

The background features a vibrant, multi-colored abstract design. On the left, there are overlapping, wavy bands of color in shades of orange, red, and yellow. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Cisco and AT&T Partnership Bringing Success with SDA to Customers

A Customer Success Story

Syed F. Ahmed : Partner Solutions Architect – Cisco Systems, Inc.

TJ Kalis : Senior Network Architect – AT&T

CSSSPG-2100

Cisco Webex App

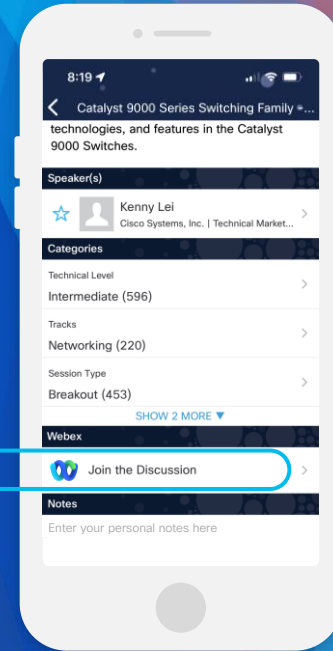
Questions?

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 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#CSSSPG-2100>

Networking

SD-Access

Learn about Cisco's Software Defined Access (SD-Access) solution that provides a secure, dynamic, and automated solution to meet the security and operational challenges faced by an ever-changing environment. The Cisco SD-Access sessions provide a comprehensive overview regarding best practices, design, deployment, migration, and monitoring of a Cisco SD-Access architecture.

START

Monday, June 5 | 10:30 a.m.

BRKENS-2810

Cisco Software Defined Access
Solution Fundamentals

Monday, June 5 | 1:00 p.m.

BRKENS-2811

Connecting Cisco SD-Access to
the External World

Monday, June 5 | 3:00 p.m.

BRKENS-2814

Role of Cisco ISE in SD-Access
Network

Tuesday, June 6 | 1:00 p.m.

BRKENS-2828

LISP Architecture Evolution - New
Capabilities Enabling SD-Access

Wednesday, June 7 | 10:30 a.m.

BRKENS-2502

Cisco SD-Access Best Practices -
Design and Deployment

Wednesday, June 7 | 1:00 p.m.

BRKENS-2819

Cisco SD-Access and
Multi-Domain Segmentation

Wednesday, June 7 | 3:00 p.m.

BRKENS-2833

LISP: Optimized Control Plane for
the Campus Fabric

Thursday, June 8 | 8:30 a.m.

BRKENS-3834

1 to 100 - Master all Steps of
Deployment, seamless Integration
and Migration of large SDA and
SD-WAN Networks

Thursday, June 8 | 10:30 a.m.

BRKENS-2827

Cisco SD-Access Migration Tools
and Strategies

Thursday, June 8 | 1:00 p.m.

BRKENS-3850

Demystifying multicast operations
in a multi-site SDA deployment.

FINISH

Agenda

- Service Provider in the Enterprise
- SDA with DNA Center at High Level
- Successful Deployment Including Lessons Learned
- Recommendations/Conclusion

Meet the Presenters



- Syed F. Ahmed
- Partner Solutions Architect
- 11 years at Cisco Systems
- CCIE #49025 Enterprise Infrastructure



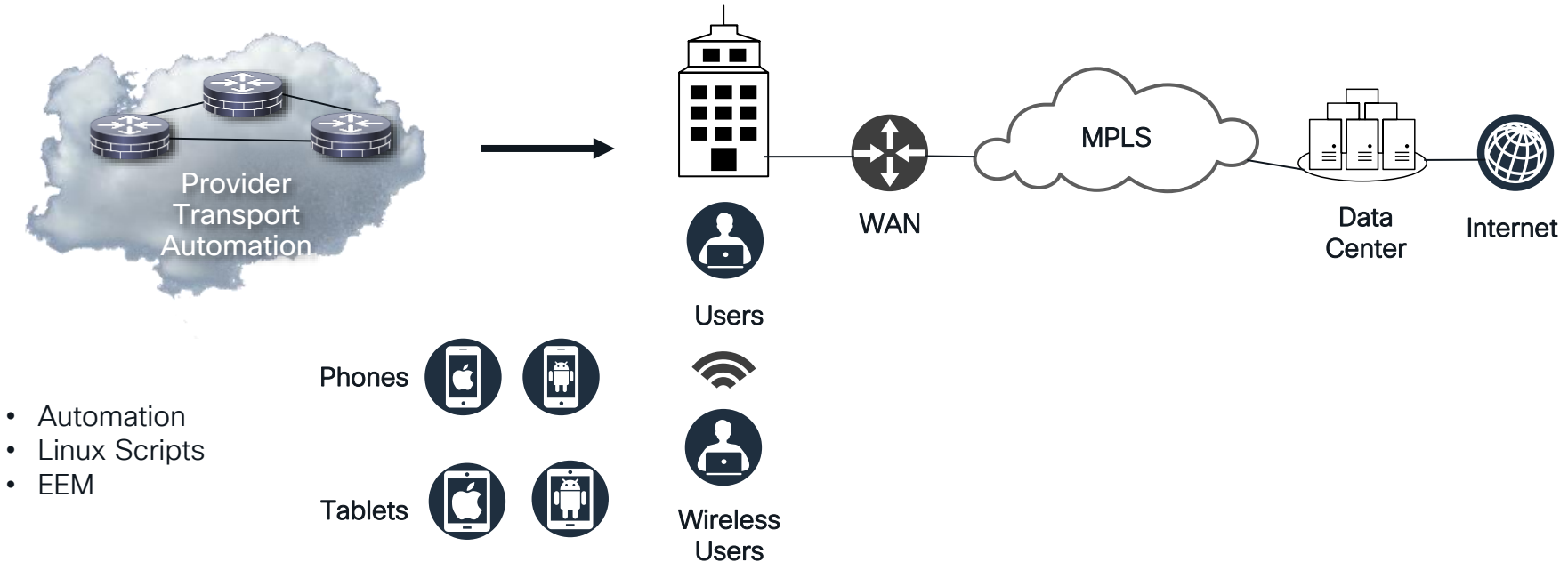
- TJ Kalis
- Senior Network Architect
- Over 20 years with AT&T
- CCIE #4666 Enterprise Infrastructure & Security

Service Provider in the Enterprise



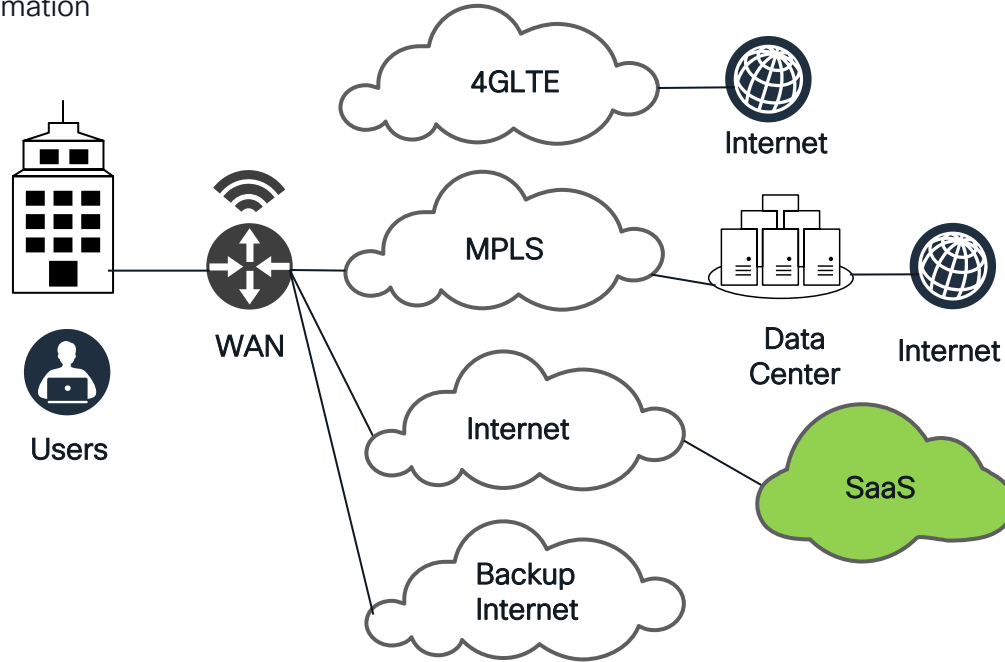
History of Backbone Transport to WAN Edge

