrate SD-Access Wireless

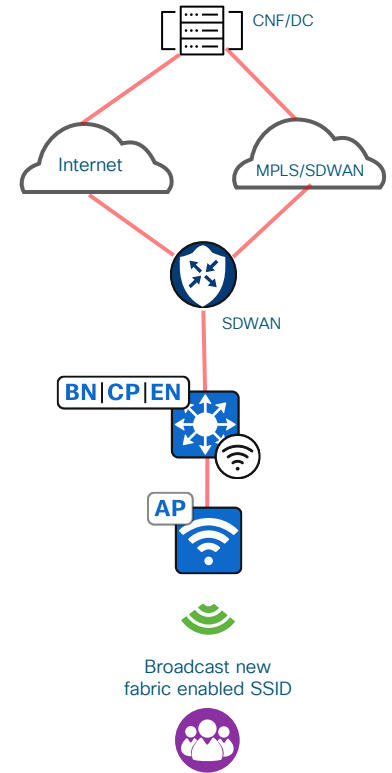
## Multiple Step

- Move from current to end state in multiple Maintenance Windows
- Suited for Medium to Large sites
- Process:
  - Day 1: SDWAN, Fusion and BN/CPs
  - Day 2+: Replace and/or upgrade targeted LAN closets to SD-Access
  - Migrate SD-Access Wireless

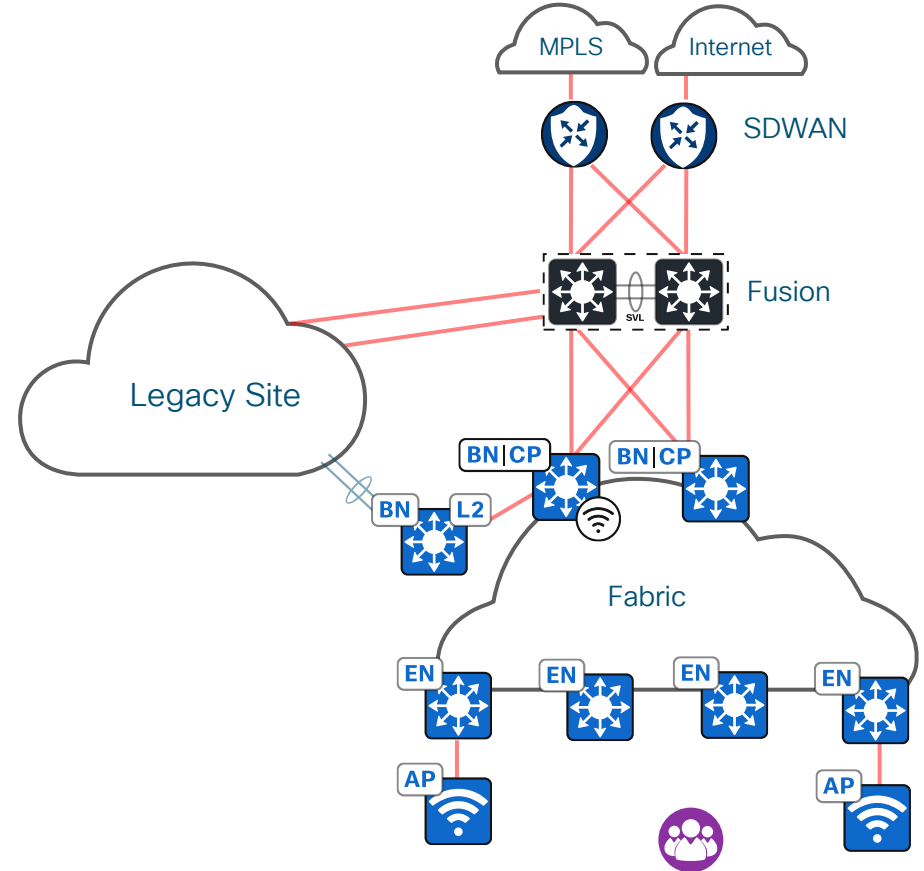
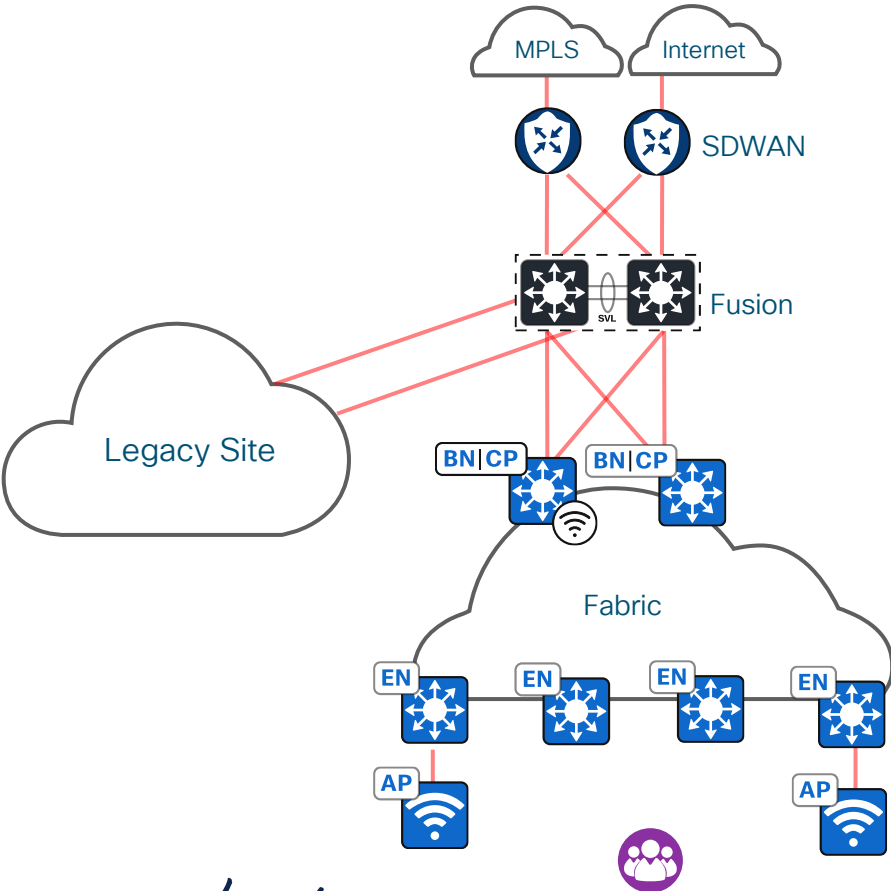
# Migration Approach – Single Step



