



You make **possible**



Inside Cisco IT: Deploying SD-WAN and SDA

Dean Sanders, IT Engineer
Jamie McGregor, IT Engineer

BRKCOC-4263

CISCO *Live!*

Barcelona | January 27-31, 2020



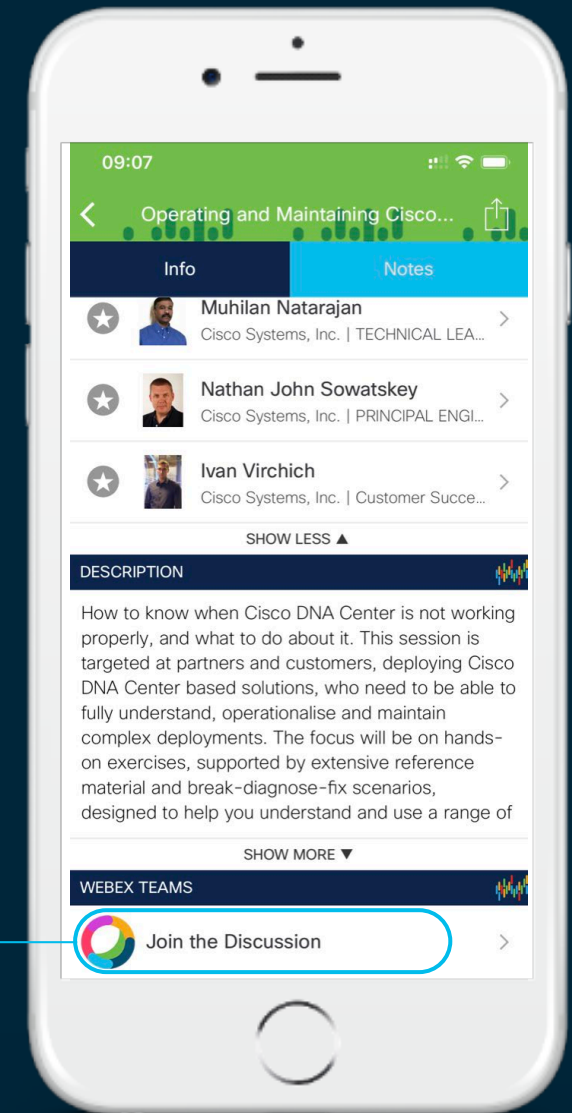
Cisco Webex Teams

Questions?

Use Cisco Webex Teams 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 Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



Related Sessions

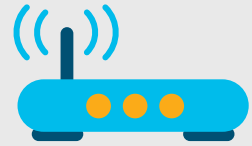
- Cisco on Cisco Booth & Mini Theatre in Cisco Showcase
 - World of Solutions – Open Daily
- Inside Cisco IT: Cisco Multicloud Backbone – securely inter-connecting clouds (BRKCOC-2294)
 - Today @ 2:45pm
- Inside Cisco IT: Enterprise Wireless Design and Assurance with Cisco IT (BRKCOC-2257)
 - Check the recording online!

Agenda

- Part 1 – Cisco IT Global Network Overview
- Part 2 – Technical Deep dive
 - SDA with Cisco DNA Center
 - SD-WAN
 - Integration
- Part 3 – Automating & Deploying Cisco DNA
 - Development Lifecycle & Version Control
 - What does a deployment involve?
 - Cisco IT Automation & ZTD Micro Service

Part 1 – Cisco IT Network Overview

Cisco at a Glance



7,198
Routers



8,693
LAN Switches



11,909
Unified Computing
System Servers

7.6

Billion DNS
requests per day

74,726



Employees

137,414



Connected
Stakeholders



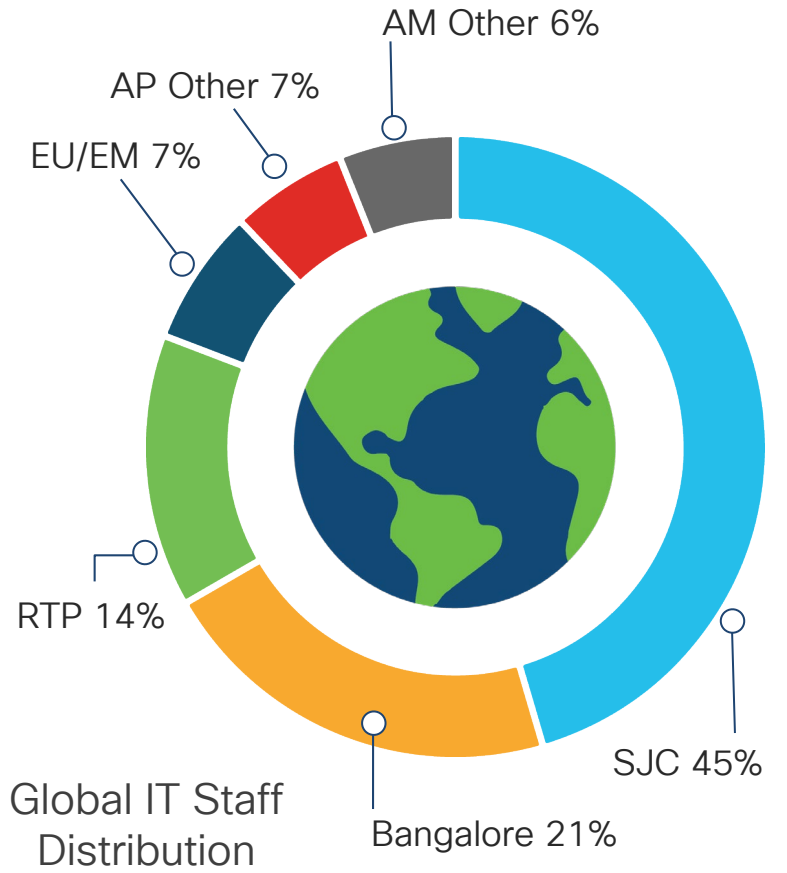
96

Countries



506

Offices



93
Services



48,811
Virtual Machines



~458k
Managed End
Devices

91 PB

Overall Usable
Storage

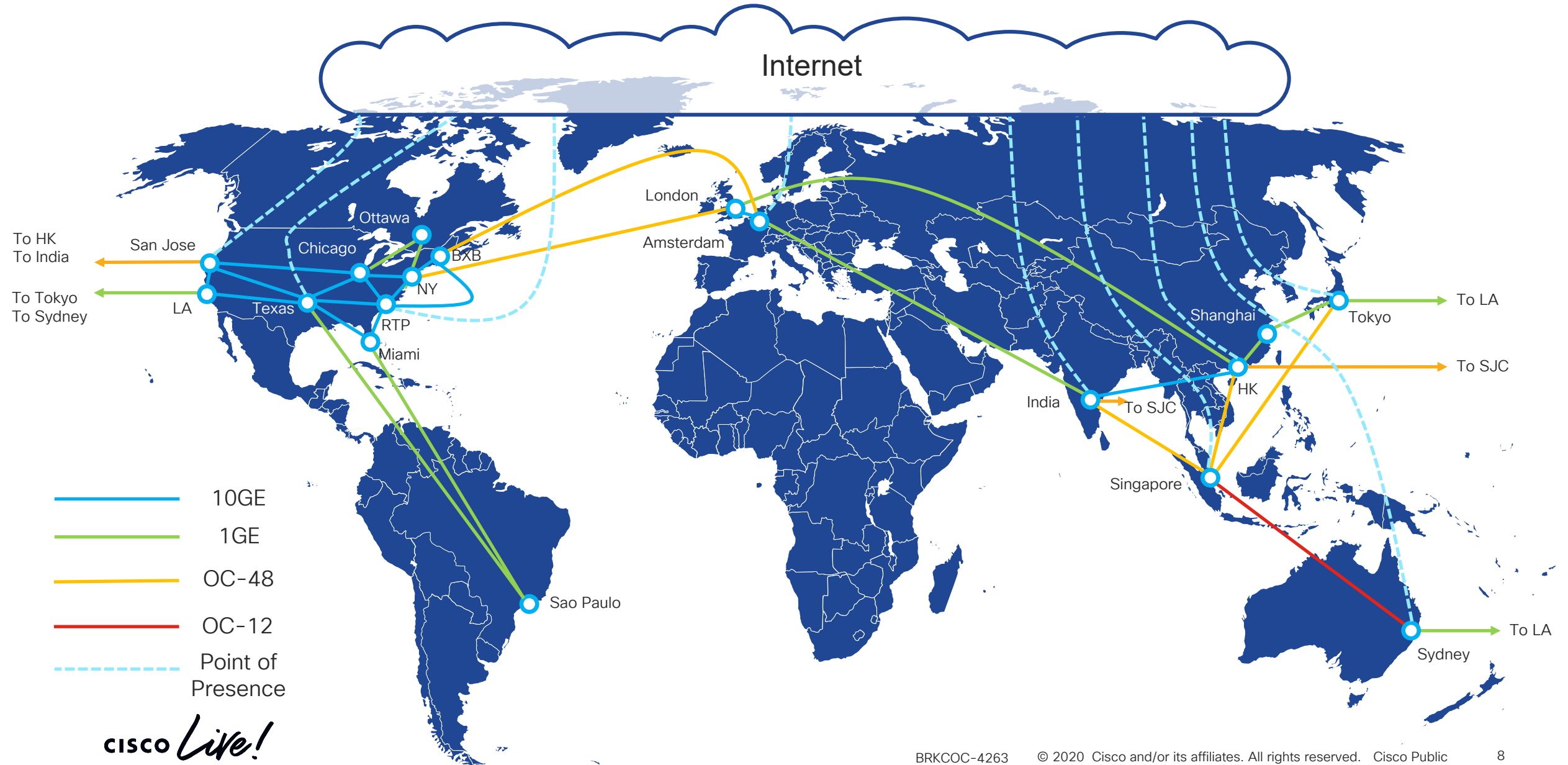
26.9 MW

Data Center
Capacity



6.39M
Internet Threats
Blocked Per Day
(WSA w/AMP)

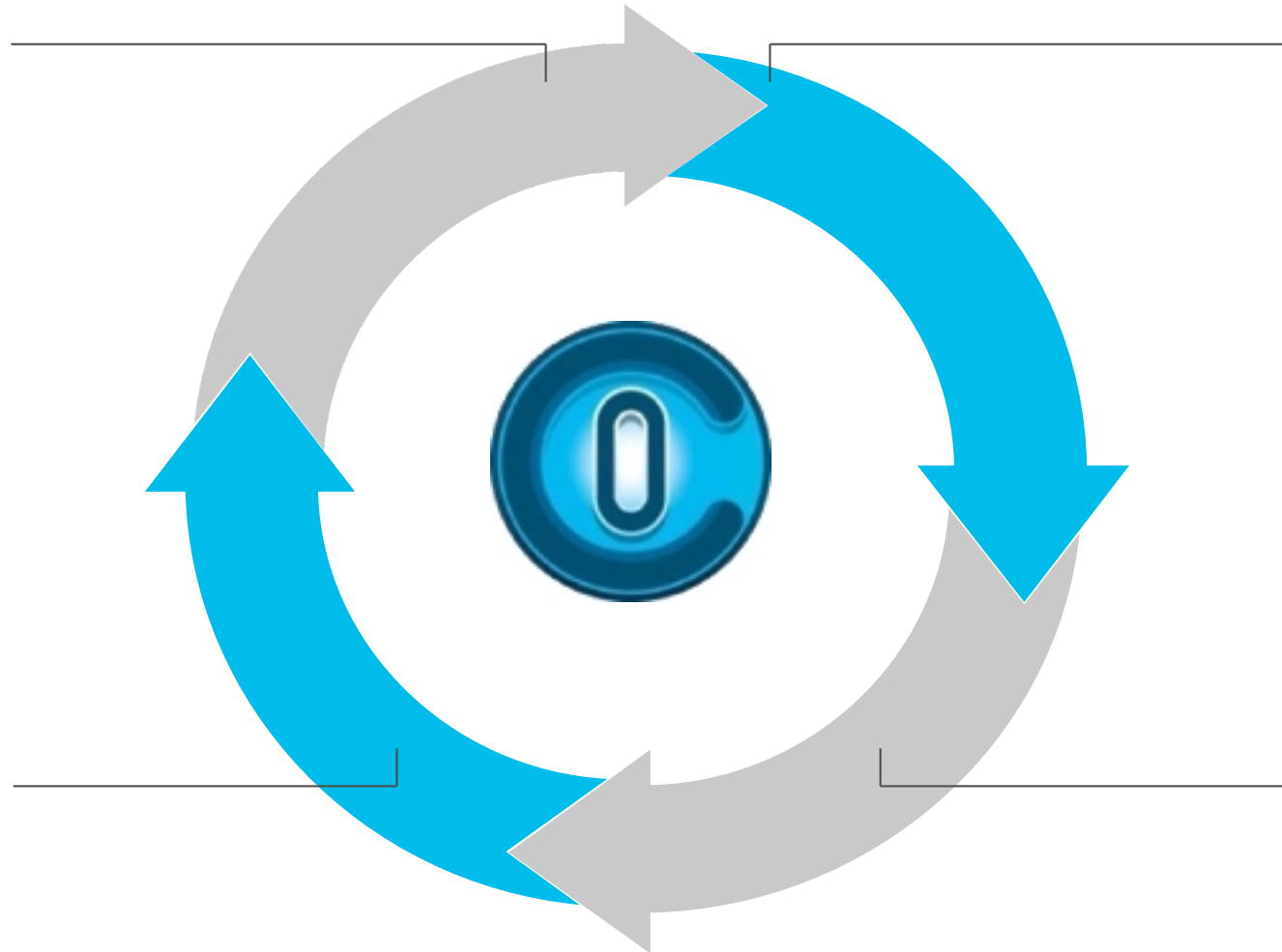
Tier 1 WAN & Internet PoPs



Cisco IT is Customer Zero

BU Development
The BU will work to implement fixes and critical feature enhancements to the product.

New Release
Cisco IT is an early adopter of new releases, putting them into pre-prod infrastructure rapidly.