Service Provider Automation
Evolution



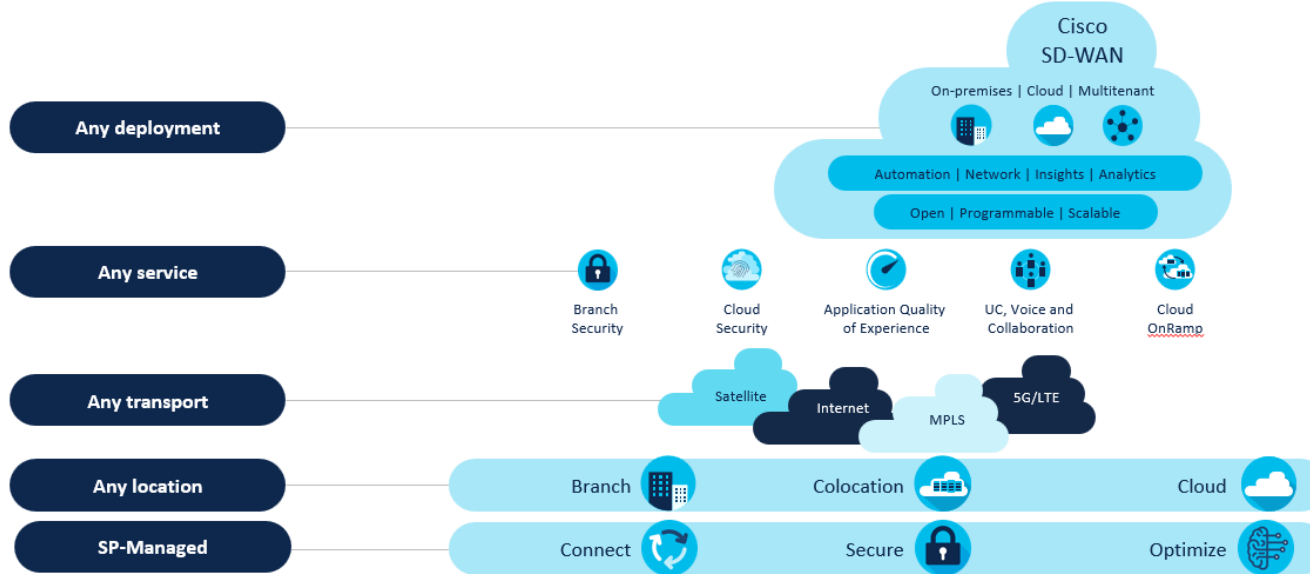
WAN Edge to Hybrid WAN

Service Provider Automation
Evolution

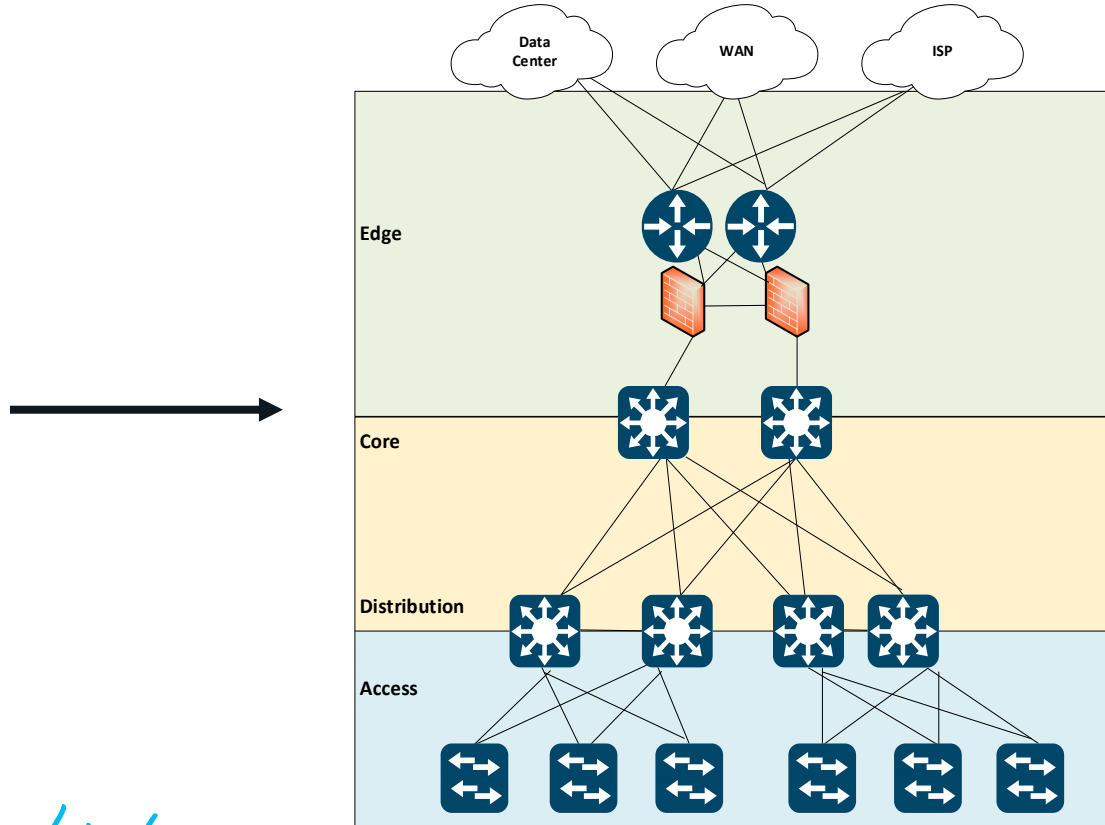


Hybrid WAN to Cisco Catalyst SD-WAN

Service Provider Automation
Evolution



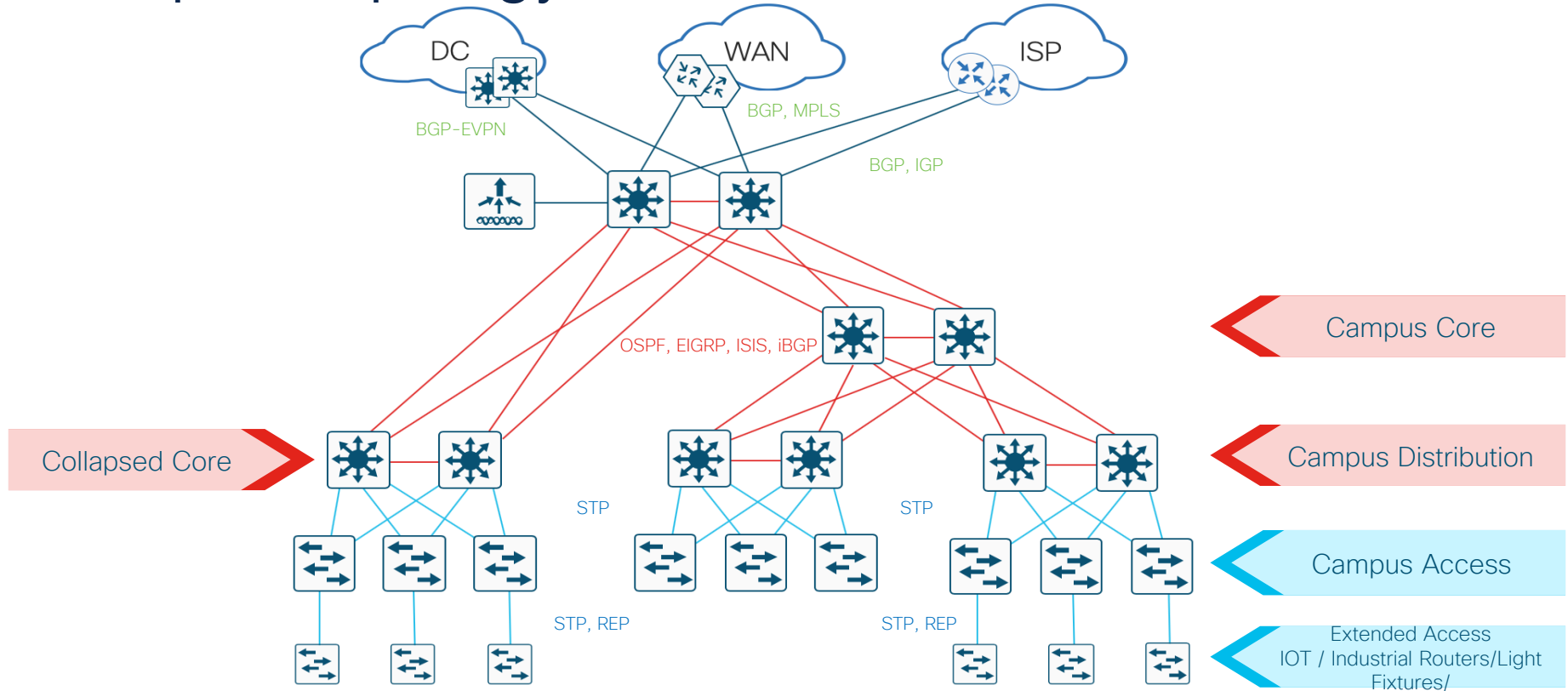
WAN Edge to the Enterprise Network



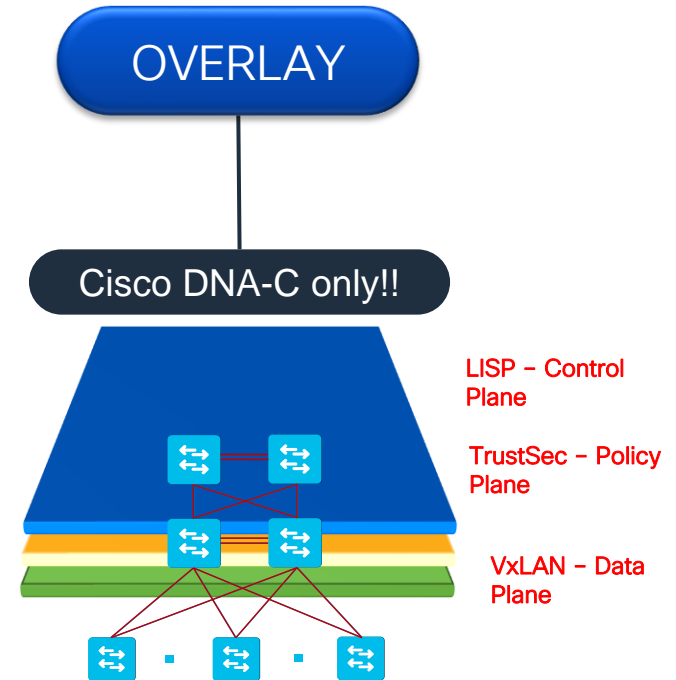
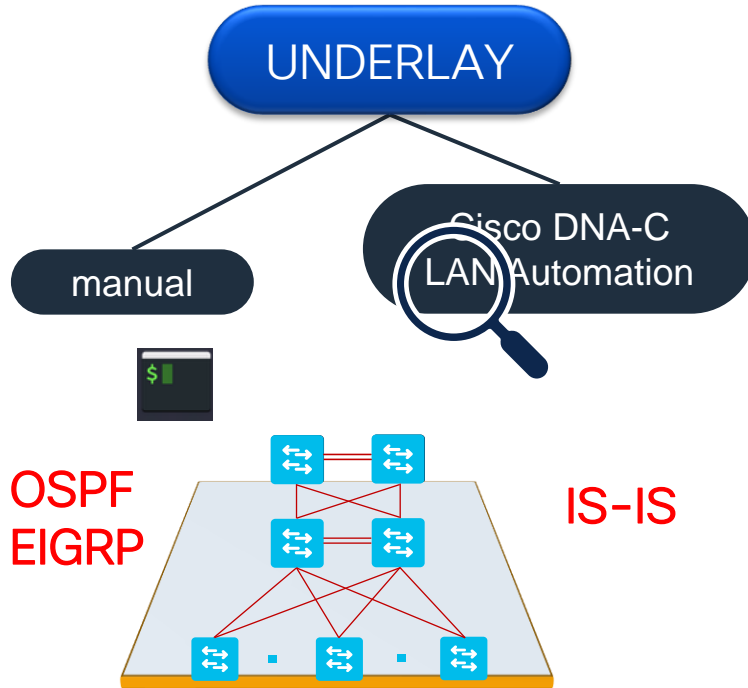
SDA with DNA Center at High Level



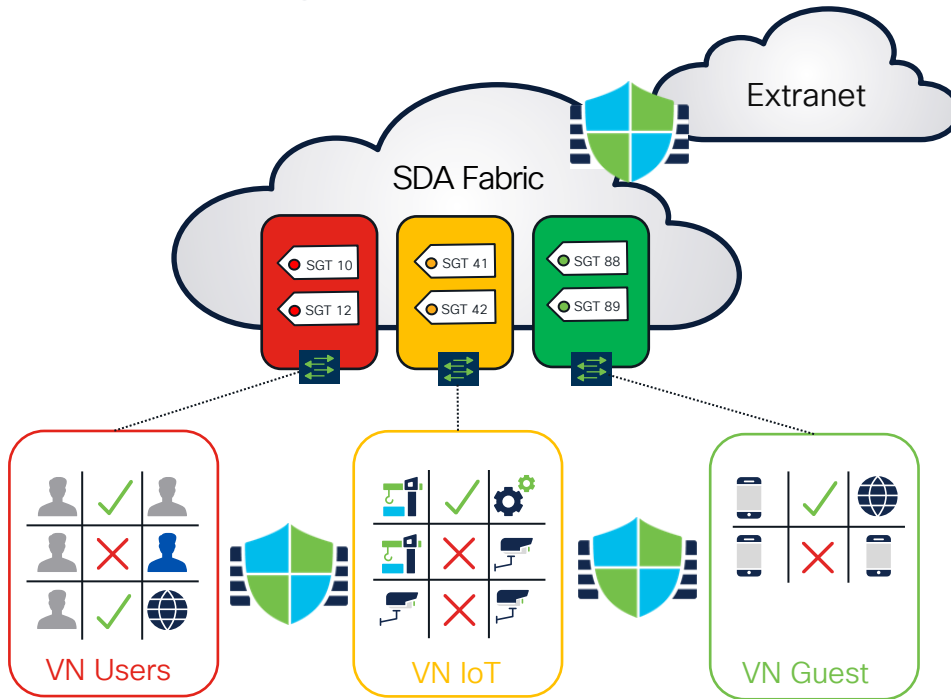
Campus Topology



Initialize the SDA Network



SDA Segmentation Basics



Virtual Network (VN)

First level Segmentation ensures **zero communication** between forwarding domains unless leaked by routing.

Scalable Group (SG)

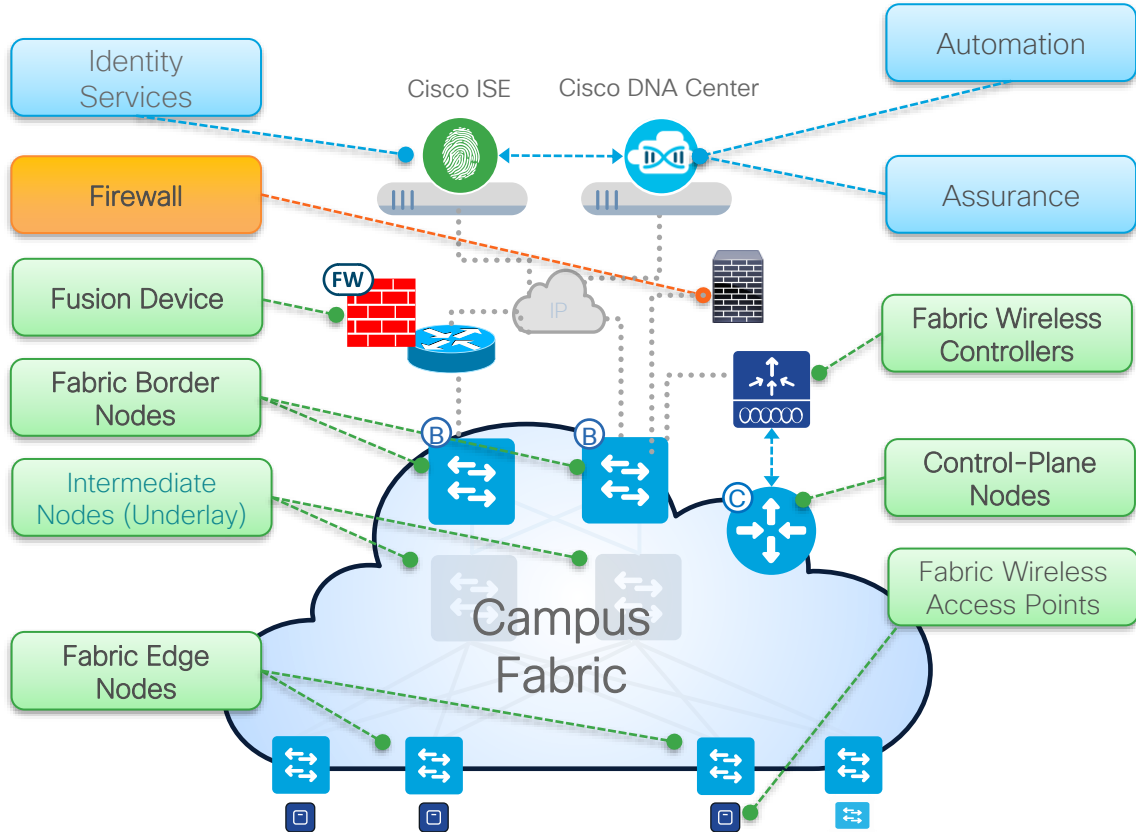
Second level Segmentation ensures **role-based access control (RBAC)** between two groups within a Virtual Network based on **contract**.

Fusion Firewall (FW)

Stateful enforcement for inter-VN and VN to Extranet segments.

Cisco SD-Access

Fabric Roles & 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
- **Fusion Device** – Connects fabric segments to global routing segments
- **Firewall** – ASA, FTD, non-Cisco FW used for stateful inspection of Fabric and non-Fabric traffic.

Success Story :

AT&T and Cisco
delivering best of
breed network,
hardware,
applications and
services together



Success Story / Lessons Learned



Customer Environment

Innovation Center

- Part of a larger global corporation based out of USA
- High visibility business unit
- Showcase site for new technology
- Multi-collaboration partner hub



Key Architectural Requirements for the Solution

- Flexible, agile, automated security policy and segmentation
- Easy device onboarding
- Consistent network configuration
- Consolidated security policy for wired and wireless endpoints
- Enhanced network visibility and assurance