OR

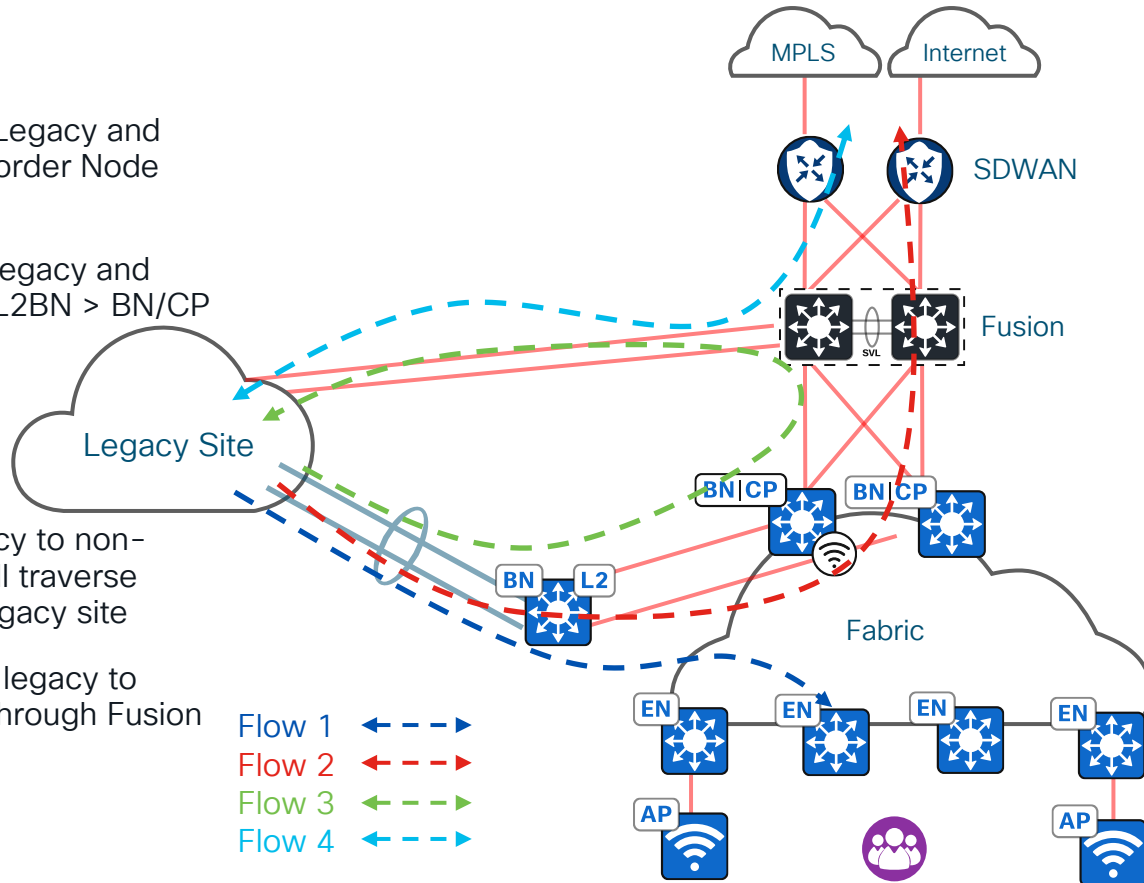


# Migration Approach – Multiple Step



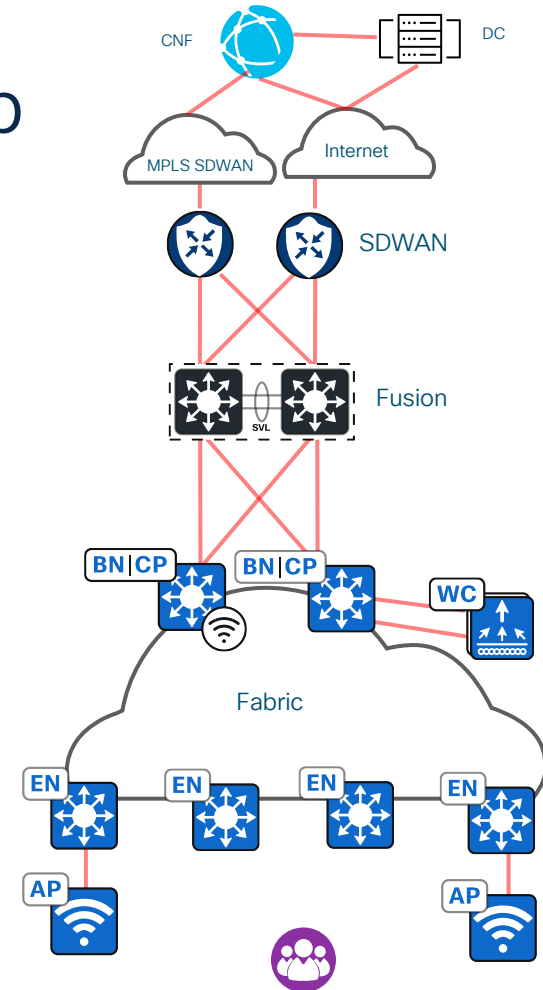
# Multi Step Migration with L2BN Traffic Flow

- Any migrated subnet traffic between Legacy and Fabric will traverse through Layer 2 Border Node (L2BN)
- Any migrated subnet traffic between legacy and remote location will traverse through L2BN > BN/CP > Fusion > SDWAN
- Any migrated subnet traffic from legacy to non-migrated subnet in legacy network will traverse through L2BN > BN/CP > Fusion > Legacy site
- Any non-migrated subnet traffic from legacy to remote location will traverse directly through Fusion > SDWAN