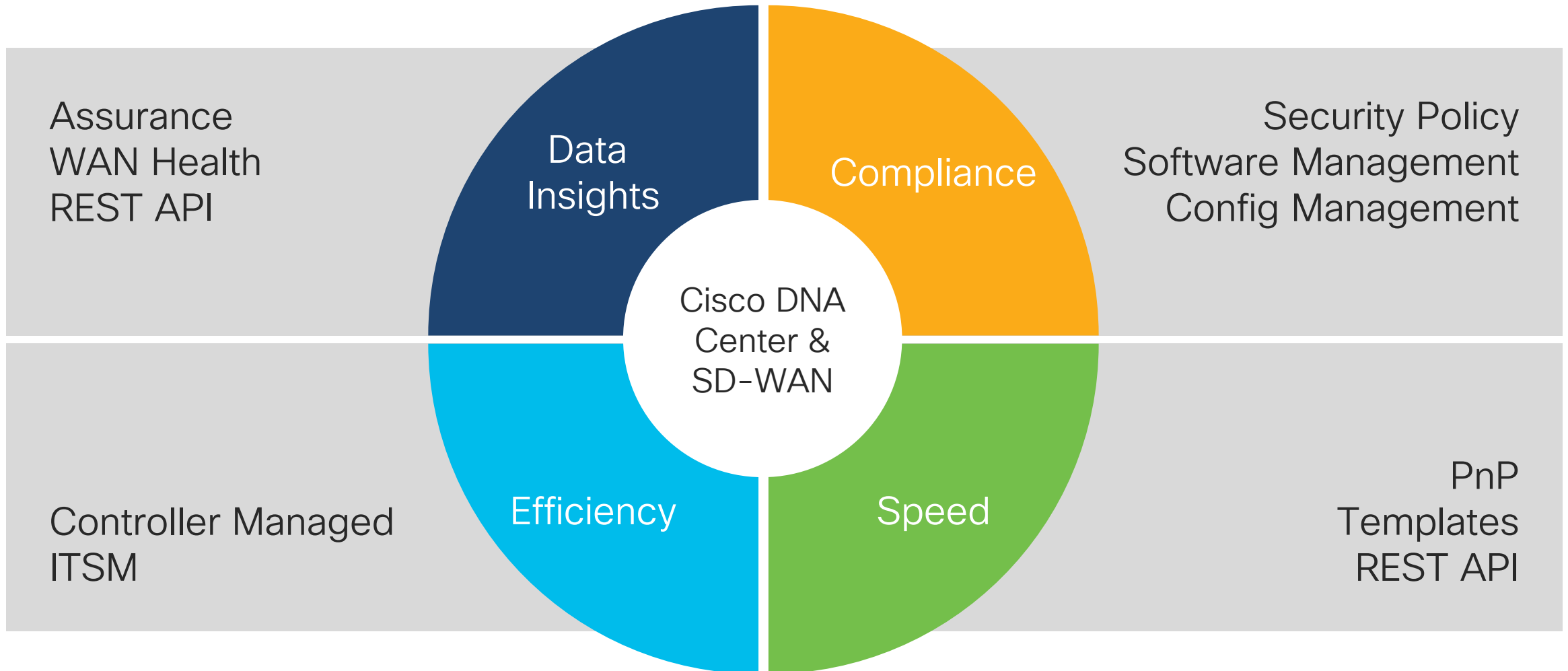
Feedback
We provide feedback to the engineering BU, and request enhancements.

Test
Cisco IT tests the release for defects, and the new features in environments that match the production network.

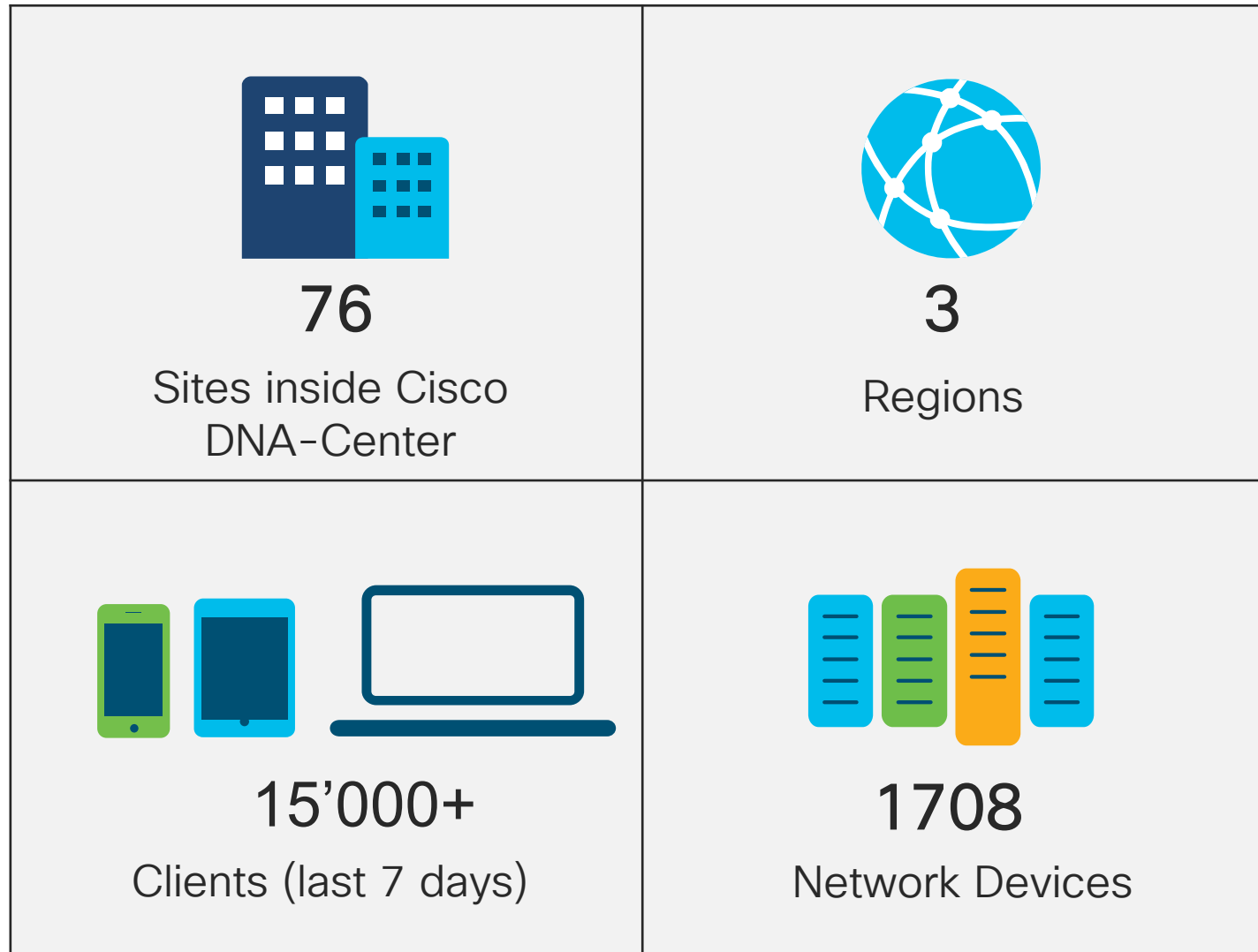
Question!

What are we doing with Cisco
DNA to assist us?

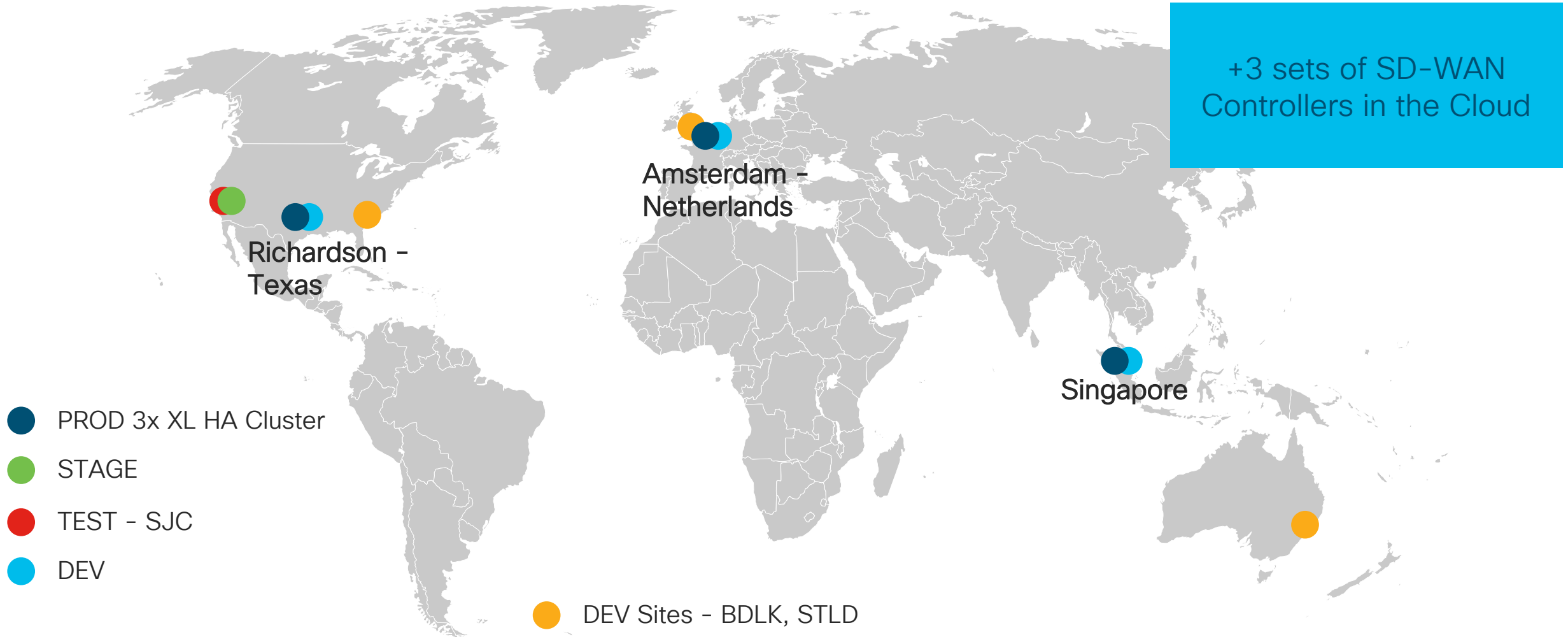
Cisco IT Drivers & Technologies



Cisco IT DNA-C Highlights



Cisco Controller Locations



Cisco Controller Locations

DNA – Center Appliances

DEV

- 2 Sites: London & Sydney
- 1x XL Cluster

STAGE

- San Jose: Solutions Verification Lab
- 3x HA XL Cluster

PRODUCTION

- 3x Campus Locations
- 3x Branch Cluster
- 3x HA XL Cluster

- PROD
- STAGE
- DEV

● DEV Sites - RTP, BDLK, STLD

DNA-Center Dashboard



DNAC Topology

Dev Environment

Name	Devices Count	Category	Reservation Status	Reserve Topology	Wait in Queue
svl1dc1	8	IDC Core (Aggregation Hub)	Available	Reserve	0
svlgold11	17	Gold	Available	Reserve	0
svlsilv11	8	Silver	Available	Reserve	0

Test Environment

Name	Devices Count	Category	Reservation Status	Reserve Topology	Wait in Queue
svl1dc2	8	IDC Core (Aggregation Hub)	Available	Reserve	0
svlsilv21	8	Silver	Available	Reserve	0

Stage Environment

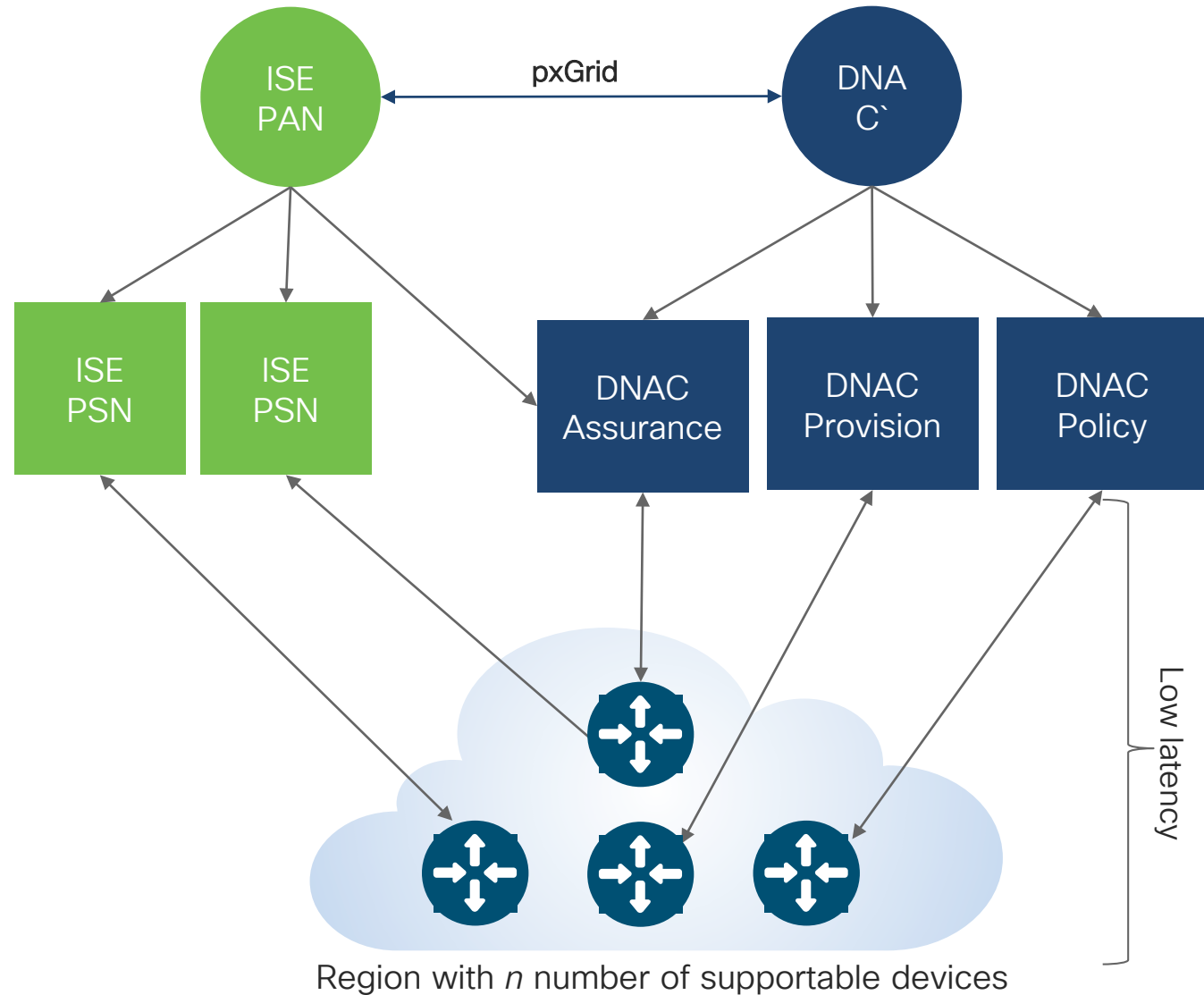
Name	Devices Count	Category	Reservation Status	Reserve Topology	Wait in Queue
svl1dc3	8	IDC Core (Aggregation Hub)	Available	Reserve	0
svlgold31	17	Gold	Available	Reserve	0
svlplat31	17	Platinum	Available	Reserve	0
svlsilv31	6	Silver	Available	Reserve	0