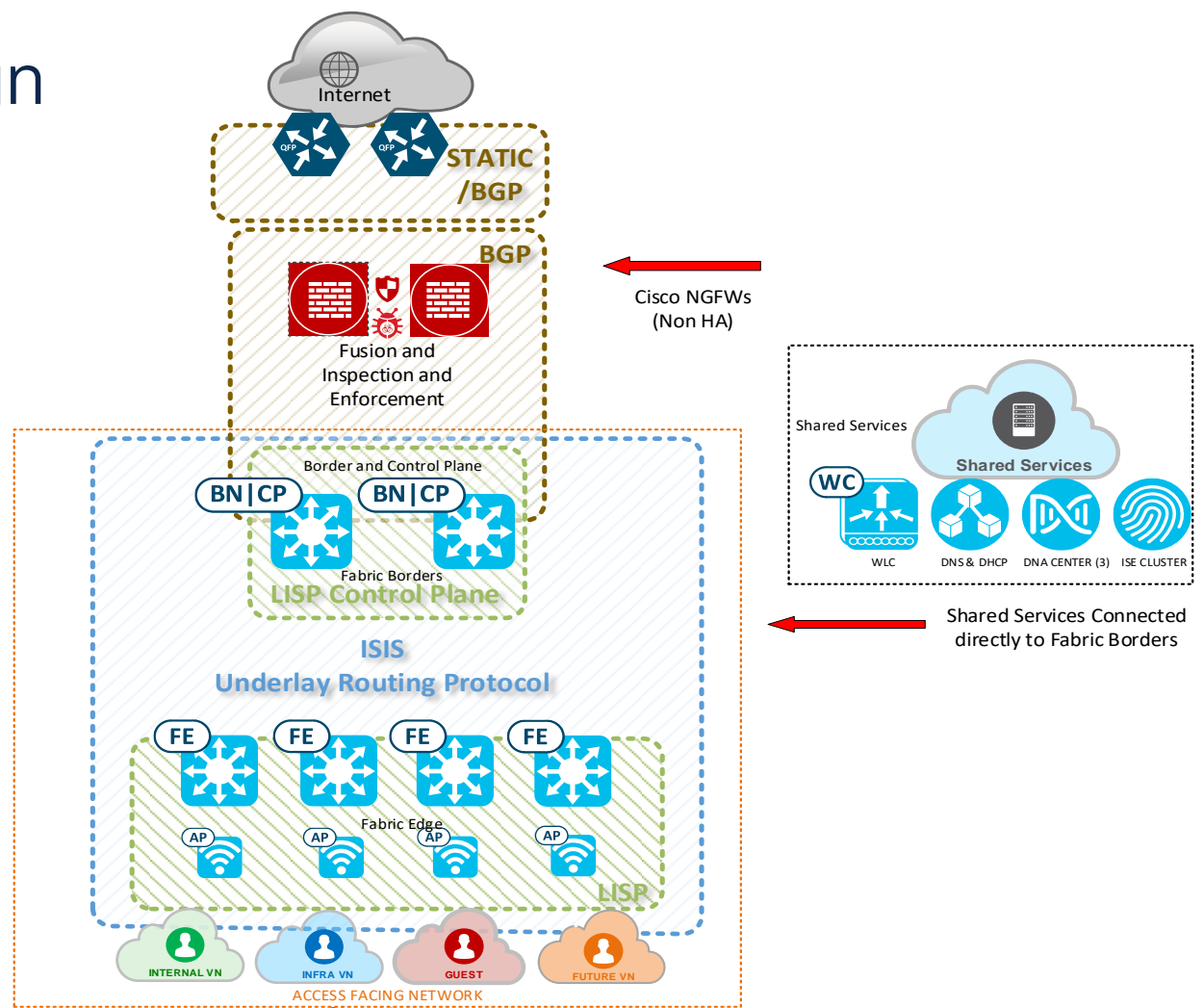
Initial SDA Architecture

- Built in the theme of an innovation showcase
- Early adopter of the technology
- Investment with limited funding
- Simple basic design according to the initial requirements
- Need for additional resilient design was requested

State of the Customer and Network

- Existing single site SDA deployment
 - Business unit success exceeded expectations
 - Growth expected at existing site
- Second SDA site to be deployed in early 2022
- More funding and multi-site requirement
- Future sites coming in late 2023 / early 2024

Original Design



Identified Pain Points with Existing Design

Cisco NGFWs not
deployed in high
availability design

Out-dated software
versions across
entire environment

No end-to-end
dynamic routing

Shared services
directly connected
to border nodes

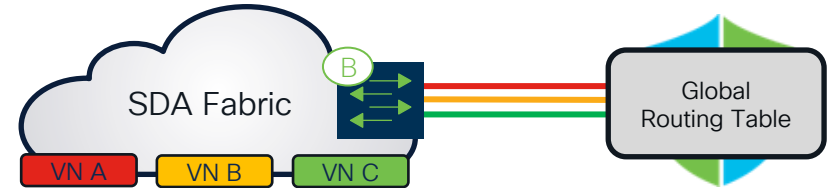
Design not setup to
accommodate
additional growth

Single points of
failure

Firewall Deployment Modes – VN Separation

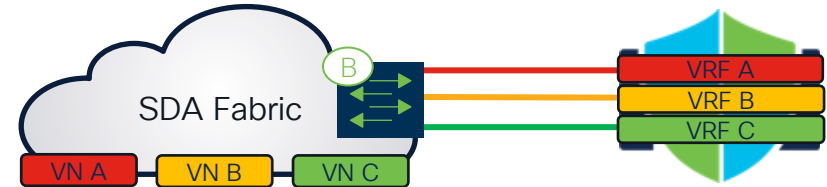
Non-VRF Aware

- **Merging VN routing tables** in GRT on the firewall
- **Single security policy** on FTD governing inter-VN and egress traffic



VN to VRF Mapping

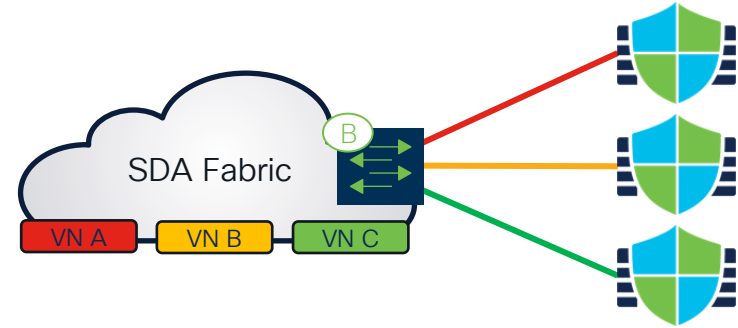
- **VN mapped to VRFs** on the firewall providing routing separation
- **Firewall leaks routes** between VNs, Shared Services and external
- Common firewall policy across VRFs on the FTD, with **VRF aware rules**



Firewall Deployment Modes – VN Separation

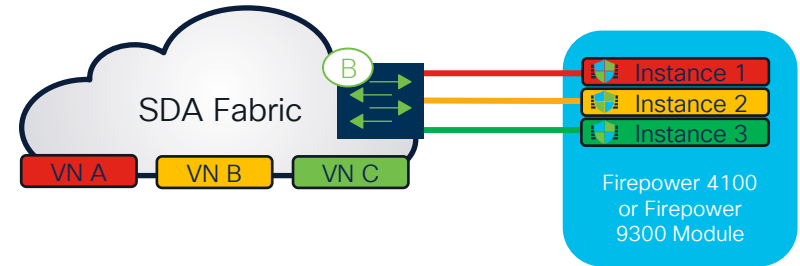
VN to Physical Device mapping

- Full physical separation between VN firewalls
- Individual firewall policies, event stores and management entities
- Multi-Tenancy support – each firewall can be managed by a different entity



VN to Instance mapping

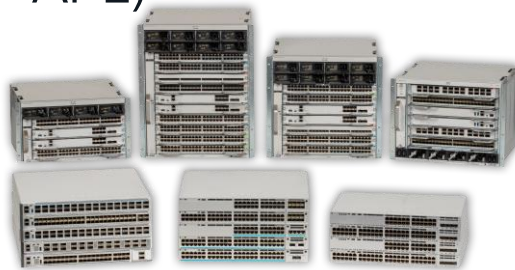
- Supported on Firepower 4100 and 9300 only
- Instantiate multiple logical devices on a single module or appliance
- Physical and logical separation between firewall instances on Supervisor level



Sample List of Network Elements



- Cisco ASR 1001Xs
- Cisco Firepower 4110 NGFWs
- Cisco Firepower Management Console (FMC) 1600 Appliance
- Cisco DNA Center 3-Node Cluster (DN2-HW-APL)
- Cisco ISE (3615 appliances)
- Cisco AnyConnect + Duo
- Catalyst 9300, 9400, 9500 Platforms
- Cisco 5520 Wireless LAN Controllers (Catalyst 9800 supply chain – future)
- Cisco 9130 Access Points



Solution Engagement Overview

- Solution engagement in partnership with Cisco consisted of two main phases:
 - Phase I – Upgrade the software versions on all the platforms and establish a new physical shared services DMZ environment
 - Phase II – Deploy a second SDA site incorporating design enhancements
 - ✓ Once second SDA site fully operational – apply the same enhancements to original SDA site

Phase I – SDA Upgrade Planning

DNA Center 3-Node Cluster Preparation

- AURA (Audit and Upgrade Readiness Advisor) Tool
 - Health/scale/readiness checks for DNA Center and Fabric
 - <https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/215840-cisco-dna-center-aura-audit-and-upgrad.html>

- Fresh backup of DNA Center Database

Note: Different storage mechanisms for automation vs. assurance

- SDA Compatibility Matrix
 - Recommended releases/approved releases for DNA, ISE, and network devices

Note: Matrix does not consider ISE integration or DNAC integration with Cisco Firepower Management Console)

- [Cisco Software-Defined Access Compatibility Matrix](#)

Adding FMC Device to DNAC Center

Cisco DNA Center

Provision - Network Devices - Inventory

Preview Devices 2.0

Inventory Plug and Play

Find Hierarchy

Global

Unassigned Devices

San Jose

DEVICES

FOCUS: Inventory

Filter Add Device Tag Device

Device Name IP Address Device Family

Add Device

Device Controllability is **Enabled**. Configuration changes will be made on network devices during discovery/inventory or when device is associated to a site. Firepower Management Center devices are not supported. [Learn more](#) | [Disable](#)

Type*
Firepower Management Center

Device IP / DNS Name*
172.28.169.108

Credentials [Validate](#)

HTTP(S) credential is mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

HTTP(S)*

Select global credential Add device specific credential

Username* vtest View Username Criteria

Password* View Password Criteria

Cancel Add

Use **Firepower Management Center** type and provide an IP Address.

Provide username and password for REST API access. Ensure these credentials are used **exclusively by DNAC**.

Phase I – SDA Upgrade Planning

DNA Center 3-Node Cluster Preparation (cont'd)

- Review Cisco DNA Center Upgrade Guide
 - [Cisco DNA Center Upgrade Guide – Cisco](#)
- Check for open caveats / review release notes
- Consider opening a proactive TAC case (case might already be open to review any outstanding issues from the AURA)

Phase I – DNA Center Upgrade Process

- There are multiple steps within DNA Center Upgrade
 - System Update -> Package Download -> Package Update
- ✓ All of this happens in hours, not minutes

How long will it take to upgrade?