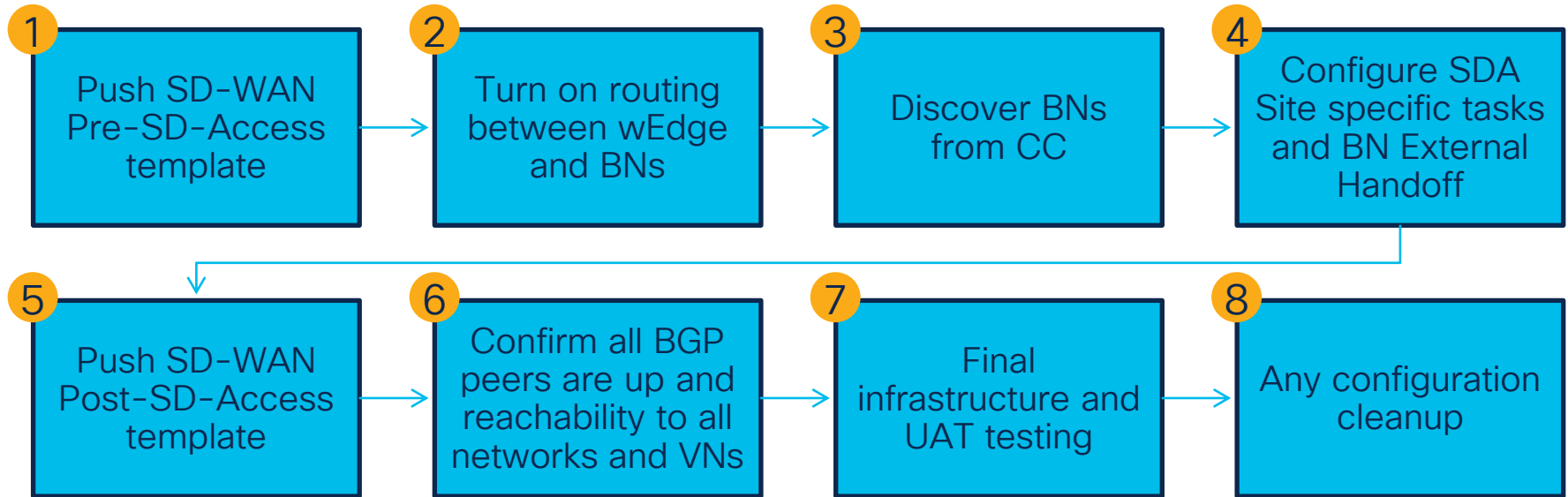


# Migration Approach – Final Step

- SDA Capable devices will be on boarded into the fabric
- Any temporary configurations will be cleaned
- Local C9800 WLC will be enabled for fabric mode and re-provisioned with fabric SSIDs
- All the APs will be provisioned to broadcast the fabric enabled SSIDs.