Part 2 Technical Deep Dive

The SDA Foundation – ISE

Cisco DNA-Center – ISE Architecture

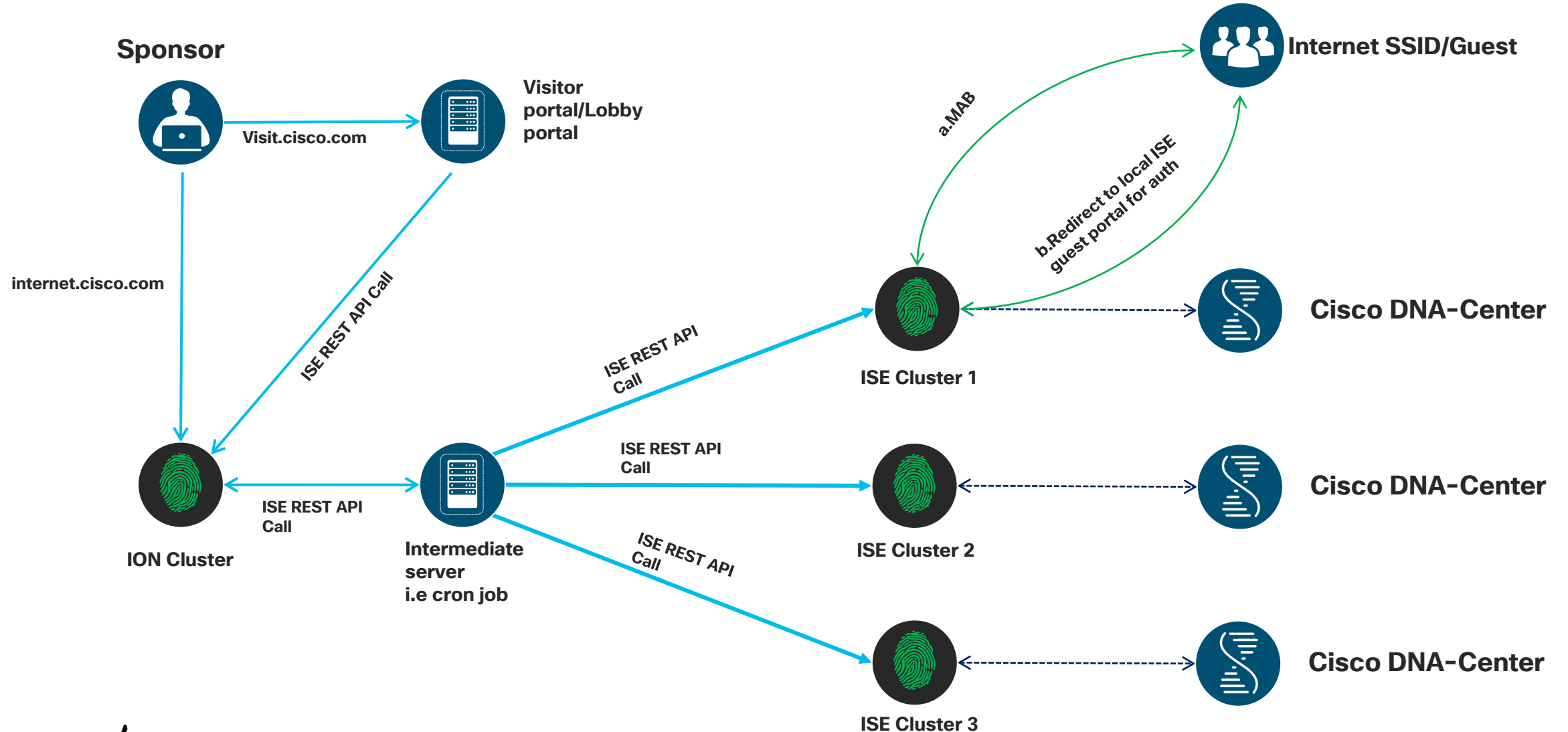


Create DNAC+ISE deployments
Which maps ISE PSN + DNAC
components to pools of devices

Question!

How does Cisco IT have this
setup for Guest?

Cisco DNA-Center – ISE Architecture



Question!

Why do we like segmentation?

Policy Based Management



Wired and Wireless
experience



Guest Services

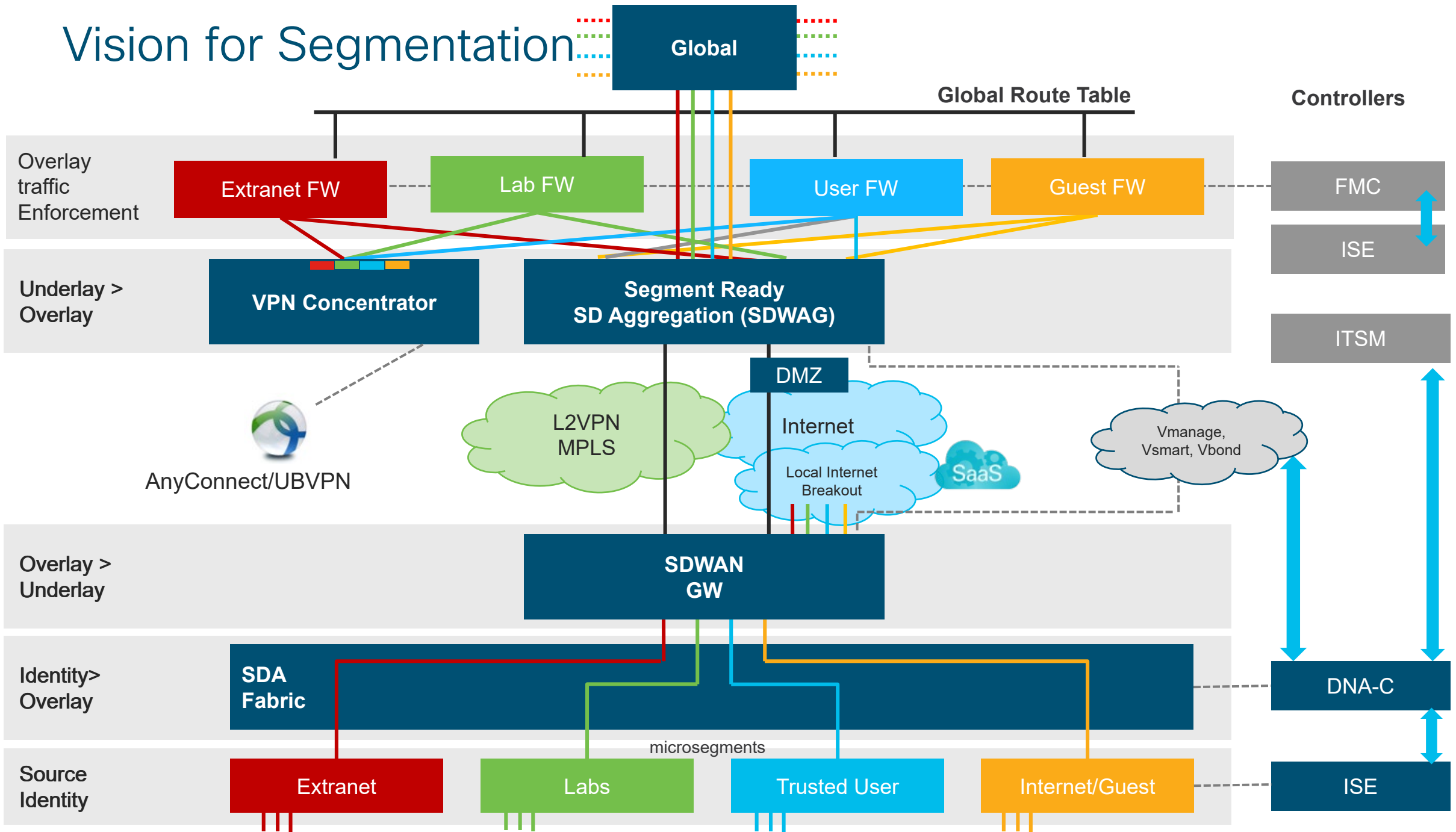


Centralized control
of user access

Segmentation Use Cases

- **Advantages of segmentation:**
 - Primarily for **boosting performance** and **improving security**, and
 - Include benefits such as *containing network problems, enabling better compliance with industry regulations, avoiding exposure to unnecessary security risks, and controlling visitor access.*
- **Segregation in *traditional* and *basic* networks** has been achieved by a combination of firewalls and VLANs (Virtual Local Area Networks).
- **Software-Defined Networking (SDN)** can enable creation and management of micro-segmented networks in more complex, dynamic and hybrid networks.
- **Proper segregating** of a network essentially **minimizes the level of access** to sensitive information for those apps, servers, and people who don't need it, while enabling access for those that do.
- Meanwhile it becomes **more difficult for a cyber-attacker** to locate and gain access to an organization's most sensitive information.

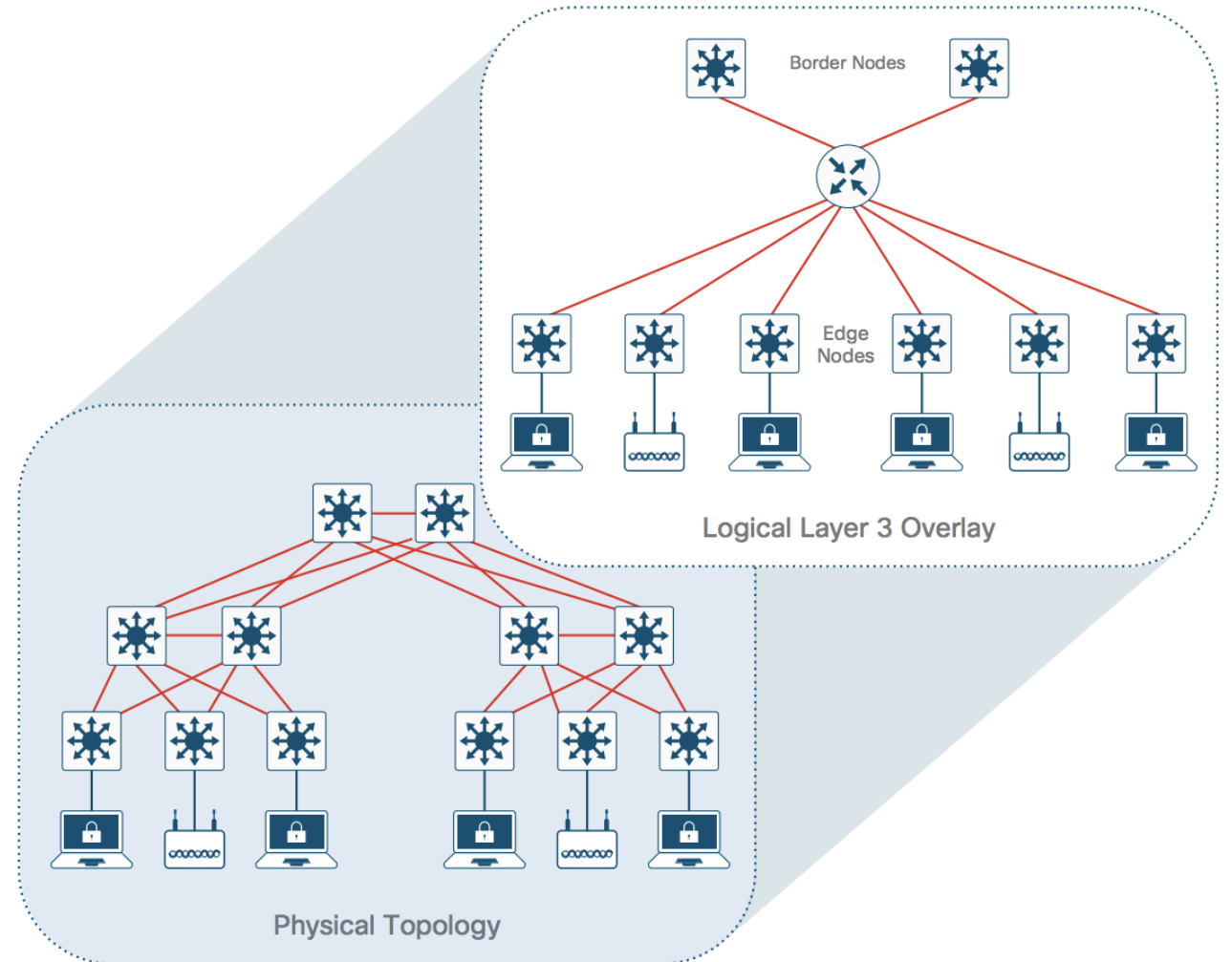
Vision for Segmentation



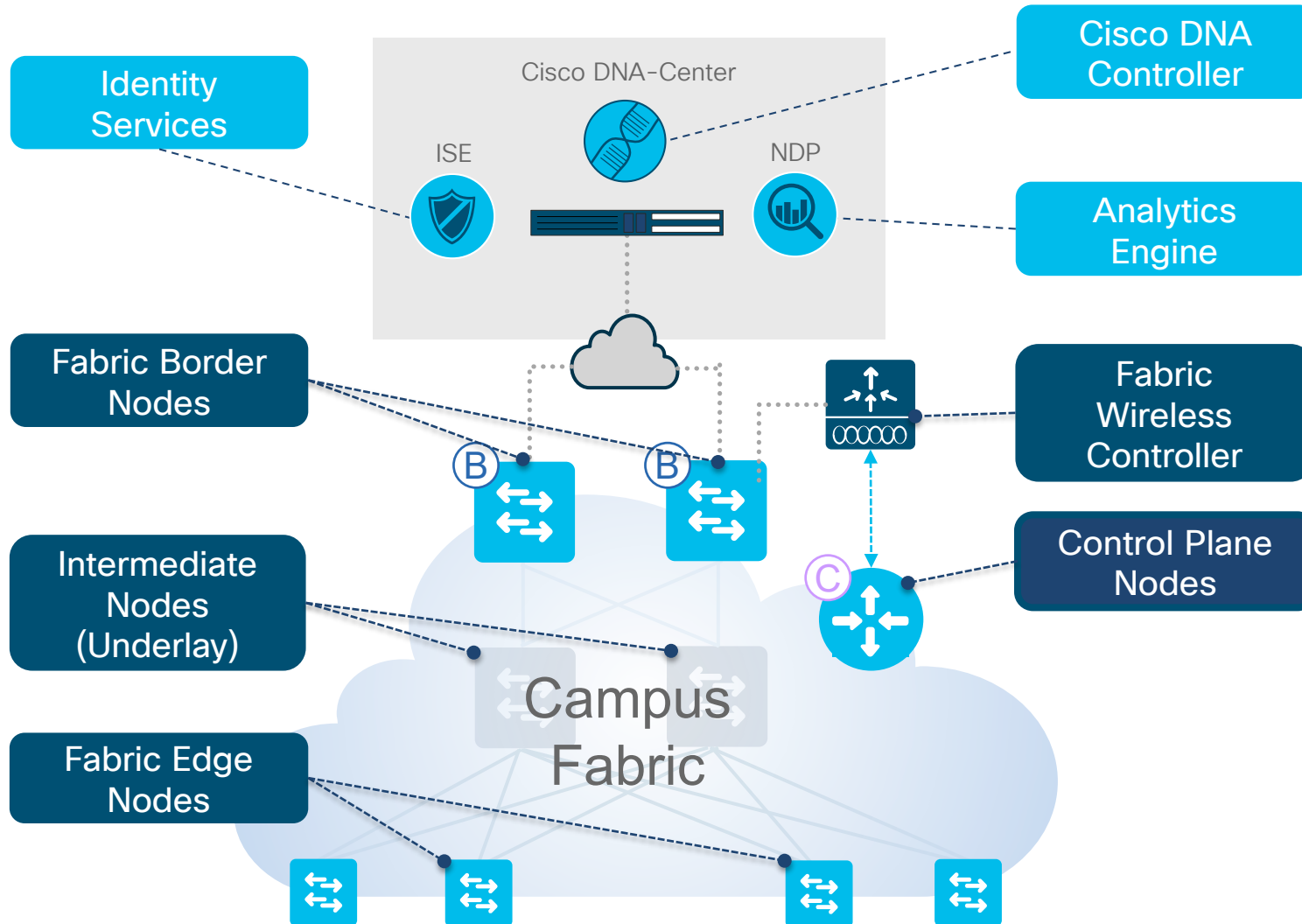
SD-Access

The Basics: Underlay and Overlay

- 1 Underlay is essentially the physical topology
- 2 For SDA deployment, it will require L3 Routed Access
- 3 Overlay abstracts IP-based activity from physical to provide Virtual Networks
- 4 Allows traffic/user segmentation and dynamic endpoint placement, independent of underlay schema



The Basics: What is SD-Access?