Use this table to estimate the time to upgrade based on the current version of your Cisco DNA Center.

Single Node ☒ 3 Node

Cisco DNA Center Update Times	Upgrade from 2.1.2.6 to 2.2.2.0	Upgrade from 2.2.2.3 to 2.2.3.0	Upgrade from 2.2.3.3 to 2.3.2.0	Upgrade from 2.2.3.5 to 2.3.3.0	Upgrade from 2.3.3.4 to 2.3.4.0	Upgrade from 2.2.3.5 to 2.3.3.0
System Update	2 hrs 35 mins	1 hr 50 mins	2 hrs 25 mins	2 hrs 35 mins	Release download 30 mins	Release download 30 mins
Package Download	30 mins	30 mins	30 mins	30 mins	Release install 3 hrs 45 mins	Release install 3 hrs 35 mins
Package Upgrade	3 hrs 5 mins	2 hrs 35 mins	2 hrs 30 mins	2 hrs 20 mins	Release install 3 hrs 45 mins	Release install 3 hrs 35 mins
Total Time	6 hrs 10 mins	4 hrs 55 mins	5 hrs 25 mins	5 hrs 25 mins	4 hrs 15 mins	4 hrs 5 mins

- [Cisco DNA Center Upgrade](#)

Phase I – DNA Center Upgrade Process

- Don't get confused by the system update screen versions
 - [Release Notes for Cisco DNA Center, Release 2.2.3.x](#)

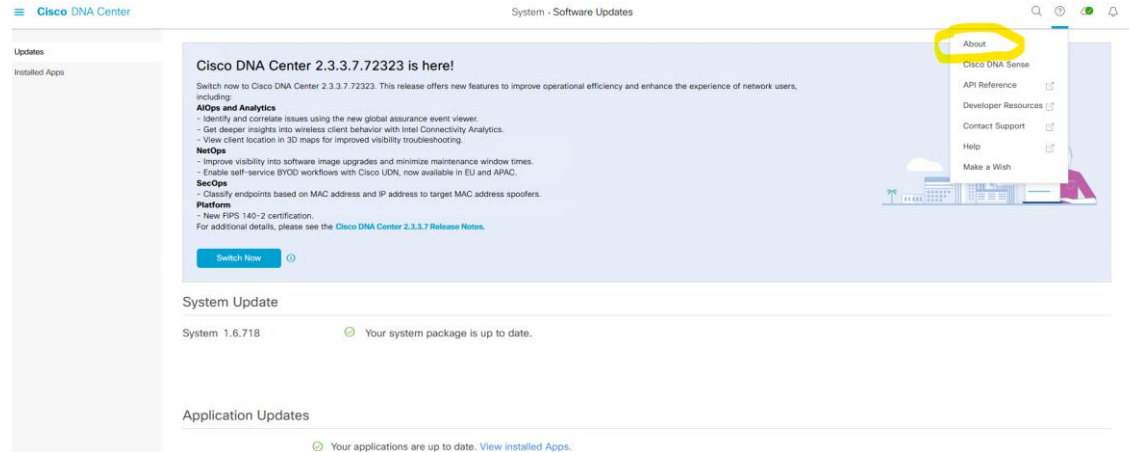
Package Versions in Cisco DNA Center, Release 2.2.3.x

To download Cisco DNA Center software, go to <https://software.cisco.com/download/home/286316341/type>.

Table 2. Updated Packages and Versions in Cisco DNA Center 2.2.3.x.

Package Name	Release 2.2.3.6	Release 2.2.3.5	Release 2.2.3.4	Release 2.2.3.3	Release 2.2.3.0
System Updates					
System	1.6.718 (The originally released package version was 1.6.711. For more information, see CSCwc40316.)	1.6.706	1.6.703	1.6.551	1.6.430

- Alternatively select about as circled



Cisco DNA Center
Version 2.2.3.6

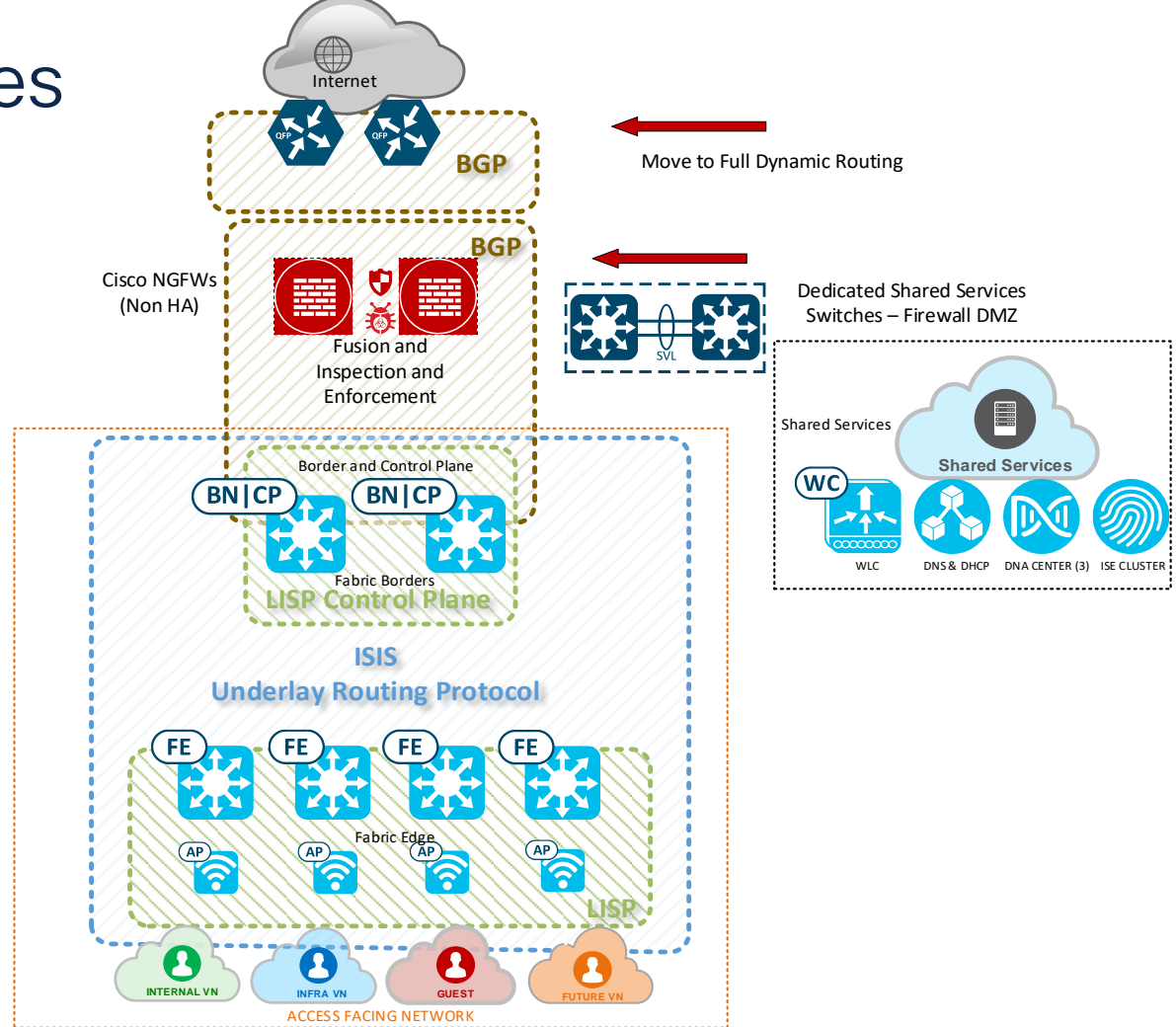
[Release Notes](#)
[Packages](#)
[Serial number](#)
[Member ID](#)

© 2023 Cisco Systems Inc. All Rights Reserved.

Phase I – Deploy Shared Services DMZ Switches

- New shared services switches (change window)
 - Catalyst 9500 in StackWise Virtual arrangement
 - DMZ interface off the firewall (default gateway = firewall)
 - Clone/Update firewall policy rules
 - Move shared services elements
- Design Benefits
 - ✓ Simpler, more scalable design in preparation for second fabric site coming on-line
 - ✓ Allows for upgrade of border nodes without disrupting shared service nodes
 - ✓ Delivers higher availability for DNA Center using NIC Bonding
 - [Cisco DNA Center Second-Generation Appliance Installation Guide, Release 2.2.2 – Prepare the Appliance for Configuration \[Cisco DNA Center\] – Cisco](#)

Shared Services



Phase II – New Fabric Site – LAN Automation

- Allows for zero touch provisioning of network devices
- Leverages DNA Center, but separate from the overall fabric enablement
- Lessons Learned (not all encompassing of overall process):
 - Only connect the uplink ports
 - Ensure the switch has no configuration “pnpa service reset”
 - Stackable switches
 - ✓ Switches need to be brought up in proper order
 - ✓ Stack renumbering is not possible once LAN automation has started

[LAN Automation: Step-by-step deployment guide and Troubleshooting – Cisco](#)

Phase II - Segmentation Considerations/Approach

- In general, SDA Fabrics 2 segmentation options
- Leveraged multiple VNs (Enterprise, Guest, Infra) for macro-segmentation
 - NGFW performing north/south and inter-VN security enforcement
 - Used firewall policy to restrict Zone access and communication
- Micro-segmentation (east/west) security strategy used to control and segment traffic within the VN
 - Secure group tags used for contextual representation of different business units, services, partners, etc...