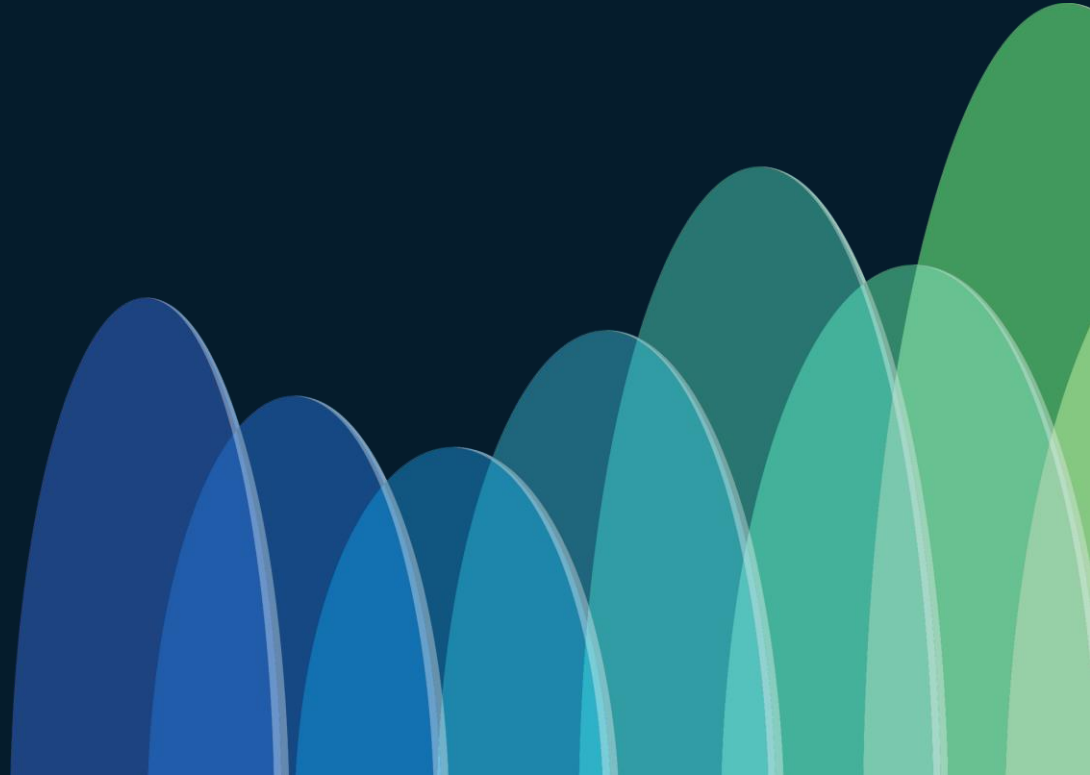


# SD-Access & SD-WAN Migration Steps





# Lessons Learned From Large Scale Migrations



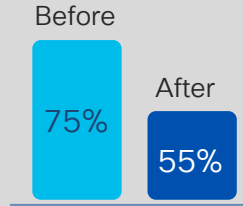
# Technical Learnings



Extensive UAT



Presence of Hubs



Automation



Catalyst Center  
Site Location



Reusable VLANs



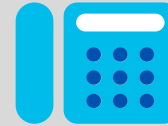
Interface & Tunnel  
Mismatch (SDWAN)