- **Cisco DNA Controller** – Enterprise SDN Controller (e.g. Cisco DNA Center) provides GUI management and abstraction via Apps that share context
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – External Data Collector(s) (e.g. NDP) are leveraged to analyze Endpoint to App flows and monitor fabric status
- **Control Plane (CP) 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 SDA Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects Wireless Endpoints to the SDA Fabric

The Basics: Virtual Networks and Secure Group Tags



Virtual Networks (VN)

Based on VRFs, enables one virtual network to be isolated from another, providing endpoint segmentation

Macro Segmentation



Scalable Group Tags (SGT)

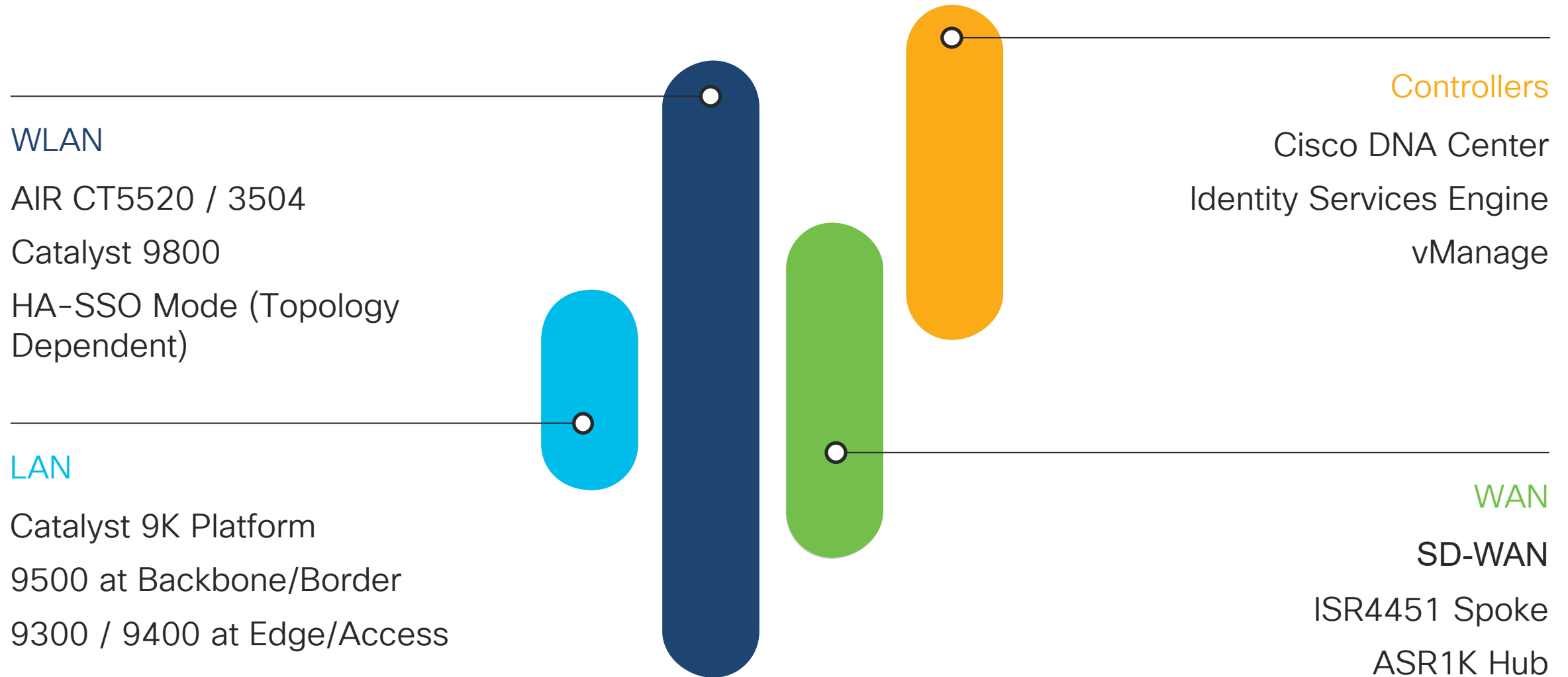
16-bit group identifier, used within a Virtual Network, and carried using the VXLAN header, East to West segmentation

Micro Segmentation

Question!

What does Cisco IT's current architecture and hardware look like?

Locking Down your 'DNA Ready' Infrastructure



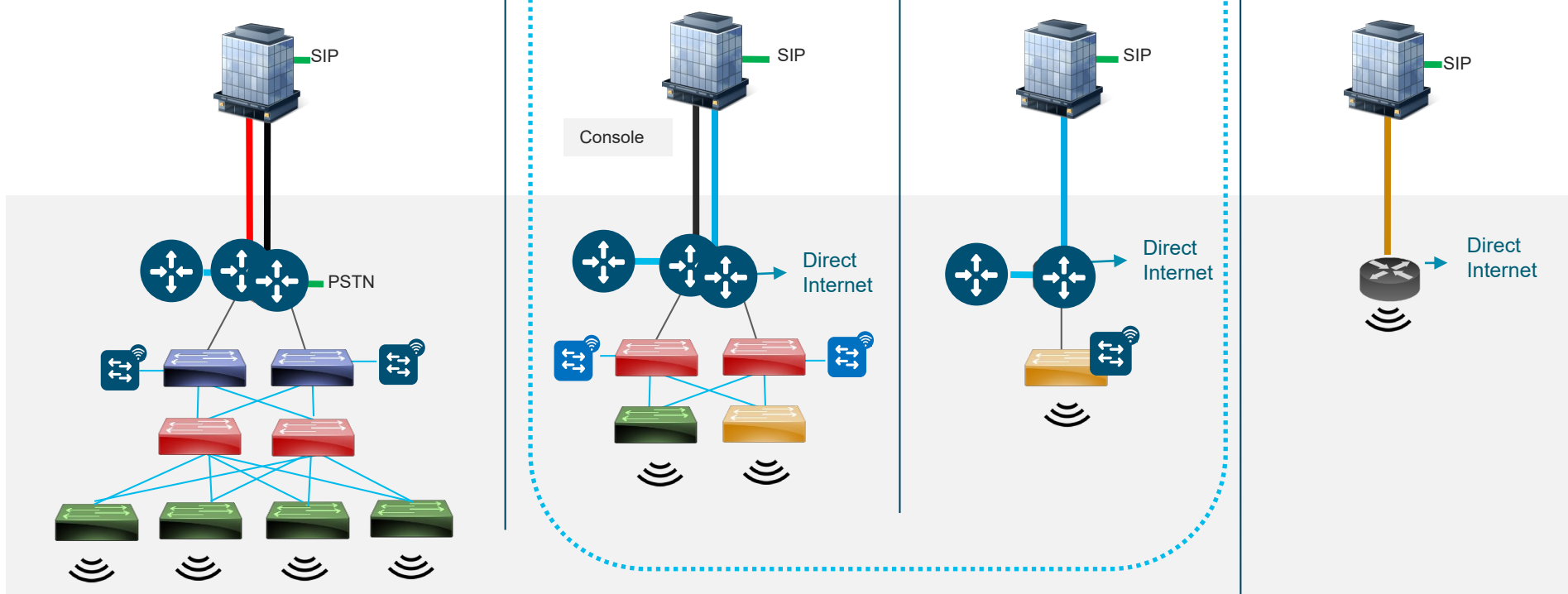
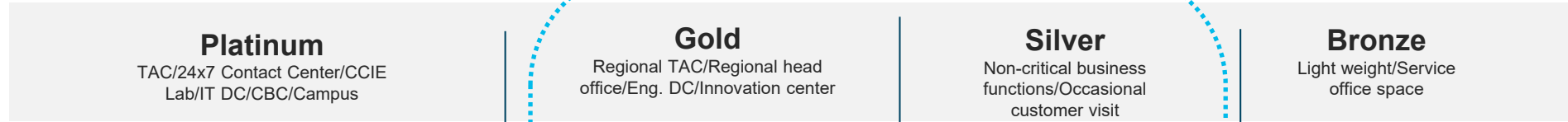
Cisco IT – Current Code Snapshot

Catalyst 9K	16.12.2s
ISR4451	16.12.2r IOS-XE SD-WAN
Wireless	8.10.105.0 (AireOS) & 16.12.2s (9800)
Cisco DNA-Center	1.3.1.4
Identity Services Engine	2.6 Patch 1
vManage	19.2.1

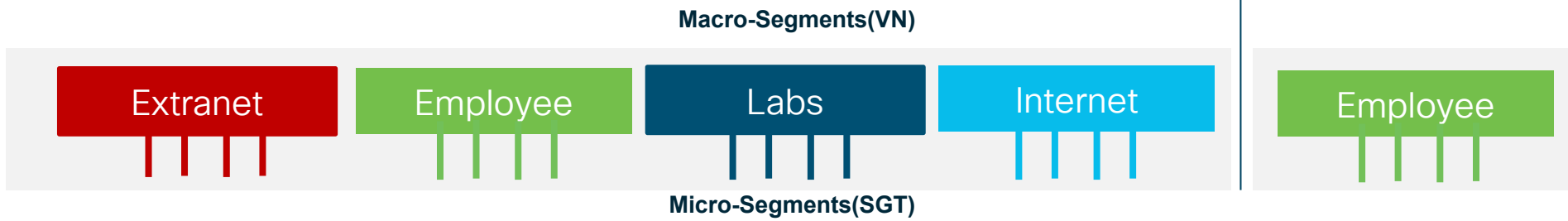
Our DNA-Ready Topology and Catalogue

- █ Private Line (2nd SP)
- █ MPLS / Private Line
- █ Internet (DIA)
- █ Landlord Internet

Business requirement



- 9500
- 9404/7
- 9300
- 4451
- WLC3504
- 9800
- 4800
- Meraki

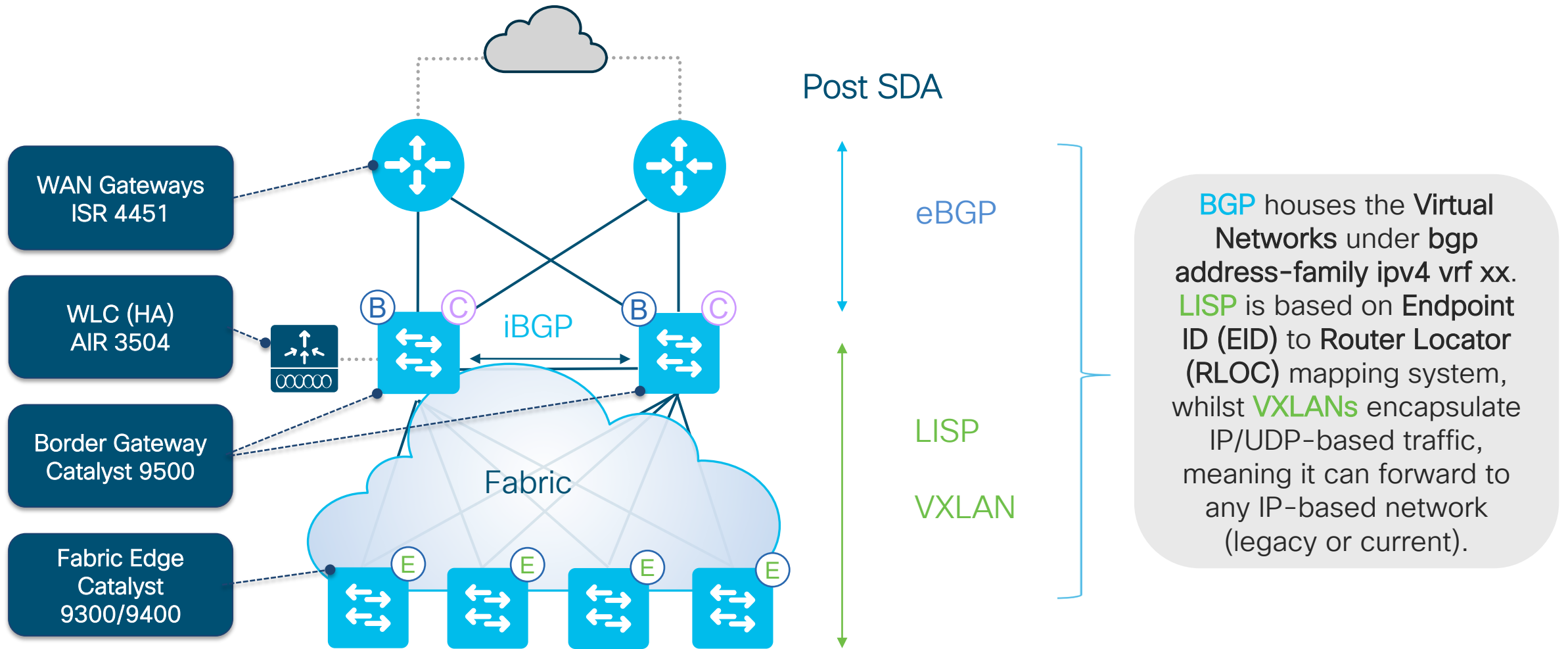


Current Target

Overlay Segments

Mapping Topologies to SDA

Our Outcome (Gold)



DNA Center Use Cases

DNA 0 PnP install (6 devices)

- Manual
- Auto

Manual

1. Console to device
2. Upload new image
3. Copy to redundant supervisor
4. Reload switch
5. Upload config
6. Save config > operational
7. Repeat for 6 devices

Time to complete operation: **480 mins**
(Day's work)

DNA-C Automation

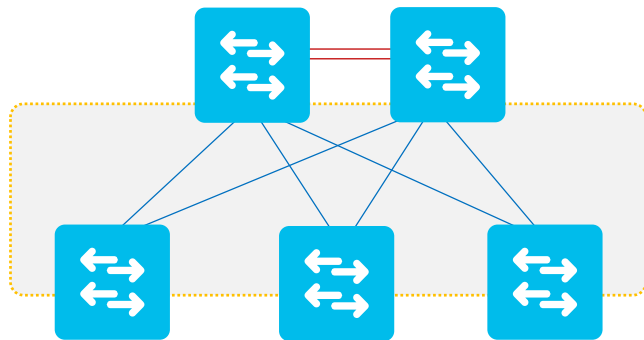
1. Device connects to DNA-C
2. Admin claims devices
3. Image is copied to devices & redundant supervisors
4. Switch reloads and reconnects to DNA-C
5. DNA-C upload latest configuration templates to devices
6. Save config > operational

Time to complete operation: **45 mins**

LAN Automation

LAN Automation builds a prescriptive, best-practice underlay for the SD-Access network using IS-IS routing.