Phase II - Segmentation Considerations/Approach

- SGT enforcement is stateless by nature
- Performed in hardware on switches with limited logging
- If using micro segmentation, Group-Based Policy Analytics within DNA Center and its direct integration with ISE can provide visibility into which tags are communicating with each other (policy validation)
- Generic Example

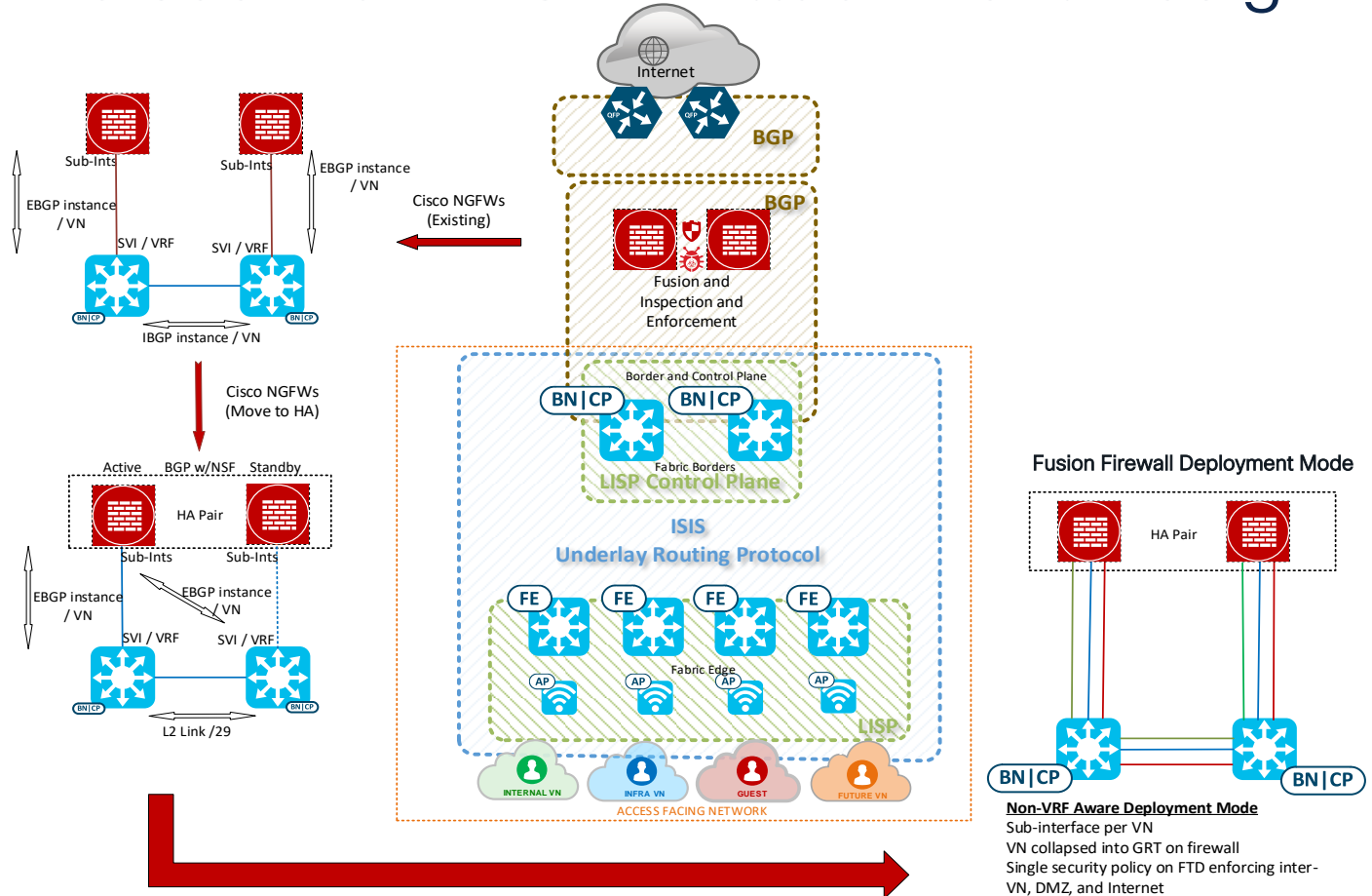


Phase II – Fusion Firewall Design

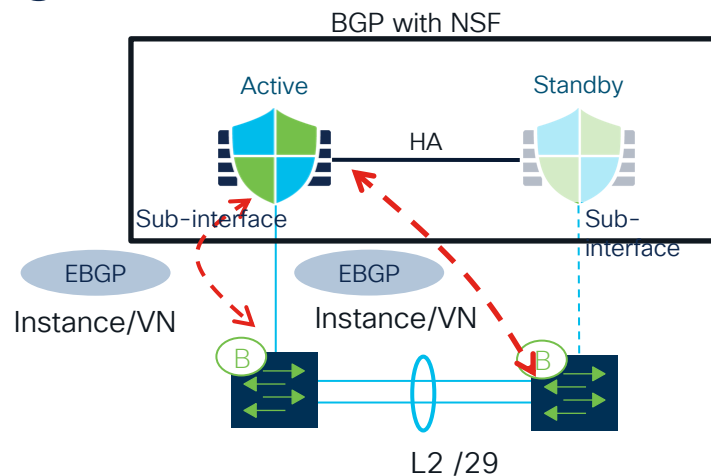
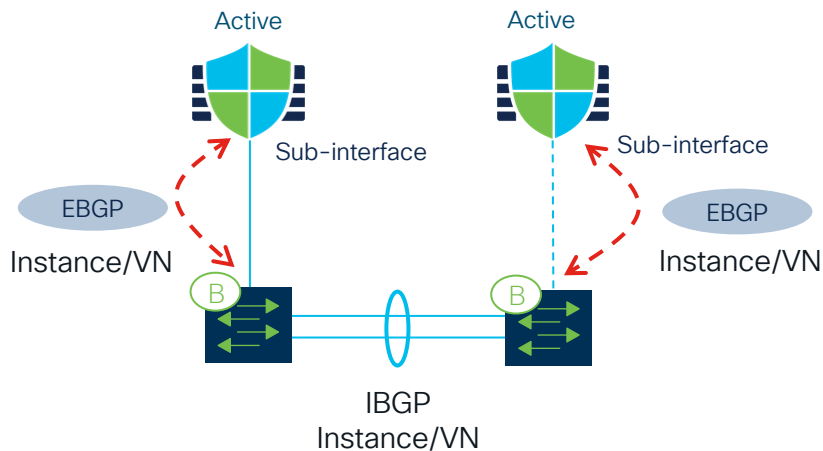
- Multiple options exist for attaching Cisco NGFWs (fusion firewalls) to the SDA Border Nodes
- Firewall configuration is not automated
- Leveraged border automation to generate majority of the required configuration on the border nodes
 - Complimented this with addition configuration required to interconnect border nodes to the firewalls (via /29s)

Note: Deployed in early 2022 – BGP/LISP model

Phase II – Cisco NGFW SDA Attachment Design



Initial Firewall (FTD) Design to HA



- Two separate BGP session (Border/Controller and Firewall)

- IBGP sessions between the Border/Controller nodes

- Not the best design for SDA

- Two Separate ASN

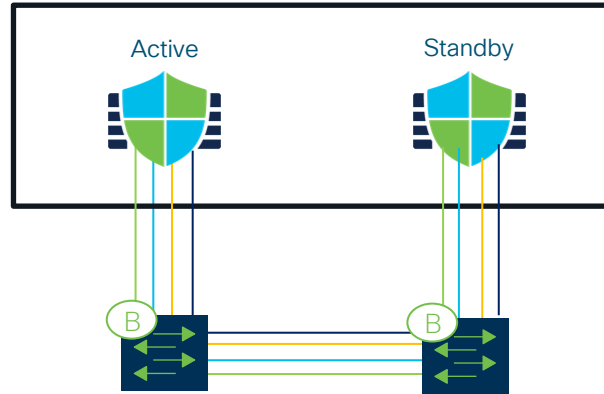
- L2 extension required between Border nodes

- Active/Standby L2 adjacency with both Borders required

- Firewall Threat Defense supports BGP with NSF (do not add BFD)