GUEST Portal Login



Static Endpoints



External  
Connectivity



Fabric Zones

# Technical Learnings Continued...



Circuit Tagging



Fusion & Legacy Core



ISE and Catalyst  
Center Sync



Manager GUI



L2BN VLAN 1



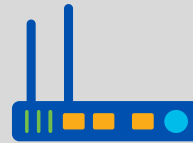
SDWAN Template Issue



DHCP Option 43



wEdge in CLI mode



Bandwidth Shaping

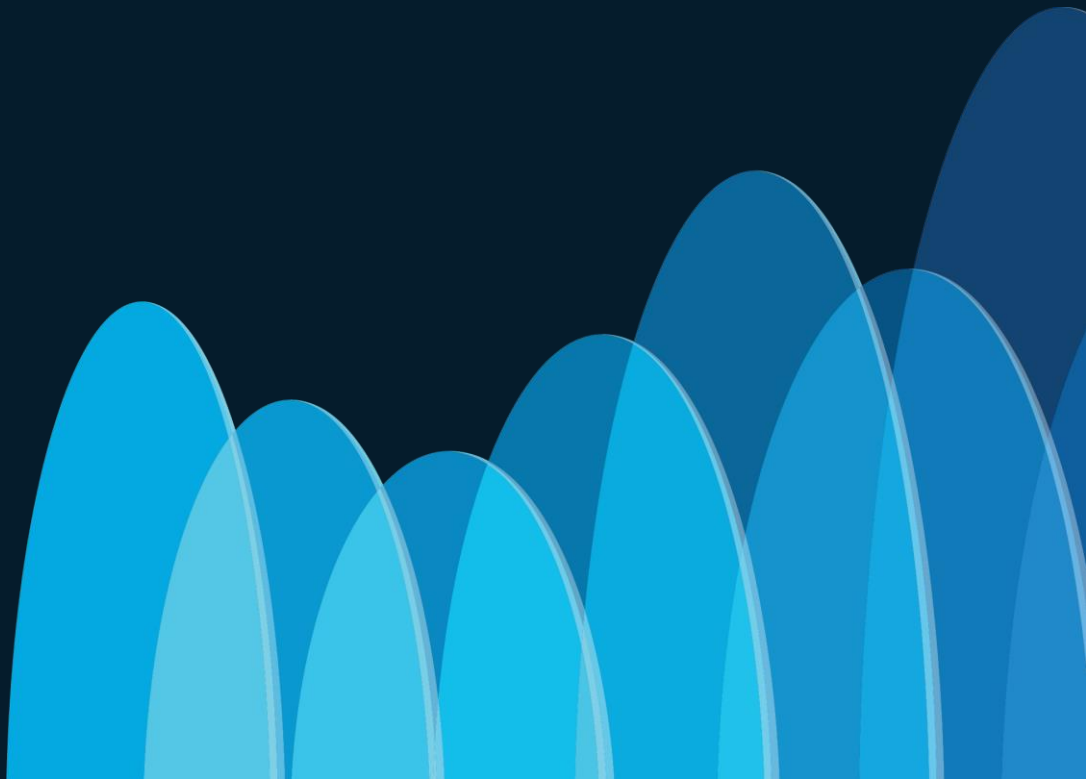


9600X SUP-2

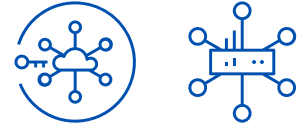
# Operational Issues

| On-Site                                      | Ad-Hoc                                  | Limitations         | Others                |
|--|---|---------------------|-----------------------|
| Circuit Testing, Circuit Handoff & labelling | Project Milestones & RACI               | Platform Limitation | Cross Team Dependency |
| Rack, Stack, Mount APs in Advance            | Snowflakes per Request                  | High burnout rate   | Hardware Upgrades     |
| BoM Lead Time                                | Scoping & Resourcing                    | Accountability      | Staging Facility      |
| Spare SFPs, Cables                           | Site Variations & Consolidation changes | Endpoint Visibility | Compliance            |
| Travel & Security Guideline                  | Unknown devices                         | Unmanaged Switches  | Timely Approvals      |

# Conclusion



# Key Takeaways



- 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

# Key Takeaways

- SD-Access and SD-WAN migrations **can be done** at rapid pace
- Consistency in design is key for at-scale migrations
- You are getting one chance to re-do the network – take that opportunity!
- Remember those **5 pillars**
- **Automation** is crucial for efficiency and accuracy
- **BEAST is not as scary as it seems!**
- **Cisco CX** is always there to work with you and accomplish success together.

# Webex App

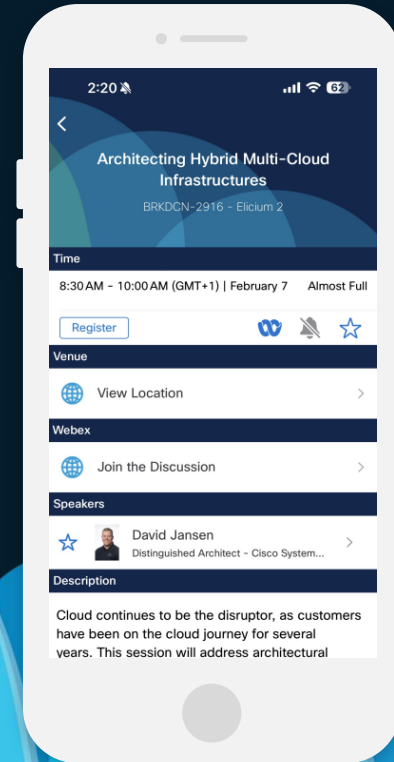
## Questions?

Use the Webex app 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 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 February 28, 2025.





# Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

---



All surveys can be taken in the Cisco Events mobile app or by logging into the Session Catalog and clicking the 'Participant Dashboard' link at <https://www.ciscolive.com/emea/learn/session-catalog.html>.



# Continue your education

CISCO *Live!*

- 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 [ciscolive.com/on-demand](https://ciscolive.com/on-demand). Sessions from this event will be available from March 3.

Contact me at: [dhprajap@cisco.com](mailto:dhprajap@cisco.com),  
[jenbowma@cisco.com](mailto:jenbowma@cisco.com)



Thank you

CISCO *Live!*

GO BEYOND

The background of the slide features a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are arranged in a way that creates a sense of depth and movement, resembling a stylized horizon or a series of waves. The overall aesthetic is clean and modern.