2 Tier - Collapsed Core Design



Layer	Role	Switch
Distribution	Seed	Catalyst 9500
Access	PnP Agent	Catalyst 9300

Seed Device (Border Nodes)

- DNA-C needs IP connectivity & SSH access to seed devices, hence some initial configuration is required

PnP Agent (Edge Nodes)

- Fresh out-of-the-box switches that are running factory default config. *Needs to be sitting at initial configuration prompt in order for the PnP Agent to be running:*

```
%INIT: waited 0 seconds for NVRAM to be available
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
```

SWIM

DEVICES (7)

FOCUS: **Software Images** ▾

📍 Global

Take a Tour



DEVICE TYPE All Routers **Switches** APs WLCs

REACHABILITY **All** Reachable Unreachable

Filter | ● Add Device Tag Device Actions ▾ ⓘ

Last updated: 11:30 AM

<input type="checkbox"/>	Device Name ▲	IP Address	Device Family	Site	Reachability	Software Image	Image Version	Update Status	Provision Status	⋮
<input type="checkbox"/>	bdlk10-beta-sd-sw1.cisco.com GOLD, gold-sw-9400, SDA	10.230.127.165	Switches and Hubs (WLC Capable)	.../BDLK/BDLK10-BETA	✔ Reachable	cat9k_iosxe.16.12.02s.SP.	16.12.2s	Activation Success	Success See Details ⚠ Out of Date	
<input type="checkbox"/>	bdlk10-beta-sd-sw2.cisco.com GOLD, gold-sw-9400, SDA	10.230.127.164	Switches and Hubs (WLC Capable)	.../BDLK/BDLK10-BETA	✔ Reachable	cat9k_iosxe.16.12.02s.SP.	16.12.2s	Activation Success	Success See Details	
<input type="checkbox"/>	bdlk10-beta-sd-sw3.cisco.com GOLD, gold-sw-9300, SDA	10.230.127.171	Switches and Hubs (WLC Capable)	.../BDLK/BDLK10-BETA	✔ Reachable	cat9k_iosxe.16.12.02s.SP.	16.12.2s	Activation Success	Success See Details	
<input type="checkbox"/>	bdlk10-beta-sd-sw4.cisco.com GOLD, gold-sw-9300, SDA	10.230.127.170	Switches and Hubs (WLC Capable)	.../BDLK/BDLK10-BETA	✔ Reachable	cat9k_iosxe.16.12.02s.SP.	16.12.2s	Activation Success	Success See Details	
<input type="checkbox"/>	bdlk10-beta-sdbb-gw1.cisco.com GOLD, gold-9500, SDA, SXP	10.230.126.3	Switches and Hubs (WLC Capable)	.../BDLK/BDLK10-BETA	✔ Reachable	cat9k_iosxe.16.12.02s.SP.	16.12.2s	Activation Success	Success See Details	
<input type="checkbox"/>	bdlk10-beta-sdbb-gw2.cisco.com GOLD, gold-9500, SDA, SXP	10.230.126.4	Switches and Hubs (WLC Capable)	.../BDLK/BDLK10-BETA	✔ Reachable	cat9k_iosxe.16.12.02s.SP.	16.12.2s	Activation Success	Success See Details	
<input type="checkbox"/>	bdlk10-pnplab-9300-1.cisco.com	10.209.71.70	Switches and Hubs	.../BDLK/BDLK09	✔ Reachable	cat9k_iosxe.16.09.03.SP... ✔ Needs Update	16.9.3	Distribution Pending	Failed See Details	



SD-WAN Use Cases

Config Management – Feature Templates

Cisco vManage

CONFIGURATION | TEMPLATES

Device Feature

+ Add Template

Template Type: Non-Default

Search: GOLD

Total Rows: 42 of 77

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
GOLD_WAN_interface_Biz-Internet_2...	Gold EMEA WAN interface - Biz-Inter...	WAN Edge Interface	ISR4451-X	2	1	deasande	07 Dec 2019 8:00:37 PM GMT	...
GOLD_Loopback_VRF3_2_1_2	Loopback3 interface for Internet VRF	WAN Edge Interface	ISR4451-X	2	2	deasande	05 Dec 2019 11:44:30 AM GMT	...
GOLD_Service_Physical_Int_Crosslink...	Config for service interface	WAN Edge Interface	ISR4451-X	4	2	deasande	07 Dec 2019 7:59:11 PM GMT	...
GOLD_WAN_interface_GW2_MPLS_2...	Gold EMEA WAN interface - MPLS for...	WAN Edge Interface	ISR4451-X	0	0	deasande	07 Dec 2019 7:57:01 PM GMT	...
GOLD_Physical_Management_2_1_2	Shuts down the physical Gig0 interfa...	WAN Edge Interface	ISR4451-X	4	2	deasande	05 Dec 2019 11:53:43 AM GMT	...
GOLD_VPN1_2_1_2	Config for VPN 1	WAN Edge VPN	ISR4451-X	4	2	deasande	07 Dec 2019 7:57:41 PM GMT	...
GOLD_VPN0_GW2_2_1_2	Config for VPN 0 with public DNS	WAN Edge VPN	ISR4451-X	1	1	deasande	05 Dec 2019 11:52:48 AM GMT	...
GOLD_Service_Interface_Crosslink1...	Config for service side LAN interface	WAN Edge Interface	ISR4451-X	2	1	deasande	05 Dec 2019 11:54:38 AM GMT	...
SDWAN_TMPL_TPT_L2VPN_GOLD...	SDWAN template for L2VPN on WAN...	WAN Edge Interface	C1111-4PLTEEA C1117-4P ISR4331...	0	0	kjawaid	07 Apr 2019 6:05:03 PM BST	...
GOLD_WAN_interface_MPLS2_physic...	GW2 Gold EMEA WAN interface - MP...	WAN Edge Interface	ISR4451-X	0	0	deasande	05 Dec 2019 11:46:27 AM GMT	...
GOLD_BGP_Internet-VRF3_2_1_2	BGP config for beta sites - _Internet-V...	BGP	ISR4451-X	0	0	deasande	05 Dec 2019 11:56:06 AM GMT	...
GOLD_WAN_interface_DIA_TLOC-EXT...	Gold EMEA WAN interface - DIA TLO...	WAN Edge Interface	ISR4451-X	0	0	deasande	05 Dec 2019 11:54:00 AM GMT	...
GOLD_Internet_SVL_g0-0-1_2_1_2	Sub-interface for Internet Handoff	WAN Edge Interface	ISR4451-X	2	2	deasande	07 Dec 2019 8:04:29 PM GMT	...
GOLD_Service_Physical_Int_Crosslink...	PnP Sub interface for g0/0/1.1 interf...	WAN Edge Interface	ISR4451-X	1	0	deasande	05 Dec 2019 11:50:48 AM GMT	...
GOLD_VPN3_2_1_2	Internet VN	WAN Edge VPN	ISR4451-X	2	2	deasande	05 Dec 2019 11:44:10 AM GMT	...
SDWAN_TMPL_SVC_VPN_1_GOLD_SI...	SDWAN Service VPN 1 (Corporate VP...	WAN Edge VPN	ISR4451-X	0	0	kjawaid	07 Apr 2019 3:07:37 PM BST	...
GOLD_WAN_interface_private1_physi...	Gold EMEA WAN interface - Private1- ...	WAN Edge Interface	ISR4451-X	2	1	deasande	05 Dec 2019 11:46:07 AM GMT	...
GOLD_NTP_2_1_2	NTP for beta sites	NTP	ISR4451-X	3	2	deasande	05 Dec 2019 11:51:07 AM GMT	...
GOLD_Service_Physical_Int_Crosslink...	Config for service interface with IP a...	WAN Edge Interface	ISR4451-X	1	0	deasande	07 Dec 2019 7:57:21 PM GMT	...
GOLD_Loopback_VRF1_2_1_2	Loopback interface in VRF 1	WAN Edge Interface	ISR4451-X	4	2	deasande	07 Dec 2019 8:04:08 PM GMT	...
GOLD_WAN_interface_MPLS2_TLOC...	Gold EMEA WAN interface - MPLS TL...	WAN Edge Interface	ISR4451-X	0	0	deasande	05 Dec 2019 11:46:43 AM GMT	...
GOLD_Service_Physical_Int_Crosslink...	Config for service interface	WAN Edge Interface	ISR4451-X	4	2	deasande	05 Dec 2019 11:55:13 AM GMT	...
GOLD_Internet_SVL_g0-0-0_2_1_2	Sub-interface for Internet Handoff	WAN Edge Interface	ISR4451-X	2	2	deasande	05 Dec 2019 11:47:01 AM GMT	...
GOLD_WAN_interface_private1_TLOC...	Gold EMEA WAN interface - Private1 ...	WAN Edge Interface	ISR4451-X	2	1	deasande	05 Dec 2019 11:45:33 AM GMT	...
GOLD_WAN_interface_MPLS2_TLOC...	Gold EMEA WAN interface - MPLS TI...	WAN Edge Interface	ISR4451-X	0	0	deasande	05 Dec 2019 11:45:17 AM GMT	...

Centralised Policy

Cisco vManage | CONFIGURATION | POLICIES | Centralized Policy > Application Aware Routing Policy > View Application Aware Route Policy

Name: Policy_AAR_EMEAR
Description: Policy_AppRouting_EMEAR

App Route

Application Route

Match Conditions	Actions
<p>1</p> <p>Application/Application Family List: List_App_VoiceVideo</p> <p>DSCP: 32 34 36 38 40 46 48</p>	<p>SLA Class: List List_SLA_Voice-Video</p> <p>Preferred Color: private1</p>
<p>2</p> <p>DSCP: 0</p>	<p>SLA Class: List List_SLA_Default</p> <p>Preferred Color: private1 biz-internet</p>
<p>3</p> <p>Application/Application Family List: List_App_Scavenger</p> <p>DSCP: 8</p>	<p>SLA Class: List List_SLA_Scavenger</p> <p>Preferred Color: biz-internet</p>

List_App_Scavenger Entries

- amazon-s3
- netflix
- megavideo
- fox-news
- espn-browsing
- cbs

Question!

What about a full end-to-end
Use Case?

The Fabric-in-a-Box Use Case Story (Silver Topology)

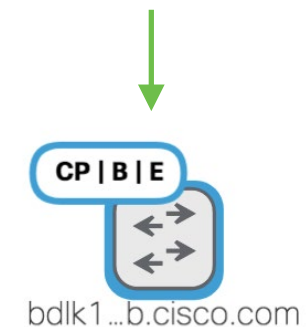
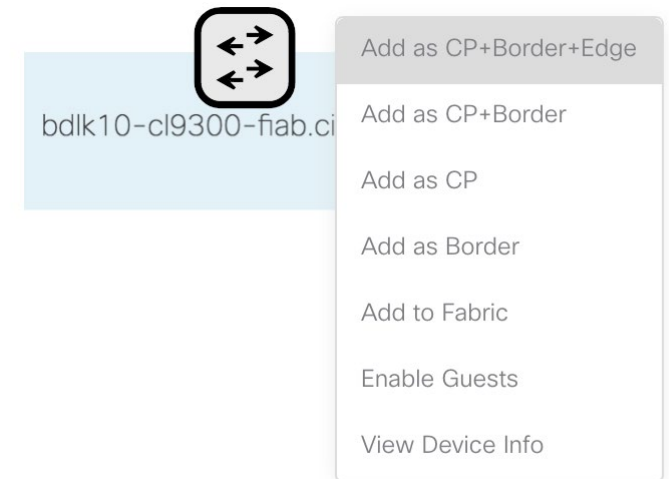


Mapping Topologies to SDA

Fabric-in-a-Box (FIAB) – Silver Topology

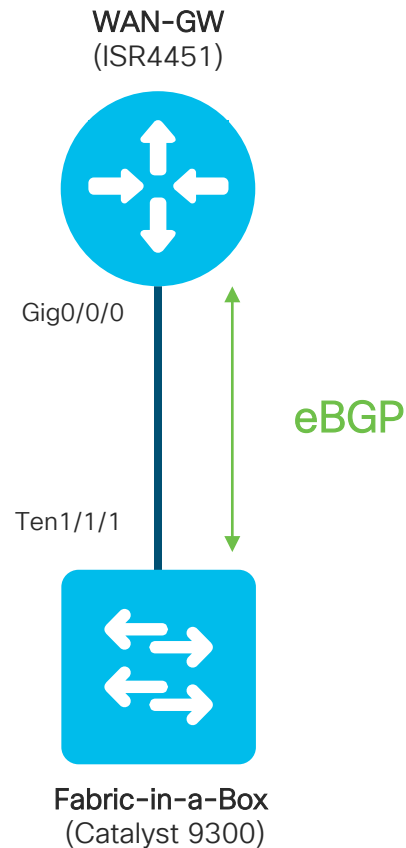
- 1 Device can be the Edge (E), Border (B), and Control Plane (CP) node simultaneously
- 2 Enable Embedded Wireless for collapsed solution on Catalyst 9300 (stack for redundancy)
- 3 However – No other additional fabric devices are required or permitted
- 4 As per our topologies, this fits into Silver Site Design (DIA only)