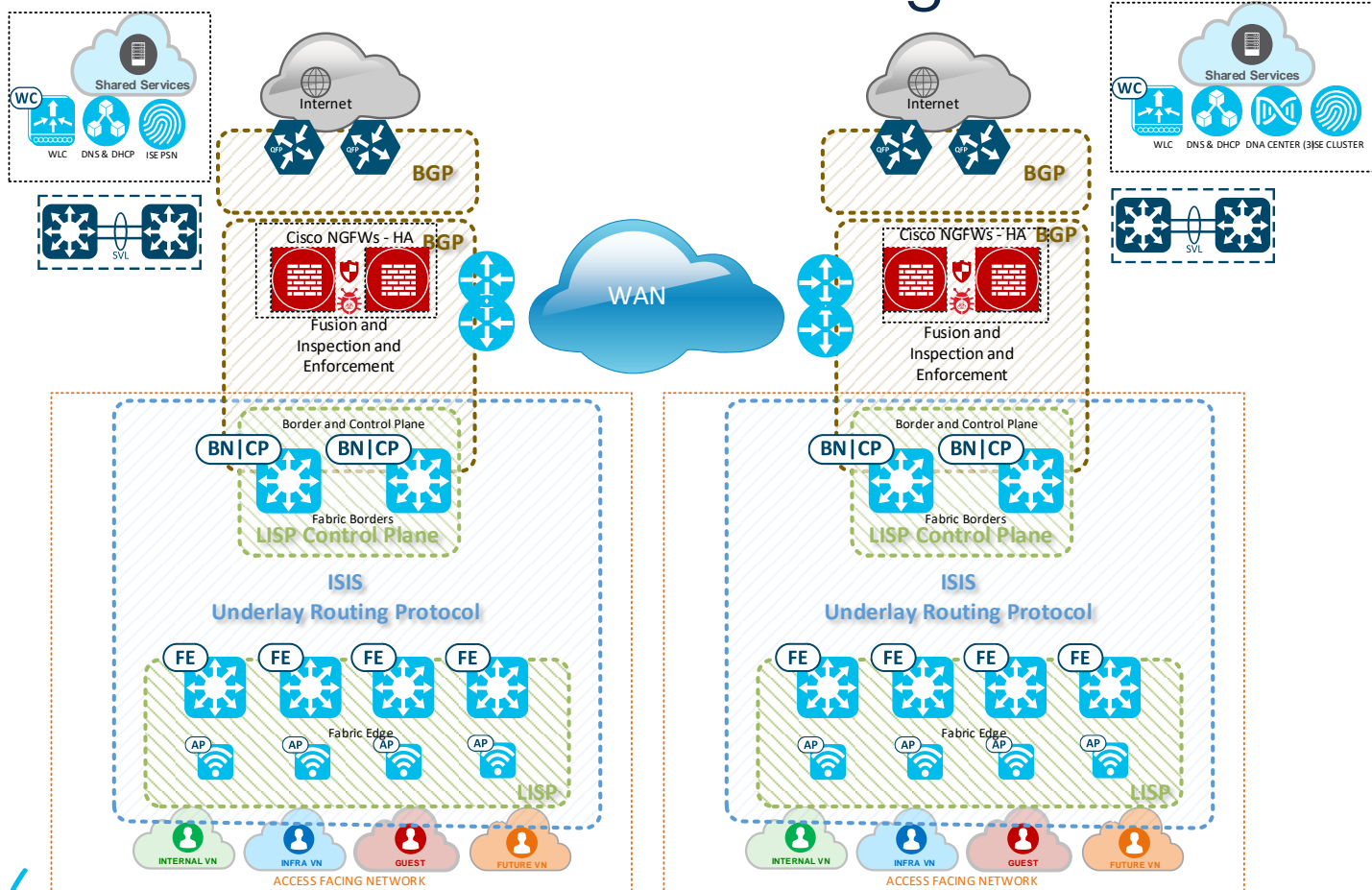
- Single ASN

Fusion Firewall Deployment Mode



- Non-VRF Deployment Mode
- Subinterface per VN
- All VN routes collapsed into F/W global routing table
- Single security policy enforcing Inter-VN, DMZ and Internet

Phase II – End State Network Diagram



Fabric Enabled Wireless Access Points

- SD-Access allows for automated AP onboarding
- AP gets IP address out of an AP pool in Cisco DNA Center in the INFRA_VN
- Cisco DNA pre-provisions configuration on FE to automatically onboard APs
- Configuration is not visible in running configuration – must use the “show derived-config xxx” to view the complete configuration

```
FABRICEDGESWITCH# sh cdp neigh ten1/0/48
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce   Holdtme    Capability  Platform  Port ID
WIRELESSAP     Ten 1/0/48      136        R T         C9130AXI-  Gig 0

FABRICEDGESWITCH##sh runn int ten1/0/48
Building configuration...

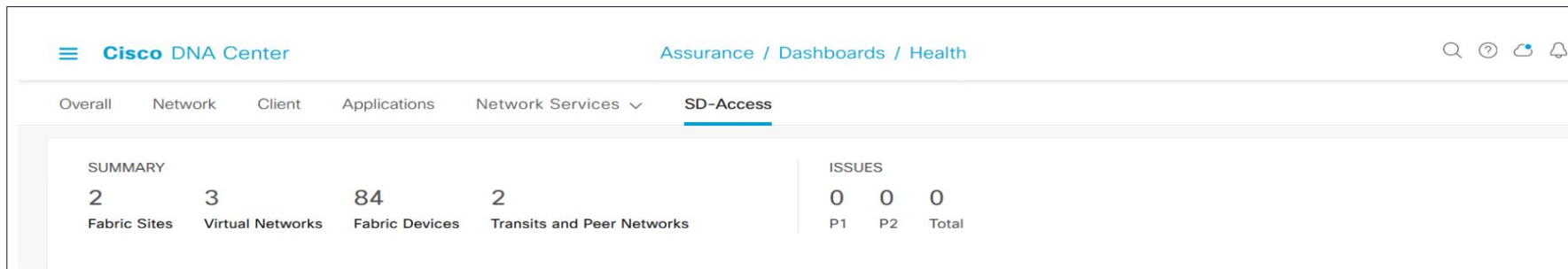
Current configuration : 118 bytes
!
interface TenGigabitEthernet1/0/48
 description WIRELESSap
 device-tracking attach-policy IPDT_POLICY
end

FABRICEDGESWITCH#show derived-config int ten1/0/48
Building configuration...

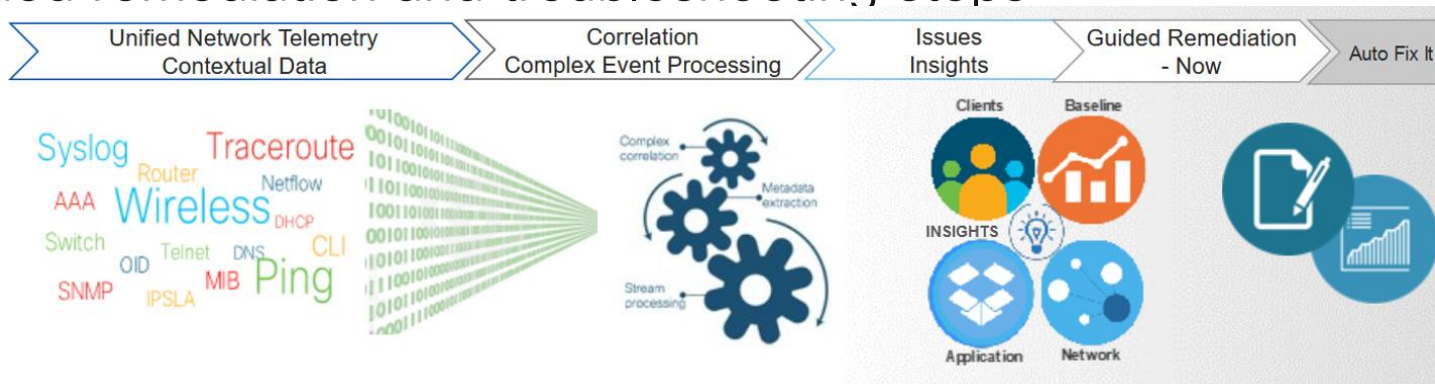
Derived configuration : 406 bytes
!
interface TenGigabitEthernet1/0/48
 description WIRELESSAP
 switchport access vlan 2045 --> Infra VLAN
 switchport mode access
 switchport block unicast
 device-tracking attach-policy IPDT_POLICY
 load-interval 30
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 15
end
```

SDA Fabric Monitoring

- DNA Center has a specific assurance section dedicated to SDA



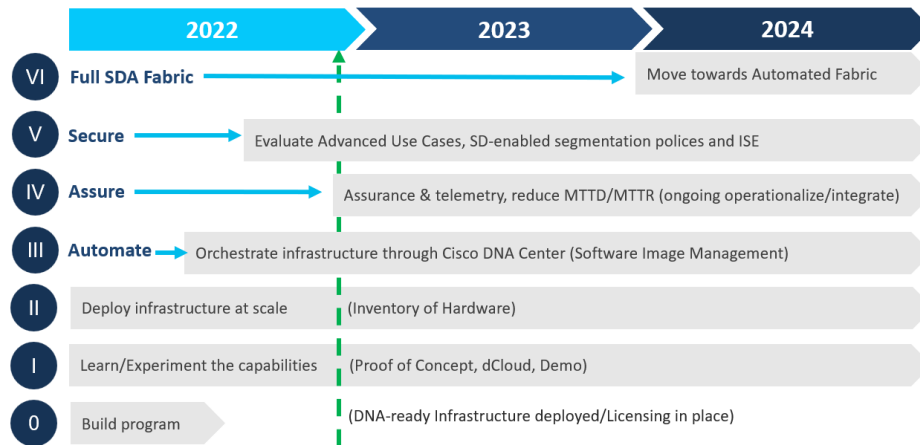
- Guided remediation and troubleshooting steps