Cisco DNA Center Provision > Fabric View



The Fabric-in-a-Box Use Case

FIAB SDA Turn-Up - Basic Underlay Configuration (Pre-SDA)



WAN Gateway (ISR4451)

```
interface Loopback0
ip address x.x.x.x 255.255.255.255
!
interface GigabitEthernet0/0/1
description to 9300 Fabric-in-a-Box
no ip address
negotiation auto
!
interface GigabitEthernet0/0/1.2011
encapsulation dot1Q 2011
ip address x.x.x.x 255.255.255.252
!
router bgp 65111
bgp router-id Loopback0
bgp log-neighbor-changes
neighbor x.x.x.x remote-as 65112 <- eBGP to 9300
!
address-family ipv4
network x.x.x.x mask 255.255.255.252 <- p2p to 9300
neighbor x.x.x.x activate
neighbor x.x.x.x default-originate
default-information originate
exit-address-family
!
```

Fabric-in-a-Box (Catalyst 9300 - Post PnP)

```
interface Loopback0
ip address x.x.x.x 255.255.255.255
!
interface TenGigabitEthernet1/1/1 <- physical link to WAN
description to cEdge ISR4451
switchport trunk allowed 2011
switchport mode trunk
!
interface Vlan2011 <- underlay SVI
ip address x.x.x.x 255.255.255.252
!
router bgp 65112
bgp router-id interface Loopback0
bgp log-neighbor-changes
neighbor x.x.x.x remote-as 65111 <- eBGP to WAN
!
address-family ipv4
network x.x.x.x mask 255.255.255.252 <- p2p to WAN
network x.x.x.x mask 255.255.255.255
redistribute connected
neighbor x.x.x.x activate
exit-address-family
!
```

The Fabric-in-a-Box Use Case

FIAB SDA Turn-Up - Discovery and Assignment

1 Discover device

The screenshot shows the 'Discovery' interface. At the top, it says 'bdlk switch fiab' with a 'Completed' status and '1 Reachable Devices' in 00h:00m:05s. A large green circle with the number '1' and the text 'Devices' is prominent. Below this, a legend shows 'Success(1)', 'Unreachable(0)', and 'Discarded(0)'. A table lists the discovered device:

IP Address	Device Name	Status	ICMP	SNMP	CLI
10.209.68.194	bdlk10-cl9300-fiab.cisco.com	Success	Success	Success	Success

Discovery Details:

CDP Level	None	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	300 second(s)	IP Address/Range	10.209.68.194-10.209.68.194

2 Provision and Assign Device to Site

The screenshot shows the 'Provision and Assign Device to Site' interface. A dropdown menu is open over a table, showing options: 'Assign Device to Site', 'Provision', 'Resync', 'Delete Device', and 'Update OS Image'. The table has columns for 'Device Name', 'Device Family', 'IP Address', and 'Site'. A row is selected with a checkmark in the 'Tags' column:

Device Name	Device Family	IP Address	Site
bdlk10-cl9300-fiab.cisco.com	Switches and Hubs	10.209.68.194	...isc... FIAB

The Fabric-in-a-Box Use Case

FIAB SDA Turn-Up - Define your Network Settings

3 Define Network Settings

AAA Server

Network Client/Endpoint

NETWORK

Servers

ISE AAA

Protocol

RADIUS TACACS

IP Address (Primary)

Select... +

DHCP Server

DHCP

IP Address +

Additional DHCP

IP Address +

DNS Server •

Domain Name

cisco.com

Primary

IP Address

Secondary

IP Address

4 Define Addressing Schema

IP Address Pools (6)

[Filter](#)

Name	IP Subnet Mask	Type	Global IP Pool	Gateway
BDLK-FIAB-AP	10.209.68.248/29	LAN	BDLK-FIAB-CiscoLiveP...	10.209.68.249
BDLK-FIAB-EMPLOYEE	10.209.68.208/28	LAN	BDLK-FIAB-CiscoLiveP...	10.209.68.209
BDLK-FIAB-GUEST	10.209.68.224/28	LAN	BDLK-FIAB-CiscoLiveP...	10.209.68.225
BDLK-FIAB-UNDERLAY	10.209.68.192/28	LAN	BDLK-FIAB-CiscoLiveP...	10.209.68.193

The Fabric-in-a-Box Use Case

FIAB SDA Turn-Up - Host Onboarding Pre-SDA Push

5 Define Host Onboarding

BDLK10 FIAB FABRIC

Fabric Infrastructure Host Onboarding

For each site assign at least 1 Control Plane and 1 Edge node. If...

Select Authentication Template
Select the default host authentication template. This will be applied to all sites.

Closed Authentication Open Authentication Easy Con...

Virtual Networks

EMPLOYEE INFRA_VN LAB
INTERNET

Edit Virtual Network: EMPLOYEE

Select an IP Pool and Traffic Type to associate it with the selected VN. Layer-2 Extension and Policy Group are optional.

1 Selected

IP Pool Name	Traffic Type	Address Pool	Layer-2 Extension	Layer-2 Flooding	Groups	Critical Pool	Auth Policy
<input type="checkbox"/> BDLK-FIAB-AP	Choose Traffic	10.209.68.248/29	<input type="checkbox"/> On	<input type="checkbox"/> Off	Choose Group	<input type="checkbox"/>	
<input checked="" type="checkbox"/> BDLK-FIAB-EMPLOYEE	Data	10.209.68.208/28	<input type="checkbox"/> On	<input type="checkbox"/> Off	Choose Group	<input type="checkbox"/>	Employee
<input type="checkbox"/> BDLK-FIAB-GUEST	Choose Traffic	10.209.68.224/28	<input type="checkbox"/> On	<input type="checkbox"/> Off	Choose Group	<input type="checkbox"/>	

The Fabric-in-a-Box Use Case

FIAB SDA Turn-Up - Scalable Group Tag/Contract Creation

6 Define SGTs (If req.)

The screenshot displays the Cisco SD-WAN GUI for configuring a Virtual Network. The main interface is titled "Virtual Network" and includes a search bar for "Find Virtual Network" and a list of existing networks: DEFAULT_VN (269), INFRA_VN (0), and DATA (4). The "DATA (4)" network is selected, and the "Available Scalable Groups" section shows a grid of group icons (AC, AD, AP, AB, AK, AL, AO, AH) with their respective descriptions. The "Groups in the Virtual Network" section shows a list of selected groups: CE (Cisco_Employee...), IP (IPT_UC_V_ENDP...), WE (Engine ring), and WI (IT). The "Extranet - Details" dialog box is open, showing the configuration for the "Engine ring" group. It includes a "Sources" field with "Engineering", a "Contract" field with "Name : deny" and "Implicit Action : DENY", and a "Destinations" field with "IT".

Dashboard | Group-Based Access Control | IP Based Access Control | Application | Traffic Copy | **Virtual Network**

Find Virtual Network +

Create or Modify Virtual Network by selecting Available Scalable Groups. [Reset] [Save]

Virtual Network Name*
DATA

Guest Virtual Network

Available Scalable Groups

Find Scalable Show Unsele... ▾

AC AD AP AB
ACS_Server ADAM APEG_PowerKey... Abraxas...

AK AL AO AH

Groups in the Virtual Network

Find Scalable

CE IP WE WI
Cisco_Employee... IPT_UC_V_ENDP... Engine ring IT

Extranet - Details ×

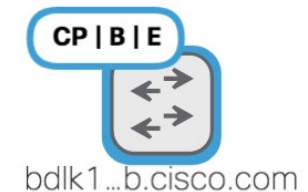
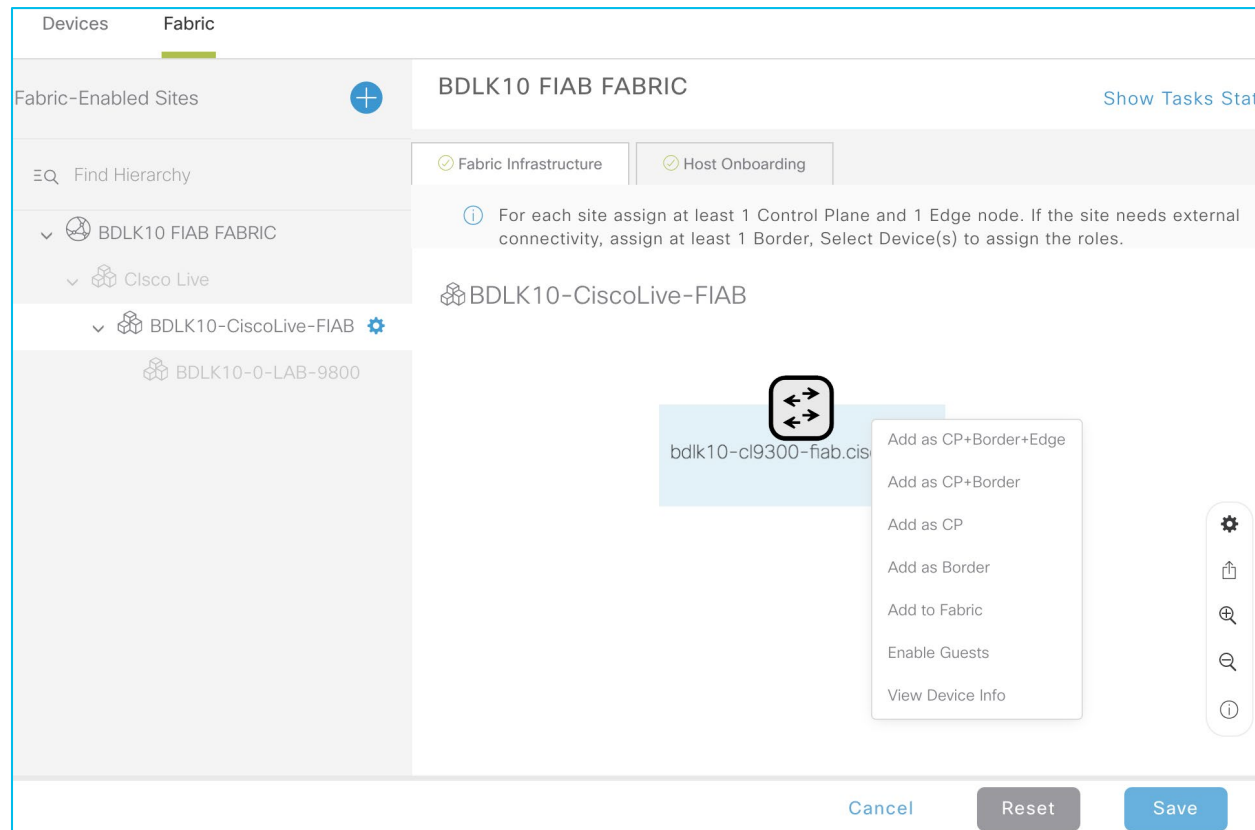
Sources	Contract	Destinations
Engineering	Name : deny Implicit Action : DENY	IT

[Cancel] [Edit]

The Fabric-in-a-Box Use Case

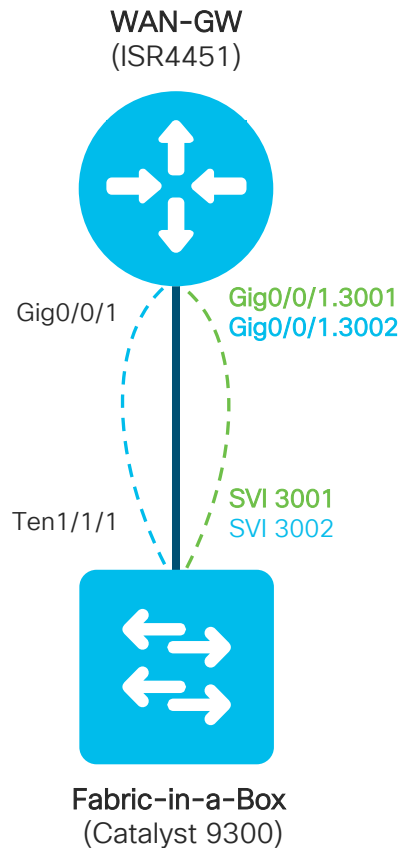
FIAB SDA Turn-Up - Fabric Push

6 Select CP, Border, and Edge Roles / Save to Complete



The Fabric-in-a-Box Use Case

FIAB SDA Turn-Up - A Look Under The Hood Post Push (Post-SDA)



Fabric-in-a-Box (Catalyst 9300)

BGP Configuration Snippet for EMPLOYEE/INTERNET

```
...
address-family ipv4
  bgp aggregate-timer 0
  network x.x.x.x mask 255.255.255.255
  redistribute connected
  redistribute lisp metric 10
  neighbor x.x.x.x activate
  exit-address-family
!
address-family ipv4 vrf EMPLOYEE
  bgp aggregate-timer 0
  network x.x.x.x mask 255.255.255.255
  network x.x.x.x mask 255.255.255.240
  aggregate-address x.x.x.x 255.255.255.240 summary-only
  redistribute lisp metric 10
  neighbor x.x.x.x remote-as 65111
  neighbor x.x.x.x update-source Vlan3001
  neighbor x.x.x.x activate
  neighbor x.x.x.x weight 65535
  exit-address-family
!
address-family ipv4 vrf INTERNET
  bgp aggregate-timer 0
  network x.x.x.x mask 255.255.255.240
  aggregate-address x.x.x.x 255.255.255.240 summary-only
  redistribute lisp metric 10
  neighbor x.x.x.x remote-as 65111
  neighbor x.x.x.x update-source Vlan3002
  neighbor x.x.x.x activate
  neighbor x.x.x.x weight 65535
  exit-address-family
```

Fabric-in-a-Box (Catalyst 9300)

LISP Configuration Snippet for EMPLOYEE

```
...
instance-id 4099
  remote-rloc-probe on-route-change
  dynamic-eid Employee
  database-mapping x.x.x.x/28 locator-set rloc_xxx
  exit-dynamic-eid
!
  service ipv4
  eid-table vrf EMPLOYEE
  map-cache 0.0.0.0/0 map-request
  route-export site-registrations
  distance site-registrations 250
  map-cache site-registration
  exit-service-ipv4
!
  exit-instance-id
!
instance-id 8190
  remote-rloc-probe on-route-change
  service ethernet
  eid-table vlan 1023
  database-mapping mac locator-set rloc_xxx
  exit-service-ethernet
!
  exit-instance-id
```

The Fabric-in-a-Box Use-Case

FIAB SDA Turn-Up - How to Verify Macro/Micro Verifications

IT User

```
bdlk10-cl9300-fiab#show access-session interface tenGigabitEthernet 1/0/1 det
  Interface: TenGigabitEthernet1/0/1
  IIF-ID: 0x16ADC532
  MAC Address: 0050.56bd.e6ee
  IPv6 Address: fe80::2c14:3033:54e7:b2b8
  IPv4 Address: x.x.x.x
  User-Name: host/JAMIE-0855A
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: C644D10A000000C970B267B1
  Acct Session ID: 0x0000c37f
  Handle: 0xff00002c
  Current Policy: PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
```

Server Policies:

Vlan Group: Vlan: 1023
SGT Value: 16

ENG User

```
bdlk10-cl9300-fiab#show access-session interface tenGigabitEthernet 1/0/2 det
  Interface: TenGigabitEthernet1/0/2
  IIF-ID: 0x171F0D4F
  MAC Address: 0050.56bd.e2ca
  IPv6 Address: fe80::650d:fdb1:5929:b1af
  IPv4 Address: x.x.x.x
  User-Name: host/CALLUM-0843A
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: C644D10A000000CB70B3BD09
  Acct Session ID: 0x0000035e
  Handle: 0x3900002e
  Current Policy: PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
```

Server Policies:

Vlan Group: Vlan: 1023
SGT Value: 17

Question!

What about the (SD-)WAN?

What did we learn on SDA <> SDWAN Hand-off?

Key Configurations

Hand-off at the cEdge 4451 Side (SDWAN)

```
bdlk10-cl4331-fiab#show run int gi0/0/1
interface GigabitEthernet0/0/1
description to bdlk10-cl9300-fiab te1/1/1
mtu 9100
no ip address
negotiation auto
```

```
bdlk10-cl4431-fiab#show run int g0/0/1.3001
interface GigabitEthernet0/0/1.3001
description Employee-VRF
encapsulation dot1Q 3001
vrf forwarding 1
ip address x.x.x.x 255.255.255.252
ip mtu 1496
```

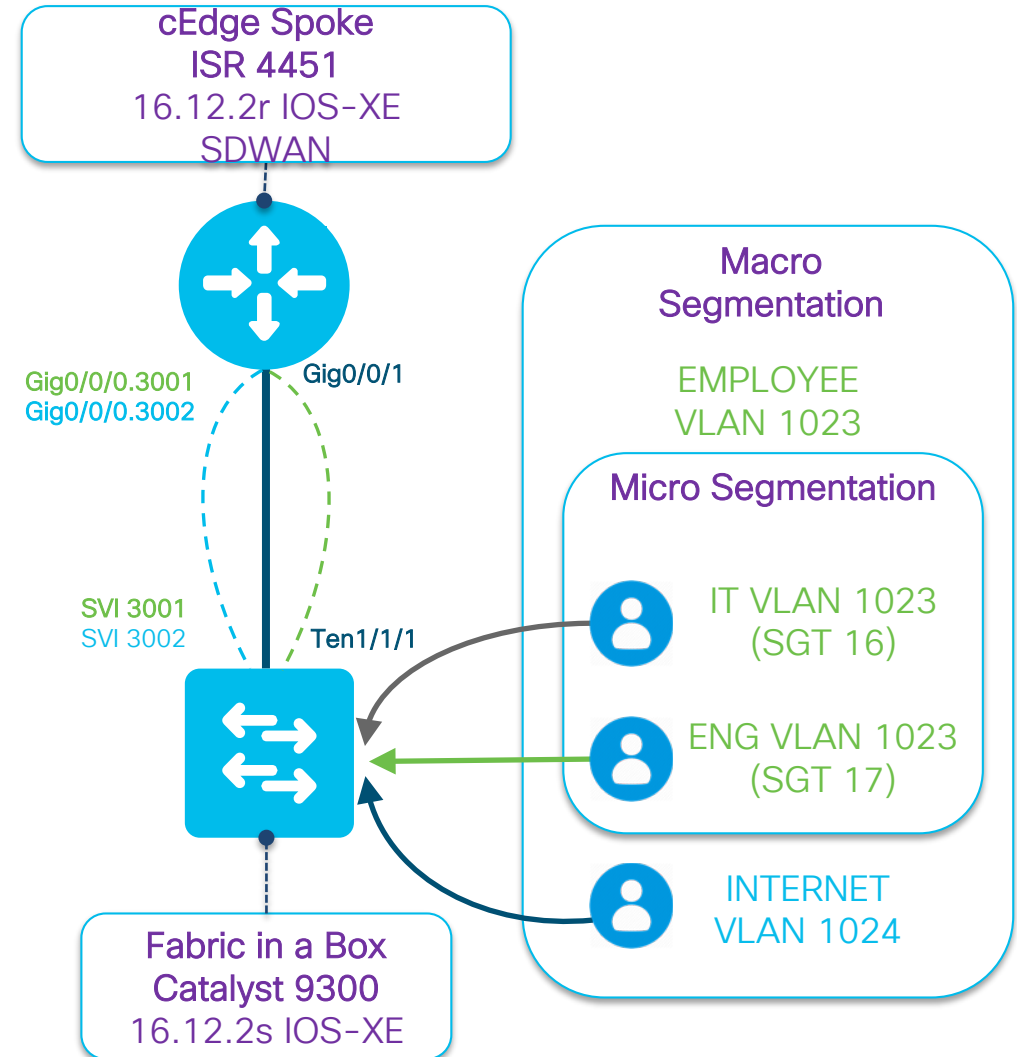
```
bdlk10-cl4331-fiab#show run int g0/0/1.3002
interface GigabitEthernet0/0/1.3002
description Internet/Guest-VRF
encapsulation dot1Q 3002
vrf forwarding 3
ip address x.x.x.x 255.255.255.252
ip mtu 1496
```

Hand-off at the FIAB 9300 Side (SDA)

```
bdlk10-cl9300-fiab#show run int te1/1/1
interface TenGigabitEthernet1/1/1
description bdlk10-cl4331-fiab gig0/0/1
switchport trunk allowed vlan 1,2011,3001,3002
switchport mode trunk
```

```
bdlk10-cl9300-fiab#show run int vlan 3001
interface Vlan3001
description vrf interface to External router
vrf forwarding EMPLOYEE
ip address x.x.x.x 255.255.255.252
no ip redirects
ip route-cache same-interface
```

```
bdlk10-cl9300-fiab#show run int vlan 3002
interface Vlan3002
description vrf interface to External router
vrf forwarding INTERNET
ip address x.x.x.x 255.255.255.252
no ip redirects
ip route-cache same-interface
```



What did we learn on SDA <> SDWAN Hand-off?

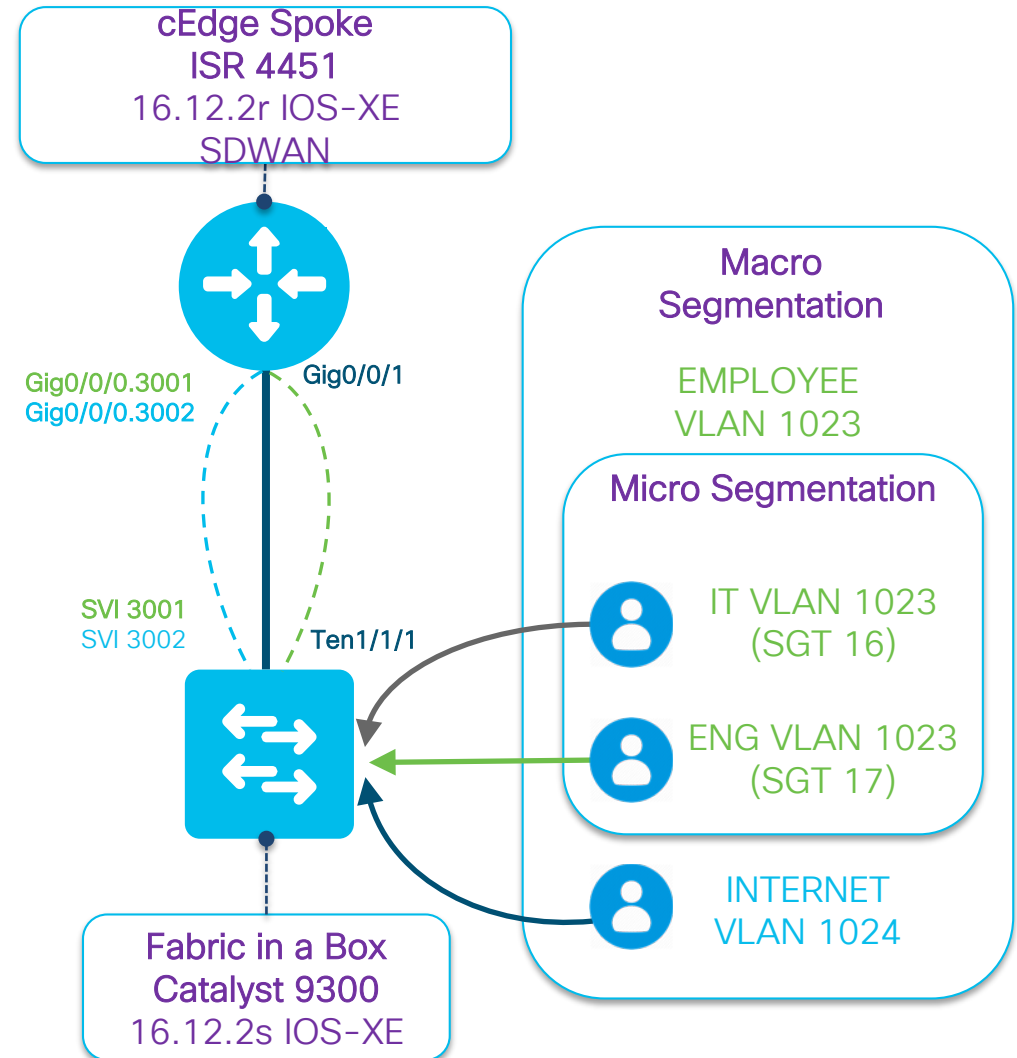
Key Configurations Cont.

cEdge 4451 Side (SDWAN) (vManage Templates)

```
router bgp 65111
...
!
address-family ipv4
network x.x.x.x mask 255.255.255.252
redistribute eigrp 109
neighbor x.x.x.x activate
neighbor x.x.x.x default-originate
default-information originate
exit-address-family
!
address-family ipv4 vrf 1
redistribute omp metric 1000
neighbor 10.209.69.129 remote-as 65112
neighbor 10.209.69.129 activate
neighbor 10.209.69.129 default-originate
exit-address-family
!
address-family ipv4 vrf 3
redistribute omp metric 1000
neighbor 10.209.69.133 remote-as 65112
neighbor 10.209.69.133 activate
neighbor 10.209.69.133 default-originate
exit-address-family
```

cEdge 4451 Side (SDWAN)

```
sdwan
interface GigabitEthernet0/0/0 (ISP)
tunnel-interface
encapsulation ipsec
color private1
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
omp
no shutdown
graceful-restart
address-family ipv4 vrf 1
advertise bgp
!
address-family ipv4 vrf 3
advertise bgp
!
address-family ipv4
advertise bgp
advertise connected
advertise static
```

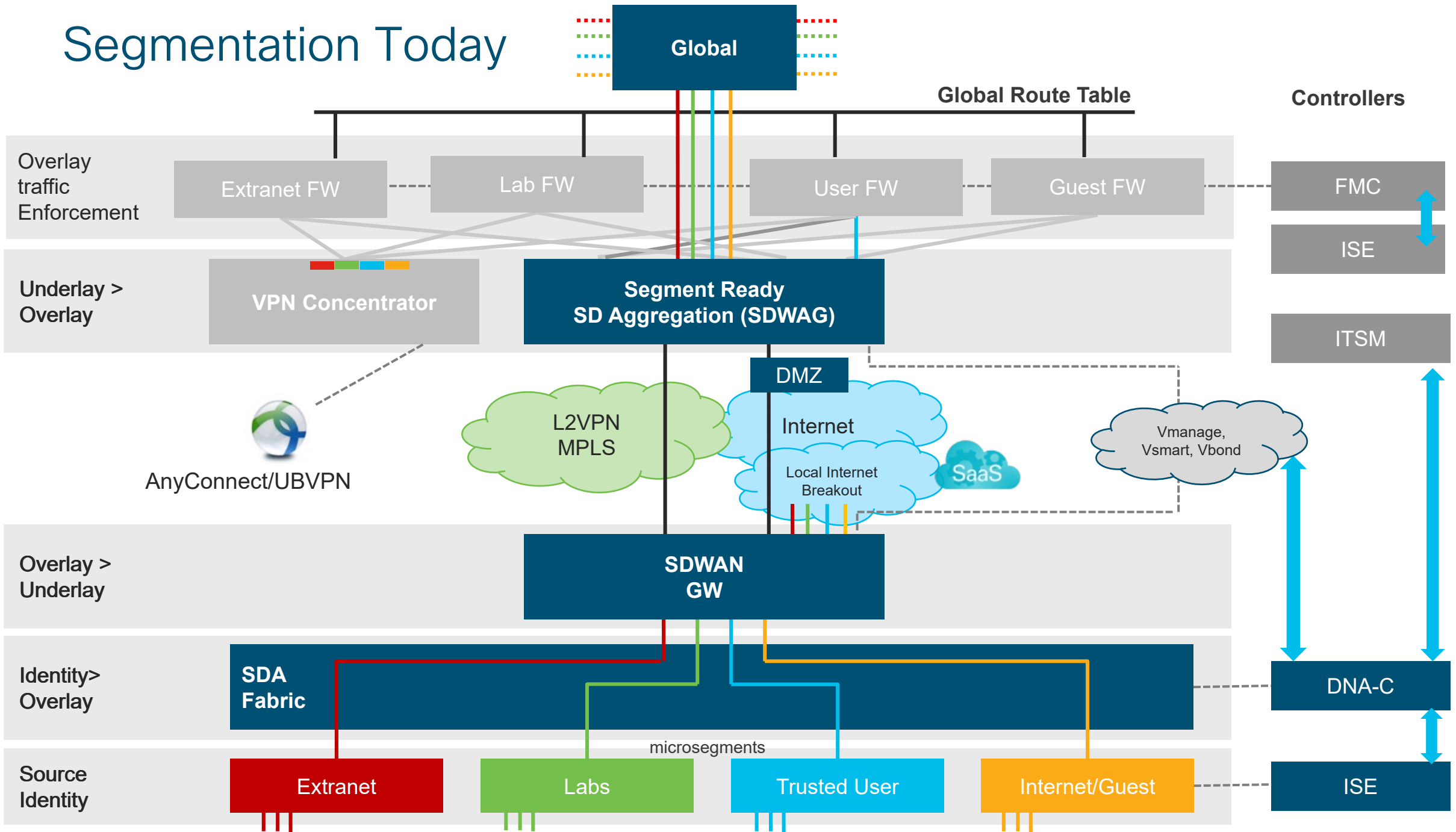


Part 3- Automation & Deployment

What's our progress?