Recommendations

- Start with a plan
- Adopt crawl, walk, run approach where possible

Sample DNA Adoption Timeline

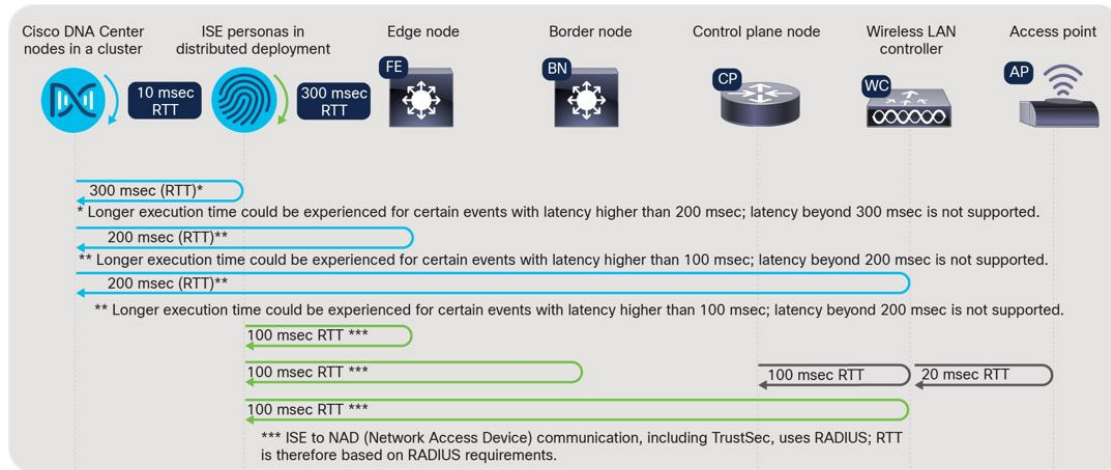


- Understand architecture scalability needs (present/future) including F/W's

• <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html>

Recommendations

- Ensure proper end-to-end latency between fabric and non-fabric devices



- Align to software versions in the SDA compatibility matrix
 - https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/sda_compatibility_matrix/index.html
- Deploy an SDA proof-of-concept with DNA Center Starter Kit

Summary and Reference

- AT&T & Cisco collaboration on SDA in the customer Enterprise
- Review and Overview of DNA Center and SDA
- Customer Success Story
- Lessons Learned
- Recommendations
- References
 - **Cisco Secure Firewall and SDA Integration Deep Dive - BRKSEC-2845**
 - <https://www.ciscolive.com/on-demand/on-demand-library.html?search=%22Chris%20Grabowski%22#/session/1655424241007001QujE>
 - **Cisco Secure Firewall Attribute Base Policy and SDA Integration Deep Dive – BRKSEC-2116**
 - <https://www.ciscolive.com/on-demand/on-demand-library.html?search=%22Chris%20Grabowski%22#/session/1670019637340001nvJI>

Cisco DNA Center Sizing



	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
Hardware description	Cisco UCS C220 M5 Rack Server 44 cores	Cisco UCS C220 M5 Rack Server 56 cores	Cisco UCS C480 M5 Rack Server 112 cores

Cisco DNA Center system scale

Number of devices ¹ (switch, router, wireless controller)	1000	2000	5,000
Number of wireless access points	4000	6000	13,000
Number of wireless sensors	600	800	1600
Number of concurrent endpoints	25,000	40,000	100,000

Fill out your session surveys!



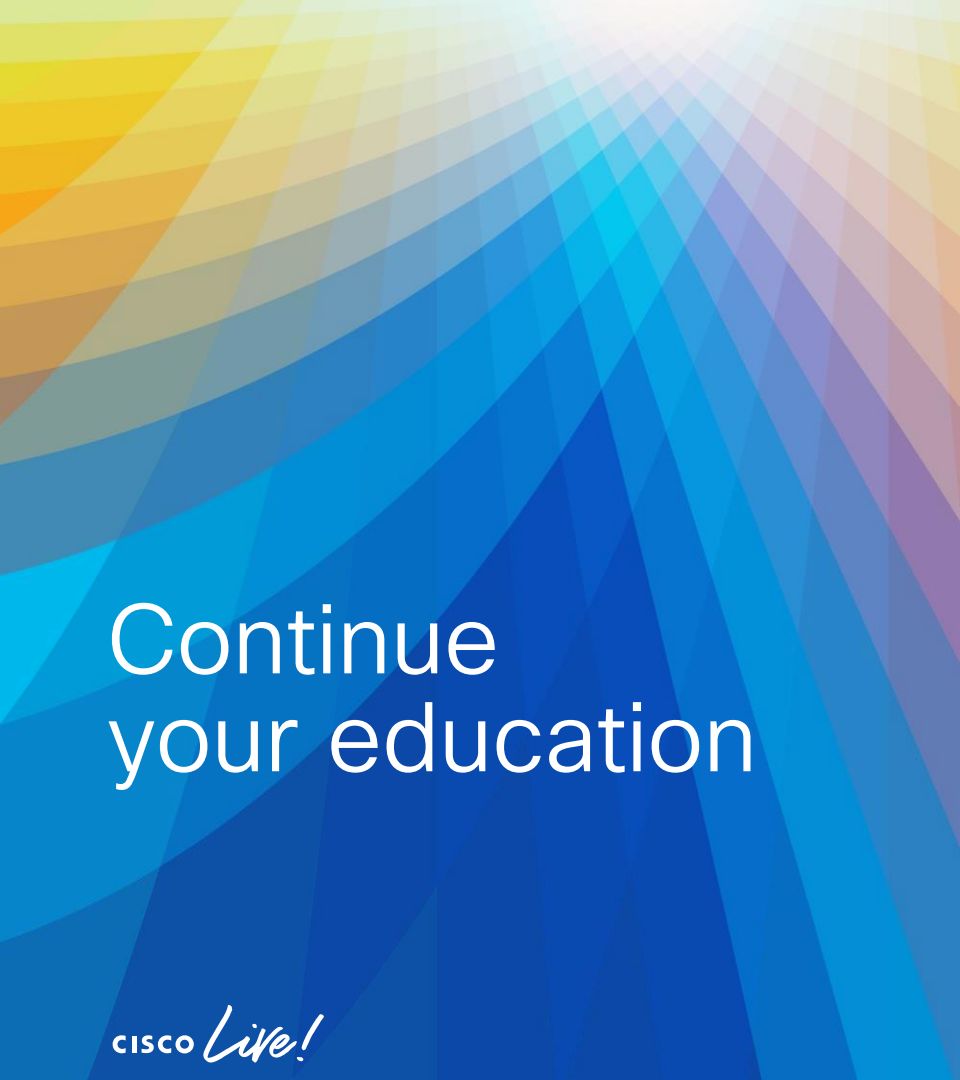
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



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



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

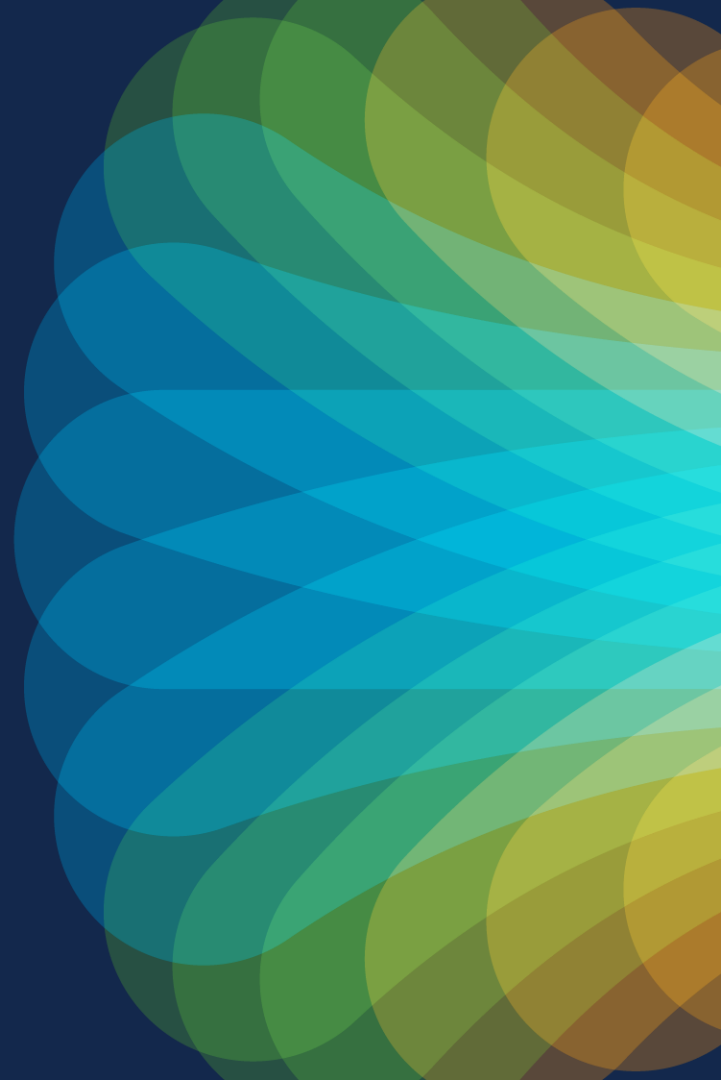


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

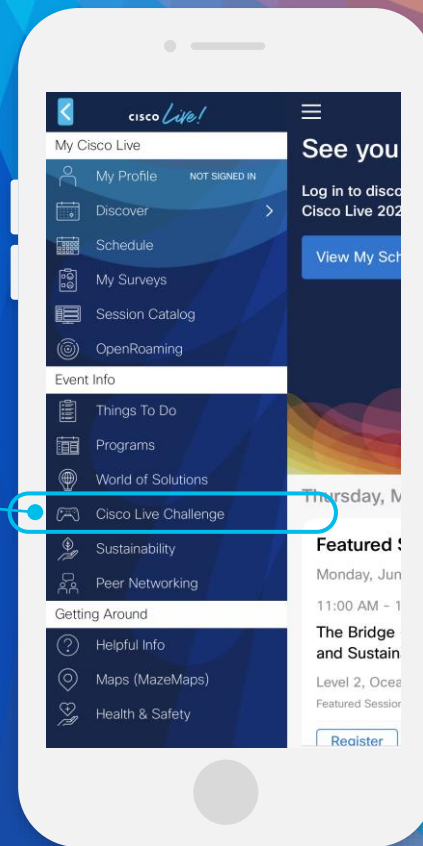


Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are large, flowing, wavy shapes in similar colors, giving the overall composition a sense of movement and energy.

cisco *Live!*

Let's go

#CiscoLive