Development	2 Beta Locations with full fabric
Hardware	147 Locations with DNA Ready hardware installed.
Segmentation	4 SD-WAN Hubs Segmentation ready
Full Fabric	2 Silver and 4 Gold Sites running full fabric – Many more to come!

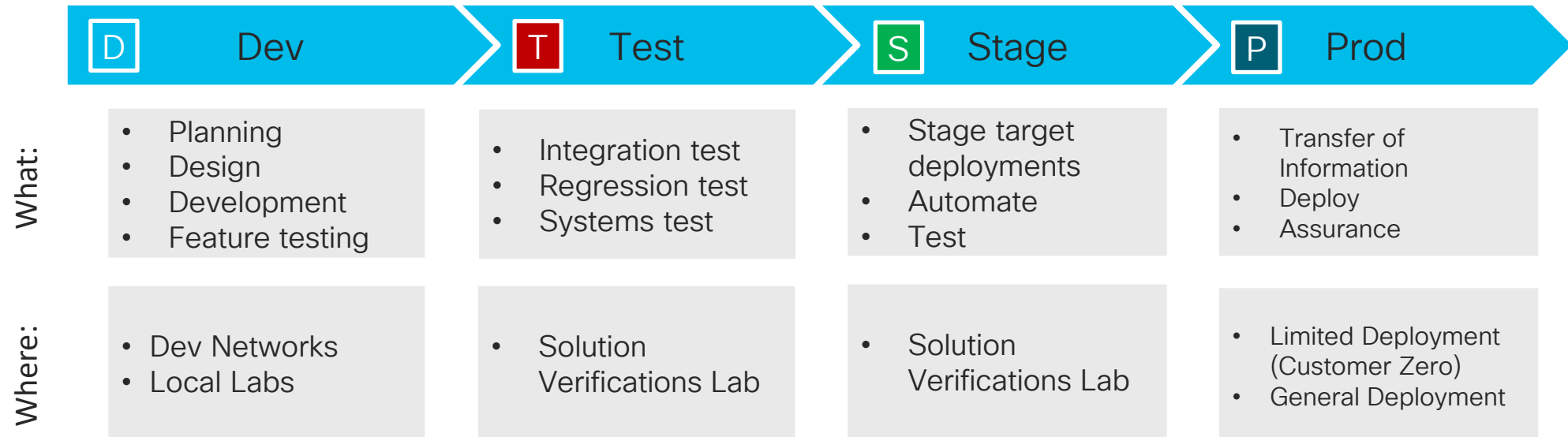
Segmentation Today



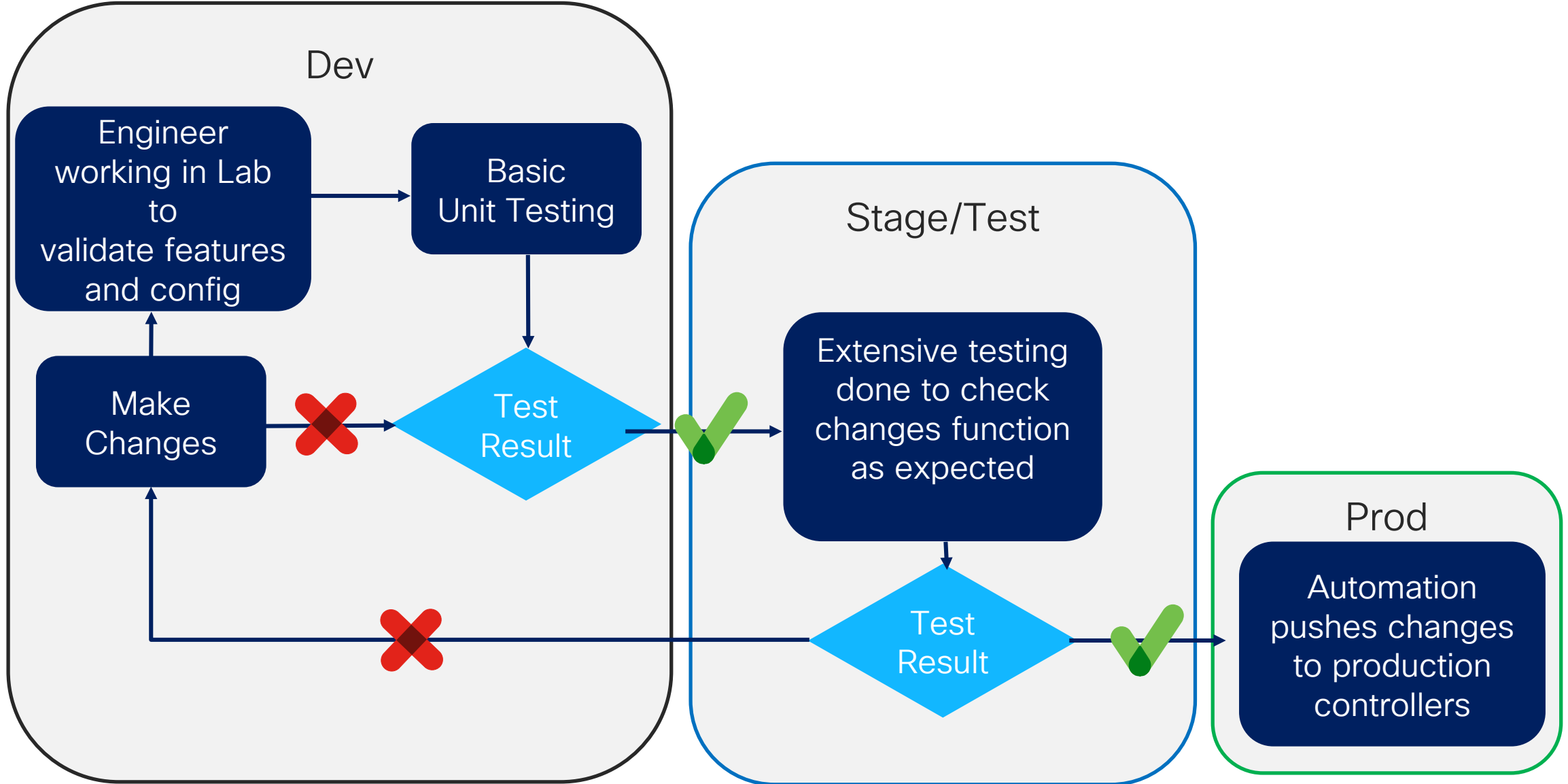
Development Lifecycle

The Requirement for A Deployment Lifecycle

Development through to Production



Cisco IT Development Lifecycle



CI/CD Workflow

- REST APIs are exposed by DNA-Center and vManage controllers for features like templates, policies, devices and sites management
- git, python+Flask, Jenkins and Docker are used to build micro-services with CI/CD pipeline
- Helps in building integrated solutions with different IT tools used for network operations



Jenkins



REST API using Flask



Configuration Management

Bitbucket Projects Repositories

gis-networking / network-standards

Source

master_dna_2_1 network-standards / standards / gold / vmanage /

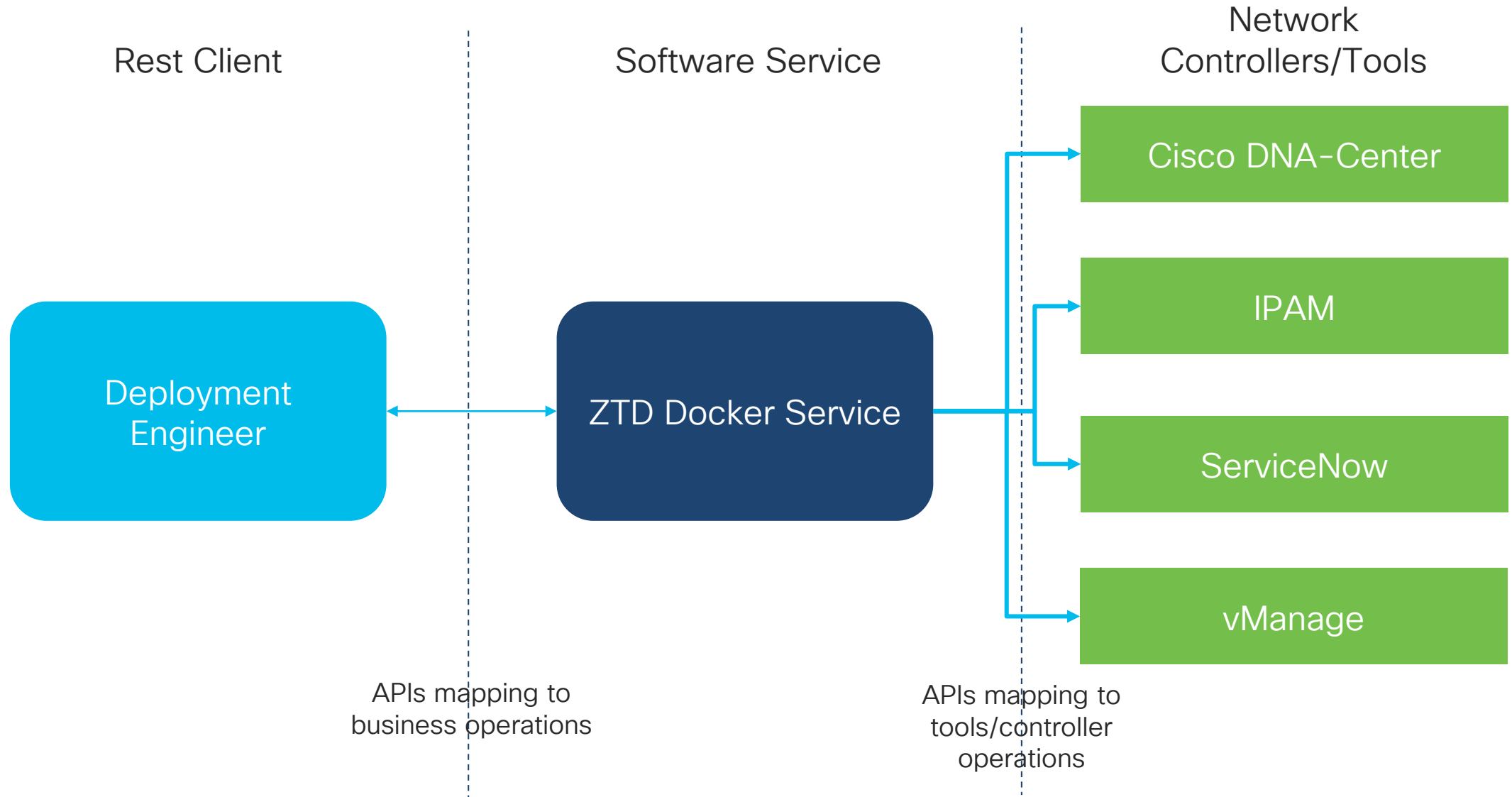
Source Description Last Modified

Source	Description	Last Modified
..		
cli		
DNA_AAA_2_1(aaa)	Gold templates for vManage 18.4.2	03 Oct 2019
DNA_BFD_2_1(bfd-vedge)	Gold templates for vManage 18.4.2	03 Oct 2019
DNA_IPSec_2_1(security-vedge)	Gold templates for vManage 18.4.2	03 Oct 2019
DNA_OMP_2_1(omp-vedge)	Gold templates for vManage 18.4.2	03 Oct 2019
DNA_PNP_DHCP_2_1(dhcp-server)	Gold templates for vManage 18.4.2	03 Oct 2019
DNA_SNMP_2_1(snmp)	Gold templates for vManage 18.4.2	03 Oct 2019
DNA_Syslog_2_1(logging)	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_Banner_2_1(banner)	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_BGP_Internet_VRF3_2_1(bgp)	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_BGP_Underlay_VRF1_2_1(bgp)	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_BGP_User_VRF2_2_1(bgp)	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_Internet_SVI_Crosslink1_2_1(vpn-vedge-interf...	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_Internet_SVI_Crosslink2_2_1(vpn-vedge-interf...	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_Loopback2_2_1(vpn-vedge-interface)	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_Loopback3_2_1(vpn-vedge-interface)	Gold templates for vManage 18.4.2	03 Oct 2019
GOLD_Loopback_VRF1_2_1(vpn-vedge-interface)	Gold templates for vManage 18.4.2	03 Oct 2019

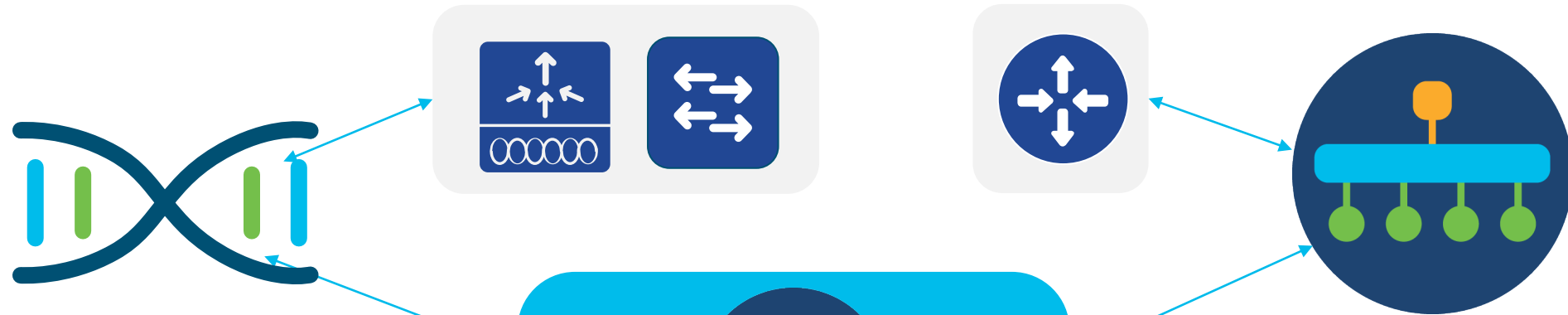
Question!

How do we use automation for our deployments?

ZTD Architecture



Service Integration



Cisco DNA Center

vManage

Cisco IT ZTD Docker Service



CISCO Live!



servicenow

DEMO: Cisco IT ZTD Docker Service

What's next?

- 1 SD-WAN Only
- 2 2.1.3 Fabric Deployments
- 3 Operationalize Assurance
- 4 Automation
- 5 Campus (Multi-Site)

Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



Meet the Engineer
1:1 meetings



Related sessions



Thank you





You make **possible**